Microsoft 365 Academy: Trailer

Michele Sensalari
MCT Trainer
michele@sensalari.com
@ilsensa7

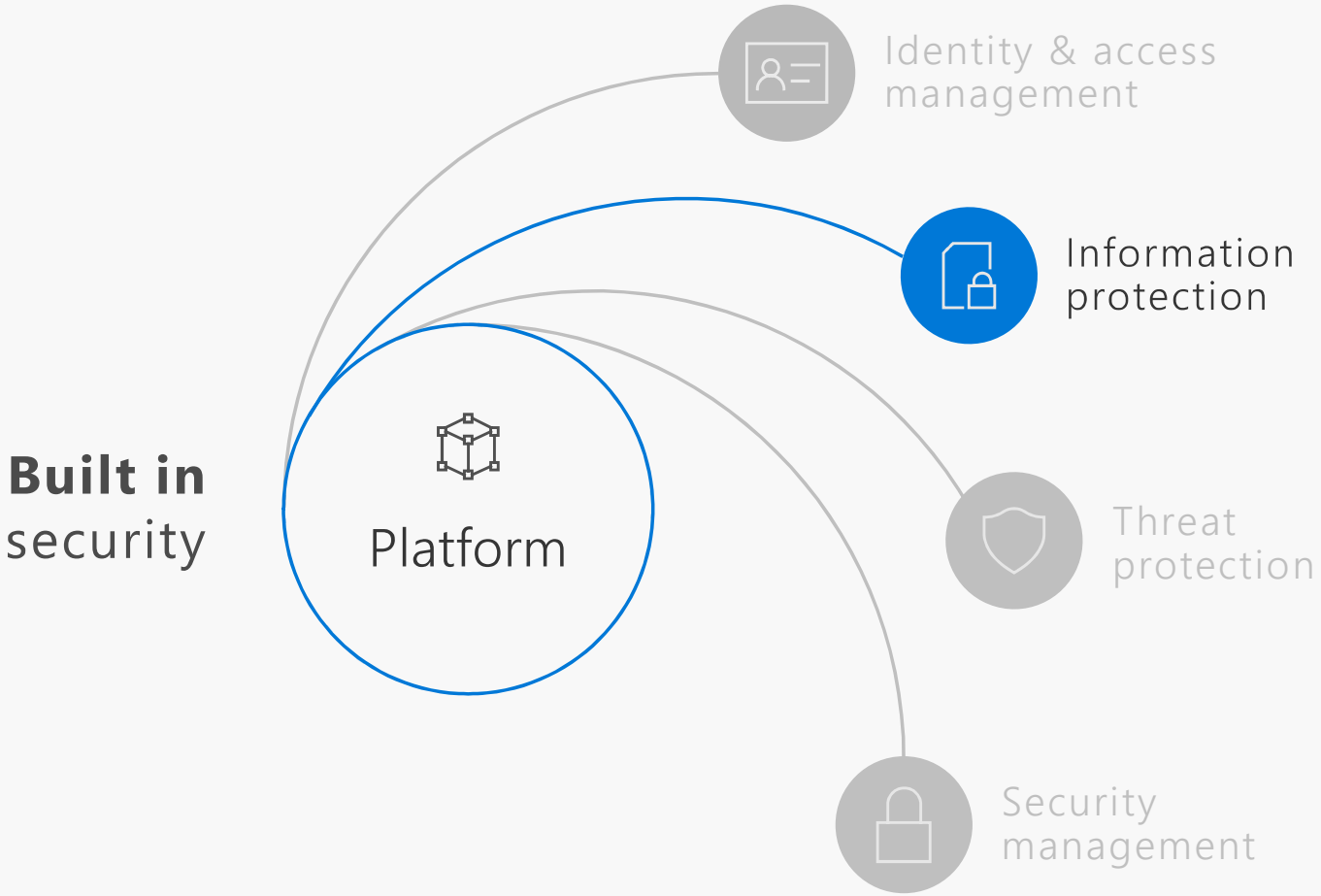
Michele Sensalari

- Senior Consultant – Speaker – Trainer
- Dipendente 50% su tecnologie Microsoft al Dipartimento di Informatica – Università degli Studi di Milano
- Freelance 50/70% (e si anche il we..)
- Docente, speaker, responsabile conferenze Overnet Education
- MCT, MCSE, MCSA. MCITP
- Contatti:
  - michele@sensalari.com
  - michele.sensalari@overneteducation.it
  - Twitter: @ilsensa7
  - Linkedin

Menù

- Information Protection
- Bitlocker
- MAM / MDM
- Microsoft Information Protection
- Windows Information Protection
- Azure Information Protection
- Office 365 ATP

Information Protection


Identity & access management
Information protection
Threat protection
Security management
Platform
Built in security

Sensitive data is at risk

80 % of employees use non-approved SaaS apps at work

88 % of organizations no longer have confidence to detect and prevent loss of sensitive data

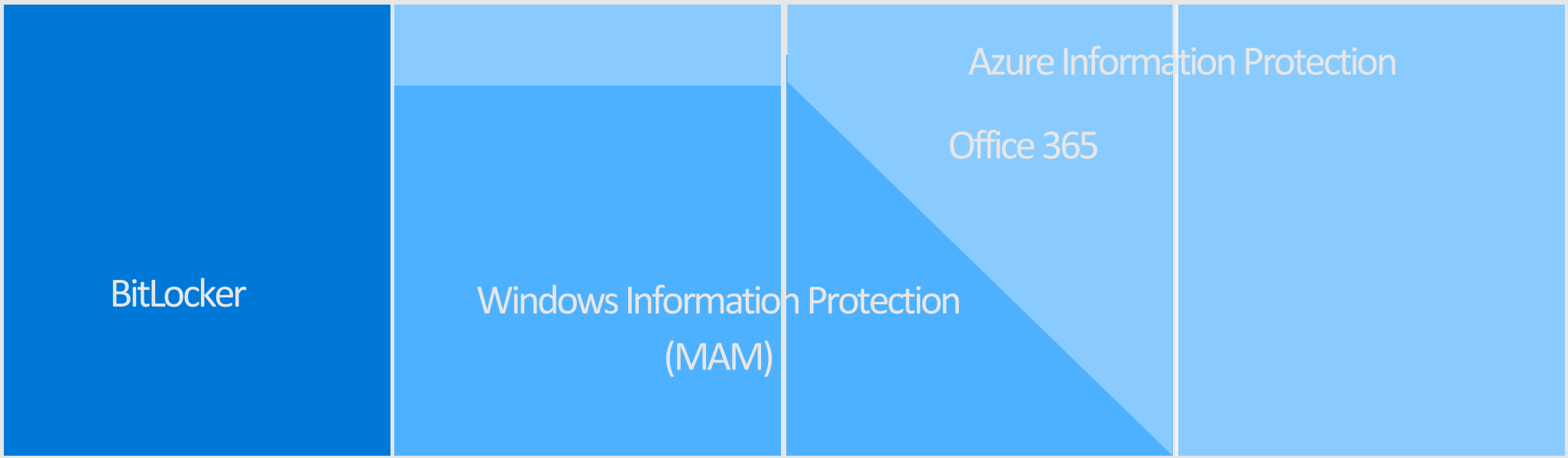
58 % Have accidentally sent sensitive information to the wrong person

85 % of enterprise organizations keep sensitive information in the cloud

YOUR INFORMATION **PROTECTION NEEDS**

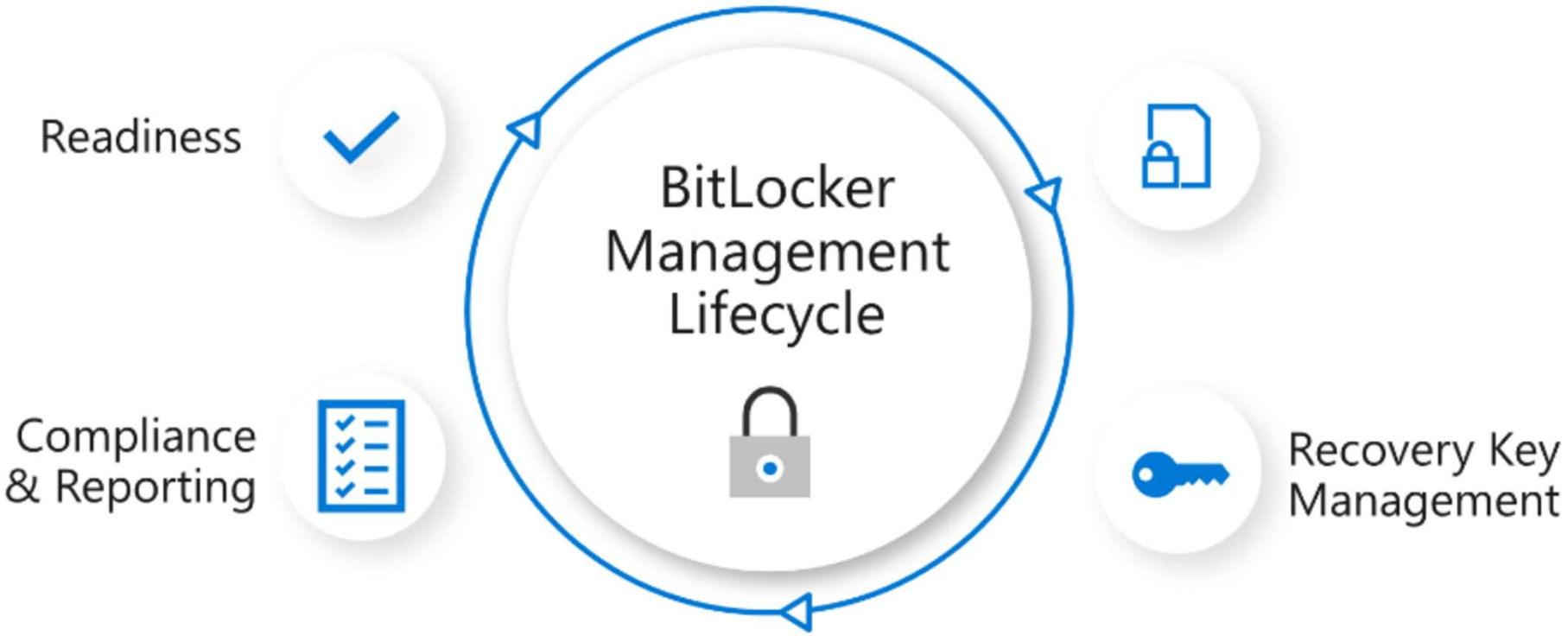
DEVICE PROTECTION	DATA SEPARATION	LEAK PROTECTION	SHARING PROTECTION
Protect system and data when device is lost or stolen	Containment Data separation	Prevent unauthorized users and apps from accessing and leaking data	Protect data when shared with others, or shared outside of organizational devices and control

YOUR INFORMATION **PROTECTION NEEDS**

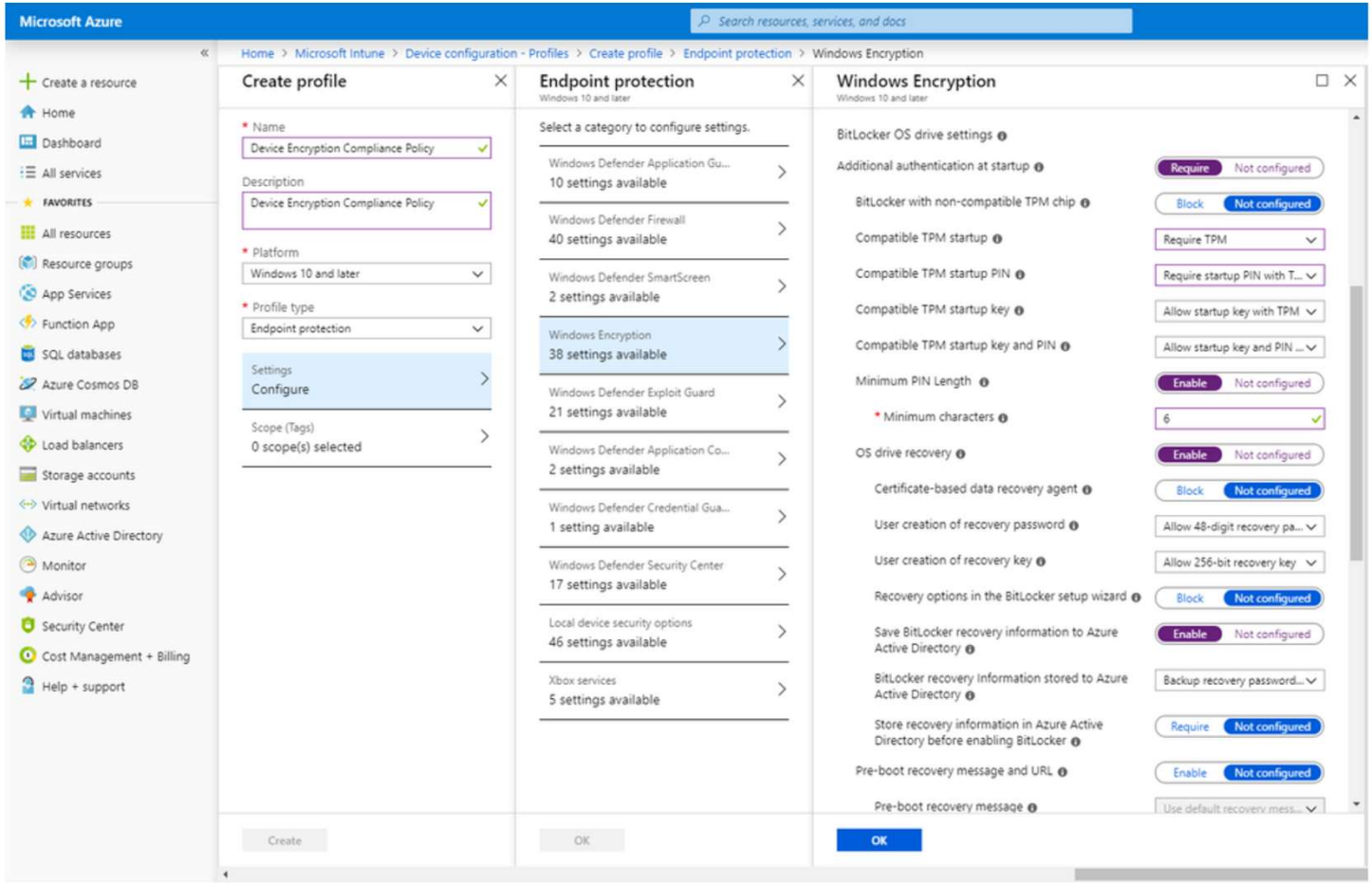


Bitlocker

Bitlocker Management



Microsoft Intune Bitlocker Management



Microsoft Intune BitLocker management platform is available today, and includes features such as compliance reporting, encryption configuration, with key retrieval and rotation on the roadmap. In the coming months, we expect Microsoft cloud-based BitLocker management to meet and exceed the MBAM capabilities you are familiar with.

