Microsoft Technical Reference Guide for CMMC 2.0

ACCELERATE YOUR JOURNEY TO CMMC WITH THE MICROSOFT CLOUD

MARCH 2022

Introduction

The Cybersecurity Maturity Model Certification (CMMC) is a unifying standard for the implementation of cybersecurity across the United States Defense Industrial Base (DIB). The DIB encompasses the commercial organizations that produce or provide products and services to the United States Department of Defense (DoD). CMMC includes a comprehensive and scalable certification element to verify the implementation of controls associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the DoD that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

The Microsoft Technical Reference Guide for CMMC includes implementation statements for an organization pursuing CMMC, while leveraging relevant Microsoft services. This includes brief descriptions of relevant Microsoft services and products, and links to further implementation documentation. The guide focuses on CMMC Level 2 (L2). CMMC L2 includes all 110 controls from NIST SP 800-171. The intended audience are Government Personnel, Government Contractors, Managed Service Providers, Compliance Personnel, and IT Security Architects who are responsible for evaluating Microsoft services for controls alignment, and implementation to meet CMMC security requirements.

Notices

This Technical Reference Guide for CMMC provides customers with a resource to pursue CMMC compliance while leveraging Microsoft products and services— This Guide does not address security controls occurring outside of Microsoft products and services.

Please further note that the CMMC compliance standard has yet to be implemented to assess the suitability of in-scope entities' security controls and configurations. As a result, there may be additional nuance or complexity associated with CMMC compliance that will only materialize (if at all) through the practical application of the standard by the CMMC Accreditation Body (CMMC AB). What's more, as of the date this Technical Reference Guide was written, the CMMC AB has not issued formal guidance for Cloud Service Providers. As a result, the information herein, including all Microsoft CMMC related offerings, are provisional and may be enhanced to align with future guidance from the DoD and CMMC AB.

Microsoft does not guarantee nor imply any ultimate compliance outcome or determination based on one's consumption of this Technical Reference Guide — all CMMC certification requirements and decisions are governed by the CMMC AB, and Microsoft has no direct or indirect insight into or bearing over CMMC AB compliance determinations. The associations between compliance domains, controls, and Microsoft Technical Reference Guide for CMMC may change at any time.

Customers must individually determine the necessary steps required to ensure their organization fully satisfies each recommended CMMC compliance control, in addition to or in place of what is described in this document. This responsibility spans all Microsoft (Azure, Microsoft 365, etc.) consumption decisions, including, among other things, which Microsoft offerings to procure, as well as all configuration decisions associated with such use and consumption.

Microsoft CMMC Acceleration Program

This Technical Reference Guide is provided through the Microsoft CMMC Acceleration Program. The Acceleration Program's main objective is to help customers close known compliance gaps and mitigate risks helping facilitate CMMC. Included with the program are a portfolio of learning resources, architectural references, and implementation tools custom-tailored to the certification journey.

Resources in the Microsoft CMMC Acceleration Program include:

- Microsoft Product Placemat for CMMC
- Microsoft Sentinel: Cloud-Native SIEM
- Microsoft Sentinel: CMMC Workbook
- Microsoft Compliance Manager with Assessment Templates
- Microsoft Defender for Cloud Apps Microsoft Defender for Cloud Apps
- Azure Blueprints
- CMMC Documentation
- Blog Posts

Learn more about how Microsoft can help organizations on their CMMC journey.

Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a unified standard for implementing cybersecurity across the DIB, which includes over 300,000 commercial companies in the supply chain. The CMMC is the DoD's response to significant compromises of sensitive defense information located on contractors' information systems.

The DoD is migrating to CMMC to assess and enhance the cybersecurity posture of the DIB. CMMC is intended to serve as a verification mechanism to ensure that DIB companies implement appropriate cybersecurity NIST controls to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.

The main benefit to organizations that obtain a CMMC certification is the improvement of their processes and enhancement of the protection of controlled unclassified information and intellectual property within the supply chain of the DIB. Meeting CMMC is a signal that the company can meet the DoD's cybersecurity objectives.

To address the range of DoD contractors, CMMC comprises three levels of cybersecurity ranging from Foundational Level One to Expert security operations at Level three for highly sensitive defense assets. The CMMC levels and the associated sets of controls are cumulative. More specifically, in order for an organization to achieve a specific CMMC level it must also demonstrate achievement of the preceding lower levels. More details on the model can be found in the CMMC Model Overview document.

For more information, see CMMC.

CMMC 2.0 Implementation Guidance

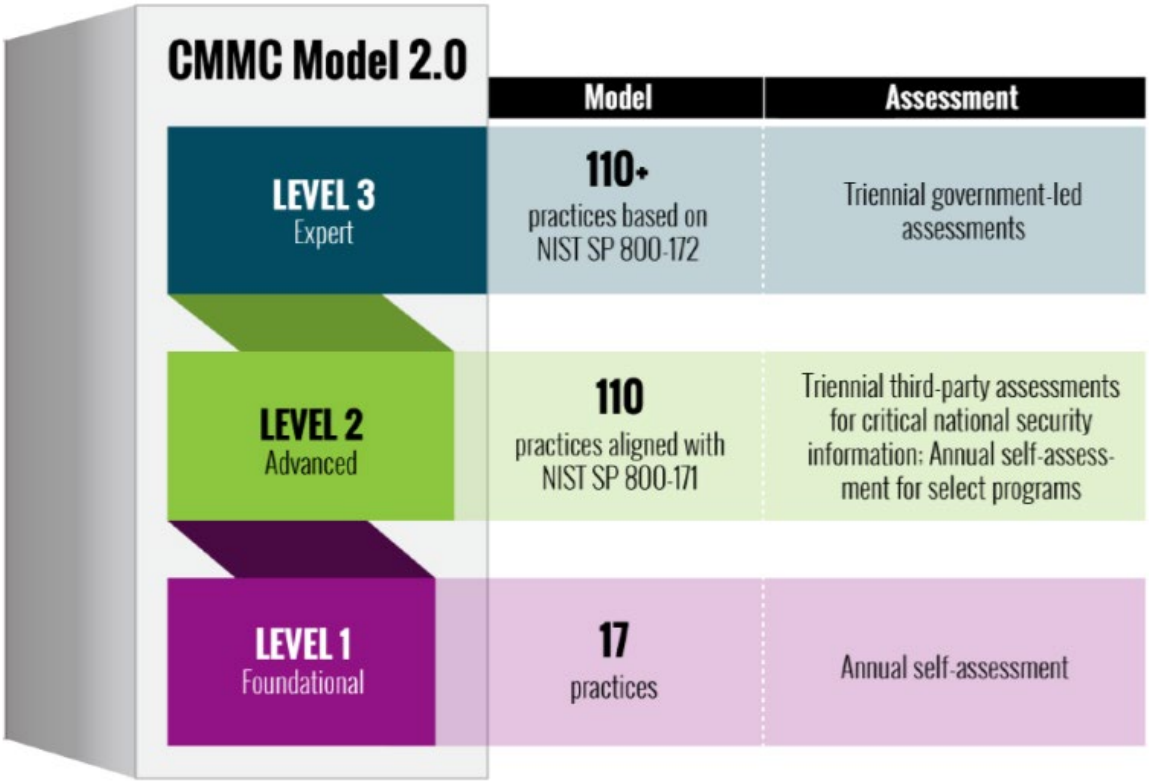
Overview of Implementation

CMMC program requirements will be implemented through the acquisition and contracting process. With limited exceptions for information with little national security need, the Department intends to require compliance with CMMC as a condition of

contract award. The required CMMC level for contractors and sub-contractors will be specified in the solicitation and in Requests for Information (RFIs), if utilized.

CMMC 2.0 NIST Alignment

NIST CMMC 2.0 aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards. Under CMMC 2.0, the "Advanced" level (Level 2) will be equivalent to the NIST SP 800-171. The "Expert" level (Level 3), which is currently under development, will be based on a subset of NIST SP 800-172 requirements. CMMC 2.0 practices have a unique identification number in the format – DD.L#-REQ for example, NIST 800-171 3.1.1 control would be written as AC.L2-3.1.1 for CMMC 2.0 Level 2 control. The format is meant to be used for quick reference only.



The US National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidelines to help protect the information and information systems of federal agencies. In response to Executive Order 13556 on managing controlled unclassified information (CUI), it published NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and*

Organizations. NIST SP 800-171 requirements are a subset of NIST SP 800-53, the standard that FedRAMP uses. Appendix D of NIST SP 800-171 provides a direct mapping of its CUI security requirements to the relevant security controls in NIST SP 800-53, for which the in-scope cloud services have already been assessed and authorized under the FedRAMP program.

Fundamentally, in order to leverage and inherit the underlying Cloud-Native controls provided by Microsoft, customers would inherit security controls that are fully audited as part of its underlying FedRAMP, mapped NIST SP 800-53 and NIST SP 800-171 controls. Accredited third-party assessment organizations, Kratos SecureInfo and Coalfire, assessed with Microsoft to attest that its in-scope cloud services meet the criteria in NIST SP 800-171, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*, when they process CUI. The Microsoft implementation of FedRAMP requirements help ensure Microsoft in-scope cloud services meet or exceed the requirements of NIST SP 800-171 using the systems and controls already in place.

Any entity that processes or stores US government CUI — research institutions, consulting companies, manufacturing contractors, must comply with the stringent requirements of NIST SP 800-171. This attestation means Microsoft in-scope cloud services can accommodate customers looking to deploy CUI workloads with the assurance that Microsoft is in full compliance. For example, all DoD contractors who process, store, or transmit 'covered defense information' using in-scope Microsoft cloud services in their information systems meet the US Department of Defense DFARS clauses that require compliance with the security requirements of NIST SP 800-171.

CMMC 2.0 Assessment Model

A CMMC assessment is the methodology to certify that a contractor is compliant with the CMMC standard. CMMC 2.0 implements tiered assessment requirements based on the sensitivity of the information shared with a contractor. Upon implementation of CMMC 2.0:

Contractors who do not handle information deemed critical to national security (Level 1 and a subset of Level 2) will be required to perform annual self-assessments against clearly articulated cybersecurity standards.

Contractors managing information critical to national security (a subset of Level 2) will be required to undergo third-party assessments.

The highest priority, most critical defense programs (Level 3) will require government-led assessments.

For more information, see:

- CMMC 2.0 Assessment Overview
  CMMC-AB Marketplace listings

POA&M

With the implementation of CMMC 2.0, the Department intends to allow companies to receive contract awards with a Plan of Actions and Milestones (POA&M) in place to complete CMMC requirements. The Department's intent is to specify a baseline number of requirements that must be achieved prior to contract award, in order to allow a remaining subset to be addressed in a POA&M within a clearly defined timeline. The Department also intends to specify a small subset of requirements that cannot be on a POA&M in support of achieving a CMMC certification. Waiver requests will require senior DoD leadership approval and will have a limited duration.

CMMC Risk Assessment

Some implementations of controls are based on categorization of data and risk. Microsoft encourages its customers to perform a thorough risk assessment for the entire environment and not rely on boundaries defined by workloads in the cloud environment.

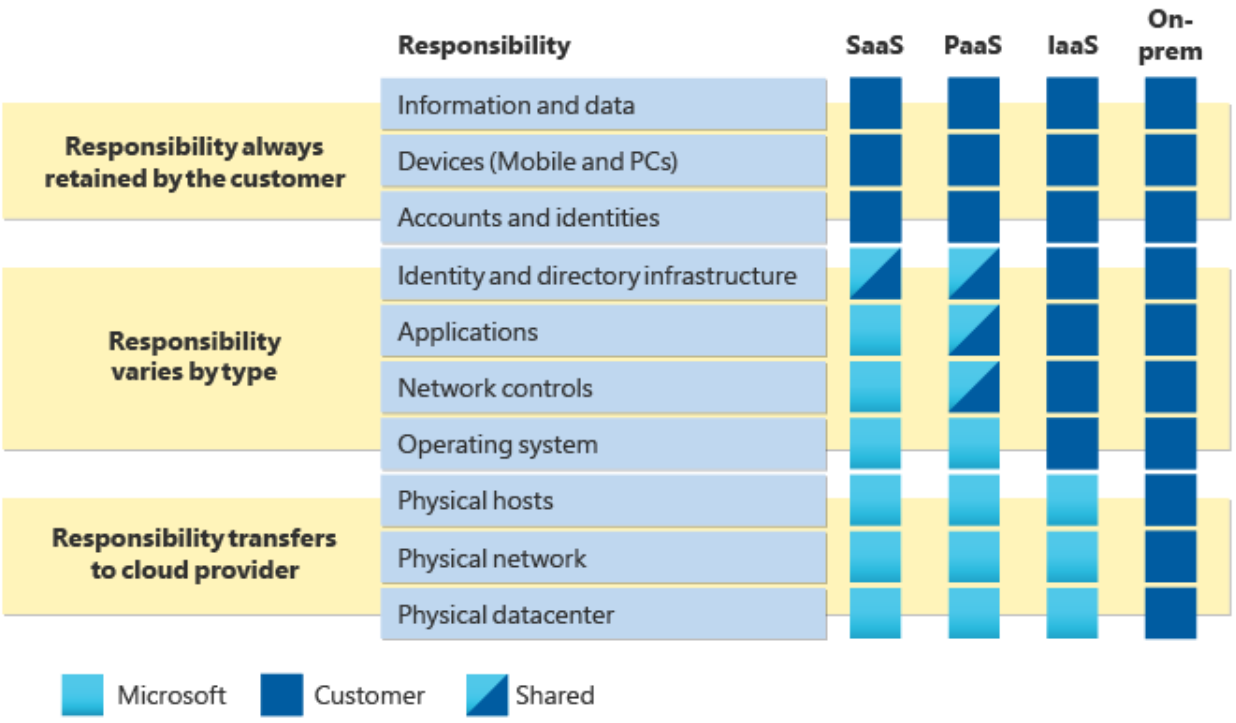
For more information, see:

NIST SP 800-30 Guide for Conducting Risk Assessments

Risk Management section of this document

Shared Responsibility in the Microsoft Cloud

It is important to understand that compliance is a shared responsibility between the customer and Microsoft, the Cloud Services Provider (CSP). The graphic below shows the CSP responsibility in respective cloud models (SaaS, PaaS, IaaS, On-Prem), spanning Microsoft, Customer, and Shared responsibilities. For example, CMMC requirements such as Physical Protection (PE) for limiting physical access (C028) is managed by the CSP. Establishment of respective policies and procedures are the customer's responsibility. Customers are advised to work with their respective C3PAO for guidance on comprehensive alignment of controls, audit and certification.



For more information see, [Shared responsibility in the cloud.]

Customer Eligibility for Azure Commercial and Azure Government

CMMC L2 and higher are intended for protection of CUI. You may demonstrate compliance with CMMC Levels 1 for the data protection of FCI in Commercial and in our Government clouds. Microsoft recommends the US Sovereign Cloud with Azure Government and Microsoft 365 Government (GCC High) for data protection of CUI in alignment with CMMC Levels 1-3.

For more information, see Understanding Compliance Between Commercial, Government and DoD Offerings.

Microsoft Services Implementation Guidance

The following family sections outline specific NIST 800-171 controls that CMMC 2.0 Level 2 requires, and services you can leverage from Microsoft to meet those Controls. This guide breaks down how customers can use these services to accelerate CMMC compliance in Microsoft.

Microsoft Primary and Secondary Services Definition

Each control that has a customer responsibility, is mapped to a Microsoft service that can help meet the requirement. Primary services are Microsoft services that directly meet the practice objective, while the secondary services require and or support the primary service in meeting the control objective. Secondary services can also provide an additional layer of protection but might not fully meet the Control requirements.

For more information, see Microsoft Product Placemat for CMMC 2.0

Azure Policy

Controls below associated with one or more Azure Policy definitions will have an Azure Policy heading and a link to the relevant NIST 800-171 R2 Azure Policy. The NIST 800-171 R2 blueprint sample provides governance guardrails using Azure Policy that help you assess specific CMMC L2 controls. This blueprint aids customers in deploying a core set of policies for any Azure-deployed architecture that must implement controls for CMMC L2. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time.

These policies may help you assess compliance with the controls implemented to meet CMMC L2 requirements; however, there often is not a one-to-one or complete match

between a control and one or more policies. As such, compliant in Azure Policy refers only to the policy definitions themselves; this does not ensure you are fully compliant with all requirements of a Control .

Microsoft Service Implementation Guidance

Access Control (AC)

AC.L2-3.1.1

Control Summary Information	
NIST 800-53 Mapping: AC-2, AC-3, AC-17	
Control : Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC Intune/Microsoft Endpoint Manager	Microsoft Information Protection Conditional Access Customer Lockbox Privileged Identity Management (PIM) Security and Compliance Center Microsoft 365 Web Apps M365 Groups

Implementation Statement:
Azure Active Directory

There are a few ways of creating identities such as, directly in Azure AD or linking to an on-premises Active Directory where Azure AD will securely authenticate the users. For more information, see:

- Azure Active Directory (AAD)
- Active Directory Federation Services (ADFS)
- Azure Active Directory pass-through authentication

It is good practice to assign permissions using the principle of least privilege this involves giving users the exact permissions they need to do their jobs properly. Users, groups, and applications are added to roles in Azure, and those roles have certain permissions. You can use the built-in roles that Azure offers, or you can create custom roles in RBAC. For more information, see:

- Grant a user access to Azure resources using RBAC
- RBAC documentation

Privileged Identity Management

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

With Azure AD PIM, you can manage, control, and monitor your privileged identities and access to your directory information and resources in an Azure environment. The main reason for using Azure AD PIM is to reduce the attack surface and to enable administrative access just-in-time. Privileged access is often configured as permanent and unmonitored, but with Azure AD PIM you can avoid security breaches and risks.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses Azure AD Multi-Factor Authentication. For example, during the activation process, a user can be forced to justify why they need to activate their role. Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

Privileged Identity Management (PIM) provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

To summarize, you should complete the following Azure AD PIM tasks for your Azure resources:

- Enable Just in Time access to Azure
- Expire access automatically
- Assign temporary access for quick tasks or on-call schedules
- Get alerts when new users or groups are assigned resource access, or when eligible assignments are activated
- Use Azure AD sign in for Azure VMs

To learn more, see Start using Privileged Identity Management.

Implementing Multi-Factor Authentication (MFA)

MFA is a security feature that requires more than one method of authentication. You can use it to add an additional layer of security to the signing in of users. It enables two-step verification, where the user first signs in using something, they know (such as a password), and then signs in with something they have (such as a smartphone), or some human characteristic (such as biometrics).

For more information, see Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication.

Azure AD Identity Protection

Azure AD Identity Protection introduces automatic, risk-based, conditional access to help protect users against suspicious logins and compromised credentials. Azure AD Identity Protections also offers insight into, and a consolidated view of, threat detection based on machine-learning. Furthermore, the service delivers an important level of remediation recommendations, as well as performing compromise risk calculations about a user and their session.

For more information, see:

- What is Identity Protection?
- Identity Protection policies

Conditional Access

Conditional Access allows you to set up access policies to prohibit a specific activity, as well as to trigger MFA according to rules that you define). It is a very powerful engine. You may target conditional access policies toward specific users or groups, or to specific apps. Additionally, you can create conditional access session control policies to enable a limited experience within specific cloud applications. For Example, you could create a policy to limit information system access to devices such as printers to block the ability to print sensitive documents on unmanaged devices.

For more information, see Conditional Access: Session.

Microsoft Intune

A cloud-based Enterprise Mobility Management (EMM) service that enables administrators to enroll mobile devices, deploy apps, and enforce security policies. As a Security Admin, use the Endpoint security node in Intune to configure device security and to manage security tasks for devices when those devices are at risk.

To protect your devices and corporate resources, you can use Azure Active Directory (Azure AD) Conditional Access policies with Intune.

Intune passes the results of your device compliance policies to Azure AD, which then uses conditional access policies to enforce which devices and apps can access your corporate resources. Conditional access policies also help to gate access for devices that aren't managed by Intune and can use compliance details from Mobile Threat Defense partners you integrate with Intune.

The following are two common methods of using conditional access with Intune:

- Device-based conditional access, to ensure only managed and compliant devices can access network resources.
- App-based conditional access, which uses app-protection policies to manage access to network resources by users on devices that you do not manage with Intune.

Microsoft 365 Web Apps

In Microsoft 365, identity is managed by Azure Active Directory. As a SharePoint or global admin in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune). Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies. Using a policy that affects all Microsoft 365 services can lead to better security and a better experience for your users.

Microsoft 365 Groups

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources.

Customer Lockbox

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. To learn more, see Customer Lockbox for Microsoft Azure.

Azure Policies

- **AC.L2-3.1.1 Azure Policies**

Customer Responsibility

- Responsible for authorizing access to the customer system.

AC.L2-3.1.2

Control Summary Information	
NIST 800-53 Mapping: AC-2, AC-3, AC-17	
Control : Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC Privileged Identity Management (PIM)	Network Security Groups Conditional Access GitHub Enterprise Cloud GitHub AE Azure AD Multi-Factor Authentication Intune/Microsoft Endpoint Manager Microsoft 365 Web Apps Microsoft 365 admin center Microsoft Defender for Cloud Apps

Implementation Guidance:

Azure Active Directory

Microsoft Azure Active Directory (AAD) offers a robust security set for enforcing the types of transactions and functions that authorized users are permitted to execute. Best practice recommendation is to segregate duties within your team by setting up Role Based Access Control (RBAC) which will help you manage who has access to Azure resources. More granularity, you can restrict what the users can do with the resources and what areas they have access to.

Ensure that the right users have the right access to the right resources by using intelligent cloud identity governance. Monitor and audit access to all resources while managing employee productivity.

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses Azure AD Multi-Factor Authentication. For example, during the activation process, a user can be forced to justify why they need to activate their role. Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

Privileged Identity Management (PIM) provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

To learn more, see, Start using Privileged Identity Management.

Network Security Groups

Network Security Groups is customizable and provide the ability to fully lock down network communication to and from your system-resources. You can restrict internet access by default, along with the use of network security groups, data segregation and isolated VPNs.

Use Azure Active Directory to manage and secure identities by requiring single sign-on and multifactor authentication to protect your users. The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access Policies. Learn how to Create a Conditional Access Policy.

Additionally, Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Explore using Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connections restrict public internet providing a private connection to Azure.

Microsoft 365 Web Apps

In Microsoft 365, identity is managed by Azure Active Directory. As a SharePoint or global admin in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune). Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies. Using a policy that affects all Microsoft 365 services can lead to better security and a better experience for your users.

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps Conditional Access App Control uses reverse proxy architecture to give you the tools you need to have real-time visibility and control over access to and activities performed within your cloud environment. With Conditional Access App Control, you can protect your organization:

- Avoid data leaks by blocking downloads before they happen

- Set rules that force data stored in and downloaded from the cloud to be protected with encryption
- Gain visibility into unprotected endpoints so you can monitor what's being done on unmanaged devices
- Control access from non-corporate networks or risky IP addresses

Microsoft 365 Admin Center

The Microsoft 365 admin center lets you manage Azure AD roles and Microsoft Intune roles. However, these roles are a subset of the roles available in the Azure AD portal and the Intune admin center.

GitHub AE

With GitHub AE, you can create an enterprise account to enable collaboration between your organization. You can control access by managing users in your enterprise. While you can grant read/write access to collaborators on a personal repository, members of an organization can have more granular access permissions for the organization's repositories.

Customer Responsibility

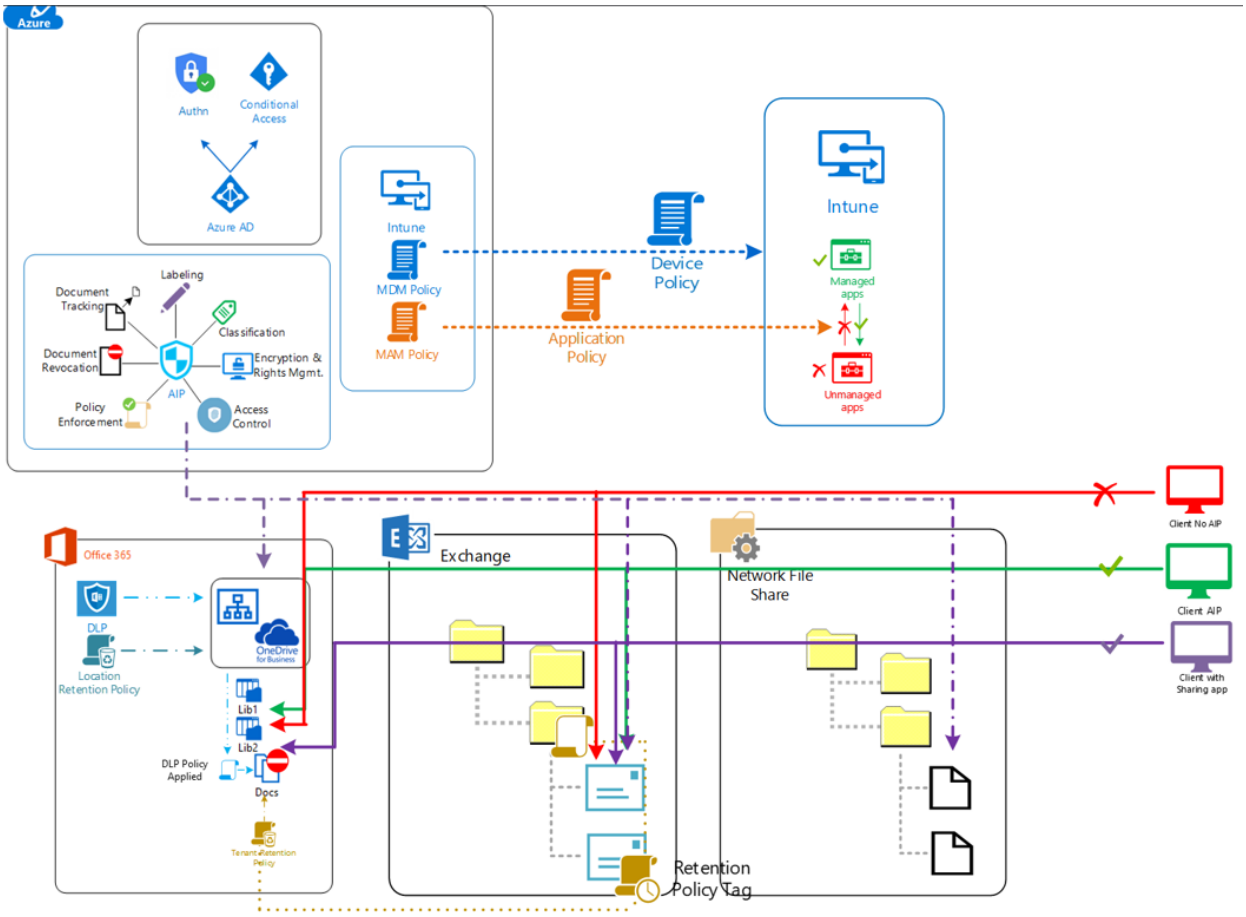
- Responsible for authorizing access to the customer system.

AC.L2-3.1.3

Control Summary Information	
NIST 800-53 Mapping: AC-4	
Control : Control the flow of CUI in accordance with approved authorizations.	
Primary Services	**Secondary Services**
Azure Web Application Firewall Microsoft Information Protection Microsoft 365 DLP	Network Security Groups Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Microsoft Defender for Identity Exchange Admin Center M365 Compliance Center Power Automate

Implementation Statement:

Example Government Flow Diagram



Microsoft Information Protection

You can secure confidential data and control information flows with Microsoft Information Protection. Microsoft Information Protection (MIP) is a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. To learn more, see [How to configure the policy settings for Microsoft Information Protection.]

Data loss prevention (DLP)

Data loss prevention (DLP) helps you prevent the unintentional or accidental sharing of sensitive information. When the risks of data leakage aren't entirely obvious, it's difficult to work out where exactly you should start with implementing DLP. Fortunately, DLP

policies can be run in "test mode", allowing you to gauge their effectiveness and accuracy before you turn them on. DLP policies for Exchange Online can be managed through the Exchange admin center. But you can configure DLP policies for all workloads through the Security & Compliance Center.

Azure Web Application Firewall

Defend your web services against common exploits and vulnerabilities using Azure Web Application Firewall deployed with Azure Front Door. It keeps your service highly available for your users and helps you meet compliance requirements. Customize Web Application Firewall rules using Azure portal. Use Azure Front Door as a scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. Learn more about Azure Web Application Firewall on Azure Front Door.

Intune/Microsoft Endpoint Manager

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Further, Intune can be configured to restrict to copying of data to publicly accessible information systems. Configure Intune to prevent data leaks on non-managed devices and setup app protection policies to secure company data on user-owned devices.

Azure Policies

- **AC.L2-3.1.3 Azure Policies**

Customer Responsibility

- Responsible for controlling the flow of information within customer-deployed resources and between interconnected systems.

Additional Resources

- Compliance and Regulatory information on managing CUI

- DFARS Controlled Unclassified Information (CUI) and covered defense information (CDI)
- Control over data travel with Microsoft Defender for Cloud Apps
- Learn more about controlling traffic with NSGs at https://aka.ms/nsg-doc
- Data protection framework using app protection policies

AC.L2-3.1.4

Control Summary Information	
NIST 800-53 Mapping: AC-5	
Control : Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC	Privileged Identity Management (PIM)

Implementation Statement:

Microsoft Azure offers a robust security set for employing separation of duties. Best practice recommendation is to segregate duties within your team by setting up Role Based Access (RBAC) which will help you manage who has access to Azure resources. Review assignments and roles regularly to ensure users have the appropriate access that is needed to perform their specific job functions.

Azure role-based access control (Azure RBAC) has several Azure built-in roles that you can assign to users, groups, service principals, and managed identities. Role assignments are the way you control access to Azure resources. If the built-in roles do not meet the specific needs of your organization, you can create your own Azure custom roles. For information about how to assign roles, see Steps to assign an Azure role.

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with access to the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

Customer Responsibility

- Responsible for the separation of duties across customer-controlled accounts.

Azure Policies

- **AC.L2-3.1.4 Azure Policies**

AC.L2-3.1.5

Control Summary Information	
NIST 800-53 Mapping: AC-6, AC-6(1), AC-6(5)	
Control : Employ the principle of least privilege, including for specific security functions and privileged accounts.	
Primary Services	**Secondary Services**
Privileged Identity Management (PIM) Privileged Access Management Azure RBAC	Azure Active Directory GitHub Enterprise Cloud GitHub AE Microsoft 365 Admin Center

Implementation Guidance:

Azure Active Directory

Microsoft Azure Active Directory (AAD) offers a robust security set for employing the principle of least privilege. Best practice recommendation is to segregate duties within your team by setting up Role Based Access Control (RBAC) which will help you manage who has access to Azure resources. There are a large number of preexisting roles available within Azure, and it is likely that an existing role will meet your needs, so you likely will not need to configure a custom role. First, you should specify exactly what actions a security principle should and should not be able to perform. Once you have generated this list, you should review the existing roles and determine if one of the existing roles meets your needs or if you need to create a custom role.

When configuring Azure RBAC, make sure that you follow the principal of least privilege. This means that you should only grant the access required to perform specific tasks. Doing so reduces the chance of unauthorized or accidental actions being performed. For example, if a group only requires the ability to view the configuration of an Azure

resource, you only need to assign a role that has the Read permission to that resource. If a group only requires Azure portal access to one virtual machine in a resource group (even though the resource group hosts multiple virtual machines), set the scope of the role assignment to the virtual machine rather than the resource group when assigning the role to that group.

To learn more, see:

- What is Azure role-based access control.
- Grant a user access to Azure resources using RBAC
- RBAC documentation
- Azure Custom roles

Microsoft 365 Admin Center

When you configure a privileged access policy with the Microsoft 365 admin center. In the Microsoft 365 admin center users can request access to elevated or privileged tasks. An approval request is generated, and the pending request notification is emailed to approvers.

Privileged Identity Management

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with access to the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

Further, you can explore the use of Just Enough Administration (JEA) to further limit admin accounts. There are prerequisites to using JEA.

Privileged access management allows granular access control over privileged admin tasks in Office 365. Privileged access management builds on the protection provided with native encryption of Microsoft 365 data and the role-based access control security model of Microsoft 365 services. When used with Azure AD Privileged Identity Management, these two features provide access control with just-in-time access at different scopes.

To summarize, you should complete the following Azure AD PIM tasks for your Azure resources:

- Enable Just in Time access to Azure
- Expire access automatically
- Assign temporary access for quick tasks or on-call schedules
- Get alerts when new users or groups are assigned resource access, or when eligible assignments are activated
- Use Azure AD sign in for Azure VMs

To learn more, see Start using Privileged Identity Management.

GitHub AE

With GitHub AE, you can create an enterprise account to enable collaboration between your organization. You can control access by managing users in your enterprise. While you can grant read/write access to collaborators on a personal repository, members of an organization can have more granular access permissions for the organization's repositories.

Customer Responsibility

- Responsible for enforcing least privilege across customer-controlled accounts.

AC.L2-3.1.6

Control Summary Information	
NIST 800-53 Mapping: AC-6(2)	
Control : Use non-privileged accounts or roles when accessing non-security functions.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC	Privileged Identity Management (PIM) Privileged Access Management Microsoft 365 Admin Center

Implementation Guidance:

When planning your access control strategy, it is a best practice to implement least privilege. Least privilege means you grant your administrators exactly the permission they need to do their job. There are three aspects to consider when you assign a role to

your administrators: a specific set of permissions, over a specific scope and for a specific period of time. Customers should avoid assigning broader roles at broader scopes even if it initially seems more convenient to do so. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised.

Azure Active Directory

Azure AD RBAC supports over 65 built-in roles. There are Azure AD roles to manage directory objects like users, groups, and applications, and also to manage Microsoft 365 services like Exchange, SharePoint, and Intune.

Privileged Access Management & Privileged Identity Management (PIM)

Privileged access management allows granular access control over privileged admin tasks in Office 365. Privileged access management builds on the protection provided with native encryption of Microsoft 365 data and the role-based access control security model of Microsoft 365 services. When used with Azure AD Privileged Identity Management, these two features provide access control with just-in-time access at different scopes.

Microsoft recommends that you enable Privileged Identity Management (PIM) in Azure AD. Using PIM, a user can be made an eligible member of an Azure AD role. They can then activate their role for a limited timeframe every time the needs to use it. Privileged access is automatically removed when the timeframe expires.

To learn more, see Start using Privileged Identity Management.

Best Practices:

- Conduct User Access reviews to review administrator's access regularly to make sure only the right people have continued access.
- Enable MFA on Azure AD roles
- Azure AD groups allow you to collect Azure security principals including users, service principals, and other groups.
- Conditional Access Policies allow you to implement more stringent authentication requirements if certain conditions are met.
- Application registration permission scopes allow you to control what resources and data an application can access.

- Custom RBAC roles can be configured if an existing RBAC role does not have permissions that are appropriate to your organization's needs.
- Microsoft recommends that you assign the Global Administrator role to fewer than five people in your organization.

Microsoft 365 Admin Center

When you configure a privileged access policy with the Microsoft 365 admin center. In the Microsoft 365 admin center users can request access to elevated or privileged tasks. An approval request is generated, and the pending request notification is emailed to approvers.

Customer Responsibility

- Responsible for requiring the use of non-privileged accounts/roles when accessing non-security functions for customer-deployed resources.

AC.L2-3.1.7

Control Summary Information	
NIST 800-53 Mapping: AC-6(9), AC-6(10)	
Control : Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC Privileged Identity Management (PIM) Azure Monitor Microsoft Sentinel Privileged Access Management	Conditional Access Intune/Microsoft Endpoint Manager Microsoft Defender for Office 365 M365 Compliance Center

Implementation Statement:

Azure Active Directory

Microsoft Azure offers a robust security set for preventing the use of non-privileged accounts from executing privileged functions. Best practice recommendation is to segregate duties within your team by setting up Role Based Access (RBAC) which will help you manage who has access to Azure resources. More granularity, you can restrict what the users can do with the resources and what areas they have access to.

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

Privileged access management requires users to request just-in-time access to complete elevated and privileged tasks through a highly scoped and time-bounded approval workflow. Privileged access management is defined and scoped at the task level, while Azure AD Privileged Identity Management applies protection at the role level with the ability to execute multiple tasks. All activity for the task is logged in the Security & Compliance Center.

