Adopting Microsoft 365 E5

Chris Gecks

Solutions Architect / Consultant

chris.gecks@cybercx.com.au

CyberCX

Agenda

01 Introduction

02 Microsoft 365 Journey

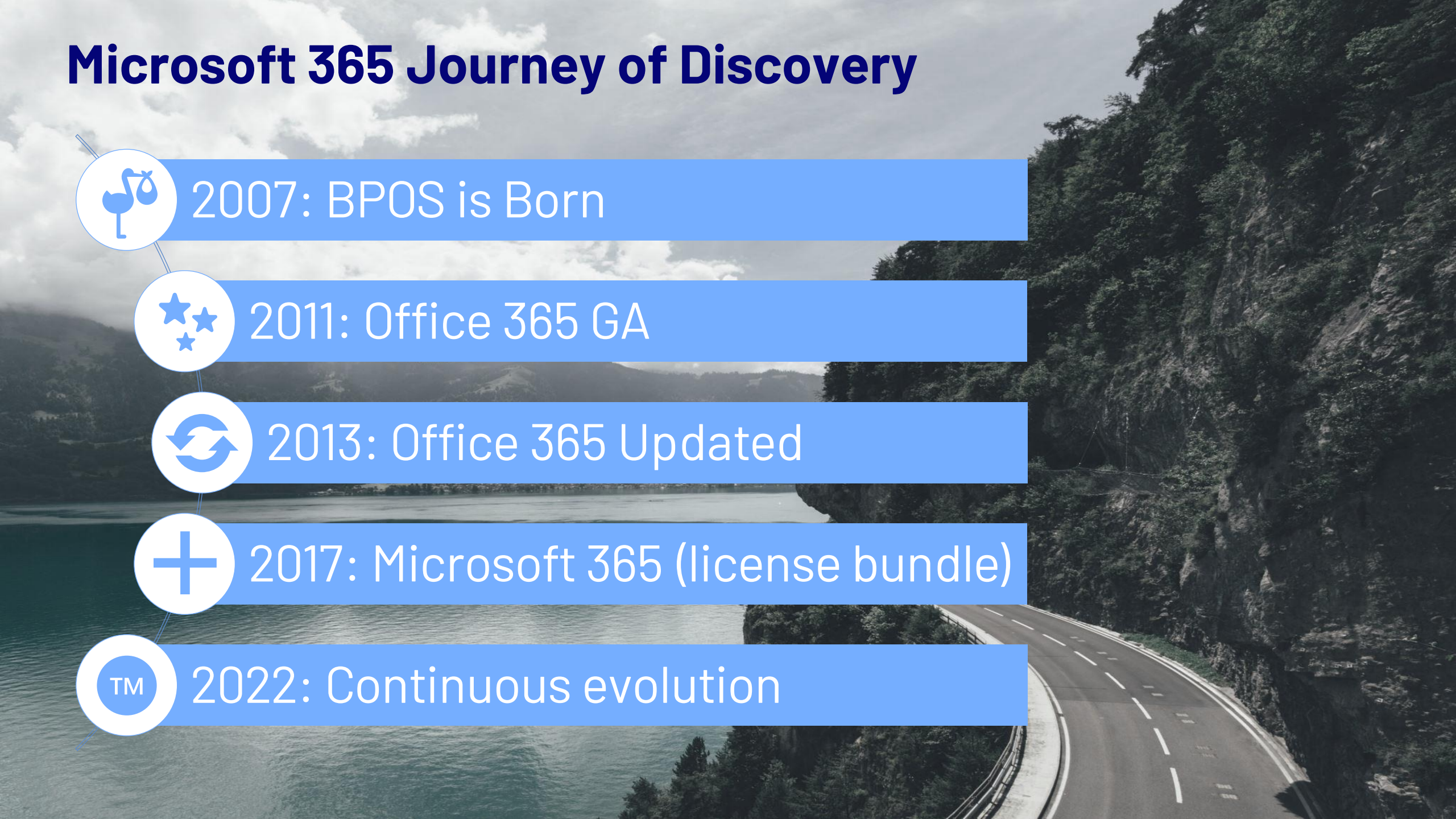
03 Microsoft Licensing & Zero Trust

04 Microsoft Defender

05 Microsoft Purview

06 Questions

Microsoft 365 Journey of Discovery



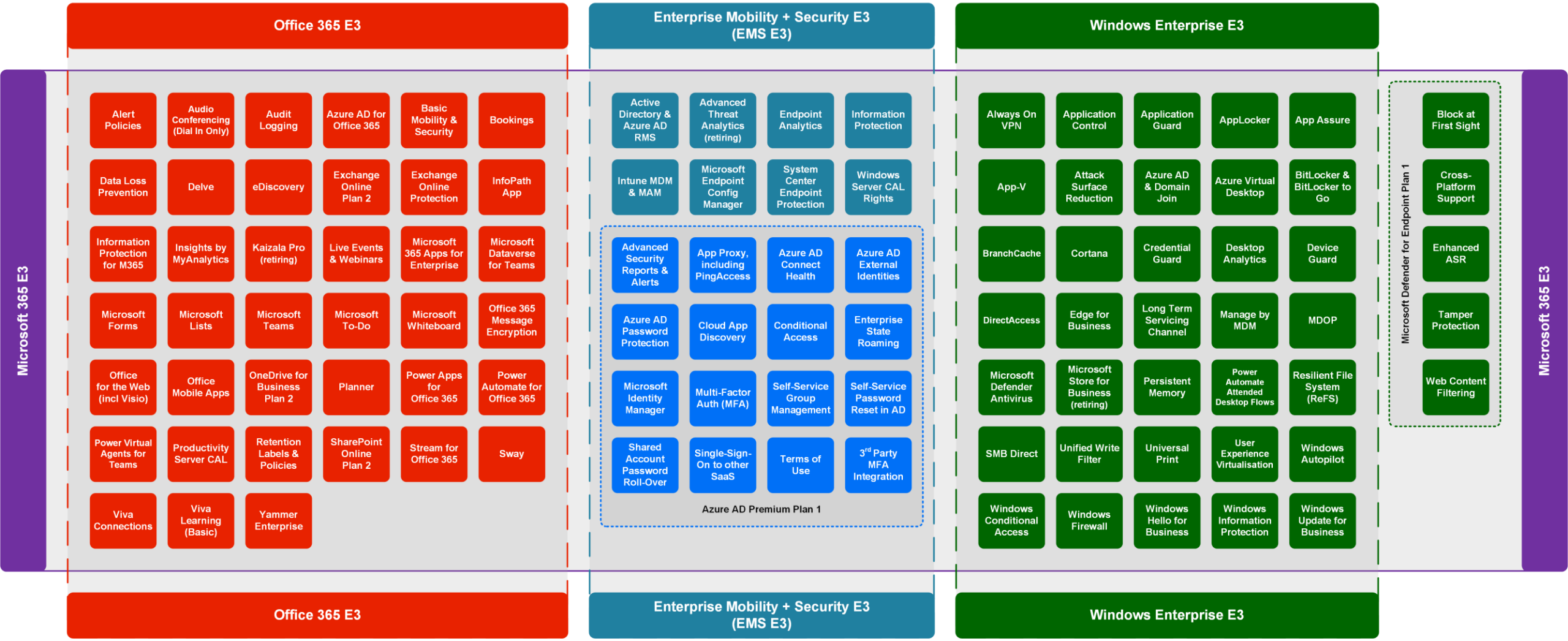
- 2007: BPOS is Born
- 2011: Office 365 GA
- 2013: Office 365 Updated
- 2017: Microsoft 365 (license bundle)
- 2022: Continuous evolution™

Licensing

Microsoft 365 E3

January 2022

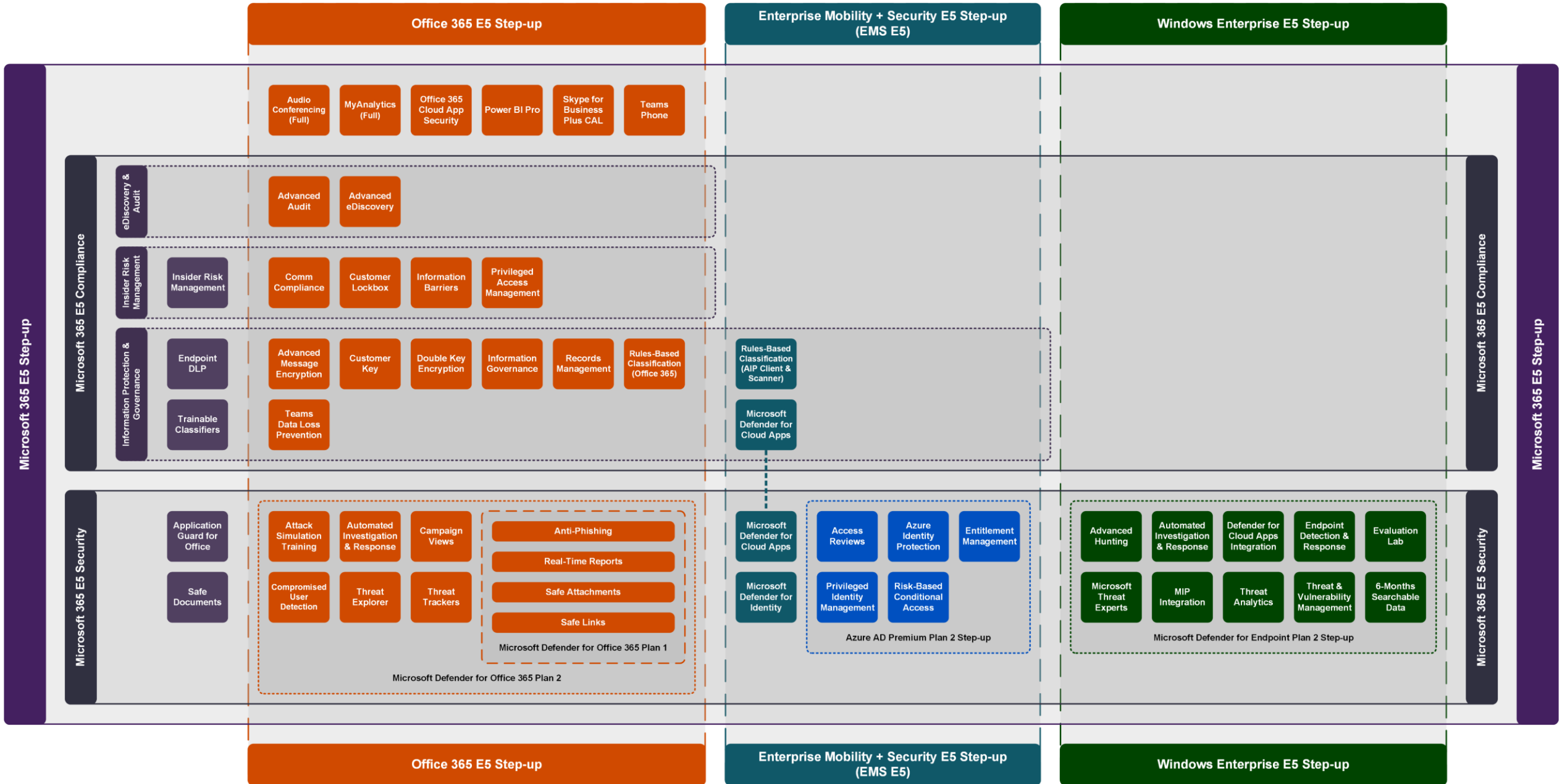
m365maps.com



Microsoft 365 E5 Step-up

January 2022

m365maps.com



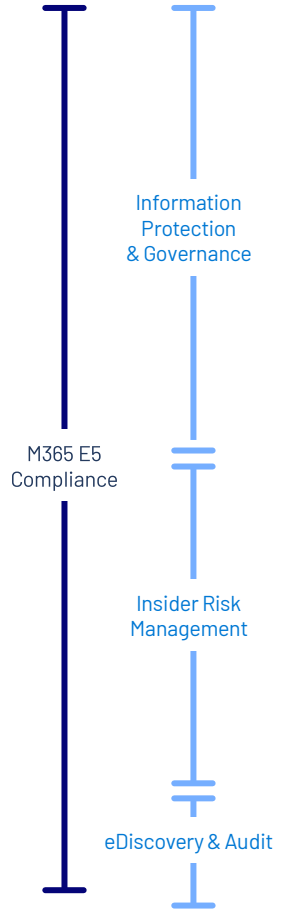
Microsoft 365 E5 Security[1]

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 Documents[2]	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 365[2]	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



Data Lifecycle and Records Management
Use retention labels and policies to retain and delete information.

Data Loss Prevention (DLP)
Identify, monitor, and automatically protect sensitive information stored across Office 365 locations.

Information Protection
Identify and protect sensitive data including credit card, bank account, and passport numbers.

Message Encryption
Send and receive encrypted email messages to people inside and outside your organization.

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 service.

Customer Key
Help meet compliance requirements by exercising control over your organization's encryption keys.

Customer Lockbox
Maintain control over your content with explicit access authorization for service operations.

Communication Compliance
Minimize communication risks by detecting, capturing, and taking remediation actions on inappropriate messages in your organization.

Privileged Access Management
Help protect your organization from breaches through granular access control over privileged admin tasks.

Insider Risk Management
Detect, investigate, and take action on risky activities in your organization.

Information Barriers
Restrict communications between specific groups of users inside your organization to safeguard internal information.

eDiscovery (Premium)
Manage the end-to-end workflow of internal and external investigations.

Audit (Premium)
Gain visibility with new auditing capabilities that help with forensic and compliance investigations.

Microsoft 365 E5 Compliance | Microsoft Security

Microsoft EMS E3 and E5 Packaging[1]

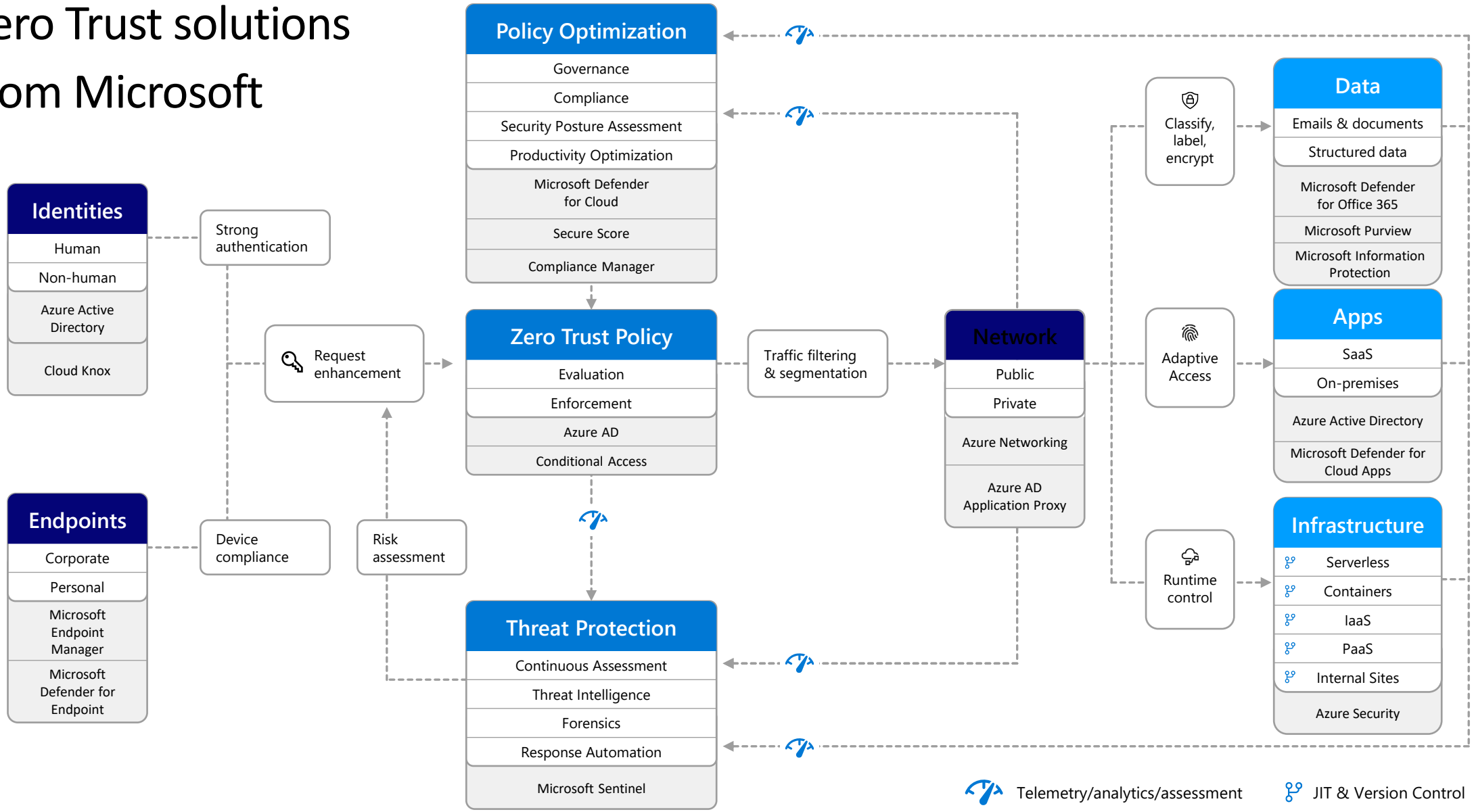
Azure Active Directory P2	Includes all P1 capabilities, as well as Identity Protection (risk based conditional access), and Identity Governance (PIM). The most trusted identity and access management solution in the market that helps you safeguard user credentials and connect people securely to the apps they need.
Azure Information Protection P2[2]	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 Analytics[3]	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

