

Adopting Microsoft 365 E5

Chris Gecks

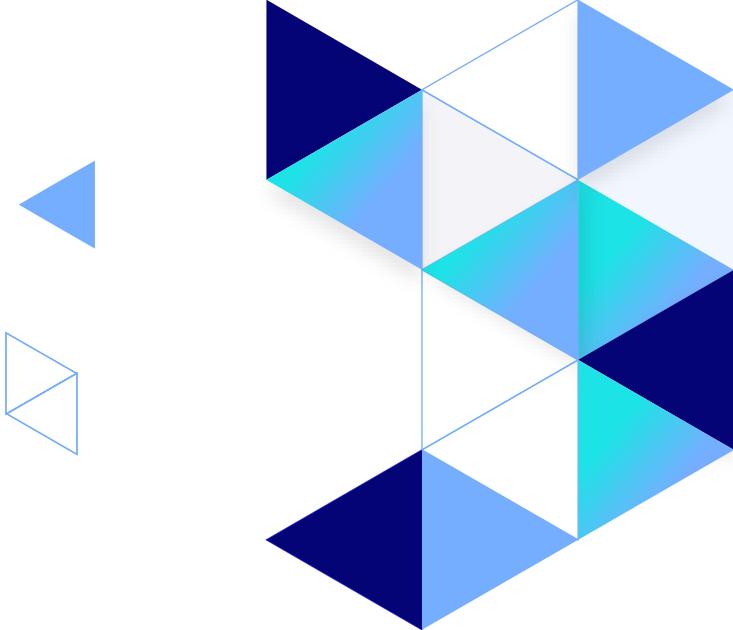
Solutions Architect / Consultant

chris.gecks@cybercx.com.au



Agenda

-
- 01 Introduction
 - 02 Microsoft 365 Journey
 - 03 Microsoft Licensing & Zero Trust
 - 04 Microsoft Defender
 - 05 Microsoft Purview
 - 06 Questions



Microsoft 365 Journey of Discovery



2007: BPOS is Born



2011: Office 365 GA



2013: Office 365 Updated

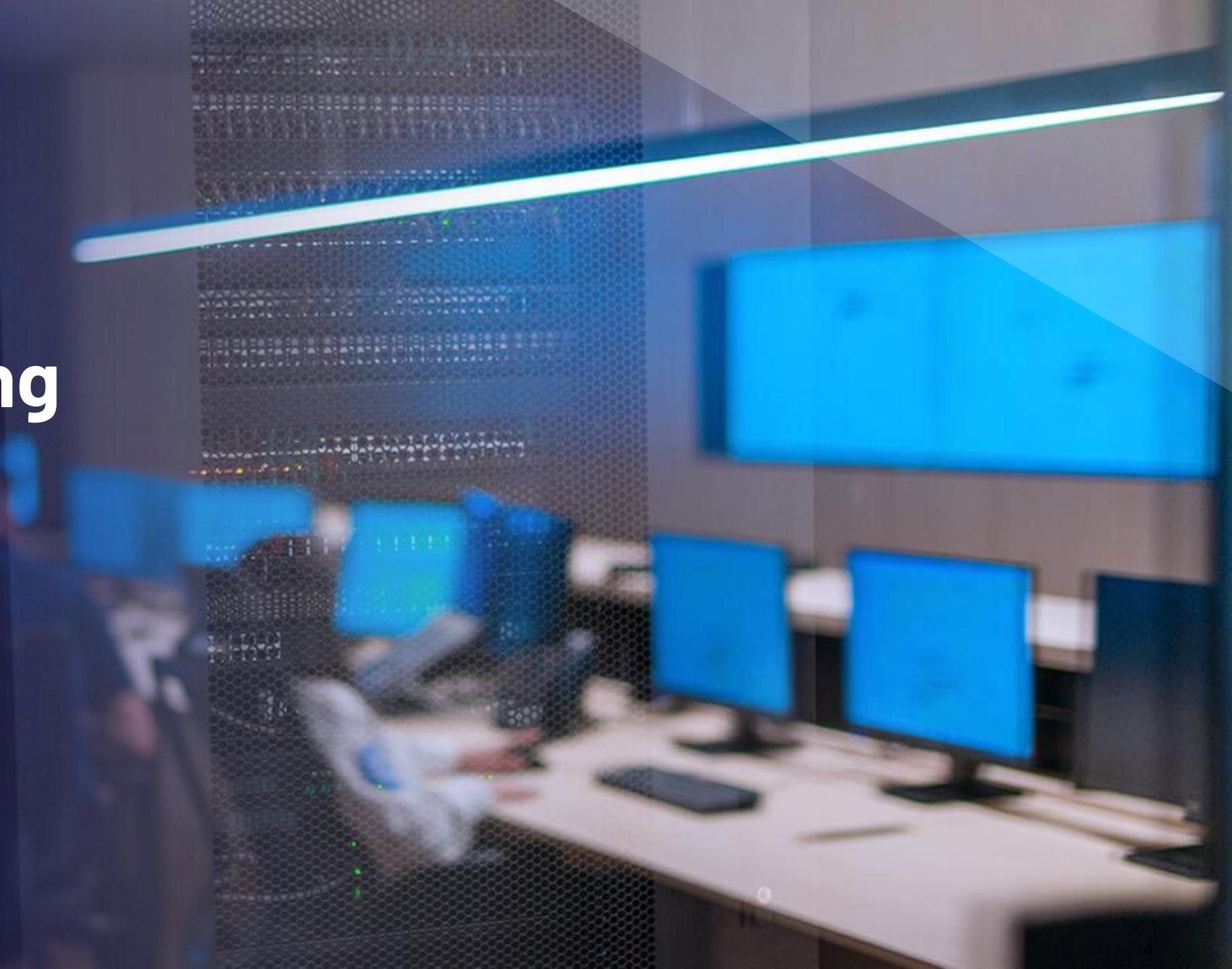
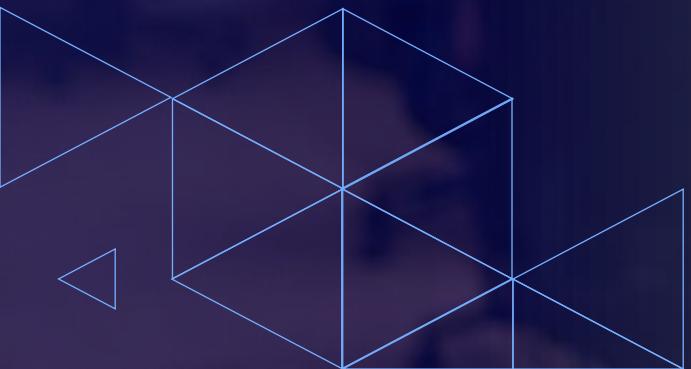


2017: Microsoft 365 (license bundle)



2022: Continuous evolution

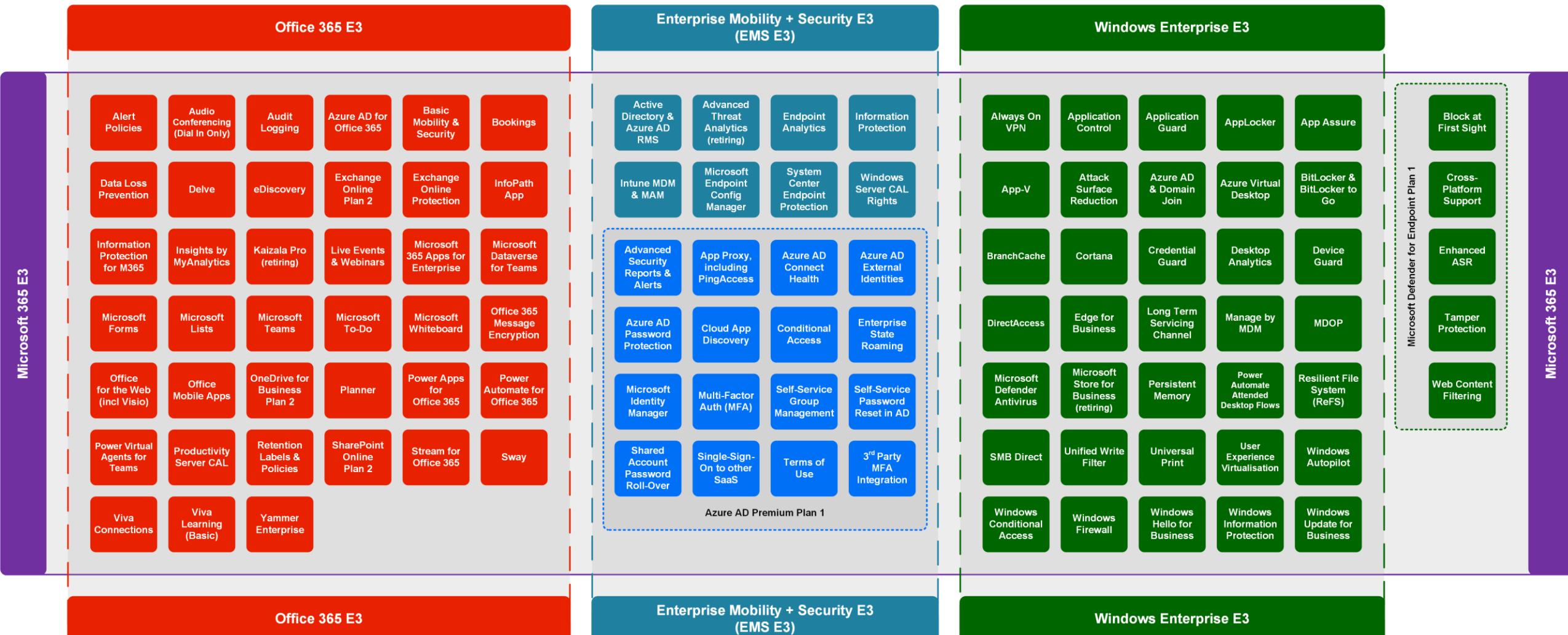
Licensing



Microsoft 365 E3

January 2022

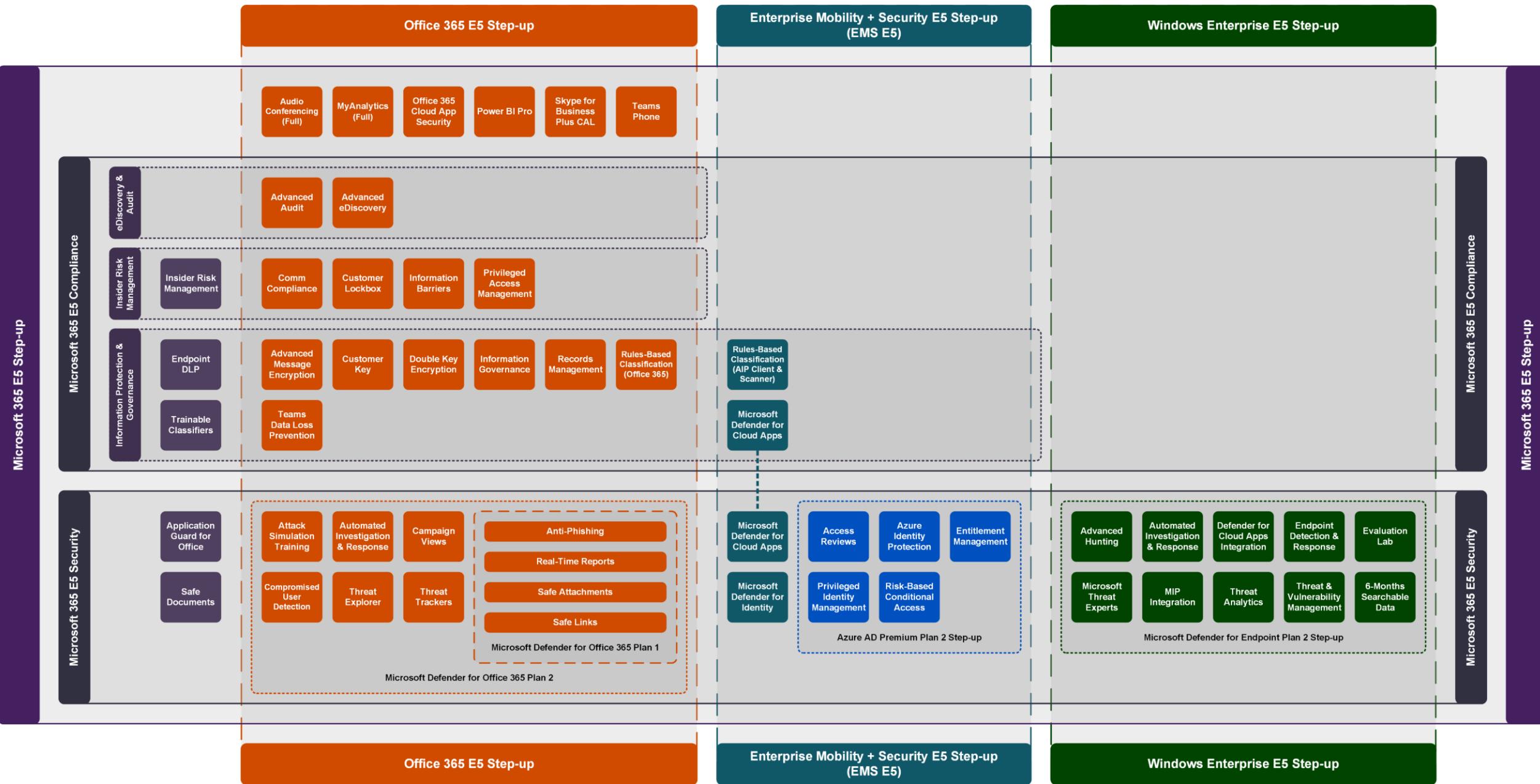
m365maps.com



Microsoft 365 E5 Step-up

January 2022

m365maps.com



Microsoft 365 E5 Security¹



M365 E5
Security

[Microsoft Defender for Office 365 Plan 2](#)

A cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection and includes features to safeguard your organization from harmful links in real time. In addition to Plan1, Plan 2 also offers automated investigation & response, threat trackers, and an attack simulator

[Microsoft Defender for Cloud Apps](#)

A multimode Cloud Access Security Broker (CASB). It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.

[Azure Active Directory Plan 2](#)

Microsoft's cloud-based identity and access management service, which helps employees sign in and access resources.
In addition to Free and P1 features, P2 also offers Identity Protection to help provide risk-based Conditional Access to apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

[Microsoft Defender for Identity](#)

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.

[Microsoft Defender for Endpoint Plan 2](#)

A unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. The product offers Threat and Vulnerability Management, tools to surgically reduce the attack surface, next-generation protection to block threats and malware, Endpoint detection and response to detect advanced attacks, automated investigation and remediation of threats and Managed threat-hunting service.

[Safe Documents²](#)

Uses Microsoft Defender for Endpoint to scan documents and files that are opened in Protected View or Application Guard to automatically check Office documents (Excel, PowerPoint, Word etc.) "against known risks and threat profiles" before users open them.