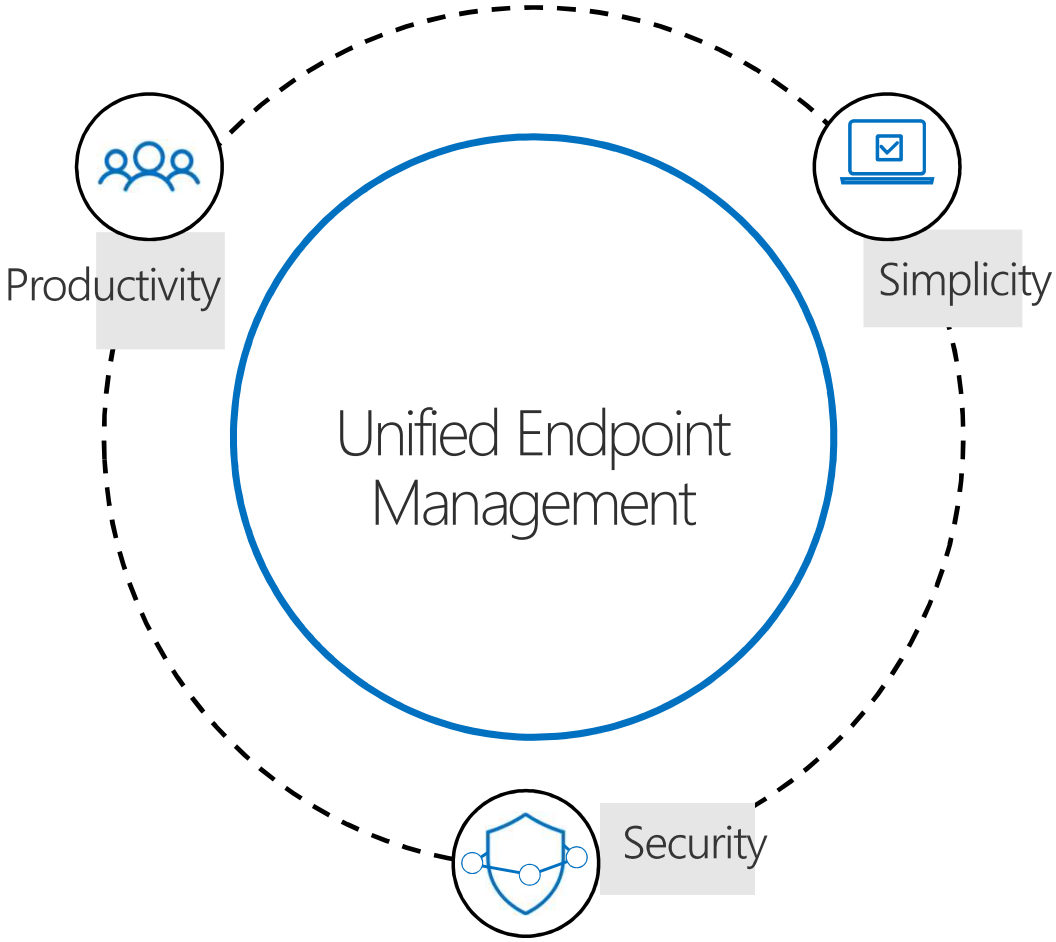
New Feature Intune Bitlocker coming in 2019

- **Key recovery auditing**
  Get reports on who accessed recovery key information in Azure AD.
- **Key recovery**
  Enables you or another admin to recover keys in the Microsoft Intune console. You may enable user self-service key recovery using the Company Portal app, available across device platforms such as web, iOS, Android, Windows, and MacOS.
- **Key management**
  Enable single-use recovery keys on Windows devices by ensuring keys are rolled on-access (by client) or on-demand (by Intune remote actions).
- **Migrating from MBAM to cloud management**
  For our current MBAM customers that need to migrate to modern BitLocker management, we are integrating that migration directly into the key rotation feature

Microsoft Intune: MAM vs MDM

Microsoft Intune

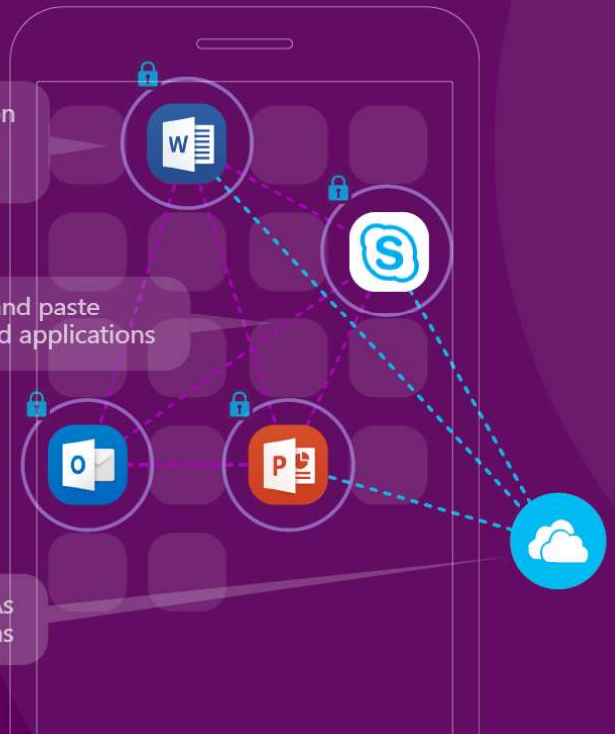
The simplest way to manage all Microsoft 365 endpoints



Protect Office 365 data, even on unmanaged devices

Employees expect access to the best tools, wherever they are—even on their own devices. IT needs confidence that critical data is secure. Intune delivers both.

Data loss prevention



Require encryption for managed app local storage

Only allow copy and paste between managed applications

Only allow Save As to secure locations

Identity-driven protection

Protect data at the app level, rather than requiring the entire device to be secured.

Employees can use their work and personal accounts with the same app

Corporate Identity

Personal Identity

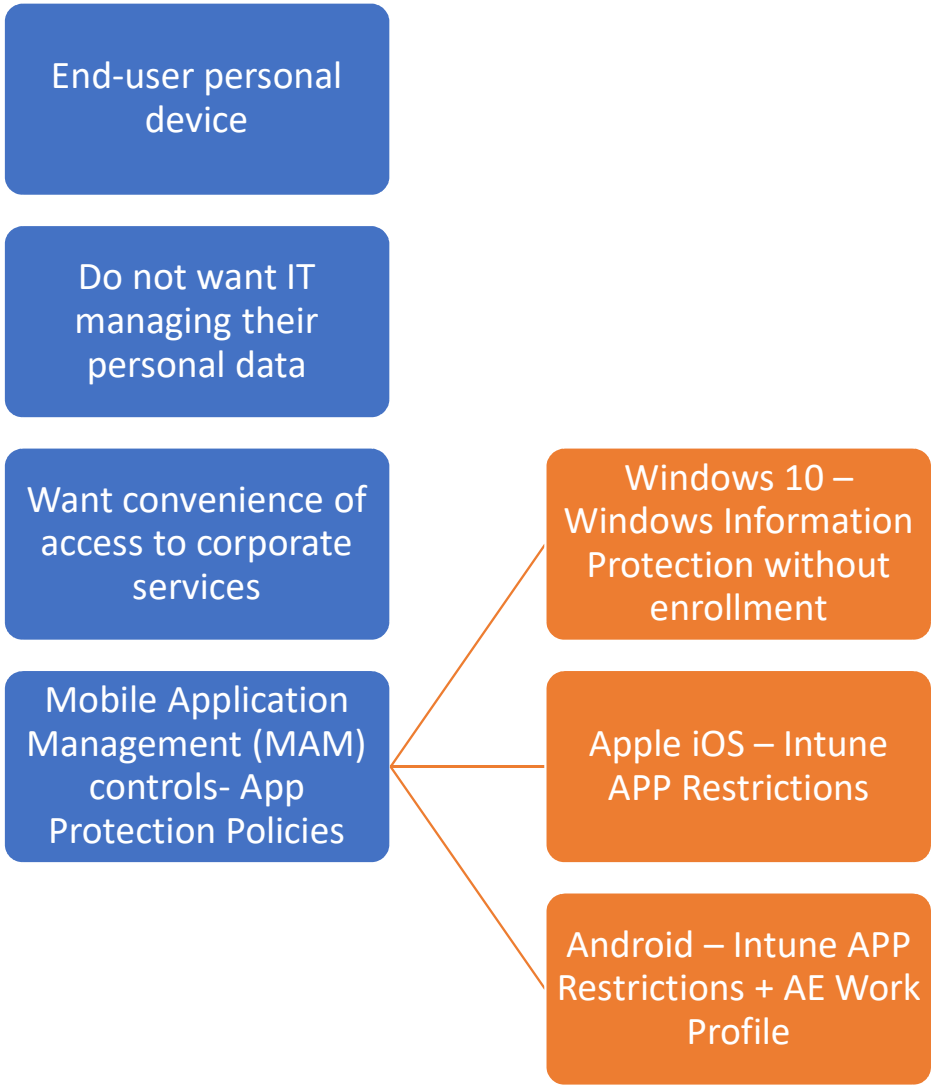
Corporate identity and data can be removed without affecting users' apps or personal data.

Compliance

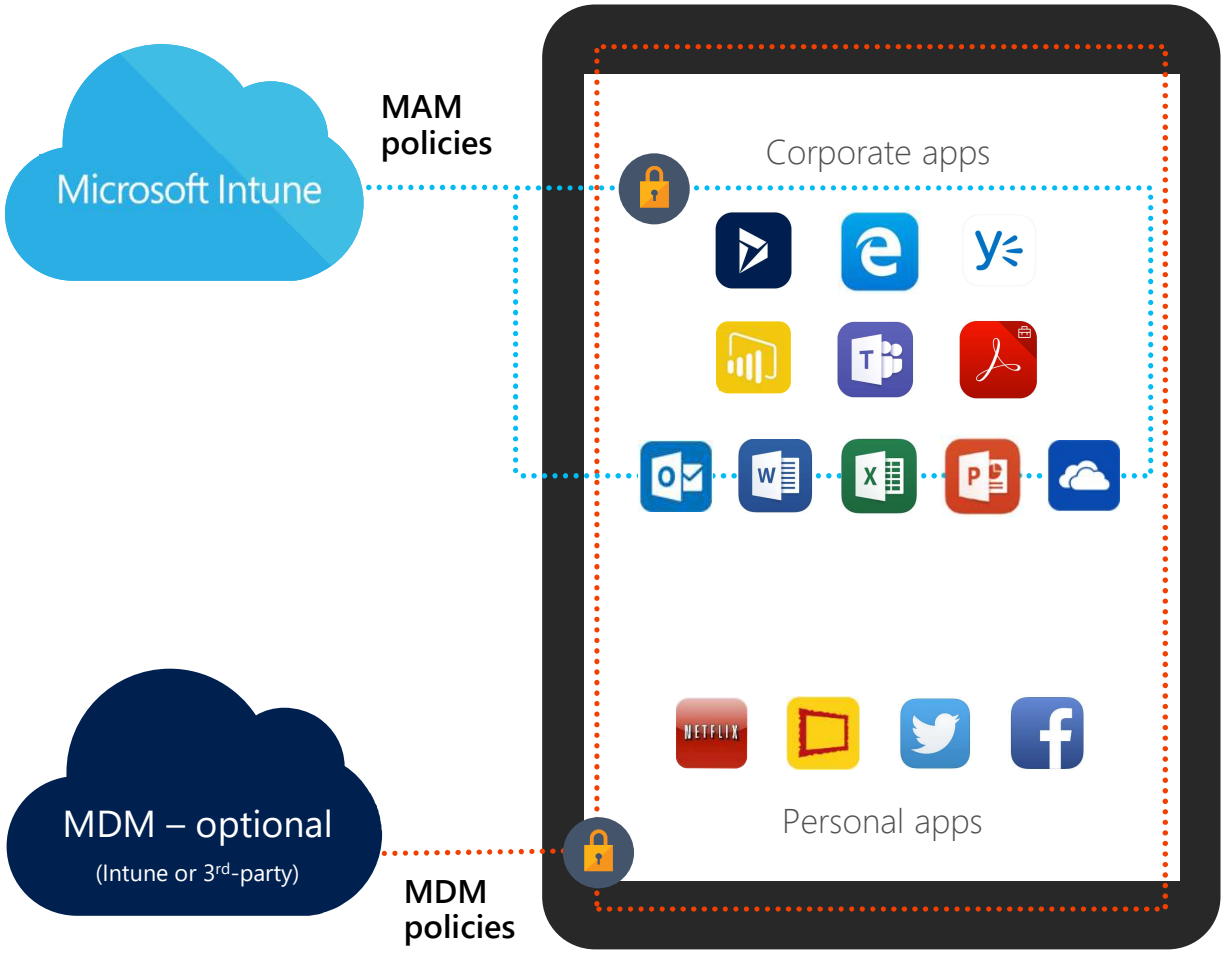
Set up a PIN for your device

Natural user prompts guide users to compliance

Can I protect app data on an unknown device?



