



CSP Level Up In-Person Technical Training



Become Copilot Ready



Security for AI Assessment | Microsoft 365 Copilot



Microsoft Security Azure Dynamics 365 Microsoft 365 Microsoft Teams Windows 365

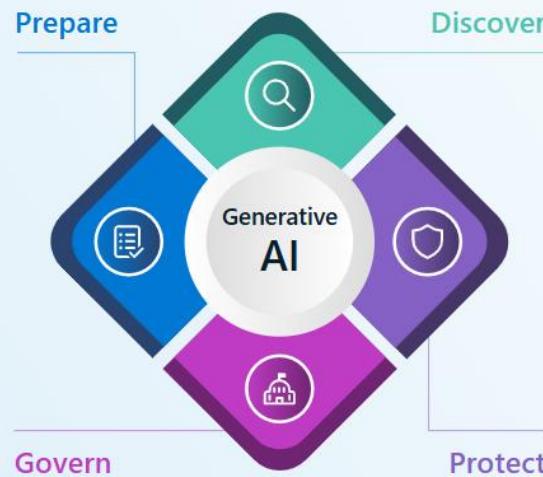
All Microsoft



Sign in

AI Security dimensions

Use our **Security for AI Assessment** to evaluate your current AI security across four key pillars: **Prepare, Discover, Protect, and Govern.**



Hover over each dimension to learn more about the key pillars used to evaluate your current AI security.

Strengthen your AI security strategy

Security for AI Assessment | Microsoft 365 Copilot

Business leaders are eager to adopt AI to drive innovation, while security teams work to defend against new and evolving risks. Security and risk leaders want to support innovation, but only if it's done safely.

Complete the **Security for AI Assessment** to receive a detailed report of your current security state and actionable recommendations.

[Start assessment](#)

<https://security-for-ai-assessment.microsoft.com/>

Building a Secure Foundation for Microsoft Copilot

Day 01: Securing Against Internal Threats

Fortify Access

Secure Data I

Shield Endpoints

Day 02: Securing Against External Threats

Protect Devices

Defend Users

Secure Data II

Become Copilot Ready

Enable AI-powered secure productivity



AI-powered productivity

Introduce the power of Generative AI with Copilot with Commercial Data Protection.

Enable the best *Copilot for Microsoft 365** experience with M365 Apps.



Protect your data

Use zero trust security to protect identities, devices, applications and data.

If you add *Copilot for M365**, it inherits security controls and protection of your tenant.



Centralize management

Manage secure productivity from a central point, unifying endpoint management in the cloud.

Deploy and secure enterprise applications, endpoints and identities.

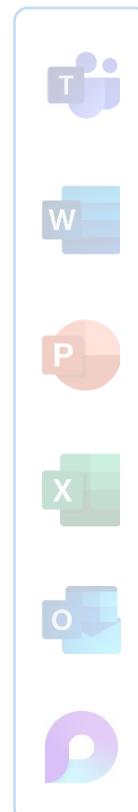
Govern access to Copilot

Microsoft Entra ID Premium P1

Users and Devices

- 1 **Govern access to Copilot** with Identity and access management

- 2 Microsoft Entra ID P1



Login to Microsoft 365 with a single & managed corporate identity.



Evaluate login attempts based on the user or group membership, IP location, device state, application.



Decide access level with Conditional Access policies.



Allow
access



Require
MFA



Limit
access



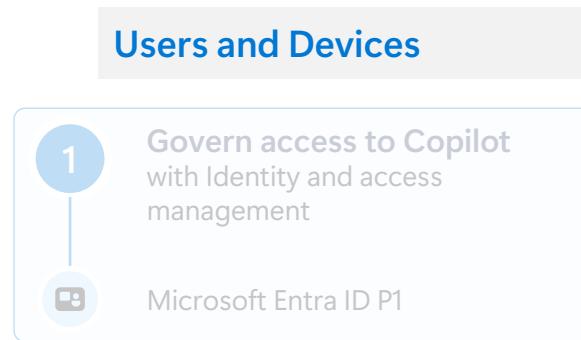
Password
reset



Monitor critical events and issue access tokens that can be revoked immediately.

Mitigate device and application risk

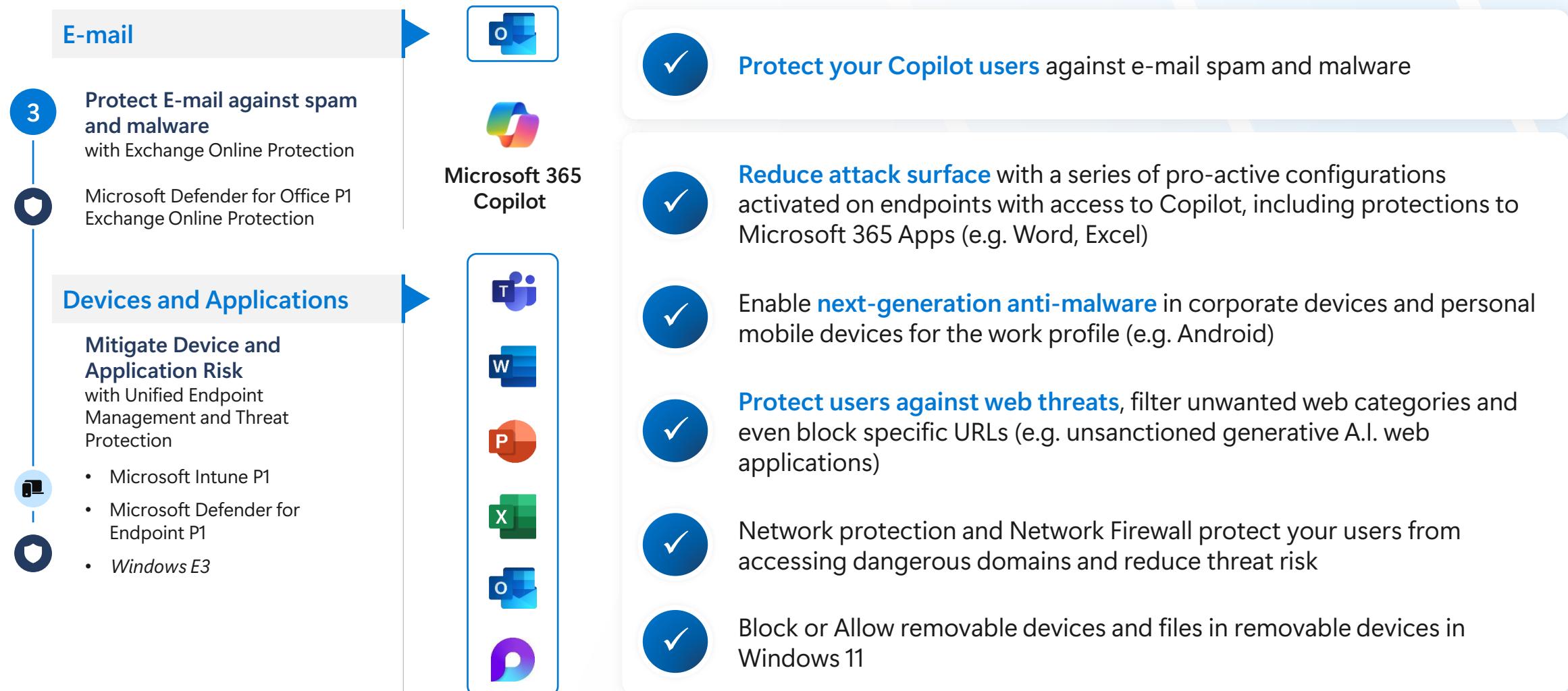
Microsoft Intune P1



- Ensure the Microsoft 365 apps are securely installed on the user's device and kept up to date.
- Limit the use of work apps, including Copilot, on personal devices
- Implement App protection policies to limit the actions users can take on devices:
 - Save generated files to unsecured apps
 - Restrict copying and pasting to non-work apps
 - DLP + Sensitivity Labels
- Wipe all work content if the device is lost or disassociated with the company or the user.

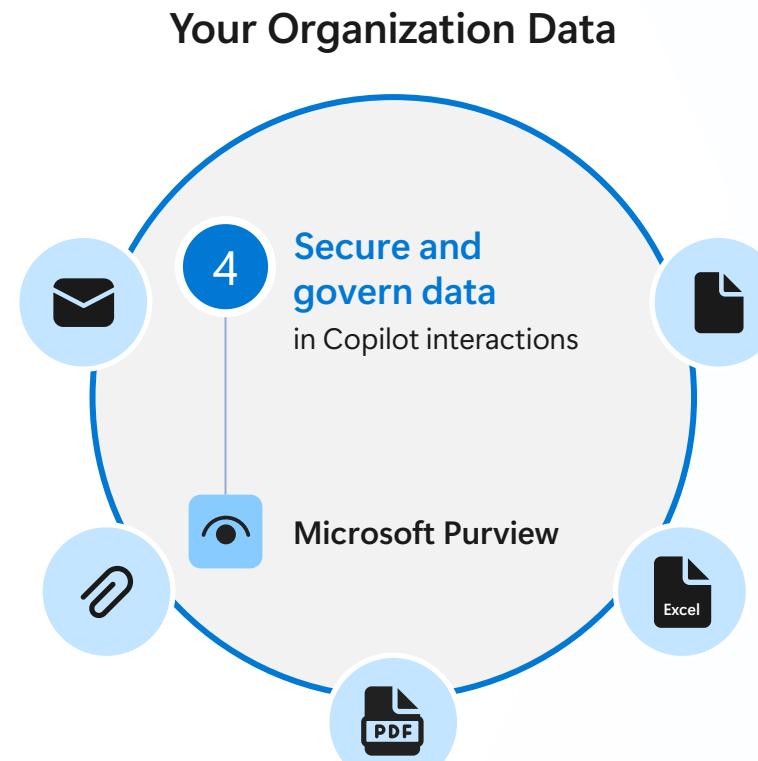
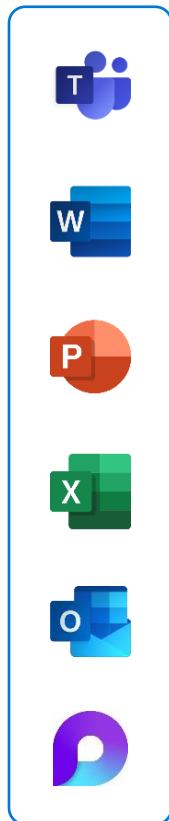
Protect E-mail, devices and apps against threats