M365 Compliance Center

Enable auditing of admin activity in M365 Compliance Center. Enabling auditing for admins allows you to capture user and administrator activities in your organization.

Audited Activities in M365 Compliance Center can be granularly selected. It is recommended to review audit logs at a frequency to meet your compliance requirements. This will assist in discovering execution of privileged functions.

Intune/Microsoft Endpoint Manager:

By default, auditing in Intune/Microsoft Endpoint Manager is enabled for all customers. This allows an organizations administrator to track and monitor events in Microsoft Intune. Audit logs include a record of activities, such as; create, update (edit), delete, assign, and remote actions all create audit events that administrators can review.

Logs can also be sent to Azure Monitor services, including storage accounts, event hubs, and log analytics. For more information: use audit logs to track and monitor events in Microsoft Intune.

Additionally, consider using Microsoft Sentinel as your Security Information and Event Management (SIEM) solution. After you connect your data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks. While Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to Create interactive reports with Azure Monitor Workbooks.

Customer Responsibility

- Responsible for auditing the execution of privileged functions on customer-deployed resources.
- Responsible for ensuring that non-privileged users cannot execute privileged functions on customer-deployed resources.

Additional Resources

- Microsoft Defender for Endpoint

AC.L2-3.1.8

Control Summary Information	
NIST 800-53 Mapping: AC-7	
Control : Limit unsuccessful logon attempts.	
Primary Services	**Secondary Services**
Azure Active Directory	Azure AD Password Protection Azure AD Smart Lockout

Implementation Guidance:

Azure Active Directory and Password Protection

Microsoft customers should consider two factors when implementing this control. They should determine the threshold for how many consecutive times a failed login will be allowed before a lock out is implemented, and then determine what would be the duration of that lock out. Having three consecutive, unsuccessful logon attempts is a common setting. Organizations should set this number at a level that fits their risk profile. Fewer unsuccessful attempts provide higher security.

Password protection has a smart lockout functionality, which ensures that the Azure AD account is locked out before the AD account is locked out, which would leave an organization susceptible to a denial-of-service attack.

You can control the lockout duration using Azure Active Directory smart lockout. Smart lockout allows customers to lock out attackers who are trying to brute force user passwords. Based on machine learning, smart lockout is able to discern when sign-ins are coming from authentic users and treat those sign-ins differently to those that appear to come from attackers or other unknown sources. For example, smart Lockout locks out an account for 60 seconds after 10 failed sign-in attempts have occurred. If there are subsequent failed sign-in attempts after this 60 second has expired, the lock out period duration increases. Smart Lockout only tracks when different passwords are used, which is the pattern during a brute force attack, so if a user enters the same incorrect password 10 times, that will only count as one bad password towards the 10 that trigger account lockout.

Azure AD Smart Lockout is enabled by default on Microsoft 365 Azure AD tenancies. Customers can configure a custom smart lockout threshold in the Authentication Methods section of the Azure AD console.

For each lockout, the duration of the lockout is increased. Customers should make sure the Azure AD lockout threshold is less than the threshold for AD (making sure Azure AD locks out first) and the duration of the lockout in Azure AD is longer than the AD reset counter. (AAD is seconds; AD is minutes!)

Customer Responsibility

- Responsible for enforcing a limit of consecutive failed login attempts on customer-deployed

AC.L2-3.1.9

Control Summary Information	
NIST 800-53 Mapping: AC-8	
Practice: Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.	
Primary Services	**Secondary Services**
Microsoft Endpoint Manager Azure Active Directory	Conditional Access Teams

Implementation Guidance:

CUI is information that requires safeguarding or disseminating controls according to law, regulation, or government-wide policy. The CUI Registry identifies approved CUI categories and subcategories. Microsoft customers should consult their specific CUI requirements which require safeguarding or dissemination controls and are either:

- Marked or otherwise identified in the contract, task order, or delivery order, and provided to the contractor by or on behalf of DoD in connection with the performance of the contract, or
- Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Teams

You can require acceptance of Company terms and conditions before accessing resources such as, Teams, SharePoint and OneDrive by using Azure Active Directory Conditional Access. Moreover, You can customize Teams meeting invitations to meet your organization's needs. You can add your organization's logo and include helpful information, such as links to your support website and legal disclaimer, and a text-only footer.

There are two ways to create your company terms and conditions:

- by using Intune
- by using the Azure Active Directory terms of use feature

To learn which method is best for you, check out the Choosing the right Terms solution for your organization blog post.

Azure Active Directory

Add Azure Active Directory (AAD) terms of use policies to ensure users see relevant disclaimers for legal or compliance requirements by requiring the user to accept or decline the terms of use. You can also view report of who has accepted and declined.

Intune/Microsoft Endpoint Manager

As an Intune admin, you can require that users accept your company's terms and conditions before using the Company Portal to:

- enroll devices
- access resources like company apps and email.

You can create multiple sets of terms and assign them to different groups, such as to support different languages.

To learn more, see Intune.

Customer Responsibility

- Responsible for implementing a compliant system use notification for all customer-deployed resources.

Additional Resources

- Add your organization's privacy info using Azure Active Directory
- Add language-specific company branding to your directory

AC.L2-3.1.10

Control Summary Information	
NIST 800-171 Mapping: 3.1.10	
NIST 800-53 Mapping: AC-11, AC-11(1)	
Control : Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	
Primary Services	**Secondary Services**
Azure Active Directory Conditional Access	Microsoft Azure Portal Azure Virtual Machines Microsoft 365 Web Apps Intune/Microsoft Endpoint Manager

Implementation Statement:

Azure Portal

The inactivity timeout setting helps to protect resources from unauthorized access if you forget to secure your workstation. After you have been idle for a while, you are automatically signed out of your Azure portal session. Admins in the Global Administrator role can enforce the maximum idle time before a session is signed out. The inactivity timeout setting applies at the directory level. The setting takes effect for new sessions. It will not apply immediately to any users who are already signed in. For more information about directories, see Active Directory Domain Services Overview.

Intune/Microsoft Endpoint Manager

Additionally, using Intune/Microsoft Endpoint Manager you can use policies to set the maximum minutes of inactivity until the screen locks on your device. Configure screen lock settings using Intune. Enforce controls using conditional access to only grant access to resources if devices are marked as compliant.

Azure Active Directory (AAD)

By default, Azure Active Directory (AAD) obscures all passwords. Microsoft's Password boxes conceal the characters typed into it for purposes of privacy. By default, the password box provides a way for the user to view their password by holding down a reveal button.

You can disable this feature for Windows 10 using policy as an added security measure to ensure your password can not be displayed on the login screen.

Conditional Access

Implement device lock by using a conditional access policy to restrict access to compliant devices. Configure policy settings on the device to enforce device lock at the OS level with MDM solutions such as Intune. Endpoint Manager or group policy objects can also be considered in hybrid deployments. For unmanaged devices, configure the Sign-In Frequency setting to force users to reauthenticate.

Microsoft 365 Web Apps

When users authenticate in any of the Microsoft 365 web apps or mobile apps, a session is established. For the duration of the session, users won't need to re-authenticate. Sessions can expire when users are inactive, when they close the browser or tab, or when their authentication token expires for other reasons such as when their password has been reset. The Microsoft 365 services have different session timeouts to correspond with the typical use of each service.

Customer Responsibility

- Responsible for incorporating a session lock on all customer-deployed resources.
- Responsible for concealing previously visible information when a session lock is initiated on customer-deployed resources.

Additional Resources

- Deploy requirements to prevent access and viewing data after a period of inactivity using Interactive Login: Machine Inactivity Limit.
- Deploy requirements for Account Lockout.
- Deploy requirements to disable the password reveal button.

AC.L2-3.1.11

Control Summary Information	
NIST 800-53 Mapping: AC-12	
Control : Terminate (automatically) user sessions after a defined condition.	
Primary Services	**Secondary Services**
Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Azure Portal Intune/Microsoft Endpoint Manager Azure AD Smart Lockout Azure Active Directory Continuous Access Evaluation	Application Security Groups Azure Bastion Conditional Access

Implementation Statement:

Azure Active Directory

Implement automatic user session re-evaluation with Azure AD features such as Risk-Based Conditional Access and Continuous Access Evaluation. Inactivity conditions can be implemented at a device level as described in:

- Sign-in risk-based Conditional Access
- User risk-based Conditional Access
- Continuous Access Evaluation

Additionally, having a lockout threshold limiting the number of unsuccessful login attempts will protect against threats such as, Brute Force Attacks by automatically locking the account after a specified number of attempts. Default lockout threshold is set to 10 failed sign-ins before the first lockout occurs. It is important to customize the lockout threshold to fit your business requirements using Azure Active Directory smart lockout (AAD).

Federated deployments that use AD FS 2016 and AD FS 2019 can enable similar benefits using AD FS Extranet Lockout and Extranet Smart Lockout. Extranet Smart Lockout (ESL) protects your users from experiencing extranet account lockout from malicious activity.

ESL enables AD FS to differentiate between sign-in attempts from a familiar location for a user and sign-in attempts from what may be an attacker. Smart lockout is always on, for all Azure AD customers, with default settings that offer the right mix of security and usability.

Intune/Microsoft Endpoint Manager

Manage your devices and applications with Microsoft Intune. Intune-managed devices can be reset to factory settings. If the device is unmanaged, you can wipe the corporate data from managed apps. These processes are effective for removing potentially sensitive data from end users' devices. However, for either process to be triggered, the device must be connected to the internet. If the device is offline, the device will still have access to any locally stored data.

Microsoft Defender for Cloud Apps

Use Microsoft Defender for Cloud Apps to block data download when appropriate. If the data can only be accessed online, organizations can monitor sessions and achieve real-time policy enforcement. Defender for Cloud Apps looks at every user session on your cloud and alerts you when something happens that is different from the baseline of your organization or from the user's regular activity. You can enable automated remediation actions on alerts generated by anomaly detection policies

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides the capability of isolating devices from the network and restricting app execution. This action can help prevent the attacker from controlling the compromised device and performing further activities such as data exfiltration and lateral movement.

Customer Responsibility

- Responsible for defining and enforcing events or conditions requiring the termination of a user session on customer-deployed resources.

AC.L2-3.1.12

Control Summary Information	
NIST 800-53 Mapping: AC-17(1)	
Control : Monitor and control remote access sessions.	
Primary Services	**Secondary Services**
Azure Active Directory Microsoft Defender for IoT Microsoft Sentinel Azure Bastion	Microsoft Azure Portal Azure ExpressRoute Network Security Groups Intune/Microsoft Endpoint Manager Microsoft Defender for Office 365 Conditional Access Direct Access

Implementation Statement:

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code. Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets. Microsoft services can help meet this practice by providing the applicable services such as, but not limited to, Azure Active Directory, Azure Bastion, Microsoft Endpoint Manager and Microsoft Sentinel

Azure Bastion

Once the Bastion service is provisioned and deployed in your virtual network, you can use it to seamlessly connect to any VM in this virtual network. As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

To learn more, see Azure Bastion.

Microsoft Defender for IoT and Sentinel

Microsoft Defender for IoT provides continuous asset discovery, vulnerability management, and threat detection for your Internet of Things (IoT) and operational technology (OT) devices and helps meet this requirement for its monitoring capabilities.

Microsoft Defender for IoT interoperates with Microsoft Sentinel which collects data across all users, devices, applications, and infrastructure, both on-premises and in the cloud to support monitoring requirements.

Azure Active Directory and Conditional Access

Use Azure Active Directory to manage and secure identities by requiring single sign-on and multifactor authentication to protect your users. The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access Policies. Learn how to Create a Conditional Access Policy.

Intune/Microsoft Endpoint Manager and Conditional Access

Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Azure ExpressRoute

Explore using Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

DirectAccess

DirectAccess allows connectivity for remote users to organization network resources without the need for traditional Virtual Private Network (VPN) connections. With DirectAccess connections, remote client computers are always connected to your organization - there is no need for remote users to start and stop connections, as is required with VPN connections. DirectAccess provides support only for domain-joined clients that include operating system support for DirectAccess. Remote Access monitoring reports remote user activity and status for DirectAccess and VPN connections. It tracks the number and duration of client connections (among other statistics) and monitors the operations status of the server.

Azure Policies

- **AC.L2-3.1.12 Azure Policies**

Customer Responsibility

- Responsible for monitoring and controlling remote access methods for customer-deployed resources.

Additional Resources:

- Learn more on how to secure access for your remote workforce
- Monitor connected remote clients for activity and status
- Use Remote Access Monitoring and Accounting

AC.L2-3.1.13

Control Summary Information	
NIST 800-53 Mapping: AC-17(2)	
Control : Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
Primary Services	**Secondary Services**
Microsoft Azure Portal Azure Active Directory	Load Balancer Intune/Microsoft Endpoint Manager Office 365 Advanced Message Encryption Azure AD Multi-Factor Authentication Azure VPN Azure Bastion Azure Firewall Azure Virtual Desktop

Implementation Statement:

Securing Remote Sessions with Encryption

Use Azure Active Directory to manage and secure identities by requiring single sign-on and multifactor authentication to protect your users. The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access Policies.

To learn more, see Learn how to Create a Conditional Access Policy.

Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Azure VPN – Azure Bastion – Azure Virtual Desktop

Azure VPN gateway supports both Point-to-Site (P2S) and Site-to-Site (S2S) VPN connections. Using the Azure VPN gateway, you can scale your employee's connections

to securely access both your Azure deployed resources and your on-premises resources. To access your resources deployed in Azure, remote developers could use Azure Bastion solution, instead of VPN connection to get secure shell access (RDP or SSH) without requiring public IPs on the VMs being accessed. Another way to support a remote workforce is to deploy a Virtual Desktop Infrastructure (VDI) hosted in your Azure virtual network, secured with an Azure Firewall. For example, Azure Virtual Desktop (AVD) is a desktop and app virtualization service that runs in Azure.

Office 365 Message Encryption

Office 365 Message Encryption is an online service that's built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection. This service includes encryption, identity, and authorization policies to help secure your email. With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization.

Customer Responsibility

- Responsible for implementing cryptographic mechanisms (e.g., TLS) to protect remote access sessions to customer-deployed resources.

Additional Resources:

- Learn more on how to secure access for your remote workforce
- Explore using Azure Load Balancer to provide secure by default connections for virtual machines
- Enable Azure AD Multi-Factor Authentication
- Learn more on choosing the right authentication method
- Learn more about Azure Government Cryptographic Mechanisms.
- Understanding Azure Virtual Desktop network connectivity

AC.L2-3.1.14

Control Summary Information	
NIST 800-53 Mapping: AC-17(3)	
Control : Route remote access via managed access control points.	
Primary Services	**Secondary Services**
Azure Bastion VPN Gateway Intune/Microsoft Endpoint Manager	Azure ExpressRoute Azure Front Door Network Security Groups Azure Web Application Firewall Conditional Access Azure Virtual Desktop Managed Windows Desktop

Implementation Statement:

Azure Bastion

Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. Using Azure Bastion, you can securely and seamlessly connect to your virtual machines over SSL directly in the Azure portal. When you use Azure Bastion, your VMs do not require a client, agent, or additional software.

Before you begin, verify that you have met the following criteria:

- A VNet with the Bastion host already installed.

Make sure that you have set up an Azure Bastion host for the virtual network in which the VM is located. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM in the virtual network. To set up an Azure Bastion host, see Create a bastion host.

- A Windows virtual machine in the virtual network.
- The following required roles:
    - Reader role on the virtual machine.
    - Reader role on the NIC with private IP of the virtual machine.
    - Reader role on the Azure Bastion resource.

- Ports: To connect to the Windows VM, you must have the following ports open on your Windows VM:
    - Inbound ports: RDP (3389)

Azure Virtual Desktop

Bring your own device (BYOD) and access your desktop and applications over the internet using an Azure Virtual Desktop. Set up Azure Virtual Desktop (formerly Windows Virtual Desktop) to enable secure remote work. Provide employees the best virtualized experience with the only solution fully optimized for Windows 11 and Microsoft 365.

VPN Gateway

Create a VPN Gateway that lets you connect to your virtual network from a remote location. There are different configurations available for VPN gateway connections. For more information on determining which configuration best fits your needs: Configuring a VPN Gateway.

Intune/Microsoft Endpoint Manager

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Named Locations

Use Named Locations to restrict Azure AD users and/or device groups using conditional access policies more granularly by configuring allowed IP address ranges within your organization. These named locations may include an organization's headquarters, VPN network or additionally, ranges that you wish to block.

Azure ExpressRoute

Explore using Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

Azure Web Application Firewall and Front Door

Optimize performance with Azure Web Application Firewall deployed with Azure Front Door. Customize Web Application Firewall rules using Azure portal. Use Azure Front Door as a scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications.

Customer Responsibility

- Responsible for routing remote access connections to customer-deployed resources through managed network access control points.

Additional Resources:

- Azure Policy Regulatory Compliance controls for Azure Virtual Network
- Working with NSG access and Azure Bastion

AC.L2-3.1.15

Control Summary Information	
NIST 800-171 Mapping: 3.1.15	
NIST 800-53 Mapping: AC-17(4)	
Control : Authorize remote execution of privileged commands and remote access to security-relevant information.	
Primary Services	**Secondary Services**
Azure Active Directory Privileged Identity Management (PIM)	Intune/Microsoft Endpoint Manager Microsoft Information Protection Microsoft Information Governance Named Locations Azure Virtual Machines Conditional Access

Implementation Statement:

Azure Active Directory Role Based Access Control

Microsoft Azure offers a robust security set for employing the principle of least privilege. Best practice recommendation is to segregate duties within your team by setting up Role Based Access (RBAC) which will help you manage who has access to Azure resources. More granularity, you can restrict what the users can do with the resources and what areas they have access to.

Privileged Identity Management

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with access to the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

Intune/Microsoft Endpoint Manager and Network Access Controls

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will

be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Use Named Locations to restrict Azure AD users and/or device groups using conditional access policies more granularly by configuring allowed IP address ranges within your organization. These named locations may include an organization's headquarters, VPN network or additionally, ranges that you wish to block.

Microsoft Information Governance and Microsoft Information Protection

Use Microsoft Information Governance (MIG) capabilities to govern your data for compliance or regulatory requirements. Implement Microsoft Information Protection (MIP) to help you discover, classify, and protect sensitive information wherever it lives or travels. MIP capabilities are included with Microsoft 365 Compliance and give you the tools to know your data, protect your data, and prevent data loss.

Customer Responsibility

- Responsible for authorizing privileged commands and access to security-relevant information via remote access for customer-deployed resources.

Additional Resources

- Explore the use of Just Enough Administration (JEA) to further limit admin accounts. There are prerequisites to using JEA.

AC.L2-3.1.16

Control Summary Information	
NIST 800-53 Mapping: AC-18	
Control : Authorize wireless access prior to allowing such connections.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager	Conditional Access Network Access Control (NAC)

Implementation Statement:

Intune/Microsoft Endpoint Manager

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Customer Responsibility

- Authorizing wireless access prior to allowing such connections to customer-deployed resources.

AC.L2-3.1.17

Control Summary Information	
NIST 800-53 Mapping: AC-18(1)	
Control : Protect wireless access using authentication and encryption.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager	Conditional Access Network Access Control (NAC)

Implementation Statement:

Wireless Access

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Additionally, using Microsoft Intune built-in Wi-Fi settings called a "profile", you can deploy specific Wi-Fi connection requirements to users with supported devices in your organization. Intune/Microsoft Endpoint Manager offers many features, including authenticating to your network, using a pre-shared key for encryption and more.

Additional Resources

- Supported device platforms & creating Intune Wi-Fi profile
- Requiring multi-factor authentication for Intune device enrollments
- Adding Wi-Fi settings for Windows 10 and newer devices in Intune

AC.L2-3.1.18

Control Summary Information	
NIST 800-171 Mapping: 3.1.18	
NIST 800-53 Mapping: AC-19	
Control : Control connection of mobile devices.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager	Microsoft 365 Admin Center Microsoft Defender for Endpoint conditional access Network Access Control

Implementation Statement:

Intune/Microsoft Endpoint Manager

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be

managed on almost any device, including personal devices in bring-your-own-device (BYOD) scenarios. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of Microsoft Intune protected apps available for public use.

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Exchange Active Sync

As an administrator, you can turn mobile access on or off, and remotely manage some phone features or options. For example, you can require passwords for your users' devices. When mobile access is turned on, users can configure their Windows Phone, iPhone, iPad, Android phone, BlackBerry®, or other phone or tablet to send and receive Microsoft 365 email and access calendar and contacts information.

Your users can also access their email on their phone or tablet by signing into Outlook Web App. Exchange ActiveSync, which is turned on by default, turns on mobile access for Windows Phone, Apple iPhone and iPad, Android phones, and BlackBerry devices. You can turn this access off via the Microsoft 365 Portal>Admin>Exchange>Mobile>Mobile Device Access.

Customer Responsibility

- Controlling connection of mobile devices to customer-deployed resources.

Additional Resources

- How to create and deploy app protection policies with Microsoft Intune
- Available Android app protection policy settings with Microsoft Intune
- Available iOS/iPadOS app protection policy settings with Microsoft Intune

AC.L2-3.1.19

Control Summary Information	
NIST 800-53 Mapping: AC-19(5)	
Control : Encrypt CUI on mobile devices and mobile computing platforms.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager Microsoft Information Protection	Conditional Access Microsoft Defender for Endpoint

Implementation Statement:

Using Intune combined with the native polices and configuration options in Azure, users can set device compliance policies and configure conditional access to deny access to unencrypted devices to your systems, ensuring compliance with this specific Control . This in addition to data and file encryption applied through Microsoft Information Protection allows organizations to encrypt the data and the container on mobile devices.

Encrypt CUI on mobile devices and mobile computing platforms using Intune/Microsoft Endpoint Manager with Conditional access to require encryption, such as BitLocker for Windows 10 and later. Require app protection policy and an approved client app for cloud app access. Create and assign Microsoft Intune app protection policies to ensure that apps are protected with a PIN and Encrypted.

See the Android app protection policy settings and iOS/iPadOS app protection policy settings for detailed information on the encryption app protection policy setting.

Microsoft Information Protection (MIP)

Microsoft Information Protection (MIP) prevents the transfer of unauthorized and unintended information transfer. Once data is marked with a sensitivity label that includes encryption settings, data and emails marked as containing CUI are protected. MIP sensitivity labels enforce controls on information sharing, such as forwarding, printing, and downloading.

Additional Resources

- Data protection framework using app protection policies

AC.L2-3.1.20

Control Summary Information	
NIST 800-53 Mapping: AC-20, AC-20(1)	
Control : Verify and control/limit connections to and use of external information systems.	
Primary Services	**Secondary Services**
Azure Active Directory Microsoft Defender for Cloud Apps Intune/Microsoft Endpoint Manager Conditional Access Network Security Groups Azure Firewall	Microsoft Azure Portal Microsoft Information Protection Microsoft Defender for IoT

Implementation Statement:

Azure Active Directory & Conditional Access

Block access by location with Azure AD Conditional access to control and limit connections to and use of external information systems. For more information about Conditional Access, see the Conditional Access documentation.

Requirements

- A subscription to Azure Active Directory Premium
- A federated Azure Active Directory tenant. See What is Conditional Access?

Conditional Access

Conditional access policies can be integrated with Defender for Cloud Apps to provide controls for cloud and on-premises applications from external systems. Mobile application management in Intune can protect organization data at the application level, including custom apps and store apps, from managed devices that interact with external systems. An example would be accessing cloud services. You can use app management on organization-owned devices and personal devices.

Microsoft Information Protection (MIP)

Microsoft Information Protection (MIP) prevents the transfer of unauthorized and unintended information transfer. Once data is marked with a sensitivity label that includes encryption settings, data and emails marked as containing CUI are protected. MIP sensitivity labels enforce controls on information sharing, such as forwarding, printing, and downloading.

Microsoft Defender for Cloud Apps

App connectors use the APIs of app providers to enable greater visibility and control by Microsoft Defender for Cloud Apps over the apps you connect to. Learn how App Connectors work providing you control of your App environment.

Additionally, Microsoft Defender for IoT provides continuous asset discovery, vulnerability management, and threat detection for your Internet of Things (IoT) and operational technology (OT) devices and helps meet this requirement for visibility of connections to external information systems.

Microsoft Defender for IoT interoperates with Microsoft Sentinel which collects data across all users, devices, applications, and infrastructure, both on-premises and in the cloud to support monitoring requirements.

Customer Responsibility

- Responsible for establishing terms and conditions allowing authorized individuals to access the customer-deployed resources from external information systems.

Additional Resources

- Restrict your Azure AD app to a set of users in an Azure AD tenant
- Configure authentication session management with conditional access
- Azure Government – trusted cloud for US Government requirements
- How to manage devices using the Azure Portal
- Connect Azure to Microsoft Defender for Cloud Apps
- Require device to be marked as compliant
- Conditions in Conditional Access policy - Device State (Preview)
- Protect with Microsoft Defender for Cloud Apps Conditional Access App Control

- Location condition in Azure Active Directory Conditional Access

AC.L2-3.1.21

Control Summary Information	
NIST 800-53 Mapping: AC-20(2)	
Control : Limit use of portable storage devices on external systems.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager Microsoft Defender for Endpoint	Named Locations Conditional Access Azure Active Directory

Implementation Guidance:

Clearly define the use of portable storage and where such devices can and cannot be used. Further apply technical controls where possible to restrict and control the use of portable devices.

- Define corporate compliance policies for portal storage devices such as, but not limited to:
  - floppy disks;
  - compact/digital video disks (CDs/DVDs);
  - flash/thumb drives;
  - external hard disk drives; and
  - flash memory cards/drives that contain nonvolatile memory.
- Apply technical controls, such as data loss controls, encryption or device state configuration requirements

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint, Device Control Removable Storage Access Control, enables you to prevent the read, write or execute access to removable storage with or without exclusion. The Microsoft 365 Defender portal shows events triggered by the Device Control Removable Storage Access Control.

To learn more see, Microsoft Defender for Endpoint Device Control Removable Storage Access Control.

Microsoft Intune

Microsoft's primary MDM tool is Microsoft Intune. Intune is part of a larger Microsoft MDM platform called Microsoft Endpoint Manager.

Using Intune, administrators can enroll, configure, and manage mobile devices on several different operating system platforms, wherever the devices happen to be. Administrators can even intervene when a threat to security occurs, by blocking a device's access to the company network and erasing any sensitive information stored on it.

Organizations can configure policies to allow, block and restrict USB drives and other peripherals.

Organizations can allow users to install only the USB drives and other peripherals included on a list of authorized devices or device types or prevent users from installing USB drives and other peripherals included on a list of unauthorized devices and device types.

Additionally, using Intune, you can apply device configuration policies to Azure AD user and/or device groups. The policies can also be set through the Device Installation CSP settings and the Device Installation GPOs. To protect your devices and corporate resources, you can use Azure Active Directory (AAD) Conditional Access policies with Intune.

Intune passes the results of your device compliance policies to Azure AD, which then uses conditional access policies to enforce which devices and apps can access your corporate resources.

Additionally, when managing devices in your organization, you want to create groups of settings that apply to different device groups. To prevent malware infections or data loss in your organization, you may want to block certain kinds of USB devices, such as a USB flash drive or camera, and allow other kinds of USB devices, such as a keyboard or mouse. Further, you may want to allow USB devices by specific device IDs. You can

complete this task using Administrative Templates in Intune. The templates are built into Intune and do not require customization.

Named Locations

Use Named Locations to restrict Azure AD users and/or device groups using conditional access policies more granularly by configuring allowed IP address ranges within your organization. These named locations may include an organization's headquarters, VPN network or additionally, ranges that you wish to block.

Customer Responsibility

- Limiting the use of portable storage devices on customer-deployed resources (e.g., laptops).

Additional Resources

- Block installation and usage of removable storage
- Use Windows 10 templates to configure group policy settings in Microsoft Intune
- Microsoft Defender for Endpoint Device Control Removable Storage Access Control

AC.L2-3.1.22

Control Summary Information	
NIST 800-53 Mapping: AC-22	
Control : Control information posted or processed on publicly accessible information systems.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager Conditional Access Microsoft Information Protection Microsoft 365 DLP	Microsoft Information Protection Network Access Control Exchange Admin Center M365 Compliance Center Microsoft Defender for Cloud App

Implementation Statement:

Intune/Microsoft Endpoint Manager

Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Further, Intune can be configured to restrict the copying of data to publicly accessible information systems. Configure Intune to prevent data leaks on non-managed devices and setup app protection policies to secure company data on user-owned devices.

Microsoft Information Protection

Controlling data usage and posting information to publicly accessible systems requires information discovery, classification and labeling. Data protection solutions such as Microsoft Information Protection (MIP) can classify and protect sensitive data, including CUI and FCI. Microsoft Information Protection unified labeling scanner can inspect any files that Windows can index. If you have configured sensitivity labels to apply automatic classification, the scanner can label discovered files to apply that classification, and optionally apply or remove protection.

Microsoft Defender for Cloud Apps Microsoft Defender for Cloud Apps lets you apply Microsoft Information Protection classification labels automatically, with or without protection, to files as a file policy governance action. You can also investigate files by filtering for the applied classification label within the Cloud App Security portal. Using classifications enables greater visibility and control of your sensitive data in the cloud. To learn more see, How to integrate Microsoft Information Protection with Cloud App Security.

Data loss prevention (DLP)

Data loss prevention (DLP) helps you prevent the unintentional or accidental sharing of sensitive information. When the risks of data leakage aren't entirely obvious, it's difficult to work out where exactly you should start with implementing DLP. Fortunately, DLP policies can be run in "test mode", allowing you to gauge their effectiveness and accuracy before you turn them on. DLP policies for Exchange Online can be managed through the Exchange admin center. But you can configure DLP policies for all workloads through the Security & Compliance Center.

Additional Resources

- Microsoft Defender for Cloud Apps Overview
- Get started with Microsoft Defender for Cloud Apps
- Deploying the Microsoft Information Protection scanner to automatically classify and protect files.
- How to configure a label for Rights Management protection
- What is Microsoft Information Protection?
- Data loss prevention reference

Customer Responsibility

- Responsible for designating authorized personnel to post publicly accessible information on customer-deployed resources.

Audit and Accountability (AU)

AU.L2-3.3.1

Control Summary Information	
NIST 800-53 Mapping: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	
Control : Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.	
Primary Services	**Secondary Services**
Microsoft Sentinel Microsoft Defender for Cloud Apps Log Analytics Workspace Azure Active Directory Intune/Microsoft Endpoint Manager Microsoft 365 compliance center Azure Storage	Azure Firewall Azure Web Application Firewall Microsoft Defender for Office 365 GitHub Enterprise Cloud GitHub AE

Implementation Statement:

Azure Active Directory

You can retain the audit and sign-in activity data for longer than the default retention period outlined here by routing it to an Azure storage account using Azure Monitor. For more information, see Archive Azure AD logs to an Azure storage account.

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud protects your Virtual Machines, data, storage and cloud native services against common threats. Go to Microsoft Defender for Cloud to turn on protection for your hybrid cloud workloads. You can also protect users, devices and applications with Microsoft defender for O365 and bring all your security analytics together into a unified view by connecting data sources to Microsoft Sentinel. Microsoft Sentinel's audit logs are maintained in the Azure Activity Logs, where the Azure Activity table includes all actions taken in your Microsoft Sentinel workspace.

For more information, see Integrated Threat Protection from Microsoft.

Intune/Microsoft Endpoint Manager

By default, auditing in Intune/Microsoft Endpoint Manager is enabled for all customers. This allows an organizations administrator to track and monitor events in Microsoft Intune. Audit logs include a record of activities, such as; create, update (edit), delete, assign, and remote actions all create audit events that administrators can review.

Logs can also be sent to Azure Monitor services, including storage accounts, event hubs, and log analytics. For more information: use audit logs to track and monitor events in Microsoft Intune.

Additionally, consider using Microsoft Sentinel as your Security Information and Event Management (SIEM) solution. After you connect your data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks. While Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to Create interactive reports with Azure Monitor Workbooks.

Once Microsoft Sentinel is enabled on your Azure Monitor Log Analytics workspace, every GB of data ingested into the workspace can be retained at no charge for a default retention limit. For more information on free retention limits and retention costs beyond that limit, please refer to Azure Monitor Log Analytics retention prices.

M365 Compliance Center

You can create and manage audit log retention policies in the Microsoft 365 compliance center. Audit log retention policies are part of the new Advanced Audit capabilities in Microsoft 365. An audit log retention policy lets you specify how long to retain audit logs in your organization. You can retain audit logs for up to 10 years. Advanced Audit in Microsoft 365 provides a default audit log retention policy for all organizations. This policy retains all Exchange Online, SharePoint Online, OneDrive for Business, and Azure Active Directory audit records for one year.

Enable auditing of admin activity in M365 Compliance Center. Enabling auditing for admins allows you to capture user and administrator activities in your organization.

Audited Activities in M365 Compliance Center can be granularly selected. It is recommended to review audit logs at a frequency to meet your compliance requirements. This will assist in discovering execution of privileged functions.

Azure Policies

- **AU.L2-3.3.1 Azure Policies**

Customer Responsibility

- Retaining audit records for customer-deployed resources to support security investigations and meet regulatory requirements. Audit records must be retained for the defined frequency.
- Ensuring all customer-deployed resources have the ability to generate records for the auditable events

Additional Resources

- Microsoft Defender for Identity Prerequisites
- Move your Microsoft Sentinel Logs to Long-Term Storage with Ease
- Manage cost by controlling data volume and retention in Log Analytics
- Storage size for activity logs
- Archive activity logs to a storage account
- Route activity logs to an event hub
- Integrate activity logs with Log Analytics

AU.L2-3.3.2

Control Summary Information	
NIST 800-53 Mapping: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	
Control : Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	
Primary Services	**Secondary Services**
Microsoft Sentinel M365 Compliance Center Azure Active Directory	Intune/Microsoft Endpoint Manager M365 Compliance Center

Implementation Statement:

Microsoft Sentinel

All account lifecycle operations (account creation, modification, enabling, disabling, and removal actions) and user activity in the Azure portal are audited within the Azure AD audit logs. All authentication and authorization events are audited within Azure AD sign-in logs, and any detected risks are audited in the Identity Protection logs. Stream logs directly Microsoft Sentinel Security Information and Event Management (SIEM) solution by connecting data from Azure Active Directory (AAD)

Visualize and monitor log data using Microsoft Sentinel which allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Connect logs from sources such as, Azure Active Directory, Microsoft Defender for Endpoint, O365 and Intune to Sentinel for optimal visibility of your users' activities. Learn more on how to connect your sources to Sentinel to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

M365 Compliance Center

By default, audit logging is on for Microsoft 365 and Office 365 enterprise organizations. If audit log search is not turned on, you can turn it on in compliance center or by using Exchange Online PowerShell. Audit user activity with M365 Compliance Center.

Audit user and admin activity in M365 Compliance Center. It is recommended to review audit logs at a frequency to meet your compliance requirements. Enable the Office 365 log connector to connect Office 365 to Microsoft Sentinel. This will enable you to view and analyze this data in your workbooks, query it to create custom alerts, and incorporate it to improve your investigation process, giving you more insight into your Office 365 security.

Intune/Microsoft Endpoint Manager Audit Logging

By default, auditing in Intune/Microsoft Endpoint Manager is enabled for all customers. This allows an organizations administrator to track and monitor events in Microsoft Intune. Audit logs include a record of activities, such as; create, update (edit), delete, assign, and remote actions all create audit events that administrators can review.

Logs can also be sent to Azure Monitor services, including storage accounts, event hubs, and log analytics. For more information: use audit logs to track and monitor events in Microsoft Intune.

Microsoft Compliance Center - eDiscovery & Audit

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft 365 to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can use Core eDiscovery cases to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the feature-rich Advanced eDiscovery solution in Microsoft 365.

Moreover, The Audit functionality in Microsoft 365 provides organizations with visibility into many types of audited activities across many different services in Microsoft 365. Basic Audit provides you with the ability to log and search for audited activities and power your forensic, IT, compliance, and legal investigations. Advanced Audit builds on the capabilities of Basic Audit by providing audit log retention policies, longer retention of audit records, high-value crucial events, and higher bandwidth access to the Office 365 Management Activity API.

Azure Policies

- **AU.L2-3.3.2 Azure Policies**

Customer Responsibility

- Configuring Azure auditing capabilities on customer-deployed resources to generate audit records containing the following: what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any subjects associated with the event.