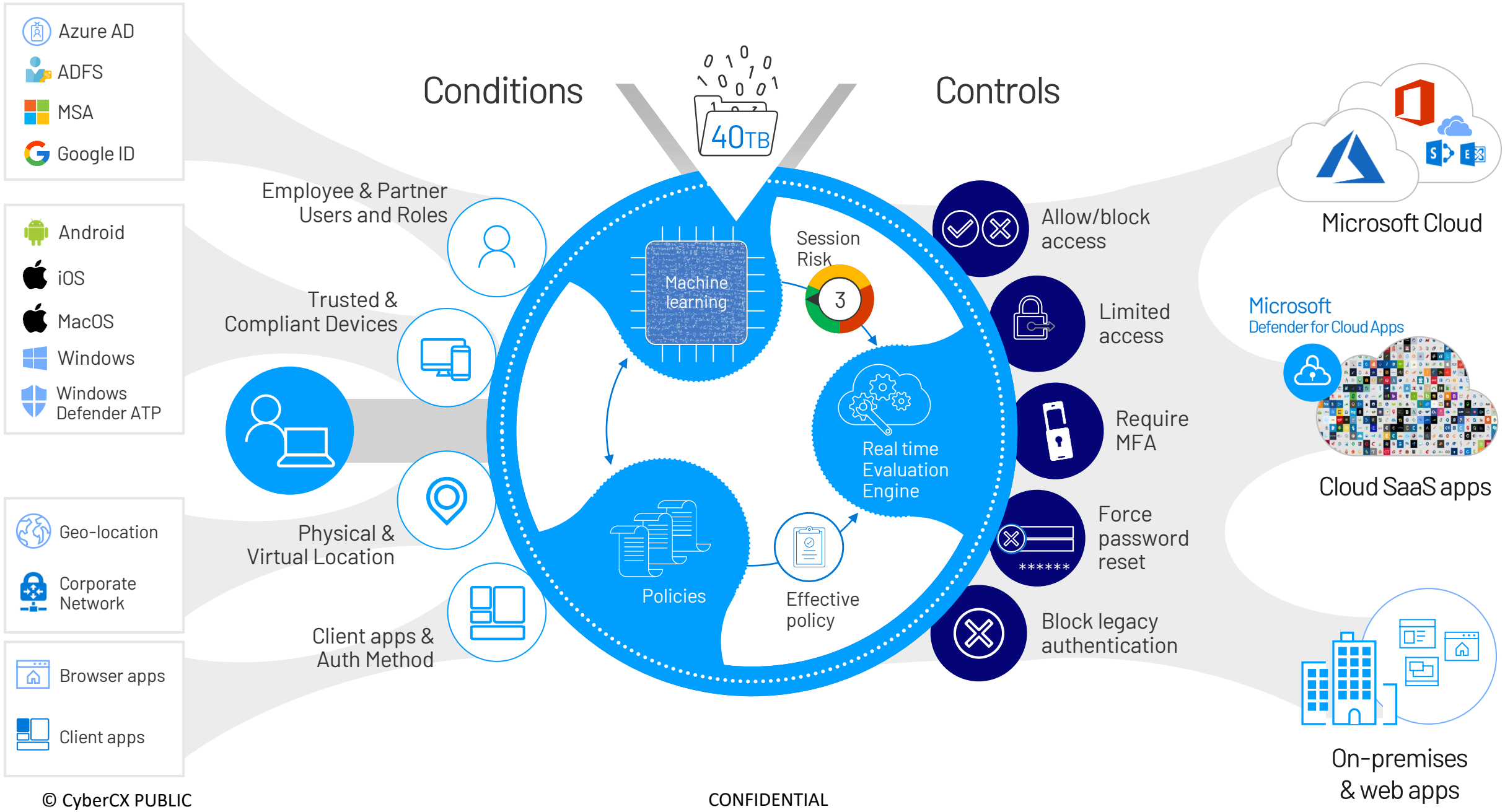
Zero Trust

Microsoft Security

Zero Trust solutions from Microsoft



Azure AD conditional access (Zero Trust)




CRAWL
WALK
RUN

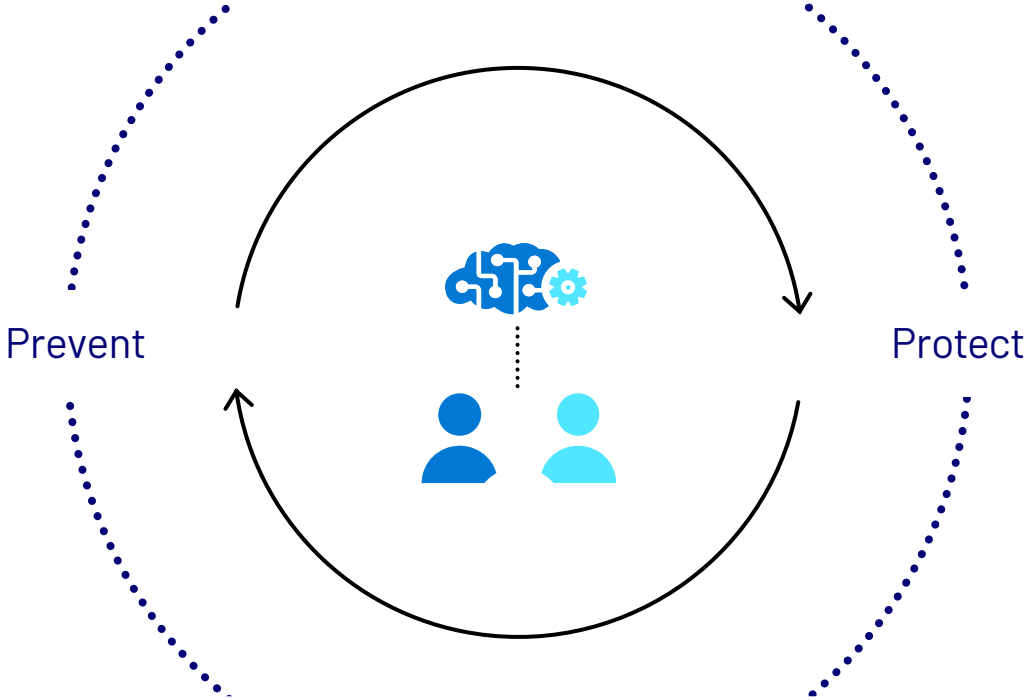
Microsoft 365 Defender

SIEM

Azure Sentinel

Multi-cloud

Partnerships



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

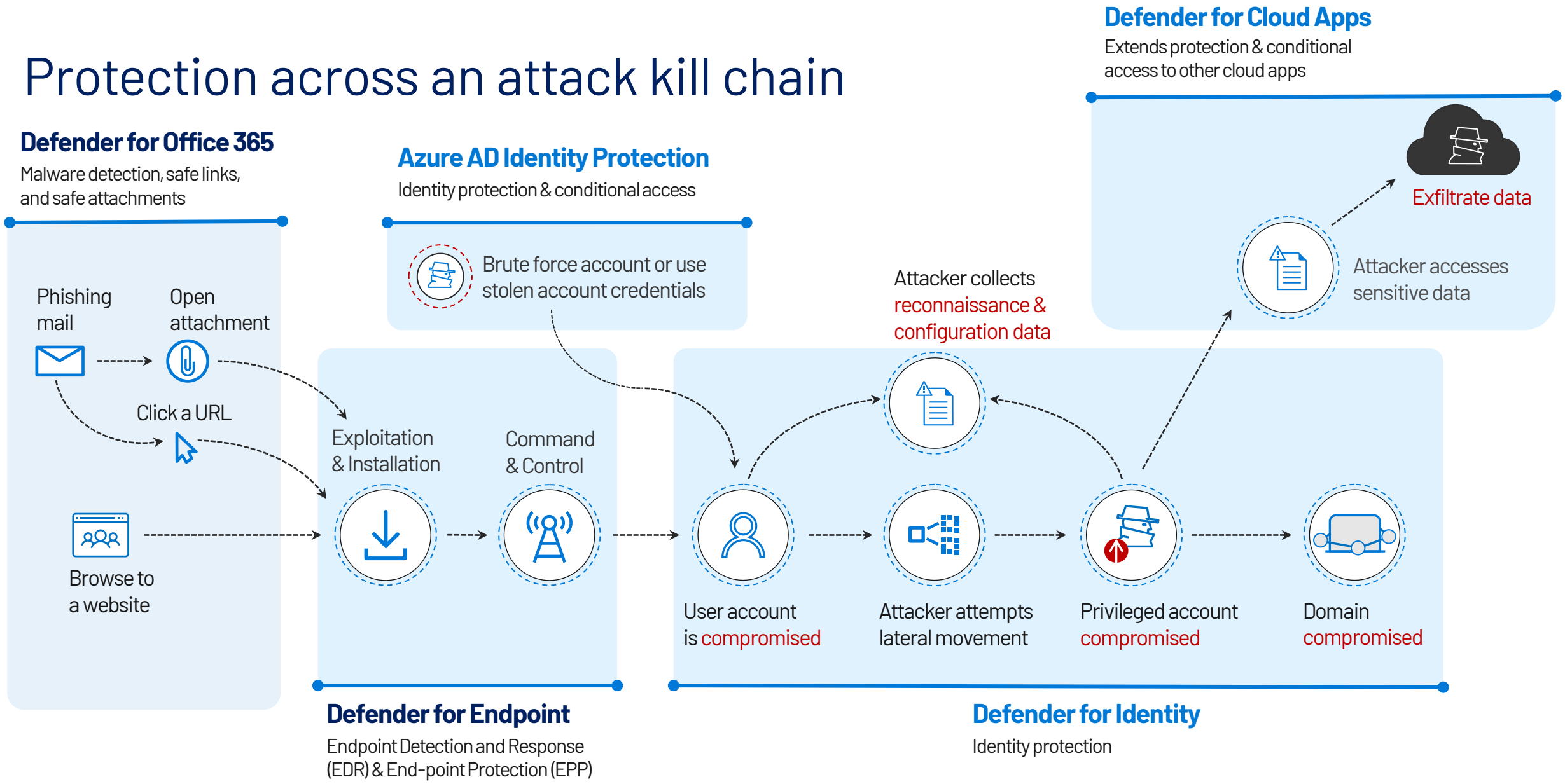
Email & collaboration

Microsoft Defender for Office 365

SIEM

Microsoft Sentinel

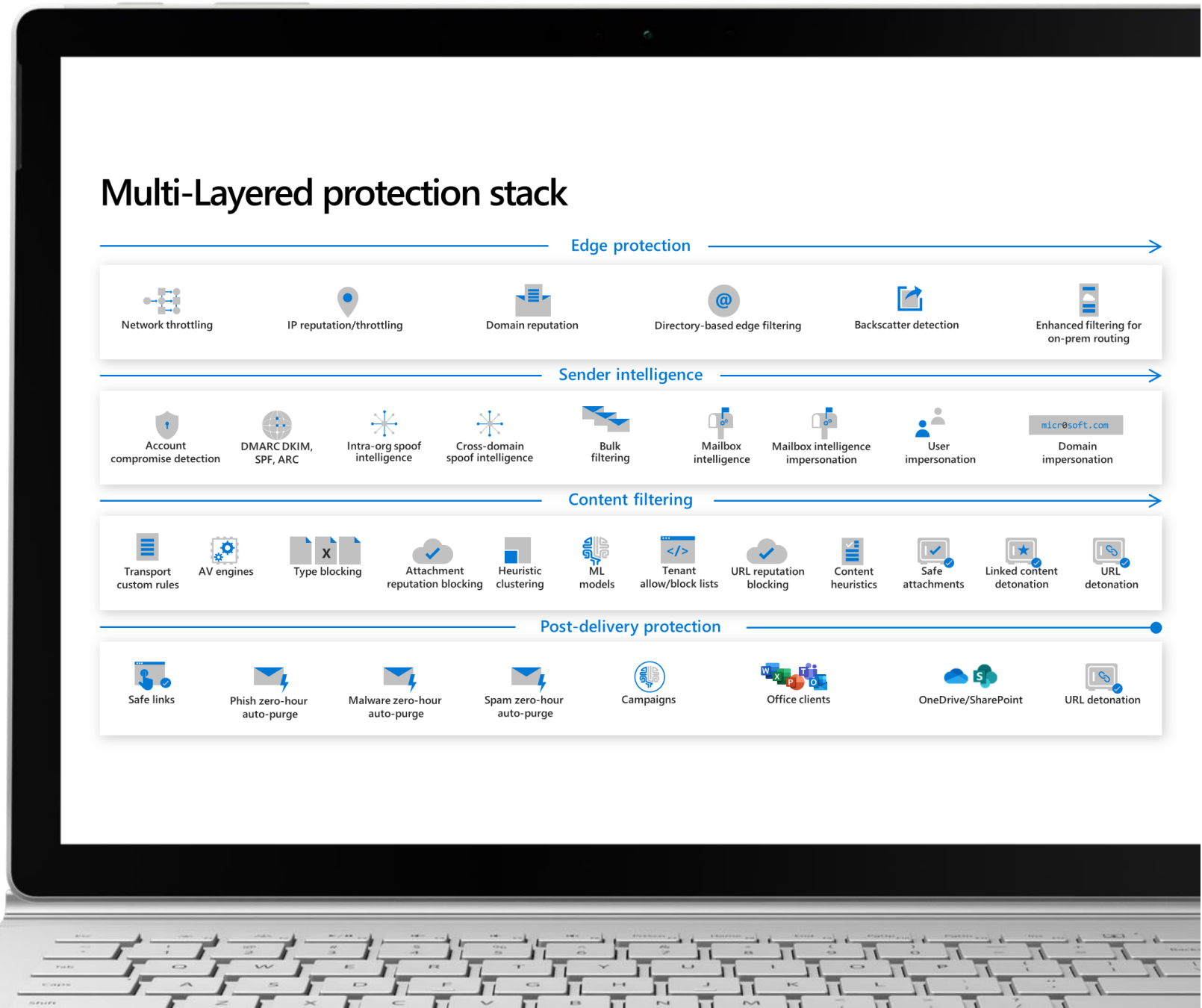
Protection across an attack kill chain



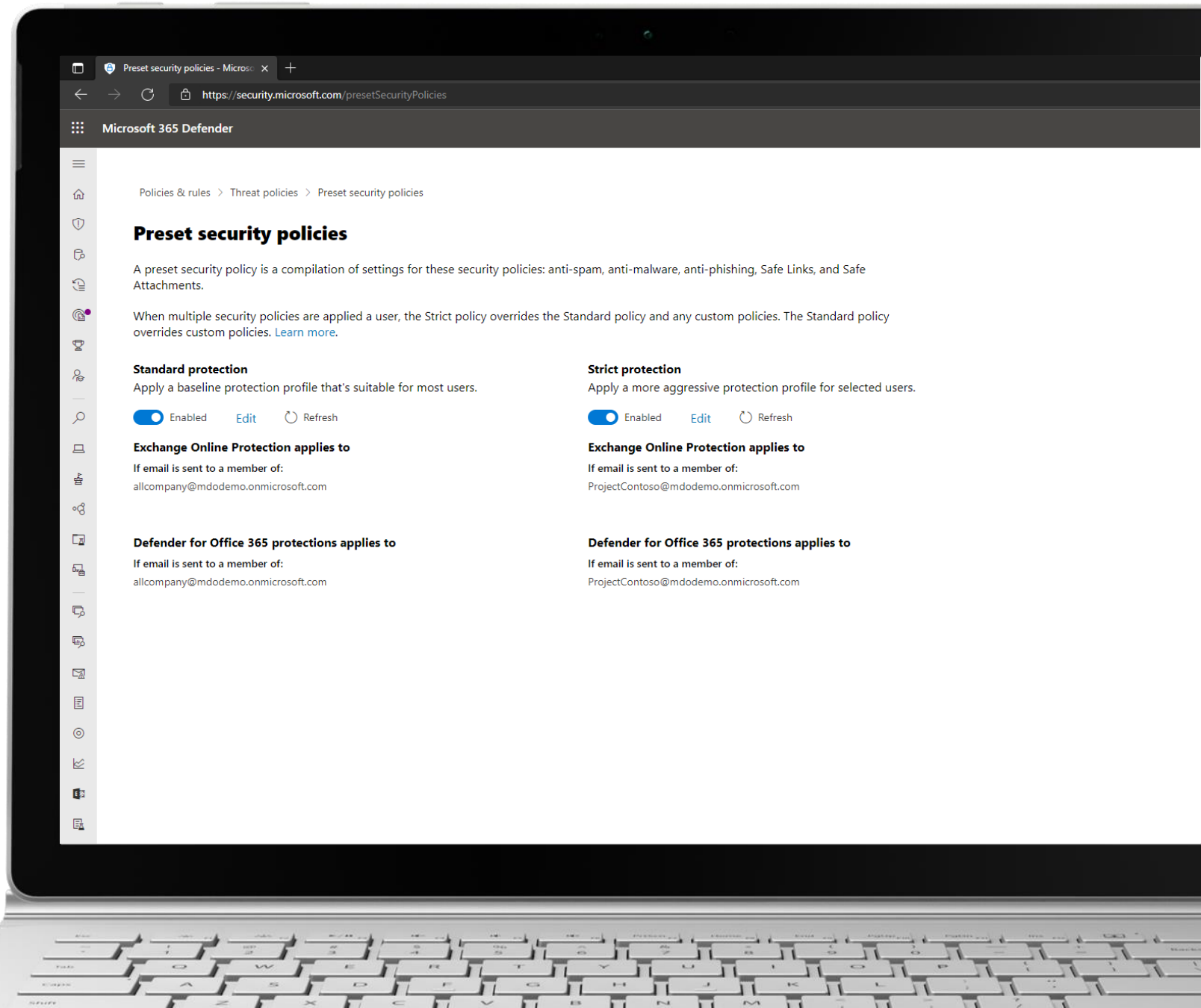
Microsoft Defender for Office 365 (MDO)

Securing your enterprise requires more than just prevention

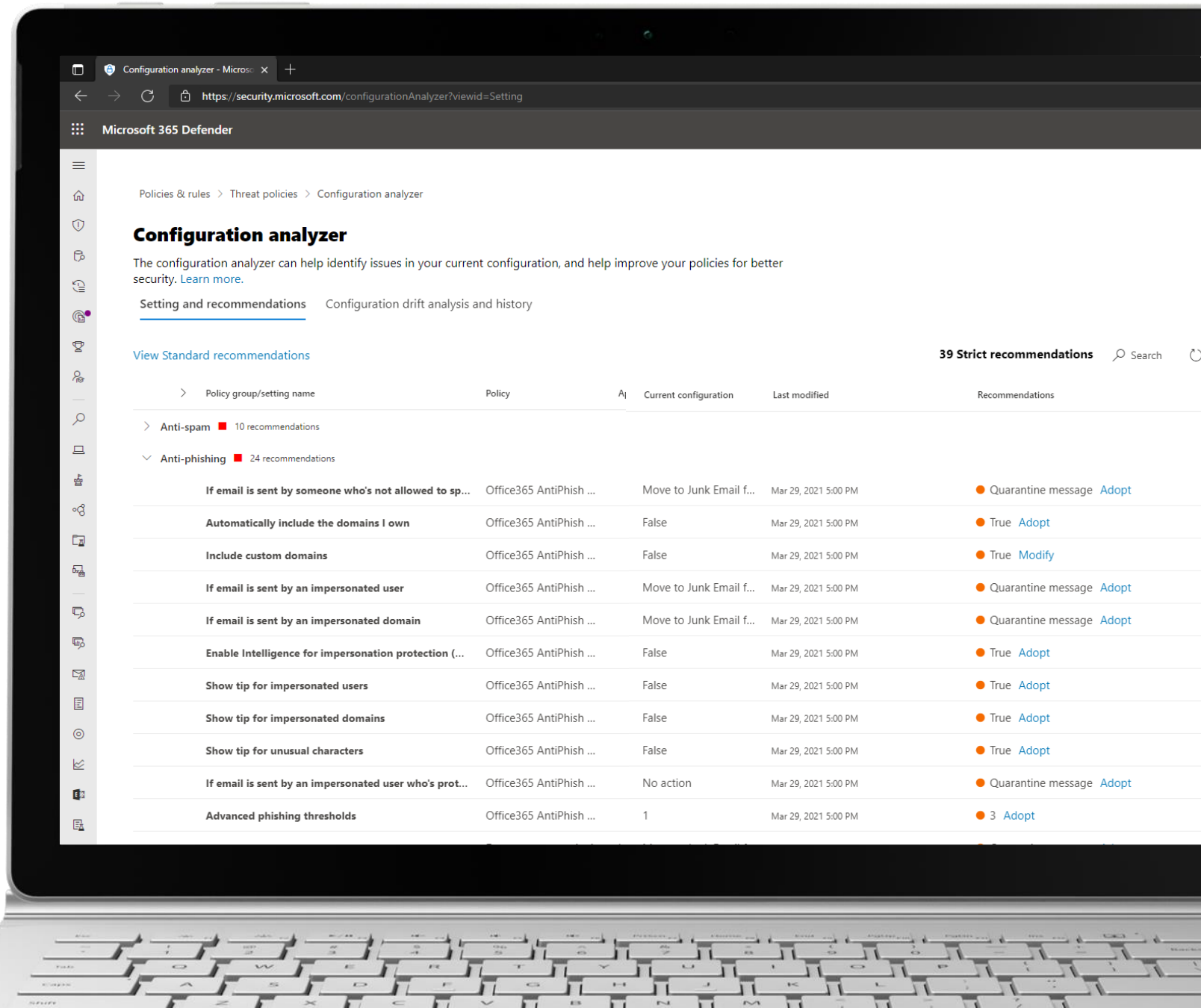
Multi-layered protection stack stops a wide variety of attacks