Introduction to Intune App Protection Policies (APP)



Familiar Office experience

- Seamless "enrollment" into app management
- Use for personal and corporate accounts

Comprehensive protection

- App encryption at rest
- App access control – PIN or credentials
- Save as/copy/paste restrictions
- App-level selective wipe

MDM mgmt. by Intune or third-party is optional

Might be a good solution for these scenarios:

- BYOD when MDM is not required
- Extending app access to vendors and partners
- Already have an existing MDM solution

When should I require a device to be fully MDM managed?

1. Corporate vs. BYOD
2. What do users need to access?
3. Are there additional security requirements; certificates, S/MIME?

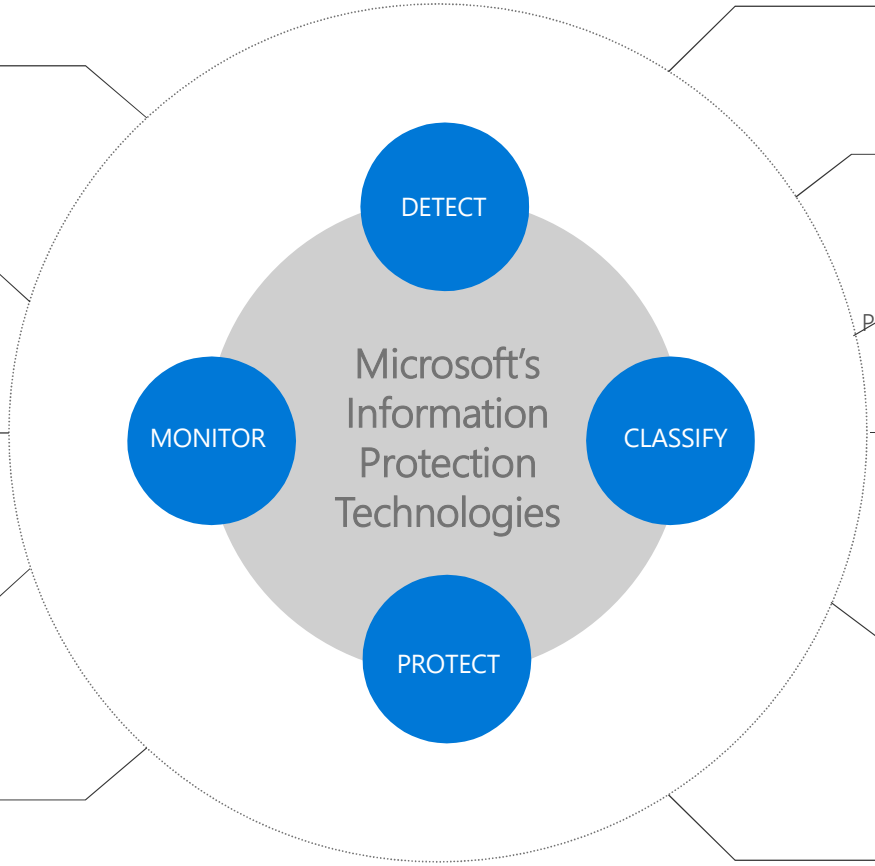
How should I protect data on a managed device?

1. Enrollment Restrictions
2. Windows Security Baseline Settings
3. Windows Hello
4. Encryption
5. Mobile Threat Defense

Microsoft Information Protection

Microsoft Information Protection solutions help you protect sensitive data throughout its lifecycle – inside and outside the organization

MICROSOFT'S INFORMATION PROTECTION SOLUTIONS



MICROSOFT CLOUD APP SECURITY

Visibility into 15k+ cloud apps, data access & usage, potential abuse

OFFICE 365 ADVANCED SECURITY MANAGEMENT

Visibility into Office 365 app usage and potential data abuse

WINDOWS INFORMATION PROTECTION/WD ATP

Separate personal vs. work data on Windows 10 devices and prevent work data from traveling to non-work locations

MESSAGE ENCRYPTION

Send encrypted emails in Office 365 to anyone – inside or outside of the company

CONDITIONAL ACCESS

Control access to files based on policy, such as identity, machine configuration, geo location

AZURE INFORMATION PROTECTION

Classify, label & protect files – beyond Office 365, including on-prem & hybrid

OFFICE 365 DLP

Prevent data loss across Exchange Online, SharePoint Online, OneDrive for Business

OFFICE APPS

Protect sensitive information while working in Excel, Word, PowerPoint, Outlook

ISV APPLICATIONS

Enable ISV partners to consume labels, apply protection

OFFICE 365 ADVANCED DATA GOVERNANCE

Apply retention and deletion policies to sensitive and important data in Office 365

SHAREPOINT & GROUPS

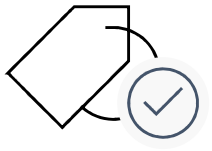
Protect files in libraries and lists

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels

Discover

Scan & detect sensitive data based on policy



Classify

Classify and label data based on sensitivity

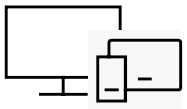
Protect

Apply protection actions, including encryption, access restrictions

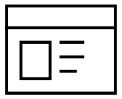
Monitor

Reporting, alerts, remediations

Comprehensive



Devices



Apps

Cloud services

On-premises

Common use cases

Discover and understand the sensitive data across your environment

Accelerate your journey to the cloud by classifying, labeling and protecting data on-premises

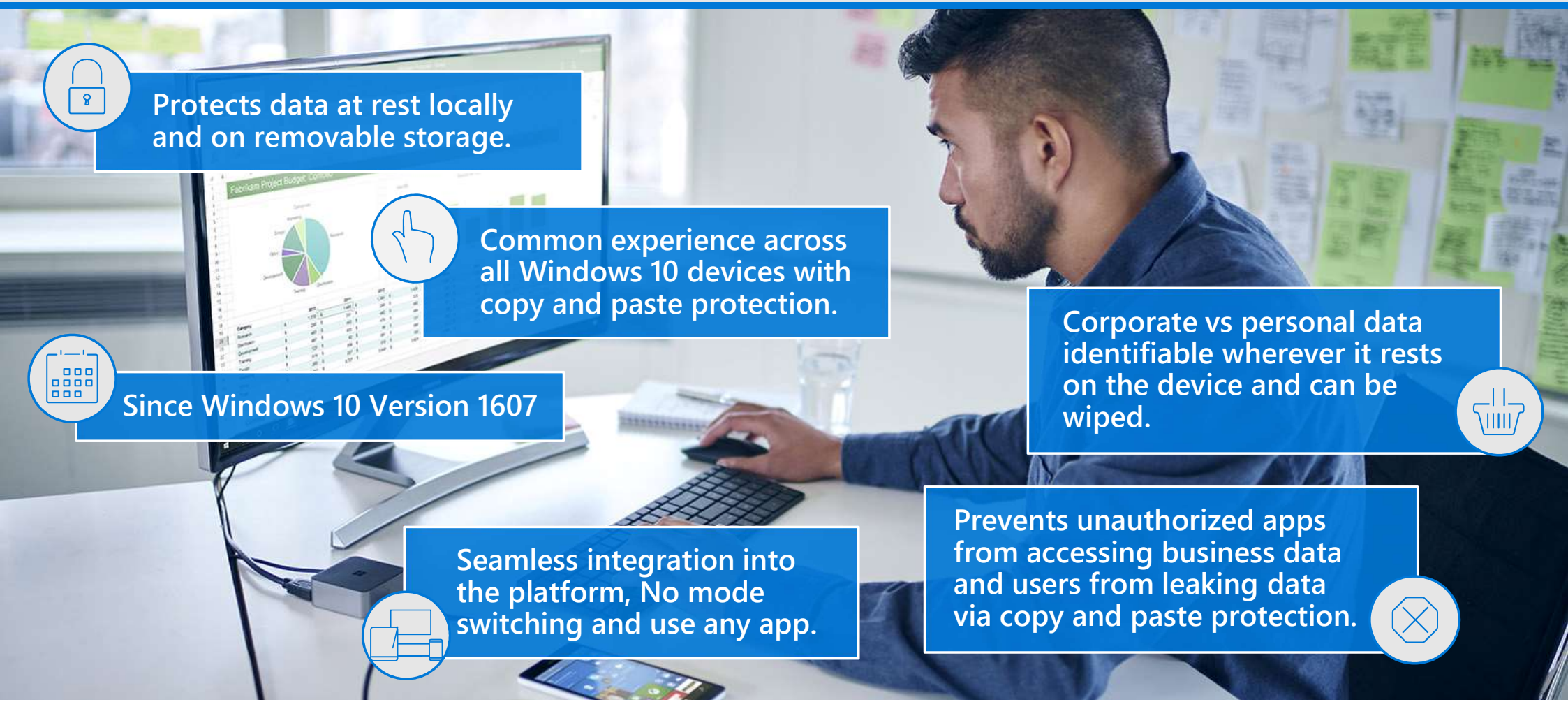
Get control of data sprawl in the cloud by classifying, labeling and protecting files in 3rd-party cloud services

Implement an information protection strategy to meet compliance obligations

Windows Information Protection

WINDOWS INFORMATION PROTECTION

Integrated protection against accidental data leaks



WIP Overview

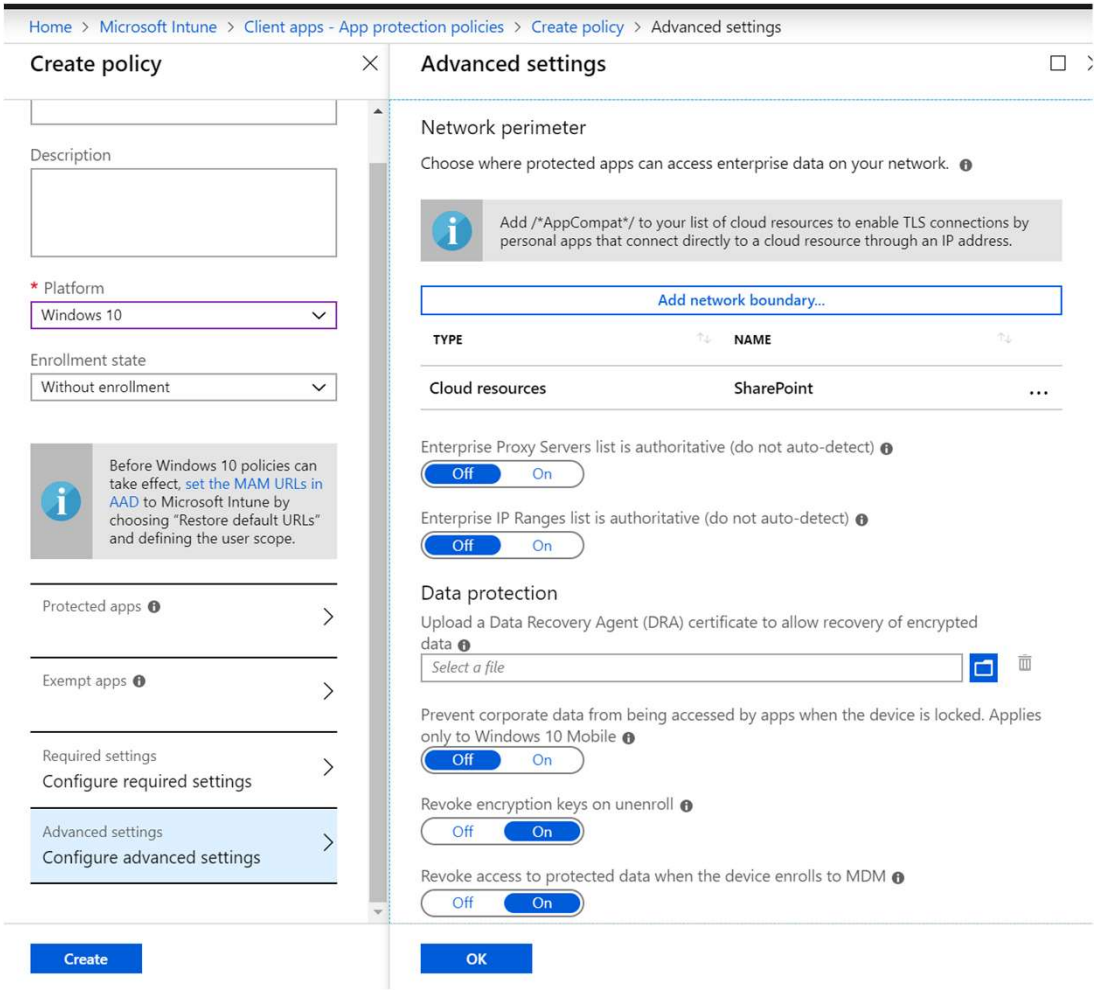
- Windows Information Protection is an extension to the Windows 10 operating system
- Windows Information Protection (WIP) helps protect against additional areas of potential data leakage without interfering with the employee experience.
- WIP uses encryption to protect sensitive (work) content. By encryption it can disallow content to be copy/pasted into other documents. It also allows document to be blocked from sharing using non-protected apps (like e-mail) or storage on non-protected locations (like an USB drive)
- WIP differentiates between corporate and personal data and apps that can exist side by side on the same device
- There are two major components to WIP. There's the application which are allowed to access protected content and there's the location where this content is stored.
- Based on the settings of the policy, users can change the ownership from work to personal and visa versa (less restrictive). Or this ownership is applied automatically (more restrictive). WIP uses a set of content locations (fileshare, cloud storage, and more) to determine if the content is either personal or work related.
- WIP settings are delivered through policies to user devices, which need an MDM or MAM solution that supports WIP

Planning for WIP

- Implementing WIP requires the following prerequisites:
  - Windows 10 version 1607 (Anniversary Edition) or later
  - A MDM or MAM solution that supports the “EnterpriseDataProtection” configuration service provider (CSP) such as Microsoft Intune
  - Windows Client must be enrolled in MDM or registered for MAM
- Once you’ve satisfied your prerequisites, you should plan for the following issues related to your WIP implementation:
  - Determine which Policy protection mode to use:
    WIP has three simple policy enforcement modes. It lets you choose how and whether the user experience in the clipboard, save dialog, and similar data-sharing cases have options (overrides) to move work content to non-work context. You can decide to *Hide Overrides*, *Allow Overrides* for your users, or even deploy in *Silent mode* just for auditing. *Silent mode* does not restrict unmanaged apps from opening work data the way *Hide Overrides* and *Allow Overrides* do
  - Configure your intelligent network boundaries