Microsoft Defender for Endpoint P1, Exchange Online Protection



Secure and govern data in Copilot interactions

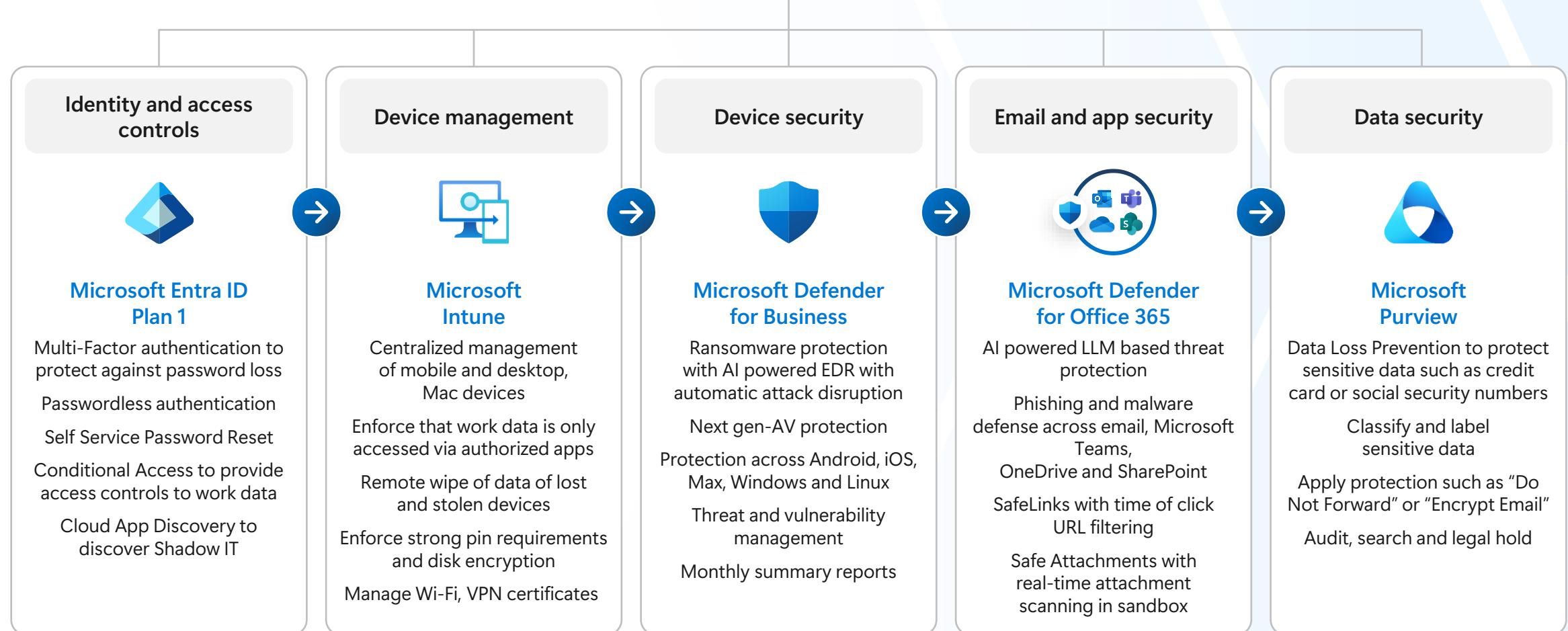
Microsoft Purview Information Protection P1



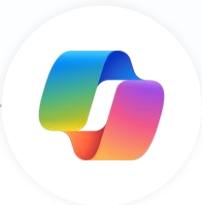
- Data consumption and processing with Copilot is limited to the user's permissions
- Copilot respects sensitive documents' sensitivity labels
- If Copilot generates sensitive data and saves it in Microsoft 365, Data Loss Prevention policies will apply
- Interactions with Copilot are retained and logged for audits or search purposes. Detect business, or code of conduct violations
- Remove inactive data to reduce obsolete insights

Becoming Copilot Ready Layered Security

Microsoft 365 Business Premium



Secure and govern Copilot with Microsoft Security



Foundational

Microsoft 365 Copilot
+ Business Basic
+ Business Standard

Multi-factor Authentication
Audit logging
Search and export
Retention or deletion policies
Restricted SharePoint Search



Core

Microsoft 365 Copilot
+ Business Premium
+ Microsoft 365 E3

+ SharePoint Advanced Management

Conditional Access
Manual sensitivity labels
Data loss prevention policies
Advanced SharePoint sitewide access controls and reporting
Search, export, eDiscovery case management, and legal hold



Best-in-class

Microsoft 365 Copilot
+ Microsoft 365 E5
+ SharePoint Advanced Management

Conditional Access based on identity risk
Automatically apply sensitivity labels
Automatically remove inactive content
Prevent data leak on endpoint devices
Detect non-compliant usage

Securing AI Environments from Threats



Securing AI Environments from External Threats



Defend Users

Block phishing with protection policies

Use Safe Links and Safe Attachments

Train users to detect and report threats



Protect Devices

Secure endpoints with compliance policies

Mitigate risks using vulnerability management

Ensure device compliance for safe AI use



Govern Data Sharing

Enable granular data governance with tools like SAM for enhanced SharePoint control

RSS to restrict unauthorized file sharing

Apply data governance to prevent oversharing

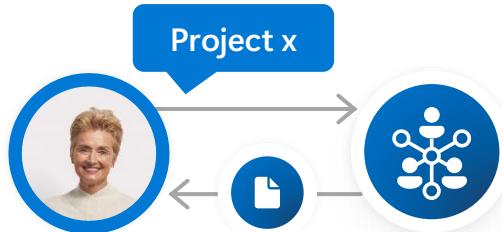
Mitigating external threats protects your people, devices, and data—ensuring a secure foundation for Copilot and beyond

Security and compliance challenges

1

Data oversharing

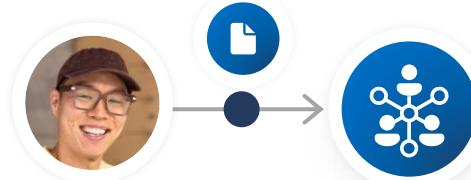
Users may access sensitive data via AI apps they're not authorized to view or edit



2

Data leak

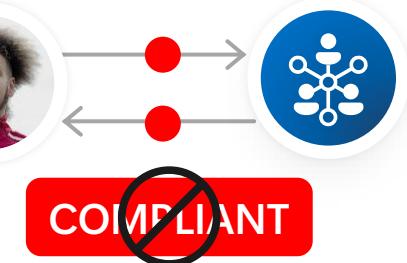
Users may inadvertently leak sensitive data to AI apps



3

Non-compliance usage

Users use AI apps to generate unethical or other high-risk content



Understanding Internal and External Threats



Internal Threats

Threats originating from within the organization, whether accidental or malicious, involving employees, contractors, or other trusted users.

Most Common Internal Threats:

- **Accidental Data Leaks:** Sharing sensitive data via email or cloud storage without safeguards.
- **Credential Misuse:** Employees using weak or compromised passwords, leading to unauthorized access.
- **Insider Threats:** Malicious actions by employees or contractors, like data theft or sabotage.

Why It Matters:

Internal threats often bypass perimeter defenses, making secure access controls (MFA, Conditional Access) and data classification critical to protect sensitive assets.



External Threats

Threats originating from outside the organization, including cyberattacks, phishing, ransomware, and malicious actors.

Most Common External Threats:

- **Phishing Attacks:** Targeting employees with fraudulent emails to steal credentials.
- **Ransomware:** Encrypting data and demanding payment to restore access.
- **Device Compromise:** Attackers exploiting vulnerabilities in endpoints or unmanaged devices.

Why It Matters:

External attacks are sophisticated and constantly evolving. Advanced protection like Safe Links, Safe Attachments, and Defender for Endpoint is critical to safeguard the organization.

