

# Supporting Your EU GDPR Compliance Journey

With Enterprise Mobility + Security



## Table of Contents

Disclaimer.....	2
Introduction .....	3
GDPR Implications.....	3
Getting Started.....	4
Key GDPR Steps.....	4
Addressing the challenges of a mobile-first cloud-first world with Microsoft EMS .....	5
How Microsoft EMS can support your EU GDPR compliance journey.....	6
Personal and Sensitive Data.....	7
How to provide persistent data protection on-premises and in the cloud .....	7
Classification and Labelling .....	8
Protection .....	9
Monitoring .....	12
How to grant and restrict access to data.....	13
Multi-Factor Authentication (MFA) .....	15
Managing Privileged Access to Data .....	15
How to protect data in mobile devices and mobile apps .....	16
How to gain visibility and control of data in cloud apps.....	18
How to detect data breaches before they cause damage.....	22
How to get started .....	27
EMS free trial .....	27
Deployment support.....	27

## Disclaimer

This white paper is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is." Information and views expressed in this white paper, including URL and other Internet website references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only.

Published May 2017

Version 1.0

© 2017 Microsoft. All rights reserved.

## Introduction

On May 25, 2018, a European privacy law is due to take effect that sets a new global bar for privacy rights, security, and compliance.

The General Data Protection Regulation, or GDPR, is fundamentally about protecting and enabling the privacy rights of individuals. The GDPR establishes strict global privacy requirements governing how you manage and protect personal data while respecting individual choice—no matter where data is sent, processed, or stored.

Microsoft and our customers are now on a journey to achieve the privacy goals of the GDPR. At Microsoft, we believe privacy is a fundamental right, and we believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. But we also recognize that the GDPR will require significant changes by organizations all over the world.

We have outlined our commitment to the GDPR and how we are supporting our customers within the [“Get GDPR compliant with the Microsoft Cloud”](#) blog post by our Chief Privacy Officer [Brendon Lynch](#) and the [“Earning your trust with contractual commitments to the General Data Protection Regulation”](#) blog post by [Rich Sauer](#) - Microsoft Corporate Vice President & Deputy General Counsel.

Although your journey to GDPR may seem challenging, we are here to help you. For specific information about the GDPR, our commitments and beginning your journey, please visit the [GDPR section of the Microsoft Trust Center](#).

## GDPR Implications

The GDPR is a complex regulation that may require significant changes in how you gather, use and manage personal data. Microsoft has a long history of helping our customers comply with complex regulations, and when it comes to preparing for the GDPR, we are your partner on this journey.

The GDPR imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where those businesses are located. Among the key elements of the GDPR are the following:

- **Enhanced personal privacy rights** - strengthened data protection for residents of EU by ensuring they have the right to access to their personal data, to correct inaccuracies in that data, to erase that data, to object to processing of their personal data, and to move it;
- **Increased duty for protecting data** - reinforced accountability of companies and public organizations that process personal data, providing increased clarity of responsibility in ensuring compliance;
- **Mandatory data breach reporting** - companies are required to report personal data breaches to their supervisory authorities without undue delay, generally no later than 72 hours; and
- **Significant penalties for non-compliance** - steep sanctions, including substantial fines that are applicable whether an organization has intentionally or inadvertently failed to comply.

As you might anticipate, the GDPR can have a significant impact on your business potentially requiring you to update privacy policies, implement and strengthen data protection controls and breach notification procedures, deploy highly transparent policies, and further invest in IT and training. Microsoft Enterprise Mobility +Security (EMS) can help you effectively and efficiently address these requirements.

In addition to expanding the territorial scope of the EU Data Protection Directive established in 1995, capturing both controllers and processors in the EU, and those outside the EU who offer goods and services to, or monitor, EU residents, the GDPR clarifies and expands the definition of the types of data to be protected.

## Getting Started

In “[Beginning your General Data Protection Regulation \(GDPR\) Journey](#)”, we addressed topics such as an introduction to GDPR, how it impacts you and what you can do to begin your journey today. We also recommended that you begin your journey to GDPR compliance by focusing on four key steps:



### Key GDPR Steps

- **Discover**—identify what personal data you have and where it resides.
- **Manage**—govern how personal data is used and accessed.
- **Protect**—establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.
- **Report**—execute on data requests, report data breaches, and keep required documentation.

For each of the steps, we outlined example tools, resources, and features in various Microsoft solutions that can be used to help you address the requirements of that step. While this document is not a comprehensive “how to,” we have included links for you to find out more details, and more information is available at [Microsoft.com/GDPR](https://Microsoft.com/GDPR).

Given how much is involved, you should not wait to prepare until GDPR enforcement begins. You should review your privacy and data management practices now.

The balance of this white paper is focused on how Microsoft Enterprise Mobility +Security (EMS) can support your compliance with the GDPR as well as approaches, recommended practices and techniques to support your GDPR compliance journey.

## Addressing the challenges of a mobile-first cloud-first world with Microsoft EMS

The GDPR is clear. If you are a data controller or data processor and your activities fall within the scope of the GDPR, you have a responsibility to meet the requirements of the regulation whether the personal data remains on-premises or in some other cloud or mobile environment.

Security was once largely limited to the boundaries of the on-premises world, but with the transition to mobility and the cloud, your employees now have increasingly complex interactions with devices, apps and data, and other users related to data processing and storage. In this new world, managing your perimeter does not guarantee the protection of your data as it travels outside of corporate boundaries.

When you add the evolving nature, and increasing number, of cybersecurity threats into this complex environment, you can see the struggle you're facing in protecting data in line with the GDPR: keeping the balance between providing the best experience to your users while maintaining compliance with regulations such as the GDPR.

Microsoft EMS is designed with this purpose: providing a holistic solution set to help you apply the latest mobility and cloud innovations; helping to protect your business from threats across your data, identities, devices, and apps; and enabling the types of business and technical controls that you will need as you work toward meeting the requirements of the GDPR.





Each of the products in EMS are outlined below and are explored in the detail sections of this white paper with references to the GDPR.

- **Azure Information Protection** - provides persistent data classification and protection; and allows secure sharing of data within or outside of your organization, including the option to monitor activities on shared data and responding in case of unexpected events.
- **Azure Active Directory Premium** - delivers multi-factor authentication; access control based on device health, user location; and, holistic security reports, audits, and alerts.
- **Microsoft Intune** - makes it easier to secure and manage iOS, Android, and Windows PCs all from one console. Deep integration with Office 365 helps keep company data secure in the Office mobile apps.
- **Microsoft Cloud App Security** - provides deep visibility and control of data inside cloud applications, and threat protection.
- **Microsoft Advanced Threat Analytics** - helps protect against advanced persistent threats and malicious attacks using machine learning, behavioral analytics, and deterministic detections.

The solutions within EMS are tightly integrated with productivity tools (like Office and Office 365) that your employees use every day, so you gain tighter control and increased security without having to impose complex processes and changing the way people work.

## How Microsoft EMS can support your EU GDPR compliance journey

With the adoption of mobility and cloud services, data is travelling to more locations than ever before. While it has helped users to become more productive and collaborative, securing and monitoring the data has become harder.

To address data protection in this mobile-first, cloud-first world, it is important to step back and think holistically about the data life cycle. You need to consider what protective measures you should take from when data is created or modified, to when a user wants to access it, when data moves to mobile and cloud apps and even when it gets breached.

In this whitepaper, we explain how Microsoft Enterprise Mobility + Security technologies can help you address the key use case scenarios you should consider through the data lifecycle. These scenarios focus on the elements of the GDPR and will help you address the following:

- How to provide persistent data protection on-premises and in the cloud
- How to grant and restrict access to data
- How to protect data in mobile devices and applications
- How to gain visibility and control of data in cloud apps
- How to detect data breaches before they cause damage

After we cover these scenarios, we provide you with useful resources not only to try EMS solutions, but to deploy them with assistance from our FastTrack program as well.

Understanding and classifying personal and sensitive data, and providing appropriate security measures to protect this data, are critical to your ability to meet your obligations under the GDPR. Let's start by reviewing what type of data you are looking for in the context of the GDPR.

### Personal and Sensitive Data

As part of your effort to comply with the GDPR, you will need to understand how the regulation defines personal and sensitive data and how those definitions relate to data held by your organization. Based on that understanding you will be able to discover where that data is created, processed, managed and stored.