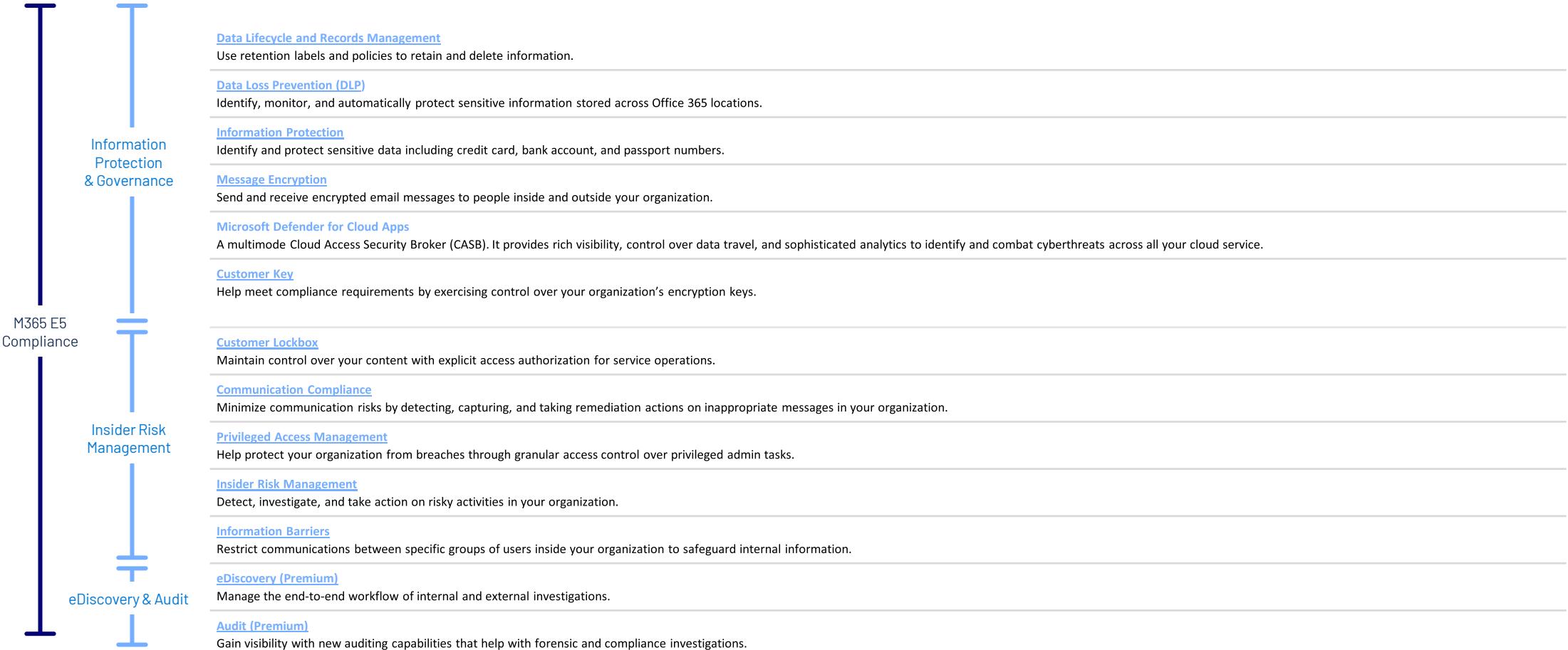
[Application Guard for Office 365²](#)

Isolates untrusted documents to protect users against malicious and potentially harmful threats. at risk. When a user encounters a malicious document, it is safely isolated.

1 Please see notes for clarification on branding changes

2 Only provided via Microsoft 365 E5 or Microsoft 365 E5 Security

Microsoft 365 E5 Compliance



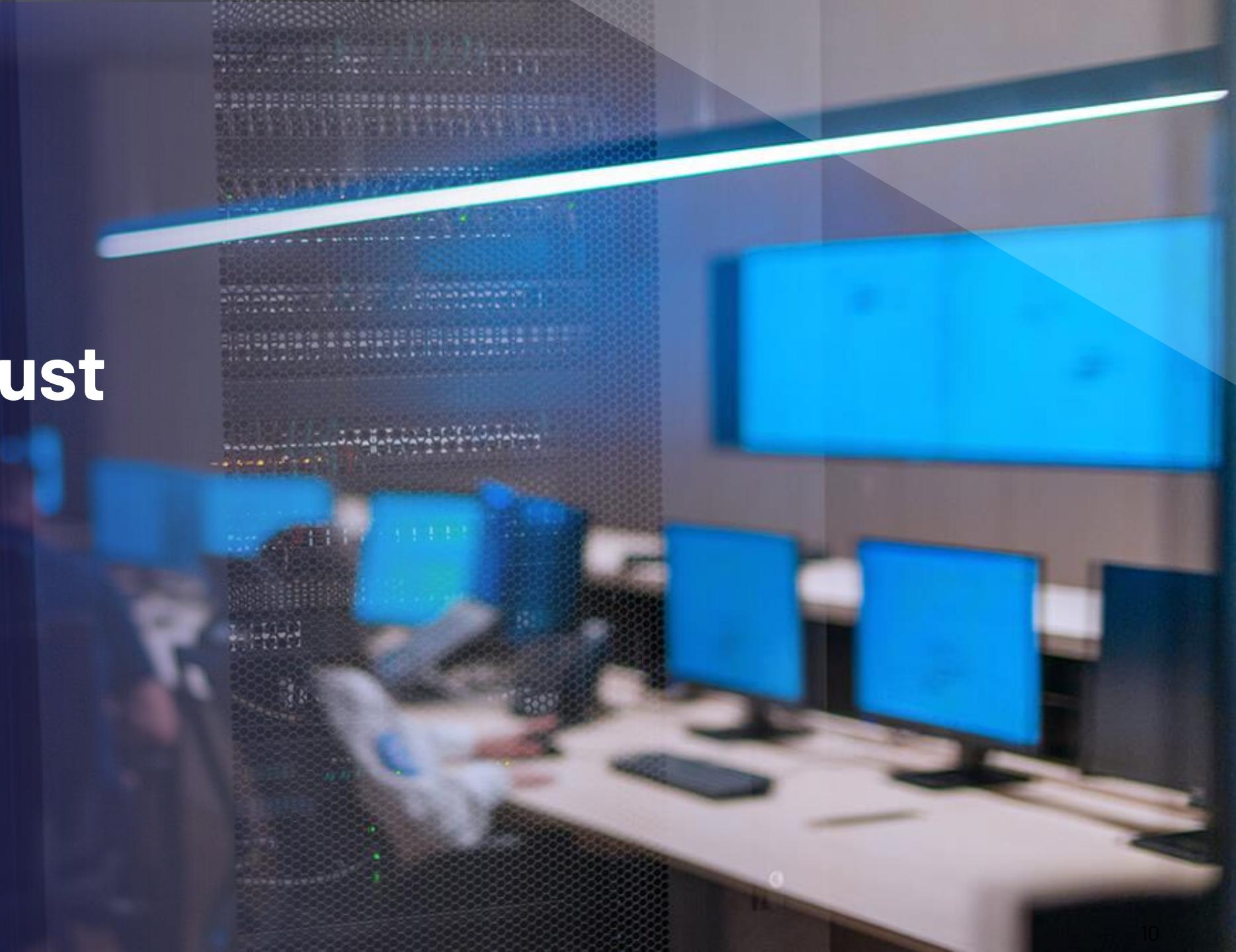
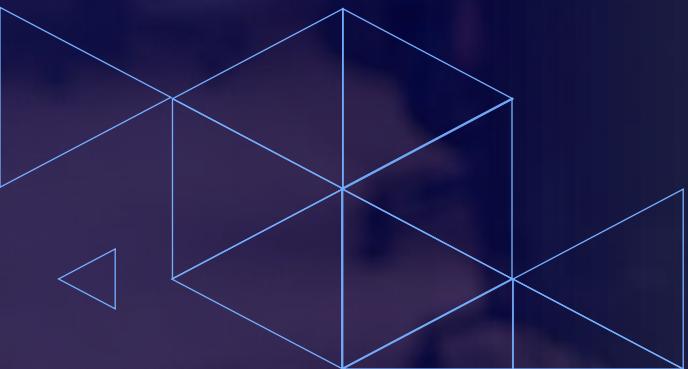
Microsoft EMS E3 and E5 Packaging¹

EMS E5	Azure Active Directory P2	Includes all P1 capabilities, as well as Identity Protection (risk based conditional access), and Identity Governance (PIM). The most trusted identity and access management solution in the market that helps you safeguard user credentials and connect people securely to the apps they need.
	Azure Information Protection P2²	Includes all P1 capabilities, intelligent classification & encryption for files, emails and documents. Control and help secure email, documents, and sensitive data that you share outside your company.
	Microsoft Defender for Identity	Cloud-based solution that helps protect your organization's identities from multiple types of advanced targeted cyberattacks.
	Defender for Cloud Apps	Cloud access security broker (CASB) with discovery, behavioral analytics, risk assessment, data protection, and threat protection.
	Microsoft Intune	A cloud-based service for mobile device management (MDM) and mobile application management (MAM). Intune integrates with Azure Active Directory (Azure AD) to control who has access, and what they can access.
	Azure Information Protection P1	Cloud-based data classification, tracking, protection, and encryption. Control and help secure email, documents, and sensitive data that you share outside your organization. Includes Azure Rights Management.
	Azure Active Directory P1	A comprehensive identity and access management cloud solution that combines core directory services, application access management, authentication, single sign-on, multifactor authentication, authorization and conditional access. This edition includes everything you need for information worker and identity administrators in hybrid environments across application access, self-service identity and access management (IAM), and security in the cloud.
	Microsoft Advanced Threat Analytics³	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.

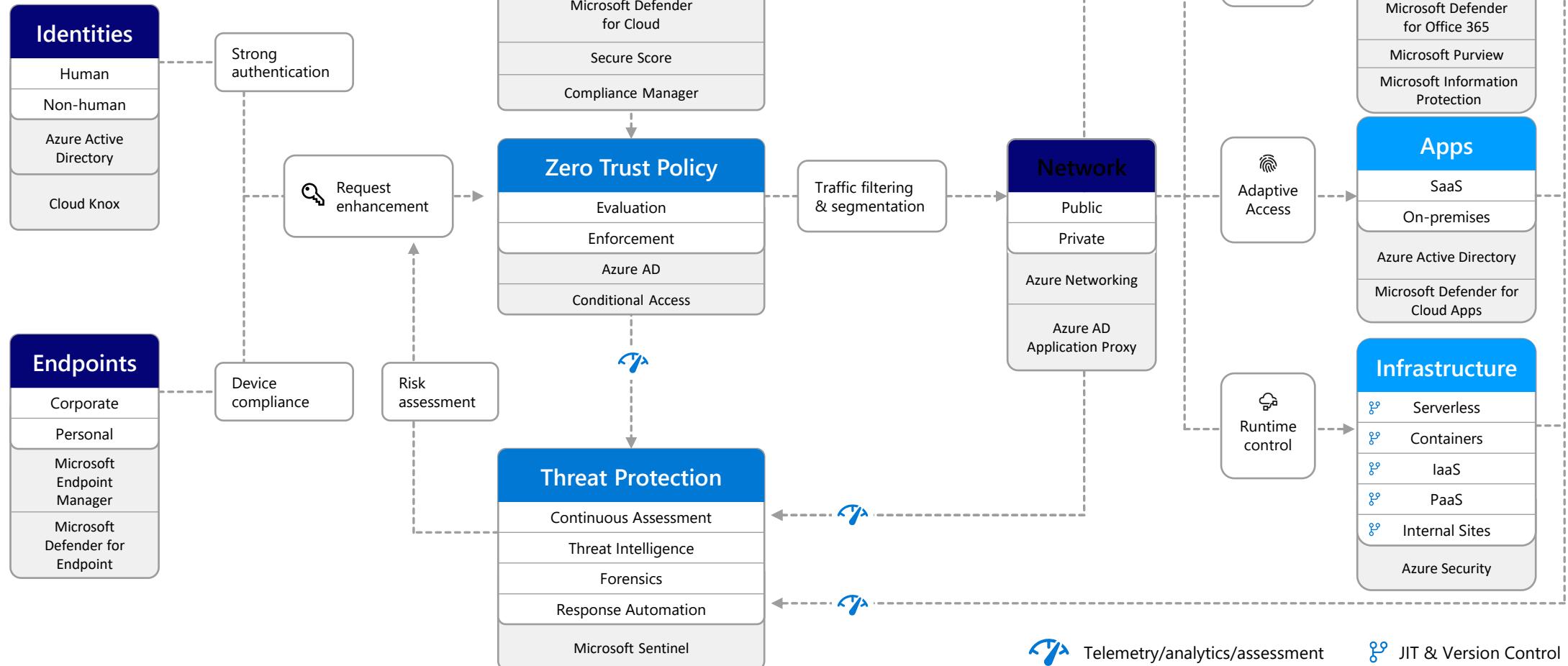
¹ Also includes Windows Server CAL Rights

² Not available as a standalone for new customers

Zero Trust



Zero Trust solutions from Microsoft



Azure AD conditional access (Zero Trust)

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Geo-location
- Corporate Network

- Browser apps
- Client apps

Conditions

Employee & Partner
Users and Roles



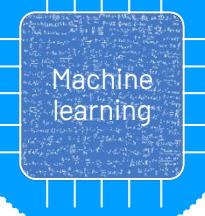
Trusted &
Compliant Devices



Physical &
Virtual Location



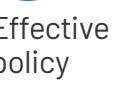
Client apps &
Auth Method



Real time
Evaluation
Engine



Policies



Effective
policy

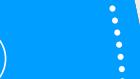
Controls



Allow/block
access



Limited
access



Require
MFA



Force
password
reset



Block legacy
authentication



Microsoft
Cloud



Microsoft
Defender for
Cloud Apps

Cloud SaaS apps



On-premises
& web apps

CONFIDENTIAL



CRAWL

WALK

RUN

Microsoft 365 Defender



Multi-cloud

SIEM

Azure Sentinel



Partnerships

Prevent

Protect



Microsoft Defender XDR

Microsoft 365 Defender

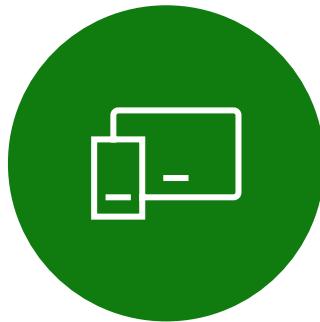


Automated cross-domain XDR security



Identities

Microsoft Defender
for Identity



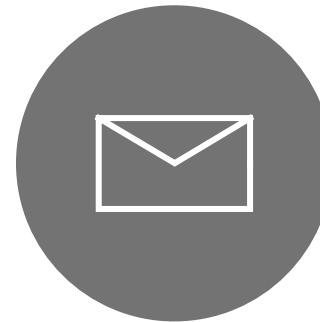
Endpoints

Microsoft Defender
for Endpoint



Cloud Apps

Microsoft Defender
for Cloud Apps



Email & collaboration

Microsoft Defender
for Office 365

SIEM

Microsoft Sentinel

Protection across an attack kill chain

Defender for Office 365

Malware detection, safe links, and safe attachments

Phishing mail
Open attachment



Browse to a website

Azure AD Identity Protection

Identity protection & conditional access



Brute force account or use stolen account credentials

Exploitation & Installation



Command & Control



User account is compromised

Attacker collects reconnaissance & configuration data



Attacker attempts lateral movement



Defender for Cloud Apps

Extends protection & conditional access to other cloud apps



Exfiltrate data



Attacker accesses sensitive data

Domain compromised



Defender for Endpoint

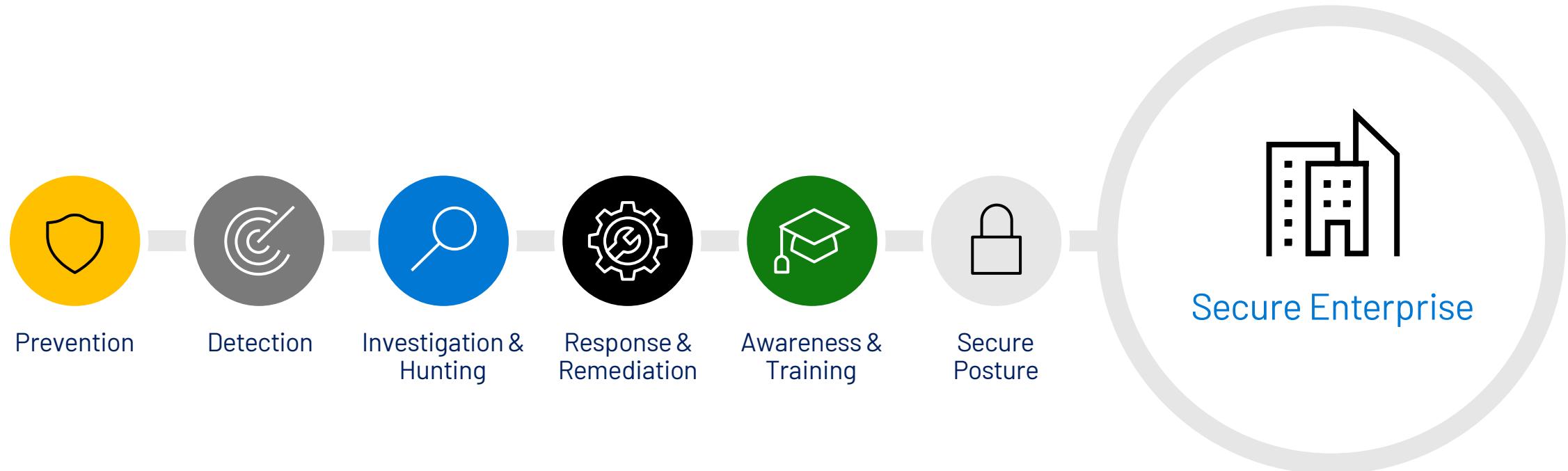
Endpoint Detection and Response (EDR) & End-point Protection (EPP)



Microsoft 365 Defender XDR

Microsoft Defender for Office 365 (MDO)

Securing your enterprise requires more than just prevention



Multi-layered protection stack stops a wide variety of attacks

Multi-Layered protection stack

Edge protection



Sender intelligence



Content filtering



Post-delivery protection



Simplified configuration guidance



The screenshot shows a Microsoft Edge browser window on a laptop. The URL is <https://security.microsoft.com/presetSecurityPolicies>. The page title is "Microsoft 365 Defender". The main content area is titled "Preset security policies". It explains that a preset security policy is a compilation of settings for anti-spam, anti-malware, anti-phishing, Safe Links, and Safe Attachments. It notes that multiple policies apply to a user, with Strict overriding Standard, and Standard overriding custom policies. A link to "Learn more" is provided.