Secure and govern Copilot with Microsoft Security



Security



Compliance



Privacy



Responsible AI



Discover AI risks

Identify sensitive data in Copilot interactions with [ready-to-use classifiers and labeling](#)

Understand user activities and detect risky access to Copilot with [audit logging](#)

Identify potentially overshared content by reviewing [SharePoint site permissions](#)



Protect sensitive data

Protect access to sensitive data in Copilot interactions with [persistent labeling and DLP policies](#)

Restrict or block risky access with [risk-based conditional access and endpoint management](#)

Prevent idle or excessive access with [SharePoint site wide access controls](#)



Govern Copilot usage

Retain and log Copilot interactions, automatically remove inactive content

Use built-in classifiers to [detect non-compliant use of Copilot](#)

Preserve, review, and analyze prompts and responses to [investigate security and compliance incidents](#)

Secure and govern Copilot with Microsoft Security



Foundational

Microsoft 365 Copilot
+ Business Basic
+ Business Standard

Multi-factor Authentication
Audit logging
Search and export
Retention or deletion policies
Restricted SharePoint Search



Core

Microsoft 365 Copilot

+ Business Premium

+ Microsoft 365 E3

+ SharePoint Advanced Management

Conditional Access
Manual sensitivity labels
Data loss prevention policies
Advanced SharePoint sitewide access controls and reporting
Search, export, eDiscovery case management, and legal hold



Best-in-class

Microsoft 365 Copilot
+ Microsoft 365 E5
+ SharePoint Advanced Management

Conditional Access based on identity risk
Automatically apply sensitivity labels
Automatically remove inactive content
Prevent data leak on endpoint devices
Detect non-compliant usage

Fortify Access: Identity & Access Management



Securing Against Internal Threats

Reducing Risk Within Your Organization

Fortify Access

Identity & Access Management



Secure Internal Data

DLP & Sensitivity Labels



Shield Devices

Endpoint & Threat Protection



61% of all breaches involve credentials¹

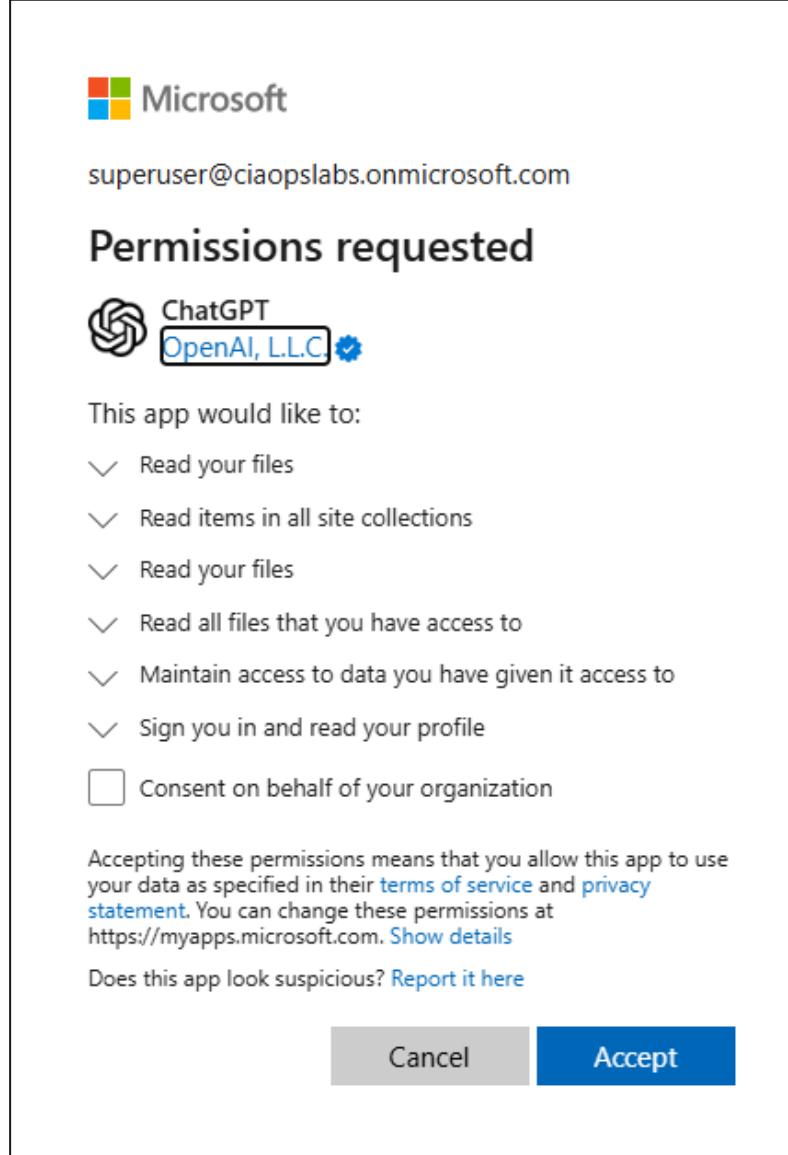
There are over **4,000 password attacks**
every second¹

**76% of businesses expect a successful
attack in the next 12 months²**

1. Ponemon Institute Cost of Breach Data 2021 | 2. Trend Micro [Cyber Risk Index \(CRI\)](#)

2. [Microsoft Security Signals Boost SDM Research Learnings](#). Hypothesis Group, Sep 2021

Prevent users making the wrong choice



Control user access

 **Users | User settings** CIAOPS

X <<  Refresh |  Got feedback?

All users

Audit logs

Sign-in logs

Diagnose and solve problems

Deleted users

Password reset

User settings

Bulk operation results

New support request

Default user role permissions

[Learn more](#)

Users can register applications   No

Restrict non-admin users from creating tenants   Yes

Users can create security groups   No

Guest user access

[Learn more](#)

Guest user access restrictions  Guest users have the same access as members (most inclusive)

Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Administration center

[Learn more](#)

Restrict access to Microsoft Entra admin center   Yes

LinkedIn account connections

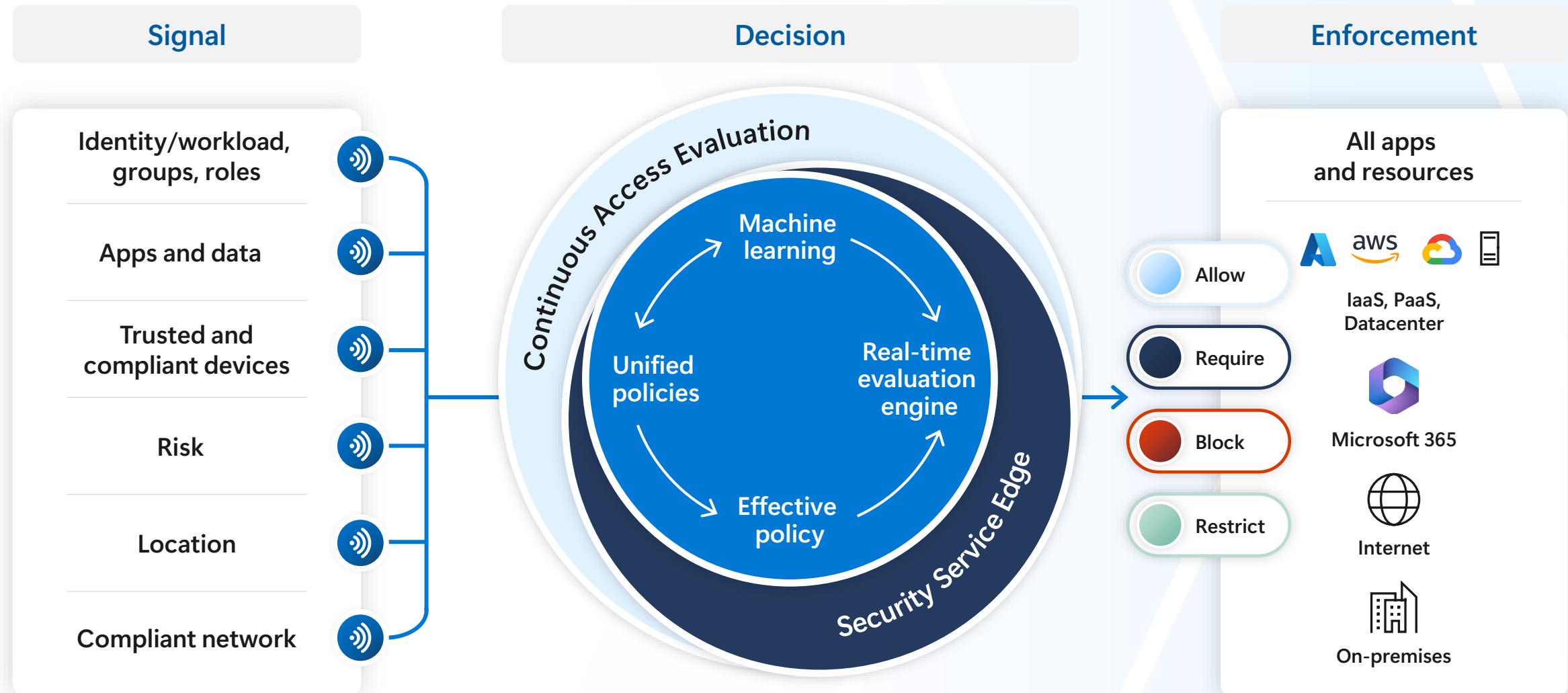
[Learn more](#)

Allow users to connect their work or school account with LinkedIn  Yes

Selected group

No

Enhance Conditional Access with new conditions and controls



Enforce real-time Conditional Access policies



Enforce access controls with adaptive policies



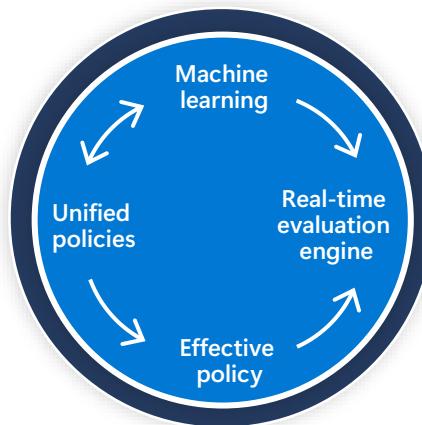
Protect data inside applications



Restrict access for vulnerable and compromised devices

Signals

Identity,
roles, groups
Apps and data
Device
Location
Risk



Verify every access attempt

- Allow access
- Require MFA
- Limit access
- Password reset
- Monitor access



Conditional Access Policy Templates



Policy templates provide a convenient method to deploy new policies aligned with Microsoft recommendations.