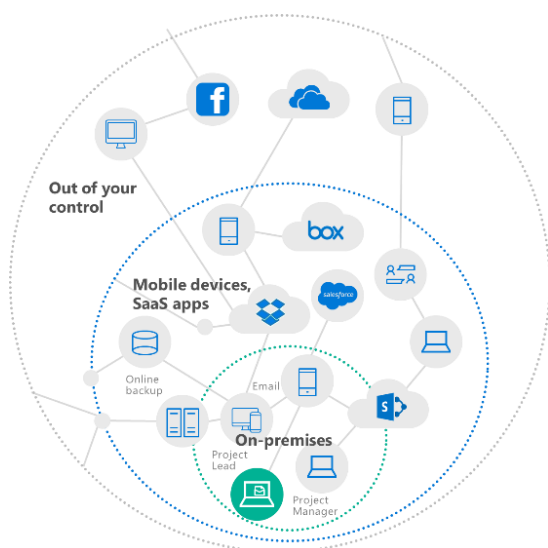
The GDPR considers personal data to be any information related to an identified or identifiable natural person. That can include both direct identification (e.g., your legal name) and indirect identification (i.e., specific information that makes it clear it is you the data references). The GDPR makes clear that the concept of personal data includes online identifiers (e.g., IP addresses, mobile device IDs) and location data where the EU Data Protection Directive had previously been somewhat unclear.

Information relating to an identified or identifiable natural person (i.e., data subject) – examples:

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)
- Genetic data (e.g., biological samples from an individual)
- Biometric data (e.g., fingerprints, facial recognition)

The GDPR introduces specific definitions for genetic data (e.g., an individual's gene sequence) and biometric data (e.g., fingerprints, facial recognition, retinal scans). Genetic data and biometric data along with other sub categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health; or data concerning a person's sex life or sexual orientation) are treated as sensitive personal data under the GDPR. Sensitive personal data is afforded enhanced protections and generally requires an individual's explicit consent where these data are to be processed.

### How to provide persistent data protection on-premises and in the cloud



Managing your perimeter, users, or devices does not guarantee protection of your data as it travels outside of corporate boundaries. Even simply identifying the data that needs protection can be a major challenge. So how can you discover and protect your data persistently when it's being stored in disparate locations and shared across boundaries?

To protect data at all times, regardless of where it is stored, with whom it is shared, or if the device is running iOS, Android or Windows, the classification and protection needs to be built into the file itself so this protection can travel with the data wherever it goes. Microsoft [Azure Information Protection](#) (AIP) is designed to provide this persistent data protection both on-premises and in the cloud.



[Azure Information Protection](#) helps you classify and label data at the time of creation or modification. Protection can then be applied to personal and sensitive data. Classification labels and protection are persistent, traveling with the data so that it's identifiable and protected at all times – regardless of where it's stored or with whom it's shared. The interface is simple and intuitive and does not interrupt your normal working experience. You also have deep visibility and control over shared data.

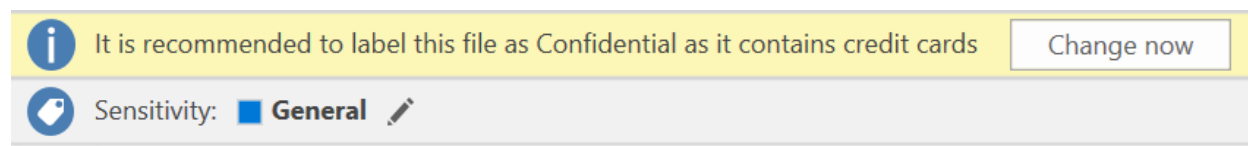
### Classification and Labelling

Data classification is an important part of any data governance plan. Adopting a classification scheme that applies throughout your business can be particularly helpful in responding to what the GDPR calls data subject (i.e., your EU employee or customer) requests, because it enables enterprises to identify more readily and process personal data requests.

Azure Information Protection can be used to help you classify and label your data at the time of creation or modification. Protection in the form of encryption, which the GDPR recognizes may be appropriate at times, or visual markings can then be applied to data needing protection.

With Azure Information Protection, you can either query for data marked with a sensitivity label or intelligently identify sensitive data when a file or email is created or modified. Once identified, you can automatically classify and label the data – all based on the company's desired policy.

In the screen shot below, you'll see that Azure Information Protection identified specific content in the document and notified the user that its recommended to label this file as Confidential. This was based on a company policy that's configured to look for specific content such as credit card numbers in documents that users are working on and recommend appropriate label for the document.



*Azure Information Protection – Recommended Classification*

Administrators and data-owners can also query for labeled files stored on file stores. As an example, a risk manager can query and investigate all "Highly Confidential" files that are located under the "Shared" folder.

The following screen shot shows an example of Azure Information Protection in action. The administrator has configured rules to detect sensitive data (in this case, credit card information) and automatically labelled the file containing sensitive data as "Confidential". When a user saves an Excel document that contains credit card information, the user sees a notification that the file has been labeled as "Confidential" and the label of the file changes from "Not set" to "Confidential".

This file was automatically labeled as Confidential because it contains at least one credit card number. OK

Sensitivity: Confidential

Date	Description	Amount	Merchant name	Account Used	Expiration date	Transaction fees	Balance
7/1/2016	Existing balance	\$2,450.00	Woodgrove Bank	AmEx	Sep-08		\$2,450.00
7/2/2016	Payment for June	-\$34.00	Woodgrove Bank	AmEx	Jan-11	\$2.00	\$2,418.00
7/3/2016	Picture frame	\$45.00	Northwind Traders	4111-1111-1111-1111	Mar-07		\$2,463.00
7/3/2016	Wine	\$600.00	Coho Winery	4012-8888-8888-1881	Aug-11	\$20.00	\$3,083.00
7/8/2016	Ticket to Maui	\$469.00	Blue Yonder Airlines	MasterCard	Apr-10		\$3,552.00
7/12/2016	Cash withdrawal	\$654.00	Woodgrove Bank	Discover	Mar-08		\$4,206.00
7/3/2016	Wine	\$600.00	Coho Winery	Visa	Nov-08	\$20.00	\$4,826.00
7/8/2016	Ticket to Maui	\$469.00	Blue Yonder Airlines	MasterCard	Oct-07		\$5,295.00
7/12/2016	Cash withdrawal	\$654.00	Woodgrove Bank	Discover	Oct-07		\$5,949.00
<b>Total</b>		<b>\$5,907.00</b>				<b>\$42.00</b>	

### Azure Information Protection – Automatic Classification of Confidential Data

#### Protection

After classifying and labeling data properly, securing and controlling data is the next step. Azure Information Protection provides an identity-based security approach that can be used for this purpose.

Azure Information Protection provides you with flexibility in defining its policies to control and protect. Once you have policies in place, you can use AIP to encrypt the files having personal data and manage access rights in accordance with the appropriate policy in line with the GDPR. The screen shot, to the right, shows an administrator policy that automatically protects all data labeled as “Confidential”. Visual markings such as a footer and watermark are also applied to such data.

