Common Attacks and Microsoft Capabilities that Protect Your Organization

Microsoft

Type of attack	Begin attack	Enter	Traverse	Exfiltrate data

Identity based

Broad-based phishing campaigns
Attacker masquerades as a trusted entity, dupes employees into opening emails, texts or IMs.

Spear-phishing
Attacker uses information specifically about a user to construct a more plausible phishing attack.

Password spray
Attacker tries a large list of possible passwords for a given account or set of accounts.

Other similar attacks
Credential stuffing, leaked passwords.

Begin attack (Identity based)

An employee clicks on a link and enters their credentials

Exchange Online Protection protects against spam, malware and other email threats.

Microsoft 365 Defender: Microsoft Defender for Office 365 natively coordinates detection, prevention, investigation & response across endpoints, identities, email.

Microsoft Defender SmartScreen protects against phishing or Malware websites and applications, and downloading of potentially malicious files.

Weak passwords are systematically identified

Azure AD Identity Protection discovers leaked credential and detects password spray attacks.

Azure AD password protections enforces a minimum requirements for passwords, dynamically bans common passwords and force resets leaked passwords.

Azure AD Smart Lockout
Helps to lock out bad actors that guess your password or use brute-force method to get in.

Enter (Identity based)

Attacker uses stolen credentials to gain access to the user's mail and files.

Azure AD Multifactor Authentication (MFA) adds a layer of protection to the sign-in process.

Azure AD Conditional Access rules block access based on risky sign-in, unmanaged PC, and other criteria that you set.

Sign-in risk-based Conditional Access represents the probability that a given authentication request isn't authorized by the identity owner.

Microsoft 365 Defender: Microsoft Defender for Identity leverages on-premises AD signals to identify, detect and investigate advanced threats, compromised identities, and malicious insider actions.

Traverse (Identity based)

Attacker moves laterally, gaining access to cloud services and resources in the environment.

Identity: Azure AD conditional access rules block access from noncompliant devices and enforce multi factor authentication for access to cloud services.

Microsoft Cloud App Security detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Microsoft Information Protection helps discover, classify & protect sensitive information.

Insider Risk: Communication compliance helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization.

Insider Risk: Insider Risk Management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization.

Insider Risk: Information barriers allow you to restrict communication and collaboration between two internal groups to avoid a conflict of interest from occurring in your organization.

Insider Risk: Privileged access management allows granular access control over privileged Exchange Online admin tasks in Office 365. It can help protect your organization from breaches that use existing privileged admin accounts with standing access to sensitive data or access to critical configuration settings.

Securing Privileged Access Roadmap is guidance to mitigate lateral traversal and credential theft techniques for your on-premises and hybrid cloud environments.

Exfiltrate data (Identity based)

Attacker removes data from the environment.

Microsoft 365 Defender: Microsoft Cloud App Security detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Microsoft 365 Exchange Email flow rules prevents auto-forwarding of mail to external domain

Microsoft Information Protection (MIP) helps you discover, classify, and protect sensitive information wherever it lives or travels.

M365 Data Loss Prevention (DLP) rules prevent sensitive data from leaving the environment.

Endpoint data loss prevention extends monitoring and protection capabilities of DLP to sensitive items that are stored on Windows 10 devices.

Intune mobile device management rules prevent business data from leaving approved business apps on mobile devices.

Insider Risk Management helps minimize internal risks by enabling you to detect, investigate and act on malicious activities.

Azure Purview helps you manage and govern your on-premises, multi-cloud, and SaaS data with automated data classification, sensitive data classification, and end-to-end data lineage.

Azure Technologies provide encryption for discs and storage, SQL Encryption, and Key vault.

Azure Backup is a service you can use to back up and restore your data in the Microsoft cloud. This service includes capabilities to protect your backups from ransomware.

Azure Sentinel is a cloud-native security information and event manager (SIEM).

Microsoft Azure Confidential Ledger Protects data at rest, in-transit and in-use with hardware-backed secure enclaves.

SQL Database dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

SQL Threat Detection alerts on suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns.

Device based

Device compromise
Malware is installed on the device. This can include viruses, spyware, ransomware, and other unwanted software that installs without concent.

Lost or stolen device

Begin attack (Device based)

Malicious files and viruses are introduced into the environment

Microsoft 365 Defender: Microsoft Defender for Endpoint helps prevent, detect, investigate and respond to advanced threats.