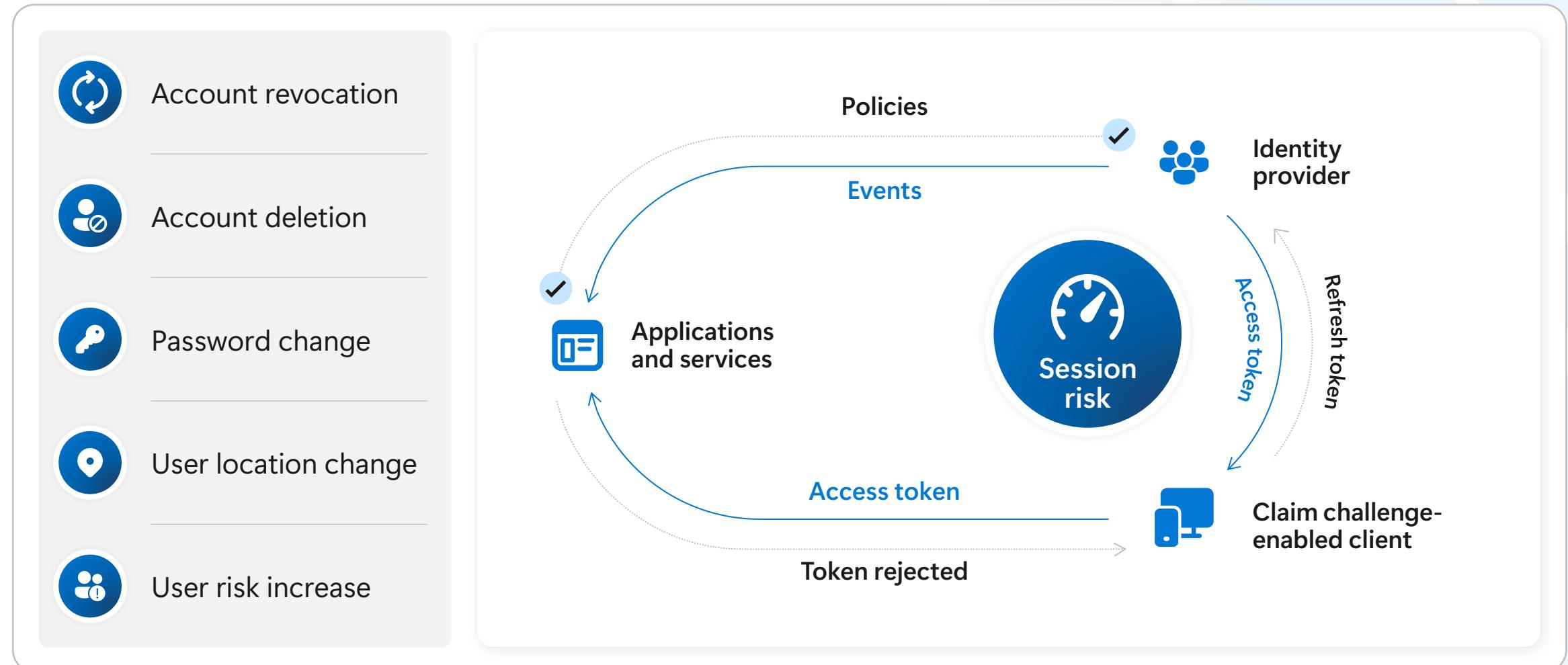
- Templates are grouped into scenario categories:
 - Secure foundation
 - Zero Trust
 - Remote work
 - Protect administrator
 - Emerging threats
 - All
- Templates can be reviewed and adapted before applying
- Ability to upload custom policy files to create your own policy templates

The screenshot shows the 'Create new policy from templates' page. At the top, there are tabs for 'Select a template' (which is selected) and 'Review + Create'. Below the tabs is a search bar with the placeholder 'Search'. Underneath the search bar, there are several category tabs: 'Secure foundation' (selected), 'Zero Trust', 'Remote work', 'Protect administrator', 'Emerging threats', and 'All'. The main area displays a list of policy templates, each with a radio button, a title, a brief description, and 'View' and 'Download JSON file (Preview)' buttons. The first template listed is 'Require multifactor authentication for admins'.

Template Category	Template Title	Description	Action Buttons
Secure foundation	Require multifactor authentication for admins	Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults. Learn more	View Download JSON file (Preview)
Secure foundation	Securing security info registration	Secure when and how users register for Azure AD multifactor authentication and self-service password. Learn more	View Download JSON file (Preview)
Secure foundation	Require multifactor authentication for all users	Require multifactor authentication for all user accounts to reduce risk of compromise. Learn more	View Download JSON file (Preview)
Secure foundation	Block legacy authentication	Block legacy authentication endpoints that can be used to bypass multifactor authentication. Learn more	View Download JSON file (Preview)
Secure foundation	Require multifactor authentication for Azure management	Require multifactor authentication to protect privileged access to Azure resources. Learn more	View Download JSON file (Preview)
Secure foundation	Require compliant or hybrid Azure AD joined device or multifactor authentication for all users	Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. (macOS or Windows only) Learn more	View Download JSON file (Preview)

Secure entire session with continuous access evaluation

Auto-revoke access in near real-time when critical events or policy violations are detected



Common Policies for Conditional Access

Some policies are commonly used across various customer types and scenarios

- Block access for unknown or unsupported device platform
- No persistent browser session
- Require approved client apps or app protection
- Require compliant or hybrid Azure AD joined device or multifactor authentication for all users
- Require compliant or Hybrid Azure AD joined device for administrators
- Require multifactor authentication for guest access
- Securing security info registration
- Use application enforced restrictions for unmanaged devices
- Require multifactor authentication for risky sign-in*
- Require password change for high-risk users*
- Block legacy authentication**
- Require multifactor authentication for admins**
- Require multifactor authentication for all users**
- Require multifactor authentication for Azure management**



Microsoft Lighthouse can help standardize and streamline the deployment of these policies.

*Requires Entra ID P2

**These four policies provide similar functionality enabled by security defaults

Exploring Microsoft Entra Sign-In Logs



The Importance of Sign-In Logs in Security

1. Detecting Suspicious Behavior

Monitor login patterns to identify unusual activities such as:

- Failed sign-in attempts
- Access from unfamiliar locations
- Unexpected login times

2. Troubleshooting Access Issues

Quickly pinpoint causes of blocked or failed sign-ins, such as Conditional Access policies, and resolve user access issues.

3. Proactive Security Management

Regularly review sign-in logs to:

- Monitor trends and detect risks
- Maintain a strong security posture
- Ensure access controls function as intended

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > Sign-in events

Date : Last 24 hours Show dates as : Local Add filters

User sign-ins (interactive) User sign-ins (non-interactive) Service

Date	Request ID	User
8/16/2023, 9:18:26 AM	0000111-aaaaa-2222	Izaak Schmitz
8/16/2023, 9:17:46 AM	111000-bbbb00-221...	Shokat Nadeem
8/16/2023, 9:17:29 AM	11100aa-111aaaa-b...	Emma Blug
8/16/2023, 9:17:26 AM	aaaa1111-000111-aa...	Kasper Graf

Incident Management and Response

End-to-end attack story



Reconstructing the story

The broader attack story is better described when relevant alerts and related entities are brought together



Incident scope

Analysts receive better perspective on the purview of complex threats containing multiple entities



Higher fidelity, lower noise

Effectively reduces the load and effort required to investigate and respond to attacks



For more details click [here](#).

The screenshot displays two main windows of the Microsoft 365 Defender platform. The top window is titled 'Incidents' and shows a list of recent incidents and alerts. It includes filters for Status (New +1), Severity (High +2), and Service sources (EDR). The list includes entries like 'Multi-stage incident on multiple endpoints' (Severity: High, 73/73 active alerts) and 'SensitiveFilesDiscovery' (Severity: Medium, 71/71 active alerts). The bottom window is a detailed view of a specific incident titled 'Multi-stage incident on multiple endpoints'. It provides an overview of the attack story, showing 73/73 active alerts, 1 MITRE ATT&CK tactics, and 1 other alert categories. It also lists 20 impacted devices and 12 impacted users. A timeline on the left shows events such as 'Suspicious connection blocked by network protection on ubuntu01' occurring on Jan 27, 2023. The right side of the bottom window shows a summary of 187 entities found, with a 'View all entities' link at the bottom.

Vulnerability management

A risk-based approach to prioritize and remediate your vulnerabilities



Continuous real-time discovery



Context-aware prioritization



Built-in end-to-end remediation process



Powered by [Microsoft Defender Vulnerability Management \(core\)](#)

The screenshot displays the Microsoft Defender Vulnerability Management dashboard. At the top, it shows an 'Organization exposure score' of 23/100. Below this is a 'Remediation activities' section with a bar chart titled 'Block Office communication application from creating 37/87 child processes'. To the right, there's a 'Top security recommendations' table:

Recommendation	Exposed devices	Threats	Impact	Tags
Update Microsoft Edge Chromium-based	213	0	10.69	
Update Ubuntu Tar for Linux	94	0	2.64	
Update Apple Safari for Mac	63	0	2.64	

Below the dashboard are sections for 'Top events (7 days)', 'Top remediation activities', and 'Top vulnerable software'. On the right side, there's a sidebar for 'Your score for' with a progress bar for 'Microsoft Secure Score for Devices' and a 'Score for device' section.