Additional Resources

- Create interactive reports with Azure Monitor Workbooks
- Microsoft Sentinel and Microsoft Defender for Cloud Apps integration
- Find activity reports in the Azure portal
- Audit activity reports in the Azure Active Directory portal
- Sign-in activity reports in the Azure Active Directory portal
- How To: Investigate risk
- Stream to Azure event hub and other SIEMs
- Learn how to get visibility into your data and potential threats
- Get started detecting threats with Microsoft Sentinel, using built-in or custom rules
- Enabling auditing for admins
- How to monitor virtual machines in Azure
- How to onboard Microsoft Sentinel
- Understand Log Analytics Workspace
- How to perform custom queries in Azure Monitor

AU.L2-3.3.3

Control Summary Information	
NIST 800-53 Mapping: AU-2(3)	
Control : Review and update logged events.	
Primary Services	**Secondary Services**
Microsoft Defender for Endpoint	Microsoft Sentinel Azure Active Directory Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Microsoft 365 compliance center Exchange admin center

Implementation Statement:

Microsoft Sentinel

Review audit logged events at a defined frequency that meets Organizational requirements for example, at least annually or when changes occur. Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient. Your organization should have a defined process for determining when to review logged events and the event types should be updated based on that review. You can connect your log sources to Microsoft Sentinel to review audit logs in one centralized location. Additionally, you can review Incident reports to determine if a specific occurrence should be audited. For example, if your company experiences a security incident, and a forensics review shows the logs appear to have been deleted by a remote user. You notice that remote sessions are not currently being logged so you update the list of events to include logging all VPN sessions.

Visualize and monitor log data using Microsoft Sentinel which allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Connect logs from sources such as, Azure Active Directory, Microsoft Defender, O365 and Intune to Sentinel for optimal visibility of your users' activities. Learn more on how to connect your sources to Sentinel to support reviewing and updating logged events.

M365 Compliance Center

The Microsoft 365 compliance center provides easy access to the data and tools you need to manage to your organization's compliance needs. You can search the audit log in Microsoft 365 Compliance Center for activities performed in different Microsoft 365 services. Review the Active alerts card, which includes a summary of the most active alerts and includes a link where you can view more detailed information, such as Severity, Status, Category, and more. Go to Policies to set up policies to govern data, manage devices, and receive alerts. You can search and review the following types of user and admin activity. Learn how to search the audit log.

Customer Responsibility

- Reviewing and updating the customer-defined events for customer-deployed resources.
- Defining a process for determining when to review logged events to ensure that the current set remains necessary and sufficient. (i.e., regular frequency, after incidents, after major system changes)
- Defining and updating event log types to ensure that the current set remains necessary and sufficient.

Additional Resources

- CMMC L2 Requirements
- Azure Monitoring Contributor for creating, modifying, and updating log alerts
- Create interactive reports with Azure Monitor Workbooks
- Microsoft Sentinel and Microsoft Defender for Cloud Apps integration
- Find activity reports in the Azure portal.
- Audit activity reports in the Azure Active Directory portal
- Sign-in activity reports in the Azure Active Directory portal
- How To: Investigate risk
- Stream to Azure event hub and other SIEMs
- Learn how to get visibility into your data and potential threats

- Get started detecting threats with Microsoft Sentinel, using built-in or custom rules
- Enabling auditing for admins
- How to monitor virtual machines in Azure
- What is Microsoft Sentinel?
- Get started with log queries in Azure Monitor
- Visualize and monitor your data
- Microsoft Defender for Cloud Apps
- Turn on Microsoft 365 Defender
- Microsoft 365 security center overview

AU.L2-3.3.4

Control Summary Information	
NIST 800-53 Mapping: AU-5	
Control : Alert in the event of an audit logging process failure.	
Primary Services	**Secondary Services**
Microsoft Sentinel	Azure Active Directory Microsoft Graph Power Automate Log Analytics Azure Monitor

Implementation Statement:

Microsoft Sentinel

Connected logs from sources such as, Azure Active Directory, Azure Monitor, O365 and Intune to Sentinel provide visibility of process failure. Learn more on how to connect your sources to Sentinel. Microsoft Sentinel classifies failures up front as either transient or permanent, based on the specific type of the failure and the circumstances that led to it. Learn more about scheduled rule failures. To view the results of the alert rules you create, go to the Incidents page, where you can triage, investigate incidents, and remediate the threats. Alerts generated in Microsoft Sentinel are available

through Microsoft Graph Security. For more information, see the Microsoft Graph Security alerts documentation.

Log Alerts

Log alerts are one of the alert types that are supported in Azure Alerts. Log alerts allow you to use a Log Analytics query to evaluate resources logs every set frequency, and fire an alert based on the results. Rules can trigger one or more actions using Action Groups.

Log alerts run queries on Log Analytics data. First you should start collecting log data and query the log data for issues. You can use the alert query examples article in Log Analytics to understand what you can discover or get started on writing your own query.

Azure Monitoring Contributor is a common role that is needed for creating, modifying, and updating log alerts. Access & query execution rights for the resource logs are also needed. Partial access to resource logs can fail queries or return partial results. Learn more about configuring log alerts in Azure.

Create custom analytics rules to help you discover threats and anomalous behaviors that are present in your environment. These rules search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate, and respond to threats with automated tracking and remediation processes.

Microsoft Graph

With the Microsoft Graph Security alerts entity, you can unify and streamline management of security issues across all integrated solutions. This also enables applications to correlate alerts and context to improve threat protection and response. With the alert update capability, you can sync the status of specific alerts across different security products and services that are integrated with the Microsoft Graph Security API by updating your alerts entity.

Azure Policies

AU.L2-3.3.4 Azure Policies

Customer Responsibility

- Providing alerts in response to audit processing failures (e.g., storage quota is reached, audit hardware/software errors) of customer-deployed resources.

Additional Resources

- Azure subscription and service limits, quotas, and constraints
- Azure Monitor limits alerts
- Log Alerts in Azure Monitor
- Azure Monitoring Contributor for creating, modifying, and updating log alerts
- Learn more about configuring log alerts in Azure
- Learn about creating in log alerts in Azure
- Understand webhooks in log alerts in Azure
- Learn about Azure Alerts
- Learn more about Log Analytics
- Finding and filtering queries
- Monitor Azure AD Connect sync with Azure AD Connect Health

AU.L2-3.3.5

Control Summary Information	
NIST 800-53 Mapping: AU-6(3)	
Control : Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	
Primary Services	**Secondary Services**
Microsoft Sentinel	Log Analytics Workspace Microsoft Defender for Cloud Apps Microsoft Defender for Identity Microsoft Defender for IoT Microsoft 365 Compliance Center Microsoft Graph

Implementation Statement:

After connecting your data sources to Microsoft Sentinel, use out-of-the-box detections, built-in templates to help you create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can assign and investigate in your environment.

To learn how to automate your responses to threats, Set up automated threat responses in Microsoft Sentinel.

Microsoft 365 Compliance Center

The Microsoft 365 compliance center provides easy access to the data and tools you need to manage to your organization's compliance needs. You can search the audit log in Microsoft 365 Compliance Center for activities performed in different Microsoft 365 services. Review the Active alerts card, which includes a summary of the most active alerts and includes a link where you can view more detailed information, such as

Severity, Status, Category, and more. Go to Policies to set up policies to govern data, manage devices, and receive alerts.

Moreover, Activity Explorer allows you to monitor what is being done with your labeled content by providing a historical view of activities on this labeled content. The activity information is collected from the Microsoft 365 unified audit logs, transformed, and made available in the Activity explorer UI. Activity explorer reports on up to 30 days' worth of data.

Azure Active Directory (Azure AD) tracks user activity and creates reports that help you understand how your users access and use Azure AD services. Use the Microsoft Graph API for Azure AD to analyze the data in these reports and to create custom solutions tailored to your organization's specific needs.

Customer Responsibility

- Analyzing and correlating audit records across customer-deployed repositories.

Additional Resources

- Manage your SOC better with incident metrics in Microsoft Sentinel
- How to respond to threats using automated playbooks
- Investigate a suspicious IoT device

AU.L2-3.3.6

Control Summary Information	
NIST 800-53 Mapping: AU-7	
Control : Provide audit record reduction and report generation to support on-demand analysis and reporting.	
Primary Services	**Secondary Services**
Microsoft Defender for IoT Microsoft Sentinel	Log Analytics Workspace Azure Active Directory Microsoft 365 Compliance Center Microsoft 365 Admin Center

Implementation Statement:

Microsoft Sentinel

You can facilitate analysis and reporting several ways with Azure. Capabilities range from threat reporting in Microsoft Sentinel, log reporting in Azure Monitor and usage reporting in Azure Advisor. Azure Active Directory provides the capability to report on user sign-in, usage, and insights. The Azure AD Sign-ins report provides user sign-in patterns, quantity of sign-ins and status of sign-ins. For more information, see Sign-in activity reports in the Azure Active Directory portal.

Visualize and monitor log data using Microsoft Sentinel which allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Centralize sources to one place, such as Microsoft Sentinel SIEM solution. Connect logs from sources such as, Azure Active Directory, O365, Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for Cloud Apps Microsoft Defender for Cloud Apps and Intune to Sentinel for optimal visibility to support analysis and reporting. Learn more on how to connect your sources to Sentinel to support on demand analysis and reporting.

Microsoft 365 Admin Center

Reporting features in Microsoft 365 provides various audit reports for Azure Active Directory (Azure AD), Exchange Online, device management, supervisory review, and data loss prevention (DLP). These reports are different and separate from the Microsoft 365 activity reports. The Reports dashboard in the Microsoft 365 admin center preview displays usage activity across Microsoft 365. M icrosoft 365 global administrators, or an Exchange Online, SharePoint Online, or Skype for Business administrator, can get granular insight into the usage of that service. For example, the number of users in a particular Microsoft 365 service, the number of users that have activated Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus), and how much mail is flowing through the organization. Reports are available for the last 7, 30, 90, and 180 days.

Customer Responsibility

- Providing an audit reduction and report generation capability for customer-deployed resources, including the support of on-demand audit review, analysis, and reporting requirements, and after-the-fact investigations of security incidents.

Additional Resources

- Continuously export Security Center data
- Threat indicators for cyber threat intelligence in Microsoft Sentinel
- Tutorial: Investigate incidents with Microsoft Sentinel
- Sign-ins logs in Azure Active Directory
- Tutorial: Automate tasks to process emails by using Azure Logic Apps, Azure Functions, and Azure Storage
- View export alerts and recommendations in Azure Monitor
- Manual one-time export of alerts and recommendations
- Monitoring and reporting in Azure

AU.L2-3.3.7

Control Summary Information	
NIST 800-53 Mapping: AU-8, AU-8(1)	
Control : Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	
Primary Services	**Secondary Services**
Windows Time Service	

Implementation Statement:

Windows Time Service

Time servers are synced to UTC and are accessed from other computers to provide scalability and robustness. Every computer has time synchronization service running that knows what time servers to use and periodically checks if computer clock needs to be corrected and adjusts time if needed.

Azure hosts are synchronized to internal Microsoft time servers that take their time from Microsoft-owned Stratum 1 devices, with GPS antennas. Virtual machines in Azure can either depend on their host to pass the accurate time (host time) on to the VM or the VM can directly get time from a time server, or a combination of both. For more information, see Time sync in Azure.

Customer Responsibility

- For generating time stamps for audit records of CUSTOMER-deployed resources using the internal system clock.
- Comparing internal system clocks with an authoritative time source at the required frequency.
- Synchronizing internal system clocks to the authoritative time source

Additional Resources

- Windows Time service tools and settings
- How to configure an authoritative time server in Windows Server
- How to configure time synchronization for Azure Windows compute resources
- How to configure time synchronization for Azure Linux compute resources

AU.L2-3.3.8

Control Summary Information	
NIST 800-53 Mapping: AU-6(7), AU-9	
Control : Protect audit information and audit logging tools from unauthorized access, modification and deletion.	
Primary Services	**Secondary Services**
Azure RBAC	Microsoft Sentinel Microsoft 365 Compliance Center Azure Storage Log Analytics Workspace Conditional Access

Implementation Statement:

Azure RBAC

Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure. Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel to protect audit information and Sentinel from unauthorized access, modification and deletion. The different roles give you fine-grained control over what users of Microsoft Sentinel can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly, or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel will inherit.

- **Custom roles.** In addition to, or instead of, using Azure built-in roles, you can create Azure custom roles for Microsoft Sentinel. Azure custom roles for Microsoft Sentinel are created the same way you create other Azure custom roles, based on specific permissions to Microsoft Sentinel and to Azure Log Analytics resources.
- **Log Analytics RBAC.** You can use the Log Analytics advanced Azure role-based access control across the data in your Microsoft Sentinel workspace. This includes both data type-based Azure RBAC and resource-context Azure RBAC. For more information, see:

- Manage log data and workspaces in Azure Monitor
- Resource-context RBAC for Microsoft Sentinel
- Table-level RBAC

Resource-context and table-level RBAC are two methods of providing access to specific data in your Microsoft Sentinel workspace without allowing access to the entire Microsoft Sentinel experience.

Microsoft 365 Compliance Center

Using the new Permissions page in the Microsoft 365 compliance center, you can manage permissions to users for compliance tasks in features like device management, data loss prevention, eDiscovery, insider risk management, retention, and many others. Users can perform only the compliance tasks that you explicitly grant them access to. To view the Permissions tab in the Microsoft 365 compliance center, users need to be a global administrator or need to be assigned the Role Management role. The Role Management role allows users to view, create, and modify role groups.

Customer Responsibility

- Preventing unauthorized access to audit information and tools.

Additional Resources

- Permissions in Microsoft Sentinel
- Custom role examples
- Manage access to log data and workspaces in Azure Monitor
- Log Analytics data security

AU.L2-3.3.9

Control Summary Information	
NIST 800-53 Mapping: AU-6(7), AU-9	
Control : Limit management of audit logging functionality to a subset of privileged users.	
Primary Services	**Secondary Services**
Azure RBAC	Conditional Access Microsoft 365 Security Center Log Analytics Workspace Intune/Microsoft Endpoint Manager Microsoft Cloud App Security Privileged Identity Management (PIM)

Implementation Statement:

Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure. Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel to limit management of audit logging functionality to a subset of privileged users. The different roles give you fine-grained control over what users of Microsoft Sentinel can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly, or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel will inherit.

- **Custom roles.** In addition to, or instead of, using Azure built-in roles, you can create Azure custom roles for Microsoft Sentinel. Azure custom roles for Microsoft Sentinel are created the same way you create other Azure custom roles, based on specific permissions to Microsoft Sentinel and to Azure Log Analytics resources.
- **Log Analytics RBAC.** You can use the Log Analytics advanced Azure role-based access control across the data in your Microsoft Sentinel workspace. This includes both data type-based Azure RBAC and resource-context Azure RBAC. For more information, see:
    - Manage log data and workspaces in Azure Monitor

- Resource-context RBAC for Microsoft Sentinel
- Table-level RBAC

Resource-context and table-level RBAC are two methods of providing access to specific data in your Microsoft Sentinel workspace without allowing access to the entire Microsoft Sentinel experience.

Microsoft 365 Compliance Center

Using the new Permissions page in the Microsoft 365 compliance center, you can manage permissions to users for compliance tasks in features like device management, data loss prevention, eDiscovery, insider risk management, retention, and many others. Users can perform only the compliance tasks that you explicitly grant them access to. To view the Permissions tab in the Microsoft 365 compliance center, users need to be a global administrator or need to be assigned the Role Management role. The Role Management role allows users to view, create, and modify role groups.

Customer Responsibility

- Restricting the management of customer-controlled audit resources to authorized users.

Additional Resources

- Permissions in Microsoft Sentinel
- Custom role examples
- Manage access to log data and workspaces in Azure Monitor
- View activity logs for Azure RBAC changes

Awareness and Training (AT)

AT.L2-3.2.1

Control Summary Information	
NIST 800-53 Mapping: AT-2, AT-3	
Control : Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	
Primary Services	**Secondary Services**
	Microsoft 365 Defender Azure Active Directory Microsoft Cloud App Security Microsoft Defender for Identity Microsoft 365 Web Apps Teams

Implementation Statement:

Viva Learning is a centralized learning hub in Microsoft Teams that lets you seamlessly integrate learning and building skills into your day. In Viva Learning, your team can discover, share, recommend, and learn from content libraries provided by both your organization and partners.

Customer Responsibility

- Providing role-based security training to users before authorizing access to customer-deployed resources or performing assigned duties.
- Providing role-based security training to all identified roles when required by changes to customer-deployed resources.
- Providing ongoing, periodic role-based security training to all identified roles.

AT.L2-3.2.2

Control Summary Information	
NIST 800-53 Mapping: AT-2, AT-3	
Control : Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	
Primary Services	**Secondary Services**
	Microsoft Defender for Office 365 Microsoft Learn Microsoft 365 Defender portal (Learning Hub)

Implementation Statement:

Microsoft Defender for Office 365

If your organization has Microsoft Defender for Office 365 Plan 2, which includes Threat Investigation and Response capabilities, you can use Attack Simulator in the M365 Compliance Center to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

Attack simulation training in Microsoft Defender for Office 365 lets you run benign cyberattack simulations on your organization to test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks. For getting started information about Attack simulation training, see Get started using Attack simulation training.

Microsoft Learn

Whether you're just starting or an experienced professional, Microsoft Learn helps organizations train their personnel on role based and security-related duties. To start learning, visit the Microsoft Learn page.

Customer Responsibility

- Providing role-based security training to users before authorizing access to customer-deployed resources or performing assigned duties.

- Providing role-based security training to all identified roles when required by changes to customer-deployed resources.
- Providing ongoing, periodic role-based security training to all identified roles.

AT.L2-3.2.3

Control Summary Information	
NIST 800-53 Mapping: AT-2(2)	
Control : Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
Primary Services	**Secondary Services**
	Microsoft Defender for Office 365 Microsoft Learn Microsoft 365 Defender portal (Learning Hub)

Implementation Statement:

If your organization has Microsoft Defender for Office 365 Plan 2, which includes Threat Investigation and Response capabilities, you can use Attack Simulator in the M365 Compliance Center to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

Attack simulation training in Microsoft Defender for Office 365 lets you run benign cyberattack simulations on your organization to test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks. For getting started information about Attack simulation training, see Get started using Attack simulation training.

Customer Responsibility

- Providing training on insider threats.

Configuration Management (CM)

CM.L2-3.4.1

Control Summary Information	
NIST 800-53 Mapping: CM-2, CM-6, CM-8, CM-8(1)	
Control : Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.	
Primary Services	**Secondary Services**
Azure Automation Change Tracking and Inventory Microsoft Defender for IoT Intune/Microsoft Endpoint Manager Microsoft Defender for Endpoint GitHub Enterprise Cloud GitHub AE	Azure Virtual Machines Microsoft 365 Lighthouse Azure Lighthouse

Implementation Statement:

Azure Automation

Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes in any cloud or on-premises datacenter. The service also imports DSC Resources, and assigns configurations to target nodes, all in the cloud. You can access Azure Automation State Configuration in the Azure portal by selecting State configuration (DSC) under Configuration Management.

Azure Automation State Configuration provides several advantages over the use of DSC outside of Azure. This service enables scalability across thousands of machines quickly and easily from a central, secure location. You can easily enable machines, assign them declarative configurations, and view reports showing each machine's compliance with the desired state you specify.

Change Tracking and Inventory

Change Tracking and Inventory feature in Azure Automation allows you to track changes in virtual machines hosted in Azure, on-premises, and other cloud environments to help you pinpoint operational and environmental issues with software managed by the Distribution Package Manager. Change Tracking and Inventory makes use of Microsoft Defender for Cloud File Integrity Monitoring (FIM) to examine operating system and application files, and Windows Registry. While FIM monitors those entities, Change Tracking and Inventory natively tracks:

- Software changes
- Windows services
- Linux daemons

Microsoft Defender for IoT

Security baselines for Azure focus on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS). Our baselines provide guidance for the control areas listed in the Azure Security Benchmark. The content is grouped by the security controls defined by the Azure Security Benchmark and the related guidance applicable to Microsoft Defender for IoT

To see how Microsoft Defender for IoT completely maps to the Azure Security Benchmark, see the full Microsoft Defender for IoT security baseline mapping file in GitHub.

Further, Azure CMMC Blueprints sample provides governance guardrails using Azure Policy that help you assess specific CMMC controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for CMMC L2.

Intune/Microsoft Endpoint Manager & Microsoft Defender for Endpoint

Microsoft Intune reports allows you to monitor the health and activity of endpoints more effectively and proactively across your organization, and also provides other reporting data across Intune such as inventory. For example, you will be able to see reports about device compliance, device health, and device trends. In addition, you can create custom reports to obtain more specific data. Learn more about Intune Reports. To learn how to view device details such as hardware information and App installs see, device details in Intune.

Microsoft Defender for Endpoint provides the capability to inventory software on devices. The Software inventory page opens with a list of software installed in your network, including the vendor's name, weaknesses found, threats associated with them, exposed devices, impact to exposure score, and tags. You can filter the list view based on weaknesses found in the software, threats associated with them, and tags like whether the software has reached end-of-support. Access the Software inventory page by selecting software inventory from the threat and vulnerability management navigation menu in the Microsoft Defender Security Center. View software on specific devices in the individual device's pages from the devices list.

To optimize device management through Intune, connect Intune to Defender for Endpoint. Device configuration management works closely with Intune device management to establish the inventory of the devices in your organization and the baseline security configuration. You will be able to track and manage configuration issues on Intune-managed Windows 10 devices.

The Windows Intune security baseline provides a comprehensive set of recommended settings needed to securely configure devices running Windows, including browser settings, PowerShell settings, as well as settings for some security features like Microsoft Defender Antivirus. In contrast, the Defender for Endpoint baseline provides settings that optimize all the security controls in the Defender for Endpoint stack, including settings for endpoint detection and response (EDR) as well as settings also found in the Windows Intune security baseline. For more information about each baseline, see:

- Windows security baseline settings for Intune
- Microsoft Defender for Endpoint baseline settings for Intune

Virtual Machine

You can establish and maintain system baselines with Azure virtual machine with inventory collection. You can enable inventory tracking for an Azure virtual machine from the virtual machine's resource page. You can collect and view the following inventory information on your computers:

- Windows software (Windows applications and Windows updates), services, files, and Registry keys
- Linux software (packages) daemons, and files

This method provides a browser-based user interface for setting up and configuring inventory collection. For more information, see Manage an Azure virtual machine with inventory collection.

Microsoft 365 Lighthouse

Microsoft 365 Lighthouse baselines provide a repeatable and scalable way for you to assess and manage Microsoft 365 security settings across multiple customer tenants. Baselines also help monitor core security policies and tenant compliance standards with configurations that secure users, devices, and data. Lighthouse simplified configuration management by recommending security configuration baselines tailored to SMB customers and providing multi-tenant views across all customer environments.

Customer Responsibility

- Developing, documenting, and maintaining a baseline configuration of customer-deployed resources.
- Developing and documenting an inventory of customer-deployed resources, that supports tracking and reporting, and includes any information the customer has deemed necessary to achieve effective accountability.

Additional Resources

- See the first security control: Network security
- Download the Azure Security Benchmark in spreadsheet format
- Azure security standards for strategy and architecture: Strategy and architectural recommendations to shape your environment's security posture.
- Azure security benchmarks: Specific configuration recommendations for securing Azure environments.
- Azure security baseline training
- Details of the CMMC L2 Regulatory Compliance built-in initiative
- Intune reports
- Software inventory - threat and vulnerability management
- Use security baselines to configure Windows 10 devices in Intune
- Increase compliance to the Microsoft Defender for Endpoint security baseline

CM.L2-3.4.2

Control Summary Information	
NIST 800-53 Mapping: CM-2, CM-6,CM-8,CM-8(1)	
Control : Establish and enforce security configuration settings for information technology products employed in organizational systems.	
Primary Services	**Secondary Services**
Azure Active Directory Intune/Microsoft Endpoint Manager Azure Automation Microsoft Defender for Endpoint	Log Analytics Agent App Locker Windows Defender for Application Control Microsoft 365 Admin Center Conditional Access

Implementation Statement:

Microsoft Defender for Endpoint

With Microsoft Defender for Endpoint (MDE), you can now deploy security configurations from Microsoft Endpoint Manager directly to your onboarded devices without requiring a full Microsoft Endpoint Manager device enrollment. This capability is known as Security Management for Microsoft Defender for Endpoint. With this capability, devices that aren't managed by a Microsoft Endpoint Manager service can receive security configurations for Microsoft Defender directly from Endpoint Manager.

Azure Automation

Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes in any cloud or on-premises datacenter. The service also imports DSC Resources, and assigns configurations to target nodes, all in the cloud. You can access Azure Automation State Configuration in the Azure portal by selecting State configuration (DSC) under Configuration Management.

Azure Automation State Configuration provides several advantages over the use of DSC outside of Azure. This service enables scalability across thousands of machines quickly and easily from a central, secure location. You can easily enable machines, assign them

declarative configurations, and view reports showing each machine's compliance with the desired state you specify.

Intune/Microsoft Endpoint Manager

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory.

Microsoft Intune includes settings and features you can enable or disable on different devices within your organization to allow only essential capabilities. These settings and features are added to "configuration profiles". You can create profiles for different devices and different platforms, including iOS/iPadOS, Android device administrator, Android Enterprise, and Windows. Then, use Intune to apply or "assign" the profile to the devices.

Administrative templates include hundreds of settings that you can configure for Internet Explorer, Microsoft Edge, OneDrive, remote desktop, Word, Excel, and other Office programs. These templates give administrators a simplified view of settings similar to group policy, and they are 100% cloud based.

Additionally, you can use Intune's preconfigured security baselines to establish and enforce security configuration settings that will help you secure and protect your users and devices. You can also customize the baselines you deploy to enforce only those settings and values you require. To learn more about security baselines in Intune, see Available security baselines.

Microsoft Defender for Cloud Apps

Consider exploring Microsoft Defender for Cloud Apps' adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application

runs other than the ones you have defined as safe. Requirements include Microsoft Defender for Cloud . Learn more about using adaptive application controls.

This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

- Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
- Comply with your organization's security policy that dictates the use of only licensed software.
- Avoid unwanted software to be used in your environment.
- Avoid old and unsupported apps to run.
- Prevent specific software tools that are not allowed in your organization.
- Enable IT to control the access to sensitive data through app usage.

Requirements include Microsoft Defender for Cloud . Learn more about using adaptive application controls.

Customer Responsibility

- Developing, documenting, and maintaining a baseline configuration of customer-deployed resources.

Additional Resources

- Five steps to securing your identity infrastructure
- Azure security baseline for Security Center
- Azure security baseline for Azure App Configuration
- Azure security baseline for Virtual Network
- CMMC L2 blueprint sample
- CIS Azure Foundations Benchmark
- Azure Active Directory deployment plans

CM.L2-3.4.3

Control Summary Information	
NIST 800-53 Mapping: CM-3	
Control : Track, review, approve or disapprove and log changes to organizational systems.	
Primary Services	**Secondary Services**
Microsoft Defender for Cloud Apps Power Automate Change Tracking and Inventory GitHub Enterprise Cloud GitHub AE	Log Analytics Workspace Azure Active Directory Intune/Microsoft Endpoint Manager Microsoft 365 Defender

Implementation Statement:

Microsoft Defender for Cloud Apps/Change Tracking and Inventory

Enable Change Tracking and Inventory to track changes in virtual machines hosted in Azure, on-premises, and other cloud environments. Change Tracking and Inventory makes use of Microsoft Defender for Cloud Apps File Integrity Monitoring (FIM) to examines operating system and application files, and Windows Registry. To track Azure Resource Manager property changes, see the Azure Resource Graph change history.

- To enable from an Automation account, see Enable Change Tracking and Inventory from an Automation account.
- To enable from the Azure portal, see Enable Change Tracking and Inventory from the Azure portal.
- To enable from a runbook, see Enable Change Tracking and Inventory from a runbook.
- To enable from an Azure VM, see Enable Change Tracking and Inventory from an Azure VM.

GitHub AE

Track, review, approve or disapprove and log changes to organizational systems using GitHub AE pull request. After initializing a pull request, you will see a review page that shows a high-level overview of the changes between your branch (the compare branch) and the repository's base branch. You can add a summary of the proposed changes,

review the changes made by commits, add labels, milestones, and assignees, and @mention individual contributors or teams.

For more information, see:

- About pull requests
- Creating a pull request

Intune/Microsoft Endpoint Manager

Use Intune to assist in the tracking, review and approval process of configuration changes to the organizational systems. Intune provides the capability to troubleshoot issues with policy as well as the ability to see if the policy is correctly applied. Having high level visibility of your policy assists in review to determine if changes are required. Microsoft Intune reports allows you to monitor the health and activity of endpoints more effectively and proactively across your organization, and also provides other reporting data across Intune. For example, you will be able to see reports about device compliance, device health, and device trends. This will help you review and track areas of improvement to determine if changes are required to perhaps create more restrictive conditional access policies.

Additionally, you can monitor Intune configuration changes such as, a modification to policy in audit logs. You can send log files from Intune to Log Analytics, there you can create alerts to automatically notify you of an unauthorized change.

To learn more, see:

- Use audit logs to track and monitor events in Microsoft Intune
- Create a Log Analytics workspace in the Azure portal
- Intune reports
- Troubleshoot policies and profiles and in Intune

Microsoft Defender for Endpoint

With Microsoft Defender for Endpoint (MDE), you can approve or reject pending remediation actions. These remediation actions are not taken unless and until your security operations team approves them. We recommend reviewing and approving any pending actions as soon as possible so that your automated investigations complete in a timely manner.

Power Automate

With Power Automate, you can manage the approval of documents or processes across several services, including SharePoint, Dynamics 365, Salesforce, OneDrive for Business, Zendesk, or WordPress.

To create an approval workflow, add the Approvals - Start and wait for an approval action to any flow. After you add this action, your flow can manage the approval of documents or processes. For example, you can create document approval flows for approval of log changes to the organizational systems. Approvers can respond to requests from their email inbox, the approvals center in Power Automate, or the Power Automate app.

Customer Responsibility

- Reviewing proposed configuration-controlled changes to customer-deployed resources.
- Documenting configuration-controlled changes associated with customer-deployed resources
- Implementing configuration-controlled changes approved
- Retaining a record of configuration-controlled changes to customer-deployed resources.

Additional Resources

- Search for role group changes or admin audit logs in Exchange Online
- Azure AD audit activity reference
- Security Control: Logging and Monitoring
- Get resource changes

CM.L2-3.4.4

Control Summary Information	
NIST 800-53 Mapping: CM-4	
Control : Analyze the security impact of changes prior to implementation.	
Primary Services	**Secondary Services**
GitHub Enterprise Cloud GitHub AE Azure DevTest Labs Microsoft 365 for enterprise Test Lab	Intune/Microsoft Endpoint Manager Microsoft Defender Endpoint Windows Virtual Desktop

Implementation Statement:

Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required. Changes to IT systems can cause unforeseen problems and have unintended consequences for both users and the security of the operating environment. Analyze the security impact of changes prior to implementation by utilizing test environments. Use purpose-built, managed developer services like Azure DevTest Labs, GitHub Code spaces, and Windows Virtual Desktop to easily manage and optimize dev/test environments, tenants, and subscriptions, without sacrificing governance, cost controls, or security.

This can uncover and mitigate potential problems before they occur. Configuration changes should be tested, validated and documented before installing them on the operational system.

Not all features or changes have the potential to impact your security or compliance stature, so it might not be necessary to deeply analyze every single change. For changes that are impactful, Microsoft provides configuration options for controlling related features. To help users adopt new features, by default, these changes are generally on - action is required on your part to disable or limit these features. Microsoft 365 changes can be planned or unplanned, depending on the nature of the changes. For example, security updates aren't always planned, because they're reactions to emergent risks or

issues in our products or services. Responsibility for managing these changes is shared between Microsoft and you as the administrator of your Microsoft 365 tenant. Microsoft provides various release options and tools to help control and deploy changes in a manner that aligns with your strategy. Microsoft 365 changes are released to both services (like SharePoint Online and Teams) and clients, referred to as Microsoft 365 Apps (like Microsoft Word, Excel, and PowerPoint). Services and clients have different release channels and deployment controls, so it's important to understand the differences as you implement your release management strategy.

Customer Responsibility

- Analyzing proposed changes to customer-deployed resources to determine potential security impacts prior to implementation.

Additional Resources

- The simulated enterprise base configuration
- Azure DevTest Labs
- Microsoft 365 for enterprise Test Lab Guides
- Evaluate the impact of Conditional Access policies before enabling widely with report-only mode

CM.L2-3.4.5

Control Summary Information	
NIST 800-53 Mapping: CM-5	
Control : Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC Change Tracking and Inventory Power Automate GitHub Enterprise Cloud GitHub AE	Azure Firewall Network Security Groups Azure Web Application Firewall Virtual Network Conditional Access Intune/Microsoft Endpoint Manager Microsoft 365 admin center Teams

Implementation Statement:

Azure Active Directory

Using Azure role-based access control (Azure RBAC), users, groups, and applications from that directory can be granted access to resources in the Azure subscription. For example, a storage account can be placed in a resource group to control access to that specific storage account using Azure AD. Access to Azure Storage can be controlled by Azure Active Directory (Azure AD), which enforces tenant isolation and implements robust measures to prevent access by unauthorized parties, including Microsoft insiders. More information about Azure AD tenant isolation is available from a white paper Azure Active Directory Data Security Considerations.

Learn about security considerations for physical isolated on-premises deployments (e.g., bare metal) vs. logically isolated cloud-based deployments (e.g., Azure).

Additionally, configure Conditional Access policies that require managed devices to access certain cloud apps in your environment. Policies should be configured to require a device to be marked as compliant by Intune/Microsoft Endpoint Manager. Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps,

and on-premises apps. Learn more about requiring managed devices with Conditional Access in Azure Active Directory.

You can manage Microsoft 365 user accounts in several different ways, depending on your configuration. You can manage user accounts in the Microsoft 365 admin center, PowerShell, in Active Directory Domain Services (AD DS), or in the Azure Active Directory (Azure AD) admin portal. User accounts are synchronized with Microsoft 365 from AD DS, so you must use on-premises AD DS tools to manage user accounts.

Teams

The Approvals app is available as a personal app for all Microsoft Teams users. The Approvals app provides a simple way to bring auditing, compliance, accountability, and workflows to both structured and unstructured Approvals in Teams. From the Teams Approvals app, users have access to create new Approvals and view Approvals that they have sent and received. Users won't have access to Approvals that are created by others unless they're either a responder or a viewer of the request.

Power Automate

Whether you need written acknowledgment from your manager or a formal authorization from a diverse group of stakeholders, getting things approved is part of almost every organization. With the approvals capability in Power Automate, you can automate sign-off requests and combine human decision-making for workflows.

Customer Responsibility

- Enforcing logical access restrictions when making changes to customer-deployed resources.

Additional Resources

- Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
- Configure Azure Storage firewalls and virtual networks
- How to: Require approved client apps for cloud app access with Conditional Access
- Windows Defender Application Control and AppLocker Overview

CM.L2-3.4.6

Control Summary Information	
NIST 800-53 Mapping: CM-7	
Control : Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
Primary Services	**Secondary Services**
Azure Active Directory Intune/ Microsoft Endpoint Manager	Microsoft 365 Defender Conditional Access

Implementation Guidance:

Least Functionality Requirements

- Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.
- Limit component functionality to a single function per device (e.g. database server, Email servers, web server, etc.), where feasible.
- Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure, in accordance Restricted List of Ports, Protocols, and/or Services.
- Identify and remove/disable unauthorized and/or non-secure functions, ports, protocols, services, and applications.
- Prevent program execution regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.

Implementation Statement:

Azure firewall/App Firewall

Review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer

Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as Azure firewall and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

For more information see:

- Azure APP Service Access Restriction
- Azure Firewall Standard
- Azure Firewall Premium
- Azure Firewall Manager

Microsoft Defender for Cloud

Consider exploring Microsoft Defender for Cloud's adaptive application controls. Adaptive application controls are an intelligent and automated solution for defining allow lists of known-safe applications for your machines. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

Azure Blueprints

Take into consideration the CIS Benchmarks, Azure Blueprints and Policy in development of operating system images, configuration scripts and configuration files deployed with the system. The baselines can help validate that only essential functions, ports, protocols, and services are enabled. Keep provisioned infrastructure and applications in compliance by using Azure Blueprints. Including an Azure policy in a blueprint enables the creation of the right pattern or design during assignment of the blueprint. The policy inclusion makes sure that only approved or expected changes can be made to the environment to protect ongoing compliance to the intent of the blueprint.