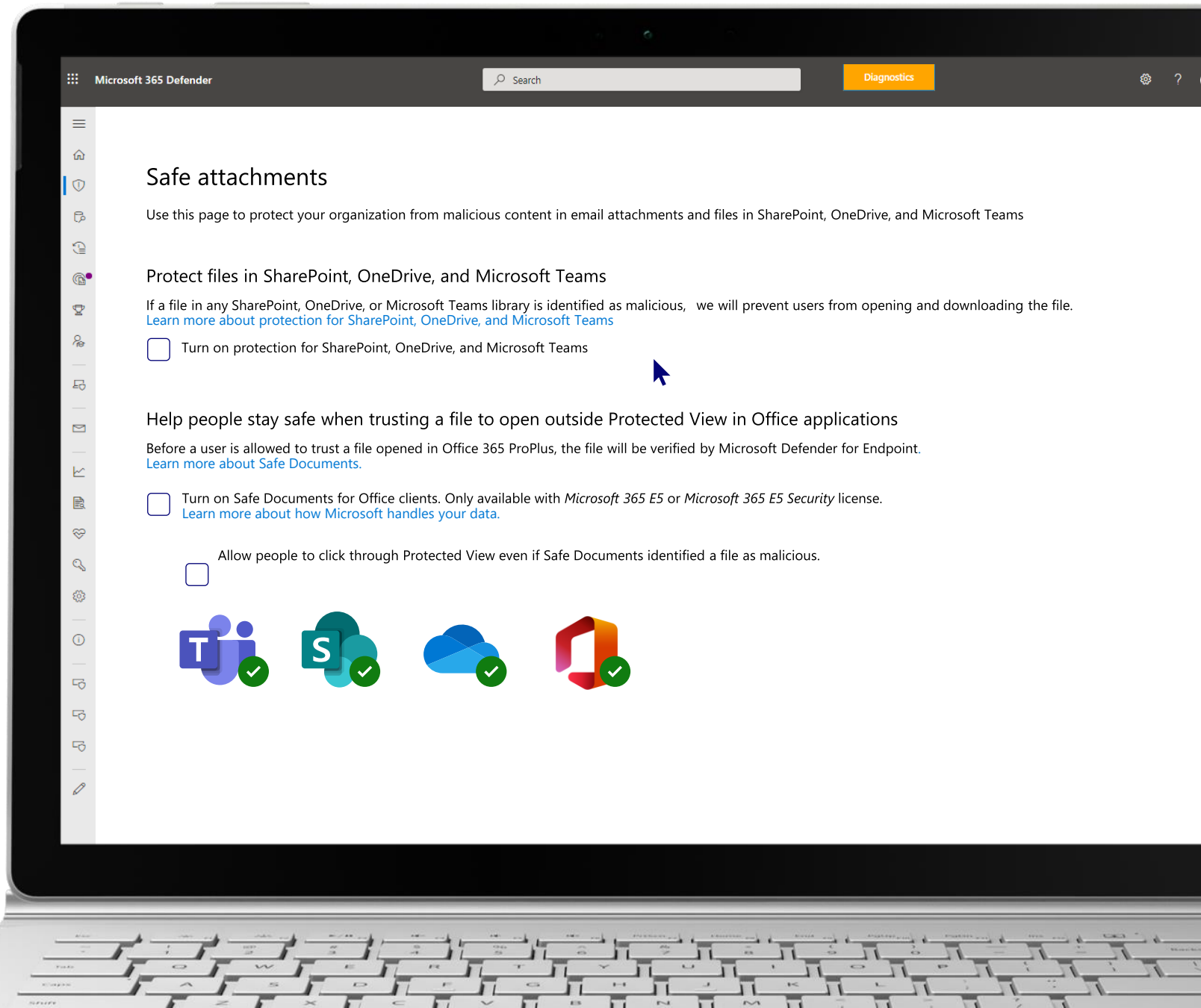
Simplified configuration guidance



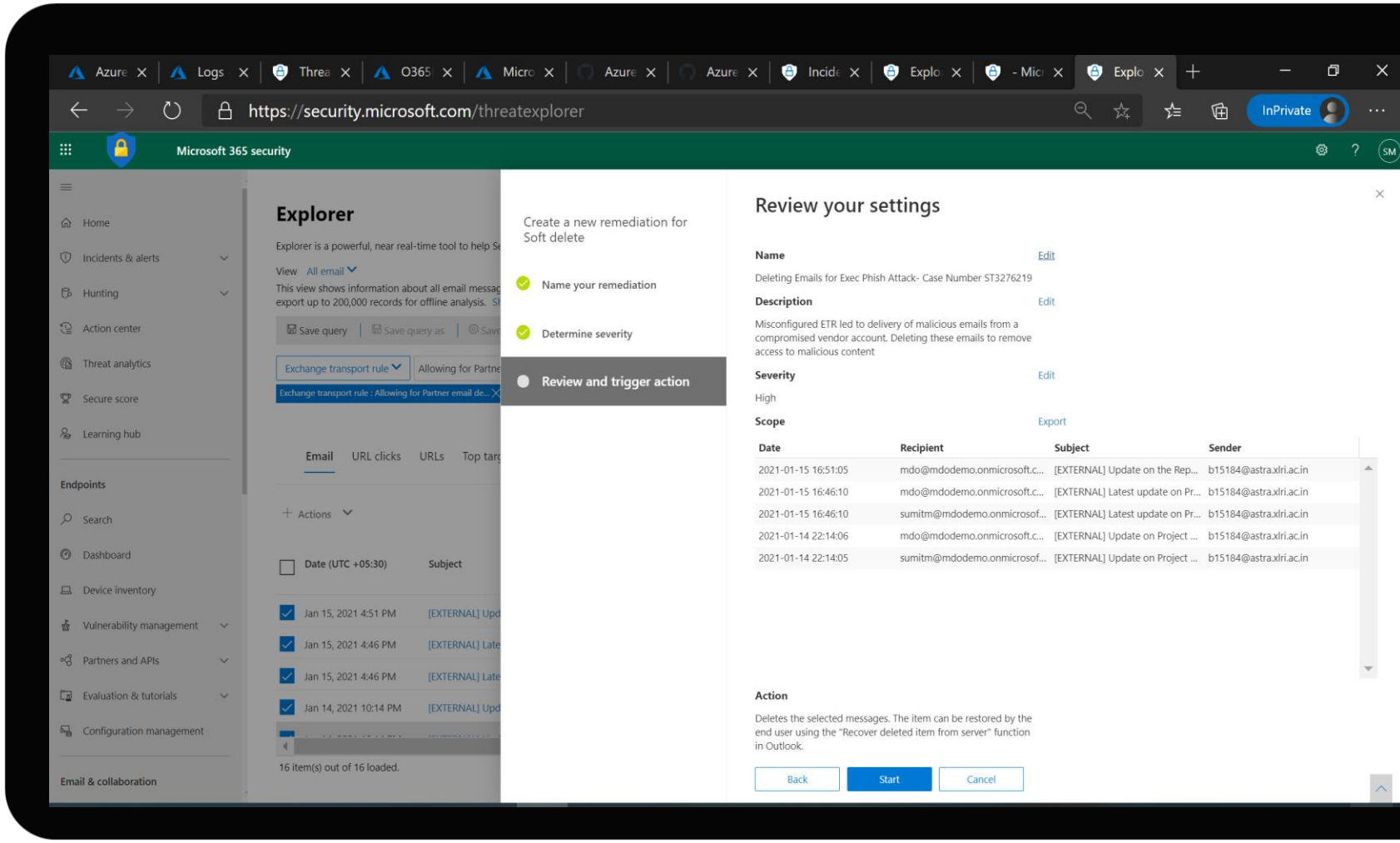
Simplified configuration guidance



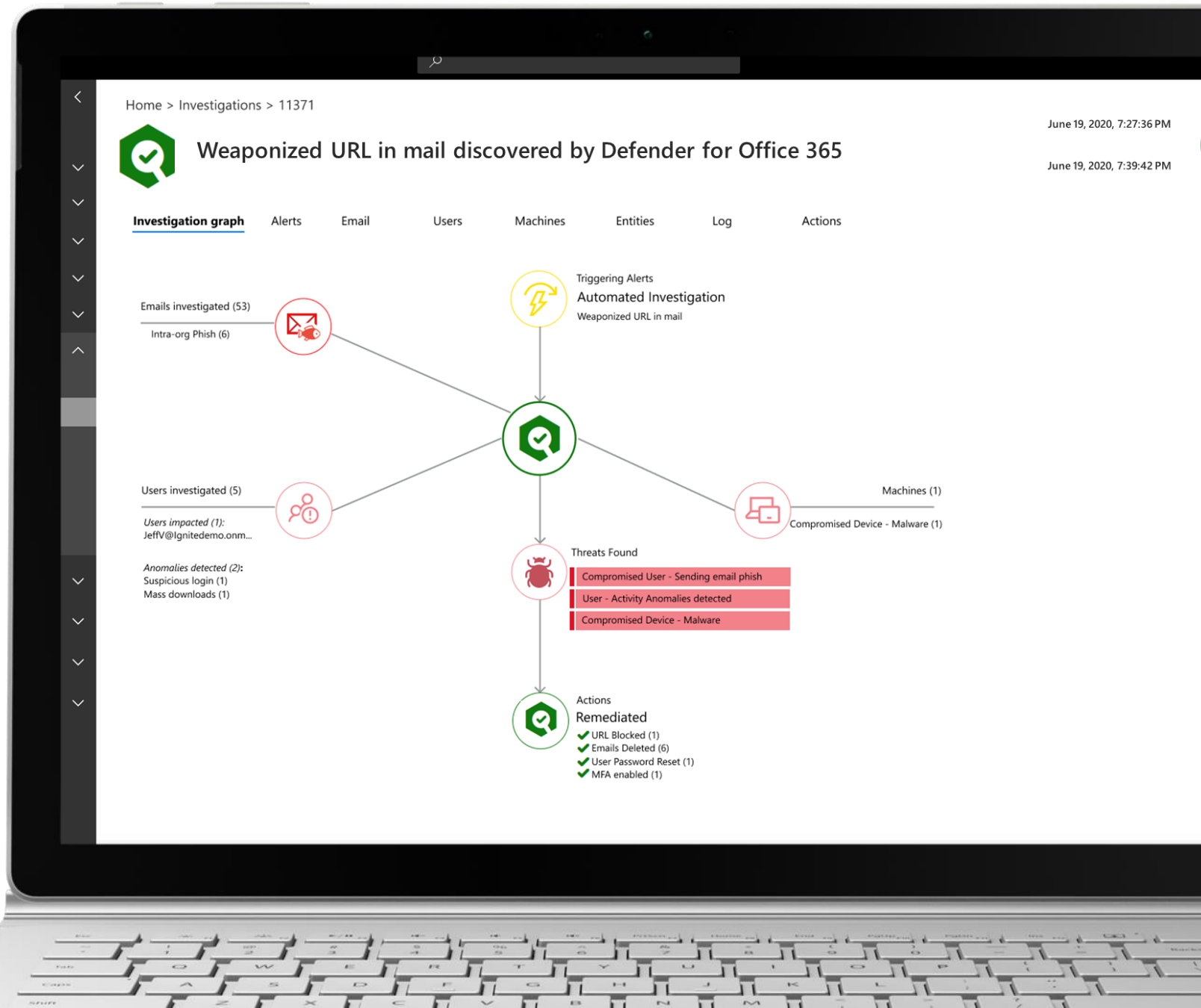
Protection beyond email



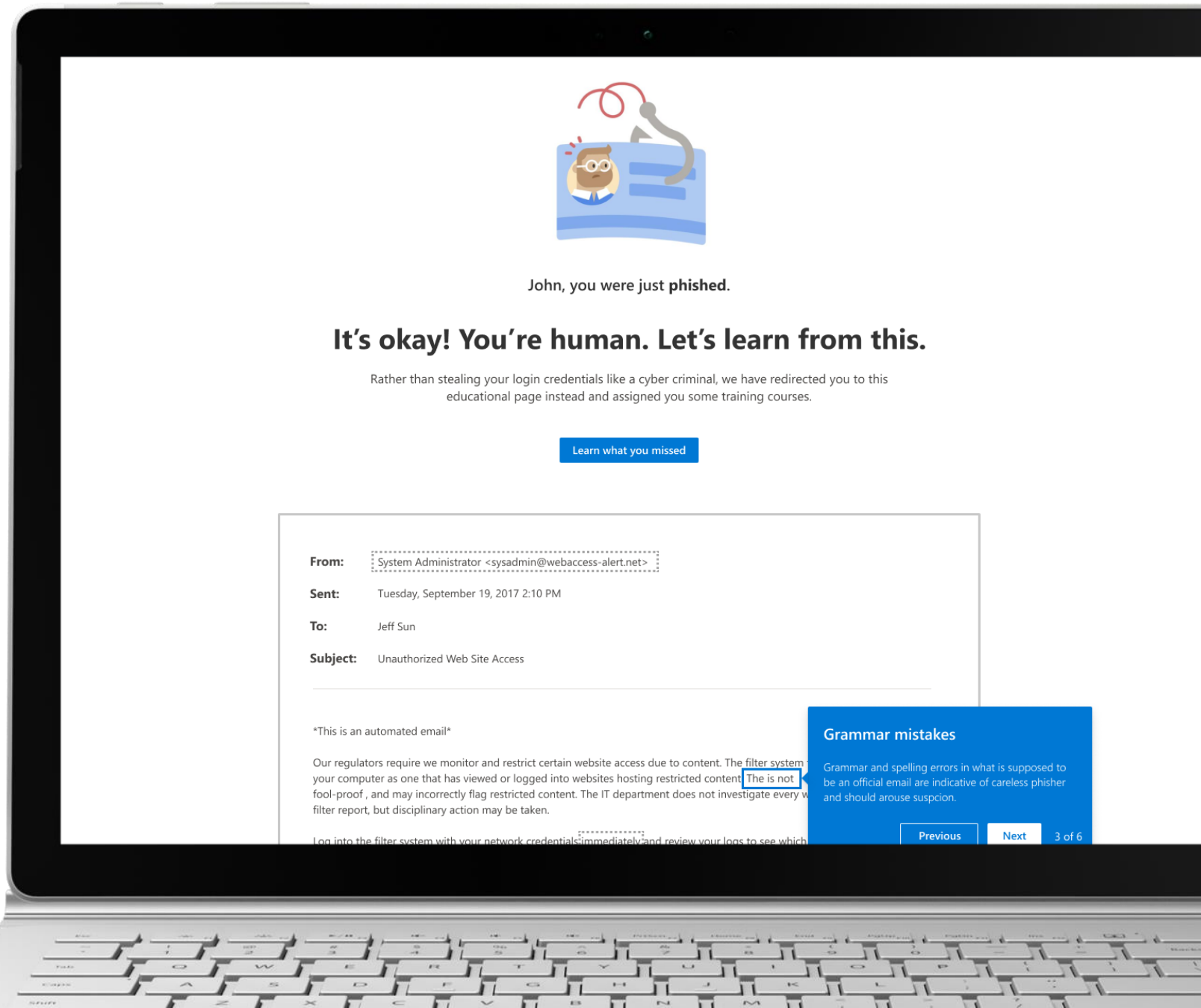
Guided hunting with inline actions



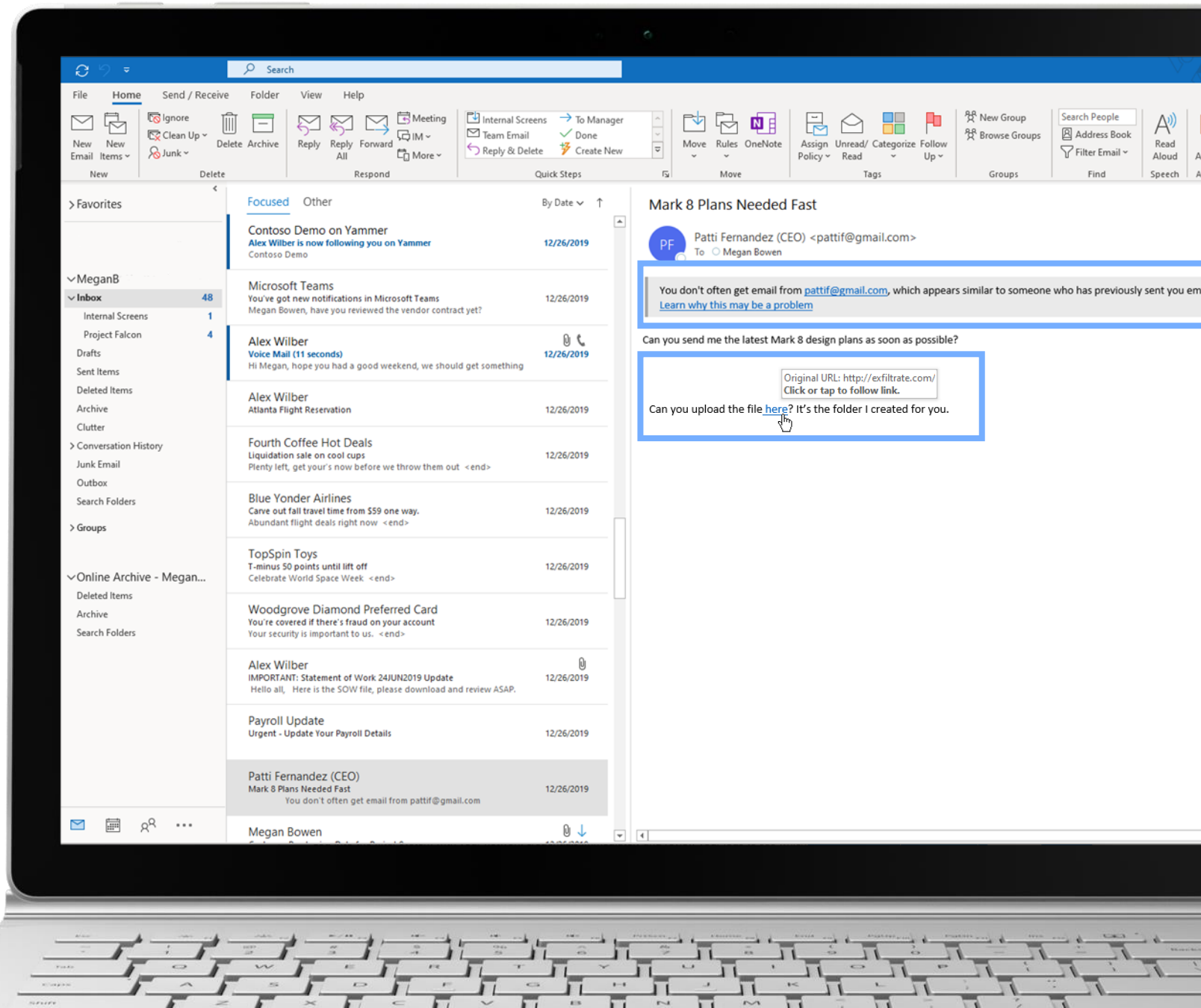
Automated response playbooks



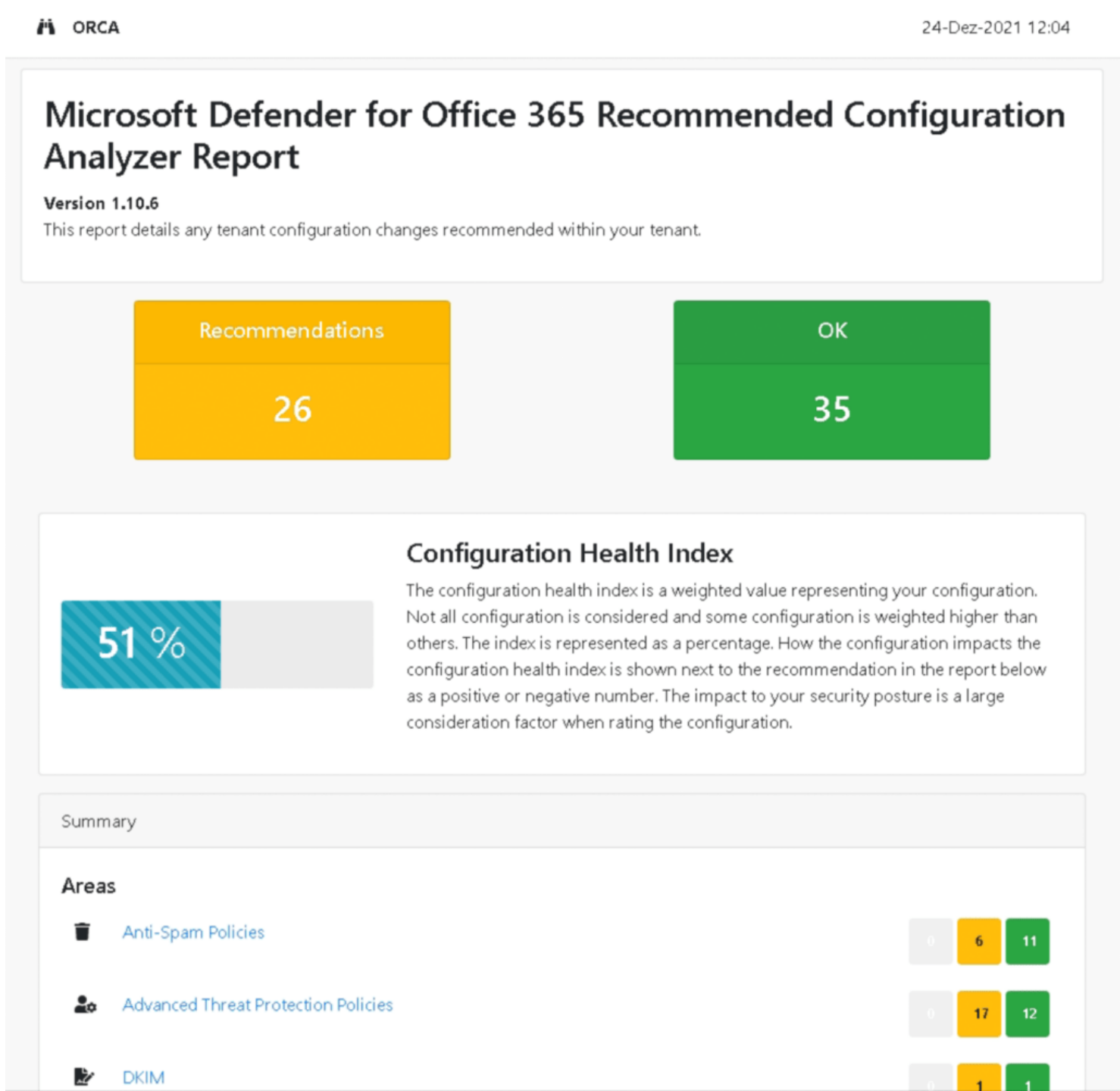
Dynamic end user training



Native experiences foster user awareness



Microsoft Defender for Office 365 Recommended Configuration Analyzer (ORCA)



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.

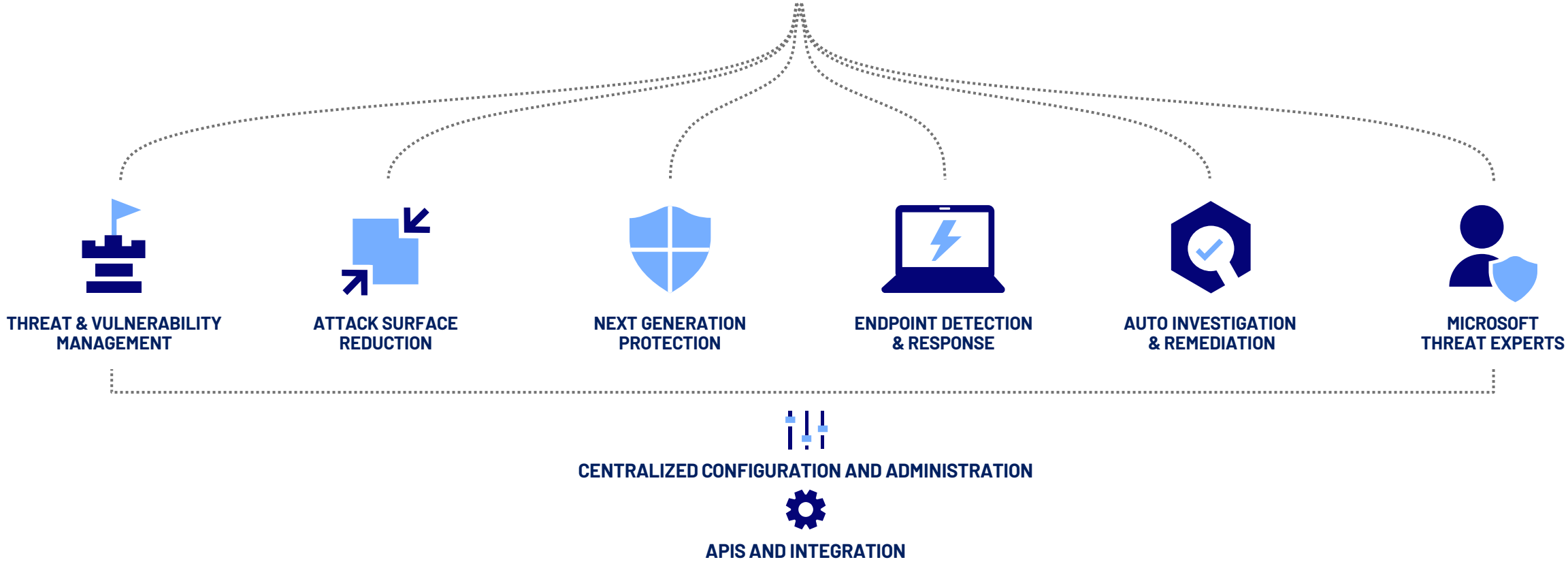
Safe Attachments, Safe Links: Scans Attachments and Links in you Microsoft 365 Services.