Defend Users: Phishing & Threat Protection



Securing Against External Threats

Reducing Risk Within Your Organization

Defend Users

Phishing & Threat Protection



Protect Devices

Endpoint Security Strategies



Secure Data II

Data Protection & Governance



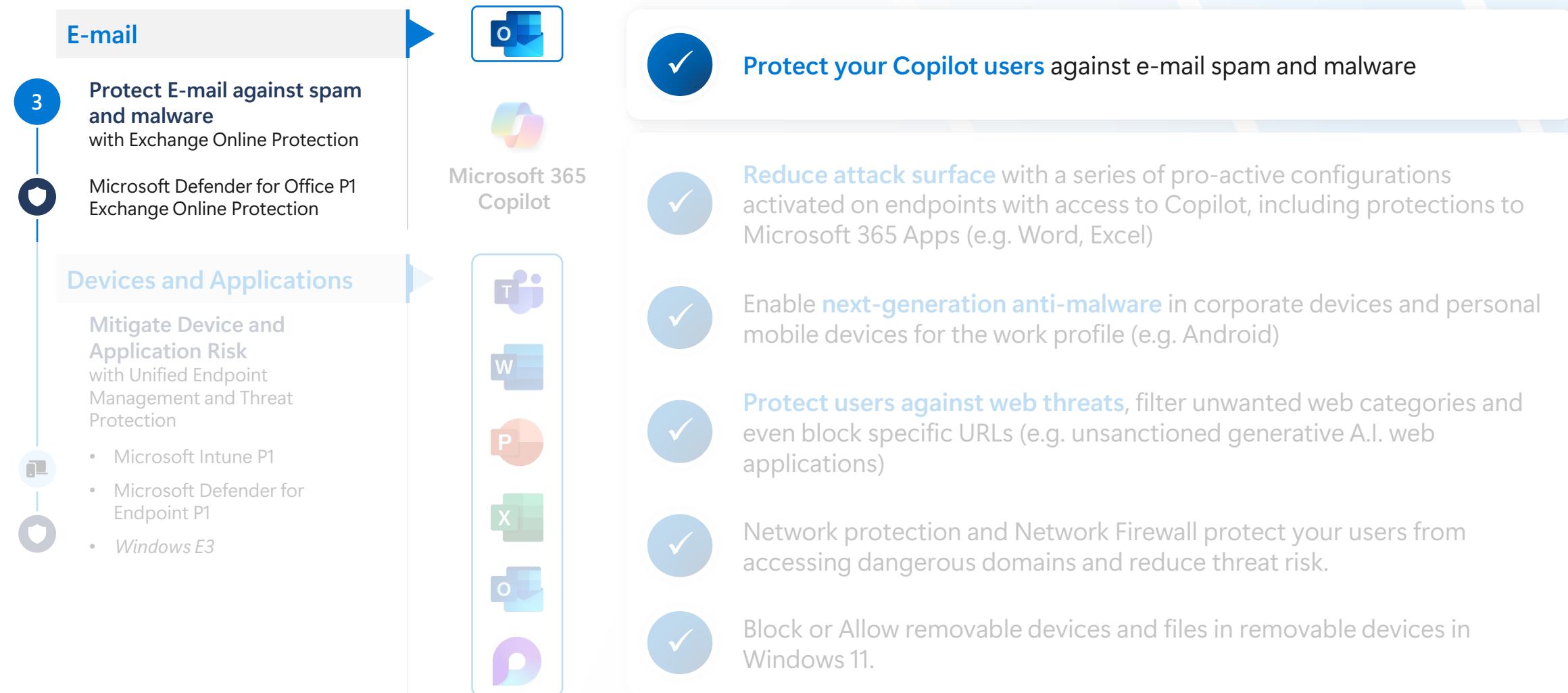
96% of phishing attacks arrive via email

3+ billion phishing emails are sent daily

\$26 billion
in business email compromise (BEC)
losses since 2021

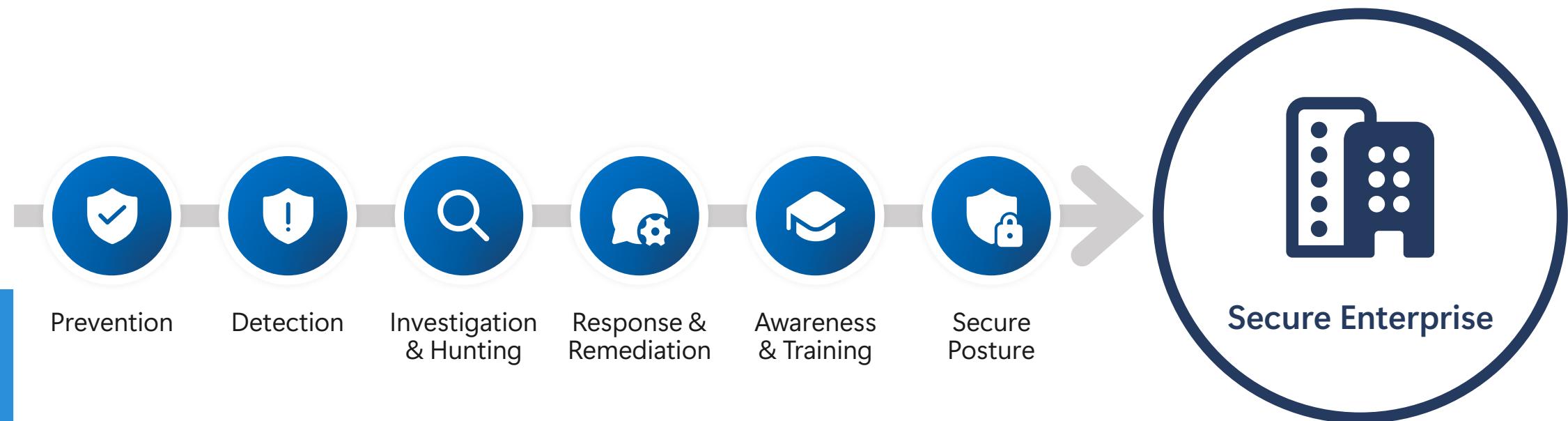
Protect E-mail, devices and apps against threats

Microsoft Defender for Endpoint P1, Exchange Online Protection



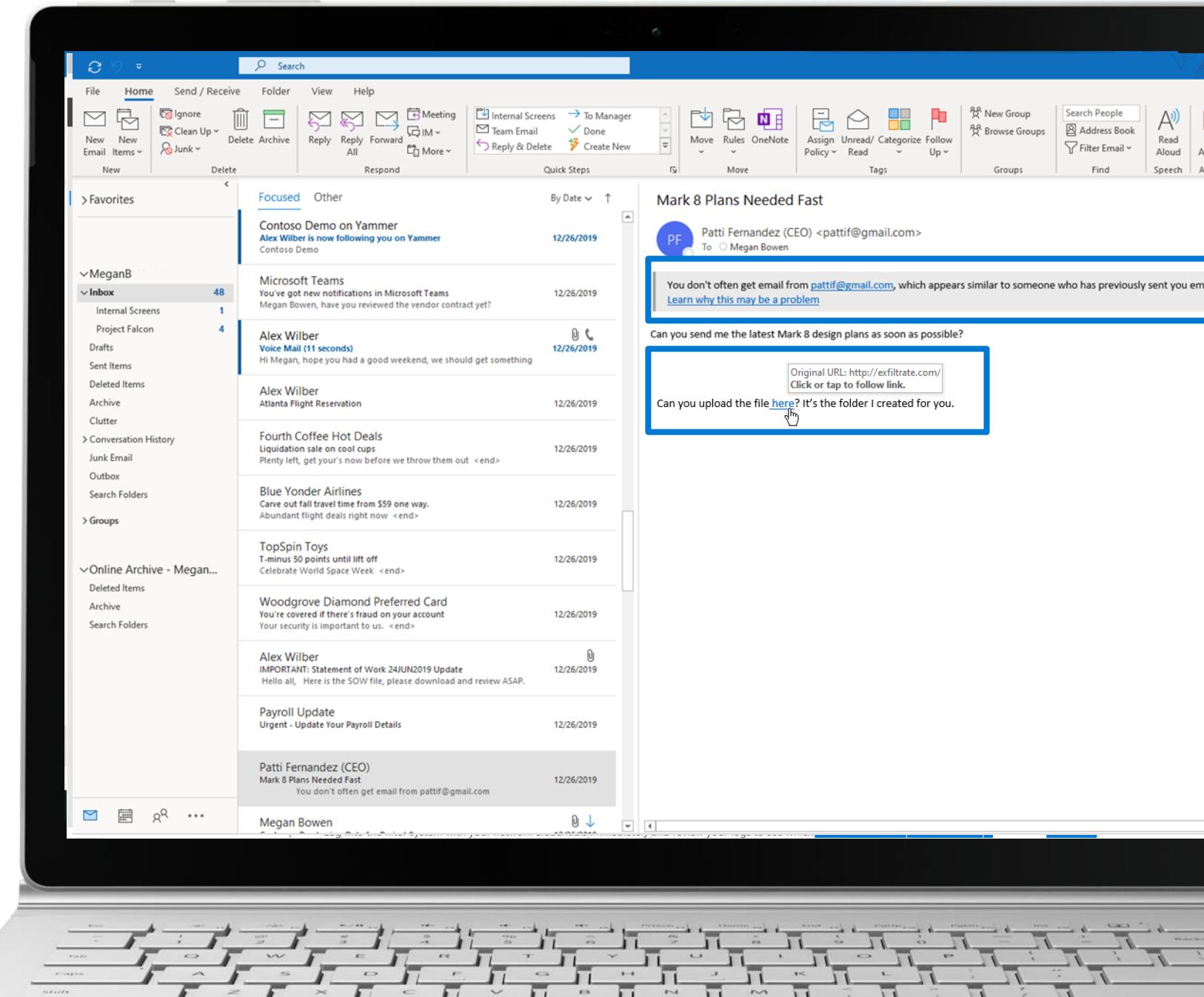
Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention



Enhancing Security with Phish Reporting

- User Reporting:** Empower users to report suspicious emails. Dynamic end user training.
- Admin Alerts:** Immediate notifications for reported phishing attempts.
- Training Reinforcement:** Supports user awareness and training programs.
- Rapid Response:** Enables quick action to mitigate threats.