#### Set permissions for documents and emails containing this label

Not configured **Protect** Remove Protection

#### Protection

Azure RMS: Contoso EMSCR10 - Confidential

#### Set visual marking (such as header or footer)

Documents with this label have a header

**Off** On

Documents with this label have a footer

Off **On**

#### \* Footer text

Sensitivity: Confidential

#### \* Font size

10

#### \* Color

Black

#### Alignment

**Left** Center Right

Documents with this label have a watermark

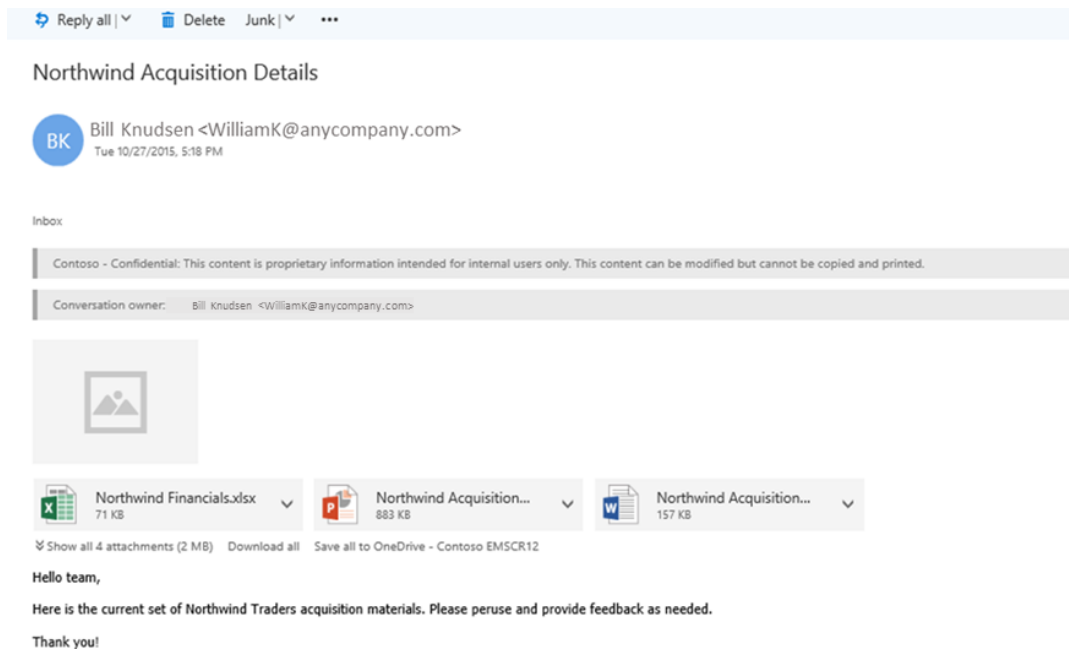
Off **On**

#### \* Watermark text

Confidential

### Azure Information Protection – Document Permission Settings

Azure Information Protection also helps your users share sensitive data in a secure manner. In the example below, information about a sensitive acquisition was encrypted and restricted to a group of people who were granted only a limited set of permissions on the information – they could modify the content but could not copy or print it.



### *Azure Information Protection – Controlled Document Access*

Decryption will be conditional to the user being authorized by the access policy – thereby enforcing the intended safeguards around the personal data (i.e., unauthorized persons will not have access). With the rights-based encryption in place, sharing becomes less cumbersome. You have the means to prevent personal Data from leaking to unauthorized persons, with audit logs to track each access.

Securing data is also about controlling its flow. The classification labels and protection set by Azure Information Protection are persistent and travel with the data so that Data Loss Prevention (DLP) systems and Cloud Access Security Broker (CASB) solutions can tap into this flow and enforce the policy with actions such as Warn, Encrypt, Notify, Block, Quarantine, and Revoke access.

In the example, below, a DLP policy is configured to block all emails with data labeled as Internal when shared externally.

Name:  
labelled as Internal

\*Apply this rule if...

✕ The recipient is located... [Outside the organization](#)

and

✕ has these properties, including any of these words ['Sensitivity:Internal'](#)

add condition


\*Do the following...

Reject the message with the explanation... ['You attempted to send a document classified as Internal to an external recipient'](#)

add action

### DLP Rule - Block External Sharing of Internal Data

The screen shot, below, shows the notification that a user receives when he tries to send confidential information outside of his company. A DLP rule configured by the admin blocks such emails and notifies users. This is great for not only securing critical company data but also educating users on the right behavior.

 Office 365

Your message to [jim@receivingcompany.com](mailto:jim@receivingcompany.com) couldn't be delivered.

A custom mail flow rule created by an admin at [admin@anycompany.com](mailto:admin@anycompany.com) has blocked your message.

You tried to send a document classified as Confidential to an external recipient.

emscr12.onmicrosoft.com	Office 365	pragyap Recipient
<b>Action Required</b>		
Blocked by mail flow rule		

**How to Fix It**

An email admin at emscr12.onmicrosoft.com has created a custom mail flow rule that blocks messages that meet certain conditions, and it appears that your message has met one or more of those conditions.

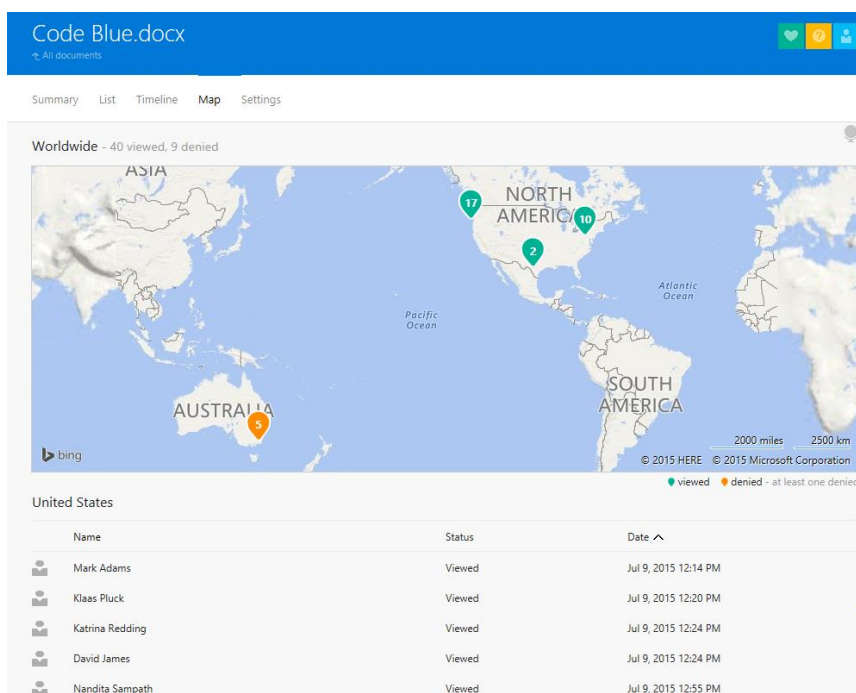
- Check the text above for a custom message from the email admin that may help explain why your message was blocked and how you might be able to fix it. For example, removing prohibited words from the message or sending the message from a different email account may be sufficient to deliver your message.

If you've tried and you're still not able to fix the problem, consider contacting the email admin at emscr12.onmicrosoft.com to discuss what to do. While they're unlikely to remove or relax the rule, if you have a legitimate need to deliver your message they may offer guidance for how to do so.

### Azure Information Protection – DLP User Notification

## Monitoring

After your content is classified (and optionally protected), you can monitor how it is used. You can analyze data flows to gain insight into your business, detect risky behaviors and take corrective measures (e.g., access revocation), track access to documents, prevent data leakage or misuse, and so on as noted in these two images.



*Azure Information Protection – Tracking Data Geographically*

The screenshot shows the 'Revoke access' form for the document 'Code Blue.docx', which was shared on April 23, 2015. The form includes a warning that recipients will no longer be able to view the file. A note states that if a recipient has already viewed the file, they will continue to be able to view it for up to 30 days after access is revoked. There is a checkbox to 'Notify recipients by email when document is revoked'. A section titled 'I am revoking this because:' contains a text area for a message to recipients who try to open the file.

*Azure Information Protection – Revoke Access to Data*

## How to grant and restrict access to data

Enterprises increasingly understand the importance of information security – but the GDPR raises the stakes. It requires that enterprises take appropriate technical and organizational measures to protect personal data from loss or unauthorized access or disclosure. If these measures are not taken, enterprises can face significant penalties if security is breached.

Mechanisms that enable you grant and restrict access (e.g., role-based access, segregation of duties) to personal data and to implement appropriate technical security measures in the product to confirm the ongoing confidentiality, integrity, and availability of personal data and processing systems will help you to meet this requirement.

[Azure Active Directory](#), Microsoft's Identity and Access Management solution, is designed to help organizations manage user identities and associated access privileges. With capabilities, such as conditional access, user and sign-in risk calculation, multi-factor authentication and privileged identity management, Azure Active Directory can help you secure and restrict access to data.