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

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

Microsoft Defender
for Endpoint (MDE)

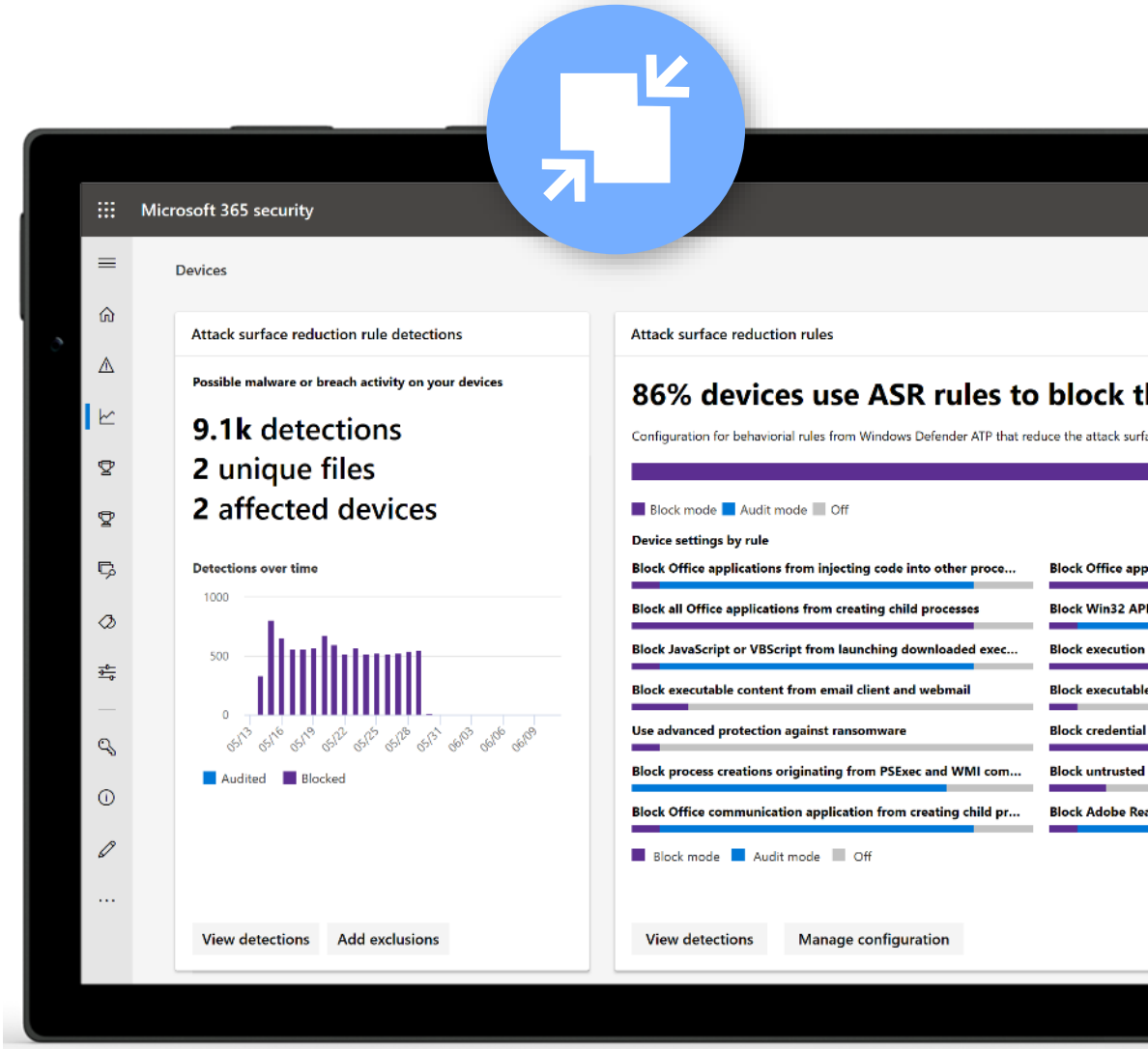
Threats are no match.



Attack Surface Reduction

Eliminate risks by reducing the surface area of attack

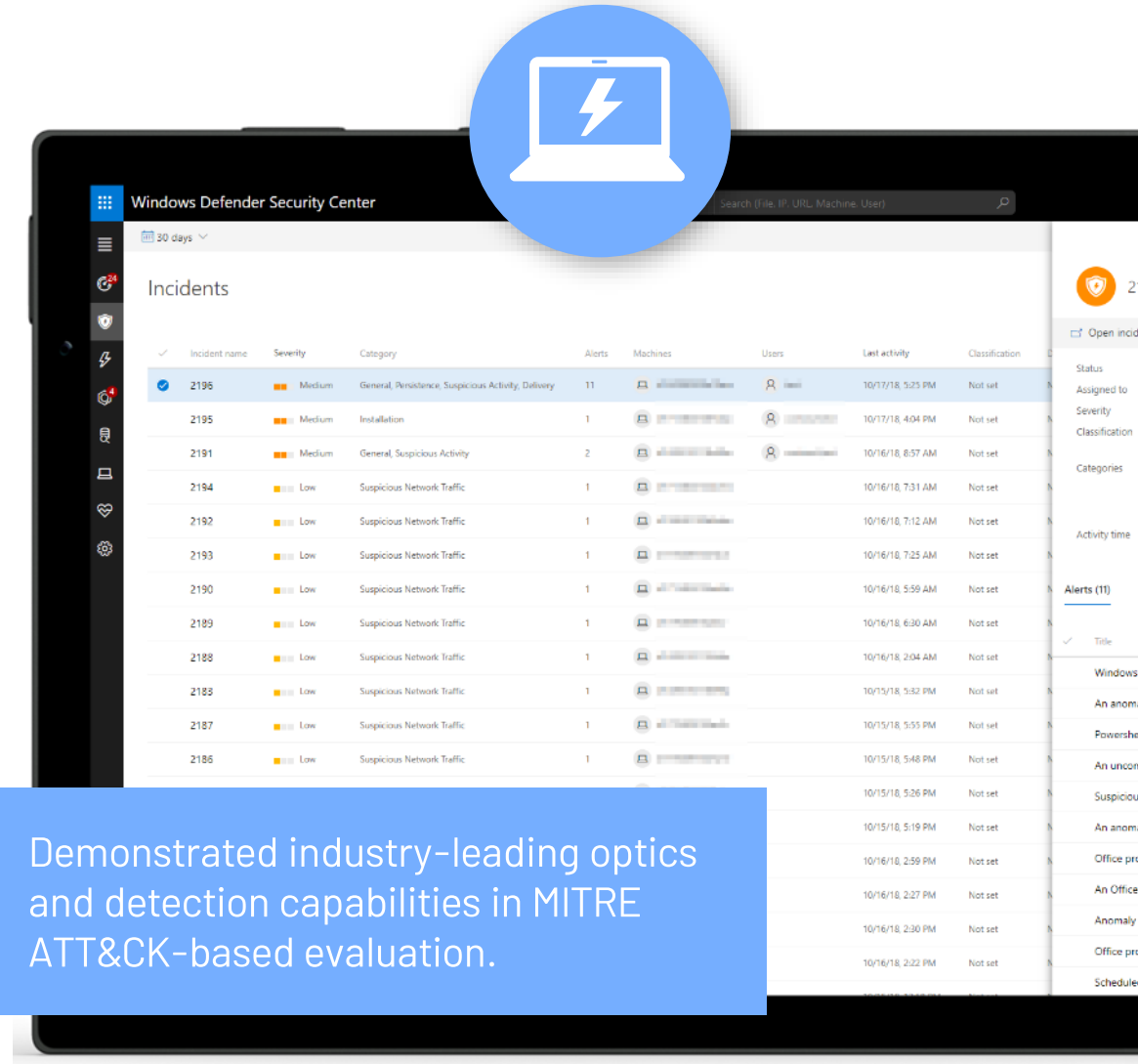
- System hardening without disruption
- Customization that fits your organization
- Visualize the impact and simply turn it on



Endpoint Detection & Response

Detect and investigate advanced persistent attacks

- Correlated behavioral alerts
- Investigation & hunting over 6 months of data
- Rich set of response actions

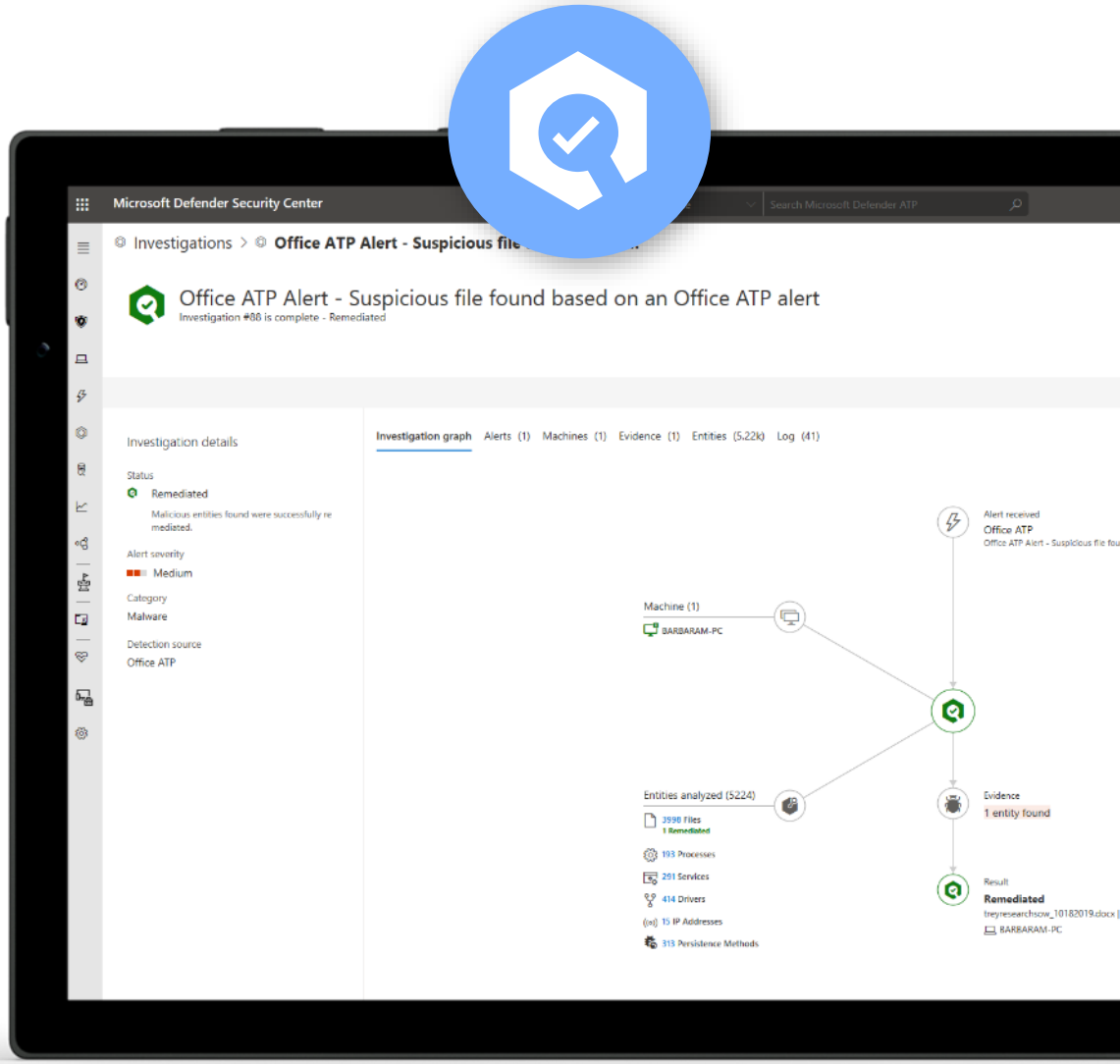


Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation.