Implementing WIP

- You can implement WIP by creating WIP policies in Microsoft Intune
- You can select a deployment for MDM (Windows 10 device is enrolled) and for MAM (Windows 10 device is not enrolled)
- To add a new WIP policy in the Azure Portal:
  1. Go to the Azure Portal
  2. Select All Services, type Intune and click it from the Service tab
  3. Open the Mobile apps from Manage
  4. Open the App protection policies from Manage
  5. Click Add a policy on the top to open the next tab



Business/Personal

One experience

Data is isolated

Data is encrypted at rest

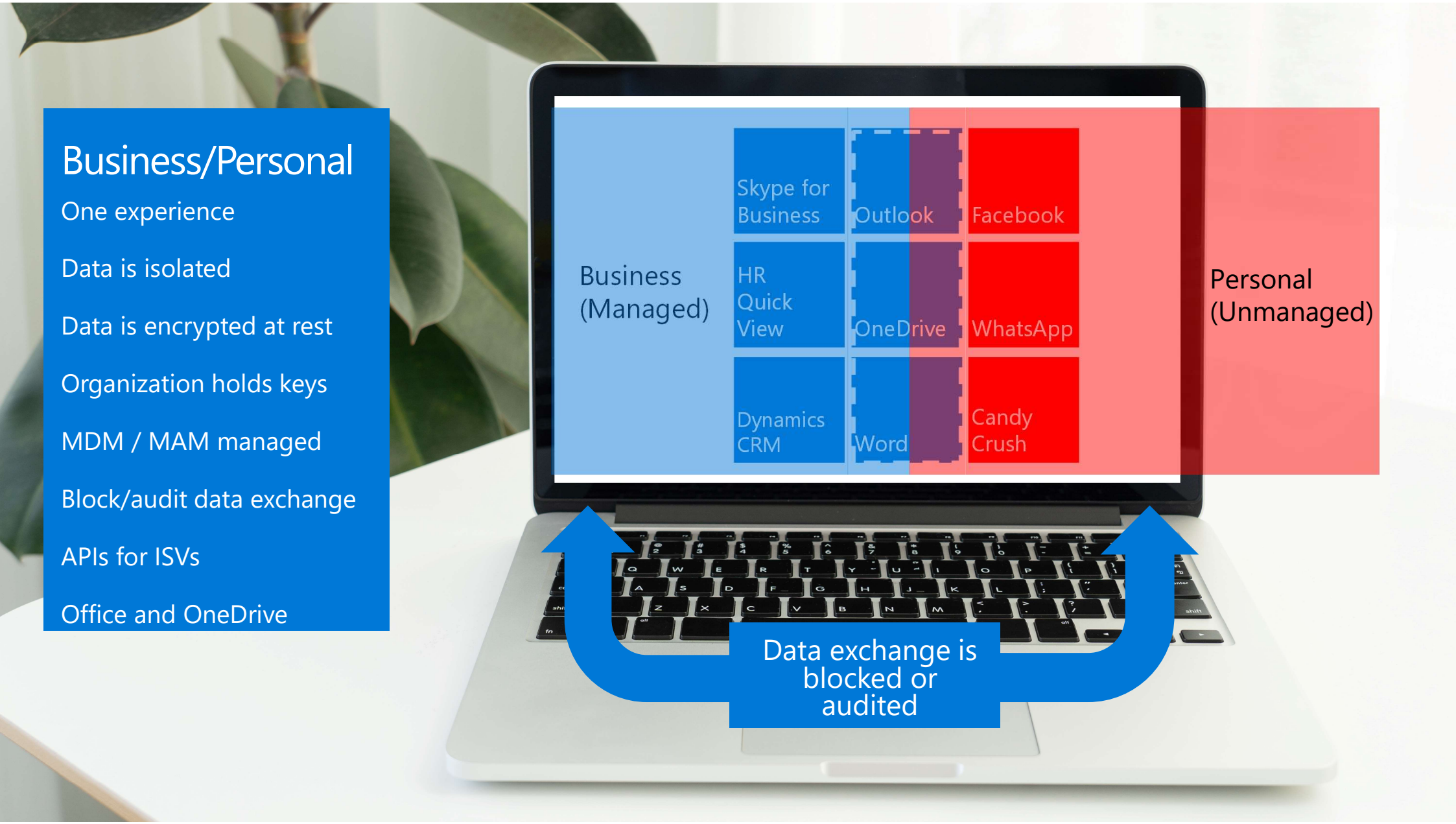
Organization holds keys

MDM / MAM managed

Block/audit data exchange

APIs for ISVs

Office and OneDrive



Enlightened Applications

Unenlightened Applications – How to manage

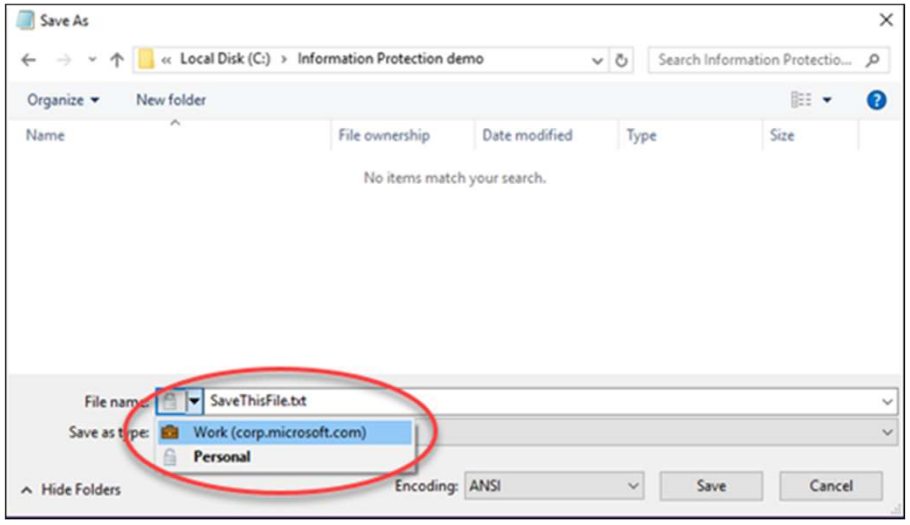
- Option 1: Use Allow policy
  - *Caution:* Auto-encrypts all files touched
  - Intended for Line of Business (LOB) apps
  - Can include in policy for fully managed devices

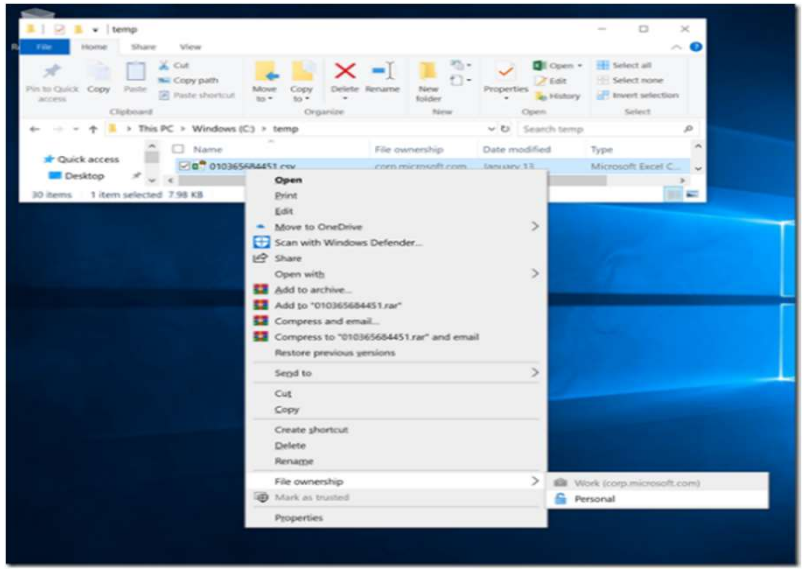
- Option 2: Use Exempt policy
  - WIP rules don’t apply to the app
  - Access work without impacting personal data

- Option 3: Enlighten the app
  - See: http://aka.ms/wip-dev-guide

Working with WIP in Windows Desktop

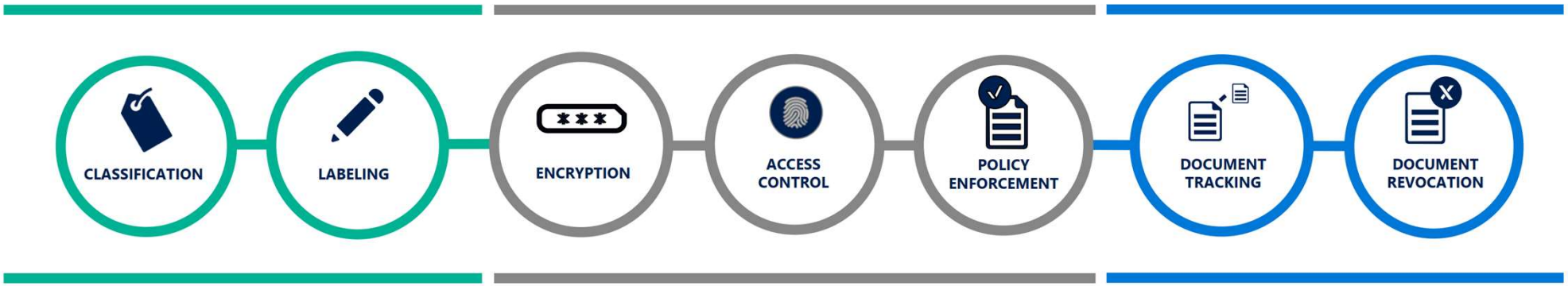
- The terms “Enlightened” and “Non-Enlightened” (or Unenlightened) describe applications with full support of separation between corporate and personal data and applications that can only recognize all their data as corporate work data





Azure Information Protection

The evolution of Information Protection



Classification & labeling

Protect

Monitor & respond

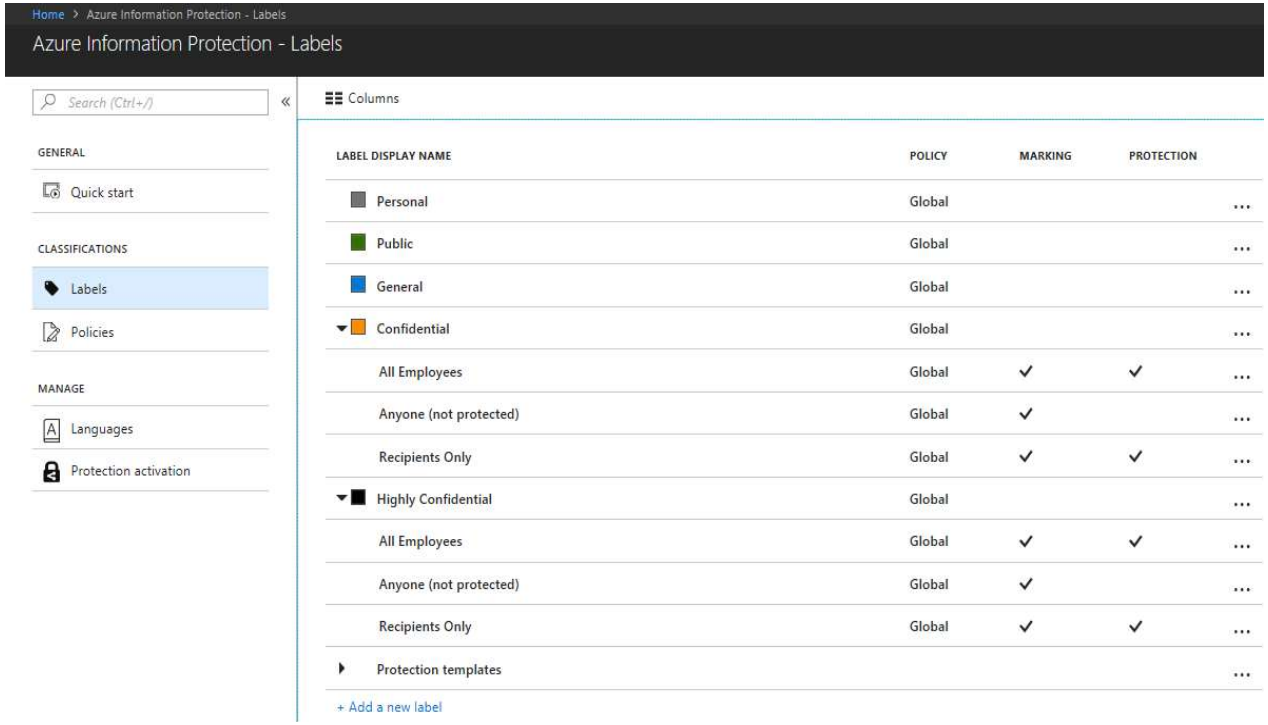
Planning AIP Solution

For AIP deployment, organizations must consider the following planning and configuration steps:

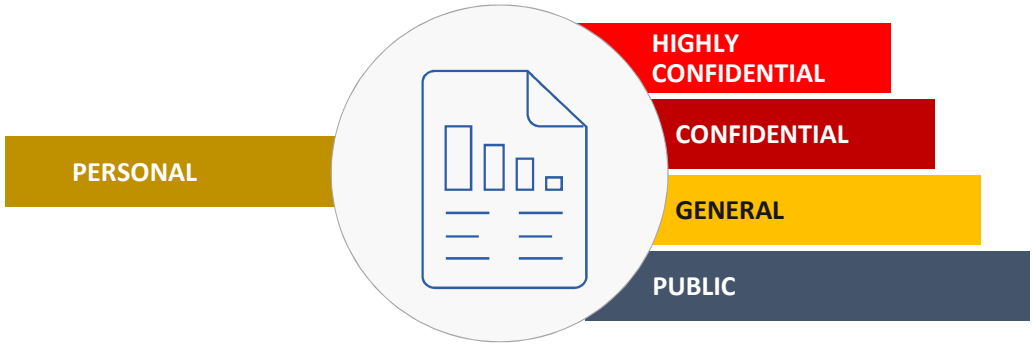
1. Prepare the Tenant for Azure Information Protection
2. Customize labels and policies
3. Deployment of Azure Information Protection client
4. Configure Rights Management and participating services
5. Rolling out AIP to the end users

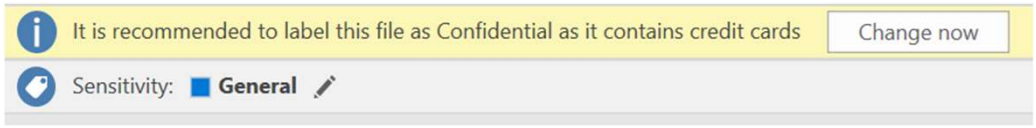
AIP Labels Overview

- Labels contain different settings on how to mark and optionally protect documents, files, and emails that are sent to your end users
- Sub-labels can add additional settings to a label
- Before customizing labels, you must create your classification strategy
- Azure Information Protection provides a set of Default labels and policies that are created when you activate AIP for your tenant



Classification and labeling





Automatic classification

Policies can be set by IT Admins for automatically applying classification and protection to data.