Intune/Microsoft Endpoint Manager

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory.

Microsoft Intune includes settings and features you can enable or disable on different devices within your organization to allow only essential capabilities. These settings and features are added to "configuration profiles". You can create profiles for different devices and different platforms, including iOS/iPadOS, Android device administrator, Android Enterprise, and Windows. Then, use Intune to apply or "assign" the profile to the devices.

Administrative templates include hundreds of settings that you can configure for Internet Explorer, Microsoft Edge, OneDrive, remote desktop, Word, Excel, and other Office programs. These templates give administrators a simplified view of settings similar to group policy, and they are 100% cloud based.

Group Policy analytics analyzes your on-premises GPOs, and shows which policy settings are supported, deprecated, and more.

Azure Active Directory

Managed identities provide Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without exposing credentials. There are two types of system managed identities.

- A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that is trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it is enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.

- A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that is trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it is assigned.

For more information, see:

- What are managed identities for Azure resources?
- Create a user-assigned managed identity

Microsoft 365 Defender

The application governance add-on feature to Defender for Cloud Apps is now available in Microsoft 365 Defender. App governance provides a security and policy management capability designed for OAuth-enabled apps that access Microsoft 365 data through Microsoft Graph APIs. App governance delivers full visibility, remediation, and governance into how these apps and their users access, use, and share your sensitive data stored in Microsoft 365 through actionable insights and automated policy alerts and actions.

Customer Responsibility

- Configuring customer-deployed resources to only provide essential capabilities (e.g., disabling extraneous services that may be provided by default, using a system for a single function rather than a system supporting multiple functions, restricting or prohibiting unused or unnecessary functions, ports, protocols, or services).

Additional Resources

- Use a Windows VM system-assigned managed identity to access Resource Manager
- Use a Linux VM system-assigned managed identity to access Resource Manager
- How to use managed identities for App Service and Azure Functions
- How to use managed identities with Azure Container Instances
- Implementing Managed Identities for Microsoft Azure Resources
- Tutorial: Create and manage policies to enforce compliance

- Configure device restriction settings in Microsoft Intune

CM.L2-3.4.7

Control Summary Information	
NIST 800-53 Mapping: CM-7(1), CM-7(2)	
Control : Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.	
Primary Services	**Secondary Services**
Network Security Groups Azure Firewall Azure Web Application Firewall Azure Active Directory Intune/Microsoft Endpoint Manager	Microsoft Defender for IoT Windows Defender Application Control App Locker Microsoft Defender for Cloud Microsoft 365 Defender Conditional Access

Implementation Statement:

Azure firewall/App Firewall

Review programs, functions, ports, protocols and services provided by information systems or individual components of information systems, to determine which are candidates for restricting or disabling (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as Azure firewall and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

For more information see:

- Azure APP Service Access Restriction
- Azure Firewall Standard

- Azure Firewall Premium
- Azure Firewall Manager

Network Security Groups

Network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify to create an augmented security rule.

Azure Active Directory

Managed identities provide Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without exposing credentials. There are two types of system managed identities.

- A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that is trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it is enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.
- A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that is trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it is assigned.

For more information, see:

- What are managed identities for Azure resources?
- create a user-assigned managed identity

Intune/Microsoft Endpoint Manager

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory.

Consider exploring Microsoft Defender for Cloud Apps' adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

- Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
- Comply with your organization's security policy that dictates the use of only licensed software.
- Avoid unwanted software to be used in your environment.
- Avoid old and unsupported apps to run.
- Prevent specific software tools that are not allowed in your organization.
- Enable IT to control the access to sensitive data through app usage.

Requirements include Microsoft Defender for Cloud for Servers. Learn more about using adaptive application controls.

Microsoft 365 Defender

The Tenant Allow/Block List in the Microsoft 365 Defender portal gives you a way to manually override the Microsoft 365 filtering verdicts. The Tenant Allow/Block List is used during mail flow for incoming messages (does not apply to intra-org messages) and at the time of user clicks.

If you override the allow or block verdict in the spoof intelligence insight, the spoofed sender becomes a manual allow or block entry that only appears on the Spoof tab in the Tenant Allow/Block List. You can also manually create allow or block entries for spoofed senders before they're detected by spoof intelligence.

Microsoft Defender for Cloud Apps

Protect your organization by monitoring and controlling cloud app use with any IdP solution and the Defender for Cloud Apps Conditional Access App Control. Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of a session using its device as a condition, create both a conditional access policy AND a session policy. You can create policies that prevent the use of functions that might pose a threat to security. For example, you could create a policy to block download capabilities for locations that aren't part of your corporate network.

Microsoft Defender for Cloud

Consider exploring Microsoft Defender for Cloud's adaptive application controls. Adaptive application controls are an intelligent and automated solution for defining allow lists of known-safe applications for your machines. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

Azure Blueprints

Take into consideration the CIS Benchmarks, Azure Blueprints and Policy in development of operating system images, configuration scripts and configuration files deployed with the system. The baselines can help validate that only essential functions, ports, protocols, and services are enabled. Keep provisioned infrastructure and applications in compliance by using Azure Blueprints. Including an Azure policy in a blueprint enables the creation of the right pattern or design during assignment of the blueprint. The policy inclusion makes sure that only approved or expected changes can be made to the environment to protect ongoing compliance to the intent of the blueprint.

AppLocker

AppLocker advances the app control features and functionality of Software Restriction Policies. AppLocker contains new capabilities and extensions that allow you to create rules to allow or deny apps from running based on unique identities of files and to specify which users or groups can run those apps.

Azure Policies

- **CM.L2-3.4.7 Azure Policies**

Customer Responsibility

- Configuring customer-deployed resources to only provide essential capabilities (e.g., disabling extraneous services that may be provided by default, using a system for a single function rather than a system supporting multiple functions).
- Prohibiting or restricting the use of specific functions, ports, protocols, and/or services to provide least functionality.
- Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services to include a defined frequency of reviews.

Additional Resources

- Virtual network integration for Azure services
- How network security groups work
- Windows Defender Application Control and AppLocker Overview

CM.L2-3.4.8

Control Summary Information	
NIST 800-53 Mapping: CM-7(4), CM-7(5)	
Control : Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	
Primary Services	**Secondary Services**
Azure Virtual Machines Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Microsoft Defender SmartScreen	Azure Firewall Network Security Groups Azure Web Application Firewall Conditional Access Microsoft Defender for Endpoint GitHub Enterprise Cloud GitHub AE

Implementation Statement:

Microsoft Defender for Cloud Apps

Consider exploring Microsoft Defender for Cloud Apps' adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

- Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
- Comply with your organization's security policy that dictates the use of only licensed software.
- Avoid unwanted software to be used in your environment.
- Avoid old and unsupported apps to run.

- Prevent specific software tools that are not allowed in your organization.
- Enable IT to control the access to sensitive data through app usage.

Requirements include Microsoft Defender for Cloud . Learn more about using adaptive application controls.

Microsoft Defender SmartScreen & Microsoft Defender for Endpoint

Potentially unwanted applications (PUA) are a category of software that can cause your machine to run slowly, display unexpected ads, or at worst, install other software that might be unexpected or unwanted. In Chromium-based Edge with PUA protection turned on, Microsoft Defender SmartScreen protects you from PUA-associated URLs. Although Microsoft Defender for Endpoint has its own blocklist based upon a data set managed by Microsoft, you can customize this list based on your own threat intelligence. If you create and manage indicators in the Microsoft Defender for Endpoint portal, Microsoft Defender SmartScreen respects the new settings.

Azure Active Directory

Managed identities provide Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without exposing credentials. There are two types of system managed identities.

- A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that is trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it is enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.
- A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that is trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it is assigned.

For more information, see:

- What are managed identities for Azure resources?
- create a user-assigned managed identity

Intune/Microsoft Endpoint Manager

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory.

Network Security Groups

Network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify to create an augmented security rule.

Azure Policies

- **CM.L2-3.4.8 Azure Policies**

Customer Responsibility

- Identifying software programs authorized to execute on customer-deployed resources.
- Employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on customer-deployed resources.

Additional Resources

- Windows Defender Application Control and AppLocker Overview

CM.L2-3.4.9

Control Summary Information	
NIST 800-53 Mapping: CM-11	
Control : Control and monitor user-installed software.	
Primary Services	**Secondary Services**
Microsoft Sentinel Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Azure Active Directory Log Analytics Agent Azure Monitor	Microsoft Defender for Endpoint Microsoft Defender for Identity Microsoft 365 Admin Center Windows Defender Application Control AppLocker GitHub Enterprise Cloud GitHub AE

Implementation Statement:

Microsoft Defender for Cloud Apps

Consider exploring Microsoft Defender for Cloud Apps' adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

- Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
- Comply with your organization's security policy that dictates the use of only licensed software.
- Avoid unwanted software to be used in your environment.
- Avoid old and unsupported apps to run.
- Prevent specific software tools that are not allowed in your organization.
- Enable IT to control the access to sensitive data through app usage.

Requirements include Microsoft Defender for Cloud . Learn more about using adaptive application controls.

Change Tracking and Inventory

Change Tracking and Inventory forwards data to Azure Monitor Logs, and this collected data is stored in a Log Analytics workspace. The File Integrity Monitoring (FIM) feature is available only when Microsoft Defender for Cloud is enabled. FIM uploads data to the same Log Analytics workspace as the one created to store data from Change Tracking and Inventory. Machines connected to the Log Analytics workspace use the Log Analytics agent to collect data about changes to installed software, Microsoft services, Windows registry and files, and Linux daemons on monitored servers. When data is available, the agent sends it to Azure Monitor Logs for processing. Azure Monitor Logs applies logic to the received data, records it, and makes it available for analysis. Learn more about enabling Change Tracking and Inventory.

Intune/Microsoft Endpoint Manager

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory.

Azure Active Directory

There are several methods to controlling user-installed software in Azure. One of the most effective methods for controlling user-installed software is enforcing least privilege, role- based access control (RBAC). Azure Active Directory Privileged Identity Management allows you to manage administrator privileges for users and groups. For more information, see Deploy Privileged Identity Management (PIM).

Microsoft Sentinel

Connect your data sources to Microsoft Sentinel to visualize and monitor the data in one central location using Microsoft Sentinel. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates

to allow you to quickly gain insights across your data as soon as you connect a data source.

GitHub AE

GitHub Packages is a software package hosting service that allows you to host your software packages privately for specified users or internally for your enterprise and use packages as dependencies in your projects. GitHub Packages combines your source code and packages in one place to provide integrated permissions management, so you can centralize your software development on GitHub AE. Learn more about GitHub Packages and Managing GitHub packages.

Microsoft 365 admin center

As a Microsoft 365 admin, you can choose to do the following tasks on the Office installation options page in the Microsoft 365 admin center:

- Choose how often to get feature updates for Office.
- Manage which version of Office is installed, including.
- Roll back to a previous version.
- Skip an upcoming version.
- Choose whether users can install Office on their own devices.

Azure Policies

- **CM.L2-3.4.8 Azure Policies**

Customer Responsibility

- Establishing a policy governing the installation of software on customer-deployed resources by users.

Additional Resources

- Discover what Software is installed on your VMs
- Using Software Restriction Policies to Protect Against Unauthorized Software
- How to manage the local administrators group on Azure AD joined devices
- Manage Change Tracking and Inventory in Azure Automation
- Enable Change Tracking and Inventory from an Automation account
- Enable Change Tracking and Inventory by browsing the Azure portal

- Enable Change Tracking and Inventory from a runbook
- Enable Change Tracking and Inventory from an Azure VM
- Microsoft Defender for Cloud

Identification and Authentication (IA)

IA.L2-3.5.1

Control Summary Information	
NIST 800-53 Mapping: IA-2, IA-3, IA-5	
Control : Identify information system users, processes acting on behalf of users or devices.	
Primary Services	**Secondary Services**
Azure Active Directory Intune/Microsoft Endpoint Manager	Network Security Groups Privileged Identity Management (PIM) Microsoft Graph

Implementation Statement:

Azure Active Directory

Microsoft Azure Active Directory (AAD) offers a robust security set for verifying the identities of users, processes or devices before allowing access to organizational information systems by configuring identification and authentication controls. Use Azure Active Directory (AAD) to manage and secure identities by requiring single sign-on and Azure Multi-Factor Authentication to protect your users. The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access Policies.

Use role-based access control (RBAC) enforced by Active Directory (AD) and Privileged Identity Management – Just in time (JIT) to control access to change functions. AD defines the access that is available, and JIT provides time-limited permission elevation when users need to use that access. AD and JIT are automated, and actions taken, including account creation, change, disabling, removal for AD and account elevation for JIT, are automatically audited.

AD cannot authenticate users who try to access integrated applications externally. In the modern workplace, users often need to access applications that are not owned or managed by their organization's AD. Active Directory Federation Service (ADFS) is able to resolve and simplify these third-party authentication challenges.

ADFS allows users from one organization to access applications of partner organizations using the standard credentials of their organization's Active Directory (AD). ADFS also

lets users access AD-integrated applications while working remotely using their standard organizational AD credentials via a web interface. When establishing a partnership to use another organization's web applications, ADFS provides a central place to manage and audit the employee identity information that is shared with their organization's partners.

To learn more, see Deploying Active Directory Federation Services in Azure.

Additionally, Azure AD offers a feature called Azure AD B2B (business-to-business) collaboration that allows you to add users who do not belong to your company. So, you can invite other users from outside of your company to be members of your Azure AD. Those users can then be given access to your resources. Users who are not part of your company are called *guest users*.

To learn more, see What is guest user access in Azure Active Directory B2B?

Microsoft Graph

A user in Microsoft Graph is one among the millions who use Microsoft 365 cloud services. It is the focal point whose identity is protected, and access is well managed. The user's data is what drives businesses. Microsoft Graph services makes this data available to businesses in rich contexts, real-time updates, and deep insights, and, always only with the appropriate permissions. A Microsoft 365 group is the fundamental entity that lets users collaborate. It integrates with other services, enabling richer scenarios in task planning, teamwork, education, and more.

Azure Policies

- **IA.L2-3.5.1 Azure Policies**

Customer Responsibility

- Uniquely identifying and authenticating organizational users
  Federal user entities are responsible for properly identifying and authenticating federal users via ADFS

Additional Resources

- Extend on-premises AD FS to Azure

- Active Directory Federation Services

IA.L2-3.5.2

Control Summary Information	
NIST 800-53 Mapping: IA-2, IA-3, IA-5	
Control : Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.	
Primary Services	**Secondary Services**
Azure Active Directory Azure AD Multi-Factor Authentication Conditional Access Intune/Microsoft Endpoint Manager	Customer Lockbox Privileged Identity Management (PIM)

Implementation Statement:

Azure Conditional Access

Administrators of Azure AD can decide if a user has access to a particular resource by requiring that the user be authenticated with a username and password and has the authorization to access that resource.

Azure Conditional Access allows you to create policies that are applied against users. These policies use *assignments* and *access controls* to configure access to your resources. Assignments define who a policy applies to. It can apply to users, groups of users, roles in your Azure AD, or to guest users. You can also specify that a policy only applies to specific applications, such as Microsoft 365.

Assignments can also define conditions that must be met (such as requiring a certain platform such as iOS, Android, Windows, and so on), specific locations by IP address, and more. Access controls determine how a Conditional Access policy is enforced. The most restrictive access control is block access, but you can also use access controls to require that a user use a device that meets certain conditions, that they are using an approved application to access your resources, that they are using MFA, and so on.

To create a Conditional Access policy, search for Azure AD Conditional Access in the Azure portal. You can also use the Microsoft 365 Admin Center, the Azure AD Admin Center, or Azure PowerShell to manage Azure AD User accounts. The Azure AD Admin Center gives you a greater set of options for managing the properties of user accounts than the Microsoft 365 Admin Center.

To learn more, see:

- What is Conditional Access?
- Building a Conditional Access policy

Azure AD Multi-Factor Authentication

By default, users can log in to your Azure AD using only a username and password. Even if you require your users to use strong passwords, allowing access to your resources with only a username and password is risky.

Multifactor authentication solves this problem. The concept behind multifactor authentication is that you must authenticate using a combination of:

- Something you know, such as a username and password
- Something you have, such as a phone or mobile device
- Something you are, such as facial recognition or a fingerprint

Even though Azure multifactor authentication is two-factor, if you are using a mobile device that includes biometric features, you might be authenticating using three-factor authentication. However, the third factor is enforced by your mobile device and not by Azure. Azure multifactor authentication does not require three-factor authentication.

To learn more, see:

- How it works: Azure AD Multi-Factor Authentication
- Plan an Azure Active Directory Multi-Factor Authentication deployment

Azure Role Role-based access control (RBAC)

Azure implements RBAC across all Azure resources, so you can control how users and applications can interact with your Azure resources. You might want to allow users who administer your databases to have access to databases in a particular resource group, but you do not want to allow those people to create new databases or delete existing databases. You might also want some web developers to be able to deploy new code to your web applications, but you do not want them to be able to scale the app to a

higher-priced plan. These are just two examples of what you can do with RBAC in Azure to manage access and authorization.

To learn more, see:

- What is Azure role-based access control (Azure RBAC)?
- Azure built-in roles
- Azure custom roles

Additional Information

The scope of RBAC is defined by where the RBAC role is assigned. For example, if you open a resource group in the portal and assign an RBAC role to a user, the scope is at the resource group level. On the other hand, if you open a web app within that resource group and assign the role, the scope is to that web app only.

RBAC roles can be scoped to the management group, subscription, resource group, or resource level.

Azure AD Connect sign-on options

Azure AD Connect supports a variety of sign in options. You configure which one you want to use when setting up Azure AD Connect. The default method, Password Synchronization, is appropriate for most organizations who will use Azure AD Connect to synchronize identities to the cloud.

To learn more, see: What is Azure AD Connect?

Active Directory Federation

This allows users to authenticate to Azure AD resources using on-premises credentials. It also requires the deployment of an Active Directory Federation Services infrastructure. This is the most complicated identity synchronization configuration for Microsoft 365 and is only likely to be implemented in environments with complicated identity configurations.

To learn more, see: AD FS Overview.

Intune/Microsoft Endpoint Manager & Conditional Access

Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions.

Customer Lockbox access approver for Microsoft Azure

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. Members of the Customer Lockbox access approver role manage customer lockbox requests for the tenancy. Users that hold this role can approve or deny requests using the Microsoft 365 Admin center. Users that hold this role are also able to enable and disable the Customer Lockbox feature. Only users that hold the Global Administrator role are able to reset the password of users that hold the Customer Lockbox access approver role.

To learn more, see Customer Lockbox for Microsoft Azure.

Azure Policies

- **IA.L2-3.5.2 Azure Policies**

Customer Responsibility

- Implementing device identification and authentication prior to establishing a connection.
- Federal user entities, as well as other customers using identity federation, are responsible for federal/customer user authenticator management and content.

Additional Resources

- Details of the CMMC L2 Regulatory Compliance built-in initiative

IA.L2-3.5.3

Control Summary Information	
NIST 800-53 Mapping: IA-2(1), IA-2(2), IA-2(3)	
Control : Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
Primary Services	**Secondary Services**
Azure AD Multi-Factor Authentication	Azure Active Directory Microsoft Azure Portal Azure Bastion Conditional Access VPN Gateway Intune/Microsoft Endpoint Manager Privileged Identity Management (PIM) GitHub Enterprise Cloud GitHub AE

Implementation Statement:

Configure Conditional Access policies to require MFA for all users using the Azure portal. Configure device management policies using Intune/Microsoft Endpoint Manager to enforce Azure AD Multi-Factor Authentication (MFA) for devices. Creating a compliance policy will define the rules and settings that a user's device must meet to be compliant. Combine this with Conditional Access to enable the ability to block users and devices that do not meet the rules.

Azure Policies

- **IA.L2-3.5.3 Azure Policies**

Customer Responsibility

- Implementing multifactor authentication for network access to privileged accounts.
- Implementing multifactor authentication for network access to non-privileged accounts.

Additional Resources

- How to enable multifactor authentication in Azure
- Multi-factor authentication and Privileged Identity Management
- GitHub – Requiring two-factor authentication in your organization
- Enable Azure AD Multi-Factor Authentication (MFA) for VPN users

IA.L2-3.5.4

Control Summary Information	
NIST 800-53 Mapping: IA-2(8),IA-2(9)	
Control : Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
Primary Services	**Secondary Services**
Azure AD Multi-Factor Authentication Intune/Microsoft Endpoint Manager Windows Hello for Business Microsoft Azure Portal Azure Active Directory	Conditional Access Privileged Identity Management (PIM)

Implementation Statement:

All Azure AD authentication methods at Authentication Assurance Level 2 & 3 use either nonce or challenges and are resistant to replay attacks. Configure Conditional Access policies to require MFA for all users using the Azure portal. Configure device management policies using Intune/Microsoft Endpoint Manager to enforce Azure AD Multi-Factor Authentication for devices. Creating a compliance policy will define the rules and settings that a user's device must meet to be compliant. Combine this with Conditional Access to enable the ability to block users and devices that meet the rules.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. Windows Hello for Business, which is configured by

Group Policy or mobile device management (MDM) policy, always uses key-based or certificate-based authentication.

Customer Responsibility

- Implementing replay-resistant authentication mechanisms for network access to privileged accounts.
- Implementing replay-resistant authentication mechanisms for network access to non-privileged accounts.

Additional Resources

- Details of the CMMC L2 Regulatory Compliance built-in initiative

IA.L2-3.5.5

Control Summary Information	
NIST 800-53 Mapping: IA-4	
Control : Prevent the reuse of identifiers for a defined period.	
Primary Services	**Secondary Services**
Azure Active Directory Entitlement Management	Intune/Microsoft Endpoint Manager M365 Compliance Center Conditional Access

Implementation Statement:

Azure Active Directory

Assign and manage individual account identifiers and status in Azure Active Directory (AAD) in accordance with existing organizational policies. Take appropriate action on those user accounts by removing their privileged access rights or by deleting the account.

Govern access for external users in Azure AD entitlement management You can manage the lifecycle of external users by blocking their access after a defined period. Ensure that organizational policy maintains all accounts that remain in the disabled state for a defined period, after which they can be removed.

Customer Responsibility

- Preventing identifier reuse for the customer-defined time period.

IA.L2-3.5.6

Control Summary Information	
NIST 800-53 Mapping: IA-4	
Control : Disable identifiers after a defined period of inactivity.	
Primary Services	**Secondary Services**
Azure Active Directory Microsoft Defender for Identity Entitlement Management	Microsoft Defender for Cloud Apps Intune/Microsoft Endpoint Manager Conditional Access

Implementation Statement:

Microsoft Defender for Identity

Use activity filters and create action policies with Microsoft Defender for Identity in Microsoft Defender for Cloud Apps. Assess dormant sensitive entities as part of your organizations security policy. Organizations that fail to secure their dormant user accounts leave the door unlocked to their sensitive data safe.

Azure Active Directory (AAD)

Assign and manage individual account identifiers and status in Azure Active Directory (AAD) in accordance with existing organizational policies. Take appropriate action on those user accounts by removing their privileged access rights or by deleting the account.

Govern access for external users in Azure AD entitlement management You can manage the lifecycle of external users by blocking their access after a defined period. Ensure that organizational policy maintains all accounts that remain in the disabled state for a defined period, after which they can be removed.

Customer Responsibility

- Disabling identifiers after a customer-defined time period of inactivity.

Additional Resources

- Create an access review of groups and applications in Azure AD access reviews
- Detect inactive user accounts
  How to manage inactive user accounts in Azure AD
  How to manage stale devices in Azure AD
- View Sign-in Logs
- Regularly check for and remove inactive user accounts on Active Directory
- Details of the CMMC L2 Regulatory Compliance built-in initiative

IA.L2-3.5.7

Control Summary Information	
NIST 800-53 Mapping: IA-5(1)	
Control : Enforce a minimum password complexity and change of characters when new passwords are created.	
Primary Services	**Secondary Services**
Azure Active Directory	Intune/Microsoft Endpoint Manager Azure AD Password Protection Conditional Access

Implementation Statement:

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password complexity means using different types of characters as well as a specified number of characters. This applies to both the creation of new passwords and the modification of existing passwords. Characters to manage complexity include numbers, lowercase and uppercase letters, and symbols. To accomplish this, you need a good password policy.

Azure Active Directory (AAD)

A good password policy is the first step on securing your environment and company data. Without a password policy, passwords may be created that increase the probability that passwords can be easily guessed, or brute forced.

To learn more, see:

- Create a customer password policy.
- Password policies and account restrictions in Azure Active Directory

Azure Active Directory Password Protection

Azure Active Directory (AAD) has a password protection feature that blocks commonly attacked passwords and variations and also enables a custom banned list of passwords that automatically have common character substitutions. This way you can block passwords that are primarily focused on organizational-specific terms like brand names and product names.

The password protection feature integrates with Active Directory through agent password filters deployed to the domain controllers and which enforce or audit the use of banned passwords that have been configured in the Azure AD tenant via a deployed proxy service for hybrid scenarios.

Microsoft has a list of global banned passwords that is kept up to date by analyzing Azure AD security telemetry data. They look for commonly used passwords that are weak and/or compromised. *It is important to note that Microsoft does not use third-party/public password lists – all data is coming from Azure AD itself.*

To learn more, see:

- Globally banned password list
- Custom banned password list

Intune/Microsoft Endpoint Manager

Using Intune/Microsoft Endpoint Manager you can use policies to enforce password requirements for devices. Creating a compliance policy will define the rules and settings that a user's device must meet to be compliant. Combine this with Conditional Access to enable the ability to block users and devices that do not meet the rules.

Azure Policies

- **IA.L2-3.5.7 Azure Policies**

Customer Responsibility

- Enforcing password complexity requirements (i.e., case sensitivity; number of characters; and the mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type).

Additional resources

- Risk detections in Azure AD Identity Protection such as leaked credentials on the dark web.
- Azure Active Directory smart lockout

IA.L2-3.5.8

Control Summary Information	
NIST 800-53 Mapping: IA-5(1)	
Control : Prohibit password reuse for a specified number of generations.	
Primary Services	**Secondary Services**
Azure Active Directory	Intune/Microsoft Endpoint Manager Azure AD Password Protection Conditional Access

Implementation Statement:

Individuals may not reuse their passwords for a defined period of time and a set number of passwords generated, you can enforce this with password history in on-premises Active Directory (AD). In Azure AD, the last password cannot be used again when the user changes a password. The password policy is applied to all user accounts that are created and managed directly in Azure AD. This password policy cannot be modified.

Azure Active Directory (AAD)

Use Azure Active Directory (AAD) to configure a custom password policy and Azure Active Directory Password Protection. To meet this requirement, use a combination of security settings; the policy should enforce password history and have a minimum password age. For example, if you configure the Enforce password history policy setting to ensure that users cannot reuse any of their last 12 passwords, but you do not configure the Minimum password age policy setting to a number that is greater than 0, users could change their password 13 times in a few minutes and reuse their original password.

To learn more, see:

- Create a customer password policy
- Password policies and account restrictions in Azure Active Directory

Intune/Microsoft Endpoint Manager

Using Intune/Microsoft Endpoint Manager you can use policies to enforce password requirements for devices. Creating a compliance policy will define the rules and settings

that a user's device must meet to be compliant. Combine this with Conditional Access to enable the ability to block users and devices that do not meet the rules.

Azure Policies

- **IA.L2-3.5.8 Azure Policies**

Customer Responsibility

- Employing password-based authentication to customer-deployed resources and defining the number of password generations that are prohibited from reuse (e.g., 10 most recent passwords may not be reused when creating a new password).

Additional Resources

- Details of the CMMC L2 Regulatory Compliance built-in initiative

IA.L2-3.5.9

Control Summary Information	
NIST 800-53 Mapping: IA-5(1)	
Control : Allow temporary password use for system logons with an immediate change to a permanent password.	
Primary Services	**Secondary Services**
Azure Active Directory	

Implementation Statement:

Azure Active Directory

When creating a new user or resetting their password using Azure Active Directory (AAD), a temporary password is auto generated for the user. The temporary password never expires. The user will be required to change the password during the next sign-in process.

The time a user must wait to change the password is determined by password policy settings, specifically the minimum password age. The Minimum password age policy setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow password changes immediately by setting the number of days to 0.

Windows security baselines recommend setting Minimum password age to one day. Note: If you set a password for a user and you want that user to change the administrator-defined password, you must select the user must change password at next logon check box. Otherwise, the user will not be able to change the password until the number of days specified by Minimum password age.

Passwordless authentication methods, such as FIDO2 and Passwordless Phone Sign-in through the Microsoft Authenticator app, enable users to sign in securely without a password. Users can bootstrap Passwordless methods in one of two ways:

- Using existing Azure AD Multi-Factor Authentication methods
- Using a Temporary Access Pass (TAP)

A Temporary Access Pass is a time-limited passcode issued by an admin that satisfies strong authentication requirements and can be used to onboard other authentication methods, including Passwordless ones. The most common use for a Temporary Access Pass is for a user to register authentication details during the first sign-in, without the need to complete additional security prompts. Authentication methods are registered at https://aka.ms/mysecurityinfo. Users can also update existing authentication methods here.

Customer Responsibility

- Employing password-based authentication to customer-deployed resources, including the ability to issue users a temporary password with the requirement to immediately change to a permanent password upon login.

Additional Resources

- Reset a user's password using Azure Active Directory to auto-generate a temporary password
- Security Considerations

IA.L2-3.5.10

Control Summary Information	
NIST 800-53 Mapping: IA-5(1)	
Control : Store and transmit only cryptographically protected passwords.	
Primary Services	**Secondary Services**
Microsoft Azure Portal Azure Key Vault Azure Virtual Machines Intune/Microsoft Endpoint Manager	Azure Active Directory Conditional Access Microsoft Defender for Endpoint Microsoft Defender for Cloud Apps

Implementation Statement:

Azure Active Directory and Azure Key Vault

Azure Key Vault security access models use Azure Active Directory (AAD) for authentication. Authentication with Key Vault works in conjunction with Azure Active Directory (Azure AD), which is responsible for authenticating the identity of any given security principal.

Store and transmit cryptographically protected passwords using Key Vault. Using the Azure portal, you can create your Key Vault. You can securely store and access secrets, such as API keys, passwords, certificates, or cryptographic keys. This is useful for websites, apps, and background processes where the application should not have access to credentials.

Azure Policies

- **IA.L2-3.5.10 Azure Policies**

Customer Responsibility

- Employing password-based authentication, which stores and transmits cryptographically protected passwords, for customer-deployed resources.

Additional Resources

- Set and retrieve a secret from Key Vault using Azure Portal
- Create and encrypt a Windows virtual machine with the Azure Portal
- Secure VM password with Key Vault
- Intune Data Warehouse application-only authentication
- Security baseline for Azure Key Vault

IA.L2-3.5.11

Control Summary Information	
NIST 800-53 Mapping: IA-6	
Control : Obscure feedback of authentication information.	
Primary Services	**Secondary Services**
Azure Active Directory	Azure Bastion Azure Virtual Machines Microsoft Azure Portal Intune/Microsoft Endpoint Manager

Implementation Statement:

By default, Azure Active Directory (AAD) obscures all passwords. Microsoft's Password boxes conceal the characters typed into it for purposes of privacy. By default, the password box provides a way for the user to view their password by holding down a reveal button.

You can disable this feature for Windows 10 using policy as an added security measure to ensure your password can not be displayed on the login screen.

Customer Responsibility

- Obscuring authentication feedback information during the authentication process for any customer-deployed resources.

Incident Response (IR)

IR.L2-3.6.1

Control Summary Information	
NIST 800-53 Mapping: IR-2, IR-4, IR-5, IR-6, IR-7	
Control : Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.	
Primary Services	**Secondary Services**
Microsoft Defender for Cloud Apps Microsoft Sentinel	Microsoft Defender for Endpoint Microsoft Defender for Office 365 Microsoft Defender for IoT Microsoft 365 Defender Insider Risk Management Azure Active Directory Microsoft Graph

Implementation Statement:

Insider risk management

Insider risk management uses the full breadth of service and 3rd-party indicators to help you quickly identify, triage, and act on risk activity. By using logs from Microsoft 365 and Microsoft Graph, insider risk management allows you to define specific policies to identify risk indicators. These policies allow you to identify risky activities and to act to mitigate these risks.

Moreover, insider risk analytics enables you to conduct an evaluation of potential insider risks in your organization without configuring any insider risk policies. This evaluation can help your organization identify potential areas of higher user risk and help determine the type and scope of insider risk management policies you may consider configuring.

You can stream each of these logs directly into a SIEM solution, such as Microsoft Sentinel. Alternatively, use Azure Event Hubs to integrate logs with third-party SIEM

solutions. Automate dynamic reconfiguration based on events within the SIEM by using Microsoft Graph or Azure AD PowerShell.

Microsoft Defender for Cloud Apps and Sentinel

Incident Response covers controls in the incident response life cycle - preparation, detection and analysis, containment, and post-incident activities. Azure services such as Microsoft Defender for Cloud Apps and Sentinel can support this control to automate the incident response process.

Ensure your organization has processes to respond to security incidents, has updated these processes for Azure, and is regularly exercising them to ensure readiness. For more information see, Implement security across the enterprise environment and Incident response reference guide

Set up security incident contact information in Microsoft Defender for Cloud Apps. This contact information is used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your data has been accessed by an unlawful or unauthorized party. You also have options to customize incident alert and notification in different Azure services based on your incident response needs.

Microsoft Defender for Cloud Apps provides high quality alerts across many Azure assets. You can use the ASC data connector to stream the alerts to Microsoft Sentinel. Microsoft Sentinel lets you create advanced alert rules to generate incidents automatically for an investigation.

Export your Microsoft Defender for Cloud Apps alerts and recommendations using the export feature to help identify risks to Azure resources. Export alerts and recommendations either manually or in an ongoing, continuous fashion. To learn more see, How to configure export and How to stream alerts into Microsoft Sentinel.

Connect your data sources such as Microsoft Defender for IoT, M365 Compliance Center, Azure Firewall and Microsoft Defender for Endpoint to Microsoft Sentinel for a centralized source of detection and reporting. Microsoft Sentinel provides out-of-the-box, built-in templates to help you create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that

looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can assign and investigate in your environment. To learn how to automate your responses to threats, Set up automated threat responses in Microsoft Sentinel.

Microsoft Sentinel provides extensive data analytics across virtually any log source and a case management portal to manage the full lifecycle of incidents. Intelligence information during an investigation can be associated with an incident for tracking and reporting purposes. Learn how to Investigate incidents with Microsoft Sentinel.

Additionally, mark resources using tags and create a naming system to identify and categorize Azure resources, especially those processing sensitive data. It is your responsibility to prioritize the remediation of alerts based on the criticality of the Azure resources and environment where the incident occurred.

Use workflow automation features in Microsoft Defender for Cloud Apps and Microsoft Sentinel to automatically trigger actions or run a playbook to respond to incoming security alerts. The playbook takes actions, such as sending notifications, disabling accounts, and isolating problematic networks. To learn more see, Set up automated threat responses in Microsoft Defender for Cloud Apps and Set up automated threat responses in Microsoft Sentinel.

Microsoft Defender for Endpoint and Microsoft 365 Defender

Investigate incidents that affect your network, understand what they mean, and collate evidence to resolve them. If enabled, Microsoft 365 Defender can automatically investigate and resolve alerts through automation and artificial intelligence. You can also perform additional remediation steps to resolve the attack including isolating the device from the network to allow for contained investigations. Additionally, Microsoft Defender for Endpoint automatically investigates all the incidents' supported events and suspicious entities in the alerts, providing you with auto response and information about the important files, processes, services, and more. Connect your data resources to Microsoft Sentinel for a centralized incident handling capability.

Customer Responsibility

- Implementing key incident handling capabilities including preparation, detection and analysis, containment, eradication, and recovery.
- Providing incident response support resources that are integral to the organizational incident response capability, providing advice and assistance to users handling security incidents.