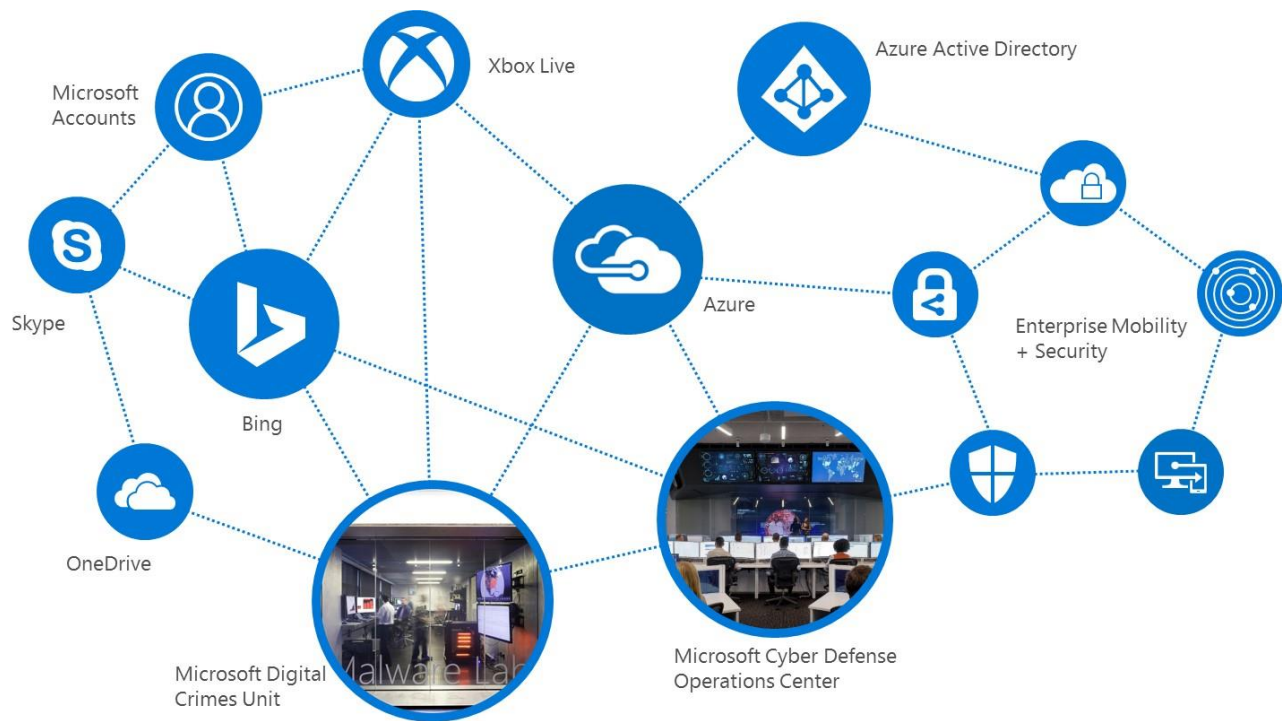
Conditional Access policies can be applied based on device state, application sensitivity, location and user rules. Additionally, Microsoft Enterprise Mobility + Security can protect your data in real-time from the most advanced threats with identity protection capabilities that calculate the risk of every access request and every user and apply automated remediation actions as needed. Risk calculation is capability provided by Azure Active Directory Identity Protection.

The risk calculation by Identity Protection is based on a set of intelligence – signals we collect – from across our products, global cloud services and cybersecurity teams and from other non-Microsoft sources. Microsoft has been turning threats into useful intelligence that can help fortify its platforms and protect customers. Today, with the immense computing advantages afforded by the cloud, we are finding new ways to use our rich analytics engines driven by threat intelligence to protect our customers.

By applying a combination of automated and manual processes, machine learning and human experts, we are able to create an Intelligent Security Graph that learns from itself and evolves in real-time, reducing our collective time to detect and respond to new incidents across our products. Microsoft security teams use the graph to correlate large-scale critical security events, using innovative cloud-first machine learning and behavior and anomaly-based search queries, to surface actionable intelligence.

The scope of the Microsoft Intelligent Security Graph spans, literally, billions of data points: 400 billion messages scanned monthly for spam and malware, over a billion enterprise and consumer devices updated monthly, 18B+ Bing scans and 450 billion authentications performed across our cloud services per month.

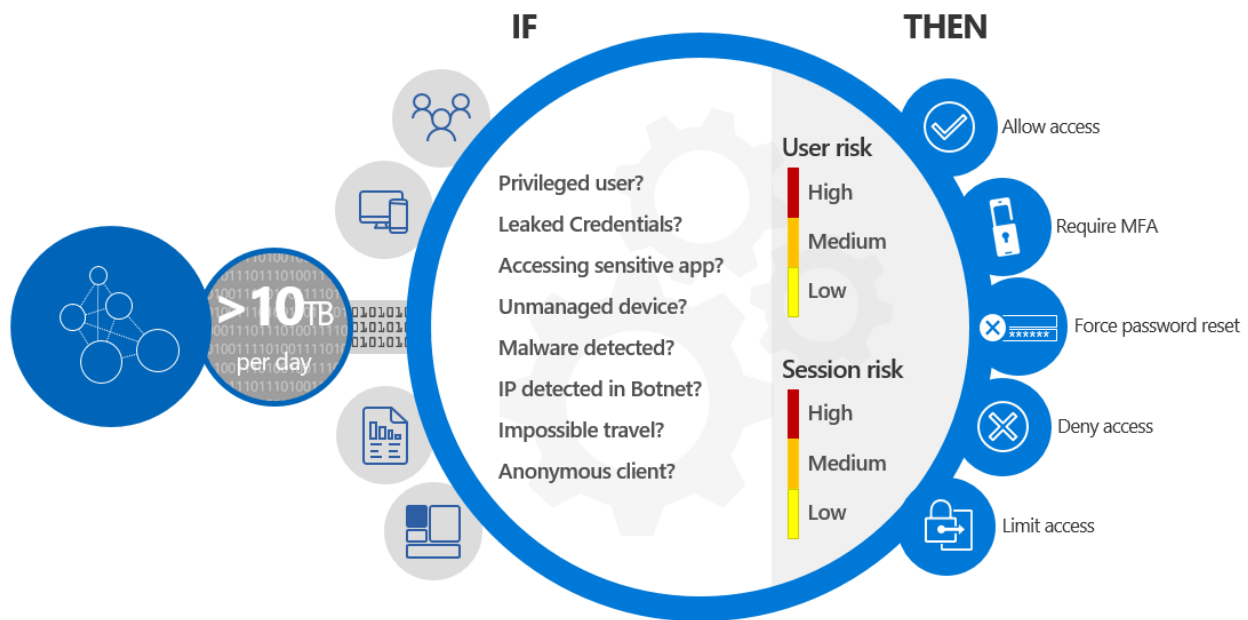




*Microsoft Intelligent Security Graph*

There are conditions and controls that you can utilize to grant access to personal and sensitive data in a fine-grained manner. These include:

- **Group membership.** Control a user's access based on membership in a group.
- **Location.** Use the location of the user to trigger multi-factor authentication, and use block controls when a user is not on a trusted network.
- **Device platform.** Use the device platform, such as iOS, Android, Windows Mobile, or Windows, as a condition for applying policy.
- **Device.** Device state, whether compliant or not, is validated during device policy evaluation. If you disable a lost or stolen device in the directory, it can no longer satisfy policy requirements.
- **Sign-in and user risk.** You can use [Azure AD Identity Protection](#) for conditional access risk policies. Conditional access risk policies help give your organization advance protection based on risk events and unusual sign-in activities.



*Conditional Access Capabilities Enhanced by Microsoft Intelligent Security Graph*

Conditional access policies can block access if a condition is not met or require additional forms of authentication such as multi-factor authentication.

### Multi-Factor Authentication (MFA)

Two-step verification is a method of authentication that requires more than one verification method and adds a critical second layer of security to user sign-ins and transactions. It works by requiring any two or more of the following verification methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something about you (biometrics)

Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution. Azure MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of verification methods, including phone call, text message, or mobile app verification.

Azure Multi-Factor Authentication provides selectable verification methods for both cloud and server. This means that you can choose which methods are available for your users: phone call, text, app notification, or app codes. For more information, see [selectable verification methods](#).

### Managing Privileged Access to Data

Securely managing access to privileged accounts has been a challenge for organizations; over time, they find that they have too many permanent accounts with high levels of privilege in their environments. Some examples of the threats that arise as result include malicious or rogue administrators,

administrator credentials leaked via phishing attacks, administrator credentials cached on compromised systems, user accounts granted temporary elevated privileges that become permanent. This can undermine the security expected by the GDPR.