AI Powered protection against phishing attacks with Microsoft Defender for Office 365



AI-powered email analysis and filtering using LLMs to help protect against Gen AI-crafted phishing emails by blocking over 100K business email compromise (BEC) emails daily with a 99.995% attacker intent accuracy and filtering



Secure email attachments and shared document links in Teams, SharePoint, and OneDrive by sandboxing potential threats with **Safe Attachments**



User impersonation protection prevents specific email addresses from being impersonated with advanced detection and prevention



Security reports enable users to swiftly identify, analyze, and respond to threats with actionable insights and tailored recommendations



Protect against malicious links in email, Teams, and other Office 365 apps with time-of-click URL filtering using **Defender for Office 365 Safe Links**

Learn more

[aka.ms/O365Plan1 >>](http://aka.ms/O365Plan1)

The screenshot shows a red warning dialog box. At the top right is a white shield icon with a large red 'X' inside. To its right, the text "This website has been classified as malicious." is displayed in white. Below this, another message reads "Opening this website might not be safe." A blue link "http://spamlink.contoso.com" is shown. At the bottom right of the dialog is a blue button labeled "X Close this page".

This website has been classified as malicious.

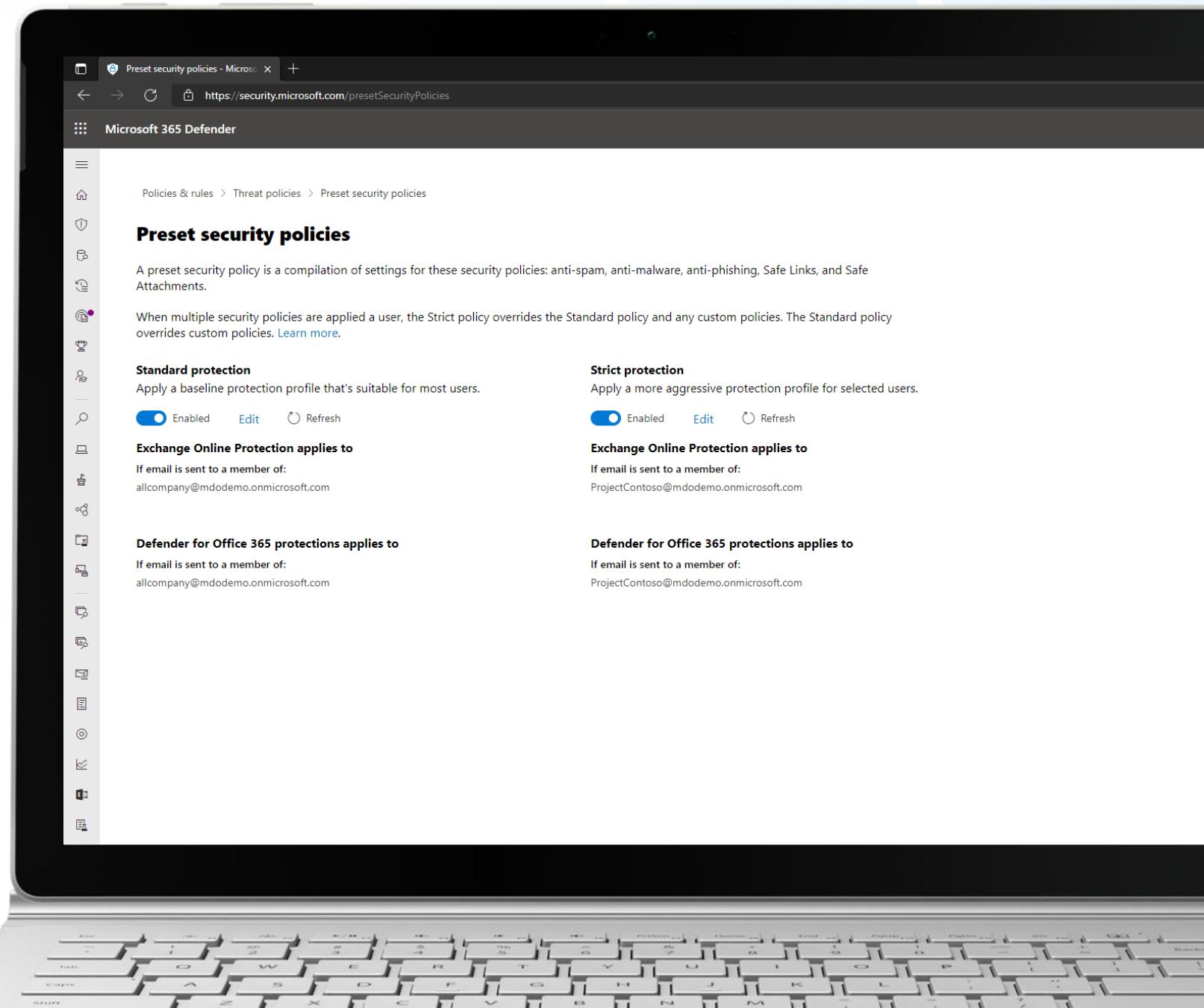
Opening this website might not be safe.

<http://spamlink.contoso.com>

X Close this page

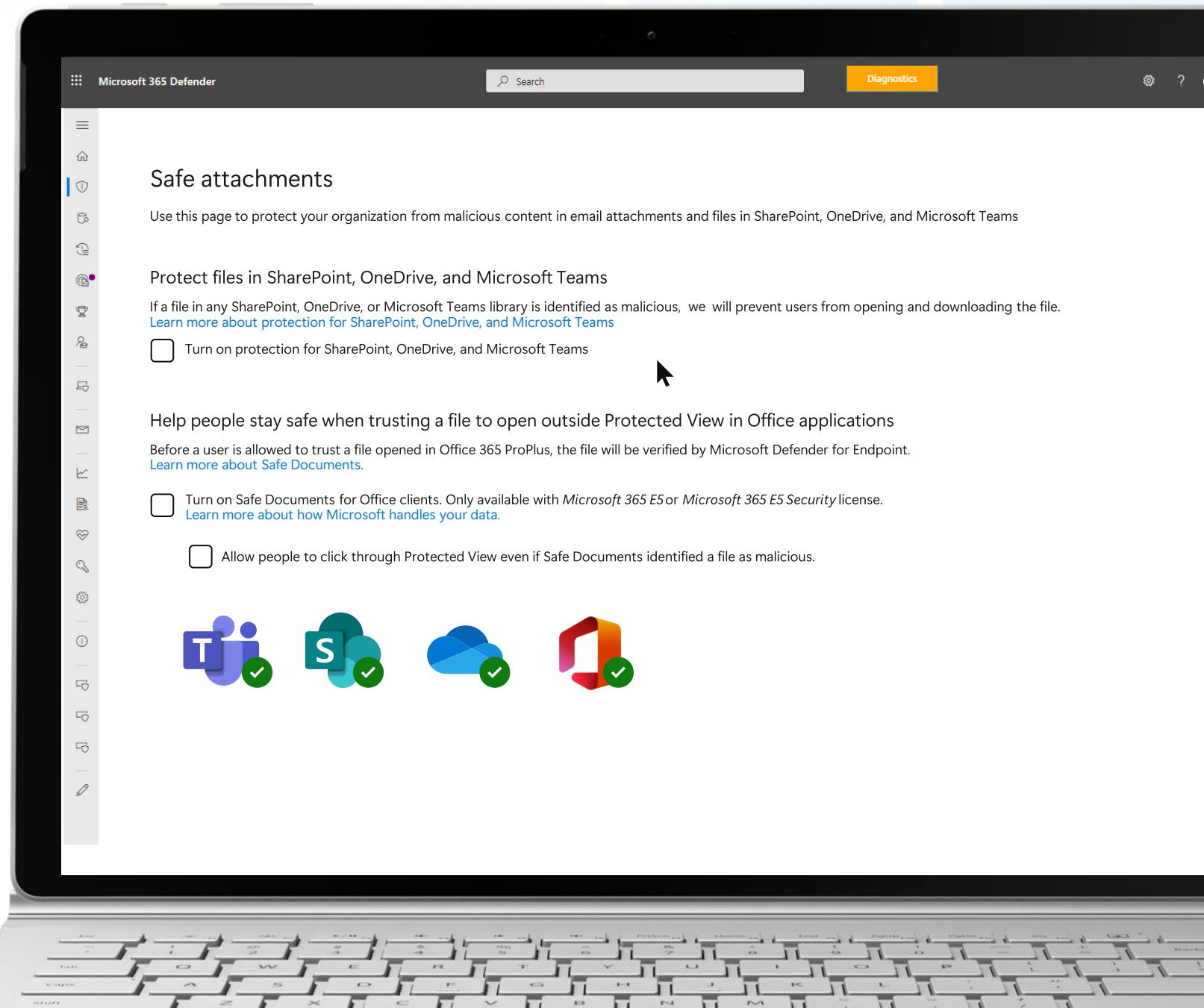
Defender for Office 365: Leveraging Preset Security Policies

- **Quick Setup:** Apply best practice security settings easily.
- **Threat Protection:** Guard against phishing and malware.
- **Customizable:** Adapt policies to fit organizational needs.
- **Regulatory Compliance:** Maintain compliance with built-in standards.



Securing Collaboration: SharePoint Online & Teams Policies

- **Controlled Access:** Manage who can access and share content.
- **Data Protection:** Ensure sensitive data remains secure during sharing.
- **Policy Enforcement:** Automatically enforce sharing policies.
- **Centralized Oversight:** Monitor and manage sharing activities from a single dashboard.