Standard protection
Apply a baseline protection profile that's suitable for most users.
 Enabled [Edit](#) Refresh

Exchange Online Protection applies to
If email is sent to a member of:
allcompany@mdodemo.onmicrosoft.com

Defender for Office 365 protections applies to
If email is sent to a member of:
allcompany@mdodemo.onmicrosoft.com

Strict protection
Apply a more aggressive protection profile for selected users.
 Enabled [Edit](#) Refresh

Exchange Online Protection applies to
If email is sent to a member of:
ProjectContoso@mdodemo.onmicrosoft.com

Defender for Office 365 protections applies to
If email is sent to a member of:
ProjectContoso@mdodemo.onmicrosoft.com

Simplified configuration guidance



The Configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security. [Learn more](#).

Setting and recommendations **Configuration drift analysis and history**

View Standard recommendations

Policy group/setting name	Policy	AI	Current configuration	Last modified	Recommendations
Anti-spam	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	Quarantine message Adopt
Automatically include the domains I own	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	True Adopt
Include custom domains	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	True Modify
If email is sent by an impersonated user	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	Quarantine message Adopt
If email is sent by an impersonated domain	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	Quarantine message Adopt
Enable Intelligence for impersonation protection (...)	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	True Adopt
Show tip for impersonated users	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	True Adopt
Show tip for impersonated domains	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	True Adopt
Show tip for unusual characters	Office365 AntiPhish ...	False	Move to Junk Email f...	Mar 29, 2021 5:00 PM	True Adopt
If email is sent by an impersonated user who's prot...	Office365 AntiPhish ...	No action	Move to Junk Email f...	Mar 29, 2021 5:00 PM	Quarantine message Adopt
Advanced phishing thresholds	Office365 AntiPhish ...	1	Move to Junk Email f...	Mar 29, 2021 5:00 PM	3 Adopt

Protection beyond email



Microsoft 365 Defender

Search

Diagnostics

Safe attachments

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, we will prevent users from opening and downloading the file.

[Learn more about protection for SharePoint, OneDrive, and Microsoft Teams](#)

Turn on protection for SharePoint, OneDrive, and Microsoft Teams

Help people stay safe when trusting a file to open outside Protected View in Office applications

Before a user is allowed to trust a file opened in Office 365 ProPlus, the file will be verified by Microsoft Defender for Endpoint.

[Learn more about Safe Documents](#).

Turn on Safe Documents for Office clients. Only available with *Microsoft 365 E5* or *Microsoft 365 E5 Security* license.

[Learn more about how Microsoft handles your data](#).

Allow people to click through Protected View even if Safe Documents identified a file as malicious.

Guided hunting with inline actions



Microsoft 365 security

https://security.microsoft.com/threatexplorer

Explorer

Explorer is a powerful, near real-time tool to help you hunt for threats in your organization. View All email This view shows information about all email messages in your organization. You can search, filter, and export up to 200,000 records for offline analysis. Save query | Save query as | ...

Exchange transport rule ▾ Allowing for Partner email de... Exchange transport rule ; Allowing for Partner email de...

Email URL clicks URLs Top targets Actions Date (UTC +05:30) Subject

Jan 15, 2021 4:51 PM [EXTERNAL] Upd...
Jan 15, 2021 4:46 PM [EXTERNAL] Late...
Jan 15, 2021 4:46 PM [EXTERNAL] Late...
Jan 14, 2021 10:14 PM [EXTERNAL] Upd...

16 item(s) out of 16 loaded.

Create a new remediation for Soft delete

Name your remediation
 Determine severity
 Review and trigger action

Review your settings

Name Deleting Emails for Exec Phish Attack- Case Number ST3276219 [Edit](#)
Description Misconfigured ETR led to delivery of malicious emails from a compromised vendor account. Deleting these emails to remove access to malicious content [Edit](#)
Severity High [Edit](#)
Scope [Export](#)

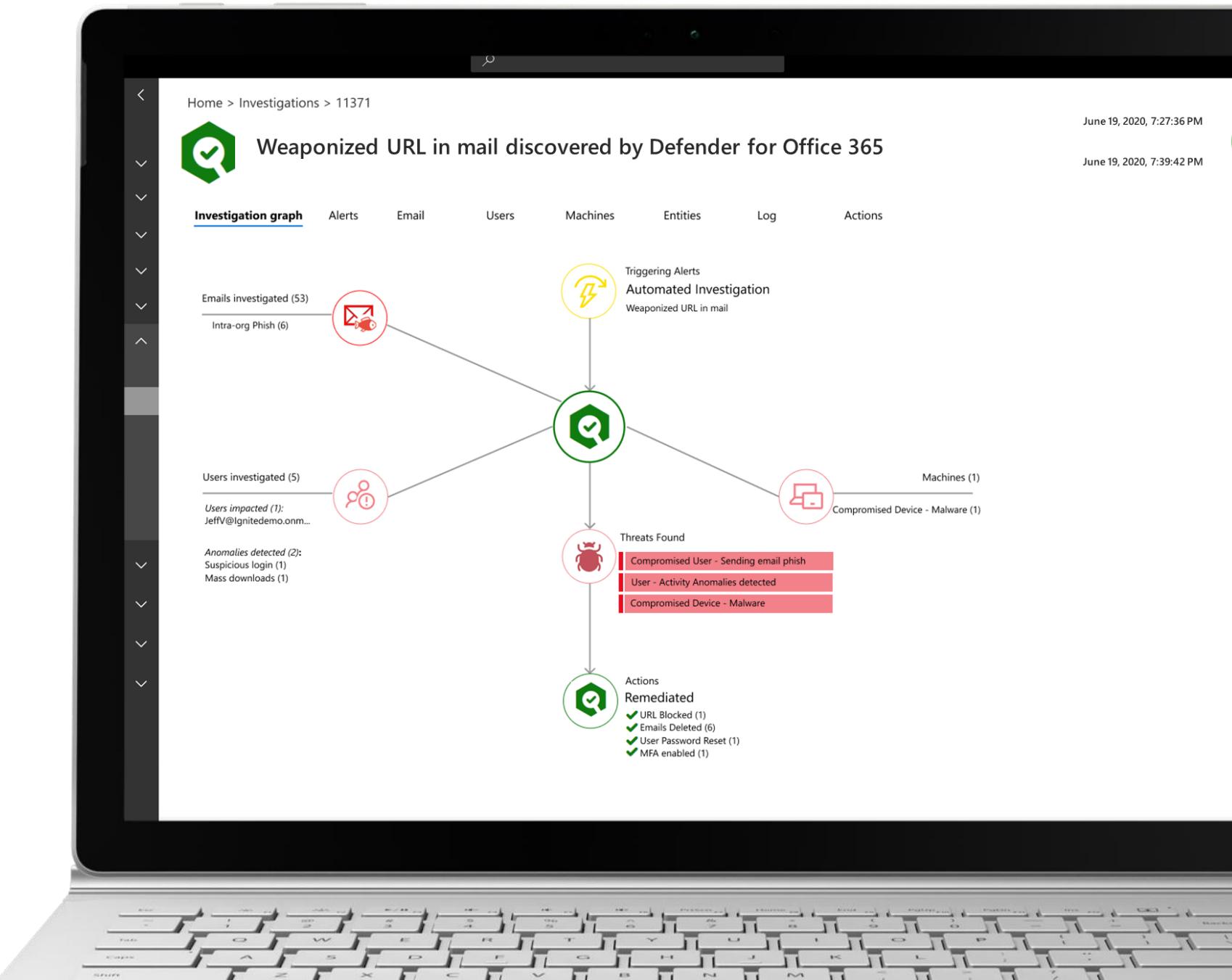
Date	Recipient	Subject	Sender
2021-01-15 16:51:05	mdo@mdodemo.onmicrosoft.c...	[EXTERNAL] Update on the Rep...	b15184@astraxlri.ac.in
2021-01-15 16:46:10	mdo@mdodemo.onmicrosoft.c...	[EXTERNAL] Latest update on Pr...	b15184@astraxlri.ac.in
2021-01-15 16:46:10	sumitm@mdodemo.onmicrosoft...	[EXTERNAL] Latest update on Pr...	b15184@astraxlri.ac.in
2021-01-14 22:14:06	mdo@mdodemo.onmicrosoft.c...	[EXTERNAL] Update on Project ...	b15184@astraxlri.ac.in
2021-01-14 22:14:05	sumitm@mdodemo.onmicrosoft...	[EXTERNAL] Update on Project ...	b15184@astraxlri.ac.in

Action

Deletes the selected messages. The item can be restored by the end user using the "Recover deleted item from server" function in Outlook.

Back Start Cancel

Automated response playbooks



Dynamic end user training



The laptop screen shows a training module for end-user cybersecurity. At the top right is a cartoon character of a person with glasses and a worried expression, with a red speech bubble above them. Below the character is the text "John, you were just phished." In the center, there is a bold heading: "It's okay! You're human. Let's learn from this." Below this, a message reads: "Rather than stealing your login credentials like a cyber criminal, we have redirected you to this educational page instead and assigned you some training courses." A blue button labeled "Learn what you missed" is visible. The main content area displays an email message with the following details:

From: System Administrator <sysadmin@webaccess-alert.net>
Sent: Tuesday, September 19, 2017 2:10 PM
To: Jeff Sun
Subject: Unauthorized Web Site Access

This is an automated email

Our regulators require we monitor and restrict certain website access due to content. The filter system monitors your computer as one that has viewed or logged into websites hosting restricted content. The filter system is not fool-proof, and may incorrectly flag restricted content. The IT department does not investigate every filter report, but disciplinary action may be taken.

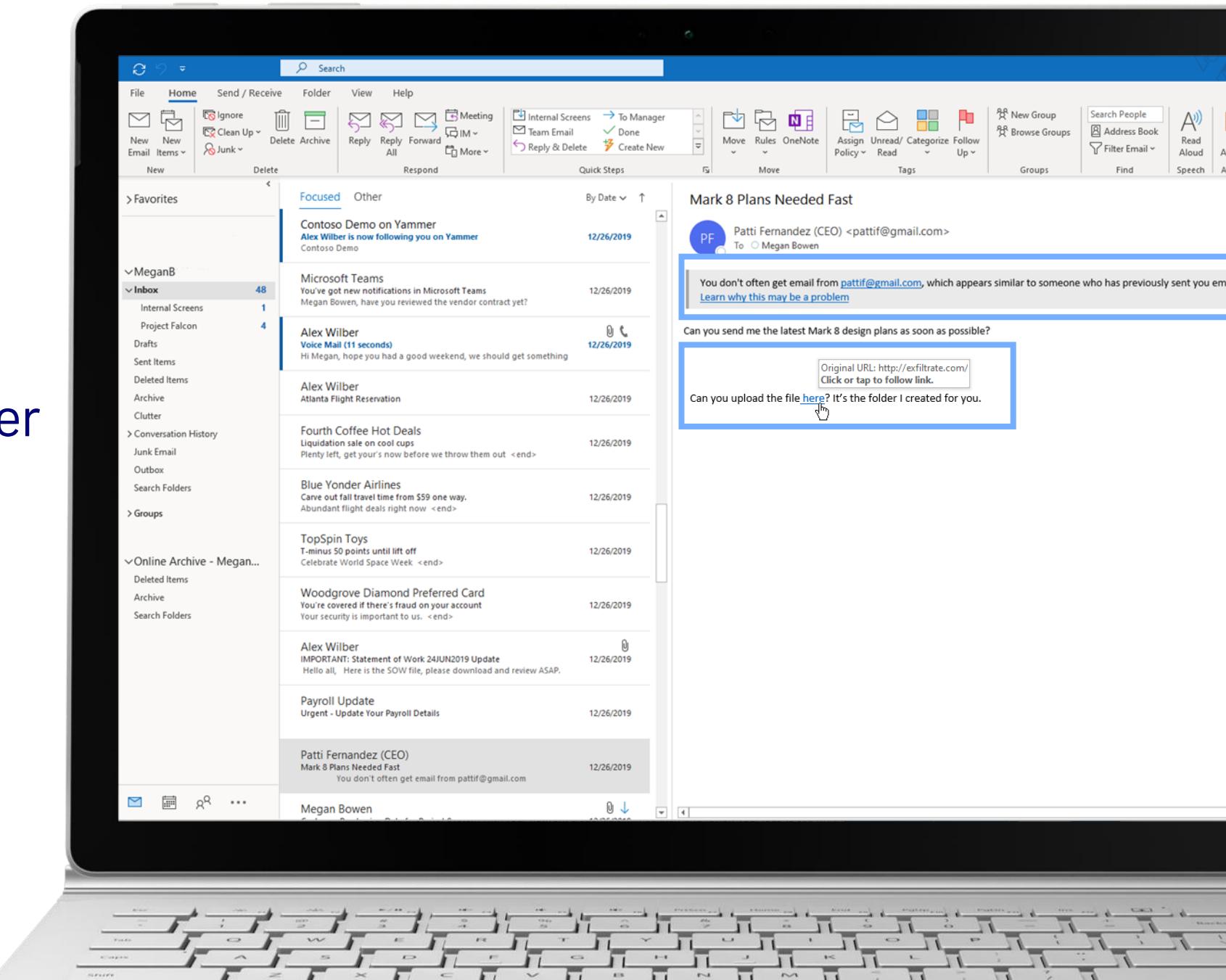
Log into the filter system with your network credentials immediately and review your logs to see which

Grammar mistakes

Grammar and spelling errors in what is supposed to be an official email are indicative of careless phisher and should arouse suspicion.

Previous Next 3 of 6

Native experiences foster user awareness



Microsoft Defender for Office 365 Recommended Configuration Analyzer (ORCA)



Microsoft Defender for Office 365 Recommended Configuration Analyzer Report

Version 1.10.6

This report details any tenant configuration changes recommended within your tenant.

Recommendations

26

OK

35

51 %

Configuration Health Index

The configuration health index is a weighted value representing your configuration. Not all configuration is considered and some configuration is weighted higher than others. The index is represented as a percentage. How the configuration impacts the configuration health index is shown next to the recommendation in the report below as a positive or negative number. The impact to your security posture is a large consideration factor when rating the configuration.

Summary

Areas

Anti-Spam Policies

0 6 11

Advanced Threat Protection Policies

0 17 12

DKIM

0 1 1

Microsoft Defender for Office 365: Best Practices

Guides: Step-by-step guides to help administrators configure and use Microsoft Defender for Office 365 by reducing distracting information like how a feature might work, and other details not directly linked to completing a process.

Microsoft Defender SecOps Guide: gives an overview of the requirements and tasks for successfully operating Microsoft Defender for Office 365 in your organization.

Best Practice Configuration (ORCA): With the tool from Microsoft, you can check all relevant settings that affect e-mail security in no time at all.

Safe Attachments, Safe Links: Scans Attachments and Links in your Microsoft 365 Services.