To prevent this, it is important to manage privileged accounts and monitor their activities because of the risk associated with their misuse.

This is an area where Azure AD Privileged Identity Management can help. Azure AD Privileged Identity Management will help you discover the Azure Active Directory privileged administrator roles and the user accounts they are assigned to. It will also enable you to revoke permanent privileged access and provide a mechanism that manages on-demand, time-limited access for Azure Active Directory privileged accounts. So, you get the ability to discover, restrict and monitor administrators and their access to resources. Users that need administrative access can get it for a preconfigured limited time (just-in-time access) after they have proved their identity with Multi-Factor Authentication.

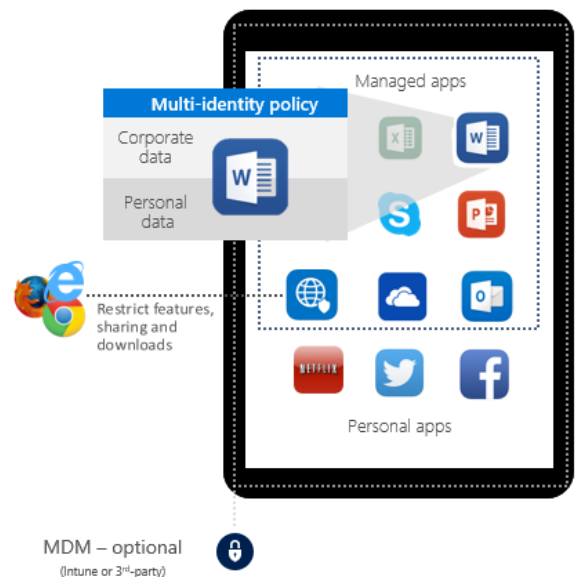
### How to protect data in mobile devices and mobile apps

Mobility is the new normal. This is why a key scenario that you need to consider in the data lifecycle is protecting the data as it travels to mobile devices and mobile apps.

[Microsoft Intune](#) provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to company applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. With support for iOS, Android, Windows, Windows Mobile and Mac OS X devices, Intune allows you to manage your diverse mobile environment in a secure and unified way.

Intune's mobile device management capabilities and device compliance policies make sure devices attempting to access your data or sensitive apps first meet your specific requirements or standards. Administrators can set policies to enforce device enrollment, domain join, strong passwords, and encryption. Policies can also require that device operating systems and apps be up-to-date with the latest patches before granting full access.

You can use [compliance policy settings](#) in Microsoft Intune to evaluate the compliance of employee devices against a set of rules you create. When devices don't meet the conditions set in the policies, Intune guides the end user through enrolling the device (if it's not already enrolled) and fixing the compliance issue.



Microsoft Intune enforces advanced security policies for mobile devices, apps, and PCs by:

- Delivering a comprehensive settings management for mobile devices and PCs including iOS, Android, Windows, and MacOS.
- Providing the ability to deny specific applications or URL addresses from being accessed on mobile devices and PCs
- Enabling the execution of remote actions such as passcode reset, device lock, and remote wipe.
- Enabling the enforcement of stricter “lock down” policies for Supervised iOS devices, Android devices using Kiosk Mode, and Windows 10 devices using Assigned Access.

Once access to mobile apps where sensitive company data or customer data may be stored is achieved, it is critical to control what happens after the data is accessed. Microsoft Intune’s mobile application management capabilities and app protection policies can protect the data at the app level including app-level authentication, copy/paste control, and save as control.

Intune’s application policies give you fine grain control of what your users can do with the data they access in apps. And because we leverage the user identity in our approach, we can enable multi-identity usage of apps - where app policies are intelligent enough to only apply to data applicable to corporate accounts.

Intune’s application management capabilities enable granular control of the data within Microsoft Office mobile apps on iOS and Android devices and help to enforce conditional access policies to Exchange Online, Exchange on-premises, SharePoint Online, and Skype for Business.

Intune supports your GDPR compliance by allowing you to:

- Enable your employees to securely access corporate information using the mobile apps and ensure that your data remains protected after it’s been accessed by restricting actions such as copy/cut/paste/save as.
- Apply policies to applications that protect data with or without enrolling the device for management, allowing you to protect corporate information without the risk of intruding on a user’s personal life.
- Apply the same mobile application management policies to your existing line-of-business (LOB) applications using the Intune App Wrapping Tool, without making code changes.
- Enable users to securely view content on devices within your managed app ecosystem using the Managed Browser and Azure Information Protection Viewer.
- Encrypt company data within apps with the highest level of device encryption provided by iOS and Android.
- Protect your company data by enforcing PIN or credential policies

With Intune, you can also selectively remove corporate data (apps, email, data, management policies, networking profiles, and more) from user devices and apps while leaving personal data intact.

Intune's Mobile Device Management and Mobile App Management capabilities help you protect access to data that may be considered as personal or sensitive data as defined by the GDPR and ensure that your data remains protected after it's been accessed by users.

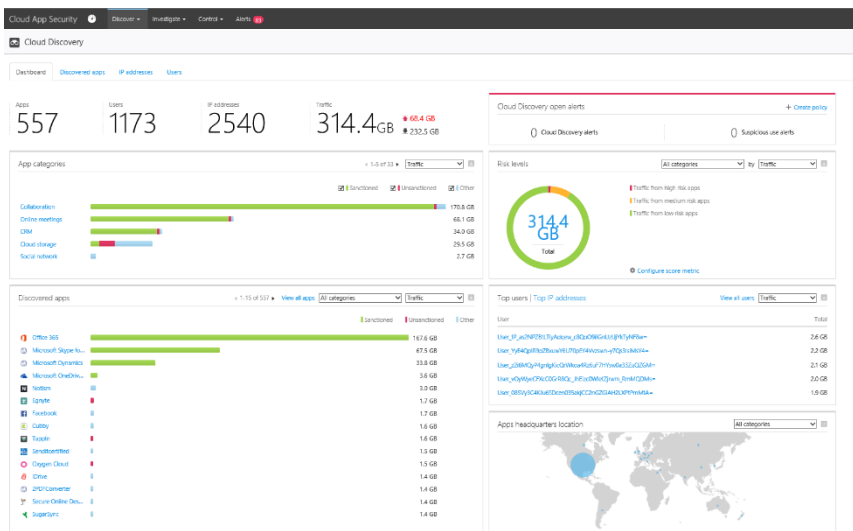
## How to gain visibility and control of data in cloud apps

If you are a data controller as defined by the GDPR, you are responsible to determine the purposes, conditions and means of the processing of personal data, and that extends to your oversight of any data processors you may have engaged. With growing number of Software as a Service (SaaS) apps used in your environment, you may have personal data stored and processed in both sanctioned and non-sanctioned cloud apps. Discovering data stored in the cloud may be complex.

More than 80 percent of employees admit using “non-approved” SaaS apps and less than half are concerned that their use of unapproved software could lead to data loss<sup>1</sup>. But you are still responsible for personal data that may be created, processed, managed, and stored in apps obtained by what is often called “shadow IT”. The more visibility and control you have into your environment, the more you can keep it safely secured and the better you can meet the security requirements of the GDPR.

[Microsoft Cloud App Security](#) is a comprehensive service providing deep visibility, granular controls and enhanced threat protection for your cloud apps. It identifies more than 13,000 cloud applications in your network—from all devices—and provides risk scoring and ongoing risk assessment and analytics. No agents required: information is collected from your firewalls and proxies to give you complete visibility and context for cloud usage and shadow IT.

We also help you to protect your employees' privacy when you're discovering SaaS apps with [our log anonymization](#) feature. Cloud Discovery data anonymization enables you to protect user privacy. Once the data log is uploaded to the Cloud App Security portal, the log is sanitized, and all username information is replaced with encrypted usernames.



Cloud App Security – Cloud Discovery Dashboard

<sup>1</sup> *The Hidden Truth Behind Shadow IT*, published in November 2013 by Strategist, a branch of Frost & Sullivan, Supporting Your EU GDPR Compliance Journey

If an admin has a reason to suspect a specific user, he can also look up the encrypted username of a known username, and then start investigating using the encrypted username. Each username conversion is audited in the portal's Governance log.