Recommended classification

Based on the content you're working on, you can be prompted with suggested classification.

Manual reclassification

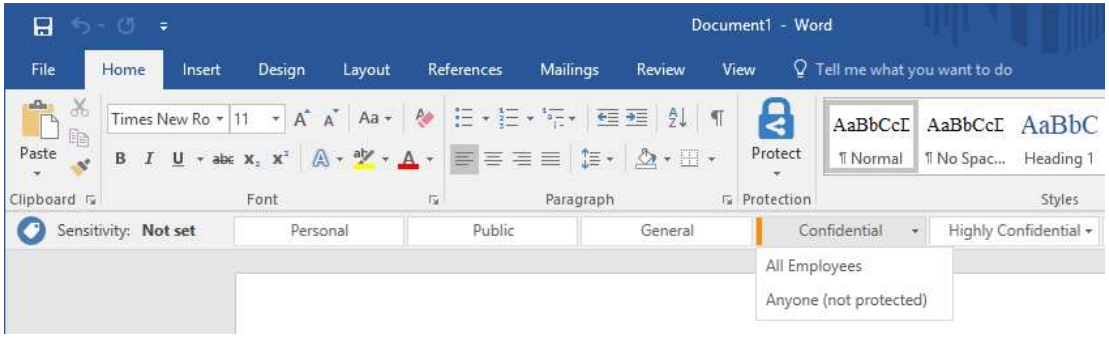
You can override a classification and optionally be required to provide a justification.

User-specified classification

Users can choose to apply a sensitivity label to the email or file they are working on with a single click.

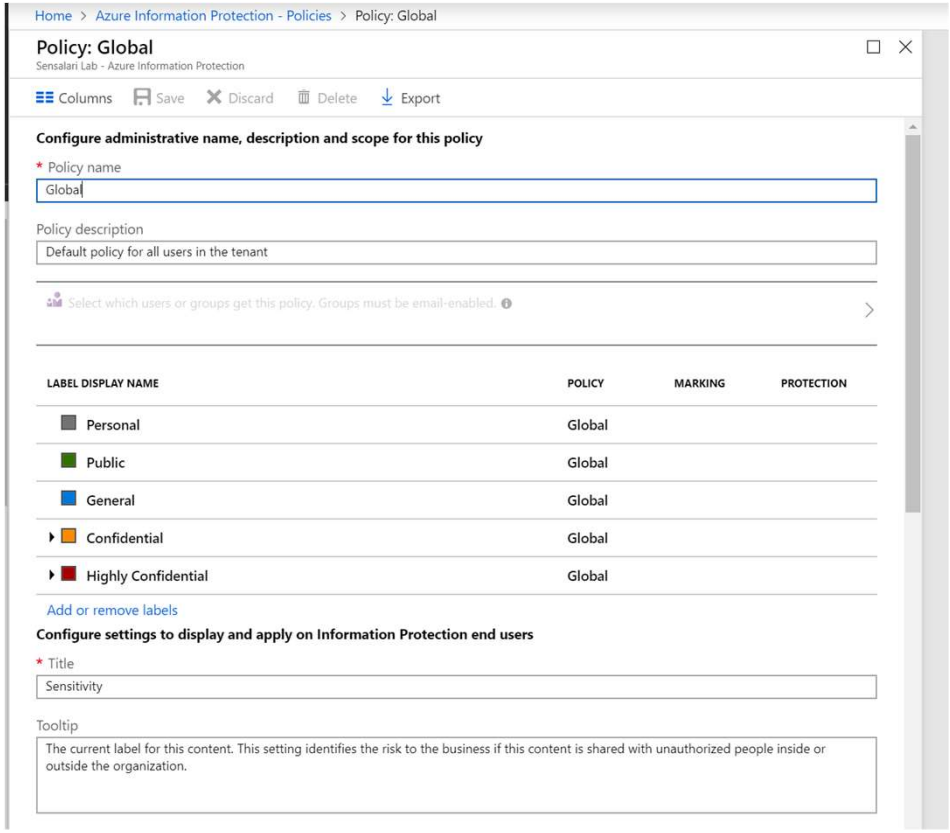
Working with AIP Labels

- You can see your configured labels and sub-labels when opening suported Office application on a client that has the Azure Information Protection client installed
- You can use Azure Portal to create additional labels (and sub-labels) with special settings for your users



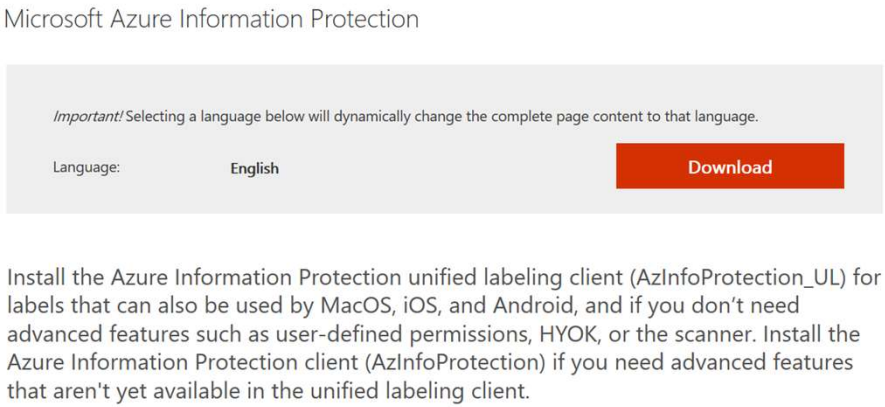
Configuring AIP Policies

- A policy is an additional set of rules that are used to group labels to be available for users or groups
- All predefined labels and sub-labels in Office 365 are configured in the default policy named “Global”
- You cannot scope Global policy to any specific users or groups
- The following rules apply when creating new policies:
  - Custom labels can be added to only one policy
  - To add a sub-label, its parent label must be in the same policy or in the global policy
- The Azure Information Protection client checks for any changes whenever a supported Office application starts



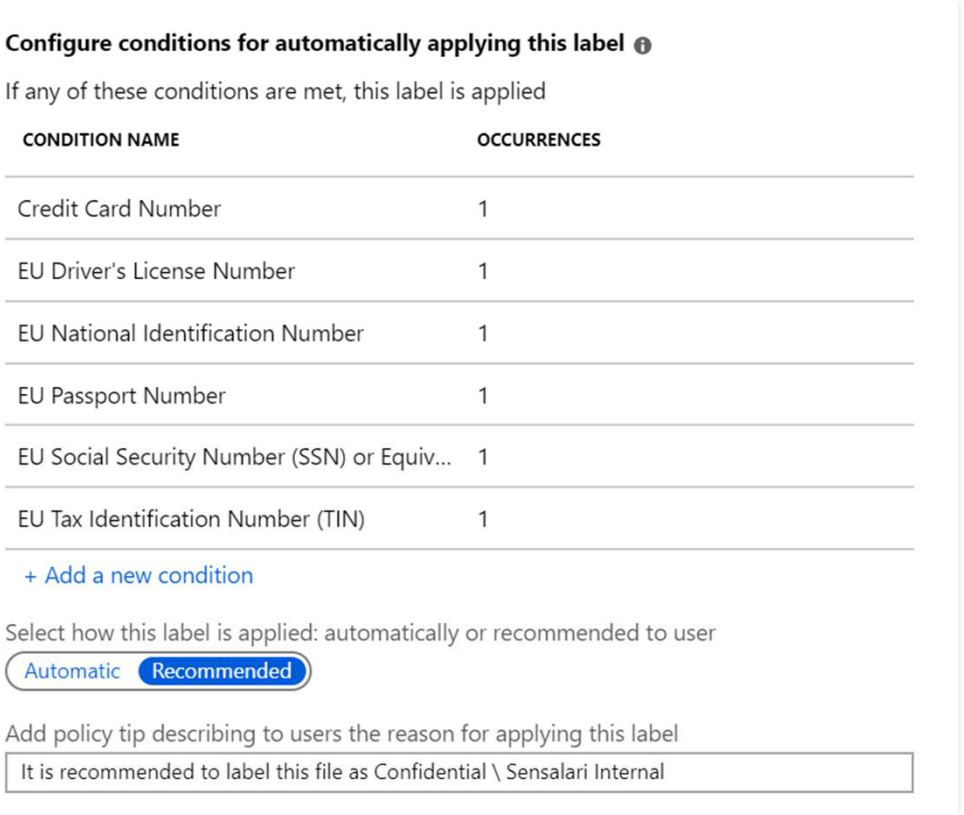
Deploying AIP Clients

- The AIP client for Windows is a client for organizations that use Azure Information Protection to classify and protect documents and emails
- AIP client also has a viewer for organizations that don’t have their own information protection infrastructure but want to consume protected content
- The stand-alone Azure Information Protection viewer app is available for Windows, Mac, Windows Phone, Android and iOS
- Rolling out the client is possible through Windows Update because it is included as both an executable (.exe) and a Windows Installer file (.msi) in the Microsoft Update catalog



Configuring Automated Labeling

- The automatic labeling feature can assign labels to documents, files, and emails without user interaction when configured conditions are fulfilled
- Automatic labeling consists of:
  - Conditions for applying labels automatically
  - Automatic processing and recommendations for emails with attachments
  - The on-premises Azure Information Protection scanner to label local documents and files
- The automatic labeling requires an Azure Information Protection Premium P2 license, which is included in the license bundle Enterprise Mobility + Security E5



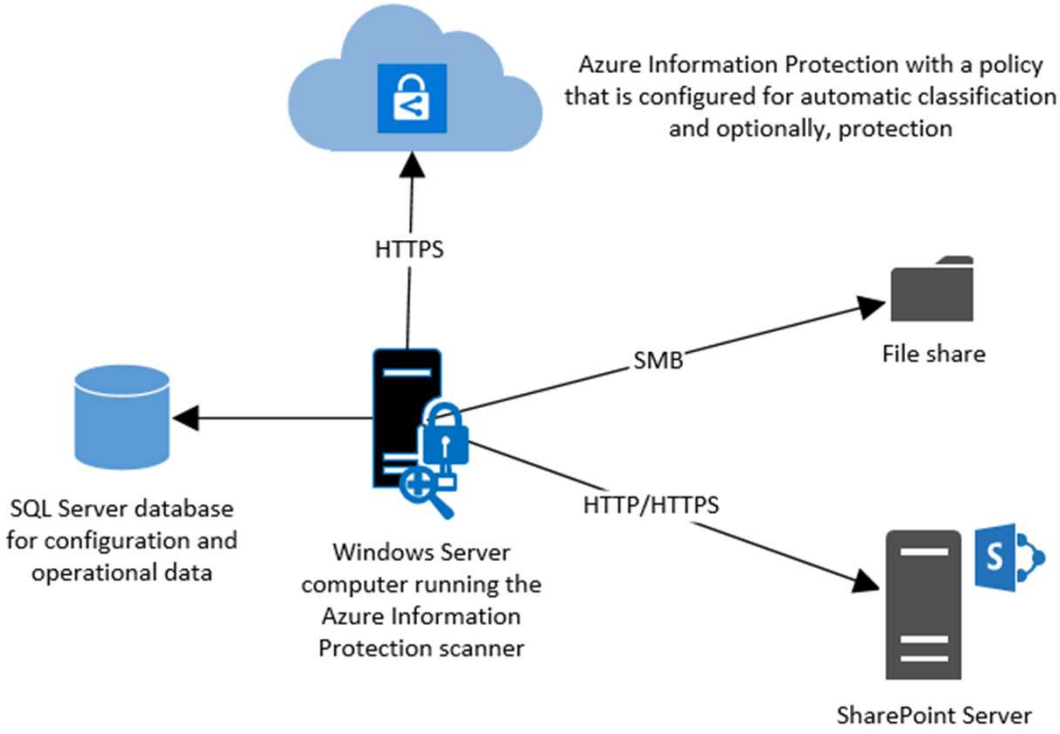
Configuring a Super User

- The Super User feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects
- The Super User feature is a feature to access all protected content of your tenant
- By default, the super user feature is not enabled
- The Super User is configured with the PowerShell cmdlets from the AADRM module
- You use **Enable-AadrmSuperUserFeature** cmdlet to enable this feature

Implementing Bulk Classification

- The Azure Information Protection scanner is a tool for automatic labeling and classification of files and documents from on-premises file shares and SharePoint servers

- The Azure Information Protection scanner can work as an extension to a Windows Server File Classification Infrastructure (FCI)
- The scanner is installed on a Windows Server with access to the on-premise environment containing the file shares and SharePoint libraries to label