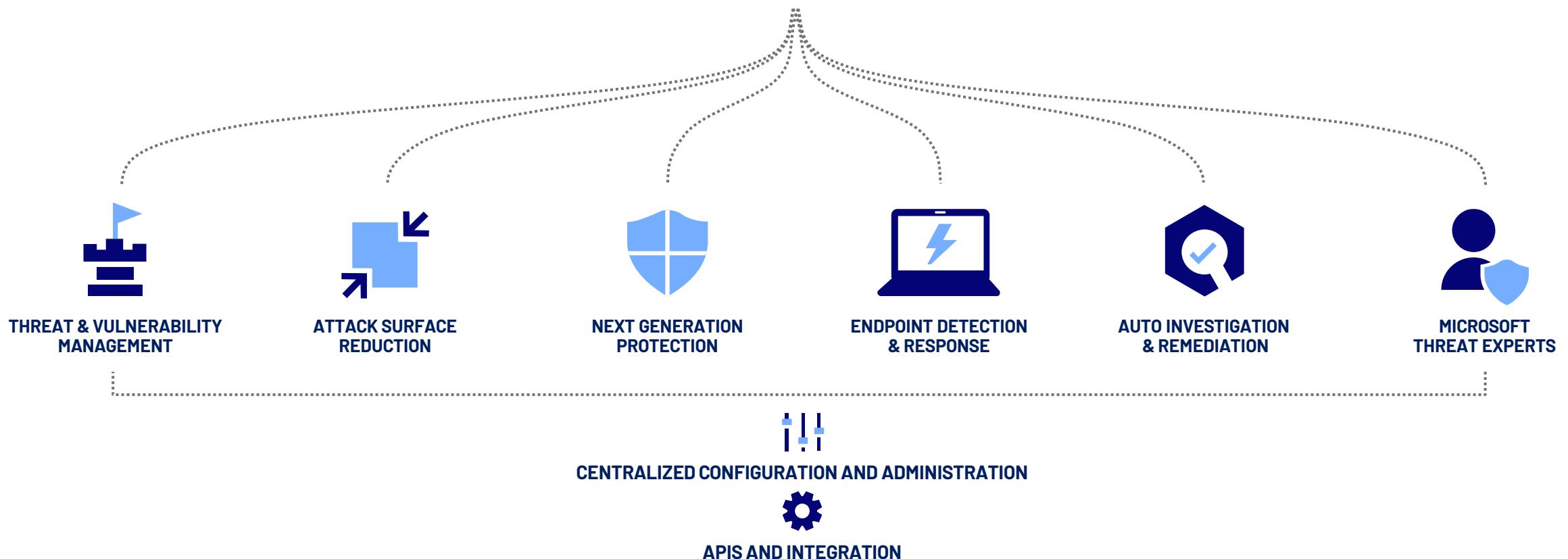
Anti-Phishing: Machine Learning, Spoof Intelligence (DRAFT, DKIM, DMARC)

ZAP Processing: Continuous checking of the mailbox for spam and malware.



Microsoft Defender for Endpoint (MDE)

Threats are no match.



Attack Surface Reduction

Eliminate risks by reducing the surface area of attack



System hardening without disruption



Customization that fits your organization



Visualize the impact and simply turn it on

The screenshot shows the Microsoft 365 security interface with a blue circular overlay containing a white document icon with arrows. The main panel displays 'Attack surface reduction rule detections' with statistics: 9.1k detections, 2 unique files, and 2 affected devices. It includes a chart titled 'Detections over time' from May 13 to June 9, showing a peak around May 16. Below the chart are buttons for 'View detections' and 'Add exclusions'. To the right, a sidebar lists 'Attack surface reduction rules' with a heading '86% devices use ASR rules to block them'. The rules listed include various behavioral blocks like 'Block Office applications from injecting code into other processes' and 'Block Adobe Reader from launching external executables'.

Endpoint Detection & Response

Detect and investigate advanced persistent attacks



Correlated behavioral alerts



Investigation & hunting over 6 months of data



Rich set of response actions

The screenshot shows the Windows Defender Security Center interface. At the top, there's a search bar and a navigation menu. Below it, a large blue circular icon contains a white laptop with a lightning bolt, symbolizing a threat. The main area is titled 'Incidents' and displays a table of 15 rows. Each row contains information about an incident, including its name (e.g., 2195, 2196), severity (Medium or Low), category (General Persistence, Suspicious Activity, Delivery, Installation, Suspicious Network Traffic), and various timestamps and user details.



Demonstrated industry-leading optics
and detection capabilities in MITRE
ATT&CK-based evaluation.

Auto Investigation & Remediation

Automatically investigates alerts and remediates complex threats in minutes



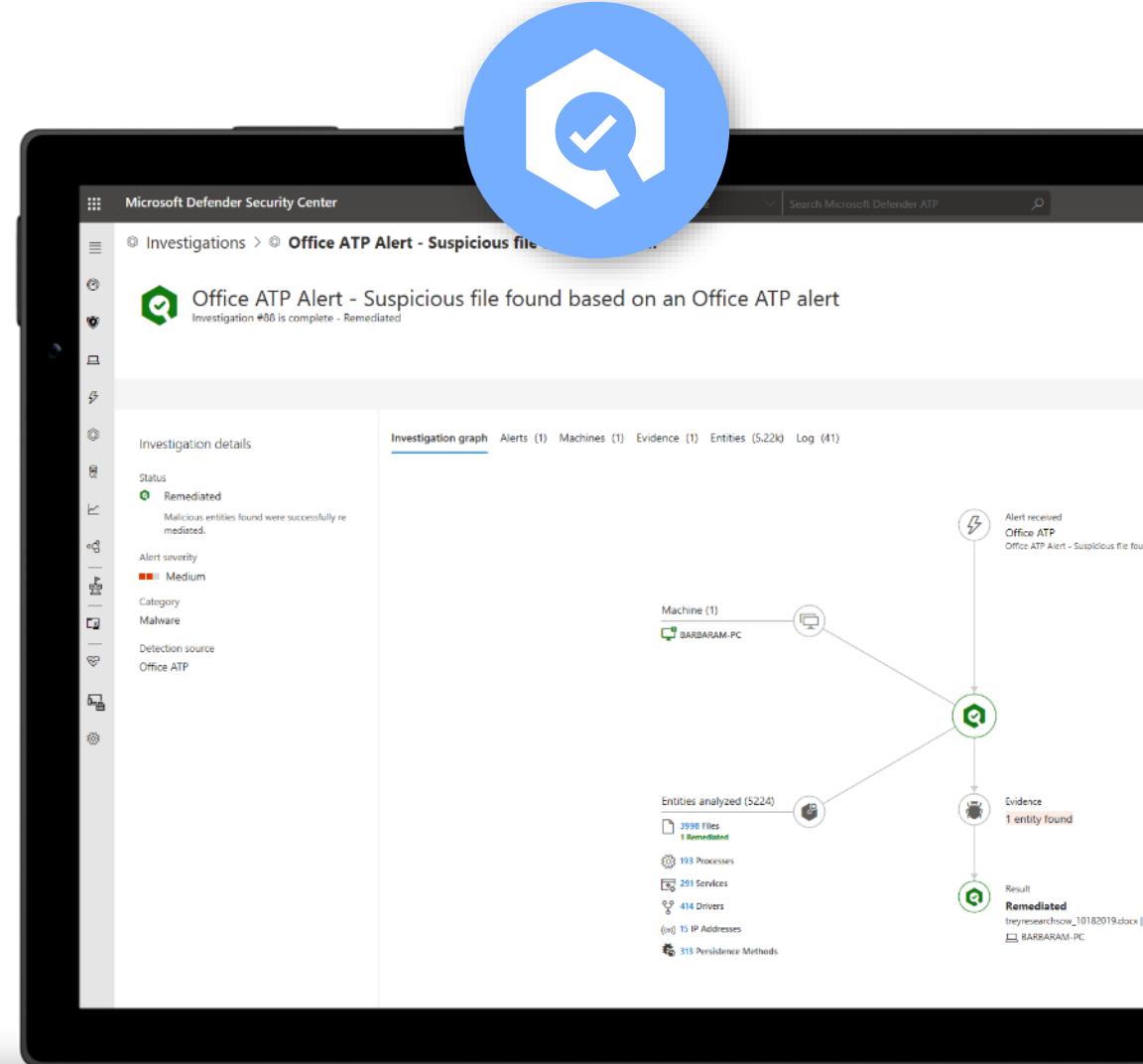
Mimics the ideal steps analysts would take



Tackles file or memory-based attacks



Works 24x7, with unlimited capacity



Microsoft Threat Experts

Bring deep knowledge and proactive threat hunting to your SOC



Expert level threat monitoring and analysis



Environment-specific context via alerts



Direct access to world-class hunters

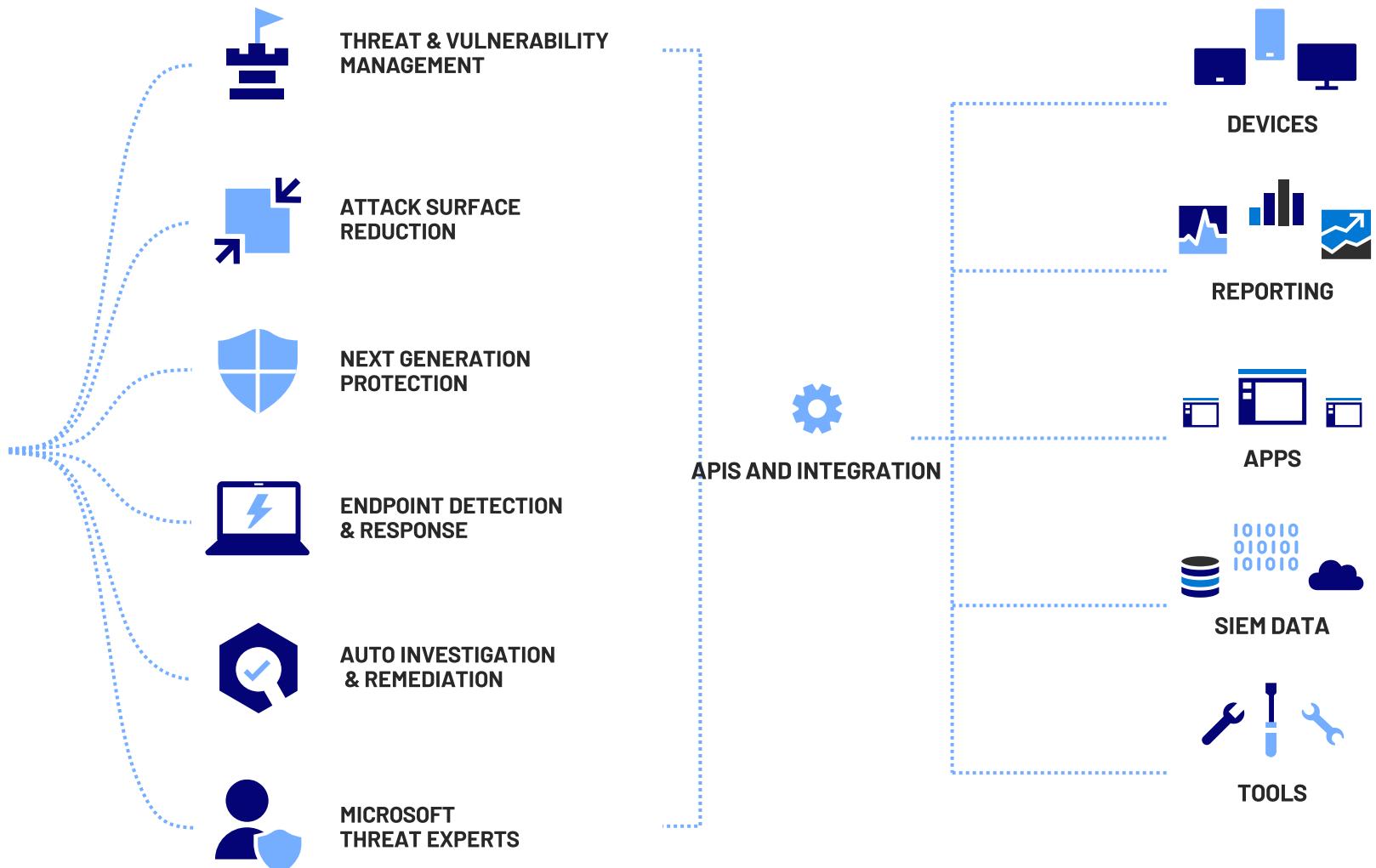
The screenshot shows the Microsoft Defender Security Center interface. A large blue circular icon with a white user silhouette and shield is overlaid on the top right. The main window displays an alert titled "Detection of file linked to adversary with supply chain attacks". The alert is from "Microsoft Threat Experts" and is associated with "BARIUM". It has a severity of "High" and a category of "Execution". The detection source is "Microsoft Threat Experts". The alert is part of Incident #54693. Below the alert details, there are sections for "Description" and "Executive summary". The "Description" section contains a detailed text about a Windows Defender AV detection of 'Winnti' malware and a documented Supply Chain attack. The "Executive summary" section provides a brief overview. Further down, there is a "Timeline of observed events" table showing three log entries: "Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe", "InstallLauncher.exe performs a connection out to a command-and-control server", and "Network connection to IP address 131.107.147.82". The final section shown is "Impacted machines", listing one machine with ID "fb7e23d4a69a1807013f69oc416f150b76e9a22" and notes "Impacted machine 1". On the right side of the interface, there are sections for "Alert context" (listing "desktop-c7ud4hh" and "janedoe") and "Recommended actions" (with a list of 6 items) and "Recommendation summary". At the bottom, there are sections for "Indicators of Compromise" (with links to "IOC", "Install (2).exe [explore]", "InstallConfig.exe [explore]", "InstallLauncher.exe [explore]", and two specific IOC entries), and "Timeline of observed events" (with links to "881ba9b12040d4576b5e09de73e5eb33de2c4ab4 [explore]" and "ab16cd1b09e5157791a568456a12659aae926901 [explore]").

Connecting with the platform



Microsoft Defender for Endpoint

Threats are no match.



Microsoft Defender for Endpoint (macOS)

Threat prevention

- Realtime MW protection for Mac OS
- Malware detection alerts visible in the Microsoft Defender for Endpoint console

Rich cyber data enabling attack detection and investigation

- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

Enterprise Grade

- Lightweight deployment & onboarding process
- Performant, none intrusive
- Aligned with compliance, privacy & data sovereignty requirements

Seamlessly integrated with Microsoft Defender for Endpoint capabilities

- Detection dictionary across the kill chain
- 6 months of raw data on all machines Inc. Mac OS
- Reputation data for all entities being logged
- Single pane of glass across all endpoints Mac OS
- Advanced hunting on all raw data including Mac OS
- Custom TI
- API access to the entire data model Inc. Mac OS
- SIEM integration
- Compliance & Privacy
- RBAC

The screenshot shows the Windows Defender Security Center interface. On the left, there's a sidebar with icons for Actions, Machine Overview (Mac-3), Domain local, OS: macOS 64-bit, and Machine IP Address. The main area has three sections: 'Logged on users (last 30 days)' with a count of 0, 'Alerts related to this machine' (No alerts found), and 'Machine timeline'. The timeline shows a list of events from Aug 2018 to Nov 2018. A green box highlights a series of events from 01/26/2019 to 01/27/2019, all of which are 'testScriptish was detected as EICAR-Test-File (not a virus) by DefenderW'. The timeline also includes filters for Value, Information level, Event type, and User account.

Microsoft Defender for Endpoint (Linux)

On the client:

- AV prevention
- Full command line experience (scanning, configuring, agent health)

```
File Edit View Search Terminal Help
parallels@t-ubuntu:~$ mdatp
-h [ --help ]          Display help
--trace                Begins tracing Microsoft Defender's activity
--verbose              Verbose output
--retry                Retry attempts to connect
--diagnostic            Gathers log files and packages them into a compressed file in the support directory
--definition-update    Checks for new definition updates
--pretty               Displays the output in human-readable format
--health [metric]       Display health information (Optional parameter, report just one metric)
--notice               Display third party notice
--logging              Logging options (see below)
--config [name] [value] Change configuration
--threat                Threat operations (see below)
--scan                  Scan operations (see below)
--exclusion             Exclusion operations (see below)
--connectivity-test     Run connectivity test
--edr                  EDR config (see below)

-logging options:
--set-level arg         Sets the current diagnostic logging level
--view-logs             Outputs the contents of log files to the terminal

-threat options:
--add-allowed arg       Adds allowed threat
--remove-allowed arg    Removes allowed threat
--get-details arg        Gets threat details
--list                  Lists all detected threats
--quarantine arg        Quarantines threat (by threat ID)
--restore arg            Restores threat (by threat ID)
--remove arg             Removes threat (by threat ID)
--type-handling [threat_type] [action] Changes the way certain threats are handled

-scan options:
--path path              Scans provided path
--quick                 Performs quick scan
--full                  Performs full system scan
--cancel                Cancels current scan (either quick, full or both)

-exclusion options:
--list                  List exclusions
--add-file arg           File path
--add-folder arg          Folder path
--add-extension arg      File extension
--add-process arg         Process name
--remove-file arg         File path
--remove-folder arg       Folder path
--remove-extension arg    File extension
```



In the Microsoft Defender Security Center, you'll see basic alerts and machine information.

EDR functionality will be gradually lit up in upcoming waves.