Microsoft Defender Application Guard for Microsoft Edge helps isolate untrusted sites. You define the trusted web sites, cloud resources, and internal networks.

Possession is unknown

Microsoft Intune mobile device management (MDM) enforces password and/or pin requirements and wipes the device after a specific failed attempts.

Enter (Device based)

An employee clicks on a malicious link or opens a malicious file

Microsoft Defender Antivirus scans for malware, virus, and security threats.

Microsoft Defender Firewall helps secure the device by allowing you to create rules that determine which network traffic is permitted to enter.

Windows Defender SmartScreen checks to see if new apps lack reputation or are known to be malicious, and responds accordingly.

Attacker gains access into the device

Windows Hello for Business replaces username and password with strong two-factor authentication tied to a device.

Intune application protection with conditional launch controls protects data at application level, including custom apps and store apps.

Traverse (Device based)

Intune device compliance policies define criteria for healthy and compliant devices.

Microsoft 365 Defender: Microsoft Defender for Endpoint helps detect, investigate and respond to advanced attacks on your network.

Windows 10 Credential Guard prevents attackers from gaining access to other resources in the organization through Pass-the-Hash or Pass-the-Ticket attacks.

Network based

DDos
Attacks aim to overwhelm online services with more traffic to make the service inoperable.

Eavesdropping
An attacker intercepts network traffic and aims to obtain passwords, credit card numbers, and other confidential information.

Code and SQL injection
An attacker transmits malicious code instead of data values over a form or through an API.

Cross site scripting
An attacker uses third-party web resources to run scripts in the victim's web browser.

Begin attack (Network based)

Attacks are conducted using network traffic vulnerabilities

Azure DDoS Protection provides enhanced DDoS mitigation features to defend against DDoS attacks.

Azure Web Application Firewall provides web protection against common exploits and vulnerabilities.

Azure Defender stands up against RDP brute force attacks, SQL Injection.

Microsoft Azure Attestation verifies the identity and security posture of a platform before you interact with it.

Enter (Network based)

Attacker gains access to the network

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, and more.

Network Security Groups filter network traffic to and from Azure resources in an Azure virtual network. These contain 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.

Azure Firewall is a managed, cloud-based network security service that protects Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

Azure AD Multifactor Authentication (MFA) adds a layer of protection to the sign-in process.

Microsoft 365 Defender: Microsoft Defender for Endpoint discovers unmanaged devices on the network.

Traverse (Network based)

Microsoft 365 Defender: Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Azure AD Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization.

Azure Defender for IoT performs Continuous asset discovery, vulnerability management, and threat detection for IoT devices.

Azure Data Encryption-at-Rest provides data encryption for services across- SaaS, PaaS or IaaS.

Azure Identity Protection automates the detection and remediation of identity based risks.

Azure Key Vault
It enhances data protection and compliance with the help of secure key management to protect data in the cloud.

Extended detection and response (XDR)

Microsoft extended detection and response (XDR) solutions deliver intelligent, automated, and integrated security across domains.

This in turn help defenders connect seemingly disparate alerts and get ahead of attackers.

Microsoft 365 Defender

Microsoft 365 Defender delivers XDR capabilities for identities, endpoints, cloud apps, email and documents. Its built-in self-healing technology fully automates remediation more than 70% of the time.

It combines:
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Cloud App Security
- Azure AD Identity Protection

aka.ms/defender365eval

Azure Defender

Delivers XDR left capabilities to protect multi-cloud and hybrid workloads, including virtual machines, databases, containers, IoT, and more.

It combines:
- Azure Defender for Servers
- Azure Defender for IoT
- Azure Defender for SQL

Azure Sentinel

To gain visibility across your entire environment and include data from other security solutions such as firewalls and existing security tools, connect Microsoft Defender to Azure Sentinel, Microsoft's cloud-native SIEM.

Azure Sentinel is deeply integrated with Microsoft Defender so you can integrate your XDR data in only a few clicks and combine it with all your security data from across your entire enterprise.

Top resources

Microsoft Security documentation
Technical guidance to help security professionals build and implement cybersecurity strategy, architecture, and prioritized roadmaps.
docs.microsoft.com/security

Microsoft 365 security documentation
docs.microsoft.com/microsoft-365/security

Evaluate and pilot Microsoft 365 Defender
aka.ms/defender365eval

Azure security documentation
docs.microsoft.com/azure/security

Microsoft