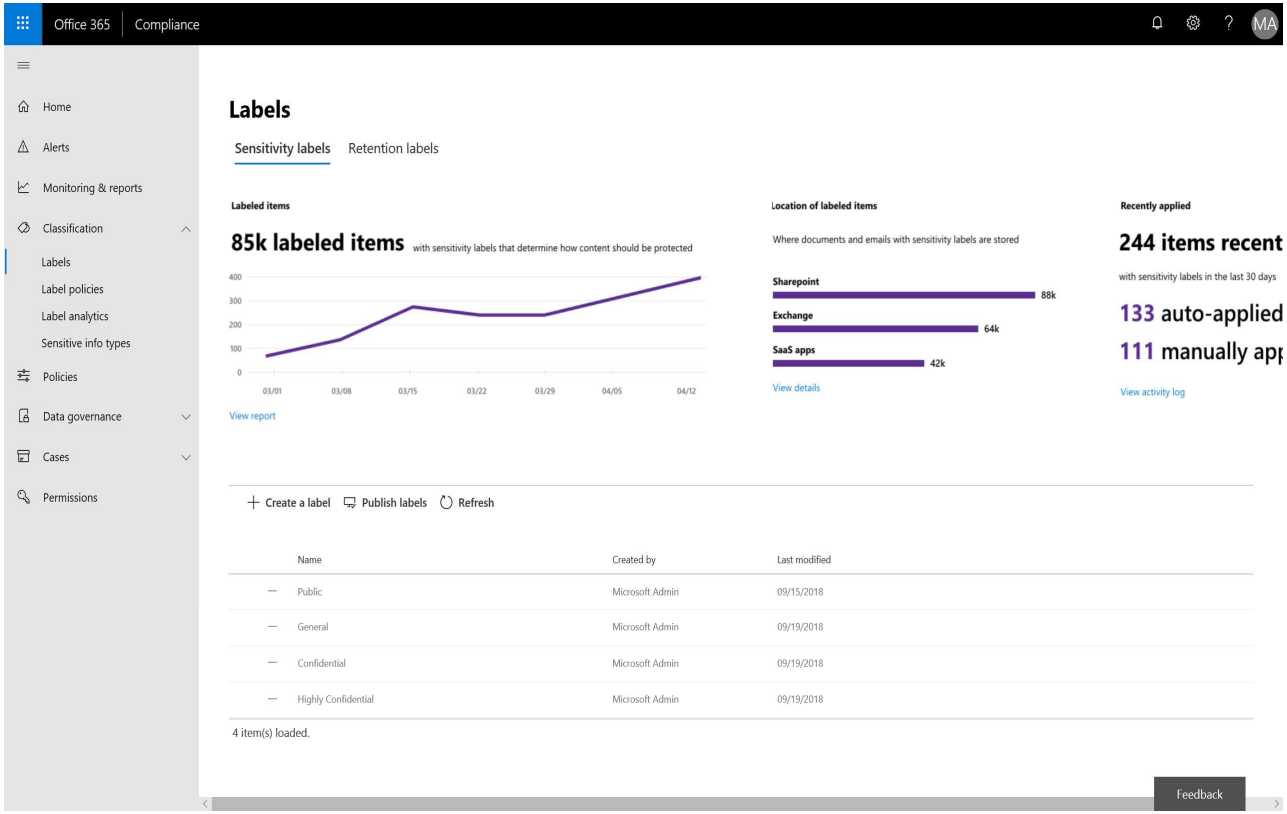
Available Now

Unified labeling across Office 365, Azure and Windows Information Protection

Centralized management
Configure and manage labels across apps and services in Office, Azure and Windows – all from the Security & Compliance Center

Unified classification
Uniform content classification to protect and preserve data across Office, Azure, Windows

Consistent across M365 & extensible to 3rd party
Consistent integration and experience across M365 apps & services. Extensible to 3rd party apps & solutions



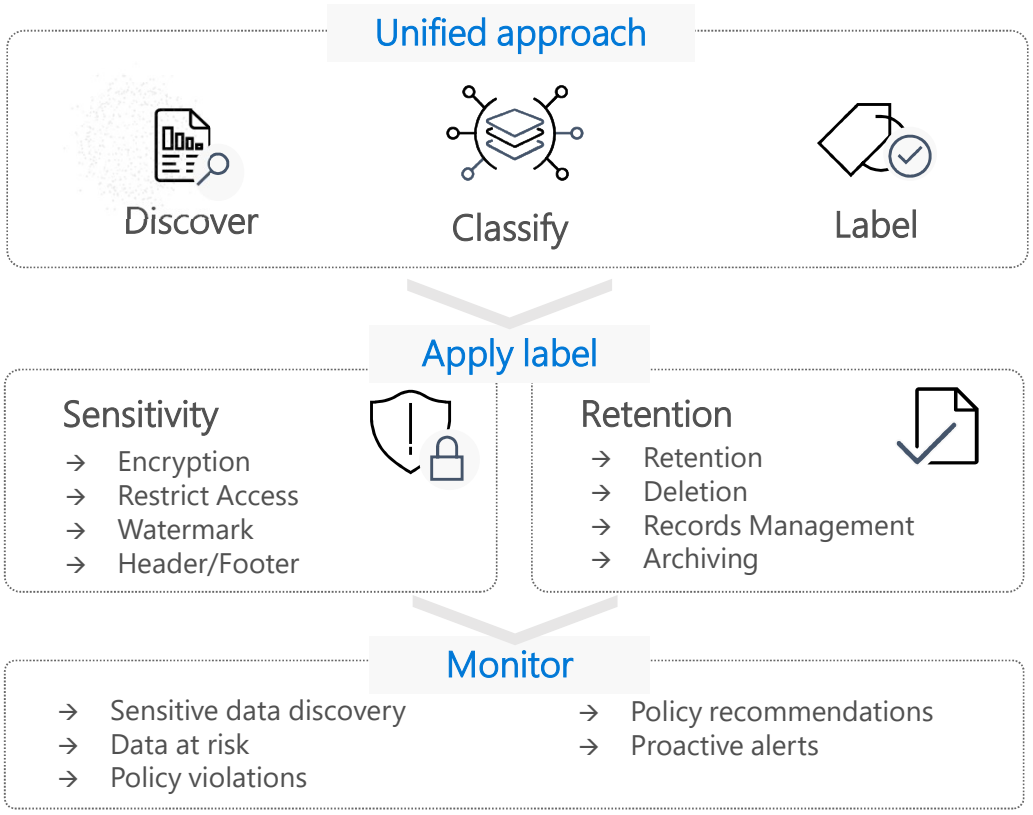
Data protection & data governance go hand-in-hand

Unified approach to discover, classify & label

Automatically apply policy-based actions

Proactive monitoring to identify risks

Broad coverage across locations



What is a sensitivity label?

Tag that is customizable,
in cleartext,
and persistent.

It becomes the basis for applying and enforcing data protection policies.

In files and emails, the label is persisted as document metadata

In SharePoint Online, the label is persisted as container metadata

Office 365 Message Encryption

Secure communication with anyone…

Inside your organization

Between your business partners

With any of your customers

…on any device, in any email client

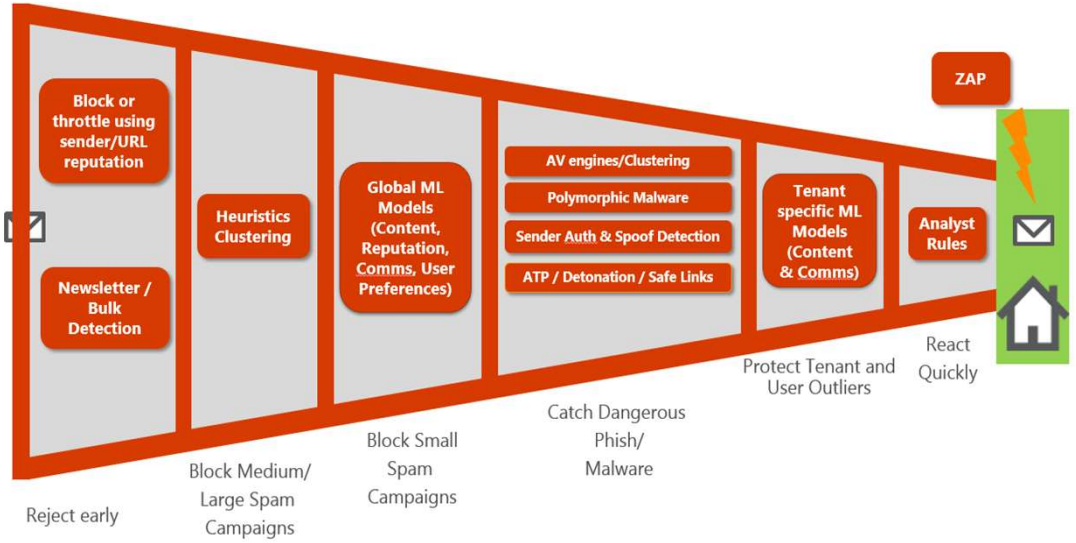
Secure enterprise productivity with Office 365 Advanced Threat Protection

Exchange EOP and Office 365 ATP

- Microsoft 365 tenants that have mailboxes hosted in Exchange Online rely on the Exchange Online Protection (EOP) service to route inbound and outbound mail
- Together, EOP and Microsoft 365 ATP provide a complete solution for protecting users against cyberthreats originating in email
- Advanced Threat Protection (ATP) extends the protection provided by EOP by filtering targeted attacks that could pass through EOP's line of defenses, including advanced threats such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs

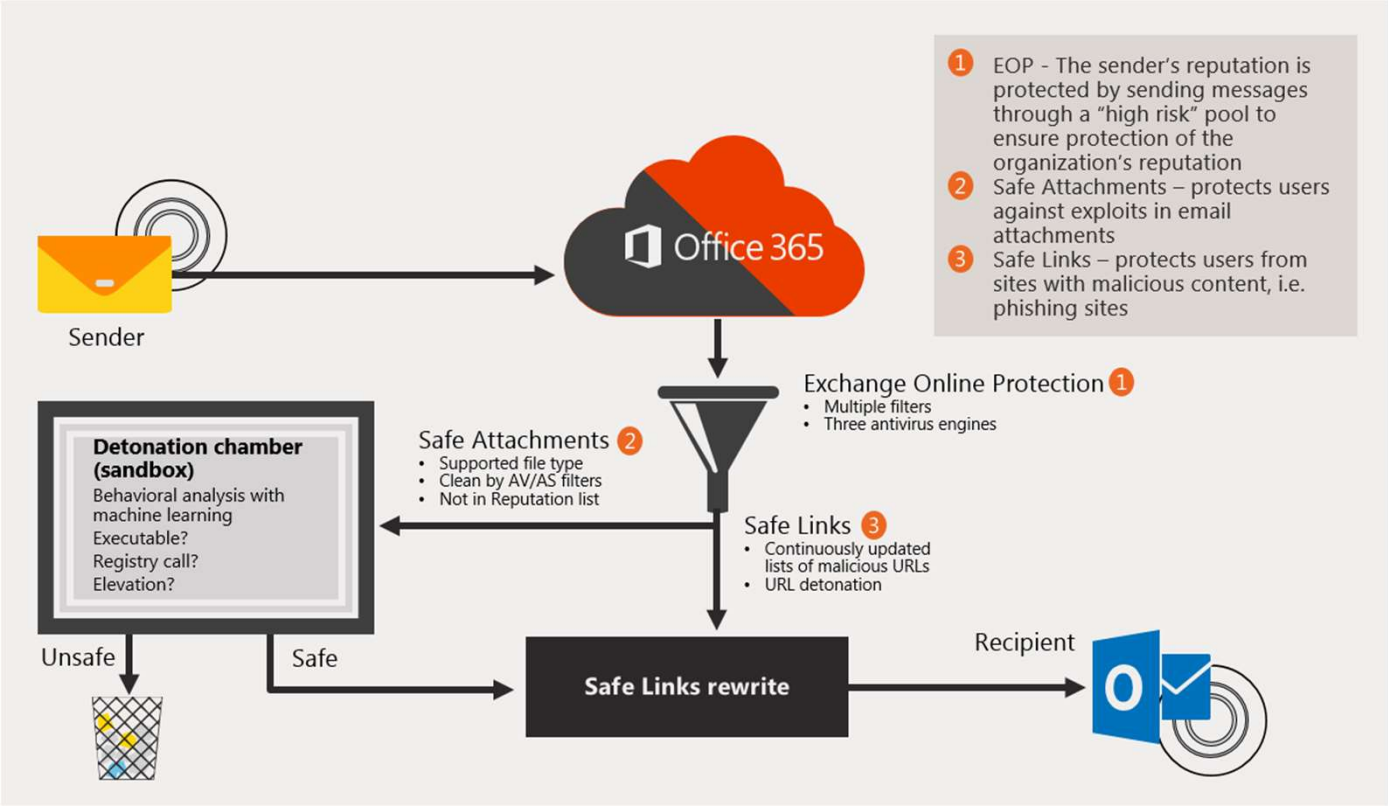
The Anti-Malware Pipeline in Microsoft 365

1. Before mail enters the Microsoft 365 network and is processed by EOP, techniques such as IP and sender reputation, combined with heuristics
2. After that, it is scanned by multiple signature-based anti-virus scanners
3. Next, EOP scans individual files using a reputation block
4. Heuristic clustering is used to identify mail as suspicious simply based on an analysis of delivery patterns
5. Once these signals are collected, the results are run through a machine-learning (ML) model
6. If Microsoft 365 Advanced Threat Protection (ATP) is enabled in the tenant, ATP extends the protection of EOP



How ATP expands protection provided by EOP

Once email passes through the front-line defenses provided by EOP, it is further analyzed by ATP's Safe Attachments and Safe Links features for anything suspicious



Safe Attachments

- Safe Attachments is a feature in Microsoft 365 ATP that opens every attachment of a supported file type in a special hypervisor environment, checks to see if the attachment is malicious, and then takes appropriate action
- Safe Attachments will analyze attachments that are common targets for malicious content
- Selecting attachments to test
- Attachment testing