Additional Resources

- Computer Security Incident Handling Guide
- Incident preparation
- Getting started with Microsoft Sentinel
- Incident response playbooks
- Respond to your first incident walkthrough

IR.L2-3.6.2

Control Summary Information	
NIST 800-53 Mapping: IR-2, IR-4, IR-5, IR-6, IR-7	
Control : Track, document and report incidents to designated officials and/or authorities both internal and external to the organization.	
Primary Services	**Secondary Services**
Microsoft Sentinel Dynamics 365 Azure Active Directory	Microsoft Defender for Cloud Apps Microsoft 365 security center Intune/Microsoft Endpoint Manager Microsoft 365 Defender

Implementation Statement:

Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies. Microsoft Sentinel supports the tracking, documenting and reporting of incidents. Connect your sources to Microsoft Sentinel for one centralized location to manage incidents in your organization.

Connect your data sources such as Microsoft Defender for IoT, Microsoft 365 security center, Azure Firewall and Microsoft Defender for Endpoint to Microsoft Sentinel for a centralized source of detection and reporting. Microsoft Sentinel provides out-of-the-box, built-in templates to help you create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can assign and investigate in your environment. To learn how to automate your responses to threats, Set up automated threat responses in Microsoft Sentinel.

Incident reporting is a formal part of the incident closure process. In Microsoft Sentinel you can use workbooks, Workbooks provide a dashboard to summarize security data visually. Microsoft Sentinel includes numerous default dashboards and customizable templates to facilitate incident analysis. For more information, see Quickstart: Get started with Microsoft Sentinel. Learn more about dashboards and graphs in Microsoft Sentinel.

Microsoft Sentinel provides extensive data analytics across virtually any log source and a case management portal to manage the full lifecycle of incidents. Intelligence information during an investigation can be associated with an incident for tracking and reporting purposes. Learn how to Investigate incidents with Microsoft Sentinel.

Additionally, mark resources using tags and create a naming system to identify and categorize Azure resources, especially those processing sensitive data. It is your responsibility to prioritize the remediation of alerts based on the criticality of the Azure resources and environment where the incident occurred.

Use workflow automation features in Microsoft Defender for Cloud Apps and Microsoft Sentinel to automatically trigger actions or run a playbook to respond to incoming security alerts. The playbook takes actions, such as sending notifications, disabling accounts, and isolating problematic networks. To learn more see, Set up automated threat responses in Microsoft Defender for Cloud Apps and Set up automated threat responses in Microsoft Sentinel

Microsoft Security Response Center

Set up security incident contact information in Microsoft Defender for Cloud Apps. This contact information is used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your data has been accessed by an unlawful or unauthorized party. You also have options to customize incident alert and notification in different Azure services based on your incident response needs. Additionally, if you are a security researcher and believe you have found a Microsoft security vulnerability, Microsoft would like to work with you to investigate it. Please note that the Microsoft Security Response Center does not provide technical support for Microsoft products. For more information, see Report an issue and submission guidelines.

Dynamics 365

Microsoft Dynamics 365 Customer Service can act as a help desk ticketing system to serve a company's employees or customers needing support. You can define custom alert rules that monitor filtered views of data and automatically send email notifications when predefined events occur.

Microsoft 365 Defender

You can manage incidents from Incidents & alerts > Incidents on the quick launch of the Microsoft 365 Defender portal. There you can create email notifications; in the navigation pane, select Settings > Microsoft 365 Defender > Incident email notifications. This will allow you to automatically report incident to designated parties.

Customer Responsibility

- providing incident response training to users of customer-deployed resources in accordance with assigned roles and responsibilities.
- implementing key incident handling capabilities including preparation, detection and analysis, containment, eradication, and recovery.
- for incident monitoring of customer-deployed resources.
- for requiring personnel to report suspected security incidents to the organizational incident response capability.

IR.L2-3.6.3

Control Summary Information	
NIST 800-53 Mapping: IR-3	
Control : Test the organizational incident response capability.	
Primary Services	**Secondary Services**
	Microsoft Sentinel Microsoft 365 Defender for Office 365 Microsoft 365 Defender for Endpoint

Implementation Statement:

Organizations are required to test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Microsoft 365 Defender has attack simulation capabilities that can be deployed to users. If your organization has Microsoft Defender for Office 365 Plan 2, which includes Threat

Investigation and Response capabilities, you can use Attack Simulator in the M365 Compliance Center to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

You can use Microsoft Sentinel to review incidents in your organization to create a walk-through or tabletop exercise simulating common threats among the organization. Dashboards and graphs are customizable for high level visibility of incidents and can be used to create incident response training presentations. Microsoft Sentinel provides extensive data analytics across virtually any log source and a case management portal to manage the full lifecycle of incidents. Intelligence information during an investigation can be associated with an incident for tracking and reporting purposes. Learn how to Investigate incidents with Microsoft Sentinel.

Customer Responsibility

- Testing the incident response capability of customer-deployed resources.

Additional Resources

- NIST's publication - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Maintenance (MA)

MA.L2-3.7.1

Control Summary Information	
NIST 800-53 Mapping: MA-2, MA-3, MA-3(1), MA-3(2)	
Control : Perform maintenance on organizational systems.	
Primary Services	**Secondary Services**
	Microsoft Azure Portal Azure Virtual Machines Intune/Microsoft Endpoint Manager Microsoft Defender for Endpoint Microsoft Endpoint Manager Configuration Manager Privileged Identity Management (PIM)

Implementation Statement:

Performing controlled maintenance ensures uptime through established processes such as change and configuration management. Maintenance windows are an important time to apply critical security updates and patches. Maintenance windows also incur risk as systems could crash without proper testing or authorized time windows. Azure Maintenance Control facilitates control of maintenance operations in the platform.

Manage platform updates, that do not require a reboot, using maintenance control. Azure frequently updates its infrastructure to improve reliability, performance, security or launch new features. Most updates are transparent to users. Some sensitive workloads, like gaming, media streaming, and financial transactions, can't tolerate even few seconds of a VM freezing or disconnecting for maintenance. Maintenance control gives you the option to wait on platform updates and apply them within a 35-day rolling window.

Maintenance control lets you decide when to apply updates to your isolated VMs. With maintenance control, you can:

- Batch updates into one update package.
- Wait up to 35 days to apply updates.

- Automate platform updates for your maintenance window using Azure Functions.
- Maintenance configurations work across subscriptions and resource groups.

To apply maintenance control to an Azure VM, the VM must be on a dedicated host or created with an isolated VM size. After 35 days, an update will be automatically applied. The controlling user must have resource contributor access. For more information, see Control updates with Maintenance Control and Azure PowerShell.

Configuration Manager

Configuration Manager sites and hierarchies require regular maintenance and monitoring to provide services effectively and continuously. Regular maintenance ensures that the hardware, software, and Configuration Manager database continue to function correctly and efficiently. Optimal performance greatly reduces the risk of failure. You can configure alerts and use the built-in status message system to understand the state of your Configuration Manager environment.

Privileged Identity Management (PIM)

PIM provides a time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions to important resources. These resources include resources in Azure Active Directory (Azure AD), Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. You assign users the role with the least privileges necessary to perform their tasks. This practice minimizes the number of Global Administrators and instead uses specific administrator roles for certain scenarios such as, performing maintenance tasks.

Customer Responsibility

- Responsible for scheduling, performing, documenting, and reviewing remote maintenance and repair records for all customer-deployed operating systems in accordance with organizational requirements.

Additional Resources

- Maintenance for virtual machines in Azure
- Handling planned maintenance notifications

MA.L2-3.7.2

Control Summary Information	
NIST 800-53 Mapping: MA-2, MA-3, MA-3(1), MA-3(2)	
Control : Provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC Privileged Identity Management (PIM)	Azure Bastion Intune/Microsoft Endpoint Manager Conditional Access Network Security Groups

Implementation Statement:

Network Security Groups

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. To simplify maintenance of your security rule definition, combine augmented security rules with service tags or application security groups. For security reasons it is good practice to lock down access to Azure resources and not leave management ports open to the internet. One way to restrict access to remote access protocols like RDS / SSH is to create a Network Security Groups (NSG) and apply this to either virtual machines or virtual network subnets.

Azure Active Directory

Controlling maintenance operations ensures confidentiality of data during maintenance operations. Maintenance windows incur risk not only to downtime, but also to unauthorized users obtaining rights to systems. One option for controlling maintenance operations is through Azure Active Directory Role Based Access and Azure AD Multi-Factor Authentication. It's a best practice to manage to least privilege. Least privilege means you grant your administrators exactly the permission they need to do their job. There are three aspects to consider when you assign a role to your administrators: a

specific set of permissions, over a specific scope, for a specific period of time. Avoid assigning broader roles at broader scopes even if it initially seems more convenient to do so. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised. Azure AD RBAC supports over 65 built-in roles. There are Azure AD roles to manage directory objects like users, groups, and applications, and also to manage Microsoft 365 services like Exchange, SharePoint, and Intune. To better understand Azure AD built-in roles, see Understand roles in Azure Active Directory. If there isn't a built-in role that meets your need, you can create your own custom roles.

Azure AD Multi-Factor Authentication

Multi Factor Authentication (MFA) is one of the strongest security controls in a cloud computing environment. MFA is an important conditional access requirement for maintenance personnel. People connect from organization-owned, personal, and public devices on and off the corporate network using smart phones, tablets, PCs, and laptops, often on multiple platforms. In this always-connected, multi-device and multi-platform world, the security of user accounts is more important than ever. Passwords, no matter their complexity, used across devices, networks, and platforms are no longer sufficient to ensure the security of the user account, especially when users tend to reuse passwords across accounts. Sophisticated phishing and other social engineering attacks can result in usernames and passwords being posted and sold across the dark web.

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Azure AD Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. A Conditional Access policy can require users to perform multi-factor authentication when certain criteria are met such as:

- All users, a specific user, member of a group, or assigned role
- Specific cloud application being accessed
- Device platform
- State of device
- Network location or geo-located IP address
- Client applications
- Sign-in risk (Requires Identity Protection)

- Compliant device
- Hybrid Azure AD joined device
- Approved client application

Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. For more information, see Planning a cloud-based Azure AD Multi-Factor Authentication deployment.

Additionally, performing controlled maintenance ensures uptime through established processes such as change and configuration management. Maintenance windows are an important time to apply critical security updates and patches. Maintenance windows also incur risk as systems could crash without proper testing or authorized time windows. Azure Maintenance Control facilitates control of maintenance operations in the platform.

Manage platform updates, that do not require a reboot, using maintenance control. Azure frequently updates its infrastructure to improve reliability, performance, security or launch new features. Most updates are transparent to users. Some sensitive workloads, like gaming, media streaming, and financial transactions, can't tolerate even few seconds of a VM freezing or disconnecting for maintenance. Maintenance control gives you the option to wait on platform updates and apply them within a 35-day rolling window.

Maintenance control lets you decide when to apply updates to your isolated VMs. With maintenance control, you can:

- Batch updates into one update package.
- Wait up to 35 days to apply updates.
- Automate platform updates for your maintenance window using Azure Functions.
- Maintenance configurations work across subscriptions and resource groups.

To apply maintenance control to an Azure VM, the VM must be on a dedicated host or created with an isolated VM size. After 35 days, an update will be automatically applied. The controlling user must have resource contributor access. For more information, see Control updates with Maintenance Control and Azure PowerShell

Azure Bastion

As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

Privileged Identity Management (PIM)

PIM provides a time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions to important resources. These resources include resources in Azure Active Directory (Azure AD), Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. You assign users the role with the least privileges necessary to perform their tasks. This practice minimizes the number of Global Administrators and instead uses specific administrator roles for certain scenarios such as, performing maintenance tasks.

Customer Responsibility

- Responsible for approving, controlling and monitoring system maintenance tools used on customer-deployed operating systems.

Additional Resources

- Add users and grant administrative permission to Intune
- Learn about Conditional Access and Intune

MA.L2-3.7.3

Control Summary Information	
NIST 800-53 Mapping: MA-2	
Control : Ensure equipment removed for off-site maintenance is sanitized of any CUI.	
Primary Services	**Secondary Services**
	Microsoft Information Protection

Implementation Statement:

To ensure equipment removed for off-site maintenance is sanitized of any CUI, you will need identify what data is considered CUI. Discovery and labeling sensitive data are the first steps to controlling data security. Labeling sensitive data is something organizations should implement across both physical and logical media. Government regulations such as NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) implicitly specify controls for protecting controlled unclassified information (CUI). This requirement spans across all industries and geographies. The European Union requires secure handing of personally identifiable information (PII) in the General Data Protection Regulation (GDPR) and California has recently implemented a similar regulation with the California Consumer Privacy Regulation (CCPA).

Microsoft Information Protection

Microsoft Information Protection (MIP) provides a capability to enable data discovery called scanner. Scanner searches for what sensitive information you have in files that are stored in an on-premises data store or within your cloud environment. For example, a local folder, network share, or SharePoint Server. For more information, see Quickstart: Find what sensitive information you have.

Customer Responsibility

- Removed CUI from equipment such as laptops removed for off-site maintenance.
- After running the MIP scanner, the customer must securely erase the CUI data.

MA.L2-3.7.4

Control Summary Information	
NIST 800-53 Mapping: MA-3(2)	
Control : Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	
Primary Services	**Secondary Services**
	Microsoft Defender for Endpoint

Implementation Statement:

As part of troubleshooting, a vendor may provide a diagnostic application to install on a system. As this is executable code, there is a chance that the file is corrupt or infected with malicious code. Implement procedures to scan any files prior to installation. The same level of scrutiny must be made as with any file a staff member may download. For example, you have recently been experiencing performance issues on one of your servers. After troubleshooting for much of the morning, the vendor has asked to install a utility that will collect more data from the server. The file is stored on the vendor's FTP server. The support technician gives you the FTP site so you can anonymously download the utility file. You also ask him for a hash of the utility file. As you download the file to your local computer, you realize it is compressed. You unzip the file and perform a manual antivirus scan, using Microsoft Defender for Endpoint which reports no issues. To verify the utility file has not been altered, you run an application to see that the hash from the vendor matches.

Customer Responsibility

- Responsible for checking media containing maintenance diagnostic and test programs for malicious code prior to deployment on customer-deployed operating systems.

Additional Resources

- Pre-scan files to be uploaded to non-compute Azure resources
- Understand Microsoft Antimalware for Azure Cloud Services and Virtual Machines
- Understand Microsoft Defender for Cloud Apps' Threat detection for data services
- Microsoft Defender for Endpoint documentation

MA.L2-3.7.5

Control Summary Information	
NIST 800-53 Mapping: MA-4	
Control : Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	
Primary Services	**Secondary Services**
Azure Active Directory Azure AD Multi-Factor Authentication Intune/Microsoft Endpoint Manager Conditional Access	Privileged Identity Management (PIM) Azure RBAC Microsoft Azure Portal

Implementation Statement:

Azure AD Multi-Factor Authentication /Privileged Identity Management (PIM)

Controlling maintenance operations ensures confidentiality of data during maintenance operations. Maintenance windows incur risk not only to downtime, but also to unauthorized users obtaining rights to systems. One option for controlling maintenance operations is through Azure Active Directory Role Based Access, Privileged Identity Management (PIM) and Azure AD Multi-Factor Authentication. It's a best practice to manage to least privilege. Least privilege means you grant your administrators exactly the permission they need to do their job. There are three aspects to consider when you assign a role to your administrators: a specific set of permissions, over a specific scope, for a specific period of time. Avoid assigning broader roles at broader scopes even if it initially seems more convenient to do so. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised. Azure AD RBAC supports over 65 built-in roles. There are Azure AD roles to manage directory objects like users, groups, and applications, and also to manage Microsoft 365 services like Exchange, SharePoint, and Intune. To better understand Azure AD built-in roles, see Understand roles in Azure Active Directory. If there isn't a built-in role that meets your need, you can create your own custom roles.

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions

on resources that you care about. Some features provide the ability to terminate sessions, such as Just-in-Time access. Here are some of the key features of Privileged Identity Management:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit

For more information, see Enable and request just-in-time access for Azure Managed Applications.

Multi Factor Authentication (MFA) is one of the strongest security controls in a cloud computing environment. MFA is an important conditional access requirement for maintenance personnel. People connect from organization-owned, personal, and public devices on and off the corporate network using smart phones, tablets, PCs, and laptops, often on multiple platforms. In this always-connected, multi-device and multi-platform world, the security of user accounts is more important than ever. Passwords, no matter their complexity, used across devices, networks, and platforms are no longer sufficient to ensure the security of the user account, especially when users tend to reuse passwords across accounts. Sophisticated phishing and other social engineering attacks can result in usernames and passwords being posted and sold across the dark web.

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Azure AD Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. A Conditional Access policy can require users to perform multi-factor authentication when certain criteria are met such as:

- All users, a specific user, member of a group, or assigned role
- Specific cloud application being accessed
- Device platform

- State of device
- Network location or geo-located IP address
- Client applications
- Sign-in risk (Requires Identity Protection)
- Compliant device
- Hybrid Azure AD joined device
- Approved client application

Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. For more information, see Planning a cloud-based Azure AD Multi-Factor Authentication deployment.

Intune/Microsoft Endpoint Manager

You can use Intune Microsoft Endpoint Manager to created conditional access policies that will restrict sessions to meeting specific requirements such as Azure AD Multi-Factor Authentication and network locations. Sessions that do not meet the conditional access policy requirements will not be granted. To learn more, see Learn about conditional access and Intune.

Azure Bastion

Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. Using Azure Bastion, you can securely and seamlessly connect to your virtual machines over SSL directly in the Azure portal. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to seamlessly connect to any VM in this virtual network. As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

Customer Responsibility

- Responsible for using strong authenticators when establishing non-local maintenance and diagnostic sessions on customer-deployed operating systems.
- Responsible for terminating session and network connections when non-local maintenance is completed on customer-deployed operating systems.

MA.L2-3.7.6

Control Summary Information	
NIST 800-53 Mapping: MA-5	
Control : Supervise the maintenance activities of personnel without required access authorization.	
Primary Services	**Secondary Services**
Azure Bastion Privileged Identity Management (PIM)	Customer Lockbox

Implementation Statement:

You can supervise maintenance personnel with Azure Active Directory Privileged Identity Management. This feature provides tight control over administrative rights including conditional access, eligibility windows, global admin approvals, admin time windows and logging. For more information, see Deploy Privileged Identity Management (PIM).

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in

response to a customer-initiated support ticket or a problem identified by Microsoft. To learn more, see Supported services and scenarios.

Additionally, Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP and SSH access to your virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in your Virtual Network (VNet) and supports all VMs in your Virtual Network (VNet) using SSL without any exposure through public IP addresses.

Once the Bastion service is provisioned and deployed in your virtual network, you can use it to seamlessly connect to any VM in this virtual network. As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

To learn more, see Azure Security baseline for Azure Bastion.

Customer Responsibility

- Managing maintenance personnel and designating organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Media Protection (MP)

MP.L2-3.8.1

Control Summary Information	
NIST 800-53 Mapping: MP-2, MP-4, MP-6	
Control : Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
Primary Services	**Secondary Services**
Azure Key Vault Microsoft Information Protection Intune/Microsoft Endpoint Manager	Azure Virtual Machines Conditional Access Azure RBAC Bitlocker

Implementation Statement:

Microsoft physically secures its datacenters and all the computing and storage media it is comprised of. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data.

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Utilizing Microsoft services, access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountabilities for all stored media.

Microsoft Information Protection

Sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered. Sensitivity labels in Microsoft 365 can help you take the right actions on the right content. With sensitivity labels, you can enforce protection settings based on that classification.

With MIP you can control and secure emails, documents, and sensitive data inside and outside your organization. Enhance data protection with API, from easy classification to embedded labels and permissions, no matter where it is stored or who it is shared with.

After you have installed and configured MIP clients, you might need to learn more about how the client interprets the different usage rights that can be used to protect documents and emails. For more information, see Configuring usage rights for Azure Information Management.

Intune/Microsoft Endpoint Manager

Intune helps protect devices and your corporate data with tools like security baselines, Azure AD conditional access, and partners for Mobile Threat Defense. Use Conditional Access with Microsoft Intune to control the devices and apps that can connect to your email and company resources. When integrated, you can gate access to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location. Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license. Through Azure Active Directory, Conditional Access brings signals together to make decisions, and enforce organizational policies. Intune enhances this capability by adding mobile device compliance and mobile app management data to the solution.

Additionally, you can use Intune to configure BitLocker Drive Encryption on devices that run Windows 10 or newer. To manage BitLocker in Intune, your account must have the applicable Intune role-based access control (RBAC) permissions. Intune provides a built-in encryption report that presents details about the encryption status of devices, across all your managed devices. After Intune encrypts a Windows 10 device with BitLocker, you can view and manage BitLocker recovery keys when you view the encryption report. You can also access important information for BitLocker from your devices, as found in

Azure Active Directory (Azure AD) encryption report that presents details about the encryption status of devices, across all your managed devices.

In addition to deploying BitLocker fixed drive encryption with Intune, you can configure removable drive encryption settings. You can find settings for BitLocker in Microsoft Endpoint Manager security profiles and configuration profiles. Removable drive settings apply to storage devices such as USB flash storage devices and external hard drives. For most situations, this is ideal from a security posture perspective to protect data on removable drives. However, when creating general profile settings, it is important to take into consideration the requirements of the organizations work environments. For Example, if the IT department routinely deploys operating systems using USB boot devices, those USB devices should not be encrypted. Consider requiring USB device encryption for specific departments that have access to CUI and other sensitive data. Additionally, you can block certain kinds of USB devices, or you can allow USB devices by device IDs.

For more information on how to create profiles, see:

- Create an endpoint security policy for BitLocker
- Restrict USB devices by using Intune Administrative Templates

Azure Key Vault

Protecting sensitive media and logical data in transit is another critical control to ensure confidentiality of data. Azure provides numerous levels of encryption for data in transit. Azure Key Vault provides a capability to securely store your application keys, certificates, and secrets. This capability reduces risk of key exposure while providing role-based access control (RBAC) for key usage and audit logging of key usage. Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This article provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.

MFA

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional

Access to make the solution fit their specific needs. Azure AD Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. For more information, see Planning a cloud-based Azure AD Multi-Factor Authentication deployment.

Customer Responsibility

- Physically control paper media containing CUI
- Physically control digital media such as, diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. containing CUI
- Securely store paper media and digital media containing CUI

Additional Resources

- Azure RBAC documentation
- Common ways to use Conditional Access with Intune
- Tutorial: Use a Windows VM system-assigned managed identity to access Azure Key Vault
- Check out or check in files in a document library
- Check out and edit files
- Manage inventory collection from VMs
- Inventory and visibility in Azure
- Change Tracking and Inventory overview

MP.L2-3.8.2

Control Summary Information
NIST 800-53 Mapping: MP-2, MP-4, MP-6
Control : Limit access to CUI on system media to authorized users.

Control Summary Information	
Primary Services	**Secondary Services**
Azure RBAC Microsoft Information Protection Conditional Access Intune/Microsoft Endpoint Manager	Network Security Groups Azure AD Multi-Factor Authentication Microsoft 365 Compliance Center Microsoft Defender for Endpoint Microsoft 365 Compliance Center

Implementation Statement:

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Microsoft (via Azure Government and/or Microsoft 365 GCC High) physically secures its datacenters and all the computing and storage media it is comprised of. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data.

Azure Active Directory

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope. This article describes how to assign roles using the Azure portal. If you need to assign administrator roles in Azure Active Directory, see Assign Azure AD roles to users.

Role-based access control (RBAC) helps you manage who has access to your organization's resources and what they can do with those resources. By assigning roles to your Intune users, you can limit what they can see and change. Each role has a set of permissions that determine what users with that role can access and change within your organization.

Intune/Microsoft Endpoint Manager and Conditional Access

Use Conditional Access with Microsoft Intune to control the devices and apps that can connect to your email and company resources. When integrated, you can gate access to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location.

Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license. Through Azure Active Directory, Conditional Access brings signals together to make decisions, and enforce organizational policies. Intune enhances this capability by adding mobile device compliance and mobile app management data to the solution.

Use device compliance policy to establish the conditions by which devices and users are allowed to access your network and company resources such as requiring a device to be marked as compliant, require multi-factor authentication, require approved client app and trusted network locations.

Microsoft Information Protection (MIP)

Configure Azure AD conditional access for Microsoft Information Protection. When a user opens a document that is protected by Microsoft Information Protection, administrators can block or grant access to users in their tenant, based on the standard conditional access controls. Requiring multi-factor authentication (MFA) is one of the most commonly requested conditions. Another one is that devices must be compliant with your Intune policies so that, for example, mobile devices meet your password requirements and a minimum operating system version, and computers must be domain-joined. For more information and some walk-through examples, see the following blog post: Conditional Access policies for Microsoft Information Protection.

Microsoft 365 Compliance Center

When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

- Only users within your organization can open a confidential document or email.

- Only users in the marketing department can edit and print the promotion announcement document or email, while all other users in your organization can only read it.

- Users cannot forward an email or copy information from it that contains news about an internal reorganization.

The encryption settings are available when you create a sensitivity label in the Microsoft 365 compliance center. You can also use the older portal, the Security & Compliance Center.

MFA

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Azure AD Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. For more information, see Planning a cloud-based Azure AD Multi-Factor Authentication deployment

Network Security Group

You can use an Azure Network Security Group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. For more information, see Azure platform considerations.

Customer Responsibility

- Identifying CUI to ensure the controls are applied to the applicable data.
- Limiting access to CUI on system media to authorized users only.

Additional Resources

- Common ways to use Conditional Access with Intune
- Virtual network integration for Azure services

- How network security groups work.
- Manage a network security group

MP.L2-3.8.3

Control Summary Information	
NIST 800-53 Mapping: MP-2, MP-4, MP-6	
Control : Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.	
Primary Services	**Secondary Services**
	Microsoft Information Protection Azure Key Vault

Implementation Statement:

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Microsoft

When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination. If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before decommissioning. The data on the drive is erased to ensure that the data cannot be recovered by any means. When such devices are decommissioned, Microsoft follows the NIST SP 800-88 R1 disposal process with data classification aligned to FIPS 199 Moderate. Magnetic, electronic, or optical media

are purged or destroyed in accordance with the requirements established in NIST SP 800-88 R1. Purge and Destroy operations must be performed using tools and processes approved by the Microsoft Cloud + AI Security Group. Records must be kept of the erasure and destruction of assets. Devices that fail to complete the Purge successfully must be degaussed (for magnetic media only) or Destroyed.

Azure Data Explorer

As a data platform, Azure Data Explorer supports the ability to delete individual records, through the use of Kusto *.purge* and related commands. You can also purge an entire table or purge records in a materialized view. Data deletion through the *.purge* command is designed to be used to protect personal data and should not be used in other scenarios. It is not designed to support frequent delete requests, or deletion of massive quantities of data, and may have a significant performance impact on the service. To learn more, see Purge process.

Microsoft Information Protection

Use Microsoft Information Protection (MIP) to help identify FCI and CUI for proper disposal by configuring new labels to protect sensitive data such as federal contracts information and controlled unclassified information (CUI). This policy is configurable to scope to a set of users who are more likely to interact with this data such as a business group. For more information, see Quickstart: Create a new Microsoft Information Protection label for specific users.

Additionally, MIP provides a capability to enable data discovery called scanner. Scanner searches for what sensitive information you have in files that are stored in an on-premises data store or within your cloud environment. For example, a local folder, network share, or SharePoint Server. For more information, see Quickstart: Find what sensitive information you have.

Azure Key Vault

When a secret is deleted from a key vault without soft-delete protection, the secret is permanently deleted. Users can currently opt out of soft-delete during key vault creation. However, Microsoft will soon enable soft-delete protection on all key vaults to protect secrets from accidental or malicious deletion by a user. Users will no longer be able to opt out of or turn off soft-delete. If your organization is subject to legal

compliance requirements and can't allow deleted key vaults and secrets to remain in a recoverable state for an extended period of time, you will have to adjust the retention period of soft-delete to meet your organization's standards. You can configure the retention period to last from 7 to 90 days.

Customer Responsibility

- Sanitizing and destroying customer-controlled information system media containing Federal Contract Information (FCI) before disposal or release for reuse.

Additional Resources

- Migrate from vault access policy to an Azure role-based access control permission model

MP.L2-3.8.4

Control Summary Information	
NIST 800-53 Mapping: MP-3	
Control : Mark media with necessary CUI markings and distribution limitations.	
Primary Services	**Secondary Services**
Microsoft Information Protection	

Implementation Statement:

For detailed information related to CUI Categories, Marking and Distribution limitations, see:

- DCSA Marking Job Aid
- DoD CUI Registry
- NARA CUI Registry
- NARA CUI Marking Handbook

The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. Labeling sensitive data is something organizations should implement across both physical and logical media. Government regulations such as NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) implicitly specify controls for protecting controlled unclassified information (CUI). This requirement spans across all industries and geographies. The European Union requires secure handing of personally identifiable information (PII) in the General Data Protection Regulation (GDPR) and California has recently implemented a similar regulation with the California Consumer Privacy Regulation (CCPA).

Microsoft Information Protection

Sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered. Sensitivity labels in Microsoft 365 can help you take the right actions on the right content. With sensitivity labels, you can enforce protection settings based on that classification. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. To learn more, see How to configure the policy settings for Microsoft Information Protection.

For example, you can implement pop-up messages in Outlook that warn, justify, or block emails being sent. This configuration uses policy advanced settings that you must configure by using M365 Compliance Center PowerShell. When you create and configure the following advanced client settings, users see pop-up messages in Outlook that can warn them before sending an email or ask them to provide justification why they are sending an email or prevent them from sending an email. Learn more, see Microsoft Information Protection (MIP) labeling, classification, and protection.

We can take this capability a step further by configuring new labels to protect sensitive data such as federal contracts information and controlled unclassified information (CUI). This policy is configurable to scope to a set of users who are more likely to interact with this data such as a business group. For more information, see Quickstart: Create a new Microsoft Information Protection label for specific users.

Additionally, MIP provides a capability to enable data discovery called scanner. Scanner searches for what sensitive information you have in files that are stored in an on-premises data store or within your cloud environment. For example, a local folder, network share, or SharePoint Server. For more information, see Quickstart: Find what sensitive information you have.

Customer Responsibility

- Marking CUI with applicable marking. (e.g., CUI/SP-XX/NOFORN in subject of email, etc. in addition to applying correct MIP label.)
- Limiting distribution to media containing CUI.

Additional Resources

- Azure RBAC documentation
- Conditional Access

MP.L2-3.8.5

Control Summary Information	
NIST 800-53 Mapping: MP-5	
Control : Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
Primary Services	**Secondary Services**
	Microsoft Information Protection Azure AD Multi-Factor Authentication Azure Key Vault Intune/Microsoft Endpoint Manager Azure RBAC Bitlocker

Implementation Statement:

Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

Microsoft physically secures its datacenters and all the computing and storage media it is comprised of. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data.

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in

response to a customer-initiated support ticket or a problem identified by Microsoft. You can now enable Customer Lockbox from the Administration module in the Customer Lockbox blade. To enable Customer Lockbox, the user account needs to have the Global Administrator role assigned.

Microsoft Defender for Endpoint

Microsoft recommends a layered approach to securing removable media, and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices. Discover plug and play connected events for peripherals in Microsoft Defender for Endpoint advanced hunting. To prevent malware infections or data loss, an organization may restrict USB drives and other peripherals. Allow or block removable devices based on granular configuration to deny write access to removable disks and approve or deny devices by using USB device IDs. Flexible policy assignment of device installation settings based on an individual or group of Azure Active Directory (Azure AD) users and devices. The controls can be set through the Intune Administrative Templates. Using Intune, you can apply device configuration policies to Azure AD user and/or device groups. The above policies can also be set through the Device Installation CSP settings and the Device Installation GPOs.

Azure RBAC, Microsoft Information Protection (MIP), Azure Rights Management (RMS)

Limiting access to sensitive data with least privilege reduces the risk of spillage or unauthorized access. Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope. Administrators can apply labels to classify data using Microsoft Information Protection. Microsoft Information Protection uses the Azure Rights Management service (Azure RMS) to protect your data. Azure RMS uses encryption, identity, and authorization policies. Similar to MIP labels, protection applied using Azure RMS stays with the documents and emails, regardless of the document or email's location, ensuring that you stay in control of your content even when it is shared with other people. After classifying data and applying labeling, Microsoft Information Protection allows you to configure which users or groups have access to that data. For more

information, see Quickstart: Create a new Microsoft Information Protection label for specific users. Additionally, The Azure portal provides you with several options to access user activity logs on the Azure Active Directory menu. You can directly get to the audit logs using this link.

Azure Key Vault

Azure Key Vault provides a capability to securely store your application keys, certificates and secrets. This capability reduces risk of key exposure while providing role-based access control (RBAC) for key usage and audit logging of key usage. Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This article provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.

Azure AD Multi-Factor Authentication

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Azure AD Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. For more information, see Planning a cloud-based Azure AD Multi-Factor Authentication deployment.

Intune/Microsoft Endpoint Manager

Microsoft's primary MDM tool is Microsoft Intune. Intune is part of a larger Microsoft MDM platform called Microsoft Endpoint Manager.

Using Intune, administrators can enroll, configure, and manage mobile devices on several different operating system platforms, wherever the devices happen to be. Administrators can even intervene when a threat to security occurs, by blocking a device's access to the company network and erasing any sensitive information stored on it.

Organizations can configure policies to allow, block and restrict USB drives and other peripherals. Organization can allow users to install only the USB drives and other peripherals included on a list of authorized devices or device types or prevent users from installing USB drives and other peripherals included on a list of unauthorized devices and device types.

Additionally, using Intune, you can apply device configuration policies to Azure AD user and/or device groups. The policies can also be set through the Device Installation CSP settings and the Device Installation GPOs. To protect your devices and corporate resources, you can use Azure Active Directory (AAD) Conditional Access policies with Intune.

Intune passes the results of your device compliance policies to Azure AD, which then uses conditional access policies to enforce which devices and apps can access your corporate resources.

When managing devices in your organization, you want to create groups of settings that apply to different device groups. You can complete this task using Administrative Templates in Intune. The templates are built into Intune and do not require customization.

Bitlocker

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

BitLocker To Go is BitLocker Drive Encryption on removable data drives. As with BitLocker, you can open drives that are encrypted by BitLocker To Go by using a password or smart card on another computer.

Customer Responsibility

- Controlling access to customer-controlled media containing CUI and maintain accountability for media during transport outside of controlled areas.

Additional Resources

- Azure security baseline for Customer Lockbox for Microsoft Azure
- Understand Customer Lockbox workflow
- How to enable auditing in Customer Lockbox
- How to view and retrieve Azure Activity Log events
- Managing BitLocker with Microsoft Endpoint Manager
- BitLocker overview

MP.L2-3.8.6

Control Summary Information	
NIST 800-53 Mapping: MP-5(4)	
Control : Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	
Primary Services	**Secondary Services**
Bitlocker Azure RBAC	Microsoft Defender for Endpoint Azure Key Vault Intune/Microsoft Endpoint Manager Microsoft Information Protection Conditional Access

Implementation Statement:

Whenever Azure Customer traffic moves between datacenters-- outside physical boundaries not controlled by Microsoft (or on behalf of Microsoft)-- a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (also known as MACsec) is applied from point-to-point across the underlying network hardware. The packets are encrypted and decrypted on the devices before being sent, preventing physical "man-in-the-middle" or snooping/wiretapping attacks. Because this technology

is integrated on the network hardware itself, it provides line rate encryption on the network hardware with no measurable link latency increase. This MACsec encryption is on by default for all Azure traffic traveling within a region or between regions, and no action is required on customers' part to enable.

Microsoft gives customers the ability to use Transport Layer Security (TLS) protocol to protect data when it is traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

Bitlocker

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

BitLocker To Go is BitLocker Drive Encryption on removable data drives. As with BitLocker, you can open drives that are encrypted by BitLocker To Go by using a password or smart card on another computer.

Azure Key Vault

Azure Key Vault provides two types of resources to store and manage cryptographic keys. Vaults support software-protected and HSM-protected (Hardware Security Module) keys. Managed HSMs only support HSM-protected keys. Vaults use FIPS 140-2

Level 2 validated HSMs to protect HSM-keys in shared HSM backend infrastructure. Managed HSM uses FIPS 140-2 Level 3 validated HSM modules to protect your keys. Each HSM pool is an isolated single-tenant instance with its own security domain providing complete cryptographic isolation from all other HSMs sharing the same hardware infrastructure.