Antivirus alerts:

- ✓ Severity
- ✓ Scan type
- ✓ Device information (hostname, machine identifier, tenant identifier, app version, and OS type)
- ✓ File information (name, path, size, and hash)
- ✓ Threat information (name, type, and state)

Device information:

- ✓ Machine identifier
- ✓ Tenant identifier
- ✓ App version
- ✓ Hostname
- ✓ OS type
- ✓ OS version
- ✓ Computer model
- ✓ Processor architecture
- ✓ Whether the device is a virtual machine

Defender for Endpoint: Best Practices

Integration with MEM: Microsoft Endpoint Manager (MEM) becomes more and more prominent for customers that are using Azure Virtual Desktop as it provides a unified way of configuring and maintaining your physical and virtual Cloud endpoint as well as other devices e.g., mobiles.

Leverage Security Baselines: Security baselines are pre-configured groups of Windows settings that help you apply the security settings that are recommended by the relevant security teams. You can also customize the baselines you deploy to enforce only those settings and values you require.

Compliance Policy: Define the rules and settings that users and devices must meet to be compliant. Include actions that apply to devices that are non-compliant. Actions for non-compliance can alert users to the conditions of noncompliance and safeguard data on non-compliant devices.

Migration Guides: Microsoft provides comprehensive guides on how you can easily transition from other vendor platforms.

Defender for Endpoint: Best Practices

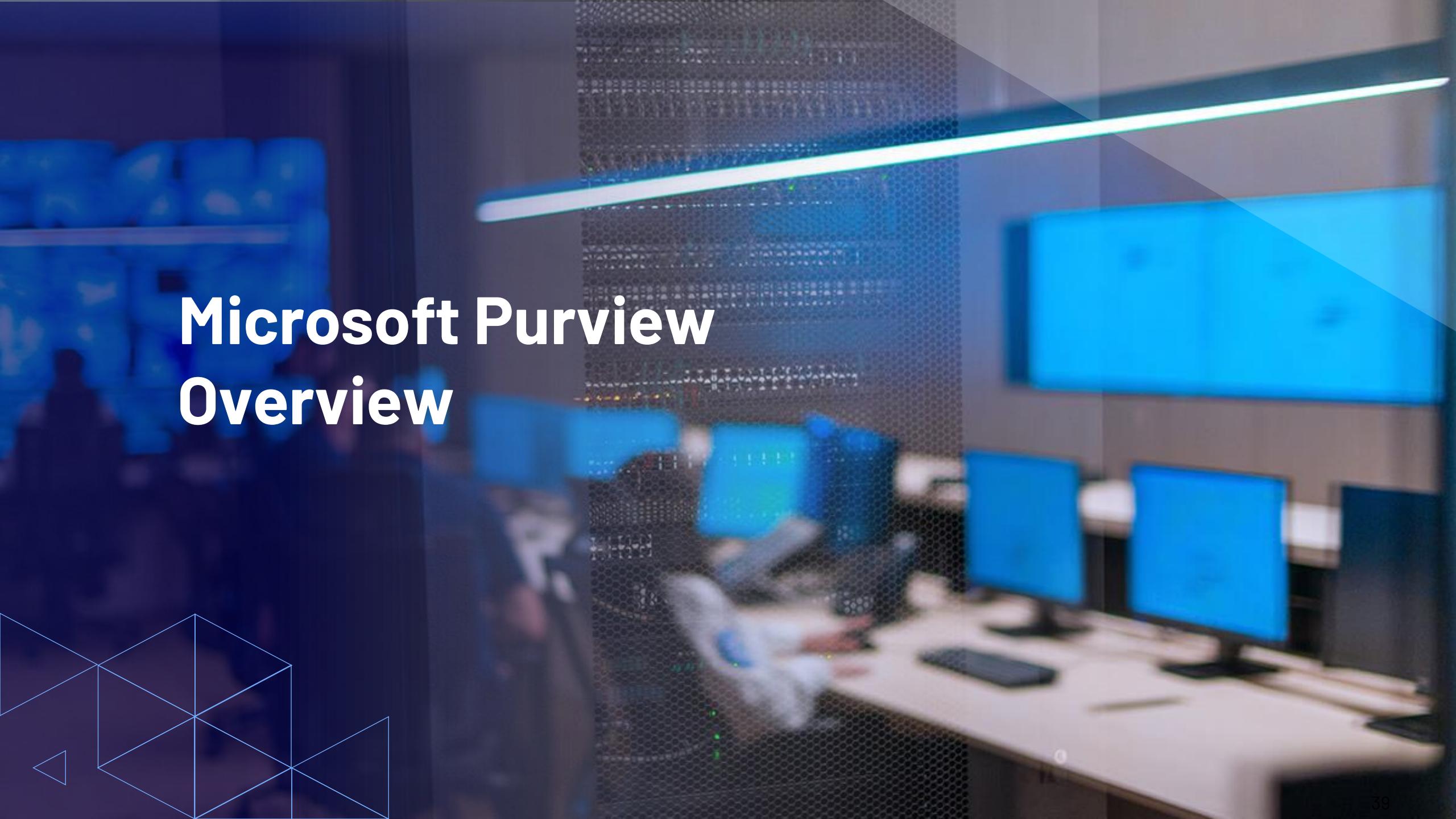
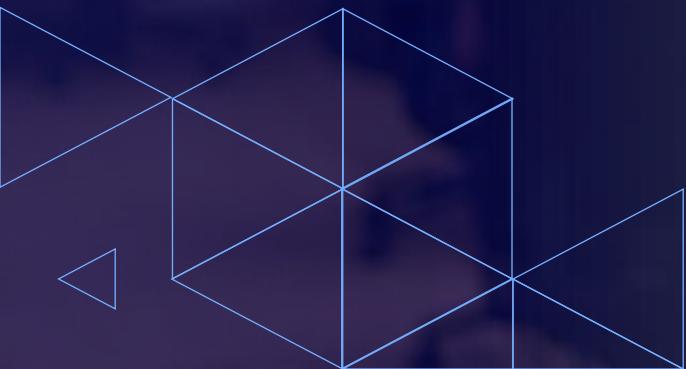
Device Management: Make sure that your environment is Hybrid Azure Active Directory enabled or Azure AD only and that your desktops are enrolled and possible to manage via Microsoft Intune via Microsoft Endpoint Manager.

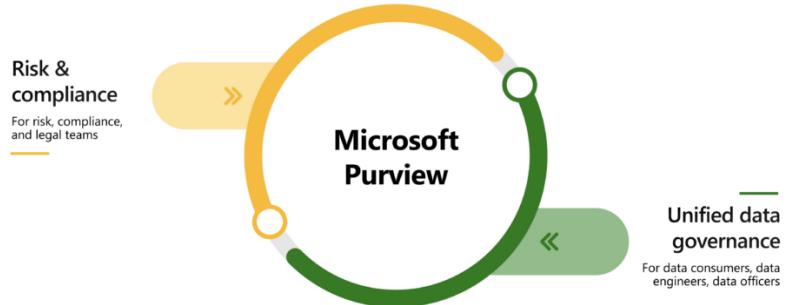
Microsoft Defender Security Center: During the setup of MDSC activation process remember to setup Microsoft Intune Connection.

Onboarding: Onboard your windows endpoints into Defender via MEM

ASR Rules: Use audit mode to evaluate how attack surface reduction rules would affect your organization if enabled. Run all rules in audit mode first so you can understand how they affect your line-of-business applications.

Microsoft Purview Overview





Current Name

- Microsoft 365 Basic Audit
- Microsoft 365 Advanced Audit
- Microsoft 365 Communication Compliance
- Microsoft Compliance Manager
- Office 365 Customer Lockbox
- Azure Purview Data Catalog
- Microsoft 365 Data Connectors
- Microsoft Information Governance
- Office 365 Data Loss Prevention
- Azure Purview Data Map
- Double Key Encryption for Microsoft 365
- Records Management in Microsoft 365
- Office 365 Core eDiscovery
- Office 365 Advanced eDiscovery
- Microsoft 365 Information Barriers
- Microsoft Information Protection
- Microsoft 365 Insider Risk Management
- Azure Purview portal
- Microsoft 365 compliance center
- Azure Purview Data Insights
- Microsoft 365 Customer Key

New Name

- Microsoft Purview Audit (Standard)
- Microsoft Purview Audit (Premium)
- Microsoft Purview Communication Compliance
- Microsoft Purview Compliance Manager
- Microsoft Purview Customer Lockbox
- Microsoft Purview Data Catalog
- Microsoft Purview Data Connectors
- Microsoft Purview Data Lifecycle Management
- Microsoft Purview Data Loss Prevention
- Microsoft Purview Data Map
- Microsoft Purview Double Key Encryption
- Microsoft Purview Records Management
- Microsoft Purview eDiscovery (Standard)
- Microsoft Purview eDiscovery (Premium)
- Microsoft Purview Information Barriers
- Microsoft Purview Information Protection
- Microsoft Purview Insider Risk Management
- Microsoft Purview governance portal
- Microsoft Purview compliance portal
- Microsoft Purview Data Estate Insights
- Microsoft Purview Customer Key

Microsoft Compliance Configuration Analyzer (MCCA)

Microsoft Compliance Configuration Analyzer (MCCA) is a diagnostic tool that generates a report to help you understand your current consumption of E5 compliance offerings.

github.com/OfficeDev/MCCA

The screenshot shows the Microsoft Compliance Configuration Analyzer (MCCA) interface. It consists of three main sections: Data Loss Prevention, Information Protection, and Information Governance. Each section contains a list of configuration items with their current status indicated by colored buttons (yellow for Improvement, grey for Recommendation, green for OK). A 'Go to Solutions Summary' link is located at the bottom right of each section.

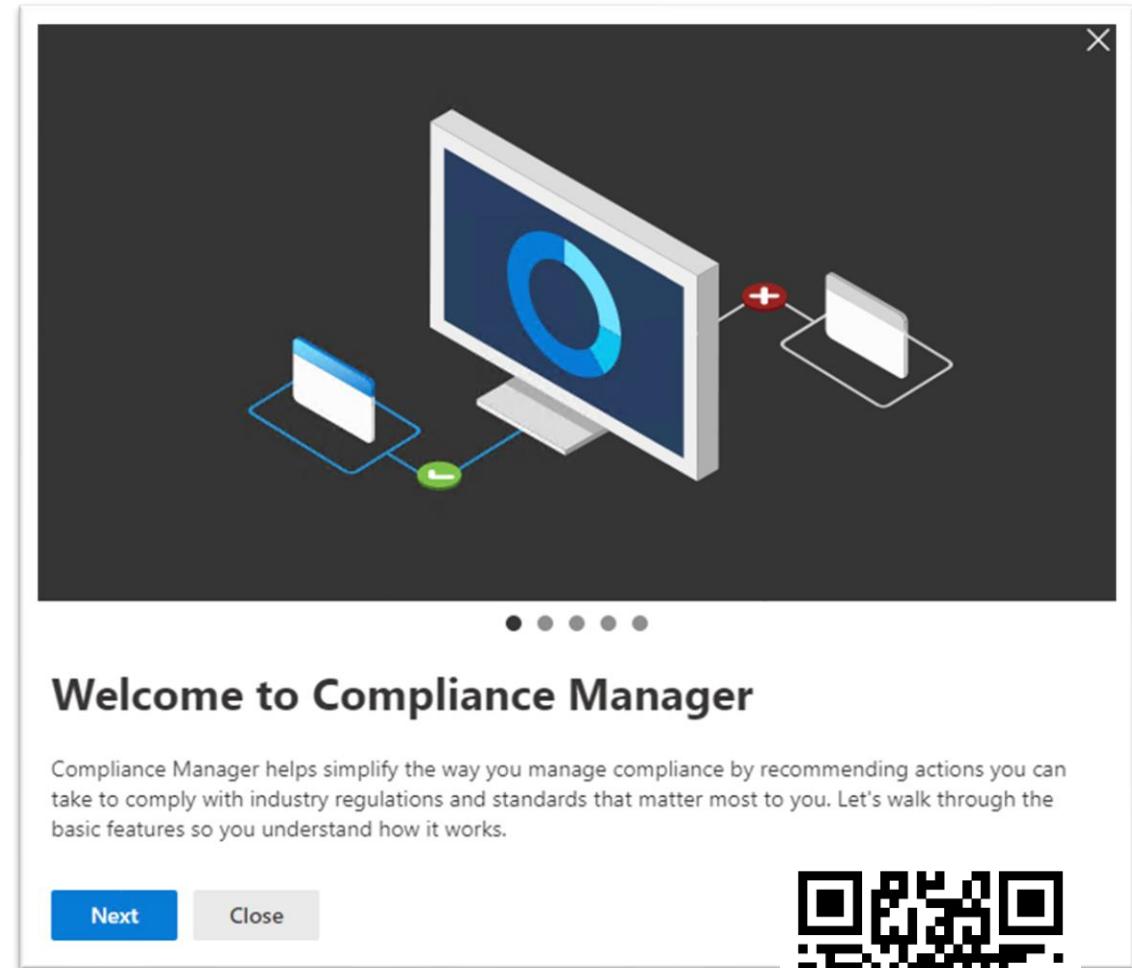
Section	Item	Status
Data Loss Prevention	Create DLP Policies for Government Data	Improvement
	Create customized or use default DLP Policies for Company Sensitive Information	Improvement
	Create customized or use default DLP Policies for ePHI	Improvement
	Create customized or use default DLP Policies for Personally Identifiable Information	Improvement
	Create customized or use default DLP Policies for Sensitive Financial Information	Improvement
Go to Solutions Summary		
Information Protection	Create service side labelling policies	Improvement
	Create Sensitivity Labels for Sensitive or Critical Data	Recommendation
	Use IRM for Exchange Online	OK
	Auto-apply client side sensitivity labels	OK
	Go to Solutions Summary	
Information Governance	Auto-Apply Retention Labels	Improvement
	Use Data Retention Labels and Policies	Improvement



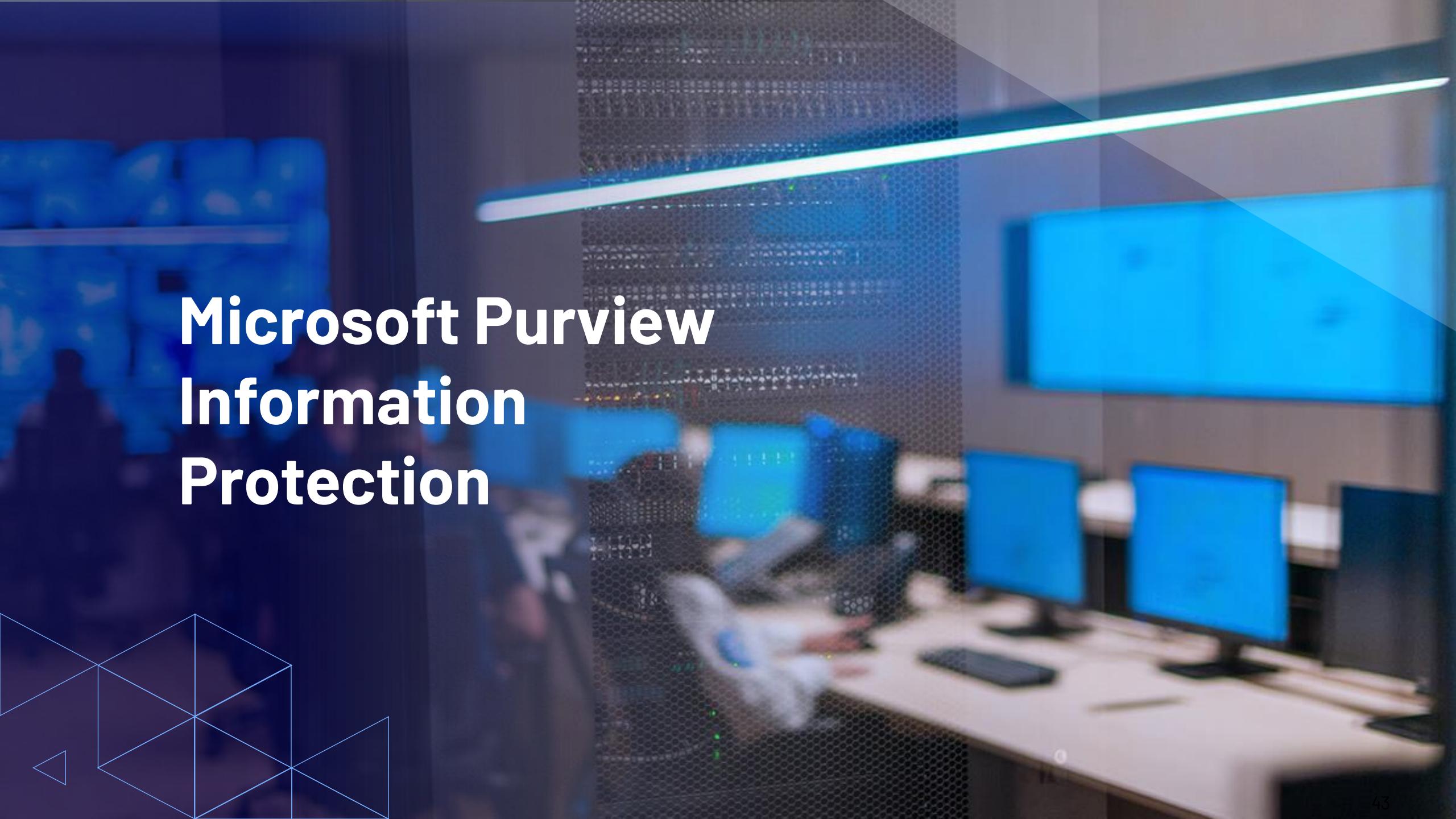
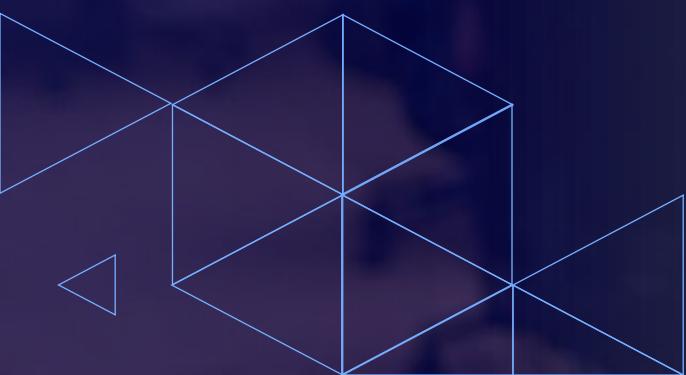
Microsoft Compliance Manager

Compliance Manager allows your organization to simplify compliance and reduce risk by completing pre-built assessments targeting industries, standards, and regulations or leveraging a custom assessment created by you and your organization.