Protect against ransomware with Microsoft Defender for Business



Enterprise-grade endpoint security with EDR to defend against ransomware attacks



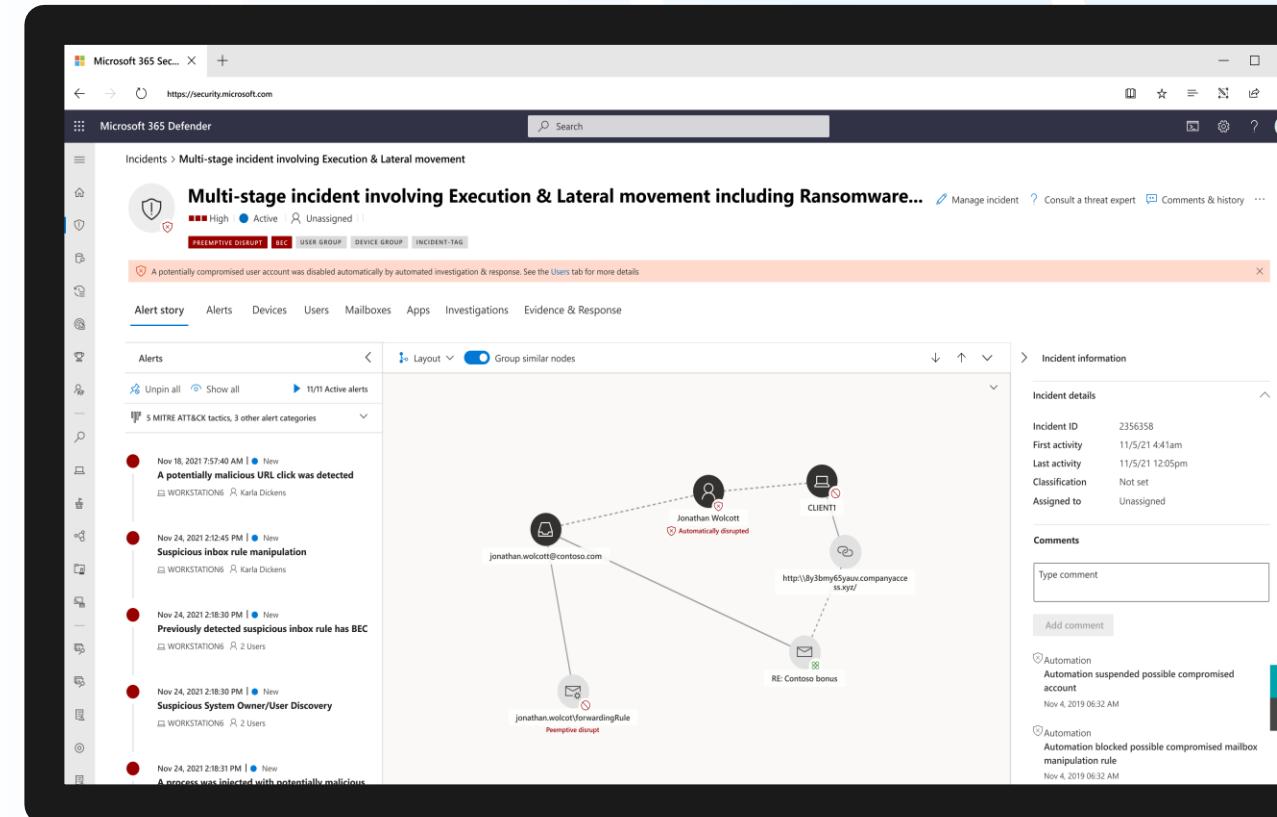
Industry first, AI-powered attack disruption to contain lateral movement of suspicious users and devices before they can act maliciously



Next gen anti-virus and protection across iOS, Android, Windows, Mac, Linux



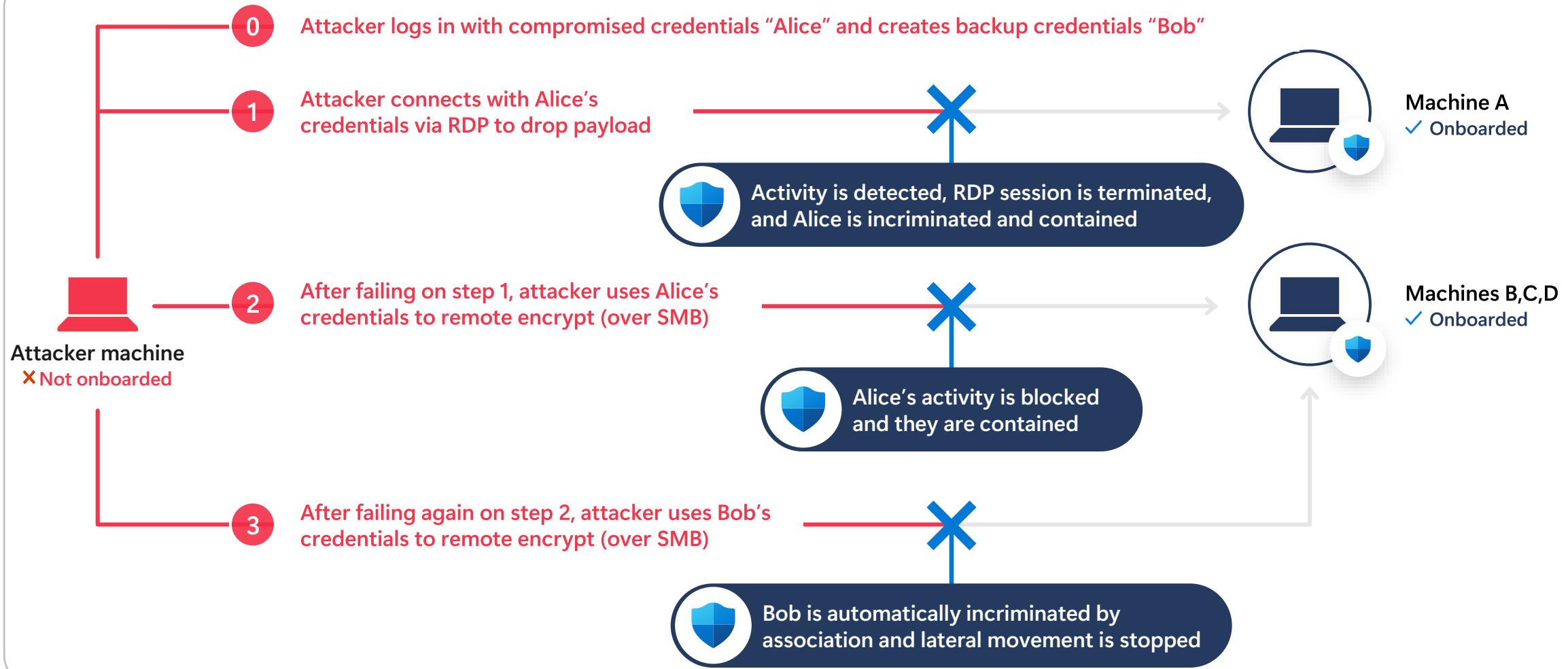
Threat and vulnerability management helps you discover, prioritize, and remediate software vulnerabilities



Learn more

aka.ms/DefenderforBusiness >>

Automatic attack disruption demo



Learn more

aka.ms/MDBAutoAttackDisrupt >>

Automatic attack disruption – What others detect, we disrupt

3 min

average time
to disrupt ransomware

7K

incidents disrupted
per month

16K+

disabled user accounts in the
last six months

180K+

devices saved from an attack
in the last six months

On by default powered by AI/ML to detect and disrupt in-progress attacks with 99% confidence

Real-life customer stories

A customer experienced an attack across:

- **10+** attack waves
- **10** compromised domain admin users
- **3** spreader IPs

Attackers targeted **2,000 devices**, **97% saved**
3% of devices were onboarded to a different security
vendor and suffered encryption

A customer experienced an attack across six users:

- **4** users were disabled at the initial access stage
- **2** users were disabled when the session cookie
was re-used