**Risk assessment.** Cloud App Security not only discovers the cloud applications where personal data may reside, but also provides a risk score by evaluating each discovered service against ~ 60 parameters: evaluating the service provider, security mechanisms, and compliance certifications. These details help determine and assess the credibility and reliability of each cloud service discovered, represented by a risk assessment. Cloud App Security gives you the tools to perform a total risk assessment for each service, based on a combination of risk score and usage.

**Powerful reporting and analytics.** Discovering which applications are in use across an organization is just the first step in making sure data is protected. Understanding use cases, identifying top users, and determining the risk associated with each application are all important components to understanding an organization's overall risk posture. With Cloud App Security, we provide ongoing risk detection, analytics, and powerful reporting on users, usage patterns, upload/download traffic, and transactions so that you can identify anomalies right away.

**Investigation.** To better understand your cloud environment, Cloud App Security investigate feature provides deep visibility into all activities, files and accounts for sanctioned and managed apps. You can gain detailed information on a file level and discover where data travels in the cloud apps.

File name	Owner	App	Collaborators	Last modified
TeamsNotebook(Shared)	MOD Administrator	Microsoft OneDrive for Bus...		Apr 18, 2017
TeamsNotebook(Shared).onetoc2	MOD Administrator	Microsoft OneDrive for Bus...		Apr 18, 2017
Notebooks	MOD Administrator	Microsoft OneDrive for Bus...		Apr 18, 2017
Attachments	MOD Administrator	Microsoft OneDrive for Bus...		Apr 18, 2017
Screen Shot 2017-03-14 at 7.00.21 AM.png.QUARANTINE.txt	demo	Box		Apr 12, 2017
Quarantine	demo	Box		Apr 12, 2017
casdemo2017@outlook.com	demo	Box		Apr 12, 2017

### *Cloud App Security – File Investigation*

Discovering which SaaS apps are in use with Cloud App Security across your organization is the initial steps for gaining visibility and control. Cloud App Security also protects the data in these apps by granular policies and governance actions and also detects possible threats with anomaly detection and behavioral analytics.



Once cloud apps that contain data the GDPR considers as personal data are discovered, these apps must be controlled with appropriate policies and controls. Cloud App Security can provide you with data control policy setting and enforcement. Granular-control security policies can be built easily. You can use out-of-the-box policies or build and customize your own. You can create:

- Activity policies
- Anomaly detection policies
- App discovery policies
- Cloud Discovery anomaly policies and
- File policies

Furthermore, through integration with Azure Information Protection, you can use the Cloud App Security portal to set policies for files sharing – based on their level of sensitivity to the business as set by Azure Information Protection.

With the integration of Azure Information Protection and Cloud App Security, we extend visibility into sensitive data at it moved to cloud locations. As shown below, Cloud App Security admins can configure policies to read Azure Information Protection labels and take appropriate actions or raise alerts.

**Policy name**

Azure Information Protection Document Monitoring

**Description**

Monitors for any Azure Information Protection labelled file that is shared publicly.

**Policy severity**

High

**Category**

DLP

**Create a filter for the files this policy will act on**

FILES MATCHING ALL OF THE FOLLOWING [Edit and preview results](#)

	Access level	equals	Public, External
	Classification label	equals	Confidential

**Apply to:**

all files

*Azure Information Protection – Policy Configuration*

## Alerts

☒ Create an alert for each matching file [Use your organization's default settings](#)

Daily alert limit

☐ Send alert as email

☐ Send alert as text message

[Save these alert settings as the default for your organization](#)

## Azure Information Protection – Alert Configuration

When there is a violation against your policies, you will receive an alert. After you have thoroughly investigated and learned about this violation, you can use governance actions to protect your data in the cloud apps right away. Every insight is actionable, allowing you to remediate with a single click or implement data sharing and granular usage policies.

For instance, you can:

- Put files into quarantine so only user can access the file
- Restrict sharing (i.e. make a link private)
- Send notifications to users who shared these sensitive files
- Protect the file with Rights Management

Cloud App Security | Discover | Investigate | Control | Alerts (61) | [Policy settings](#)

Policies > File containing PII detected in the cloud (built-in DLP engine) | [Policy settings](#)

Matching now | History

AUTHORIZATION | APP | OWNER | ACCESS LEVEL | FILE TYPE | OWNER OU | Advanced

1 - 3 of 3 files

File name	Owner	App	Collaborators	Content matches	Detection date
Customer US Store Purchases.xlsx	Miriam Graham	Microsoft SharePoint Online	26 collaborators	35 matches	Feb 6, 2017
Northwind Customer Data.xlsx	Provisioning User	Microsoft SharePoint Online	27 collaborators	35 matches	
Project Falcon Customer Data.xlsx	Provisioning User	Microsoft SharePoint Online	27 collaborators	9 matches	

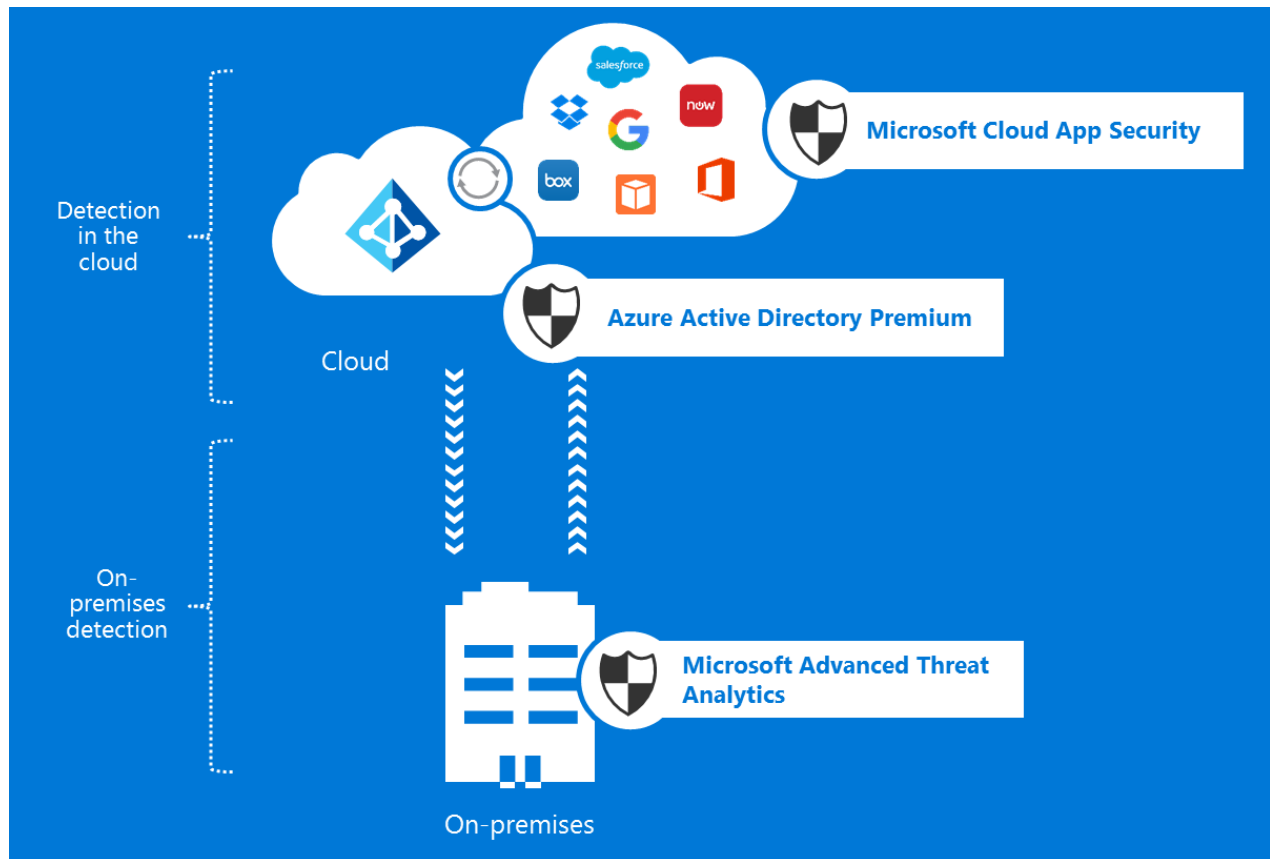
Context menu actions:

- Open in Microsoft SharePoint Online
- Refresh file
- View hierarchy
- View related activity
- View related governance
- Protect
- Put in user quarantine
- Scan for advanced threats
- Make private
- Remove a collaborator

## Cloud App Security – Governance Actions for a Policy Violation

## How to detect data breaches before they cause damage

The GDPR defines the timeline and conditions under which you must provide notice of a personal data breach to a controller (if you are a processor), the relevant supervisory authority as well as impacted data subjects. Our innovative and sophisticated solutions set can help you meet this requirement. Microsoft EMS solutions uses cutting-edge behavioral analytics and anomaly detection technologies to uncover suspicious activity and pinpoint threats—on-premises and in the cloud. That includes known malicious attacks (i.e. Pass the Hash, Pass the Ticket) and security vulnerabilities in your system.