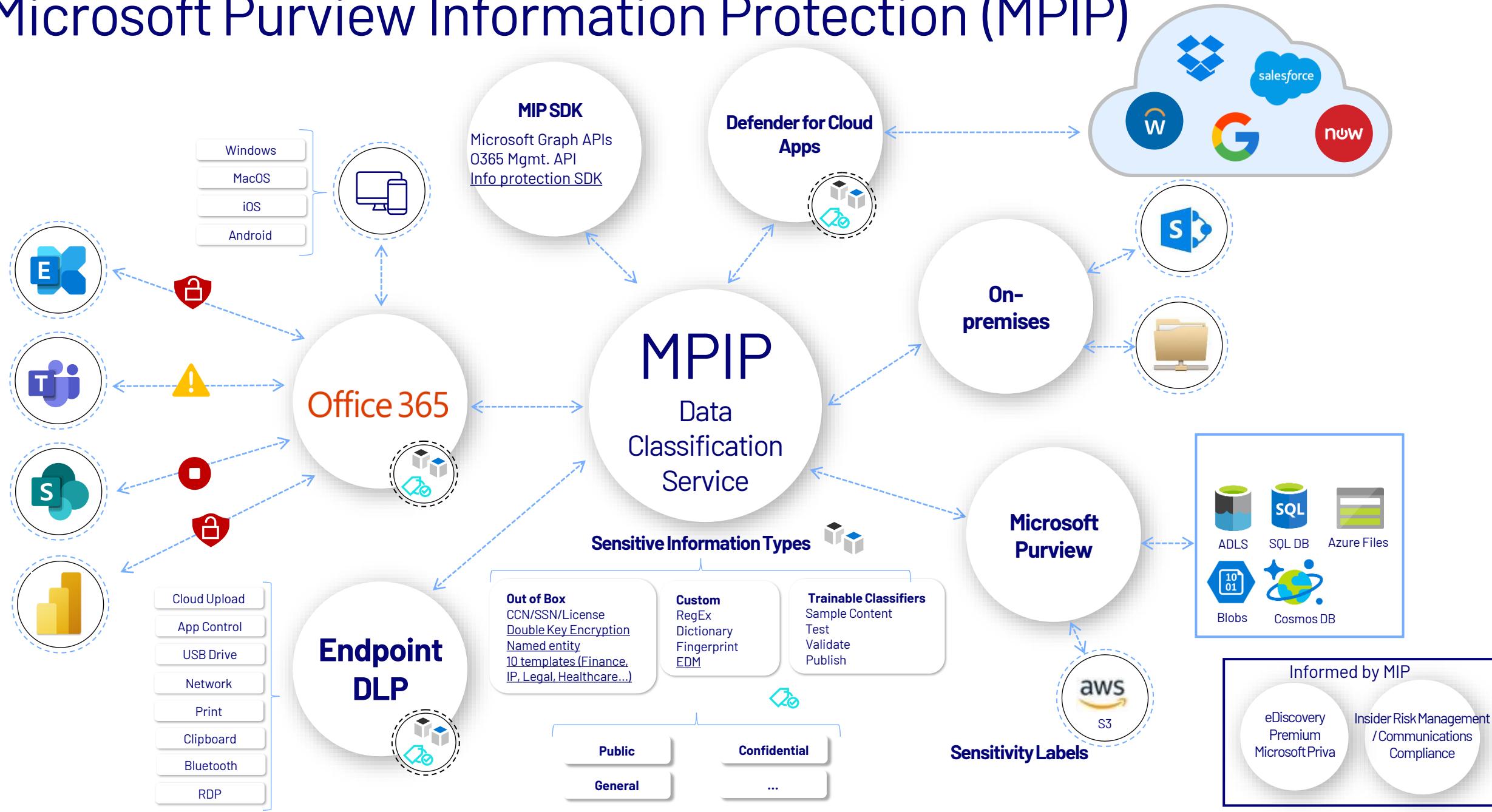
bit.ly/m365compliancemanager



Microsoft Purview Information Protection

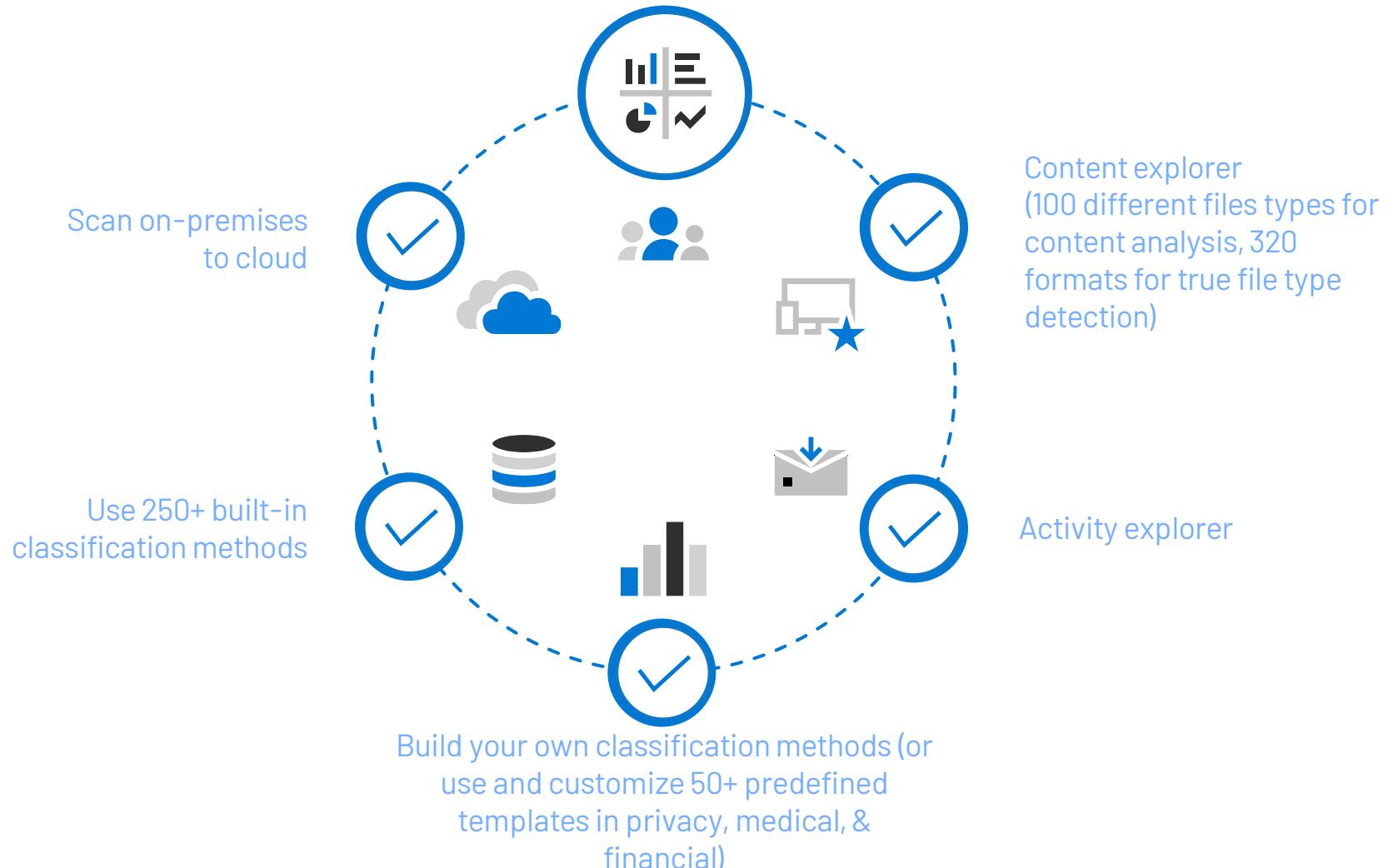


Microsoft Purview Information Protection (MPIP)



Flexible options to know your data

Understand what's sensitive, what's business critical & across your environment

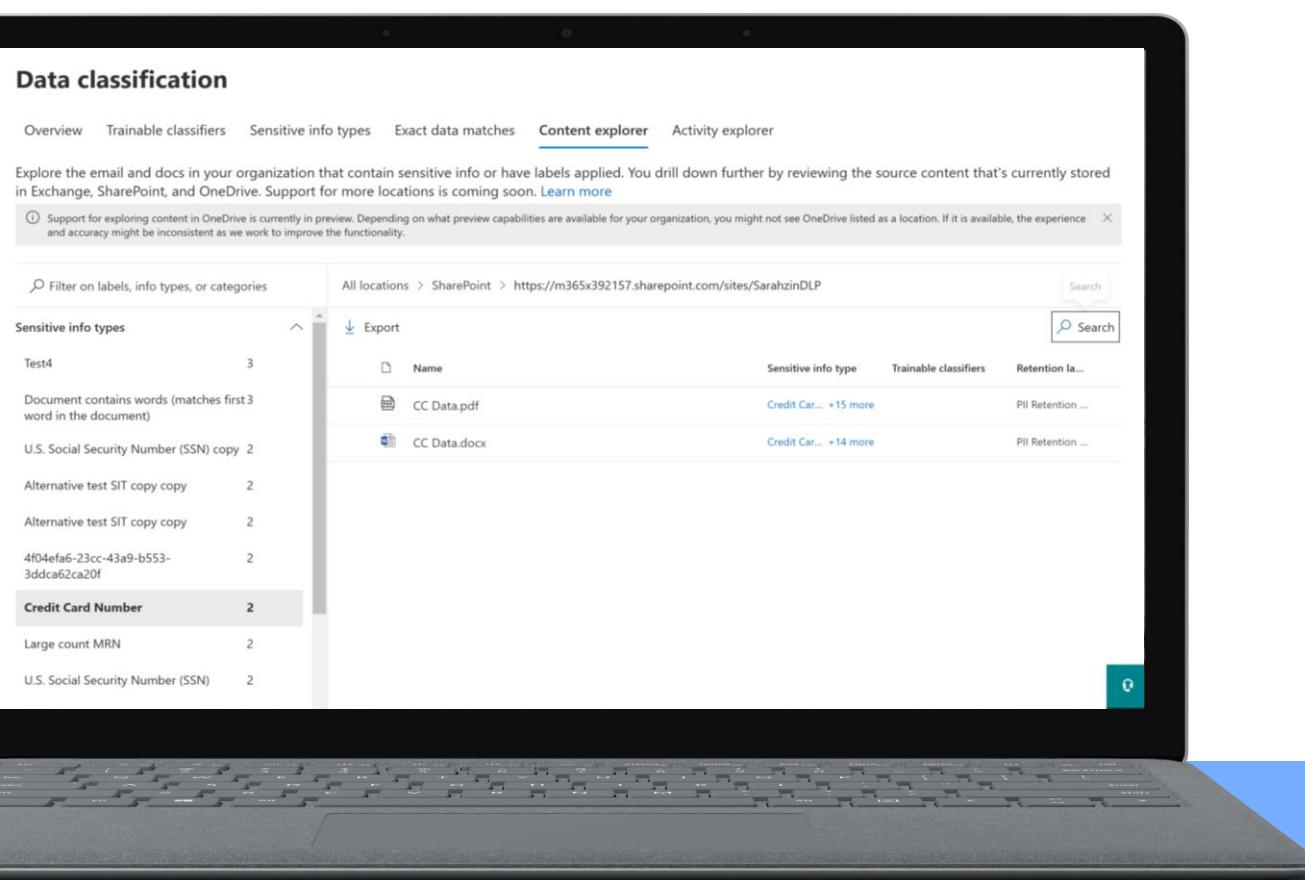


NEW AND RECENT BUILT-IN CLASSIFIERS

- Named entity detection region specific (full names, physical addresses, medical terms & conditions)
- 10 advanced policy authoring templates (GDPR, HIPAA, GLBA, & more)
- 9 ML-trainable classifiers (Finance, Tax, Legal, IP, Healthcare, & more)

Content explorer

A deeper view into your underlying data



The screenshot shows the Microsoft Content Explorer interface running on a laptop. The title bar says "Content explorer". The main area displays a list of documents under the heading "Sensitive info types". The list includes:

Sensitive info type	Name	Trainable classifiers	Retention la...
Test4	CC Data.pdf	Credit Car... +15 more	PII Retention ...
Document contains words (matches first 3 word in the document)	CC Data.docx	Credit Car... +14 more	PII Retention ...
U.S. Social Security Number (SSN) copy			
Alternative test SIT copy			
Alternative test SIT copy			
4f04efa6-23cc-43a9-b553-3ddca62ca20f			
Credit Card Number			
Large count MRN			
U.S. Social Security Number (SSN)			

At the bottom left, there's a sidebar titled "Data classification" with a list of categories like "Test4", "Document contains words", etc. A status bar at the bottom indicates "Large count MRN" and "U.S. Social Security Number (SSN)".