Azure Key Vault provides a capability to securely store your application keys, certificates and secrets. This capability reduces risk of key exposure while providing role-based access control (RBAC) for key usage and audit logging of key usage. Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This article provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.

Intune/Microsoft Endpoint Manager

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any device, including personal devices in bring-your-own-device (BYOD) scenarios. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of Microsoft Intune protected apps available for public use.

Use Conditional Access with Microsoft Intune to control the devices and apps that can connect to your email and company resources. When integrated, you can gate access to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location.

Conditional Access is an Azure Active Directory capability that is included with an Azure Active Directory Premium license. Through Azure Active Directory, Conditional Access brings signals together to make decisions, and enforce organizational policies. Intune enhances this capability by adding mobile device compliance and mobile app management data to the solution.

Use device compliance policy to establish the conditions by which devices and users are allowed to access your network and company resources such as requiring a device to be marked as compliant, require multi-factor authentication, require encryption, require approved client app and trusted network locations.

Microsoft Information Protection

Microsoft Information Protection uses the Azure Rights Management service (Azure RMS) to protect your data. Azure RMS is integrated with other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory, and can also be used with your own or third-party applications and information protection solutions. Azure RMS works with both on-premises and cloud solutions.

Azure RMS uses encryption, identity, and authorization policies. Similar to MIP labels, protection applied using Azure RMS stays with the documents and emails, regardless of the document or email's location, ensuring that you stay in control of your content even when it is shared with other people. To learn more, see How does Azure RMS work?

Additional Resources

- Data protection framework using app protection policies
- Available Android app protection policy settings with Microsoft Intune
- Available iOS/iPadOS app protection policy settings with Microsoft Intune
- Azure encryption overview
- About Managed HSM
- About Key Vault
- Key types and protection methods

MP.L2-3.8.7

Control Summary Information	
NIST 800-53 Mapping: MP-7	
Control : Control the use of removable media on system components.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager Microsoft Defender for Endpoint	

Implementation Statement:

Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices.

Microsoft recommends a layered approach to securing removable media, and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices. Discover plug and play connected events for peripherals in Microsoft Defender for Endpoint advanced hunting. To prevent malware infections or data loss, an organization may restrict USB drives and other peripherals. Allow or block removable devices based on granular configuration to deny write access to removable disks and approve or deny devices by using USB device IDs. Flexible policy assignment of device installation settings based on an individual or group of Azure Active Directory (Azure AD) users and devices. The controls can be set through the Intune Administrative Templates. Using Intune, you can apply device configuration policies to Azure AD user and/or device

groups. The above policies can also be set through the Device Installation CSP settings and the Device Installation GPOs.

Customer Responsibility

- Controlling the use of removable media on customer-controlled systems.

MP.L2-3.8.8

Control Summary Information	
NIST 800-53 Mapping: MP-7(1)	
Control : Prohibit the use of portable storage devices when such devices have no identifiable owner.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager Microsoft Defender for Endpoint	Conditional Access

Implementation Statement:

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

Microsoft recommends a layered approach to securing removable media, and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices. Discover plug and play connected events for peripherals in Microsoft Defender for Endpoint advanced hunting. To prevent malware infections or data loss, an organization may restrict USB drives and other peripherals. Allow or block removable devices based on granular configuration to deny write access to removable disks and approve or deny devices by using USB device IDs. Flexible policy assignment of device installation settings based on an individual or group of Azure Active Directory (Azure AD) users and devices. The controls can be set through the Intune Administrative Templates. Using Intune, you can apply device configuration policies to Azure AD user and/or device

groups. The above policies can also be set through the Device Installation CSP settings and the Device Installation GPOs.

Customer Responsibility

- Prohibiting the use of portable storage devices that have no identifiable owner, on customer-controlled systems.

MP.L2-3.8.9

Control Summary Information	
NIST 800-171 Mapping: 3.8.9	
NIST 800-53 Mapping: CP-9	
Control : Protect the confidentiality of backup CUI at storage locations.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC	Azure Key Vault Azure Backup Azure Virtual Network Microsoft Information Protection Azure AD Multi-Factor Authentication

Implementation Statement:

There are several methods to protecting backups including access management, redundancy and encryption. Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Azure Backup provides three built-in roles to control backup management operations. For more information, see Use Role-Based Access Control to manage Azure Backup recovery points.

Secure your backups and protect against ransomware by enabling multifactor authentication using a security PIN generated in the Azure portal. If it is enabled, you are asked to authenticate from another device (for example, a mobile phone) while signing into the Azure portal. When you perform critical operations in Backup, you have to enter a security PIN, available on the Azure portal. Enabling Azure AD Multi-Factor Authentication adds a layer of security. Only authorized users with valid Azure credentials, and authenticated from a second device, can access the Azure portal.

Fully control how you protect and access your data with customer-managed keys that use 256-bit AES encryption. You can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to

protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.

Create private endpoints within your Azure Virtual Network to securely backup and restore data from your Recovery Services vaults. Azure Backup allows you to securely backup and restore your data from your Recovery Services vaults using private endpoints. Private endpoints use one or more private IP addresses from your VNet, effectively bringing the service into your VNet. Private endpoints for Backup can be only created for Recovery Services vaults that do not have any items protected to it (or have not had any items attempted to be protected or registered to it in the past). So, we suggest you create a new vault to start with. For more information about creating a new vault, see Create and configure a Recovery Services vault.
All your backed-up data is automatically encrypted when stored in the cloud using Azure Storage encryption, which helps you meet your security and compliance commitments. This data at rest is encrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 Validated. In addition to encryption at rest, all your backup data in transit is transferred over HTTPS. It always remains on the Azure backbone network.

For more information, see Azure Storage encryption for data at rest.

Microsoft Information Protection

You can secure confidential data and control information flows with Microsoft Information Protection. Microsoft Information Protection (MIP) is a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. For more information, see How to configure the policy settings for Microsoft Information Protection.

Customer Responsibility

- Responsible for conducting backups of user-level information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.

- Responsible for conducting backups of system-level information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.
- Responsible for conducting backups of system documentation information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.
- Responsible for protecting the confidentiality, integrity, and availability (CIA) of customer-controlled backup data. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the protection of backup data.

Additional Resources

- Azure Backup security capabilities for protecting cloud backups

Personnel Security (PS)

PS.L2-3.9.1

Control Summary Information	
NIST 800-53 Mapping: PS-3, PS-4, PS-5	
Control : Screen individuals prior to authorizing access to organizational systems containing CUI.	
Primary Services	**Secondary Services**

Implementation Statement:

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

You can ensure all employees who need access to CUI undergo organization-defined screening before being granted access based on the types of screening requirements for a given position and role. Clearly define positions and roles within your organization. Implement roles using Azure RBAC. For example, administrators with access to CUI and specific roles with permissions to view CUI should follow an organizationally defined screening process.

Customer Responsibility

- Screening individuals prior to authorizing access to customer-deployed resources.

PS.L2-3.9.2

Control Summary Information	
NIST 800-53 Mapping: PS-3, PS-4, PS-5	
Control : Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC	Microsoft Information Protection Conditional Access Microsoft Defender for Endpoint Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps

Implementation Statement:

Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Azure Active Directory

To protect organizational system containing CUI it is important to have controls in place that can identify users and remove access when needed. Azure Active Directory (AAD) is the cornerstone of identity in Azure. AAD enables hybrid identities through Azure AD Connect, an on-premises solution that is used to synchronize Active Directory identities with AAD, as well as to deploy Active Directory Federation Services (ADFS). ADFS lets you establish a federation between your premises and AAD (among others). When users log in, they are redirected to the ADFS login page (in your perimeter) and are prompted for their credentials, which are validated against your on-premises Active Directory. This makes your ADFS a single point of failure, because in such a setup, user passwords are not synced with AAD. Thus, credential validation can only be performed against your on-premises directory.

Azure Active Directory Pass-through Authentication is an alternative that consists of validating user credentials on-premises. It also validates credentials online, should your on-premises login page not be available. From a pure authentication perspective, it is a more robust approach than ADFS, but it requires user passwords to be synced with AAD, which is often still considered unwise by many organizations. You can also go full cloud and only use AAD.

Conditional Access allows you to set up access policies to prohibit a specific activity, as well as to trigger MFA according to rules that you define). It is a very powerful engine. You may target conditional access policies toward specific users or groups, or to specific apps.

RBAC helps in the creation and assignment of different permissions to different identities. This helps in segregating duties within teams, rather than everyone having all permissions. RBAC helps in making people responsible for their job because others might not even have the necessary access to perform it. It should be noted that providing permissions at a greater scope automatically ensures that child resources inherit those permissions. For example, providing an identity with read access for a resource group means that the identity will have read access to all the resources within that group, too.

Each role definition has certain allowed and disallowed actions. For example, the owner role has all actions permitted and none of the actions are prohibited. Additionally, customers can define a custom role. Custom roles are created by combining multiple permissions. For example, a custom role can consist of operations from multiple resources.

It is good practice to assign permissions using the principle of least privilege; this involves giving users the exact permissions they need to do their jobs properly. Users, groups, and applications are added to roles in Azure, and those roles have certain permissions. You can use the built-in roles that Azure offers, or you can create custom roles in RBAC.

For more information, see Grant a user access to Azure resources using RBAC.

Scenarios that could require an administrator to revoke all access for a user include compromised accounts, employee termination, and other insider threats. Depending on the complexity of the environment, administrators can take several steps to ensure access is revoked. Access tokens and refresh tokens are frequently used with thick client applications, and also used in browser-based applications such as single page apps.

When users authenticate to Azure AD, authorization policies are evaluated to determine if the user can be granted access to a specific resource. Access tokens can be a security concern if access must be revoked within a time that is shorter than the lifetime of the token, which is usually around an hour. For this reason, Microsoft is actively working to bring continuous access evaluation to Office 365 applications, which helps ensure invalidation of access tokens in near real time. To remove a user or group assignment to an application, follow the steps listed in the Remove a user or group assignment from an enterprise app in Azure Active Directory article. To disable all user sign-ins to an application, follow the steps listed in the Disable user sign-ins for an enterprise app in Azure Active Directory article.

Azure AD Identity Protection introduces automatic, risk-based, conditional access to help protect users against suspicious logins and compromised credentials. Azure AD Identity Protections also offers insight into, and a consolidated view of, threat detection based on machine-learning. Furthermore, the service delivers an important level of remediation recommendations, as well as performing compromise risk calculations about a user and their session.

For more information, see:

- What is Identity Protection?
  Identity Protection policies

Microsoft Intune

A cloud-based enterprise mobility management (EMM) service that enables administrators to enroll mobile devices, deploy apps, and enforce security policies As a Security Admin, use the *Endpoint security* node in Intune to configure device security and to manage security tasks for devices when those devices are at risk.

To protect your devices and corporate resources, you can use Azure Active Directory (Azure AD) Conditional Access policies with Intune.

Intune passes the results of your device compliance policies to Azure AD, which then uses conditional access policies to enforce which devices and apps can access your corporate resources. Conditional access policies also help to gate access for devices that aren't managed by Intune and can use compliance details from Mobile Threat Defense partners you integrate with Intune.

Customer Responsibility

- Appropriately terminating customer personnel within a customer-defined time period.
- Appropriately transferring personnel and reviewing current logical and physical access authorizations to customer-deployed resources/facilities when individuals are reassigned or transferred.

Additional Resources

- Manage user assignment for an app in Azure Active Directory

Physical Protection (PE)

PE.L2-3.10.6

Control Summary Information	
NIST 800-53 Mapping: PE-17	
Control : Enforce safeguarding measures for CUI at alternate work sites.	
Primary Services	**Secondary Services**
Azure AD Multi-Factor Authentication Intune/Microsoft Endpoint Manager Azure RBAC Azure VPN Azure Firewall Bitlocker Azure Data Center	Named Locations Microsoft Information Protection Conditional Access Microsoft 365 DLP

Implementation Statement:

Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. Many people work from home or travel as part of their job. Define and implement safeguards to account for protection of information beyond the enterprise perimeter. Safeguards may include physical protections, such as locked file drawers, as well as electronic protections such as encryption, audit logging, and proper access controls.

Intune/Microsoft Endpoint Manager

Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud-based mobile application management (MAM), and cloud-based PC management for your organization. Intune helps you ensure that your company's devices, apps, and data meet your company's security requirements. You have the control to set which requirements need to be checked and what happens when those requirements aren't met.
The Microsoft Endpoint Manager admin center is where you can find the Microsoft Intune service, as well as other device management related settings.

Microsoft Intune device compliance policies - Cloud-based device compliance leverages Microsoft Intune Compliance Policies, which can query the device state and define compliance rules for the following, among other things.

- Antivirus status
- Auto-update status and update compliance
- Password policy compliance
- Encryption compliance
- Device health attestation state (validated against attestation service after query)

Azure Active Directory

Azure Active Directory provides administrators the flexibility to apply granular user authentication per their requirements. As an administrator, choosing authentication methods for Azure AD Multi-Factor Authentication and self-service password reset (SSPR) it is recommended that you require users to register multiple authentication methods. When an authentication method is not available for a user, they can choose to authenticate with another method. Authentication methods include password, security questions, email address, Microsoft Authenticator app, OATH Hardware token, SMS, Voice call, and App passwords. For more information, see Authentication methods.

Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope. For more information, see Grant a user access to Azure resources using RBAC.

Privileged Identity Management

You can secure administrative rights with Azure Active Directory Privileged Identity Management. This feature provides tight control over administrative rights including conditional access, eligibility windows, global admin approvals, admin time windows and logging. For more information, see Deploy Privileged Identity Management (PIM).

Microsoft Information Protection

You can secure confidential data and control information flows with Microsoft Information Protection. Microsoft Information Protection (MIP) is a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. For more information, see How to configure the policy settings for Microsoft Information Protection.

Conditional Access

Microsoft Azure leverages adaptive access control through Azure Active Directory (AAD) conditional access. The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions. Conditional access policies incorporate Azure AD Identity Protection risk detections and include three default policies:

- Require all users to register for Azure AD Multi-Factor Authentication.
- Require a password change for users that are high risk.
- Require multi-factor authentication for users with medium or high sign-in risk.

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane. Conditional access policies are highly configurable and include several capabilities:

- Require MFA for admins
- End user protection
- Block legacy authentication
- Require MFA for Service Management
- Block access by location
- Require trusted location for MFA registration
- Require compliant devices

For more information, see What is Conditional Access?

Additionally**,** The VPN client is now able to integrate with the cloud-based Conditional Access Platform to provide a device compliance option for remote clients. Conditional

Access is a policy-based evaluation engine that lets you create access rules for any Azure Active Directory (Azure AD) connected application. For more information, see Configure Conditional Access.

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. You can manage connections and block access to external resources by creating an Azure Firewall and configuring respective policies. For more information, see Deploy and configure Azure Firewall.

Microsoft 365 DLP

Microsoft 365 DLP policies are how you monitor the activities that users take on sensitive items at rest, sensitive items in transit, or sensitive items in use and take protective actions. For example, when a user attempts to take a prohibited action, like copying a sensitive item to an unapproved location, or sharing medical information in an email or other conditions laid out in a policy.

Customer Responsibility

- Safeguarding measures for CUI are defined for alternate work sites.
- Enforcing safeguarding measures for CUI for alternate work sites.

Additional Resources

- Dive into the technical requirements and capabilities of Intune
- See feature differences between Intune and Intune for US Government
- Microsoft Intune for US Government GCC High
  Implementing a Zero Trust security model at Microsoft

Risk Assessment (RA)

RA.L2-3.11.1

Control Summary Information	
NIST 800-53 Mapping: RA-3	
Control : Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI.	
Primary Services	**Secondary Services**
Microsoft Defender for IoT	Microsoft Sentinel Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Microsoft Defender for Endpoint Insider Risk Management

Implementation Statement:

Risk arises from anything that can reduce an organization's assurance of mission/business success; cause harm to image or reputation; or harm individuals, other organizations, or the Nation. Risk assessments should be performed at defined regular intervals (e.g., yearly). Mission risks include anything that will keep an organization from meeting its mission. Function risk is anything that will prevent the performance of a function. Image and reputation risks refer to intangible risks that have value and could cause damage to potential or future trust relationships. For example, you evaluate the new risk involved with storing CUI. When conducting the assessment you consider increased legal exposure, financial requirements of safeguarding CUI, potentially elevated attention from external attackers, and other factors. After determining how storing CUI affects your overall risk profile, you use that as a basis for a conversation on how that risk should be mitigated.

Microsoft Defender for Cloud

To help assess risk, Microsoft Defender for Cloud provides the Secure Score calculation to provide a readily consumable assessment of your risk posture. Security Center mimics the work of a security analyst, reviewing your security recommendations and applying

advanced algorithms to determine how crucial each recommendation is. Microsoft Defender for Cloud constantly reviews your active recommendations and calculates your Secure Score based on them, the score of a recommendation is derived from its severity and security best practices that will affect your workload security the most. Security Center also provides you with an Overall Secure Score.

Overall Secure Score is an accumulation of all your recommendation scores. You can view your overall Secure Score across your subscriptions or management groups, depending on what you select. The score will vary based on subscription selected and the active recommendations on these subscriptions. To check which recommendations, impact your Secure Score most, you can view the top three most impactful recommendations in the Security Center dashboard or you can sort the recommendations in the recommendations list blade using the Secure Score impact column. For more information, see Improve your secure score in Microsoft Defender for Cloud .

Sentinel

Consider using Microsoft Sentinel as your Security Information and Event Management (SIEM) solution. After you connect your data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks. While Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to Create interactive reports with Azure Monitor Workbooks

Microsoft Sentinel provides hunting capabilities to align cyber defenders to threat tactics and facilitate building threat profiles. These profiles allow cyber defenders to target the phase of the attack lifecycle. Microsoft Sentinel hunting is aligned to the MITRE ATT&CK™ (adversarial tactics, techniques, and common knowledge) framework. These adversary tactics and techniques are grouped within a matrix. For more information, see Threat hunting: Part 1—Why your SOC needs a proactive hunting team.

The Microsoft Intelligent Security Graph uses advanced analytics to link a massive amount of threat intelligence and security data from Microsoft and partners to combat cyberthreats. Insights from the Intelligent Security Graph power real-time threat protection in Microsoft products and services. Also, many organizations utilize threat

intelligence platform (TIP) solutions to aggregate threat indicator feeds from a variety of sources. If your organization utilizes an integrated TIP solution the platforms data connector allows you leverage your TIP to import threat indicators into Microsoft Sentinel. The Threat Intelligence Platforms data connector works with the Microsoft Graph Security *Indicators* API to bring threat indicators into Azure. For more information, see Bring your threat intelligence to Microsoft Sentinel.

Microsoft Defender for Endpoint and Microsoft Defender for IoT

Utilizing Microsoft services such as Microsoft Defender for IoT and Microsoft Defender for Endpoint you can get full visibility into assets and risk across your entire IoT/OT environment to support risk mitigation. Microsoft Defender for IoT can proactively address vulnerabilities in your IoT/OT environment. Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your crown jewel assets.

Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. See Microsoft Defender for Endpoint page to learn more.

Get a bird's-eye view across IT/OT boundaries with interoperability with Microsoft Sentinel, cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with Microsoft Defender for Cloud Apps, and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud. Plus, get interoperability with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

Insider risk management

Insider risk management uses the full breadth of service and 3rd-party indicators to help you quickly identify, triage, and act on risk activity. By using logs from Microsoft 365 and Microsoft Graph, insider risk management allows you to define specific policies to

identify risk indicators. These policies allow you to identify risky activities and to act to mitigate these risks.

Moreover, insider risk analytics enables you to conduct an evaluation of potential insider risks in your organization without configuring any insider risk policies. This evaluation can help your organization identify potential areas of higher user risk and help determine the type and scope of insider risk management policies you may consider configuring.

Customer Responsibility

- Responsible for conducting a risk assessment that addresses the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of CUSTOMER-deployed resources and processed, stored, or transmitted information.
- Responsible for reviewing the Microsoft Azure Security Authorization package and performing a risk assessment for any controls deferred to CUSTOMER relating to shared touch points as identified in the Microsoft Azure CUSTOMER Responsibility Matrix.
- Responsible for conducting a risk assessment and documenting the risk assessment results in the security plan, risk assessment report, and/or other CUSTOMER-defined document.
- Responsible for conducting a risk assessment and reviewing its results at a CUSTOMER-defined frequency.
- Responsible for conducting a risk assessment and disseminating its results to CUSTOMER-defined personnel/roles.
- Responsible for updating the risk assessment at the CUSTOMER-defined frequency when there are significant changes to CUSTOMER-deployed resources (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

RA.L2-3.11.2

Control Summary Information	
NIST 800-53 Mapping: RA-5, RA-5(5)	
Control : Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
Primary Services	**Secondary Services**
Microsoft 365 Defender Microsoft Defender for IoT Microsoft Defender for Endpoint Microsoft Defender for Office 365 Threat and Vulnerability Management	Intune/Microsoft Endpoint Manager GitHub Enterprise Cloud GitHub AE GitHub Advanced Security (Add-On)

Implementation Statement:

Microsoft Defender for Cloud

Microsoft Defender for Cloud includes a built-in vulnerability scanner powered by Qualys. There is also capability for direct integration with the vulnerability scanner of your choice via the Azure Security Marketplace. Qualys's scanner is a leading tool for real-time identification of vulnerabilities in your Azure Virtual Machines. It's only available to users on the standard pricing tier. You do not need a Qualys license or even a Qualys account – everything is handled seamlessly inside Security Center. For more information, see Integrated vulnerability scanner for virtual machines (Standard tier only).

Microsoft Defender for IoT and Microsoft Defender for Endpoint

Utilizing Microsoft services such as Microsoft Defender for IoT and Microsoft Defender for Endpoint you can get full visibility into assets and risk across your entire IoT/OT environment to support risk mitigation. Microsoft Defender for IoT can proactively address vulnerabilities in your IoT/OT environment. Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and

firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your crown jewel assets.

Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. All devices onboarded in Microsoft Defender for Endpoint are scanned for vulnerabilities. See Microsoft Defender for Endpoint page to learn more.

Get a bird's-eye view across IT/OT boundaries with interoperability with Microsoft Sentinel, cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with Microsoft Defender for Cloud Apps, and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud. Plus, get interoperability with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

Threat and vulnerability management

Threat and vulnerability management is built in, real time, and cloud powered. It's fully integrated with Microsoft endpoint security stack, the Microsoft Intelligent Security Graph, and the application analytics knowledge base. To discover endpoint vulnerabilities and misconfiguration, threat and vulnerability management uses the same agentless built-in Defender for Endpoint sensors to reduce cumbersome network scans and IT overhead.

Moreover, threat and vulnerability management helps customers prioritize and focus on the weaknesses that pose the most urgent and the highest risk to the organization allowing security administrators and IT administrators to collaborate seamlessly to remediate issues.

Azure Policies

- **RA.L2-3.11.2 Azure Policies**

Customer Responsibility

- Responsible for performing periodic vulnerability scanning on all CUSTOMER-deployed resources, including applications built on those resources.
  responsible for performing scans of their applications running within or connected to their purchased Microsoft Azure VMs or deployments.
- Responsible for employing vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.
- Responsible for analyzing scan reports and results from security control assessments.
- Responsible for remediating vulnerabilities in CUSTOMER-deployed resources in accordance with CUSTOMER risk assessment.
- Responsible for sharing information obtained from the vulnerability scanning process and security control assessments to help eliminate similar vulnerabilities across CUSTOMER-deployed resources.
- Responsible for implementing privileged access for executing CUSTOMER-defined vulnerability scanning activities.

Additional Resources

- View findings from vulnerability assessment solutions in Microsoft Defender for Cloud Apps
- Adaptive application controls in Microsoft Defender for Cloud Apps
- Vulnerabilities in my organization - threat and vulnerability management
- MITRE ATT&CK® mappings released for built-in Azure security controls

RA.L2-3.11.3

Control Summary Information	
NIST 800-53 Mapping: RA-5	
Control : Remediate vulnerabilities in accordance with risk assessments.	
Primary Services	**Secondary Services**
Microsoft 365 Defender Microsoft Defender for Endpoint Microsoft Defender for IoT Microsoft Defender for Cloud	Intune/Microsoft Endpoint Manager GitHub Enterprise Cloud Microsoft Secure Score GitHub AE GitHub Advanced Security (Add-On) Insider Risk Management Threat and Vulnerability Management

Implementation Statement:

Microsoft Defender for IoT, Microsoft Defender for Endpoint and Microsoft 365 Defender

A vulnerability is a weakness that a threat actor could leverage, to compromise the confidentiality, availability, or integrity of a resource. Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. See Microsoft Defender for Endpoint page to learn more.

Managing vulnerabilities applies to Microsoft Defender for Endpoint and Microsoft 365 Defender. Managing vulnerabilities reduces organizational exposure, hardens endpoint surface area, increases organizational resilience, and reduces the attack surface of your resources. Threat and Vulnerability Management provides visibility into software and security misconfigurations and provide recommendations for mitigations.

Utilizing Microsoft services such as Microsoft Defender for IoT and Microsoft Defender for Endpoint you can get full visibility into assets and risk across your entire IoT/OT environment to support risk mitigation. Microsoft Defender for IoT can proactively

address vulnerabilities in your IoT/OT environment. Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your crown jewel assets.

Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. See Microsoft Defender for Endpoint page to learn more.

Get a bird's-eye view across IT/OT boundaries with interoperability with Microsoft Sentinel, cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with Microsoft Defender for Cloud Apps, and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud. Plus, get interoperability with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

Microsoft Defender for Cloud

Microsoft Defender for Cloud includes a built-in vulnerability scanner powered by Qualys. There is also capability for direct integration with the vulnerability scanner of your choice via the Azure Security Marketplace. Qualys's scanner is a leading tool for real-time identification of vulnerabilities in your Azure Virtual Machines. It is only available to users on the standard pricing tier. You do not need a Qualys license or even a Qualys account – everything is handled seamlessly inside Security Center. For more information, see Integrated vulnerability scanner for virtual machines (Standard tier only).

Microsoft Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level. To increase your security, review Security Center's recommendations page for the outstanding actions necessary to raise your score. Each recommendation includes instructions to help you remediate the specific issue.

Recommendations are grouped into **security controls**. Each control is a logical group of related security recommendations and reflects your vulnerable attack surfaces. Your score only improves when you remediate *all* of the recommendations for a single resource within a control. To see how well your organization is securing each individual attack surface, review the scores for each security control. Single click remediation is part of the Microsoft Defender for Cloud. Single-click remediations include policies to fix common vulnerabilities. For more information, see Microsoft Defender for Cloud single click remediation. For more information, see How your secure score is calculated.

Insider risk management

Insider risk management uses the full breadth of service and 3rd-party indicators to help you quickly identify, triage, and act on risk activity. By using logs from Microsoft 365 and Microsoft Graph, insider risk management allows you to define specific policies to identify risk indicators. These policies allow you to identify risky activities and to act to mitigate these risks.

Moreover, insider risk analytics enables you to conduct an evaluation of potential insider risks in your organization without configuring any insider risk policies. This evaluation can help your organization identify potential areas of higher user risk and help determine the type and scope of insider risk management policies you may consider configuring.

Customer Responsibility

- Remediating vulnerabilities in customer-deployed resources in accordance with the customer risk assessment.

Security Assessment (CA)

CA.L2-3.12.1

Control Summary Information	
NIST 800-53 Mapping: CA-2, CA-5, CA-7, PL-2	
Control : Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	
Primary Services	**Secondary Services**
	Microsoft Sentinel Azure Monitor Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Defender for IoT Microsoft Secure Score

Implementation Statement:

Azure Monitor

Azure Monitor maximizes the availability and performance of applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a unified infrastructure security management system that strengthens the security posture of your datacenters and provides advanced threat protection across your hybrid workloads in the cloud, be it Azure, any other cloud, or on-premises. Microsoft Defender for Cloud Apps helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard. In the dashboard, Security Center provides insights into your compliance posture based on continuous assessments of your Azure environment. Security Center analyzes risk factors in your hybrid cloud environment according to security best

practices. These assessments are mapped to compliance controls from a supported set of standards. In the Regulatory compliance dashboard, you can see the status of all the assessments within your environment in the context of a particular standard or regulation. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves. For more information, see Tutorial: Improve your regulatory compliance.

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native security information and event manager (SIEM) platform that uses built-in AI to analyze large volumes of data across the enterprise from all sources in a few seconds at a fraction of the cost. It includes built-in connectors for easy onboarding of popular security solutions and allows you to collect data from any source with support for open standard formats like CEF and Syslog. There are good practice baselines for Microsoft Sentinel. This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Microsoft Sentinel. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the **security controls** defined by the Azure Security Benchmark and the related guidance applicable to Microsoft Sentinel. To learn more, see Azure security baseline for Microsoft Sentinel.

Microsoft Secure Score

Microsoft Secure Score is a numerical summary of your security posture based on system configurations, user behavior, and other security-related measurements. Microsoft Secure Score represents the extent to which you have adopted security controls in your Microsoft environment that can help offset the risk of being breached.

Azure Service Health

Azure Service Health provides personalized alerts and guidance when Azure service issues affect our customers' business. It can notify you, help you understand the impact of issues, and keep you updated as the issue resolves. It can also help prepare for planned maintenance and changes that could affect the availability of your resources.

Azure Governance

Governance validates that your organization can achieve its goals through an effective and efficient use of IT. It meets this need by creating clarity between business goals and

IT projects. With Azure you build and scale your applications quickly while maintaining control.

Azure Blueprints

Azure Blueprints enable quick, repeatable creation of fully governed environments. This service helps you deploy and update cloud environments in a repeatable manner using artifacts such as policies, resource groups, deployment templates, and role-based access controls. This service is built to help DevOps set up governed Azure environments and scale to support production implementations for large-scale migrations.

Azure Blueprints provides an avenue to apply security controls, policies and resources. Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they are building within organizational compliance with a set of built-in components — such as networking — to speed up development and delivery. Azure Blueprints can actively apply controls with the *deployifnotexists* option or can be leveraged for monitoring controls passively with the *auditifnotexists* option. For more information, see Tutorial: Protect new resources with Azure Blueprints resource locks

Customer Responsibility

- Assessing the security controls in organizational systems to determine if the controls are effective in their application.

CA.L2-3.12.2

Control Summary Information	
NIST 800-53 Mapping: CA-2, CA-5, CA-7, PL-2	
Control : Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
Primary Services	**Secondary Services**
	Microsoft Defender for Endpoint Threat and Vulnerability Management Microsoft Sentinel Microsoft Secure Score Microsoft 365 Web Apps

Implementation Statement:

Microsoft Defender for Endpoint

Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization. Your score for devices is visible in the threat and vulnerability management dashboard of the Microsoft Defender Security Center. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. Improve your security configuration by remediating issues from the security recommendations list. As you do so, your Microsoft Secure Score for Devices improves, and your organization becomes more resilient against cybersecurity threats and vulnerabilities.

For more information see, learn how it works.

Customer Responsibility

- Develop & implement a POA&M to correct identified deficiencies and reduce or eliminate identified vulnerabilities
- Document, review and approve the POA&M
- Identify deficiencies and vulnerabilities to be addresses by the POA&M

- Identify personnel responsible for the development and implementation of the POA&M

CA.L2-3.12.3

Control Summary Information	
NIST 800-53 Mapping: CA-2, CA-5, CA-7, PL-2	
Control : Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	
Primary Services	**Secondary Services**
	Microsoft Sentinel Microsoft 365 Defender Microsoft Secure Score Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint M365 Compliance Center Azure Monitor

Implementation Statement:

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions.

Azure Monitor

Azure Monitor maximizes the availability and performance of applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud and on-premises environments. It helps you understand how your applications are

performing and proactively identifies issues affecting them and the resources they depend on.

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a unified infrastructure security management system that strengthens the security posture of your datacenters and provides advanced threat protection across your hybrid workloads in the cloud, be it Azure, any other cloud, or on-premises. Microsoft Defender for Cloud Apps helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard. In the dashboard, Security Center provides insights into your compliance posture based on continuous assessments of your Azure environment. Security Center analyzes risk factors in your hybrid cloud environment according to security best practices. These assessments are mapped to compliance controls from a supported set of standards. In the Regulatory compliance dashboard, you can see the status of all the assessments within your environment in the context of a particular standard or regulation. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves. For more information, see Tutorial: Improve your regulatory compliance.

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native security information and event manager (SIEM) platform that uses built-in AI to analyze large volumes of data across the enterprise from all sources in a few seconds at a fraction of the cost. It includes built-in connectors for easy onboarding of popular security solutions and allows you to collect data from any source with support for open standard formats like CEF and Syslog. There are good practice baselines for Microsoft Sentinel. This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Microsoft Sentinel. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the **security controls** defined by the Azure Security Benchmark and the related guidance applicable to Microsoft Sentinel. To learn more, see Azure security baseline for Microsoft Sentinel.

Microsoft Secure Score

Microsoft Secure Score is a numerical summary of your security posture based on system configurations, user behavior, and other security-related measurements.

Microsoft Secure Score represents the extent to which you have adopted security controls in your Microsoft environment that can help offset the risk of being breached.

Azure Service Health

Azure Service Health provides personalized alerts and guidance when Azure service issues affect our customers' business. It can notify you, help you understand the impact of issues, and keep you updated as the issue resolves. It can also help prepare for planned maintenance and changes that could affect the availability of your resources.

Azure Governance

Governance validates that your organization can achieve its goals through an effective and efficient use of IT. It meets this need by creating clarity between business goals and IT projects. With Azure you build and scale your applications quickly while maintaining control.

Azure Blueprints

Azure Blueprints enable quick, repeatable creation of fully governed environments. This service helps you deploy and update cloud environments in a repeatable manner using artifacts such as policies, resource groups, deployment templates, and role-based access controls. This service is built to help DevOps set up governed Azure environments and scale to support production implementations for large-scale migrations.

Azure Blueprints provides an avenue to apply security controls, policies and resources. Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they are building within organizational compliance with a set of built-in components — such as networking — to speed up development and delivery. Azure Blueprints can actively apply controls with the *deployifnotexists* option or can be leveraged for monitoring controls passively with the *auditifnotexists* option. For more information, see Tutorial: Protect new resources with Azure Blueprints resource locks.

Customer Responsibility

- Identifying security controls to be continuously monitored.

- Define a frequency to continuously monitor to support risk-based decision making.
- Provide output of monitoring activities to stake holders.

CA.L2-3.12.4

Control Summary Information	
NIST 800-53 Mapping: CA-2, CA-5, CA-7, PL-2	
Control : Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.	
Primary Services	**Secondary Services**
	Microsoft 365 Web Apps Power Automate Microsoft Lists

Implementation Statement:

Microsoft 365 can help remind you to perform updates on documents such as the SSP. With Microsoft 365, reminders to review documentation are made simple. Setup details such as description, review date, owner and receive an email reminder for items due soon with a pre-built Power Automate flow in Microsoft Lists or SharePoint.

Customer Responsibility:

- Developing a system security plan (SSP) that meets the criteria defined by the target authorization (e.g., FedRAMP). Customers may reference NIST Special Publication 800-18 R1, *Guide for Developing Security Plans for Federal Information Systems*. The customer SSP should address controls inherited from Microsoft Azure.
- Distributing the system security plan.
- Reviewing the system security plan.
- Updating the system security plan.
- Protecting the system security plan.

Systems and Communications Protection (SC)

SC.L2-3.13.1

Control Summary Information	
NIST 800-53 Mapping: SC-7, SA-8	
Control : Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	
Primary Services	**Secondary Services**
Microsoft Sentinel Microsoft Information Protection Azure Firewall	Microsoft Azure Portal Azure Monitor Azure Bastion Azure ExpressRoute VPN Gateway Load Balancer Log Analytics Workspace Network Security Groups Azure Web Application Firewall Azure Virtual Machines Virtual Network Conditional Access Customer Lockbox Intune/Microsoft Endpoint Manager Conditional Access Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Defender for Office 365 Microsoft 365 DLP Microsoft Defender for IoT

Implementation Statement:

Azure Firewall

Implement boundary protection through the use of controlled devices at the network boundary and at key points within the information system. The overarching principle should be to allow only connection and communication that is necessary for systems to operate, blocking all other ports, protocols and connections by default.

If you configure network rules and application rules, then network rules are applied in priority order before application rules. The rules are terminating. If a match is found in a network rule, no other rules are processed. If there is no network rule match, and if the protocol is HTTP, HTTPS, or MSSQL, then the packet is then evaluated by the application rules in priority order. If still no match is found, then the packet is evaluated against the infrastructure rule collection. If there is still no match, then the packet is denied by default.