*Detection On-Premises and in the Cloud*

Traditional IT security tools provide limited protection against sophisticated cybersecurity attacks when user credentials are stolen. Initial set up, creating rules, and fine-tuning are cumbersome and may take years. Every day, you may receive several reports full of false positives.

Most of the time, you may not have the resources to review this information and even if you could, you may still not have the answers, since these tools are designed to protect the perimeter, primarily stopping attackers from gaining access.

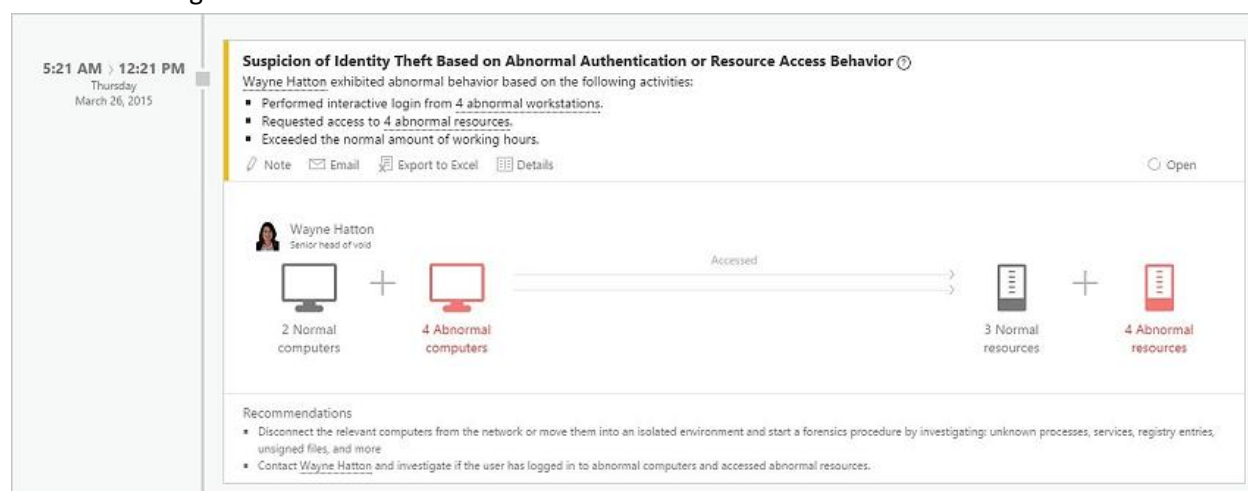
Network logs are not sufficient for threat detection— finding attackers through log analysis is like searching for a needle in the haystack. Even if you find a clue, figuring out when, how and from where it really happened is a challenge. Today’s complex cybersecurity attacks require a different approach.

[Microsoft Advanced Threat Analytics](#) (ATA) is an on premises, non-intrusive solution that leverages deep packet inspection (DPI) technology to analyze Active Directory related network traffic, as well as information from Security Information and Event Management (SIEM) and Active Directory.

ATA analyzes this information to create dynamic behavioral profiles for each entity in your organization and builds an Organizational Security Graph (an entity interaction map representing the context and activities of the users, devices and resources).

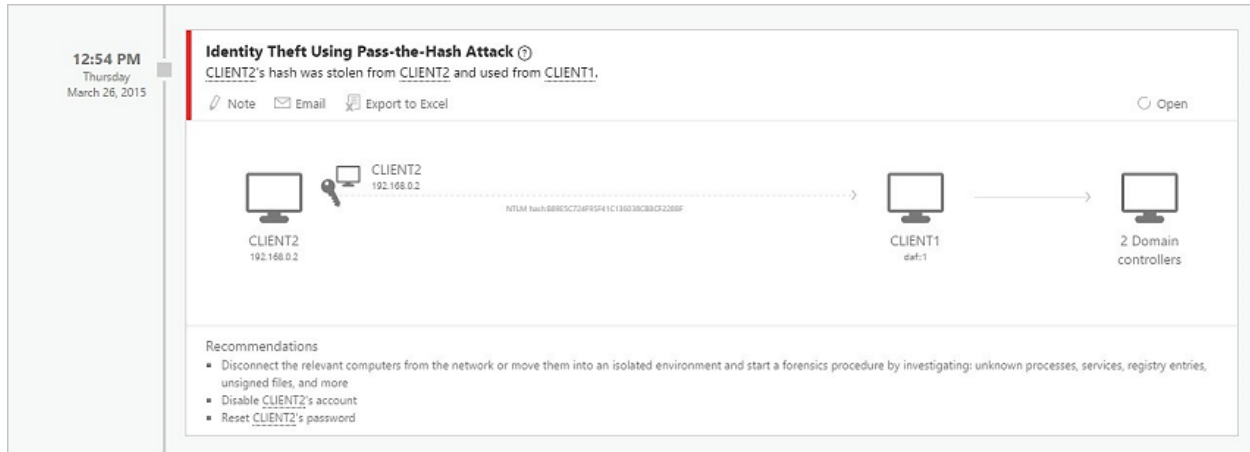
After building this interaction map, it identifies **abnormal behavior** of entities, **advanced attacks and security risks** without the need to create rules, policies, or install desktop and server agents. Microsoft Advanced Threat Analytics focuses on detecting the following anomalies:

- **Abnormal behaviour:** ATA uses Machine Learning algorithms to identify normal and abnormal entity behaviour and will detect anomalous logins, abnormal resource access, and even unusual working hours.



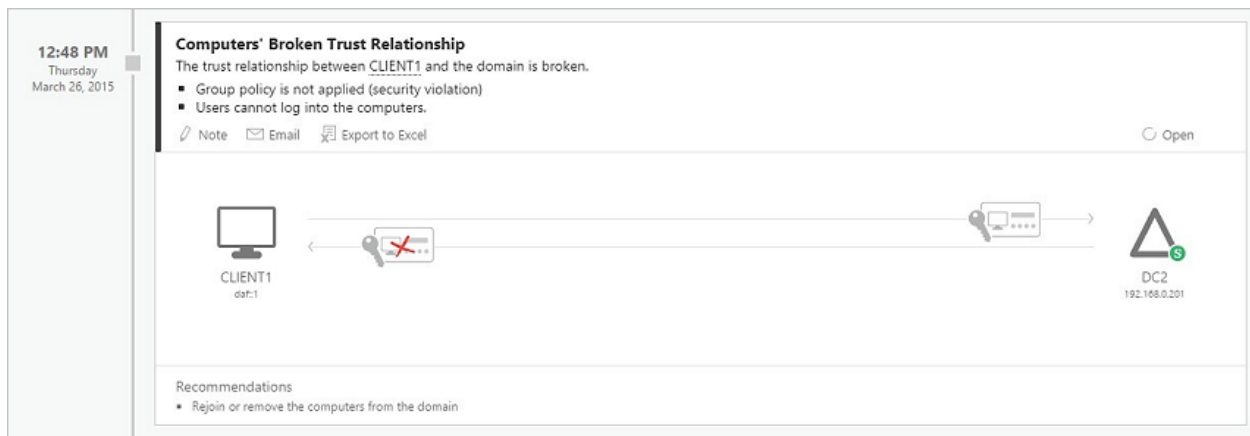
*Advanced Threat Analytics – Abnormal User Behavior Alert*

- **Advanced attacks in near real-time based on TTPs:** ATA uses Deep Packet Inspection technology and information from other sources to identify advanced attacks such as Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash, Forged PAC, Golden Ticket, and Remote Execution on the Domain Controllers, Skeleton Key Malware, Honey token activities and more.