Auto Investigation & Remediation

Automatically investigates alerts and remediates complex threats in minutes

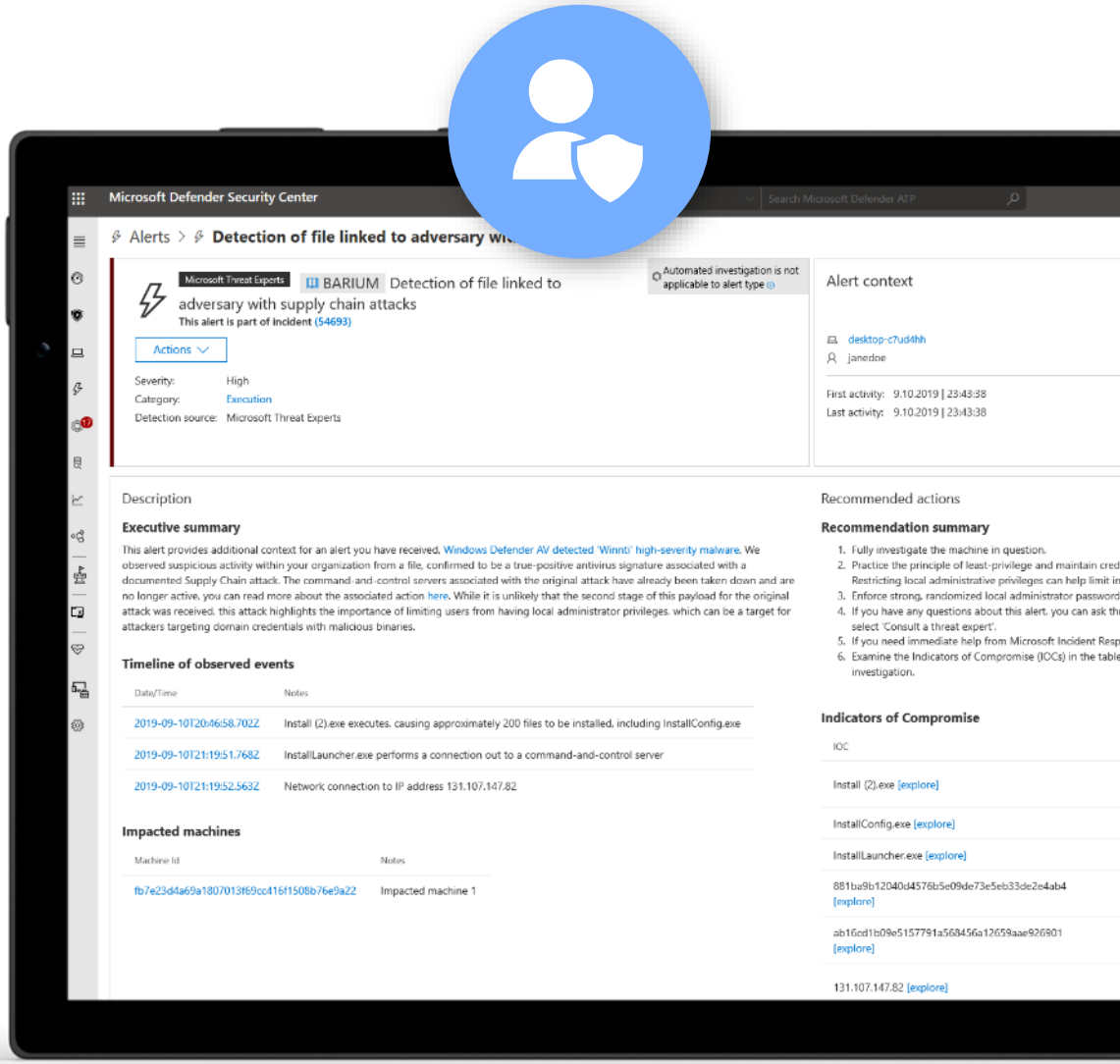
- Mimics the ideal steps analysts would take
- Tackles file or memory-based attacks
- Works 24x7, with unlimited capacity



Microsoft Threat Experts

Bring deep knowledge and proactive threat hunting to your SOC

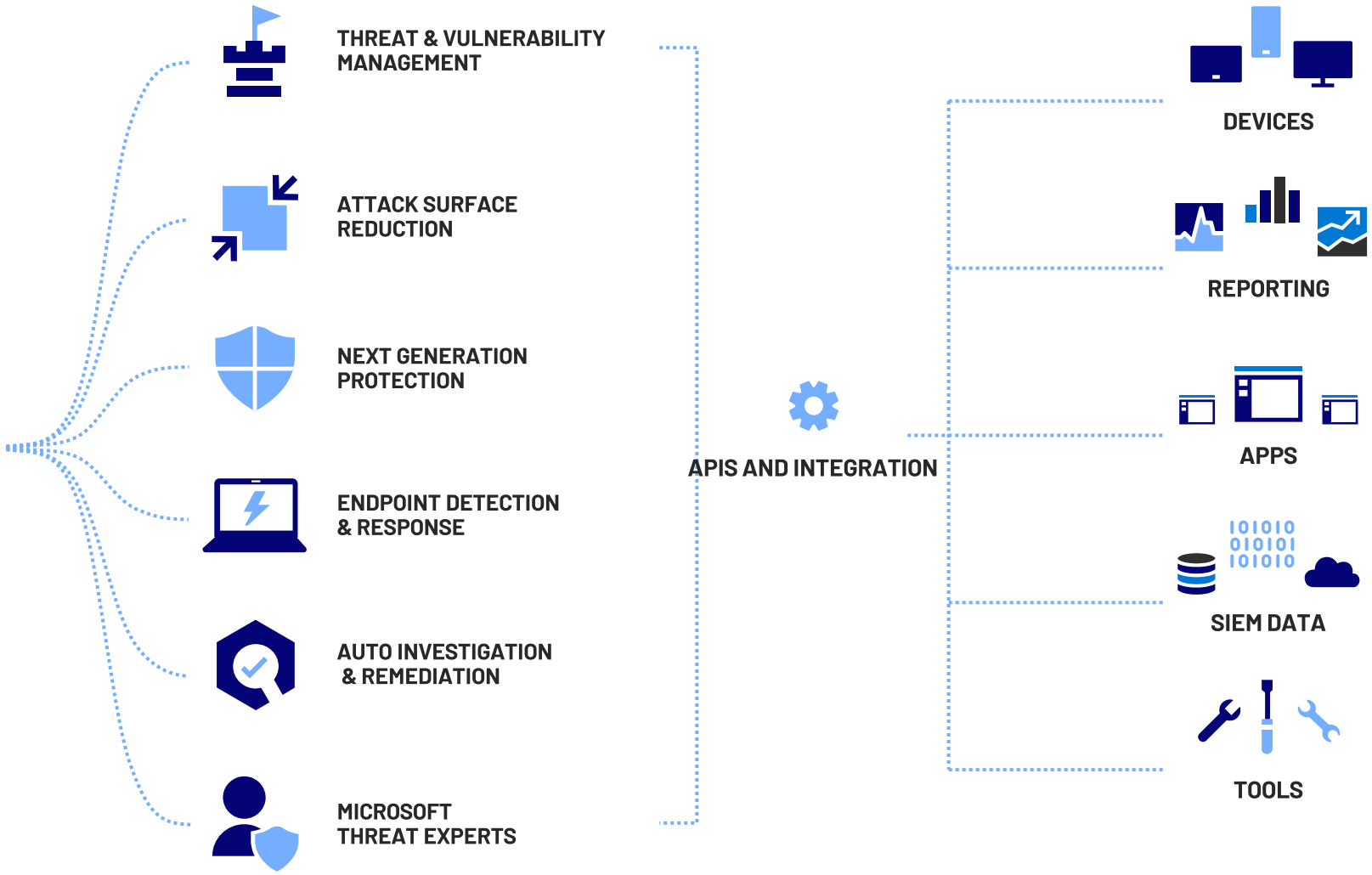
- Expert level threat monitoring and analysis
- Environment-specific context via alerts
- Direct access to world-class hunters



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

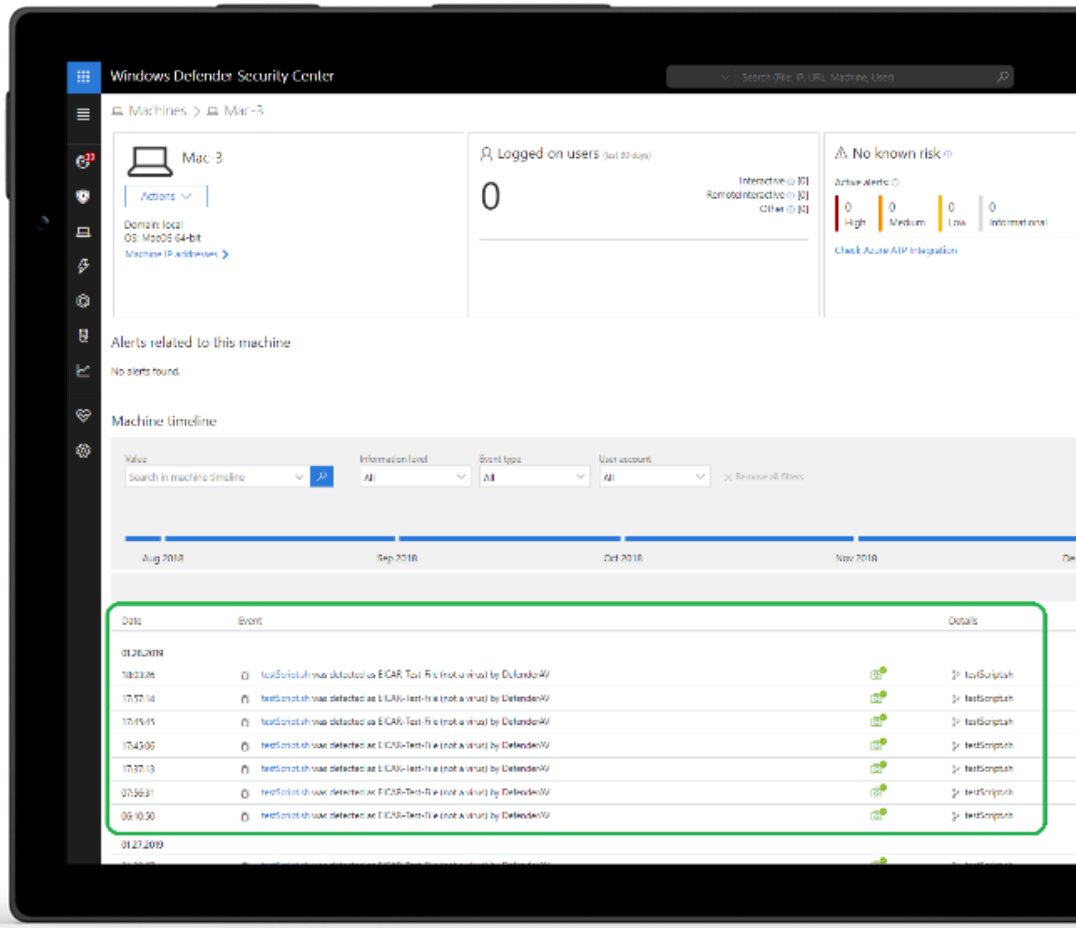
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

Enterprise Grade

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

Seamlessly integrated with Microsoft Defender for Endpoint capabilities

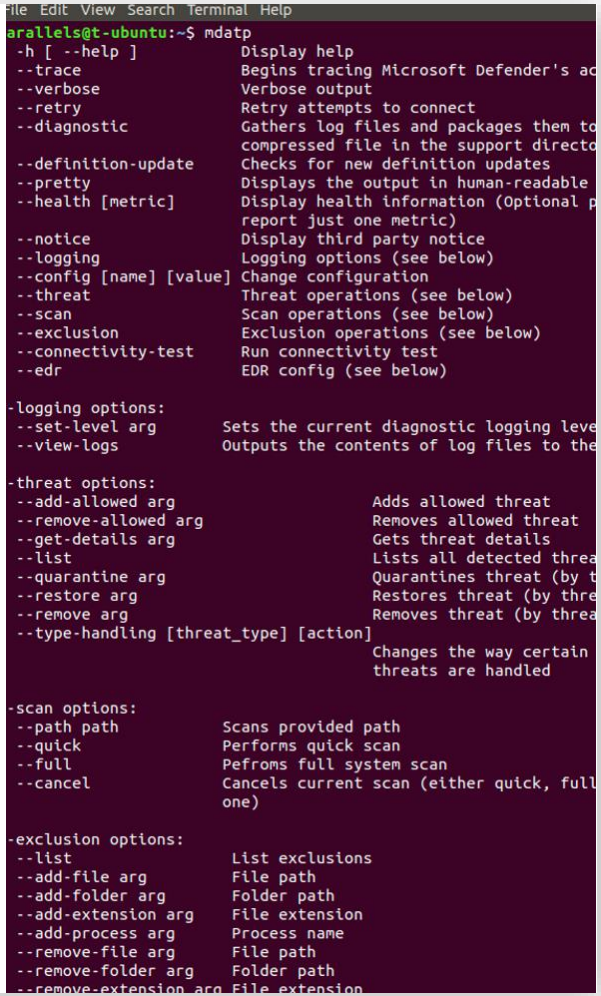
- Detection dictionary across the kill chain
- 6 months of raw data on all machines Inc. Mac OS
- Reputation data for all entities being logged
- Single pane of glass across all endpoints Mac OS
- Advanced hunting on all raw data including Mac OS
- Custom TI
- API access to the entire data model Inc.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



Microsoft Defender for Endpoint (Linux)

On the client:

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



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.

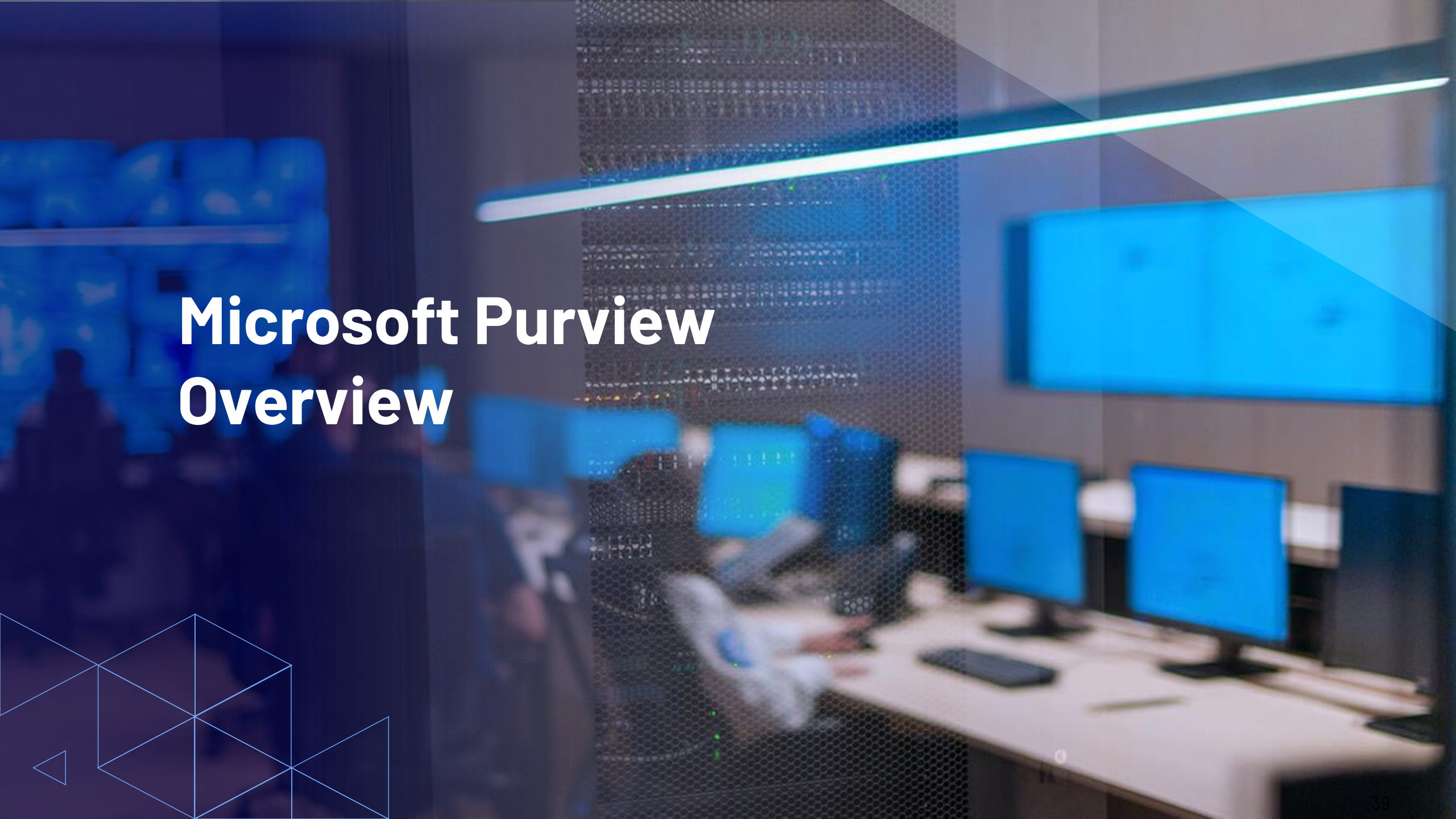
Defender for Endpoint: Best Practices

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.