Inbound Internet connectivity can be enabled by configuring Destination Network Address Translation (DNAT) as described in Tutorial: Filter inbound traffic with Azure Firewall DNAT using the Azure portal. NAT rules are applied in priority before network rules. If a match is found, an implicit corresponding network rule to allow the translated traffic is added. For security reasons, the recommended approach is to add a specific internet source to allow DNAT access to the network and avoid using wildcards. For more information, see Deploy and configure Azure Firewall using the Azure portal.

Application rules are not applied for inbound connections. If you want to filter inbound HTTP/S traffic, you should use Web Application Firewall (WAF). For more information, see What is Azure Web Application Firewall?

Intune/Microsoft Endpoint Manager

Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory

Network Security Groups

Network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify to create an augmented security rule.

Conditional Access

Conditional access policies can be integrated with Defender for Cloud Apps to provide controls for cloud and on-premises applications from external systems. Mobile application management in Intune can protect organization data at the application level, including custom apps and store apps, from managed devices that interact with external systems. An example would be accessing cloud services. You can use app management on organization-owned devices and personal devices.

Microsoft 365 inter-tenant collaboration

Microsoft 365 inter-tenant collaboration options include using a central location for files and conversations, sharing calendars, using IM, audio/video calls for communication, and securing access to resources and applications.

Microsoft Information Protection (MIP)

Microsoft Information Protection (MIP) prevents the transfer of unauthorized and unintended information transfer. Once data is marked with a sensitivity label that includes encryption settings, data and emails marked as containing CUI are protected. MIP sensitivity labels enforce controls on information sharing, such as forwarding, printing, and downloading.

Microsoft 365 DLP

Data loss prevention (DLP) helps you prevent the unintentional or accidental sharing of sensitive information. When the risks of data leakage aren't entirely obvious, it's difficult to work out where exactly you should start with implementing DLP. Fortunately, DLP policies can be run in "test mode", allowing you to gauge their effectiveness and accuracy before you turn them on. DLP policies for Exchange Online can be managed through the Exchange admin center. But you can configure DLP policies for all workloads through the Security & Compliance Center.

Azure Policies

- **SC.L2-3.13.1 Azure Policies**

Customer Responsibility

- monitoring and controlling communications at and within the boundaries of the CUSTOMER-deployed system.
- implementing subnetworks for CUSTOMER-deployed resources to logically separate publicly accessible resources from internal resources.
- restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the CUSTOMER's security architecture.
- configuring all CUSTOMER-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
- configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. CUSTOMER’s who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

SC.L2-3.13.2

Control Summary Information	
NIST 800-53 Mapping: SC-7, SA-8	
Control : Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.	
Primary Services	**Secondary Services**

Implementation Statement:

Promote effective information security within your organizational systems by implementing secure security design principles. Microsoft recommendations for security design principles support these three key strategies (Security Strategy, Enterprise Segmentation Strategy and Account Control Strategy) and describe a securely architected system hosted on cloud or on-premises datacenters (or a combination of both). Application of these principles will dramatically increase the likelihood your security architecture will maintain assurances of confidentiality, integrity, and availability.

Customer Responsibility

- monitoring and controlling communications at and within the boundaries of the CUSTOMER-deployed system.
- implementing subnetworks for CUSTOMER-deployed resources to logically separate publicly accessible resources from internal resources.
- restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the CUSTOMER's security architecture.
- configuring all CUSTOMER-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
- configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. CUSTOMERs who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong

encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

SC.L2-3.13.3

Control Summary Information	
NIST 800-53 Mapping: SC-2	
Control : Separate user functionality from system management functionality.	
Primary Services	**Secondary Services**
Azure Active Directory Azure RBAC	Conditional Access Privileged Identity Management (PIM)

Implementation Statement:

Azure Active Directory (AAD) Role Based Access Control

Azure AD roles allow you to grant granular permissions to your admins, abiding by the principle of least privilege. Azure AD built-in and custom roles operate on concepts similar to those you will find in the role-based access control system for Azure resources (Azure roles). The difference between these two role-based access control systems is:

- Azure AD roles control access to Azure AD resources such as users, groups, and applications using Graph API
- Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

Both systems contain similarly used role definitions and role assignments. However, Azure AD role permissions cannot be used in Azure custom roles and vice versa.

Microsoft Azure Active Directory (AAD) offers a robust security set for enforcing the separation of user functionality from system management functionality. A good practice is to segregate duties within your team by setting up Role Based Access Control (RBAC) which will help you manage who has access to Azure resources.

Ensure that the right users have the right access to the right resources by using intelligent cloud identity governance. Monitor and audit access to all resources while managing employee productivity.

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

Privileged Identity Management (PIM)

With Azure AD PIM, you can manage, control, and monitor your privileged identities and access to your directory information and resources in an Azure environment. The main reason for using Azure AD PIM is to reduce the attack surface and to enable administrative access just-in-time. Privileged access is often configured as permanent and unmonitored, but with Azure AD PIM you can avoid security breaches and risks.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses Azure AD Multi-Factor Authentication. For example, during the activation process, a user can be forced to justify why they need to activate their role. Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

Privileged Identity Management (PIM) provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

Network Security Groups

Network Security Groups are customizable and provide the ability to fully lock down network communication to and from your system-resources. You can restrict internet access by default, along with the use of network security groups, data segregation and isolated VPNs.

Use Azure Active Directory to manage and secure identities by requiring single sign-on and multifactor authentication to protect your users. The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access Policies. Learn how to Create a Conditional Access Policy.

Additionally, Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with

Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Explore using Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

Customer Responsibility

- Separating system functionality into two separate categories: user functionality and management functionality.

SC.L2-3.13.4

Control Summary Information	
NIST 800-53 Mapping: SC-4	
Control : Prevent unauthorized and unintended information transfer via shared system resources.	
Primary Services	**Secondary Services**
Microsoft Information Protection Microsoft 365 DLP	Network Security Groups Azure Web Application Firewall Azure Virtual Machines Virtual Network

Control Summary Information	
	Intune/Microsoft Endpoint Manager Azure RBAC Microsoft Defender for Office 365 Privileged Identity Management (PIM) Azure AD Multi-Factor Authentication Conditional Access

Implementation Statement:

Microsoft Information Protection

Microsoft Information Protection (MIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content. MIP is part of the Microsoft Information Protection (MIP) solution, and extends the labeling and classification functionality provided by Microsoft 365.

By default, built-in labeling is turned off in Office apps when the Microsoft Information Protection client is installed. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. For more information, including how to change this default behavior, see Office built-in labeling client and the Microsoft Information Protection client.

Even when you use built-in labeling in Office apps, you can also use the Microsoft Information Protection unified labeling client with sensitivity labels for the following:

- A scanner to discover sensitive information that is stored on-premises, and then optionally, label that content
- Right-click options in File Explorer for users to apply labels to all file types
- A viewer to display encrypted files for text, images, or PDF documents
- A PowerShell module to discover sensitive information in files on premises and apply or remove labels and encryption from these files.

If you are new to Microsoft Information Protection, or if you are an existing Microsoft Information Protection customer who has recently migrated your labels, see Choose

your Windows labeling solution from the Microsoft Information Protection documentation.

When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

- Only users within your organization can open a confidential document or email.
- Only users in the marketing department can edit and print the promotion announcement document or email, while all other users in your organization can only read it.
- Users cannot forward an email or copy information from it that contains news about an internal reorganization.
- The current price list that is sent to business partners cannot be opened after a specified date.

There are several features that assist in protecting against unauthorized and unintended information transfer. To learn more, see Restrict access to content by using sensitivity labels to apply encryption.

Microsoft 365 DLP

Data loss prevention (DLP) helps you prevent the unintentional or accidental sharing of sensitive information. When the risks of data leakage aren't entirely obvious, it's difficult to work out where exactly you should start with implementing DLP. Fortunately, DLP policies can be run in "test mode", allowing you to gauge their effectiveness and accuracy before you turn them on. DLP policies for Exchange Online can be managed through the Exchange admin center. But you can configure DLP policies for all workloads through the Security & Compliance Center.

Azure Active Directory (AAD) Role Based Access Control

Azure AD roles allow you to grant granular permissions to your admins, abiding by the principle of least privilege. Azure AD built-in and custom roles operate on concepts similar to those you will find in the role-based access control system for Azure

resources (Azure roles). The difference between these two role-based access control systems is:

- Azure AD roles control access to Azure AD resources such as users, groups, and applications using Graph API
- Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

Both systems contain similarly used role definitions and role assignments. However, Azure AD role permissions cannot be used in Azure custom roles and vice versa.

Microsoft Azure Active Directory (AAD) offers a robust security set for preventing unauthorized and unintended information transfer via shared system resources. Best practice recommendation is to segregate duties within your team by setting up Role Based Access Control (RBAC) which will help you manage who has access to Azure resources.

Ensure that the right users have the right access to the right resources by using intelligent cloud identity governance. Monitor and audit access to all resources while managing employee productivity.

Additionally, you can secure privileged access within your organization using Privileged Identity Management (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces Just In Time access for these accounts which allows timed permission to be granted for specific resources.

Privileged Identity Management (PIM)

With Azure AD PIM, you can manage, control, and monitor your privileged identities and access to your directory information and resources in an Azure environment. The main reason for using Azure AD PIM is to reduce the attack surface and to enable administrative access just-in-time. Privileged access is often configured as permanent and unmonitored, but with Azure AD PIM you can avoid security breaches and risks.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses Azure AD Multi-Factor Authentication. For example, during the activation process, a user can be forced to justify why they need to activate their role.

Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

Privileged Identity Management (PIM) provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

Network Security Groups

Network Security Groups are customizable and provide the ability to fully lock down network communication to and from your system-resources. You can restrict internet access by default, along with the use of network security groups, data segregation and isolated VPNs.

Use Azure Active Directory to manage and secure identities by requiring single sign-on and multifactor authentication to protect your users. The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access Policies. Learn how to Create a Conditional Access Policy.

Additionally, Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Explore using Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

Customer Responsibility

- preventing unauthorized and unintended information transfer between CUSTOMER-deployed resources.

SC.L2-3.13.5

Control Summary Information	
NIST 800-53 Mapping: SC-7	
Control : Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	
Primary Services	**Secondary Services**
	Azure Bastion Azure Firewall Load Balancer Network Security Groups Azure Web Application Firewall Virtual Network

Implementation Statement:

Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.

A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs. An internal (or private) load balancer is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario. Standard load balancers and standard public IP addresses are closed to inbound connections unless opened by Network Security Groups. NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach

this resource. To learn about NSGs and how to apply them to your scenario, see Network Security Groups.

Employ Remote Desktop Gateways services as the internal/external managed interface for interactive access to the infrastructure environment. Require encrypted connections for connectivity from any of the solutions used to access the environment remotely or from the corporate network.

Azure Bastion is a fully managed platform PaaS service from Azure that is hardened internally to provide you secure RDP/SSH connectivity. You do not need to apply any NSGs on Azure Bastion subnet. Because Azure Bastion connects to your virtual machines over private IP, you can configure your NSGs to allow RDP/SSH from Azure Bastion only. This removes the hassle of managing NSGs each time you need to securely connect to your virtual machines. Create an Azure Bastion host and connect to a Windows VM.

Azure Policies

- **SC.L2-3.13.5 Azure Policies**

Customer Responsibility

- monitoring and controlling communications at and within the boundaries of the CUSTOMER-deployed system.
- implementing subnetworks for CUSTOMER -deployed resources to logically separate publicly accessible resources from internal resources.
- restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the CUSTOMER 's security architecture.
- configuring all CUSTOMER -deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
- configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. CUSTOMER’s who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

SC.L2-3.13.6

Control Summary Information	
NIST 800-53 Mapping: SC-7(5)	
Control : Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).	
Primary Services	**Secondary Services**
Azure Firewall	Microsoft Defender for IoT Load Balancer Network Security Groups Azure Web Application Firewall Virtual Network Conditional Access Intune/Microsoft Endpoint Manager

Implementation Statement:

Azure Firewall

You can configure NAT rules, network rules, and applications rules on Azure Firewall. The rules are processed according to the rule type and traffic is dropped by default if it is not permitted.

Outbound: If you configure network rules and application rules, then network rules are applied in priority order before application rules. The rules are processed such that when a match is found in a network rule, no further rules are processed. If there is no network rule match, and if the protocol is HTTP, HTTPS, or MSSQL, then the packet is then evaluated by the application rules in priority order. If still no match is found, then the packet is evaluated against the infrastructure rule collection. If there is still no match, then the packet is denied by default.

Inbound Internet connectivity can be enabled by configuring Destination Network Address Translation (DNAT) as described in Tutorial: Filter inbound traffic with Azure Firewall DNAT using the Azure portal. NAT rules are applied in priority before network rules. If a match is found, an implicit corresponding network rule to allow the translated traffic is added. For security reasons, the recommended approach is to add a specific

internet source to allow DNAT access to the network and avoid using wildcards. For more information, see Deploy and configure Azure Firewall using the Azure portal.

Application rules are not applied for inbound connections. If you want to filter inbound HTTP/S traffic, you should use the Web Application Firewall (WAF). For more information, see What is Azure Web Application Firewall?

Intune/Microsoft Endpoint Manager

Use the endpoint security Firewall policy in Intune to configure a devices built-in firewall for devices that run macOS and /11. Intune and Azure Active Directory work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and on-premises apps. Additionally, you can set a policy in Azure Active Directory to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Azure Active Directory

Network Security Groups

Network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify to create an augmented security rule.

Customer Responsibility

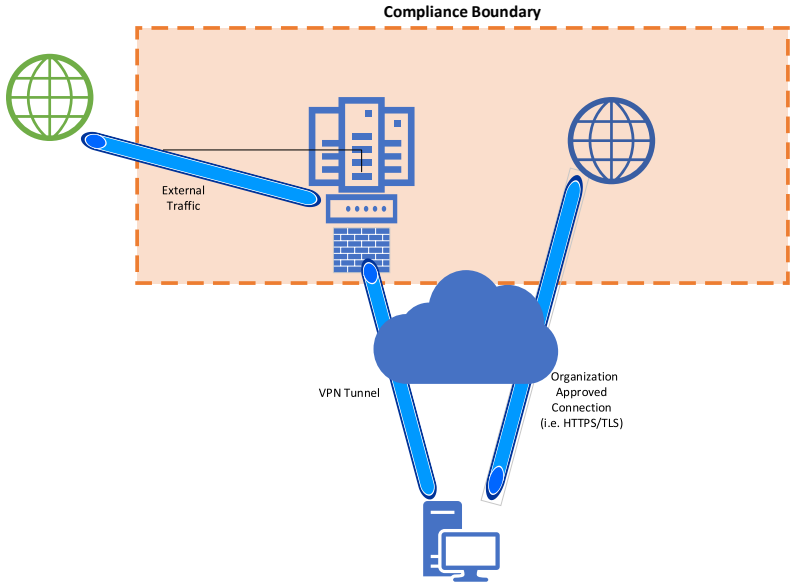
- Configuring managed network interfaces to deny all traffic by default and permit by exception.

SC.L2-3.13.7

Control Summary Information	
NIST 800-53 Mapping: SC-7(7)	
Control : Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	
Primary Services	**Secondary Services**
Azure VPN Azure Firewall	Azure ExpressRoute Azure Virtual Desktop Azure Active Directory

Implementation Statement:

External networks are those networks, or Internet services, that are outside the organization's scoped compliance boundary. A remote user connected to the internal network [scoped compliance boundary] must not be able to connect to an external network / Internet service directly. The external network traffic must flow through the organization's managed network security devices (i.e., outbound proxy firewall).



SC.3.184 Compliance Boundary

In the above illustration, both the Enterprise Datacenter and the Cloud Service Provider (e.g., Microsoft 365) fall within the organization's scoped compliance boundary. All applications and services hosted within the compliance boundary demonstrate compliance with CMMC maturity Level 2 (or higher) for protection of CUI.

Remote Users

The remote user's device when connected to the organizational internal network, must be configured with a routing table, such that all traffic for external networks will flow through the organization's managed network security devices. An organization could use the Azure VPN to securely connect to their Azure resources and apply appropriate routing tables.

For those that run an on-premises VPN solution, Azure ExpressRoute can be used to extend your on-premises datacenter, such that your Azure resources (e.g., virtual machines) can be considered part of your hybrid managed datacenter. Routing tables must be configured to ensure access to external networks / Internet services are monitored and controlled by the organization.

"Dynamic Routing", *not to be confused with external network split-tunning*, is achieved by configuring a conditional access rule on the organization's VPN to route to services *directly* within the organization's scoped compliance boundary. For example, cloud services like Microsoft 365 that fall within the compliance boundary are whitelisted in a manner where traffic from a trusted endpoint may bypass the VPN device in the enterprise datacenter and communicate directly with the cloud service provider.

Azure Virtual Machines

Forced tunneling lets you redirect, or "force", all Internet-bound traffic initiated from your Azure VMs through your firewall for inspection and auditing. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Unauthorized Internet access can potentially lead to information disclosure or other types of security breaches. For more information, see Configure forced tunneling using the Azure Resource Manager deployment model.

Azure Firewall

A cloud-based firewall such as Azure Firewall may act as the central security control point for network traffic, providing a ubiquitous and separate security layer in the cloud through which web traffic may flow. Azure Firewall not only protects Azure Virtual Network resources but offers Premium features such as URL Filtering and a network intrusion detection and prevention system (IDPS) allowing you to monitor the network for malicious activity, log information about this activity, report it, and optionally attempt to block it. Azure Firewall may also provide a proxied connection to SaaS services including Office 365.

Azure AD Application Proxy

In addition to Azure Firewall, Azure Active Directory's Application Proxy can provide secure remote access to web applications hosted in Azure or even in an on-premises datacenter. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal. For example, Application Proxy can provide remote access and single sign-on to line of business (LOB) web applications. It's here where security policies can be applied, ensuring policy enforcement regardless of whether the user is behind a firewall or logging on from home.

Customer Responsibility

- Preventing split tunneling for remote devices connecting to the CUSTOMER-deployed system.

Additional Resources

- CMMC and Split Tunnels to Cloud Services Whitepaper
- Zero Trust Architecture
- Using a Zero Trust strategy to secure Microsoft's network during remote work
- Time to Rethink How You Provide Secure Internet Access for Remote Workers
- CMMC, Split Tunneling, and COVID
- Implementing VPN Split Tunneling for Microsoft 365

SC.L2-3.13.8

Control Summary Information	
NIST 800-53 Mapping: SC-8, SC-8(1)	
Control : Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
Primary Services	**Secondary Services**
Microsoft Information Protection Office 365 Message Encryption (OME)	Azure ExpressRoute Azure Key Vault Load Balancer Network Security Groups Azure Virtual Machines Virtual Network VPN Gateway Intune/Microsoft Endpoint Manager Conditional Access Bitlocker Microsoft Defender for Cloud Apps Microsoft Azure Portal

Implementation Statement:

You can have multiple layers of encryption in place at the same time. For example, you can encrypt email messages and also the communication channels through which your email flows. With Office 365, your data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES). Microsoft 365 provides Microsoft-managed solutions for volume encryption, file encryption, and mailbox encryption in Office 365. In addition, Microsoft provides encryption solutions that you can manage and control. These encryption solutions are built on Azure.

Office 365 Message Encryption

With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Office 365

Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content. Office 365 Message Encryption is an online service that's built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection. This service includes encryption, identity, and authorization policies to help secure your email. You can encrypt messages by using rights management templates, the Do Not Forward option, and the encrypt-only option.

Encrypt CUI on mobile devices and mobile computing platforms using Intune/Microsoft Endpoint Manager with Conditional access to require encryption, such as BitLocker for Windows 10 and later. Require app protection policy and an approved client app for cloud app access. Create and assign Microsoft Intune app protection policies to ensure that apps are protected with a PIN and Encrypted.

See the Android app protection policy settings and iOS/iPadOS app protection policy settings for detailed information on the encryption app protection policy setting.

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Additionally, using Microsoft Intune built-in Wi-Fi settings called a "profile", you can deploy specific Wi-Fi connection requirements to users with supported devices in your organization. Intune/Microsoft Endpoint Manager offers many features, including authenticating to your network, using a pre-shared key for encryption and more.

The Azure platform offers several mechanisms for keeping sessions secure including encryption in flight, and key management with Azure Key Vault. For more information see, Azure encryption overview.

Microsoft gives customers the ability to use Transport Layer Security (TLS) protocol to protect data when it is traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling

detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

Explore using Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

Azure Virtual Machines

You can connect and sign in to a VM by using the Remote Desktop Protocol (RDP) from a Windows client computer, or from a Mac with an RDP client installed. Data in transit over the network in RDP sessions can be protected by TLS. You can also use Remote Desktop to connect to a Linux VM in Azure.

For remote management, you can use Secure Shell (SSH) to connect to Linux VMs running in Azure. SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. It is the default connection protocol for Linux VMs hosted in Azure. By using SSH keys for authentication, you eliminate the need for passwords to sign in. SSH uses a public/private key pair (asymmetric encryption) for authentication.

Key Vault

Without proper protection and management of the keys, encryption is rendered useless. Key Vault is the Microsoft-recommended solution for managing and controlling access to encryption keys used by cloud services. Permissions to access keys can be assigned to services or to users through Azure Active Directory accounts.

Key Vault relieves organizations of the need to configure, patch, and maintain hardware security modules (HSMs) and key management software. When you use Key Vault, you maintain control. Microsoft never sees your keys, and applications do not have direct access to them. You can also import or generate keys in HSMs. For more information, see About Azure Key Vault.

VPN

You can use an Azure VPN gateway to send encrypted traffic between your virtual network and your on-premises location across a public connection, or to send traffic between virtual networks.

Site-to-site VPNs use IPsec for transport encryption. Azure VPN gateways use a set of default proposals. You can configure Azure VPN gateways to use a custom IPsec/IKE policy with specific cryptographic algorithms and key strengths, rather than the Azure default policy sets.

Intune/Microsoft Endpoint Manager

Use Intune to configure encryption at rest using BitLocker Drive Encryption on devices that run Windows 10. Some settings for BitLocker require the device have a supported TPM. To manage BitLocker in Intune, your account must have the applicable Intune role-based access control (RBAC) permissions. For more information on how to enforce BitLocker encryption using Intune, see Create and deploy policy.

Intune can also manage macOS FileVault disk encryption. FileVault is a whole-disk encryption program that is included with macOS. You can use Intune to configure FileVault on devices that run macOS 10.13 or later**.** For more information on how to enforce FileVault encryption using Intune, see Create device configuration policy for FileVault

Additionally, Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Azure Storage Account

Azure Storage uses server-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments. Data in

Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is like BitLocker encryption on Windows.

Azure Storage encryption is enabled for all storage accounts, including both Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled. Because your data is secured by default, you do not need to modify your code or applications to take advantage of Azure Storage encryption.

However, you can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.

You must use one of the following Azure key stores to store your customer-managed keys:

- Azure Key Vault
- Azure Key Vault Managed Hardware Security Module (HSM) (preview)

You can switch between customer-managed keys and Microsoft-managed keys at any time. For more information about Microsoft-managed keys, see About encryption key management. To learn more, see Enable Customer-Managed keys for a storage account.

Azure Policies

- **SC.L2-3.13.8 Azure Policies**

Customer Responsibility

- Configuring all customer-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
- Configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. Customers who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong

encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

- For protecting information in transit by using cryptographic mechanisms to prevent the unauthorized disclosure of and/or detecting changes to customer-controlled information during transmission.

SC.L2-3.13.9

Control Summary Information	
NIST 800-53 Mapping: SC-10	
Control : Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	
Primary Services	**Secondary Services**
	Microsoft Azure Portal Azure Virtual Machines VPN Gateway Azure Active Directory Intune/Microsoft Endpoint Manager M365 Web Apps Conditional Access

Implementation Statement:

Azure Active Directory

Implement automatic user session re-evaluation with Azure AD features such as Risk-Based Conditional Access and Continuous Access Evaluation. Inactivity conditions can be implemented at a device level as described in:

- Sign-in risk-based Conditional Access
- User risk-based Conditional Access
- Continuous Access Evaluation
- Configurable token lifetimes - Microsoft identity platform | Microsoft Docs

The Azure AD default for browser session persistence allows users on personal devices to choose whether to persist the session by showing a “Stay signed in?” prompt after successful authentication. If browser persistence is configured in AD FS using the guidance in the article AD FS Single Sign-On Settings, we will comply with that policy and persist the Azure AD session as well. You can also configure whether users in your tenant see the “Stay signed in?” prompt by changing the appropriate setting in the company branding pane in Azure portal using the guidance in the article Customize your Azure AD sign-in page.
For more information, see Configure authentication session management with Conditional Access.

Microsoft 365 web apps

When users authenticate in any of the Microsoft 365 web apps or mobile apps, a session is established. For the duration of the session, users won't need to re-authenticate. Sessions can expire when users are inactive, when they close the browser or tab, or when their authentication token expires for other reasons such as when their password has been reset. The Microsoft 365 services have different session timeouts to correspond with the typical use of each service.

Azure VPN Gateway

Azure virtual network gateways provide an easy way to view and disconnect current Point-to-site VPN sessions. The session status is updated every 5 minutes. Learn more on how to view and disconnect current sessions.

Customer Responsibility

- implementing a network disconnect for CUSTOMER-deployed resources at the end of a communication session or after a CUSTOMER-defined time period of inactivity.

SC.L2-3.13.10

Control Summary Information	
NIST 800-53 Mapping: SC-12	
Control : Establish and manage cryptographic keys for cryptography employed in organizational systems.	
Primary Services	**Secondary Services**
Azure Key Vault GitHub AE	Microsoft Information Protection GitHub Enterprise Cloud Bitlocker Distributed Key Manager Customer Key

Implementation Statement:

Secure key management is essential to protect data in the cloud. Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and Microsoft processes your keys in FIPS 140-2 Level 3 validated Thales Luna 7 HSM.

Azure Dedicated HSM is a cloud-based service that provides HSMs hosted in Azure datacenters that are directly connected to a customer's virtual network. These HSMs are dedicated Thales Luna 7 HSM network appliances. They are deployed directly to a customers' private IP address space and Microsoft does not have any access to the cryptographic functionality of the HSMs. Only the customer has full administrative and cryptographic control over these devices. Customers are responsible for the management of the device, and they can get full activity logs directly from their devices. Dedicated HSMs help customers meet compliance/regulatory requirements such as FIPS 140-2 Level 3, HIPAA, PCI-DSS, and eIDAS and many others.

With Key Vault, Microsoft does not see or extract your keys. Monitor and audit your key use with Azure logging—pipe logs into Azure HDInsight or your security information and event management (SIEM) solution such as Microsoft Sentinel for more analysis and

threat detection. For more information, see Quickstart: Set and retrieve a secret from Azure Key Vault using the Azure portal.

BitLocker, Customer Key and Distributed Key Manager (DKM)

Microsoft 365 provides baseline, volume-level encryption enabled through BitLocker and Distributed Key Manager (DKM). Microsoft 365 offers an added layer of encryption for your content. This content includes data from Exchange Online, Skype for Business, SharePoint Online, OneDrive for Business, and Microsoft Teams.

Customer Key provides extra protection against viewing of data by unauthorized systems or personnel, and complements BitLocker disk encryption in Microsoft data centers. Service encryption is not meant to prevent Microsoft personnel from accessing your data. Instead, Customer Key helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on. Customer Key is built on service encryption and lets you provide and control encryption keys. Microsoft 365 then uses these keys to encrypt your data at rest.

Customer Responsibility

- Managing cryptographic keys used within CUSTOMER-deployed resources in accordance with CUSTOMER-defined requirements for key generation, distribution, storage, access, and destruction.

SC.L2-3.13.11

Control Summary Information	
NIST 800-53 Mapping: SC-13	
Control : Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
Primary Services	**Secondary Services**
Azure Key Vault Bitlocker	Microsoft Azure Portal Azure Firewall Azure Virtual Machines Microsoft Information Protection Intune/Microsoft Endpoint Manager Conditional Access GitHub AE

Implementation Statement:

The Federal Information Processing Standard (FIPS) Publication 140 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

Microsoft maintains an active commitment to meeting the FIPS 140 requirements, having validated cryptographic modules since the standard's inception in 2001. Microsoft certifies the cryptographic modules used in Microsoft products with each new release of the Windows operating system. For technical information on Microsoft Windows cryptographic modules, the security policy for each module, and the catalog of CMVP certificate details, see the Windows and Windows Server FIPS 140 documentation.

Windows provides the security policy setting, *System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing*. This setting is used by some Microsoft products to determine whether to run in FIPS mode. When this policy is turned on, the validated cryptographic modules in Windows will also operate in FIPS mode. This policy may be set using Local Security Policy, as part of Group Policy, or through a Modern

Device Management (MDM) solution. For more information on the policy, see System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing.

Through the Microsoft Security Development Lifecycle (SDL), all Azure services use FIPS 140-2 approved algorithms for data security because the operating system uses FIPS 140-2 approved algorithms while operating at a hyper scale cloud. Moreover, Azure customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM).

Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and Microsoft processes your keys in FIPS validated HSMs (hardware and firmware) - FIPS 140-2 Level 2 for vaults and FIPS 140-2 Level 3 for HSM pools. With Key Vault, Microsoft does not see or extract your keys. Monitor and audit your key use with Azure logging—pipe logs into Azure HDInsight or your security information and event management (SIEM) solution for more analysis and threat detection.

While the current CMVP FIPS 140-2 implementation guidance precludes a FIPS 140-2 validation for a cloud service itself; cloud service providers can choose to obtain and operate FIPS 140 validated cryptographic modules for the computing elements that comprise their cloud service. Microsoft online services that include components, which have been FIPS 140-2 validated include, among others:

- Azure and Azure Government
- Dynamics 365 and Dynamics 365 Government
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense
- Federal Information Processing Standard (FIPS) 140
- Attestation documents – FIPS

Microsoft Information Protection

Microsoft Information Protection (MIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content. Labels help identify CUI to ensure the right level of control can be enforced. Microsoft Information Protection is compliant with FIPS 140-2 when your tenant key size is 2048 bits, which is the default when the Azure Rights Management service is

activated. MIP is part of the Microsoft Information Protection (MIP) solution, and extends the labeling and classification functionality provided by Microsoft 365.

By default, built-in labeling is turned off in these apps when the Microsoft Information Protection client is installed. For more information, including how to change this default behavior, see Office built-in labeling client and the Microsoft Information Protection client.

Even when you use built-in labeling in Office apps, you can also use the Microsoft Information Protection unified labeling client with sensitivity labels for the following:

- A scanner to discover sensitive information that is stored on-premises, and then optionally, label that content
- Right-click options in File Explorer for users to apply labels to all file types
- A viewer to display encrypted files for text, images, or PDF documents
- A PowerShell module to discover sensitive information in files on premises and apply or remove labels and encryption from these files.

If you are new to Microsoft Information Protection, or if you are an existing Microsoft Information Protection customer who has recently migrated your labels, see Choose your Windows labeling solution from the Microsoft Information Protection documentation. For more information about the cryptographic controls, see Cryptographic controls used by Azure RMS: Algorithms and key length.

Windows provides the security policy setting, *System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing*. This setting is used by some Microsoft products to determine whether to run in FIPS mode. When this policy is turned on, the validated cryptographic modules in Windows will also operate in FIPS mode. This policy may be set using Local Security Policy, as part of Group Policy, or through a Modern Device Management (MDM) solution. For more information on the policy, see System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing.

Through the Microsoft Security Development Lifecycle (SDL), all Azure services use FIPS 140-2 approved algorithms for data security because the operating system uses FIPS 140-2 approved algorithms while operating at a hyper scale cloud. Moreover, Azure

customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM).

Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and Microsoft processes your keys in FIPS validated HSMs (hardware and firmware) - FIPS 140-2 Level 2 for vaults and FIPS 140-2 Level 3 for HSM pools. With Key Vault, Microsoft does not see or extract your keys. Monitor and audit your key use with Azure logging—pipe logs into Azure HDInsight or your security information and event management (SIEM) solution for more analysis and threat detection.

Additional Resources

- FIPS 140-2 Validation
- FIPS PUB 140-2
- Microsoft Windows FIPS 140 Validation

SC.L2-3.13.12

Control Summary Information	
NIST 800-53 Mapping: SC-15	
Control : Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager	Microsoft Defender for Endpoint Teams Windows Hello for Business Azure Active Directory

Implementation Statement:

Intune/Active Directory/Windows Hello

Remote activation of collaborative computing devices can be restricted by enforcing authentication mechanisms such as, Windows Hello for Business, Intune/Microsoft Endpoint Manager and Azure Active Directory. Windows Hello for Business Windows stores biometric data that is used to implement Windows Hello securely on the local device only. The biometric data does not roam and is never sent to external devices or servers. Configure Windows Hello for Business is by Group Policy or Intune/Microsoft Endpoint Manager policy. Because Windows Hello only stores biometric identification data on the device, there is no single collection point an attacker can compromise to steal biometric data. For more information about biometric authentication with Windows Hello for Business, see Windows Hello biometrics in the enterprise.

Azure Portal

Users can view connected devices such as laptops and phones from the devices page in their account.

Teams

As a Teams administrator you can disable video. Teams allows the organizer and presenters to disable mic or camera of all the attendees, or of individuals, at any time during the meeting. By default, Teams provides indication when your camera or mic is in use. Users can control the use of their camera and mic in Teams as long as administrators have not restricted the devices.

Customer Responsibility

- Prohibiting remote activation for any collaborative computing devices within or controlled from customer-deployed resources and defining exceptions where remote activation is allowed (if any).

SC.L2-3.13.13

Control Summary Information	
NIST 800-53 Mapping: SC-18	
Control : Control and monitor the use of mobile code.	
Primary Services	**Secondary Services**
Azure Web Application Firewall Microsoft Sentinel	Azure Virtual Machines Intune/Microsoft Endpoint Manager Conditional Access GitHub Advanced Security (Add-On) Microsoft Defender for Endpoint

Implementation Statement:

Manage and control Mobile code that can run on multiple systems such as customer-developed mobile code, Java, Flash, ActiveX, PDF, Shockwave, Postscript, VBScripts via policies to allow only trusted sites. One option is to block the execution of mobile code in the browser but grant the user the liberty to allow mobile code to run. This can be accomplished via group policy settings. Granting users, the ability to allow mobile code does expose them to more threats however training users on mobile code threats can help reduce this risk. If you have plenty of IT staff, then only allowing mobile code when there is a business need is the best approach. This should be done in line with your change control procedures.

Microsoft Defender

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention.

Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. The solution can remediate threats such as malicious code as it scans for vulnerabilities. See code samples to enable and configure Microsoft Antimalware for

Azure Resource Manager (ARM) virtual machines. Learn more about Microsoft Antimalware.

Intune and Microsoft Defender for Endpoint

Intune can integrate data from a Mobile Threat Defense (MTD) vendor as an information source for device compliance policies and device Conditional Access rules. You can use this information to help protect corporate resources like Exchange and SharePoint, by blocking access from compromised mobile devices. Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune**.** You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Additionally, turn tamper protection on (or off) for all or part of your organization using Intune Fine-tune tamper protection settings in your organization. Manage tamper protection for your organization using Intune. Bad actors like to disable your security features to get easier access to your data, to install malware, or to otherwise exploit your data, identity, and devices. Tamper protection helps prevent these kinds of things from occurring.

With tamper protection, malicious apps are prevented from taking actions such as:

- Disabling virus and threat protection
- Disabling real-time protection
- Turning off behavior monitoring
- Disabling antivirus (such as IOfficeAntivirus (IOAV))
- Disabling cloud-delivered protection
- Removing security intelligence updates

Azure Web Application Firewall

Help protect your web apps from malicious attacks and common web vulnerabilities, such as SQL injection and cross-site scripting. Configure and enable Azure Web Application Firewall on your web application. Then, centrally define your rules and reuse them across all the web apps that you need to protect. Learn how to customize web application firewall rules in the Azure portal.

GitHub Advanced Security (Add-On)

A GitHub Advanced Security license provides the following additional features:

• Code scanning - Search for potential security vulnerabilities and coding errors in your code. For more information, see "About code scanning."
• Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. For more information, see "About secret scanning."
• Dependency review - Show the full impact of changes to dependencies and see details of any vulnerable versions before you merge a pull request. For more information, see "About dependency review."