Visibility into amount of sensitive data in a document that triggered the classification to be applied



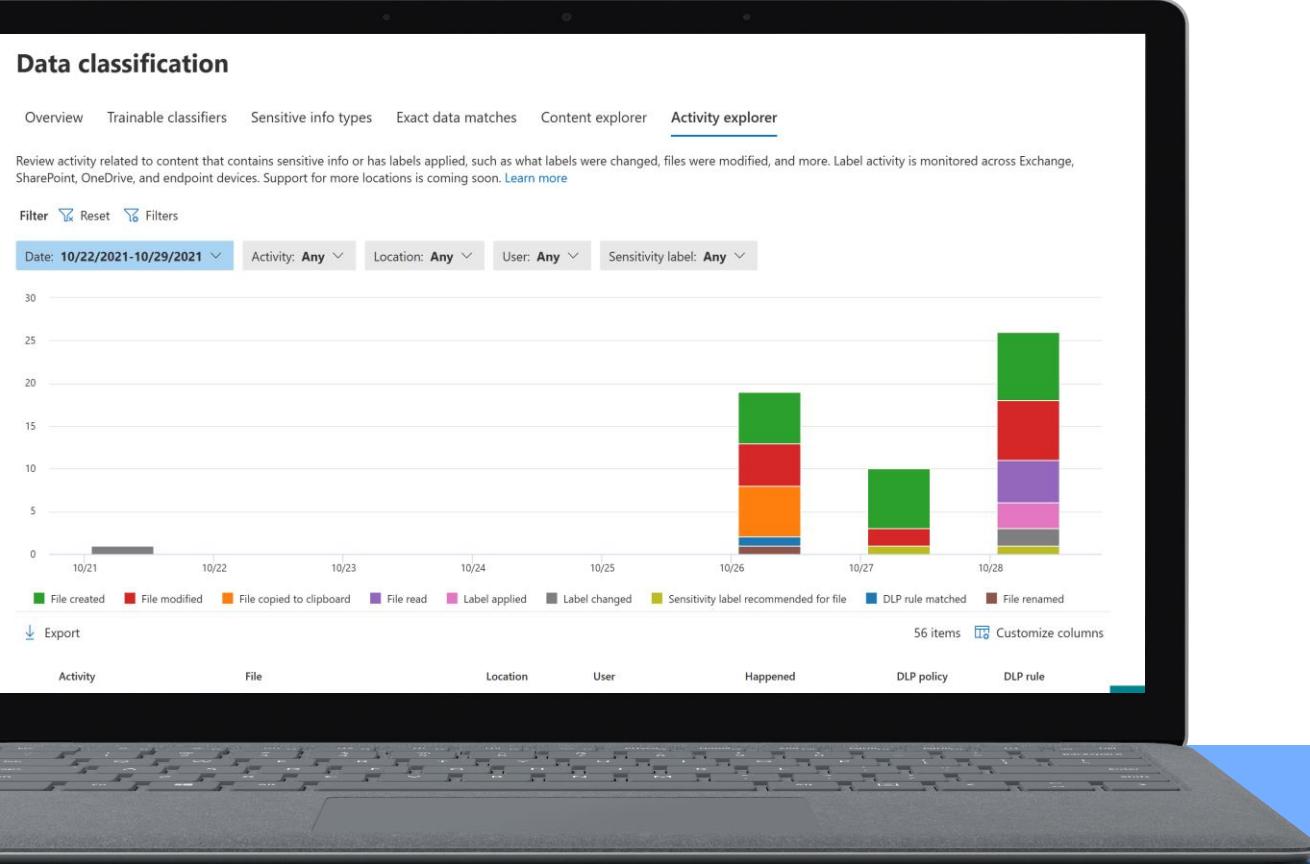
Ability to filter by label to get a more detailed view including locations of where documents are stored



Integrated native viewer displays a rich view of documents, providing context for policy creation

Activity explorer

A better understanding of activities related to your data



Visibility into activities on sensitive data, including data sharing and label downgrades



Ability to filter the data to see all the details for a specific label, file, file types, user and importantly interesting activities



Understanding of a broad-spectrum of activities across documents by location

Protect your data

Classify data and apply unified sensitivity labels to sensitive data

Customizable

Persists as container metadata or file metadata

Enables protection policies like DLP based on labels

Manual or Automated Labels

Label data at rest, data in use, or data in transit

Extensible: readable by other systems



NEW AND RECENT ADVANCEMENTS

- Protect content with Sensitivity Labels using double-key encryption
- Auto labeling on SPO/ODB and EXO DIT with additional conditions & increased scopes
- Enhanced simulation mode

Information Protection: Best Practices

Classification Taxonomy: Defining the right label taxonomy and protection policies is the most critical step in a Microsoft Information Protection deployment. Labels will be the interface for users to understand content sensitivity, how it matches company policies, and will be the primary input for users to flag content that needs to be protected.

Detect your data: Discover your sensitive information in your existing repositories. This is the first step we recommend as part of our best practice approach to detect the data you own and be ready to configure it as part of your sensitivity label configurations as well as data loss prevention policies later in this guide.

Interaction: Consider the methods in which users will interact with MIP labels and how you intend to implement this.

Communication: Schedule multiple workshops with stakeholders during the testing phase to validate the label taxonomy is working effectively and catch any changes needed before wholesale deployment to production has occurred avoiding the need to reclassify large amounts of data in the future.

Information Protection: Best Practices

Sublabels: Labels are generally used to represent the actual sensitivity of the content that is labeled, while sublabels are typically used to represent variations in the protection or the scope of the content.

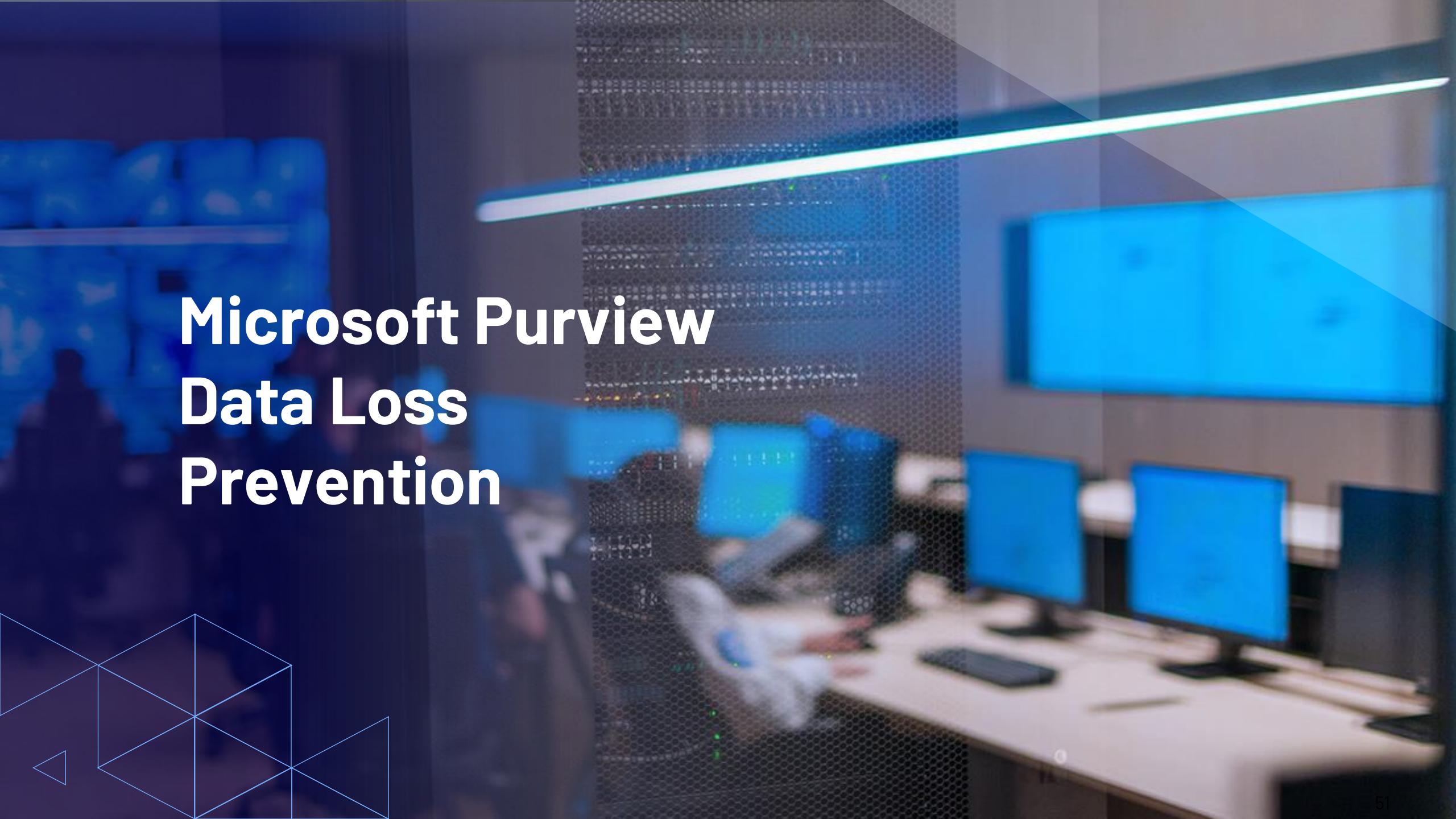
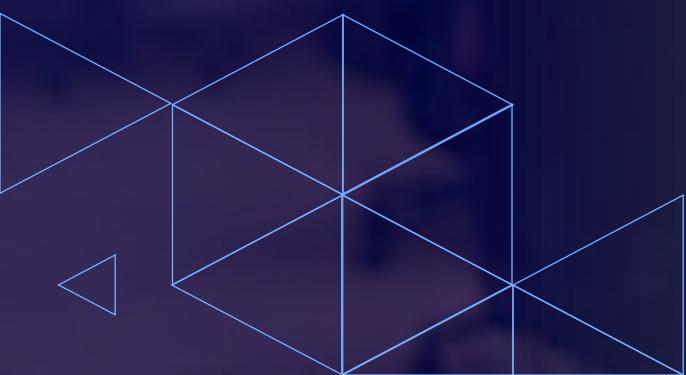
Keep it Simple: no more than five top level labels and five sublabels. User experience research shows that with five or fewer labels, users can target the desired label directly in a single movement, whereas if there are more elements in the list the user will typically have to read through them each time, making mistakes more likely.

Future Proof: Define labels that will last a long time. Since labels often become part of a company's culture and language, it is critical that they are not frequently altered, especially when it comes to the names and meanings of the top-level labels.

Testing: Ensure you have a well-documented test plan with clear tasks, testing scenarios and clear outcomes.

OCM: Establish end user training and education. Measure their understanding of the organization information protection policies.

Microsoft Purview Data Loss Prevention



Microsoft Purview Data Loss Prevention (MPDLP)

Prevent accidental or unauthorized sharing of sensitive data



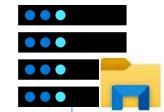
Microsoft 365
Cloud DLP - Service based



Endpoint
Endpoint - Platform based



Non-Microsoft apps
3rd party API based



On-premises
On-prem service



Guided onboarding
Unified & flexible policy management
Integrated with Microsoft Purview Information Protection
Unified alerting & remediation
Agentless and integrated within end user experiences

Unified and flexible policy management

Microsoft 365 compliance

Data Loss Prevention > Create a policy

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info on Windows devices is now in preview. Learn more about the capabilities

Status	Location	Included	Excluded
On	Exchange email	All	Choose distribution group
On	SharePoint sites	All	Choose site
On	OneDrive accounts	All	Choose account
On	Teams chat and channel messages	All	Choose account
On	Devices	All	Choose user or group
On	Microsoft Cloud App Security	All	Choose instance

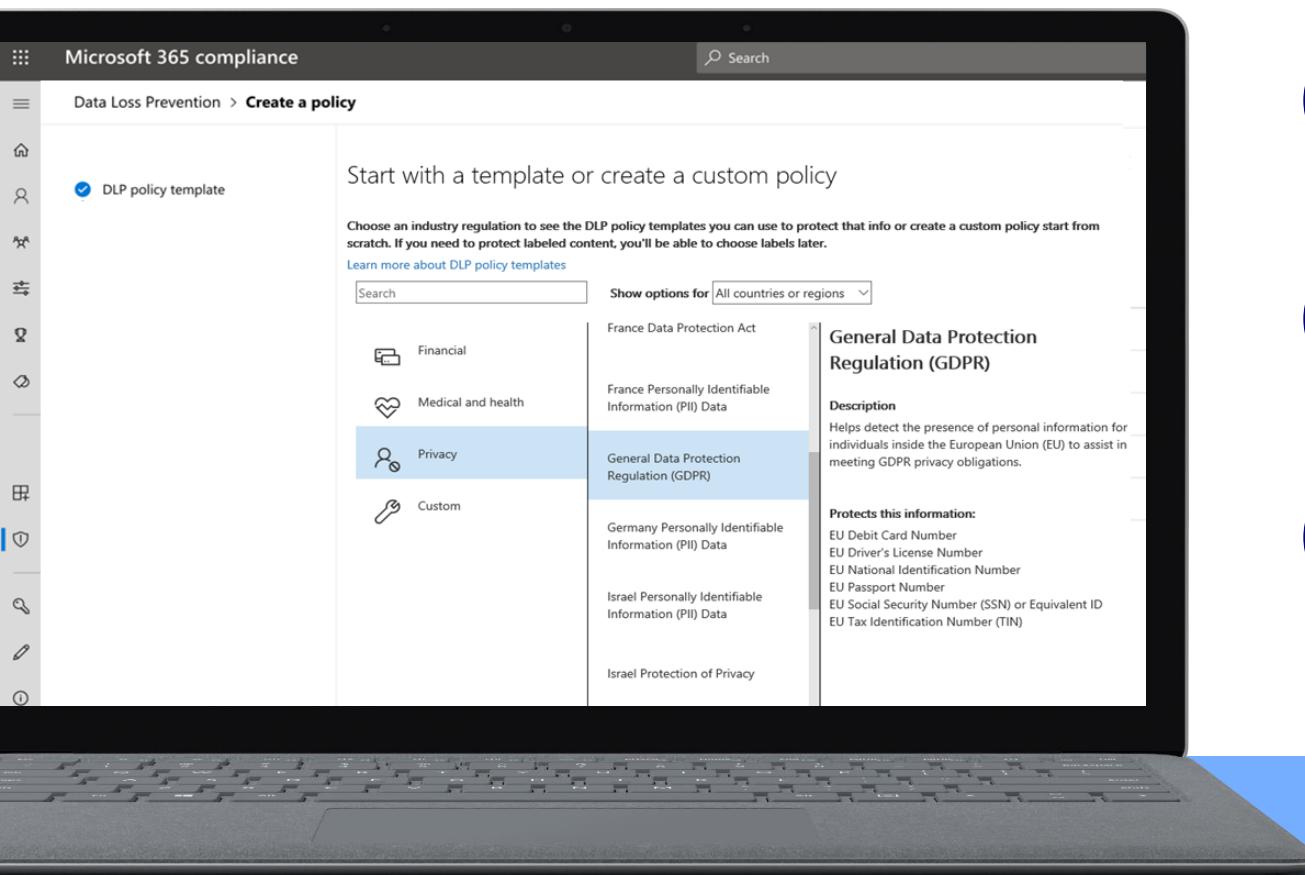


Unified, flexible policy management and enforcement across devices, apps and services from Microsoft 365 compliance center



Rich flexibility in configuring rules and enforcement actions

Integrated with Microsoft Purview Information Protection



100+ sensitive information types



40+ built-in policy templates



Labels as condition in DLP

Unified alerting and remediation

The screenshot shows the Microsoft 365 Admin Center interface, specifically the Data Loss Prevention section. The 'Alerts' tab is selected. A red box highlights a specific alert entry in the list:

DLP rule match detected : "CCN Rule" in "Sensitive Data Policy"

Details for the alert:

- Alert ID:** 98340HDFN9HGRWYHW2352
- Status:** New
- Alert severity:** High severity alert (red)
- User activity count:** 1
- Time detected:** 4:26 PM PST on 6/27/18
- Policy match:** Sensitive Data Policy
- Location(s):** Exchange, SharePoint
- Sensitive info types detected:** Employee Internal Data, Business Confidential Information, Confidential 85%, Social Security Number, Confidential 20%
- Actor(s) detected:** John Watson (john.watson@contoso.com)
- Notification sent to:** Sarah Chambers (sarah.chambers@contoso.com), Vincente Dion (vincente.dion@contoso.com)



Data-centric protection approach



Rich detail to triage and remediate



API support enabling SIEM integration

Data Loss Prevention: Best Practices

Stakeholder Engagement / Data Custodians: Identify the appropriate stakeholders and personas in your organization to collaborate for the design of DLP policies and workloads to be monitored.

Data Classifications: Identify the types of information you need to protect and where this information is stored. Consider using the Data Classification page in the M365 SCC to help with this identification.

Migrate Old Rules: Existing Exchange Online mail flow and DLP rules created in the Exchange Admin Center (EAC) will need to be gradually migrated to the M365 SCC, but will continue to function together with new policies created in the M365 SCC.

Test Mode: Always create DLP policies initially in test mode as this gives you an opportunity to determine not only if the policy is alerting correctly via email (nothing will flow through to the DLP reports in audit mode by design) but this will also allow you to determine if the thresholds you have configured for each rule are appropriate.

Out of the Box (OOTB): Consider using the out of the box (OOTB) SITs policy templates first, then start customizing the OOTB as you need if necessary.

Data Loss Prevention: Best Practices

Separate policies per workload: When creating DLP policies, consider separate policies per workload. For example, you might have a policy named “PCI-DSS-ExchangeOnline” and one named “PCI-DSS-SharePointOnline”. The reason for this is that when combining workloads, the DLP rules interface will only show conditions common to each workload chosen, which can lead to many options missing when incompatibilities occur.

Timing: When adding files to SharePoint Online and OneDrive for Business, there is an expected lag time between when the file is added, and indexing occurs.

DLP rule exceptions: Define exceptions to your DLP rules that are based on sensitivity labels. MIP labels are highly synergistic with traditional DLP.

Endpoint DLP: should be done automatically within a Mobile Device Management (MDM) when possible, such as Microsoft Intune or System Center Configuration Manager.