*Advanced Threat Analytics – Known Malicious Attack detection*

- **Known security issues and risks:** ATA will identify known security issues and risks such as service account expose passwords in cleartext over the network, broken trust, weak protocols and protocol vulnerabilities.



*Advanced Threat Analytics – Detection of Known Security Issues*

The constant reporting of traditional security tools and sifting through them to locate the important and relevant alerts can get overwhelming. ATA provides an attack timeline - a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving you the power of perspective on the who, what, when, and how. ATA also provides recommendations for investigation and remediation for each suspicious activity.

In addition to the capabilities we have outlined in how to gain visibility and data control for your cloud apps scenario, [Cloud App Security](#) helps you to protect your data in cloud apps from cybersecurity threats. You can identify anomalies in your cloud usage that may be indicative of a data breach. Cloud App Security advanced machine learning heuristics learn how each user interacts with each SaaS application and, through behavioral analysis, assesses the risks in each transaction. This includes simultaneous logins from two countries, the sudden download of terabytes of data, or multiple failed login attempts that may signify a brute force attack.

Cloud App Security

DiscoverInvestigateControlAlerts24

Microsoft

General Anomaly Detection4 minutes agoMedium

Google AppsExchange OnlineGeneral Anomaly Detectionmarianna@acme.com

The user marianna@acme.com triggered a suspicious session with a combined risk score of 65.95/100 based on the factors below.

- The IP 109.163.234.2 is an anonymous proxy
- The user marianna@acme.com is an administrator
- The ISP "Voxility S.R.L."
  - was first used by any user across the organization
  - was first used by any user for administrative activity across the organization
- The session contains 6 failed login attempts
- The user connected from Boardman (Oregon), United States and then from Ramat Gan (Tel Aviv), Israel in about an hour. These locations are 11,003 km apart.

It is recommended to confirm the user is familiar with these actions.

Resolve

Activity logrelevant for this alert

1 - 13 of 13 activities

Activity	User	App	IP address	Location	Device	Date
Send mail: ***** to: mathew@acm...	marianna	Exchange Online	84.109.184.235	Israel		Mar 1, 2016, 8:59 PM
Send mail: RE: ***** to: marie@acme.com	marianna	Exchange Online	84.109.184.235	Israel		Mar 1, 2016, 8:57 PM
Send mail: RE: ***** to: mariyah@acme.com	marianna	Exchange Online	84.109.184.235	Israel		Mar 1, 2016, 8:57 PM
Log out marianna@acme.com	marianna	Google Apps	109.163.234.2	—		Mar 1, 2016, 8:37 PM
Suspend user: marie@acme.com	marianna	Google Apps	109.163.234.2	—		Mar 1, 2016, 8:36 PM
Log on	marianna	Google Apps	109.163.234.2	—		Mar 1, 2016, 8:35 PM

*Cloud App Security – General Anomaly Detection*

Anomaly detection draws from Microsoft’s vast amount of threat intelligence and security research data. Cloud App Security benefits from Microsoft’s holistic, agile security platform, and is informed by insights from Microsoft Intelligent Security Graph.

*Azure Active Directory Monitoring and Reporting*

A key aspect of the GDPR you will need to meet are the audit requirements associated with the controls and protections you have in place. Azure AD provides important auditing reporting. As an example, advanced security reporting to protect against suspicious behaviors and advanced attacks.

You can use Azure Active Directory's access, usage, and security reports to gain visibility into the integrity and security of your organization’s directory. With this information, a directory administrator can better determine where possible security risks may lie so that they can adequately plan to mitigate those risks.



In the Azure Management Portal, reports are categorized in the following ways:

- **Security reports**- Provides two types of reports user flagged for risk and risky sign-ins (sign-ins from anonymous IPs, impossible travel, unfamiliar locations and infected devices)
- **User-specific reports** – Display device/sign in activity data for a specific user.
- **Activity logs** – Contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days, as well as group activity changes, and password reset and registration activity.

DATE	TARGET ID	INITIATED BY (ACTION)	ACTIVITY
5/15/2017 5:42:25 AM	User: garth@contosobuild.com	admin@contosobuild.com	Update user
5/15/2017 5:42:25 AM	User: garth@contosobuild.com, User	admin@contosobuild.com	Set user manager
5/15/2017 5:42:25 AM	User: garth@contosobuild.com	admin@contosobuild.com	Update user
5/11/2017 9:31:41 AM	User: Ahadi@contosobuild.com	fsm_password_service@support.microsoft.com	Reset password
5/11/2017 9:31:41 AM	User: Ahadi@contosobuild.com	Ahadi@contosobuild.com	Reset password (self-service)
5/11/2017 9:31:41 AM	User: Ahadi@contosobuild.com	Ahadi@contosobuild.com	Self-serve password reset flow activity progress
5/11/2017 9:31:23 AM	User: Ahadi@contosobuild.com	Ahadi@contosobuild.com	Self-serve password reset flow activity progress
5/11/2017 9:31:23 AM	User: Ahadi@contosobuild.com	Ahadi@contosobuild.com	Self-serve password reset flow activity progress
5/11/2017 9:31:07 AM	User: Ahadi@contosobuild.com	Ahadi@contosobuild.com	Self-serve password reset flow activity progress
5/11/2017 9:30:47 AM	User: Ahadi@contosobuild.com	Ahadi@contosobuild.com	Self-serve password reset flow activity progress
5/11/2017 7:47:24 AM	User: garth@contosobuild.com, Role: Company Administrator	MSRM	Remove member from role
5/11/2017 7:46:59 AM	User: garth@contosobuild.com, Role: Company Administrator	MSRM	Add member to role
5/10/2017 9:21:35 AM	User: garth@contosobuild.com, Role: Company Administrator	MSRM	Remove member from role
5/10/2017 9:21:17 AM	User: garth@contosobuild.com, Role: Company Administrator	MSRM	Add member to role
5/9/2017 12:54:21 PM	ServicePrincipal: Reporting API application, User: jeremylink@contosobuild.com	jeremylink@contosobuild.com	Add app role assignment grant to user

*Azure Active Directory – Audit Logs*

Access and usage reports that give visibility into the integrity and security of your organization's directory with access and usage reports. The sign-ins option gives you a complete overview of all sign-in events to applications that contain personal and sensitive data.

USER	APPLICAT...	SIGN-IN S...	SGIN-IN ...	IP ADDRE...	CLIENT	USER NA...	LOCATION
Jon Doe	Azure Po...	Success	2016-09...	167.220...	Window...	admin@...	US
Jon Doe	Azure Po...	Success	2016-09...	167.220...	Window...	admin@...	US
Jon Doe	Azure Po...	Success	2016-09...	167.220...	Window...	admin@...	US
Jon Doe	Azure Po...	Success	2016-09...	167.220...	Window...	admin@...	US
Jon Doe	Azure Po...	Success	2016-09...	167.220...	Window...	admin@...	US
ee28acaf...	Azure Po...	Success	2016-09...	167.220...	Window...	ee28acaf...	US
Jon Doe	Azure Po...	Success	2016-09...	167.220...	Window...	admin@...	US

*Azure Active Directory – Sign-In Analysis*

## How to get started

### EMS free trial

We know that experiencing technology first hand can help you make the right purchasing decision for your business. That is why we provide a free 90-day trial so you can try and evaluate Enterprise Mobility + Security solutions and how it meets your business challenges. You can also request a one-on-one demo from one of our trained experts to explore EMS without leaving your office. To get started, please visit our [trial page](#).

### Deployment support

Microsoft's FastTrack service is included as part of your EMS subscription(s). You can engage with FastTrack to accelerate a successful deployment. Using a Success Plan, FastTrack offers you free deployment services with dedicated engineers in the respective areas of expertise to help you deploy EMS products smoothly, with resources and expertise you need to realize business value and compliance faster. To get started with the support from the exclusive Microsoft FastTrack program, please visit [here](#).

Want more information on GDPR? Visit the following links:

- [Microsoft GDPR site](#)
- [Microsoft & GDPR whitepaper](#)
- [Microsoft's commitment to GDPR video](#)

### Licensing

For more information regarding [EMS licensing](#), please visit EMS licensing page. If you have any questions, please call 800-426-9400 (US) or 877-568-2495 (Canada).