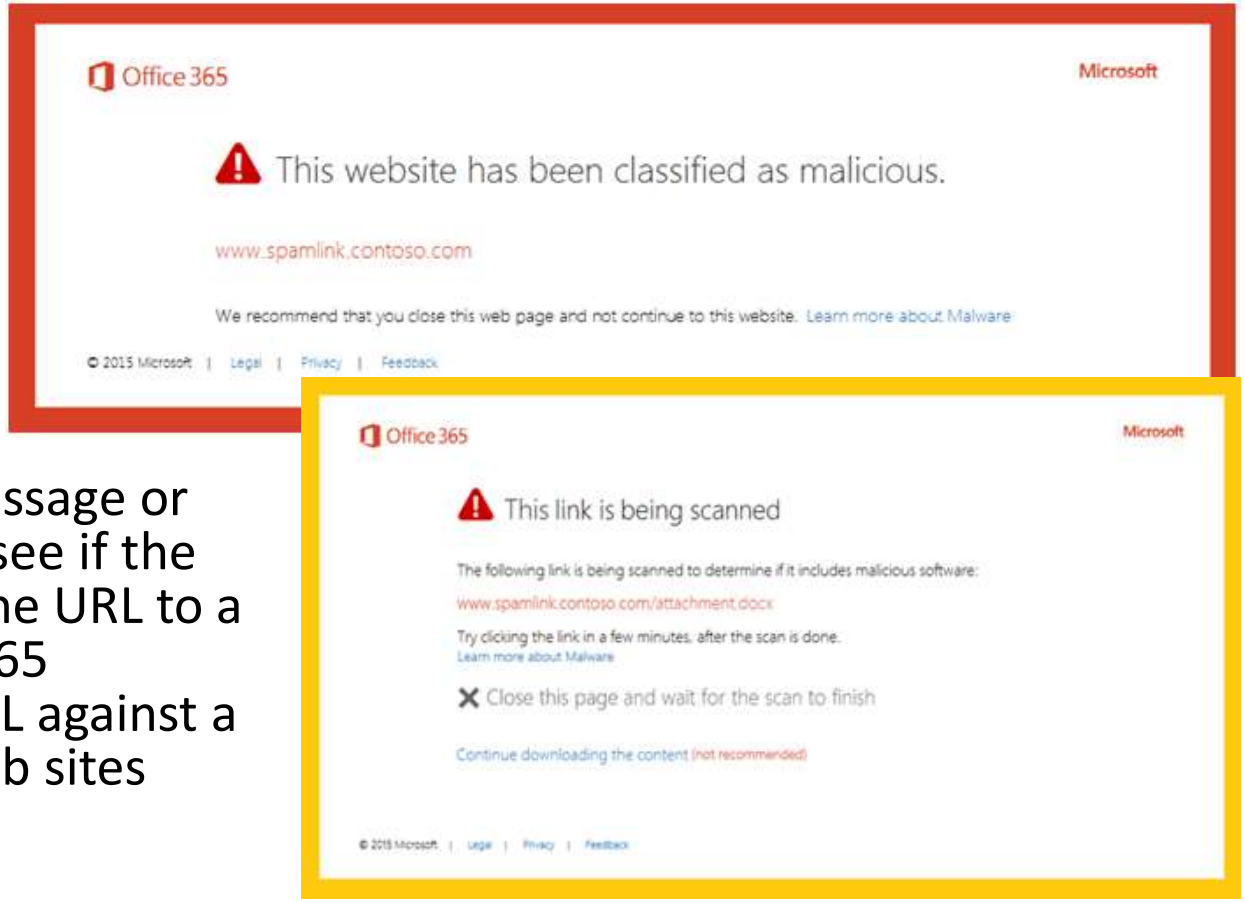
Safe Attachments Policy Options

ATP Safe Attachments policy options:

- Off
- Monitor
- Block
- Replace
- Dynamic Delivery
- Enable redirect

Safe Links

- Safe Links is a feature in ATP that protects users from malicious URLs that are commonly used in phishing attacks to extract sensitive information from a user



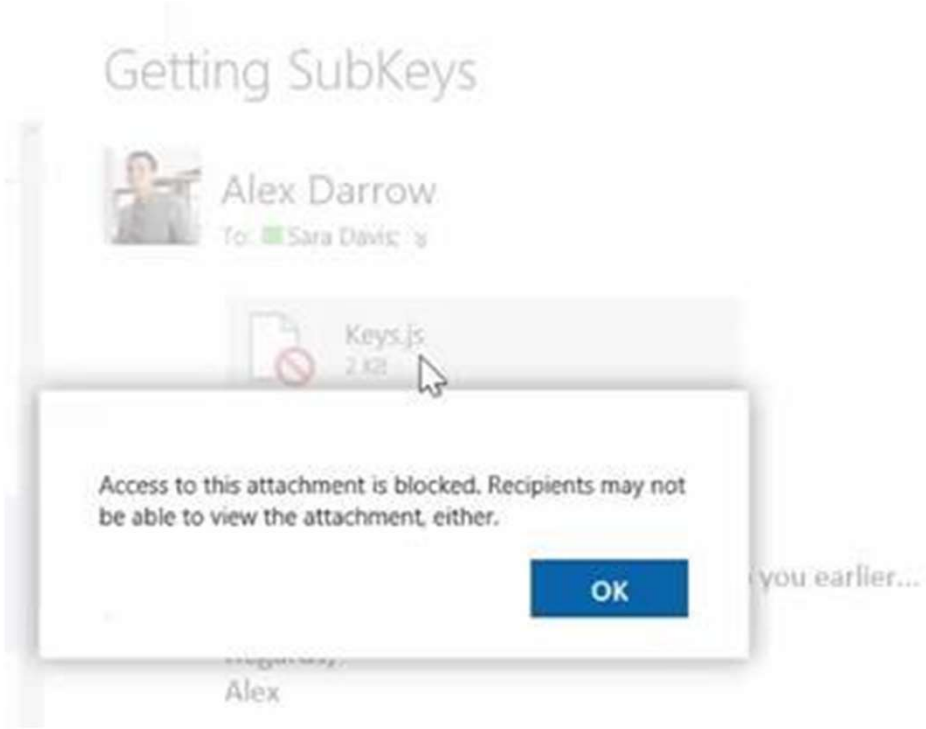
- When a user clicks a link in a message or document, Safe Links checks to see if the link is malicious by redirecting the URL to a secure server in the Microsoft 365 environment that checks the URL against a block list of known malicious web sites

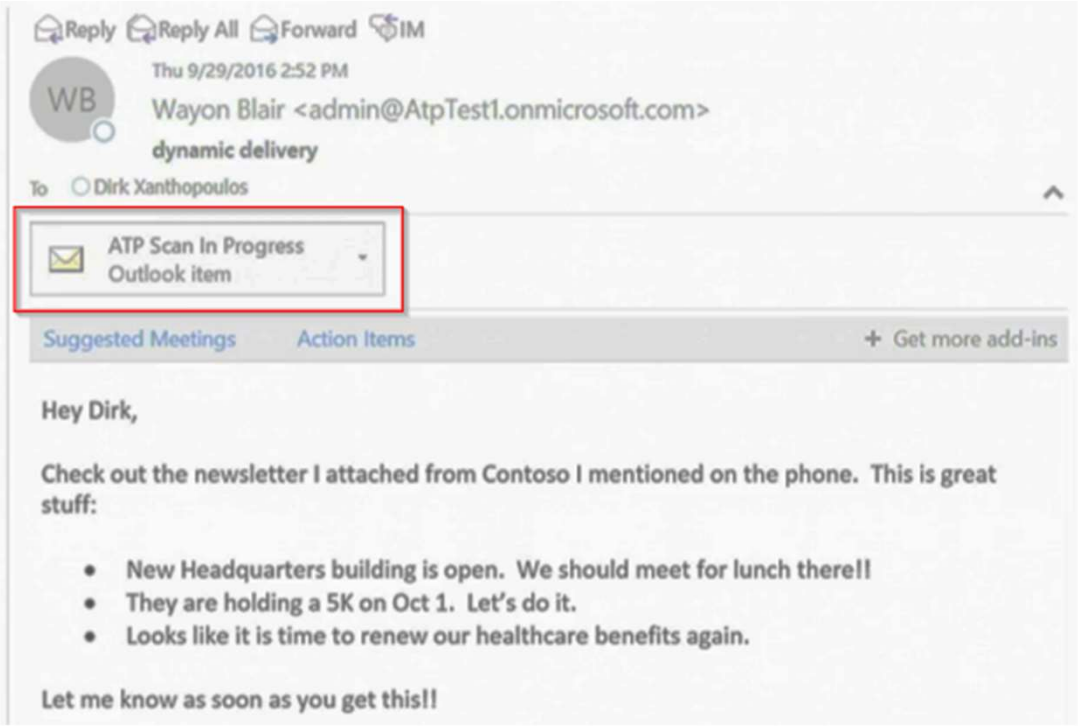
Safe Links Policy Options

ATP Safe Links policy options:

- Block the following URLs
- Office 2016 on Windows
- Don't track when users click ATP safe links
- Don't let users click through ATP safe links to original URL
- Use Safe Attachments to scan downloadable content
- Apply safe links to messages sent within the organization
- Do not track user clicks
- Do not allow users to click through to original URL
- Do not rewrite the following URLs

End-User Experience with Safe Attachments





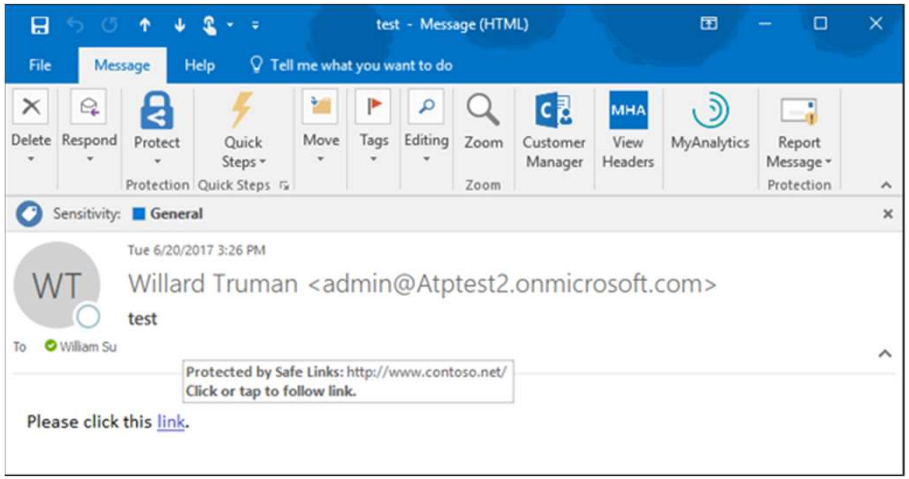
End-User Experience with Safe Links

Safe Links works in email by executing following steps:

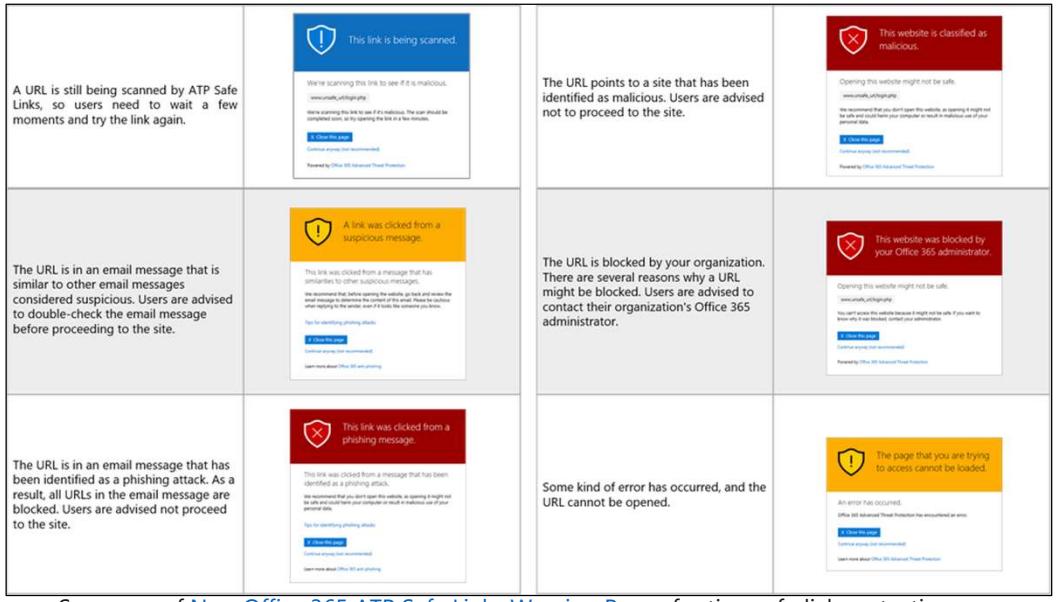
1. Someone sends a user an email message that contains a URL to a web site.
2. The message flows through the anti-malware pipeline, and assuming it passes through all the initial checks, it eventually arrives in the recipient's inbox.
3. The user opens the message and clicks the link.
4. When the user clicks the link, the URL is redirected to a secure server that checks the URL against a block list of known malicious web sites.
    1. If the link is safe, the user's browser navigates to the target web site.
    2. If the link is malicious, the user's browser displays a warning page.

Securing the end user

- Critical to combating phishing and social engineering related attack vectors.
- Native protection built right into Office 365.
- Strong complement to your end user awareness and security training.
- Protection that extends to collaboration scenarios across desktop, web/online, and mobile clients.