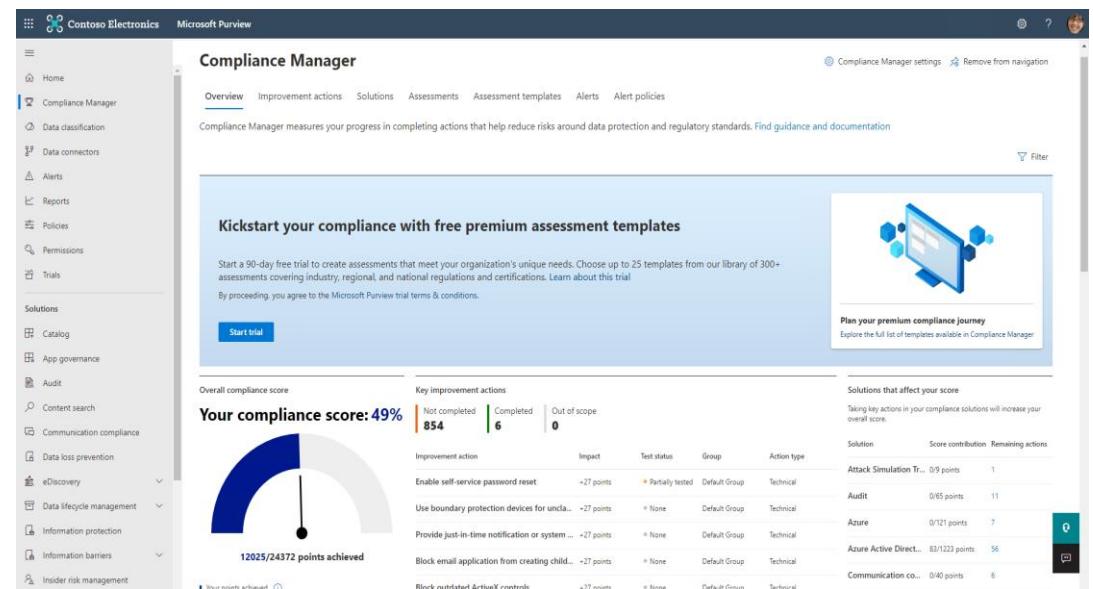
Microsoft 365 Platform Resources

Microsoft Secure & Compliance Score

Microsoft Secure Score: Assess your current security posture and identify potential improvements across all your Microsoft 365 workloads with centralized visibility from Secure Score.



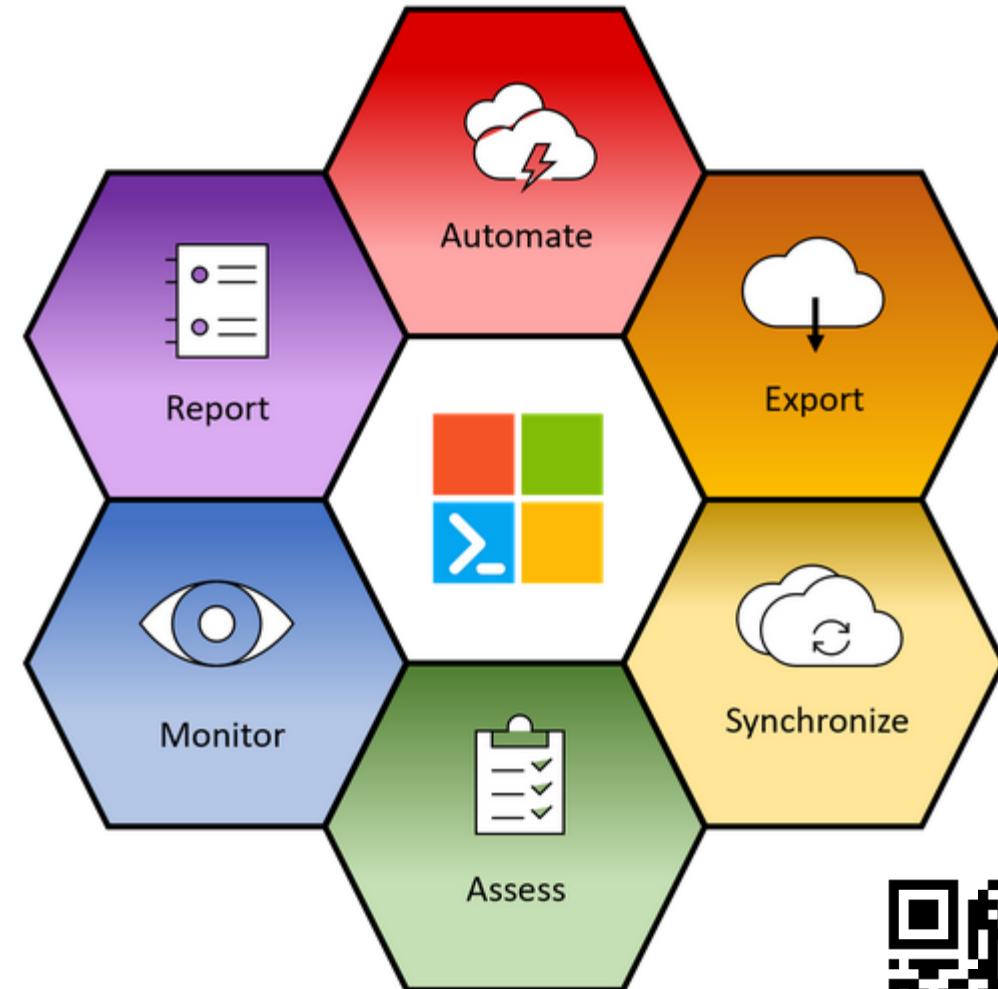
Microsoft Compliance Score: Part of the Microsoft Compliance Manager this scans through your Microsoft 365 environments and detect your system settings, continuously and automatically updating your technical control status.



Microsoft365DSC

Microsoft365DSC is an Open-Source initiative lead by Microsoft engineers and maintained by the community. It allows you to write a definition for how your Microsoft 365 tenant should be configured, automate the deployment of that configuration and ensures the monitoring of the defined configuration, notifying and acting on detected configuration drifts.

microsoft365dsc.com



Microsoft 365 Roadmap

Search for a specific item:

Filter the items below:

Product

Release phase

Platform

Cloud instance

New or updated

Clear all

Showing 430 updates: Launched Microsoft Teams In development

[Download](#) | [Share](#) | [RSS](#)

68 In development

Updates that are currently in development and testing

66 Rolling out

Updates that are beginning to roll out and are not yet available to all applicable customers

362 Launched

Fully released updates that are now generally available for applicable customers

[Sort by General Availability date](#)

[Newest to oldest](#)

> Microsoft Teams: New file sharing experience

GA: March 2021

> Microsoft Teams: Android On-Demand Chat Translation

GA: May 2021

<https://aka.ms/roadmap>



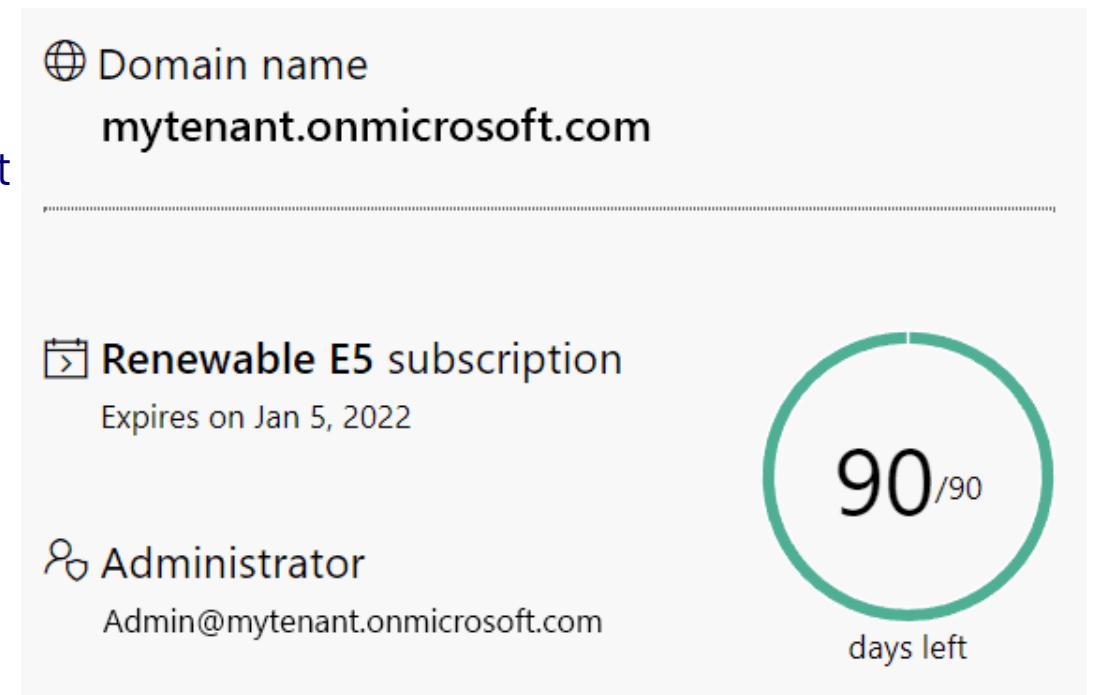
Microsoft 365 Developer Program

Be your own administrator and prototype apps and solutions on your fully pre-provisioned sandbox subscription.

- Includes 25 user licenses for development purposes
- Preconfigured for sideloading Teams apps
- Fully loaded sample data with 16 sample users, user data, and content to help you model your solutions.
- Easy access to pre-provisioned core Microsoft 365 workloads and capabilities (Windows not included), including:
 - All Office 365 apps
 - Everything you need for Power Platform development
 - Office 365 Advanced Threat Protection
 - Advanced analytics with Power BI
 - Azure Active Directory for building advanced IDAM solution



<https://bit.ly/m365devprogram>



FastTrack for Microsoft 365

FastTrack for Microsoft 365 helps organizations enable hybrid work with expert guidance—delivered remotely by Microsoft engineers and approved FastTrack Ready Partners at no additional cost for the life of your eligible subscription.

Eligibility:

All customers can access self-serve resources on this site. Log in for guidance and planning resources to support your Microsoft 365 deployment.

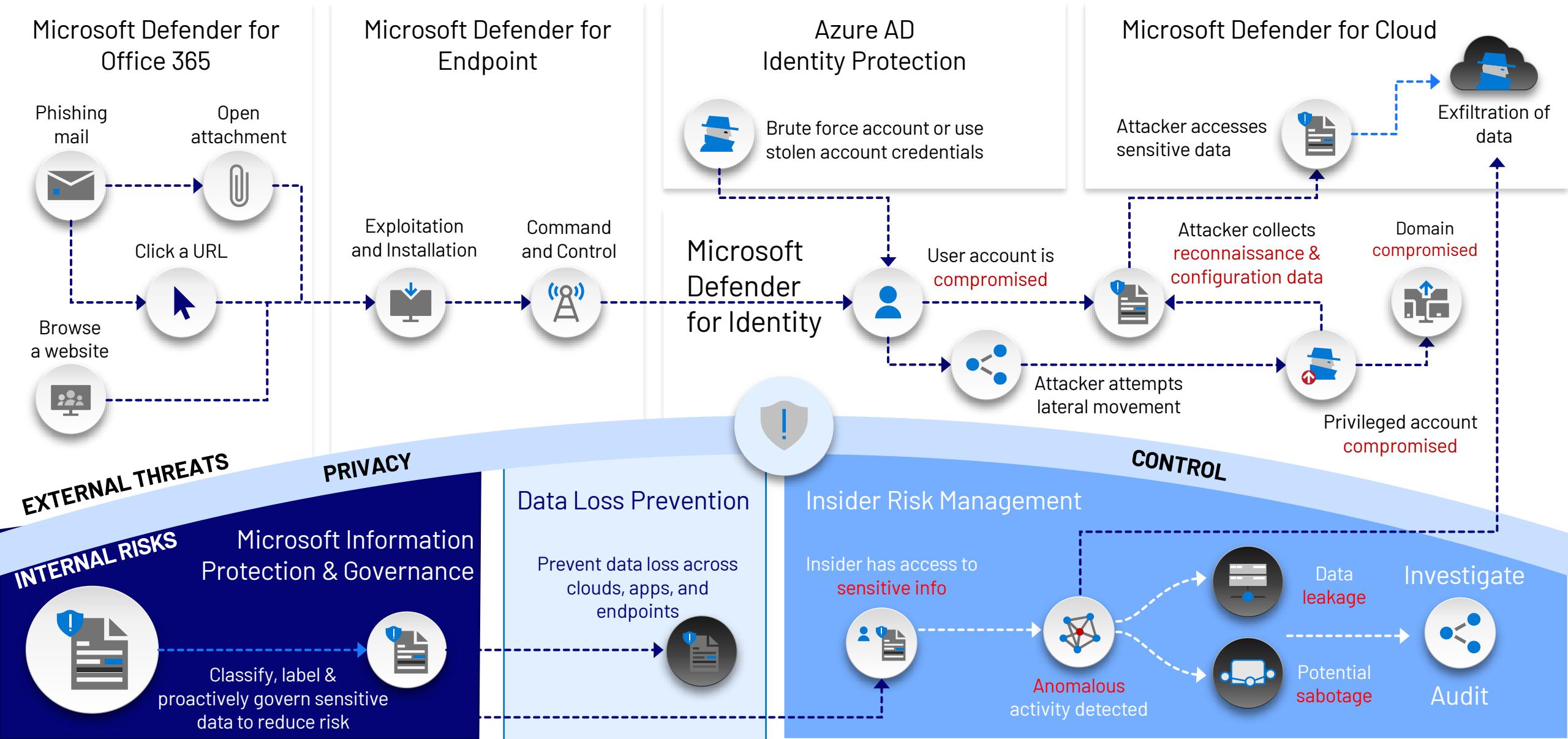
Your subscription **of 150+ licenses** includes ongoing access to FastTrack specialists to remotely support your Microsoft 365 cloud deployment and adoption.

With your subscription **of 500+ licenses**, FastTrack will assist with migrating your data and email, freeing up time to deploy more solutions at once.

bit.ly/msfasttrack



Internal and external protection across the spectrum



Final Thoughts

- **Resources:** Microsoft and the community have ENDLESS amount of amazing resources to help support you on your adoption journey.
- **Flexibility:** benefit of being able to simply enable (vs deploy) a LOT of the stack in audit mode - running side-by-side existing investments - to ramp up visibility and response capabilities, then rapidly turn the screws on protective controls/displacing existing investments.
- **Guard rails not roadblocks:** leverage the integrated end-user experience to coach good behaviour, instead of iron-clad blocking and business disruption.
- **Start with the business:** Define what it is that is sensitive to your business: use the built-in SITs as a starting point. Enable in audit/warn first and learn. Use Content Explore and Activity Explorer to make data driven decisions.
- **Run the Insider Risk assessment** it's a few clicks of effort and can provide a good view of immediate risks.



Where to from here?

Microsoft Licensing Maps: m365maps.com

Microsoft 365 Defender: aka.ms/ms365d

Defender Eligibility: aka.ms/ms365d-eligibility

Defender Try Today: security.microsoft.com

Defender for Office 365: aka.ms/DefenderO365

Stay up to date: aka.ms/MDOblog

Defender for Office 365: aka.ms/MDOdocs

Fasttrack advisory services: bit.ly/msfasttrack

Microsoft Dev Program: bit.ly/m365devprogram

Microsoft 365 Roadmap: aka.ms/roadmap

Partner Community: microsoftpartnercommunity.com

Ninja Content: bit.ly/M365DefenderNinja

Compliance One Stop Shop: aka.ms/mipc/oss

Blogs: aka.ms/ipgblog

IP&G sessions: aka.ms/VideoHub/IPG

Online roadmap tool: aka.ms/mipc/roadmap

Licensing: aka.ms/compliancesd

Mapping of features to SKUs: aka.ms/MIPLicensing

Microsoft Purview Website: aka.ms/MicrosoftPurview

Documentation: aka.ms/DLPdocs

Blogs: aka.ms/DLPblogs

Microsoft Purview CxE:

microsoft.github.io/ComplianceCxE/dag

Microsoft Defender for Office 365 Security Operations Guide:

aka.ms/opmdo

Couldn't save every link?

Bonus points to anyone who saved all the links in todays presentations.

However, If you didn't have time to save every link no stress you can find this presentation on GitHub.

github.com/chrisgecks/presentations





Thank You!
Questions?