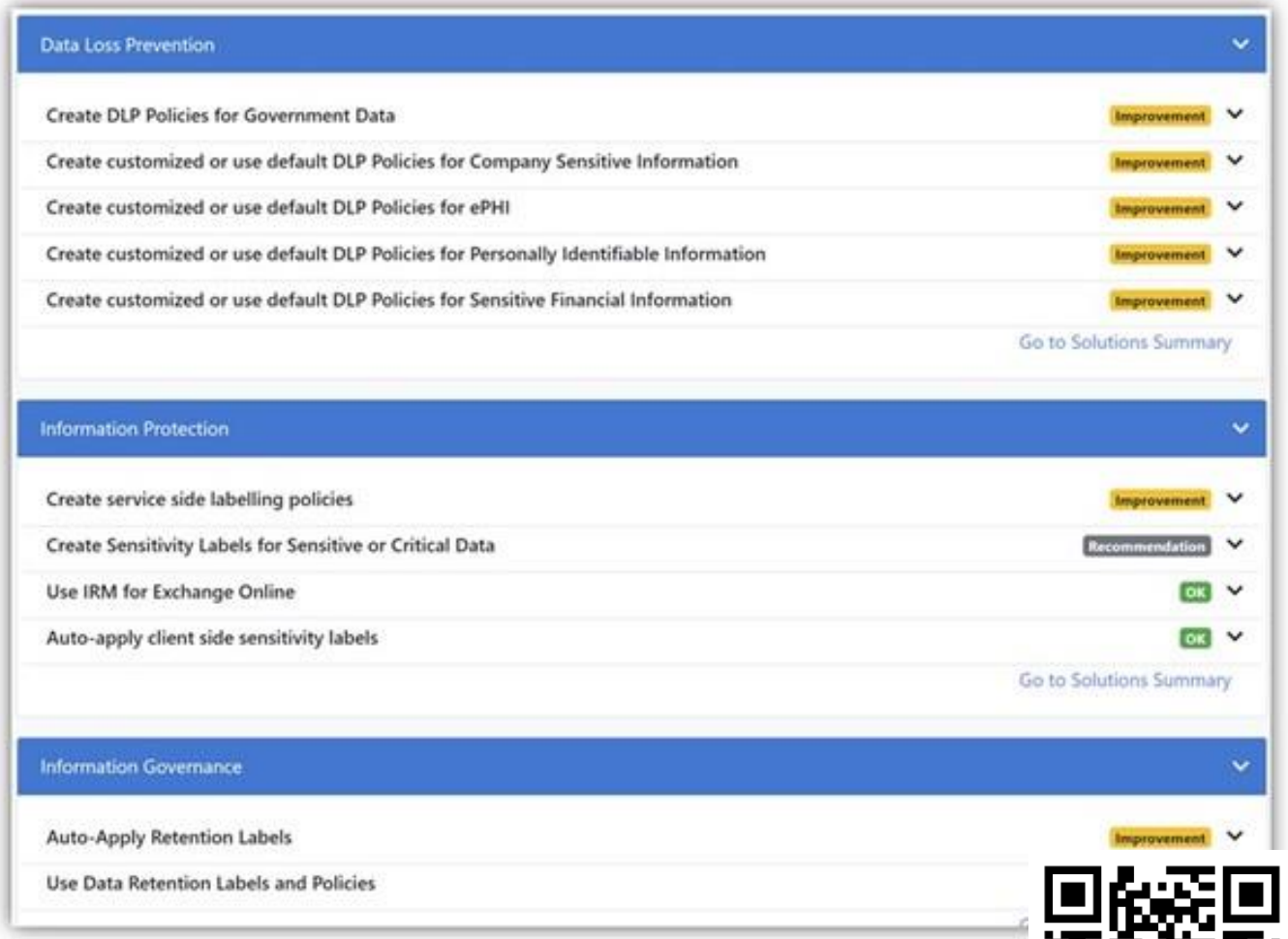
Microsoft Purview Overview

Current Name	New Name
Microsoft 365 Basic Audit	Microsoft Purview Audit (Standard)
Microsoft 365 Advanced Audit	Microsoft Purview Audit (Premium)
Microsoft 365 Communication Compliance	Microsoft Purview Communication Compliance
Microsoft Compliance Manager	Microsoft Purview Compliance Manager
Office 365 Customer Lockbox	Microsoft Purview Customer Lockbox
Azure Purview Data Catalog	Microsoft Purview Data Catalog
Microsoft 365 Data Connectors	Microsoft Purview Data Connectors
Microsoft Information Governance	Microsoft Purview Data Lifecycle Management
Office 365 Data Loss Prevention	Microsoft Purview Data Loss Prevention
Azure Purview Data Map	Microsoft Purview Data Map
Double Key Encryption for Microsoft 365	Microsoft Purview Double Key Encryption
Records Management in Microsoft 365	Microsoft Purview Records Management
Office 365 Core eDiscovery	Microsoft Purview eDiscovery (Standard)
Office 365 Advanced eDiscovery	Microsoft Purview eDiscovery (Premium)
Microsoft 365 Information Barriers	Microsoft Purview Information Barriers
Microsoft Information Protection	Microsoft Purview Information Protection
Microsoft 365 Insider Risk Management	Microsoft Purview Insider Risk Management
Azure Purview portal	Microsoft Purview governance portal
Microsoft 365 compliance center	Microsoft Purview compliance portal
Azure Purview Data Insights	Microsoft Purview Data Estate Insights
Microsoft 365 Customer Key	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.

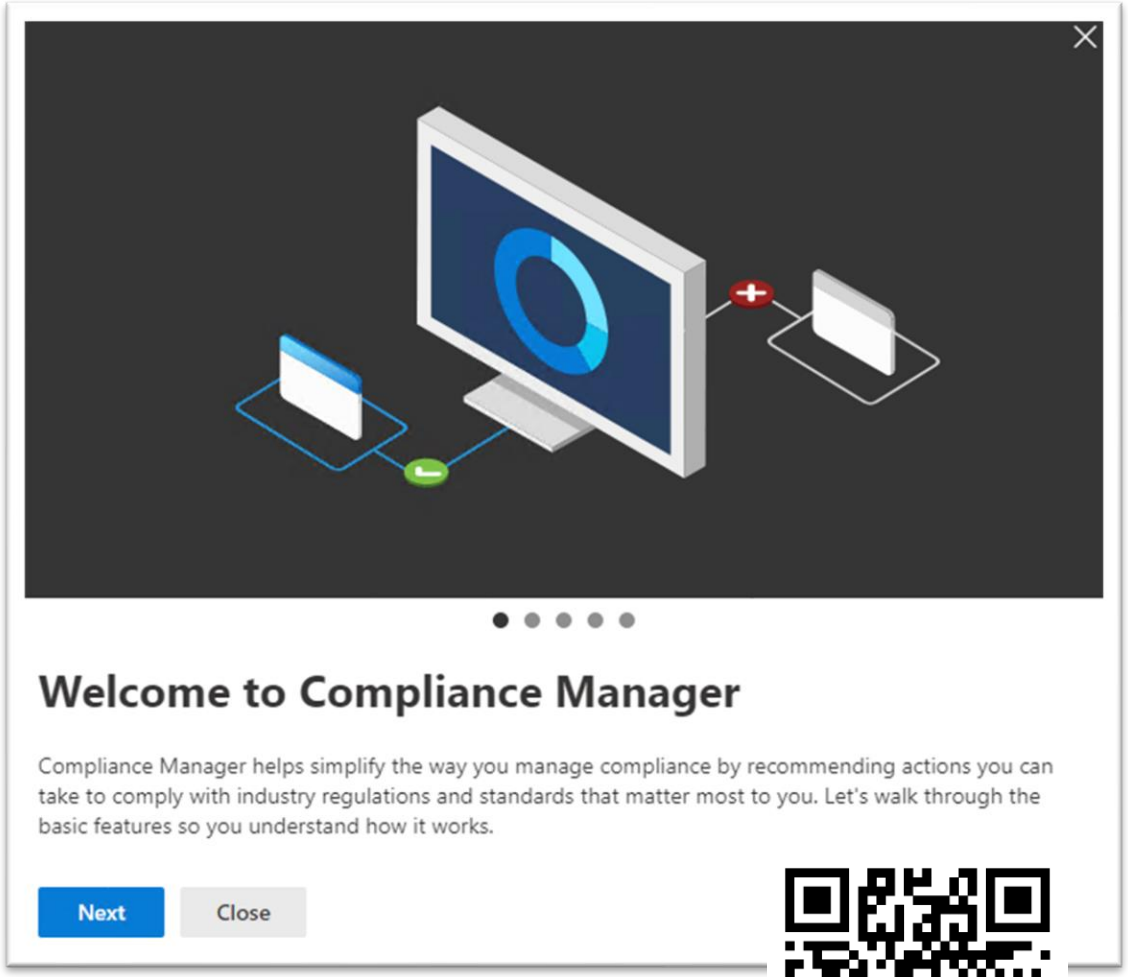
github.com/OfficeDev/MCCA

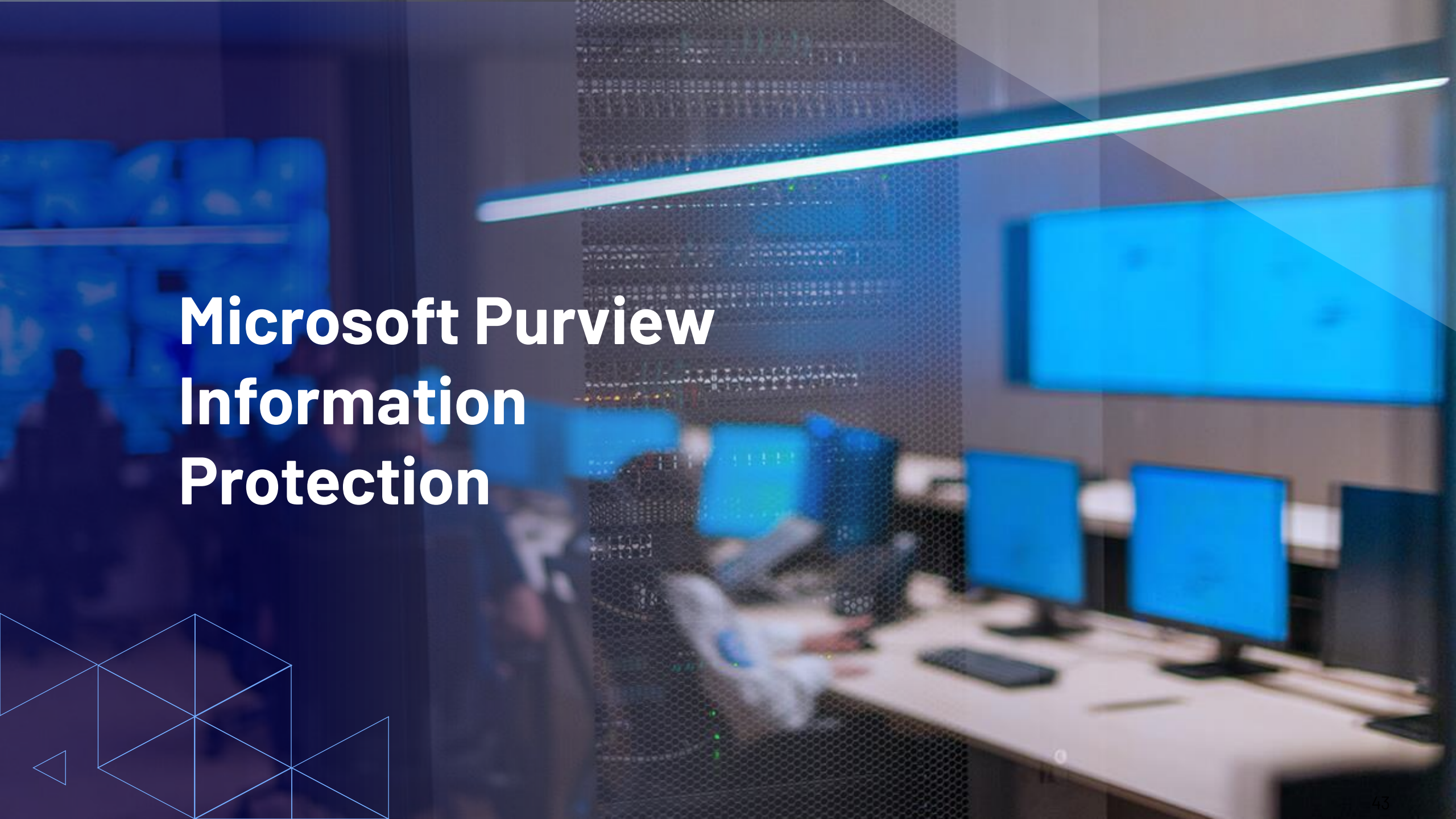


Microsoft Compliance Manager

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.

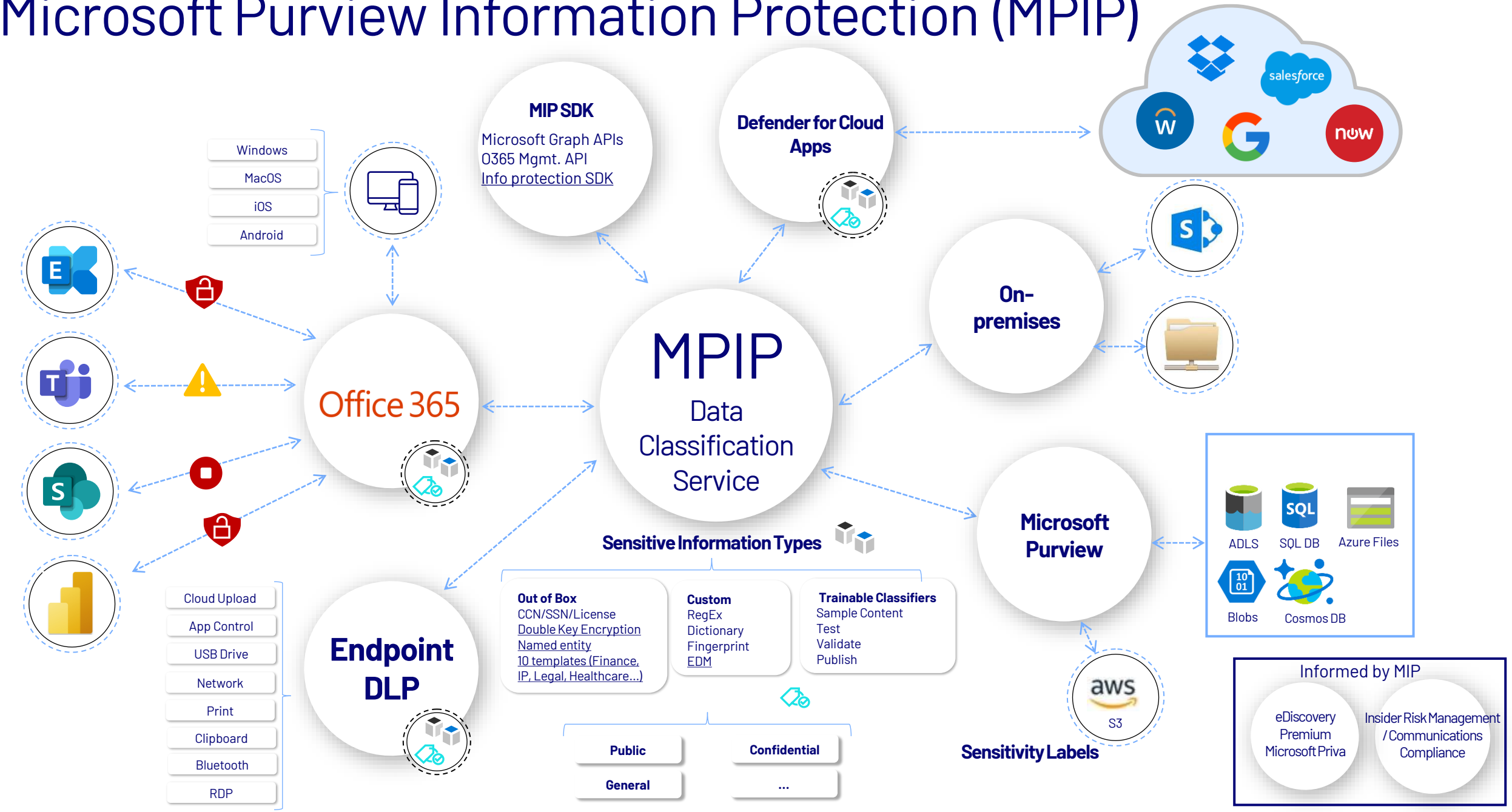
bit.ly/m365compliancemanager





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

Scan on-premises to cloud

Use 250+ built-in classification methods

Content explorer (100 different files types for content analysis, 320 formats for true file type detection)