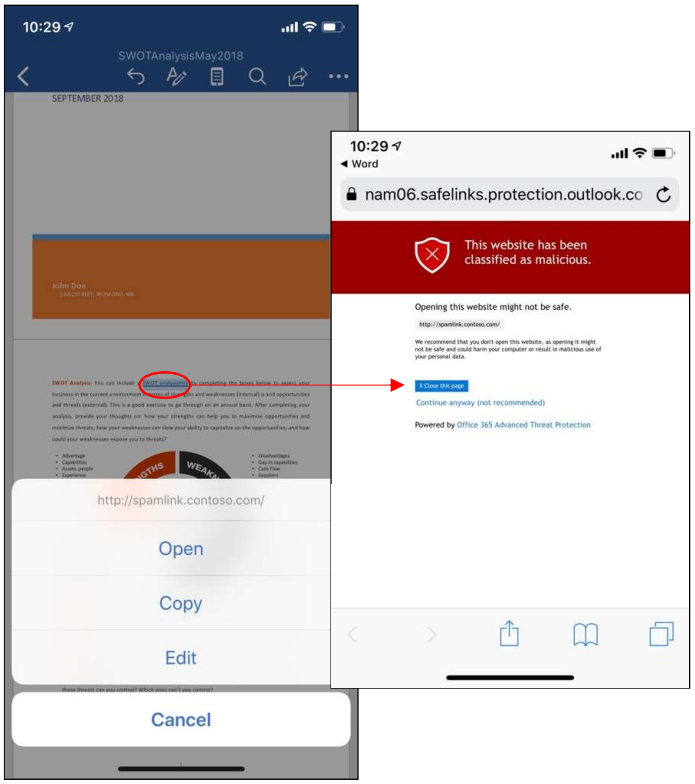
Office 365 ATP Safe Links: Native Link rendering showing the original URL in **Outlook**



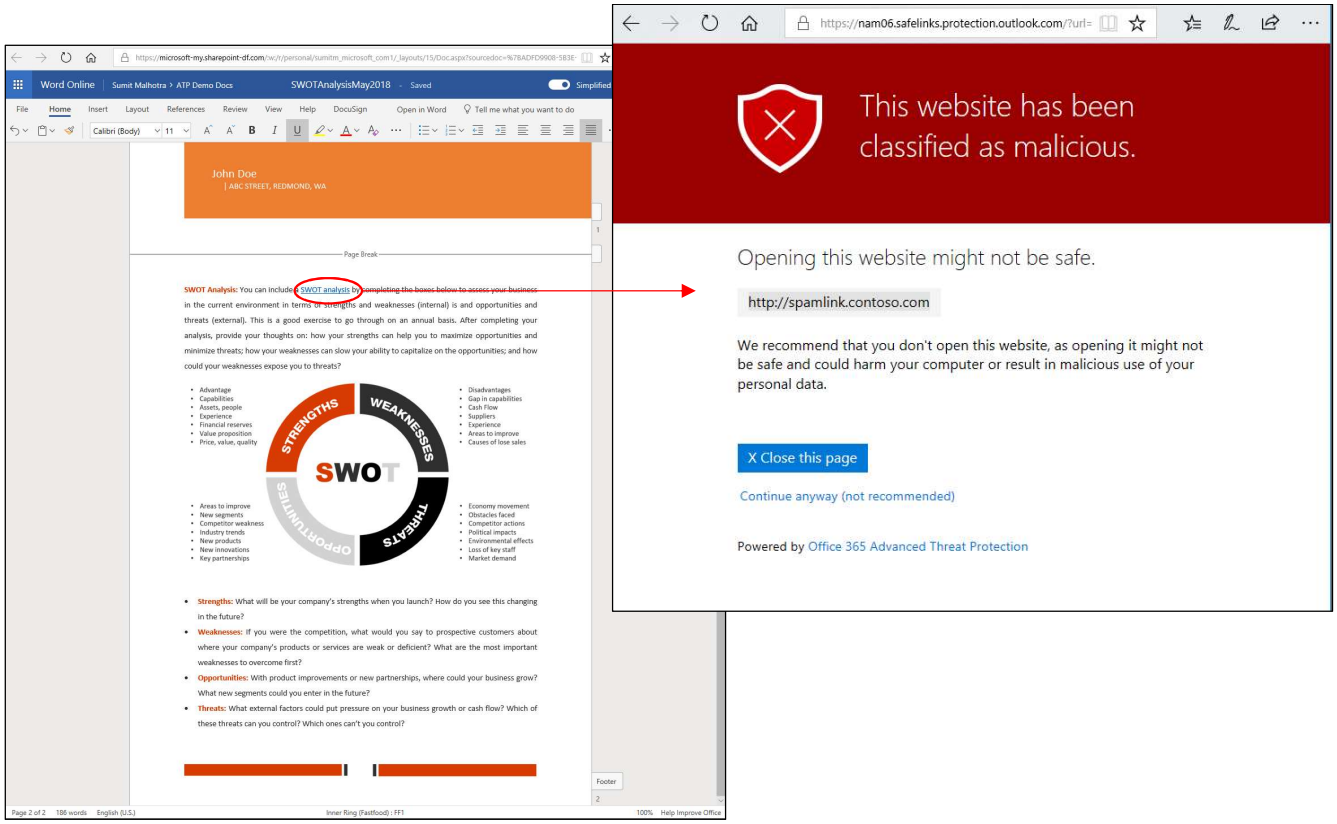
Summary of New Office 365 ATP Safe Links Warning Pages for time-of-click protection

Securing your productivity scenarios:

Office clients and Office online



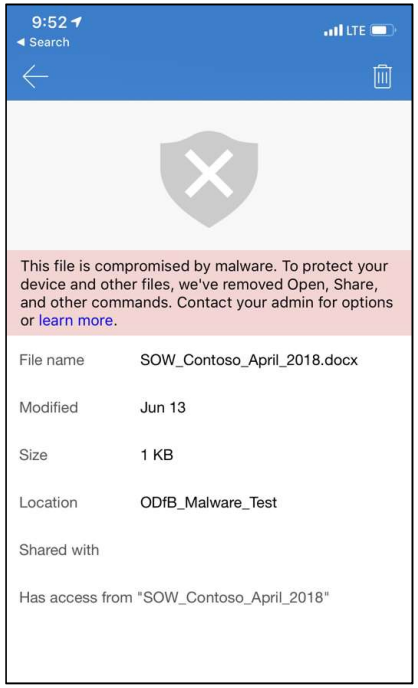
Word iOS client showing **Office 365 ATP Safe Links** block from a click within a document.



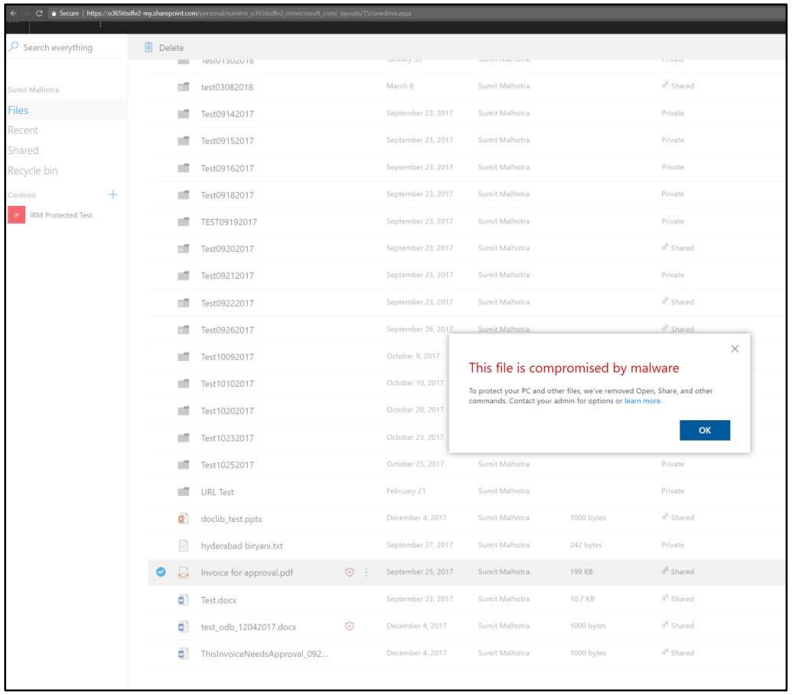
Word Online showing **Office 365 ATP Safe Links** block from a click within a document.

Securing your collaboration scenarios:

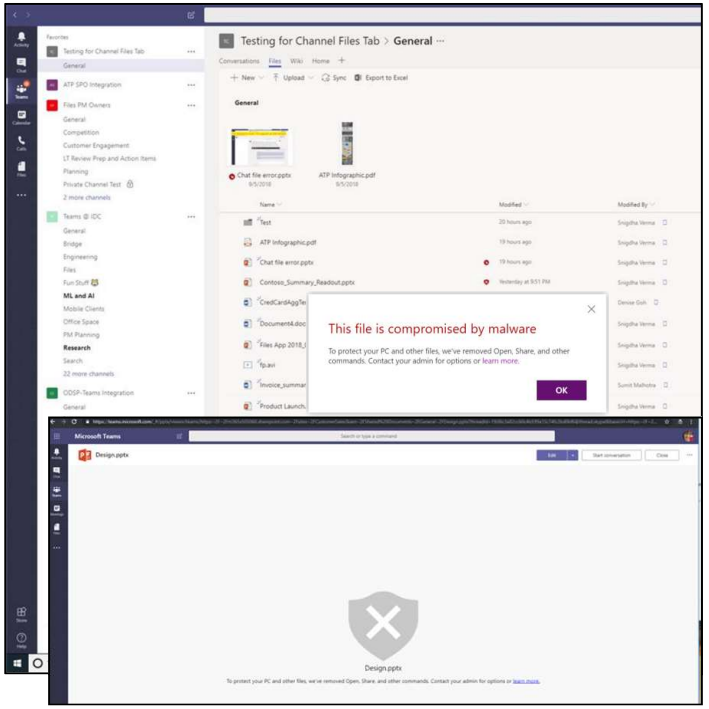
SharePoint Online, OneDrive for Business and Microsoft Teams



OneDrive iOS app showing files detected and blocked by Office 365 ATP



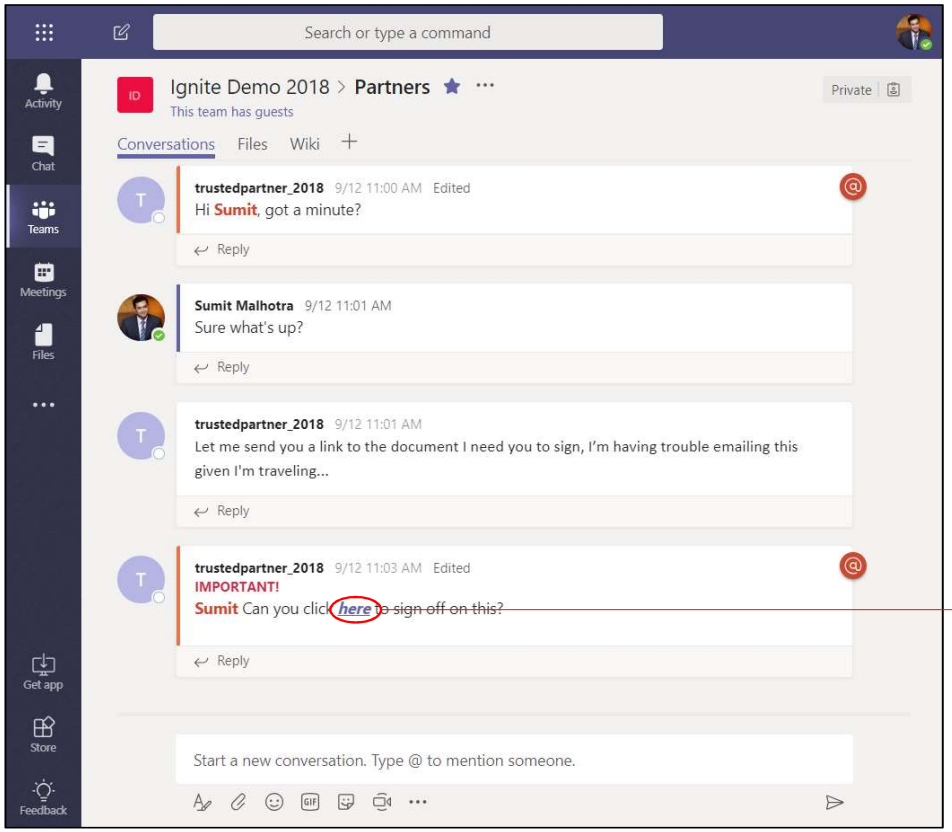
SharePoint Online WebUX showing files detected and blocked by Office 365 ATP



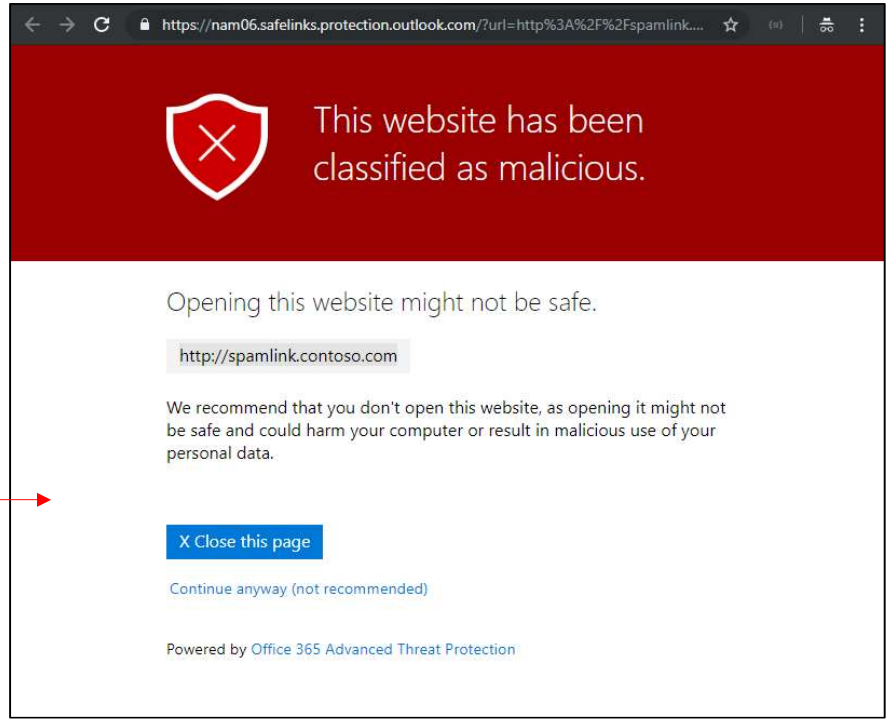
Microsoft Teams desktop client showing files detected and blocked by Office 365 ATP

Securing your collaboration scenarios:

Office 365 ATP Safe Links protection in Microsoft Teams



Malicious URL in conversations from Guest/External user in **Teams desktop client**



Office 365 ATP blocks a malicious link click from **Teams desktop client**


Microsoft 365
Grazie