Customer Responsibility

- The customer is responsible for defining acceptable and unacceptable mobile code technologies.
- The customer is responsible for establishing usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
- The customer is responsible for establishing usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

SC.L2-3.13.14

Control Summary Information	
NIST 800-53 Mapping: SC-19	
Control : Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	
Primary Services	**Secondary Services**
Teams Microsoft Sentinel	Microsoft Defender for IoT Intune/Microsoft Endpoint Manager Conditional Access Azure Active Directory

Implementation Statement:

To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application. When a user of your application calls another user of your application over an internet or data connection for example via Teams, the call is made over Voice Over IP (VoIP). In this case, both signaling and media flow over the internet. You can configure and monitor usage in Teams, to learn more, see understand calling in Microsoft Teams.

Microsoft Defender for IoT and Sentinel

This monitoring encompasses all IoT devices, including VoIP technologies. Controls are enabled through integration with other services. Proactively address vulnerabilities in your IoT/OT environment, Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your assets.

Further, you can get a bird's-eye view across IT/OT boundaries with interoperability with Microsoft Sentinel, cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with Microsoft Defender for Cloud Apps, and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud.

Sentinel now has an integrated connector for collecting Office 365 logs such as Teams. Teams serves a central role in communication and data-sharing in the Microsoft 365 Cloud. Since Teams touches on so many technologies in the Cloud, it can benefit from human and automated analysis. This applies to both hunting in logs, and real-time monitoring of meetings. Microsoft Sentinel offers admins these solutions. For more information, see Connect Office 365 Logs to Microsoft Sentinel.

Combining queries from resources like Azure Active Directory (Azure AD), or other Office 365 workloads can be used with Teams queries. For example, combine the detection of suspicious patterns in Azure AD SigninLogs, and use that output while

hunting for Team Owners. Also, you can make the SigninLogs detections specific to Teams by adding a filter for only Teams-based logons. For more information, see Expanding your threat hunting opportunities.

Intune/Microsoft Endpoint Manager

Not only can you control Microsoft native resources, but you can also control access to resources with VoIP capabilities for third party applications such as ZOOM using Intune Mobile Device Management. System administrators can use a mobile device Management (MDM) to remotely configure the Zoom app on managed devices such as iOS devices and Android. For more information, see Using Intune to Configure Zoom on iOS and Android.

Additionally, you can further control access to ZOOM by connecting Zoom with Azure to use your company's Azure credentials to login to your Zoom account via Single Sign-On (SSO). You can assign users Zoom licenses based on their group in Azure. For more information, see Configuring Zoom with Azure.

Customer Responsibility

- Authorizing, monitoring, and controlling the use of Voice over internet Protocol (VoiP) technologies within customer-deployed resources.

Additional Resources

- Quickstart: Add voice calling to your app
- Mass deployment with preconfigured settings for Windows

SC.L2-3.13.15

Control Summary Information	
NIST 800-53 Mapping: SC-23	
Control : Protect the authenticity of communications sessions.	
Primary Services	**Secondary Services**
Azure Active Directory	Azure ExpressRoute Azure Key Vault

Control Summary Information	
	Load Balancer Network Security Groups Azure Virtual Machines Virtual Network VPN Gateway Microsoft Information Protection Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Azure AD Multi-Factor Authentication Teams

Implementation Statement:

Azure Portal

Microsoft Azure Government provides the same ways to build applications and manage identities as Azure commercial. Azure Government customers may already have an Azure Active Directory (Azure AD) Public tenant or may create a tenant in Azure AD Government. Integrating Applications with Azure Active Directory shows how you can use Azure AD to provide secure sign-in and authorization to your applications. This process is the same for Azure Public and Azure Government once you choose your identity authority.

Key Vault

Authentication with Key Vault works in conjunction with Azure Active Directory (Azure AD), which is responsible for authenticating the identity of any given security principal**.** By default, Key Vault allows access to resources through public IP addresses. For greater security, you can also restrict access to specific IP ranges, service endpoints, virtual networks, or private endpoints. For more information, see Access Azure Key Vault behind a firewall.

Azure ExpressRoute

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With Azure

ExpressRoute , you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365. Azure ExpressRoute connections do not go over the public Internet. This allows Azure ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using Azure ExpressRoute , see Azure ExpressRoute connectivity models.

Azure Virtual Machines

Improve the security of Windows virtual machines (VMs) in Azure by integrating with Azure Active Directory (AD) authentication. You can use Azure AD as a core authentication platform to RDP into your VM. To use Azure AD login in for Windows VM in Azure, you need to first enable Azure AD login option for your Windows VM and then you need to configure Azure role assignments for users who are authorized to login in to the VM. You can centrally control and enforce Azure RBAC and Conditional Access policies that allow or deny access to the VMs.

MFA

Users and groups can be enabled for Azure AD Multi-Factor Authentication to prompt for additional verification during the sign-in event. Security defaults are available for all Azure AD tenants to quickly enable the use of the Microsoft Authenticator app for all users.

For more granular controls, Conditional Access policies can be used to define events or applications that require MFA. These policies can allow regular sign-in events when the user is on the corporate network or a registered device, but prompt for additional verification factors when remote or on a personal device.

Additionally, as an administrator in Exchange Server, you can enable Secure/Multipurpose Internet Mail Extensions (S/MIME) for your organization. S/MIME is a widely accepted method (more precisely, a protocol) for sending digitally signed and encrypted messages. S/MIME allows you to encrypt emails and digitally sign them. When you use S/MIME, it helps the people who receive the message by:

- Ensuring that the message in their inbox is the exact message that started with the sender.

- Ensuring that the message came from the specific sender and not from someone pretending to be the sender.

To do this, S/MIME provides for cryptographic security services such as authentication, message integrity, and non-repudiation of origin (using digital signatures). S/MIME also helps enhance privacy and data security (using encryption) for electronic messaging.

S/MIME requires a certificate and publishing infrastructure that is often used in business-to-business and business-to-consumer situations. The user controls the cryptographic keys in S/MIME and can choose whether to use them for each message they send. Email programs such as Outlook search a trusted root certificate authority location to perform digital signing and verification of the signature.

For a more complete background about the history and architecture of S/MIME in the context of email, see Understanding S/MIME.

Teams

Network communications in Teams are encrypted by default. By requiring all servers to use certificates and by using OAUTH, Transport Layer Security (TLS), and Secure Real-Time Transport Protocol (SRTP), all Teams data is protected on the network.

Customer Responsibility

- Protecting the authenticity of communications sessions involving customer-deployed resources.

Additional Resources

- Public Key Infrastructure
- How it works: Azure AD Multi-Factor Authentication
- Azure network security overview
- Message Encryption

SC.L2-3.13.16

Control Summary Information	
NIST 800-53 Mapping: SC-28	
Control : Protect the confidentiality of CUI at rest.	
Primary Services	**Secondary Services**
Azure Key Vault Bitlocker	Log Analytics Workspace Microsoft Sentinel Azure Virtual Machines Microsoft Information Protection Intune/Microsoft Endpoint Manager Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Defender for Office 365 Distributed Key Manager Customer Key

Implementation Statement:

Azure Key Vault

The storage location of the encryption keys and access control to those keys is central to an encryption at rest model. The keys need to be highly secured but manageable by specified users and available to specific services. For Azure services, Azure Key Vault is the recommended key storage solution and provides a common management experience across services. Keys are stored and managed in key vaults, and access to a key vault can be given to users or services. Azure Key Vault supports customer creation of keys or import of customer keys for use in customer-managed encryption key scenarios. Permissions to use the keys stored in Azure Key Vault, either to manage or to access them for Encryption at Rest encryption and decryption, can be given to Azure Active Directory accounts.

Software as a Service (SaaS) customers typically have encryption at rest enabled or available in each service. Microsoft 365 has several options for customers to verify or enable encryption at rest. For information about Microsoft 365 services, see Encryption in Microsoft 365.

Platform as a Service (PaaS) customer's data typically resides in a storage service such as Blob Storage but may also be cached or stored in the application execution environment, such as a virtual machine. To see the encryption at rest options available to you, examine the Data encryption models: supporting services table for the storage and application platforms that you use.

Like PaaS, IaaS solutions can leverage other Azure services that store data encrypted at rest. In these cases, you can enable the Encryption at Rest support as provided by each consumed Azure service. The Data encryption models: supporting services table enumerates the major storage, services, and application platforms and the model of Encryption at Rest supported.

Any customer using Azure Infrastructure as a Service (IaaS) features can achieve encryption at rest for their IaaS VMs and disks through Azure Disk Encryption. For more information on Azure Disk encryption, see the Azure Disk Encryption documentation. Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the BitLocker feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.

BitLocker, Customer Key and Distributed Key Manager (DKM)

Microsoft 365 provides baseline, volume-level encryption enabled through BitLocker and Distributed Key Manager (DKM). Microsoft 365 offers an added layer of encryption for your content. This content includes data from Exchange Online, Skype for Business, SharePoint Online, OneDrive for Business, and Microsoft Teams.

Customer Key provides extra protection against viewing of data by unauthorized systems or personnel, and complements BitLocker disk encryption in Microsoft data centers. Service encryption is not meant to prevent Microsoft personnel from accessing your data. Instead, Customer Key helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on. Customer Key is built on service

encryption and lets you provide and control encryption keys. Microsoft 365 then uses these keys to encrypt your data at rest.

Intune/Microsoft Endpoint Manager

Use Intune to configure encryption at rest using BitLocker Drive Encryption on devices that run Windows 10. Some settings for BitLocker require the device have a supported TPM. To manage BitLocker in Intune, your account must have the applicable Intune role-based access control (RBAC) permissions. For more information on how to enforce BitLocker encryption using Intune, see Create and deploy policy.

Intune can also manage macOS FileVault disk encryption. FileVault is a whole-disk encryption program that is included with macOS. You can use Intune to configure FileVault on devices that run macOS 10.13 or later**.** For more information on how to enforce FileVault encryption using Intune, see Create device configuration policy for FileVault

Additionally, Intune/Microsoft Endpoint Manager integrates with Network Access Control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Transparent Data Encryption (TDE)

You can use Transparent Data Encryption (TDE) to encrypt SQL Server and Azure SQL Database data files at rest. With TDE you can encrypt the sensitive data in the database and protect the keys that are used to encrypt the data with a certificate. TDE performs real-time I/O encryption and decryption of the data and log files to protect data at rest. TDE can assist in the ability to comply with many laws, regulations, and guidelines established in various industries. If a malicious party would be able to steal your data files, they still would not be able to use them at all because they would need the keys as well. For more information about TDE, see Transparent Data Encryption (TDE).

Azure Policies

- **SC.L2-3.13.16 Azure Policies**

Customer Responsibility

- Protecting customer-controlled information at rest.

Additional Resources

- Encryption in Azure Backup
- Federal Information Processing Standard (FIPS) 140

System and Information Integrity (SI)

SI.L2-3.14.1

Control Summary Information	
NIST 800-53 Mapping: SI-2,SI-3,SI-5	
Control : Identify, report and correct information and information system flaws in a timely manner.	
Primary Services	**Secondary Services**
Microsoft Sentinel	Intune/Microsoft Endpoint Manager Microsoft Defender for Endpoint Microsoft Defender for Cloud Power Automate

Implementation Statement:
Microsoft Sentinel

You can use Microsoft Intune, Microsoft Endpoint Configuration Manager, the Update Compliance add-in for Microsoft Operations Management Suite, or Microsoft Sentinel SIEM (by consuming Windows event logs) to monitor protection status and create reports about endpoint protection.

Review usage reports for Azure Active Directory in the Azure portal to determine suspicious activity, including the possibly of infected devices report. Configure Microsoft Defender for Endpoint to report on Microsoft Defender Antivirus events and connect your resources such as the Microsoft Defender for Endpoint connector to Microsoft Sentinel SIEM tool to have a centralized location for security alerts and advisories. Connect data sources to visualize and monitor your data in Sentinel.

Additionally, you can use the Microsoft Defender for Cloud Apps alert connector to ingest Microsoft Defender for Cloud Apps alerts from Microsoft Defender for Cloud Apps and stream them into Microsoft Sentinel. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

The vulnerability scanner included with Microsoft Defender for Cloud is powered by Qualys. Qualys' scanner is one of the leading tools for real-time identification of vulnerabilities. It is only available with Microsoft Defender for Cloud. You do not need a Qualys license or even a Qualys account - everything is handled seamlessly inside Security Center. Moreover, the systems can also be onboarded to Microsoft Defender for Endpoint to gain similar Threat & Vulnerability Management visibility.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides endpoint protection, detection and response, vulnerability managements and mobile threat defense. Vulnerability management allows you to quickly discover, prioritize, and remediate vulnerabilities and misconfigurations. To support this CMMC Control , consider the following Microsoft Defender for Endpoint configurations:

- Enable cloud-delivered protection. You can enable cloud-delivered protection with Microsoft Endpoint Configuration Manager, Group Policy, Microsoft Intune, and PowerShell cmdlets.
- Specify the cloud-delivered protection level. You can specify the level of protection offered by the cloud with Group Policy and Microsoft Endpoint Configuration Manager. The protection level will affect the amount of information shared with the cloud and how aggressively new files are blocked.
- Configure and validate network connections for Microsoft Defender Antivirus. There are certain Microsoft URLs that your network and endpoints must be able to connect to for cloud-delivered protection to work effectively. This article lists the URLs that should be allowed via firewall or network filtering rules, and instructions for confirming your network is properly enrolled in cloud-delivered protection.
- Configure the block at first sight feature. The "block at first sight" feature can block new malware within seconds, without having to wait hours for traditional Security intelligence. You can enable and configure it with Microsoft Endpoint Manager and Group Policy.
- Configure the cloud block timeout period. Microsoft Defender Antivirus can block suspicious files from running while it queries our cloud-delivered protection

service. You can configure the amount of time the file will be prevented from running with Microsoft Endpoint Manager and Group Policy.

Power Automate

Environment admins can access analytics for Power Automate in the Microsoft Power Platform admin center. The reports provide insights into runs, usage, errors, types of flows created, shared flows, and details on connectors associated with all the different flow types like automated flows, button flows, scheduled flows, approval flows, business process flows.

Azure Policies

- **SC.L2-3.14.1 Azure Policies**

Customer Responsibility

- Flaw remediation on customer-deployed resources, including the identification, reporting, and correction of flaws.

Additional Resources

- Manage updates for mobile devices and virtual machines (VMs)
- Create interactive reports with Azure Monitor Workbooks.

SI.L2-3.14.2

Control Summary Information	
NIST 800-53 Mapping: SI-2,SI-3,SI-5	
Control : Provide protection from malicious code at appropriate locations within organizational information systems.	
Primary Services	**Secondary Services**
Azure Web Application Firewall App Locker	Azure DNS Azure Virtual Machines Microsoft Defender for Office 365 Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Intune/Microsoft Endpoint Manager

Implementation Statement:

Microsoft Antimalware for Azure and Microsoft Defender for Cloud Apps

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention.

Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. The solution can remediate threats such as malicious code as it scans for vulnerabilities. See code samples to enable and configure Microsoft Antimalware for Azure Resource Manager (ARM) virtual machines. Learn more about Microsoft Antimalware.

Additionally, Microsoft Defender for Cloud Apps monitors the status of antimalware protection and reports this under the Endpoint protection issues blade. Security Center highlights issues, such as detected threats and insufficient protection, which can make your virtual machines (VMs) and computers vulnerable to antimalware threats. By using the information under Endpoint protection issues, you can identify a plan to address any

issues identified. To learn more about the features of Microsoft Defender for Cloud Apps, see Feature coverage for machines.

Intune and Microsoft Defender for Endpoint

Intune can integrate data from a Mobile Threat Defense (MTD) vendor as an information source for device compliance policies and device Conditional Access rules. You can use this information to help protect corporate resources like Exchange and SharePoint, by blocking access from compromised mobile devices. Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune. You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Microsoft Defender for Endpoint works with devices that run Android, iOS/iPadOS and Windows 10 or later. When you integrate Intune with Microsoft Defender for Endpoint, you can take advantage of Microsoft Defender for Endpoints Threat & Vulnerability Management (TVM) and use Intune to remediate endpoint weakness identified by TVM. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Additionally, turn tamper protection on (or off) for all or part of your organization using Intune Fine-tune tamper protection settings in your organization. Manage tamper protection for your organization using Intune. Bad actors like to disable your security features to get easier access to your data, to install malware, or to otherwise exploit your data, identity, and devices. Tamper protection helps prevent these kinds of things from occurring.

With tamper protection, malicious apps are prevented from taking actions such as:

- Disabling virus and threat protection
- Disabling real-time protection
- Turning off behavior monitoring
- Disabling antivirus (such as IOfficeAntivirus (IOAV))
- Disabling cloud-delivered protection
- Removing security intelligence updates

Azure Web Application Firewall

Help protect your web apps from malicious attacks and common web vulnerabilities, such as SQL injection and cross-site scripting. Configure and enable Azure Web Application Firewall on your web application. Then, centrally define your rules and reuse

them across all the web apps that you need to protect. Learn how to customize web application firewall rules in the Azure portal.

App Locker

When a user runs a process, that process has the same level of access to data that the user has. As a result, sensitive information could easily be deleted or transmitted out of the organization if a user knowingly or unknowingly runs malicious software. AppLocker can help mitigate these types of security breaches by restricting the files that users or groups are allowed to run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers

Azure Policies

- **SC.L2-3.14.2 Azure Policies**

Customer Responsibility

- Protecting customer-deployed resources against malicious code by using code protection mechanisms at entry and exit points to detect and eradicate malicious code (e.g., viruses, malware, rootkits, worms, and scripts).

Additional Resources

- Endpoint protection assessment and recommendations in Microsoft Defender for Cloud Apps
- Enable and configure Microsoft Antimalware for Azure Resource Manager VMs

SI.L2-3.14.3

Control Summary Information	
NIST 800-53 Mapping: SI-2, SI-3, SI-5	
Control : Monitor system security alerts and advisories and take action in response.	
Primary Services	**Secondary Services**
Microsoft Sentinel Azure Active Directory Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Microsoft Defender for Cloud Microsoft 365 Defender Microsoft Defender for IoT	

Implementation Statement:

Defender

Microsoft Defender for Endpoint provides endpoint protection, detection and response, vulnerability management and mobile threat defense. It identifies and can report on advisories specific to each device monitored. You can use Microsoft Endpoint Manager to monitor Microsoft Defender Antivirus or create email alerts. Or you can monitor protection using Microsoft Intune. Vulnerability management allows you to quickly discover, prioritize, and remediate vulnerabilities and misconfigurations.

Microsoft Defender for IoT is a unified security solution for identifying IoT/OT devices, vulnerabilities, and threats. It identifies and can report on advisories specific to each device monitored. Go to Microsoft Defender for Cloud to turn on protection for your hybrid cloud workloads.

Microsoft Sentinel connector can stream security alerts from Microsoft Defender for Cloud Apps into Microsoft Sentinel. Learn more about connecting Microsoft Defender for Cloud Apps with Microsoft Sentinel. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Review usage reports for Azure Active Directory in the Azure portal to determine suspicious activity, including the possibly of infected devices report. Configure Microsoft Defender for Endpoint to report on Microsoft Defender Antivirus events and connect your resources such as the Microsoft Defender for Endpoint connector to Microsoft

Sentinel SIEM tool to have a centralized location for security alerts and advisories. Connect data sources to visualize and monitor your data in Sentinel.

Additionally, Microsoft Sentinel allows you to import threat indicators to enhance your organization's ability to detect and respond to known threats. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Customer Responsibility

- Receiving security alerts, advisories, and directives from customer-defined external organizations on an ongoing basis.

Additional Resources

- The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.
- Alerts and Sensor Reporting
- Connect your data from Defender for IoT to Microsoft Sentinel

SI.L2-3.14.4

Control Summary Information	
NIST 800-53 Mapping: SI-3	
Control : Update malicious code protection mechanisms when new releases are available.	
Primary Services	**Secondary Services**
Microsoft Defender for Endpoint Microsoft Defender for Office 365 Microsoft Defender for Cloud Apps Microsoft Defender Antivirus cloud protection Microsoft Defender for Cloud Microsoft 365 Defender Azure Automation	Intune/Microsoft Endpoint Manager Azure Virtual Machines

Implementation Statement:

Azure Automation

You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines in Azure, physical or VMs in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management.

Microsoft Defender/Microsoft Antimalware

Keeping Microsoft Defender Antivirus up to date is critical to assure your devices have the latest technology and features needed to protect against new malware and attack techniques. Make sure to update your antivirus protection even if Microsoft Defender Antivirus is running in passive mode. To see the most current engine, platform, and signature date, visit the Security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware.

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. Microsoft Antimalware automatically updates malicious code signatures and includes the features below. When you deploy

and enable Microsoft Antimalware for Azure for your applications, the following core features are available:

- **Real-time protection**: monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution.
- **Scheduled scanning**: Scans periodically to detect malware, including actively running programs.
- Malware remediation – automatically acts on detected malware, such as deleting or quarantining malicious files and cleaning up malicious registry entries.
- **Signature updates**: automatically installs the latest protection signatures (virus definitions) to ensure protection is up to date on a pre-determined frequency.
- **Antimalware Engine updates**: automatically updates the Microsoft Antimalware engine.
- **Antimalware Platform updates**: automatically updates the Microsoft Antimalware platform.
- **Active protection**: reports telemetry metadata about detected threats and suspicious resources to Microsoft Azure to ensure rapid response to the evolving threat landscape, as well as enabling real-time synchronous signature delivery through the Microsoft Active Protection System (MAPS).
- **Samples reporting**: provides and reports samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting.
- **Exclusions**: allows application and service administrators to configure exclusions for files, processes, and drives.
- **Antimalware event collection**: records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log and collects them into the customer's Azure Storage account.

You can find information on default configuration settings and more here: Microsoft Antimalware for Azure Cloud Services and Virtual Machines.

Intune/Microsoft Endpoint Manager

If you use an unsupported version of Window 10, your users will not get the latest security updates, new features, bug fixes, latency improvements, accessibility improvements, and performance investments. The user will not be able to be co-managed with System Center Configuration Manager and Intune. Intune follows Windows 10 lifecycle for supported Windows 10 versions. In the Microsoft Endpoint

Manager admin center, use the Discovered apps feature to find apps with these versions. On a user's device, the Company Portal version is shown in the **settings** page of the company portal. Update to a supported Windows/Company Portal version.

Learn what is new each week in Microsoft Intune in Microsoft Endpoint Manager admin center. You can also find important notices, past releases, and information about how Intune service updates are released.

Turn tamper protection on (or off) for all or part of your organization using Intune Fine-tune tamper protection settings in your organization. Manage tamper protection for your organization using Intune. Bad actors like to disable your security features to get easier access to your data, to install malware, or to otherwise exploit your data, identity, and devices. Tamper protection helps prevent these kinds of things from occurring.

With tamper protection, malicious apps are prevented from taking actions such as:

- Disabling virus and threat protection
- Disabling real-time protection
- Turning off behavior monitoring
- Disabling antivirus (such as IOfficeAntivirus (IOAV))
- Disabling cloud-delivered protection
- Removing security intelligence updates

Azure Virtual Machines

Software updates in Azure Automation Update Management provides a set of tools and resources that can help manage the complex task of tracking and applying software updates to machines in Azure and hybrid cloud. An effective software update management process is necessary to maintain operational efficiency, overcome security issues, and reduce the risks of increased cyber security threats. Update Management supports the deployment of first-party updates and the pre-downloading of them. This support requires changes on the systems being updated. See Configure Windows Update settings for Azure Automation Update Management to learn how to configure these settings on your systems.

Before attempting to manage updates for your VMs, ensure that you have enabled Update Management on them using one of these methods:

- Enable Update Management from an Automation account
- Enable Update Management by browsing the Azure portal
- Enable Update Management from a runbook
- Enable Update Management from an Azure VM

Customer Responsibility

- Updating malicious code protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures

Additional Resources

- Expedite Windows 10 quality updates in Microsoft Intune

SI.L2-3.14.5

Control Summary Information	
NIST 800-53 Mapping:SI-3	
Control : Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.	
Primary Services	**Secondary Services**
Microsoft Defender for Endpoint Microsoft Defender for Office 365 Microsoft Defender SmartScreen Microsoft Defender for Cloud Apps Microsoft Defender Antivirus cloud protection	Intune/Microsoft Endpoint Manager

Implementation Statement:
Microsoft Defender/Microsoft Antimalware

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious

or unwanted software tries to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention. Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. The solution can remediate threats such as malicious code as it scans for vulnerabilities. See code samples to enable and configure Microsoft Antimalware for Azure Resource Manager (ARM) virtual machines. Learn more about Microsoft Antimalware.

Enable and configure Microsoft Defender Antivirus always-on protection in Group Policy. Always-on protection consists of real-time protection, behavior monitoring, and heuristics to identify malware based on known suspicious and malicious activities. The feature allows you to scan all downloaded files and attachments automatically. Downloaded files and attachments are automatically scanned. This operates in addition to the Windows Defender SmartScreen filter, which scans files before and during downloading.

Windows Defender SmartScreen

When you use the new Microsoft Edge , Microsoft Defender SmartScreen helps you identify reported phishing and malware websites and also helps you make informed decisions about downloads. SmartScreen helps protect you in three ways:

- As you browse the web, it analyzes pages and determines if they might be suspicious. If it finds suspicious pages, SmartScreen will display a warning page, giving you an opportunity to provide feedback and advising you to continue with caution.
- SmartScreen checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen will show you a warning letting you know that the site has been blocked for your safety.
- SmartScreen checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen will warn you that the download has been blocked for your safety. SmartScreen also checks the files that you download against a list of files that are well known and downloaded by many people who use Internet Explorer. If the file that you're downloading isn't on that list, SmartScreen will warn you.

Intune/Microsoft Endpoint Manager

Use the Endpoint security node in Intune to configure device security and to manage security tasks for devices when those devices are at risk. The Endpoint security policies are designed to help you focus on the security of your devices and mitigate risk. The available tasks can help you identify at-risk devices, to remediate those devices, and restore them to a compliant or more secure state. Deploy security baselines that establish best practice security configurations for devices. Intune includes security baselines for Windows devices and a growing list of applications, like Microsoft Defender for Endpoint and Microsoft Edge. Security baselines are pre-configured groups of Windows settings that help you apply a configuration that is recommended by the relevant security teams recommend.

Intune allows you to perform a Quick Scan – This will have Defender run a quick scan of the device for malware and then submit the results to Intune. A quick scan looks at common locations where there could be malware registered, such as registry keys and known Windows startup folders.

Additionally, you can run a Full scan – Having Defender run a scan of the device for malware and then submit the results to Intune. A full scan looks at common locations where there could be malware registered, and also scans every file and folder on the device.

Customer Responsibility

- Protecting customer-deployed resources against malicious code by configuring mechanisms to: perform periodic scans at a customer-defined frequency and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; block malicious code, quarantine malicious code, and/or send an alert to an administrator; and take any customer-defined action(s) in response to malicious code detection.

SI.L2-3.14.6

Control Summary Information	
NIST 800-53 Mapping: AU-2, AU-2(3), AU-6, SI-4, SI-4(4)	
Control : Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	
Primary Services	**Secondary Services**
Azure Firewall Microsoft Sentinel Microsoft Defender for IoT Microsoft Defender for Identity	Azure DNS Azure Key Vault Network Security Groups Azure Web Application Firewall Virtual Network Conditional Access Microsoft Defender for Endpoint Microsoft Defender for Office 365 Microsoft Defender for Cloud Apps

Implementation Statement:

Microsoft Defender for IoT

Control what traffic is being monitored using Microsoft Defender for IoT sensors. Sensors automatically perform deep packet detection for IT and OT traffic and resolve information about network devices, such as device attributes and behavior. You onboard a sensor by registering it with Microsoft Defender for IoT and downloading a sensor activation file. Learn more on how to Onboard, view, and manage sensors in the Defender for IoT portal. Learning and Smart IT Learning modes instructs your sensor to learn your network's usual activity. This activity becomes your baseline.

When Smart IT Learning is enabled, the sensor tracks network traffic that generates nondeterministic IT behavior based on specific alert scenarios. Working with Smart IT Learning helps you reduce the number of unnecessary alerts and notifications caused by noisy IT scenarios. Microsoft recommends to enable all security detection engines. Self-

learning analytics engines eliminate the need for updating signatures or defining rules. The engines use ICS-specific behavioral analytics and data science to continuously analyze OT network traffic for anomalies, malware, operational problems, protocol violations, and baseline network activity deviations.

Additionally, to enhance device enrichment, you can configure multiple DNS servers to carryout reverse lookups. You can resolve host names or FQDNs associated with the IP addresses detected in network subnets. For example, if a sensor discovers an IP address, it might query multiple DNS servers to resolve the host name.

Microsoft Defender for Identity

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) monitors your domain controllers by capturing and parsing network traffic and leveraging Windows events directly from your domain controllers, then analyzes the data for attacks and threats. Utilizing profiling, deterministic detection, machine learning, and behavioral algorithms Defender for Identity learns about your network, enables detection of anomalies, and warns you of suspicious activities. Installed directly on your domain controller or AD FS servers, the Defender for Identity sensor accesses the event logs it requires directly from the servers. After the logs and network traffic are parsed by the sensor, Defender for Identity sends only the parsed information to the Defender for Identity cloud service (only a percentage of the logs are sent). To learn more, see Microsoft Defender for Identity Architecture.

Microsoft Defender for Cloud Apps

Integrating Cloud App Security with Microsoft Defender for Endpoint gives you the ability to use Cloud Discovery beyond your corporate network or secure web gateways. With the combined user and device information, you can identify risky users or devices, see what apps they are using, and investigate further in the Defender for Endpoint portal. Cloud Discovery analyzes traffic logs collected by Defender for Endpoint and assesses identified apps against the cloud app catalog to provide compliance and security information. By configuring Cloud Discovery, you gain visibility into cloud use, Shadow IT, and continuous monitoring of the unsanctioned apps being used by your users. Set up Cloud Discovery.

Microsoft Sentinel

Connect your sources such as, Microsoft Defender for Endpoint to Sentinel for monitoring your organization. Enable Fusion technology based on machine learning, allowing Microsoft Sentinel to automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities that are observed at various stages of the kill-chain. Based on these discoveries, Microsoft Sentinel generates incidents that would otherwise be difficult to catch. fusion incidents can indicate

Customized for your environment, this detection technology not only reduces false positive rates but can also detect attacks with limited or missing information.

Virtual Network/Azure Firewall

To secure Azure application workloads, you use protective measures like authentication and encryption in the applications themselves. You can also add security layers to the virtual machine (VM) networks that host the applications, both to protect inbound flows from users, as well as outbound flows to the Internet that your application might require. This article describes Azure Virtual Network security services like Azure Firewall and Azure Application Gateway, when to use each service, and network design options that combine both.

Azure Firewall is a managed next-generation firewall that offers network address translation (NAT). Azure Firewall bases packet filtering on Internet Protocol (IP) addresses and Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ports, or on application-based HTTP(S) or SQL attributes. Azure Firewall also leverages Microsoft threat intelligence to identify malicious IP addresses. Azure Firewall Premium includes all functionality of Azure Firewall Standard plus additional features such as TLS-inspection and IDPS (Intrusion Detection and Protection System) For more information, see the Azure Firewall documentation.

Azure Application Gateway is a managed web traffic load balancer and HTTP(S) full reverse proxy that can do Secure Socket Layer (SSL) encryption and decryption. Application Gateway also uses Web Application Firewall to inspect web traffic and detect attacks at the HTTP layer. For more information, see the Application Gateway documentation.

Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway to provide inspection of HTTP request and prevent malicious attacks at the web layer such as SQL Injection or Cross-Site Scripting. For more information, see the Web Application Firewall documentation.

Azure Policies

- **SC.L2-3.14.6 Azure Policies**

Customer Responsibility

- Monitoring customer-deployed resources to detect attacks and indicators of potential attacks in accordance with customer-defined monitoring objectives; and unauthorized local, network, and remote connections.
- Monitoring customer-deployed resources, including the monitoring of inbound and outbound communications traffic at the customer-defined frequency, for unusual or unauthorized activities/conditions.

Additional Resources

- Best practices for configuring Windows Defender Firewall
- Checklist: Creating Outbound Firewall Rules.
- Checklist: Creating Inbound Firewall Rules.
- Isolating Microsoft Store Apps on Your Network
- Discover and manage shadow IT in your network

SI.L2-3.14.7

Control Summary Information	
NIST 800-53 Mapping: SI-4	
Control : Identify unauthorized use of organizational systems.	
Primary Services	**Secondary Services**
Microsoft Sentinel	Azure Bastion Load Balancer Network Security Groups Azure Virtual Machines VPN Gateway Privileged Identity Management (PIM) Microsoft Defender for Office 365 Azure Active Directory Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint Azure Firewall

Implementation Statement:

Microsoft Defender for Cloud Apps

Integrating Cloud App Security with Microsoft Defender for Endpoint gives you the ability to use Cloud Discovery beyond your corporate network or secure web gateways. With the combined user and device information, you can identify risky users or devices, see what apps they are using, and investigate further in the Defender for Endpoint portal. Cloud Discovery analyzes traffic logs collected by Defender for Endpoint and assesses identified apps against the cloud app catalog to provide compliance and security information. By configuring Cloud Discovery, you gain visibility into cloud use, Shadow IT, and continuous monitoring of the unsanctioned apps being used by your users. Set up Cloud Discovery.

Microsoft Sentinel

Connect your sources such as, Microsoft Defender for Endpoint to Sentinel for monitoring your organization. Enable Fusion technology based on machine learning, allowing Microsoft Sentinel to automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities that are observed at

various stages of the kill-chain. Based on these discoveries, Microsoft Sentinel generates incidents that would otherwise be difficult to catch. Customized for your environment, this detection technology not only reduces false positive rates but can also detect attacks with limited or missing information.

Virtual Network/Azure Firewall

To secure Azure application workloads, you use protective measures like authentication and encryption in the applications themselves. You can also add security layers to the virtual machine (VM) networks that host the applications, both to protect inbound flows from users, as well as outbound flows to the Internet that your application might require. This article describes Azure Virtual Network security services like Azure Firewall and Azure Application Gateway, when to use each service, and network design options that combine both.

Azure Firewall is a managed next-generation firewall that offers network address translation (NAT). Azure Firewall bases packet filtering on Internet Protocol (IP) addresses and Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ports, or on application-based HTTP(S) or SQL attributes. Azure Firewall also leverages Microsoft threat intelligence to identify malicious IP addresses. Azure Firewall Premium includes all functionality of Azure Firewall Standard plus additional features such as TLS-inspection and IDPS (Intrusion Detection and Protection System) For more information, see the Azure Firewall documentation.

Azure Application Gateway is a managed web traffic load balancer and HTTP(S) full reverse proxy that can do Secure Socket Layer (SSL) encryption and decryption. Application Gateway also uses Web Application Firewall to inspect web traffic and detect attacks at the HTTP layer. For more information, see the Application Gateway documentation.

Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway to provide inspection of HTTP request and prevent malicious attacks at the web layer such as SQL Injection or Cross-Site Scripting. For more information, see the Web Application Firewall documentation.

Additionally, Microsoft Defender for Cloud Apps Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. When a user requests access to a VM, Security Center checks that the user has Role-

Based Access Control (RBAC) permissions for that VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. For more information see, Secure your management ports with just-in-time access.

Customer Responsibility

- Monitoring customer-deployed resources to identify unauthorized use through customer-defined techniques and methods.

CMMC Blogs

- Accelerating CMMC compliance for Microsoft cloud
- Microsoft CMMC Acceleration Program Update
- Understanding Compliance Between Commercial, Government and DoD Offerings
- The Microsoft 365 Government (GCC High) Conundrum - DIB Data Enclave vs Going All In
- Microsoft expands qualification of contractors for Government cloud offerings
- Microsoft Sentinel Cybersecurity Maturity Model Certification (CMMC) Workbook
- CMMC on Azure DevBlogs
- CMMC on Tech Community

CMMC Resources

- CMMC FAQ's
- CMMC 2.0 Model
- CyberAssist CMMC Resources
- SECURING THE DEFENSE INDUSTRIAL BASE- CMMC 2.0
- CMMC Accreditation Body

CMMC Tools

- Microsoft Product Placemat for CMMC 2.0