Activity explorer

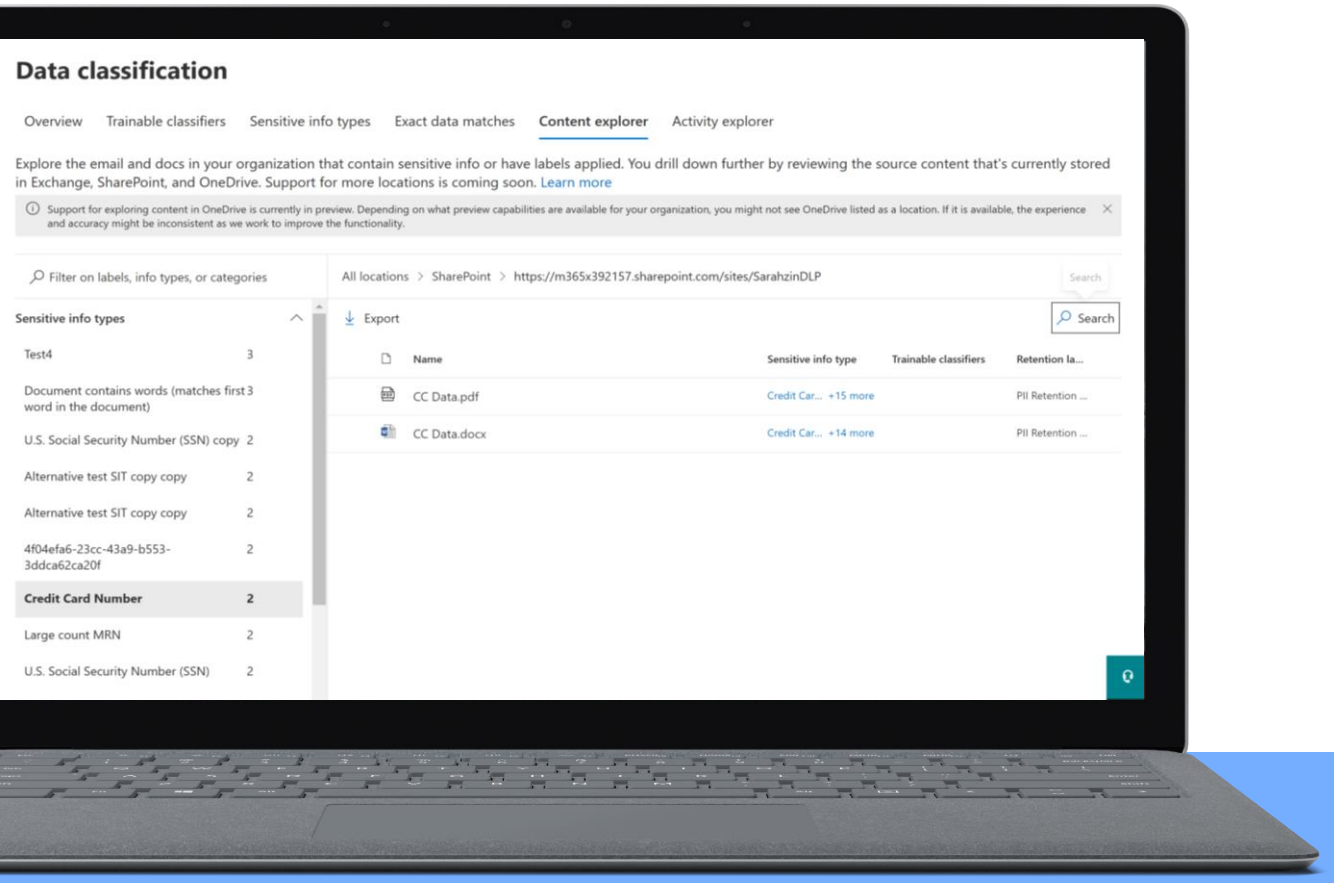
Build your own classification methods (or use and customize 50+ predefined templates in privacy, medical, & financial)

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



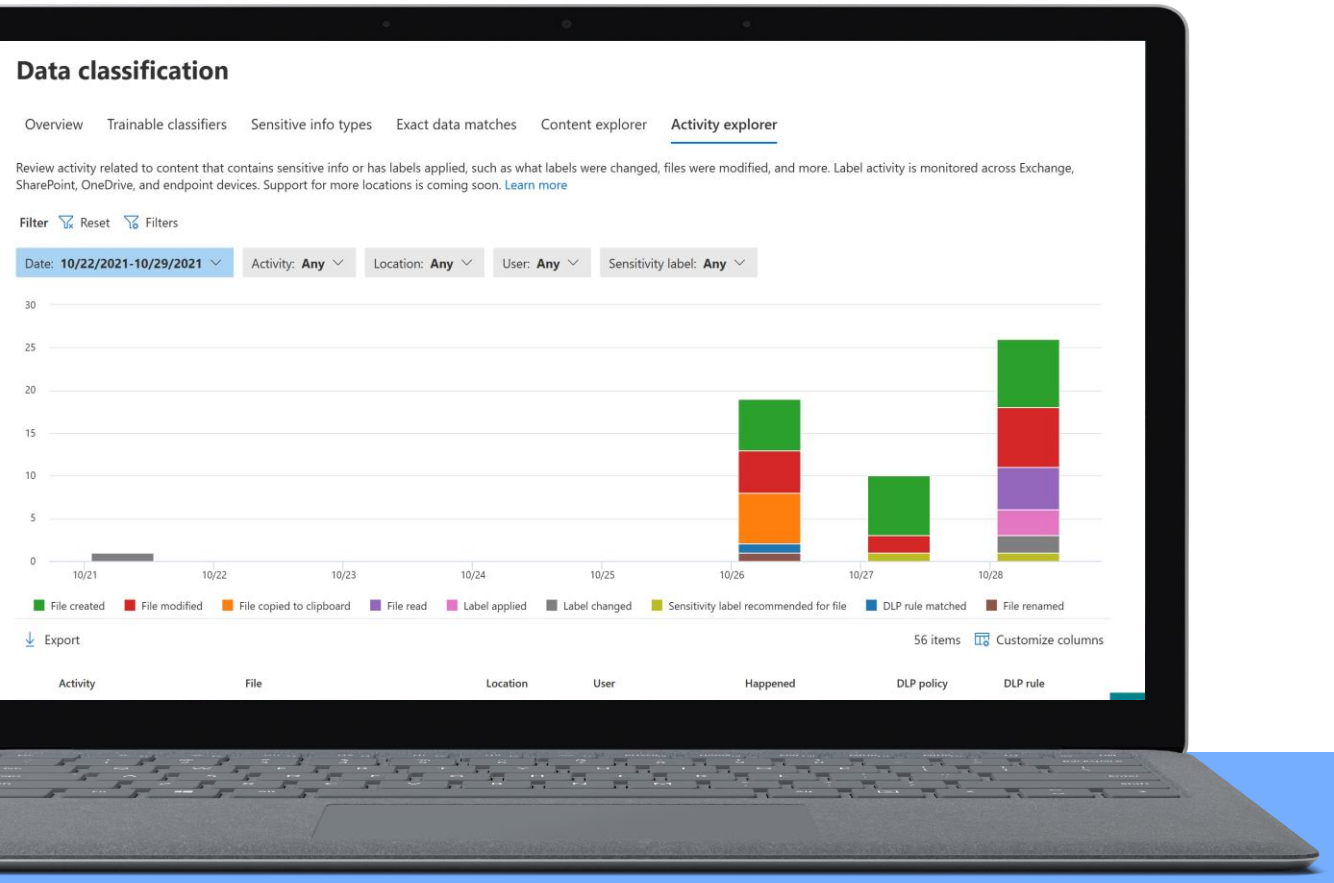
Visibility into amount of sensitive data in a document that triggered the classification to be applied

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 metada 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

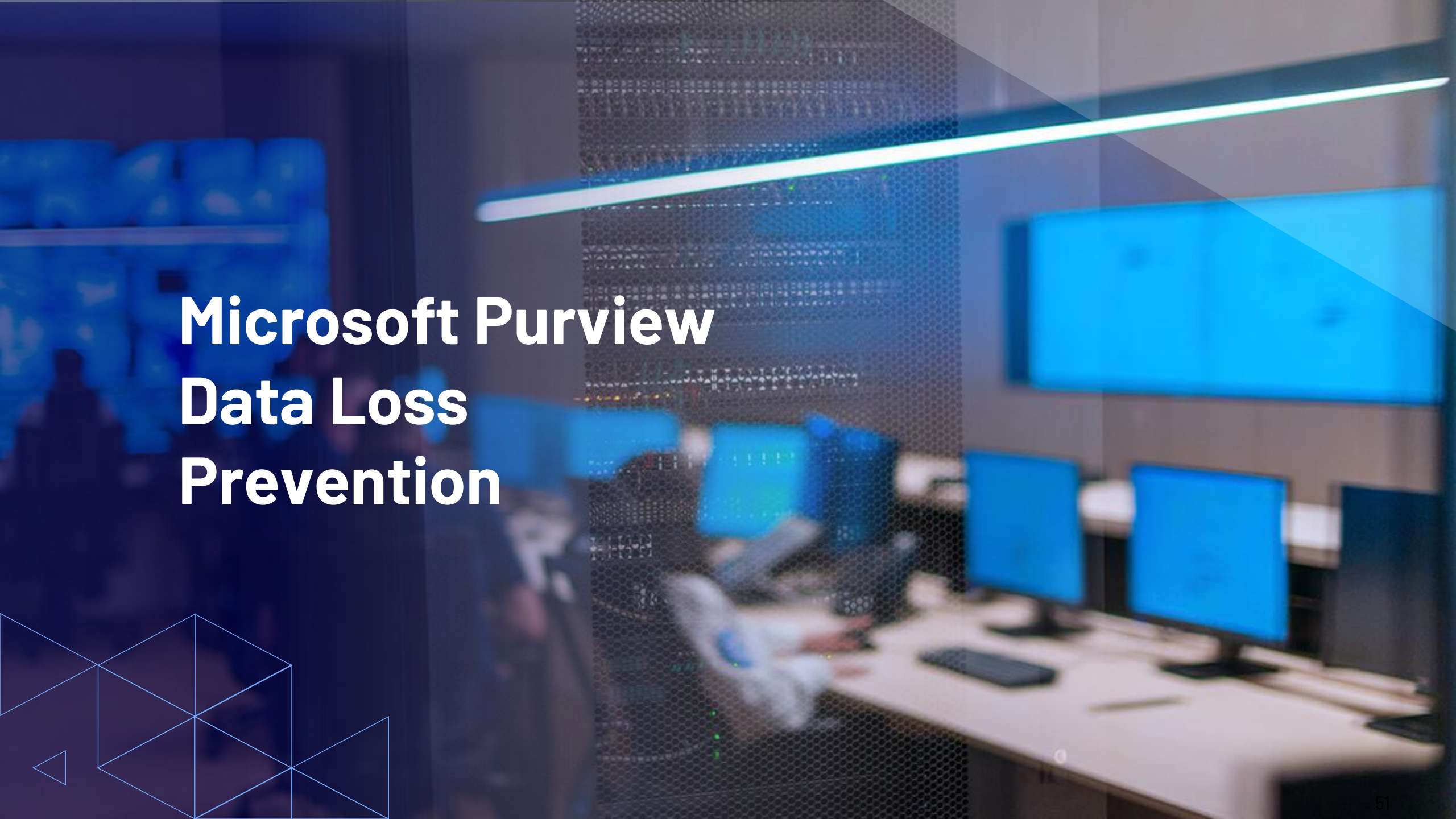
Sublabels: Labels are generally used to represent the actual sensitivity of the content that is labeled, while sublabels are typically used to represent variations in the protection or the scope of the content.

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

Data in use

Data in motion

Data at rest

Guided onboarding

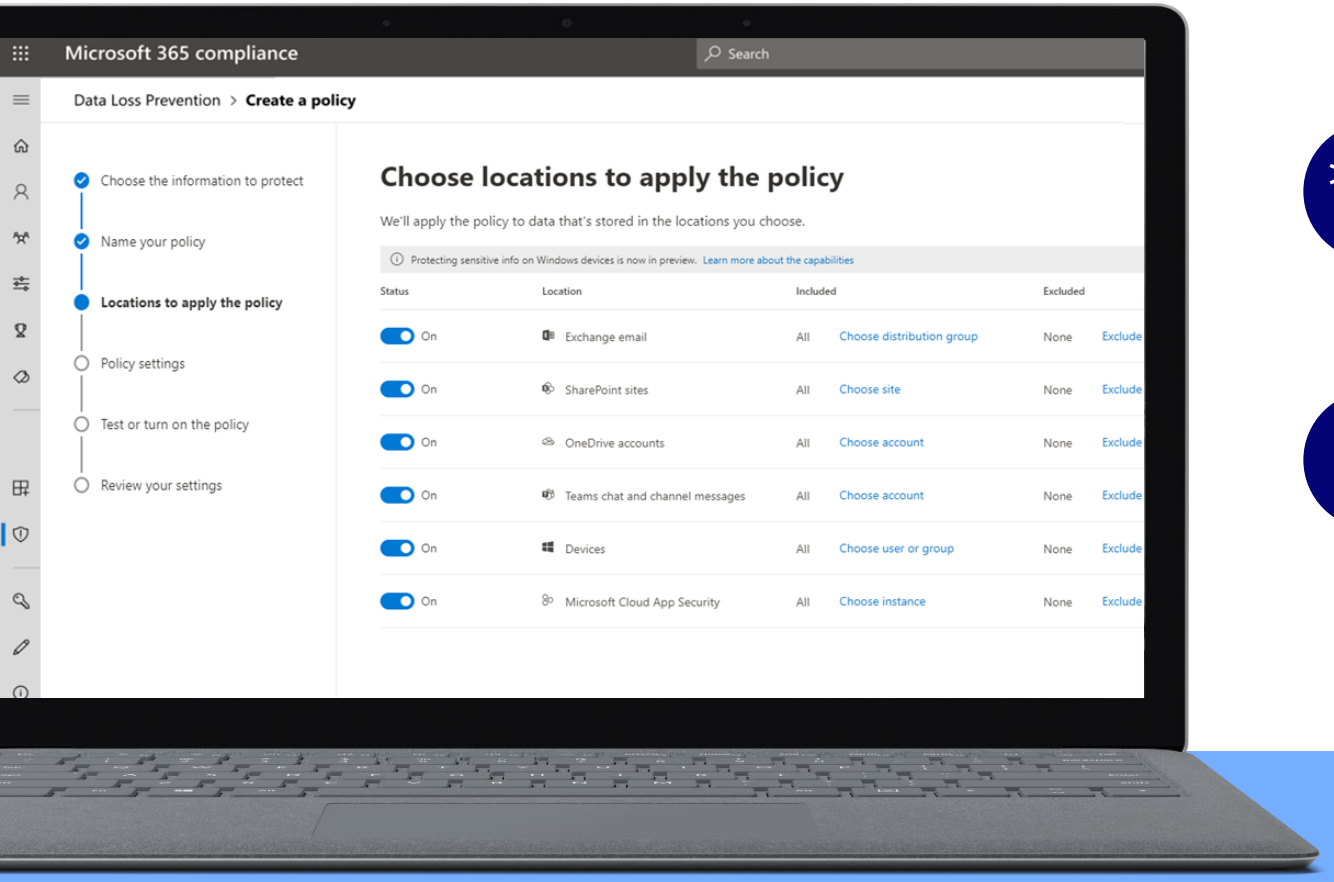
Unified & flexible policy management

Integrated with Microsoft Purview Information Protection

Unified alerting & remediation

Agentless and integrated within end user experiences

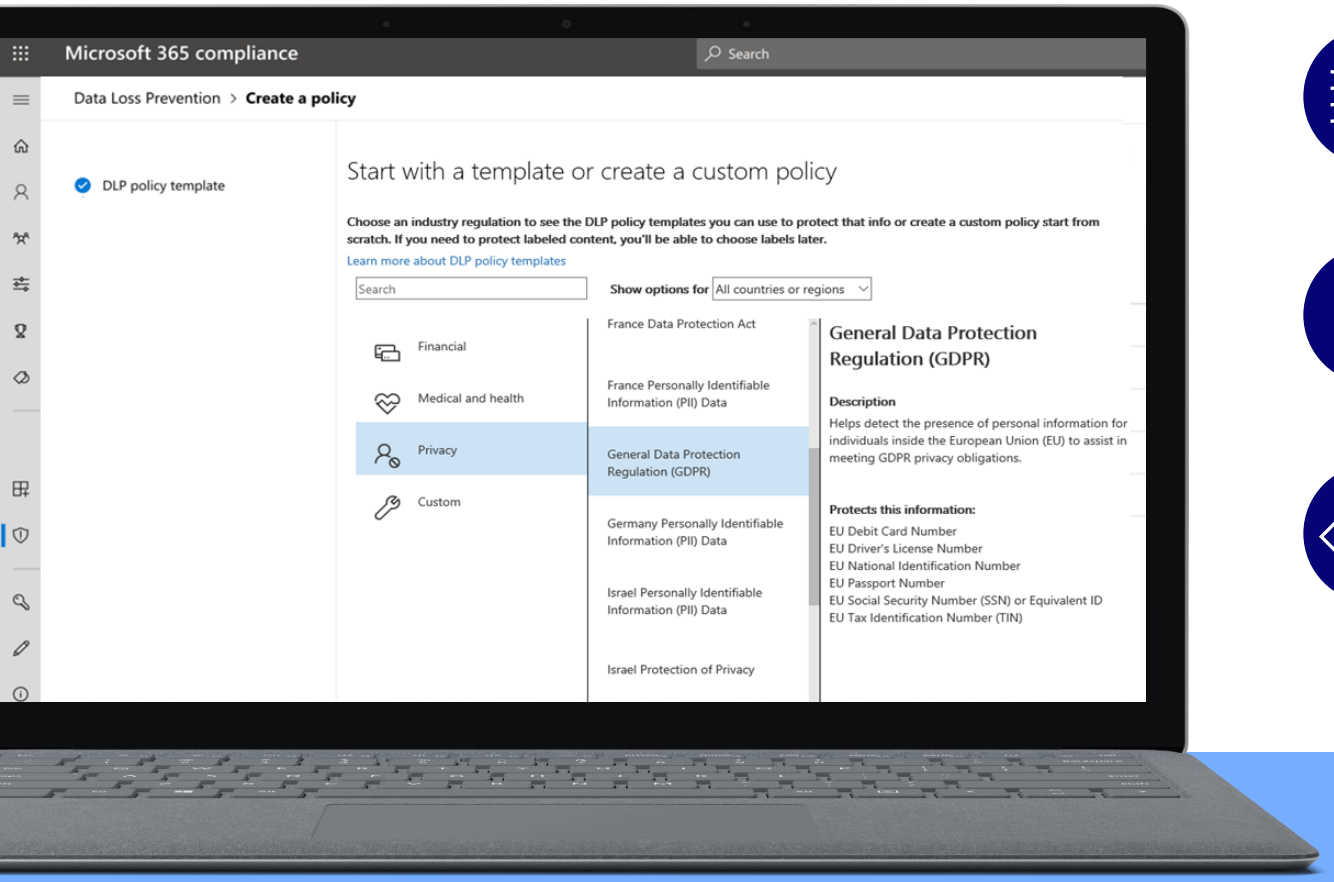
Unified and flexible policy management



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

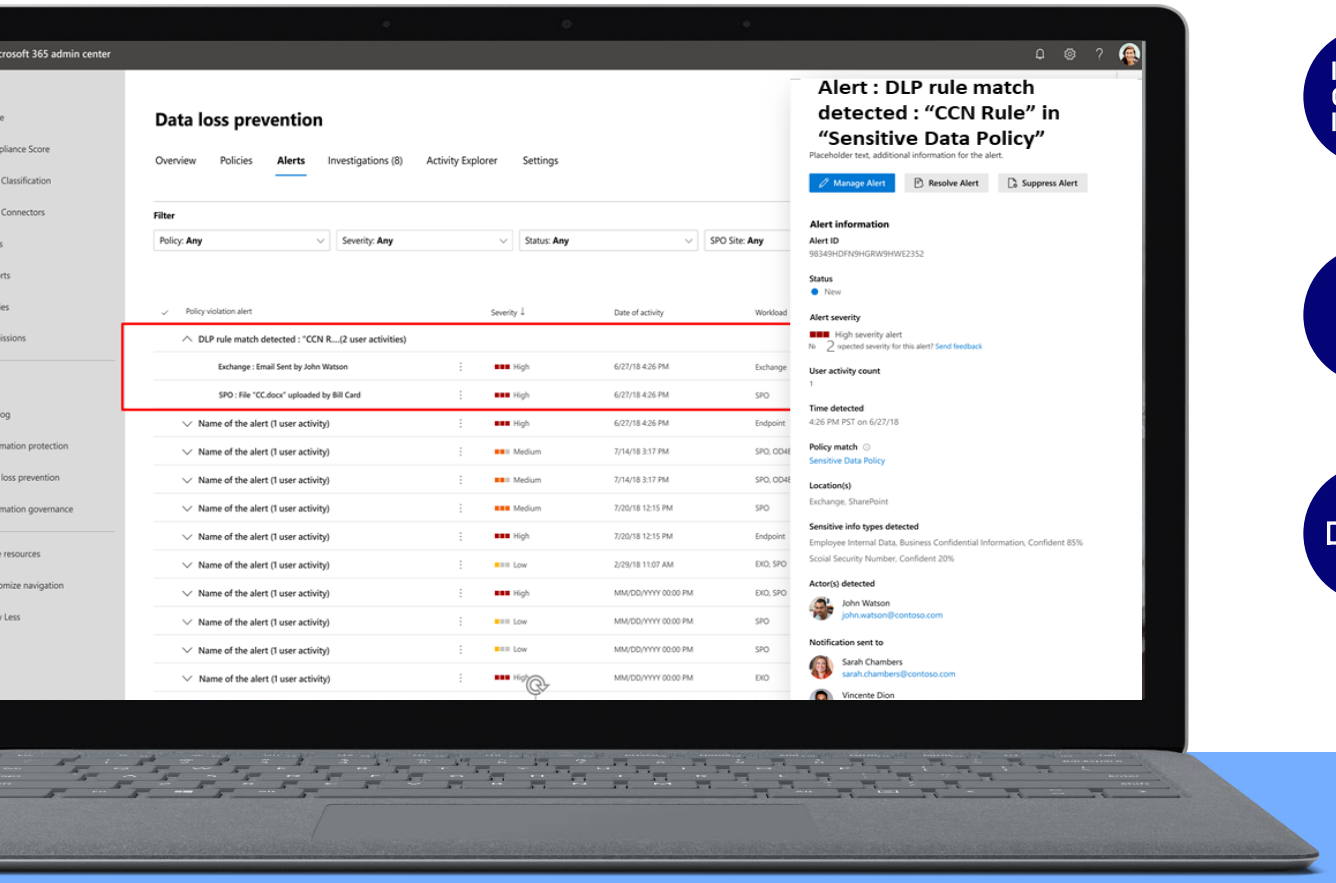


100+ sensitive information types

40+ built-in policy templates

Labels as condition in DLP

Unified alerting and remediation



- 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 (OOB): 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.

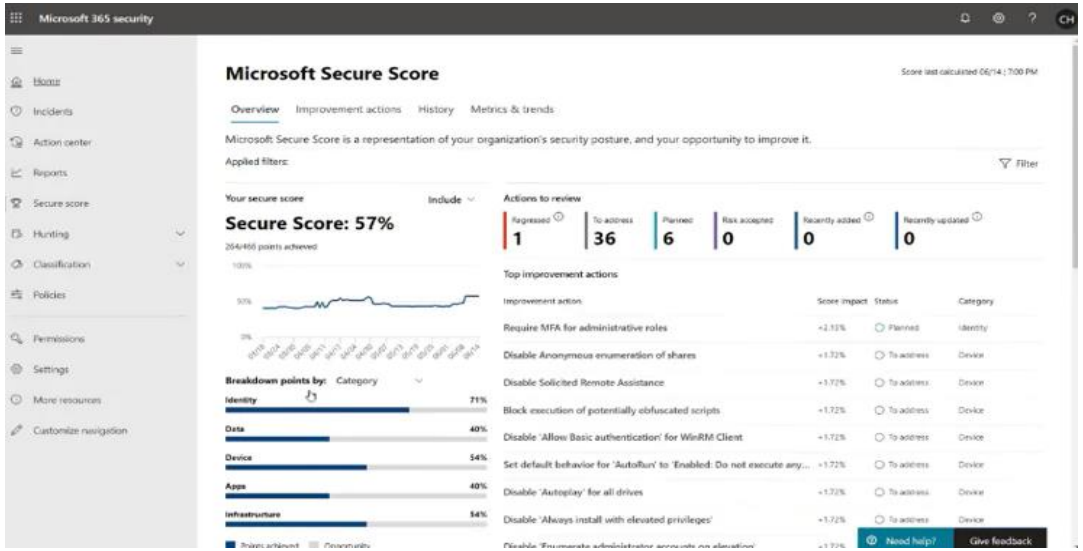
DLP rule exceptions: Define exceptions to your DLP rules that are based on sensitivity labels. MIP labels are highly synergistic with traditional DLP.

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

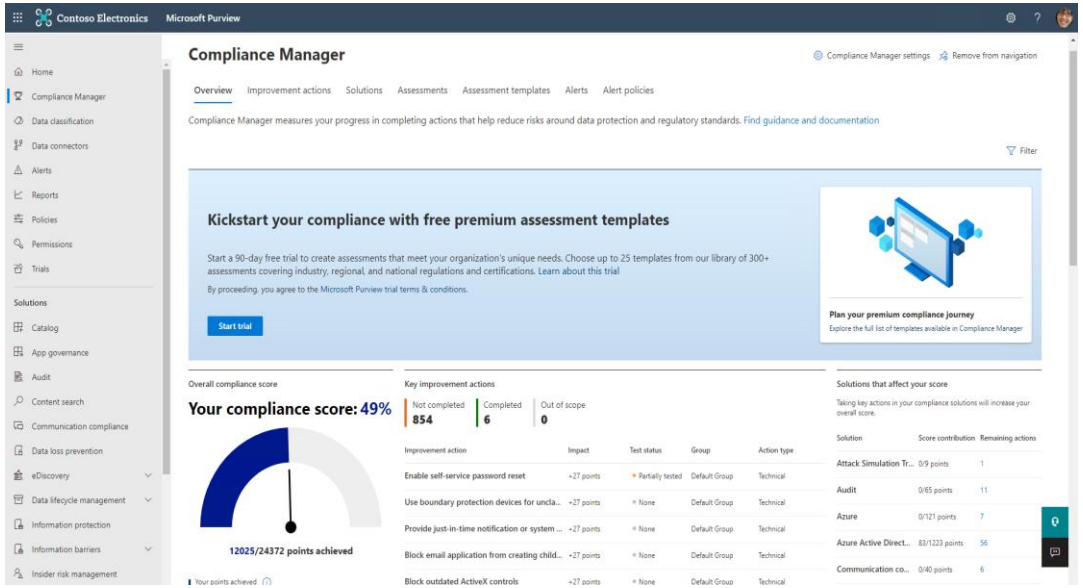
Microsoft 365 Platform Resources

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.

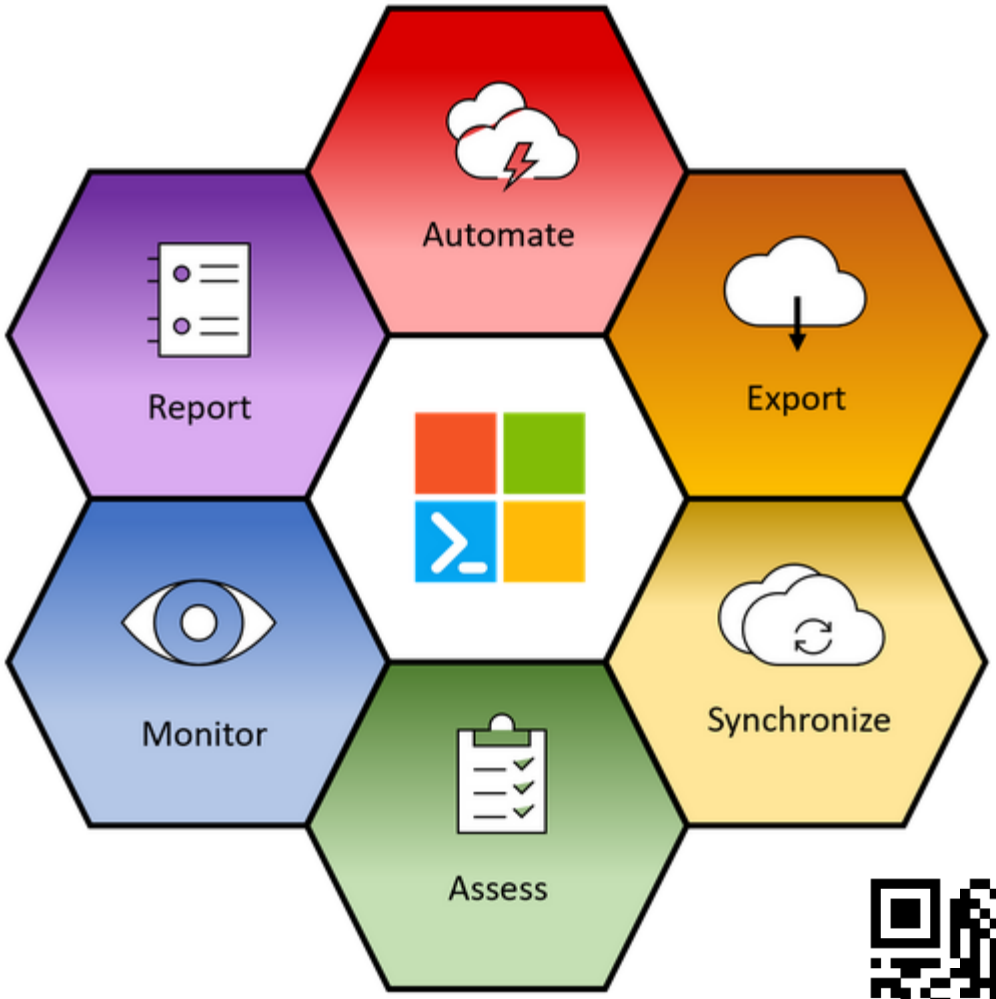


Microsoft Compliance Score: Part of the Microsoft Compliance Manager this scans through your Microsoft 365 environments and detect your system settings, continuously and automatically updating your technical control status.



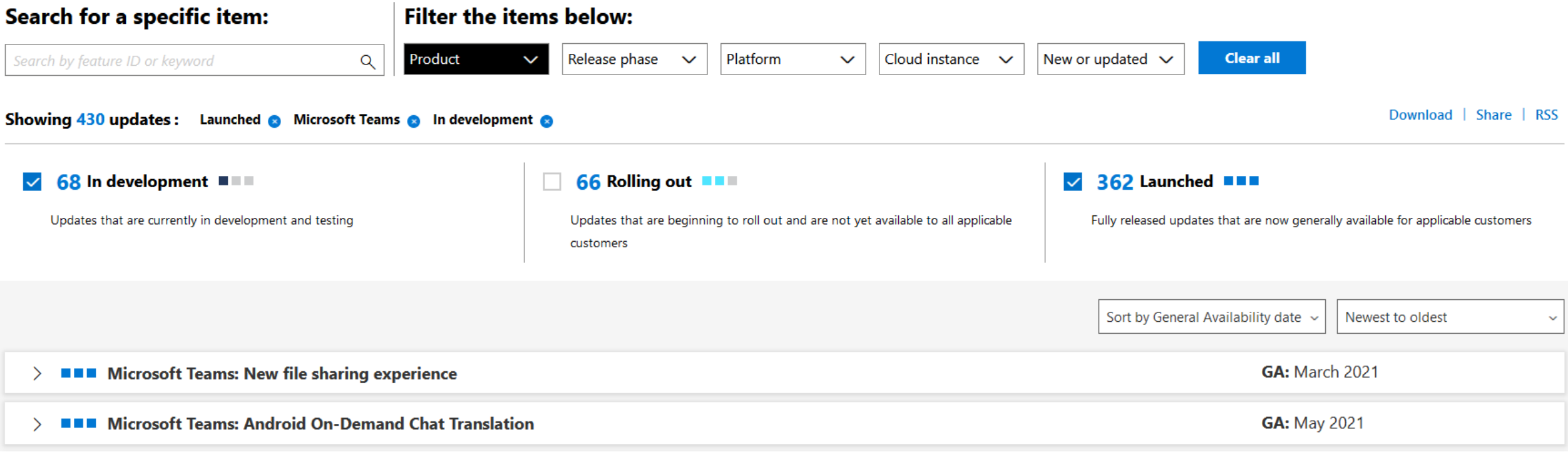
Microsoft365DSC

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

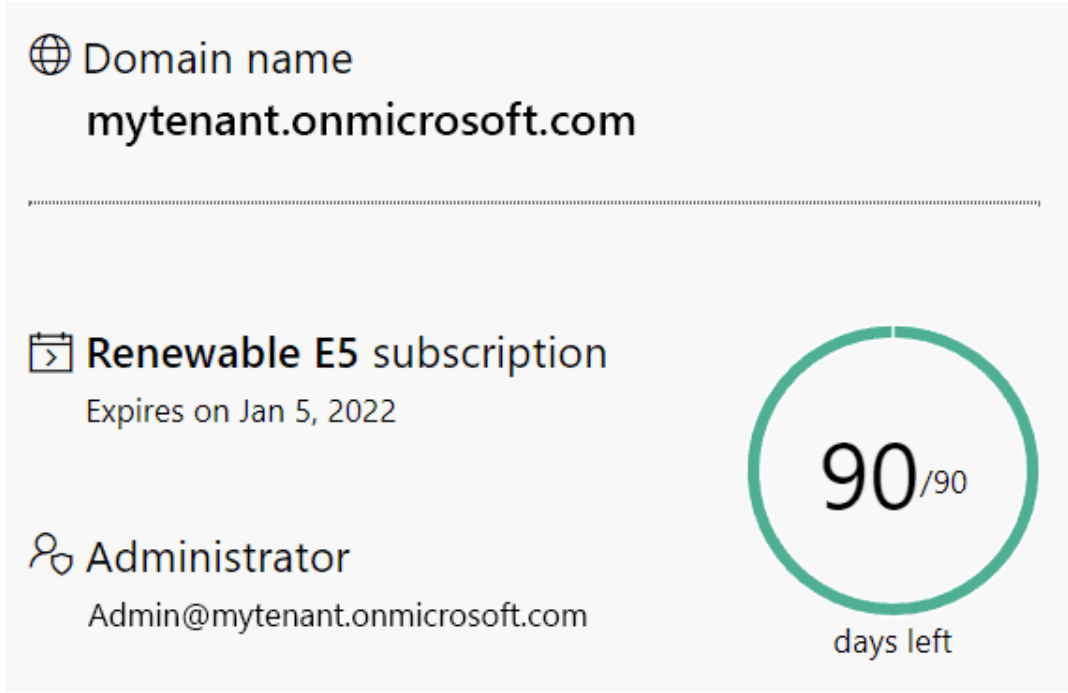


https://aka.ms/roadmap

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:

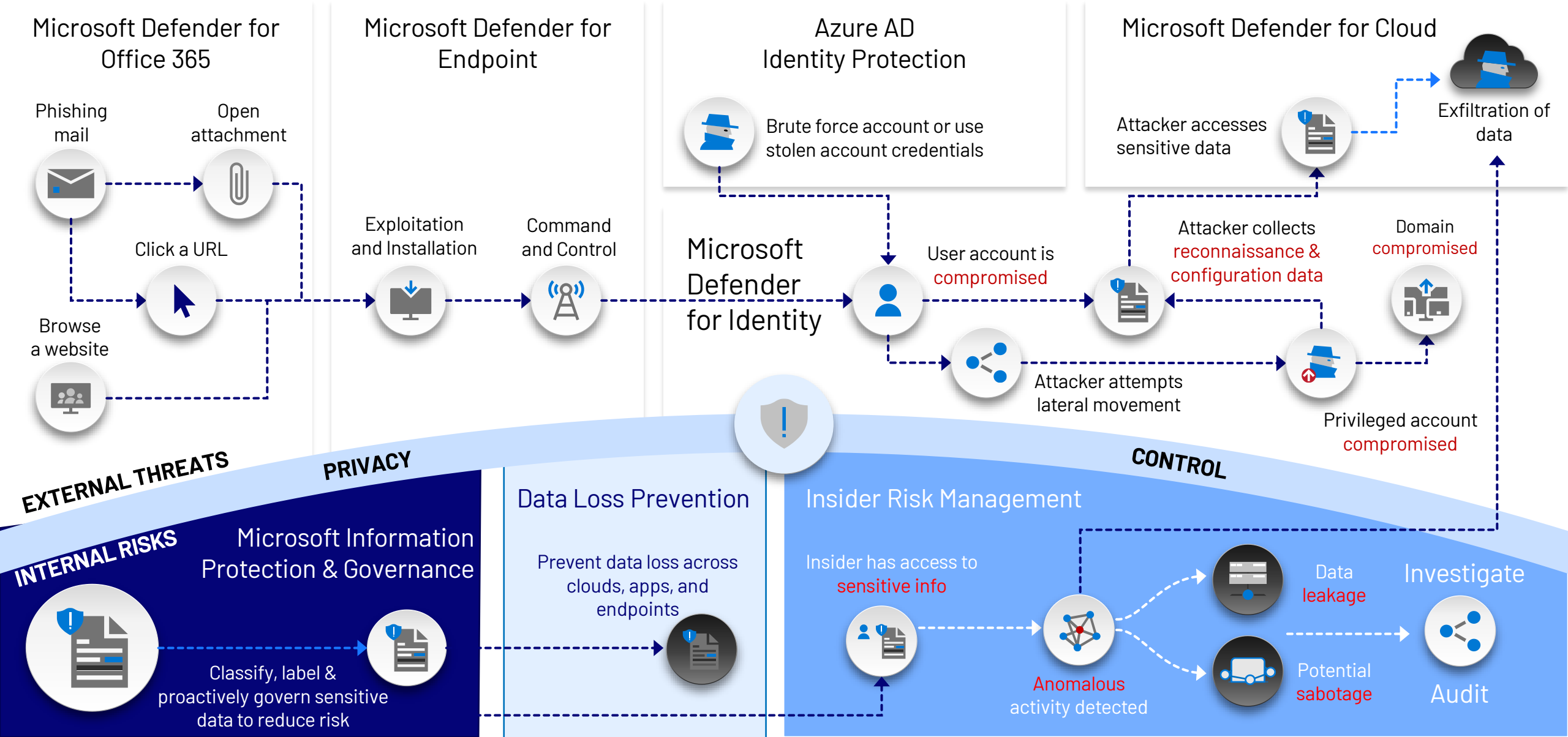
All customers can access self-serve resources on this site. Log in for guidance and planning resources to support your Microsoft 365 deployment.

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 of resource 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/Defender0365

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?

CyberCX