Early disruption in the kill chain prevented a business
email compromise attack

Protect Devices: Endpoint Security Strategies



Securing Against External Threats

Reducing Risk Within Your Organization

Defend Users

Phishing & Threat Protection



Protect Devices

Endpoint Security Strategies



Secure Data II

Data Protection & Governance

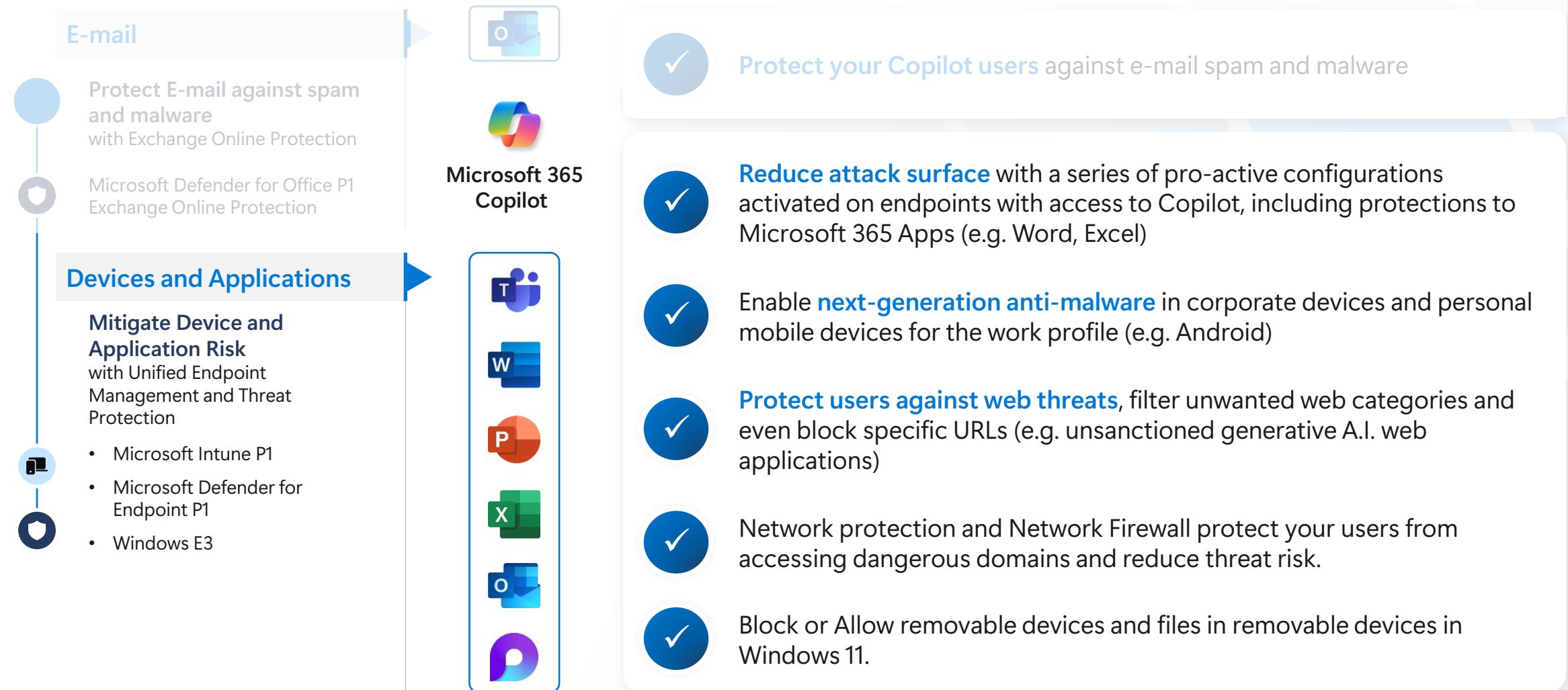


46% of compromised systems had
no malware on them

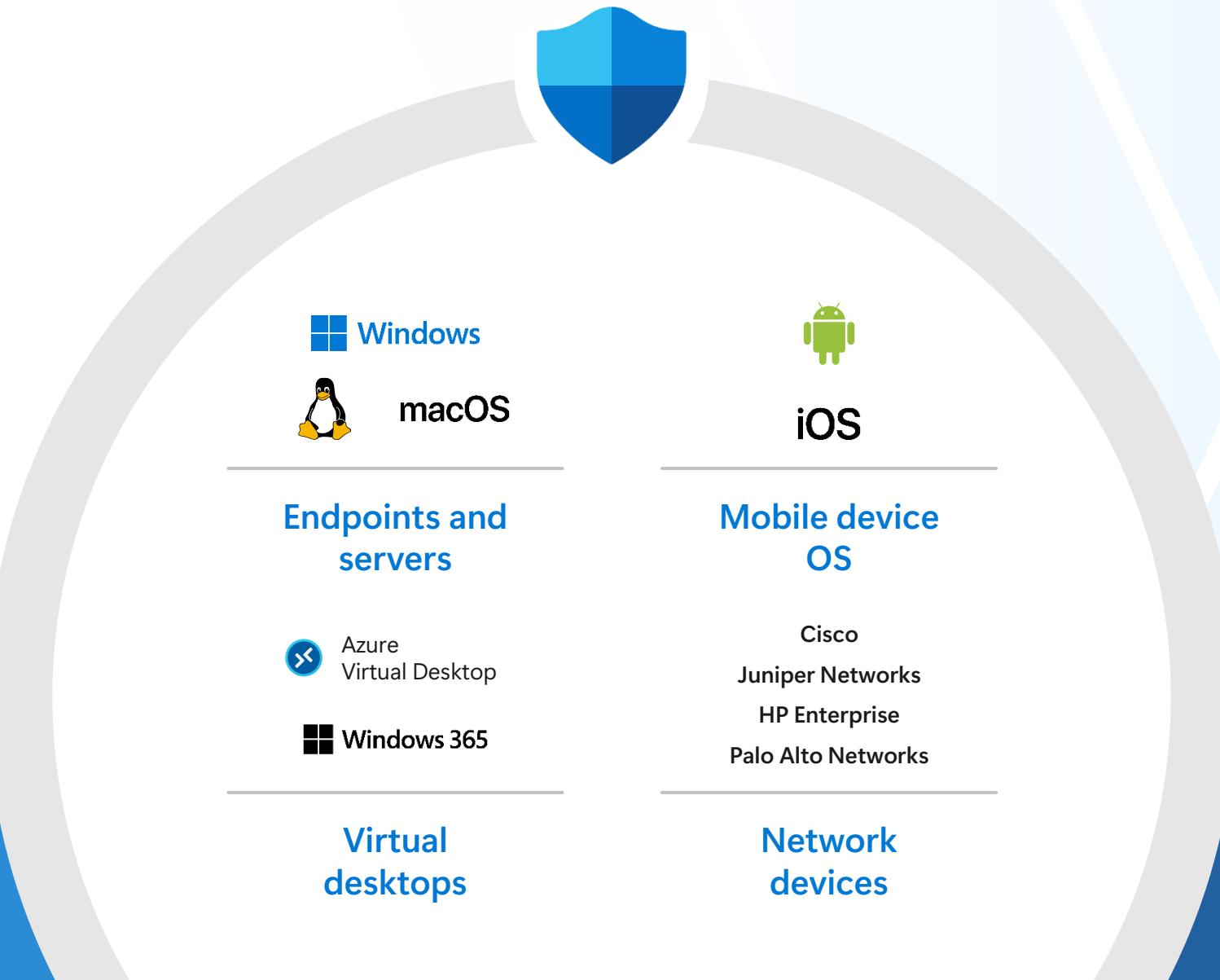
Collecting **evidence**
and alerts, even from one infected
device, can be a long **time-consuming**
process

Protect E-mail, devices and apps against threats

Microsoft Defender for Endpoint P1, Exchange Online Protection



Delivering endpoint security across platforms

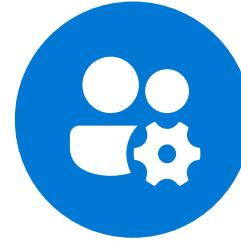


Historical roles and friction



Security Team

- Responsible for security monitoring and reducing risk
- Analyze threats, security incidents, exposure and identify mitigations
- Define security policies
- Priority is on quick remediation on impacted devices/users



IT Team

- Responsible for policy configuration including security policies
- Analyzes change impact and stages rollout of global policies
- Priority is a stable IT environment and low costs

Attack surface reduction

Eliminate risks by reducing the surface area of attack



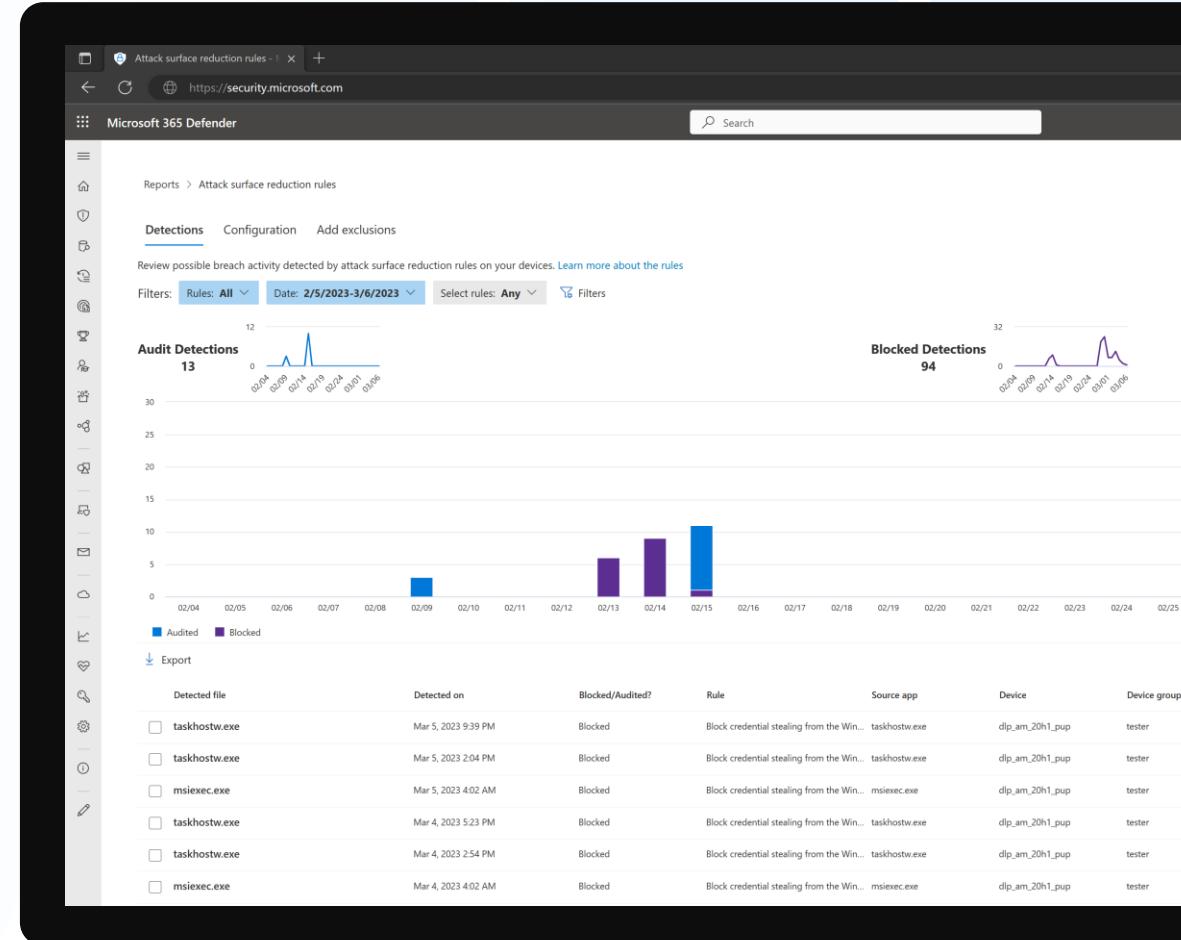
System hardening without disruption



Customization that fits your organization



Visualize the impact and simply turn it on



Attack surface reduction

Resist attacks and exploitations



HW-based isolation

Application control

Exploit protection

Network protection

Controlled folder access

Device control

Web protection

Ransomware protection

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

Block traffic to low reputation destinations

Protect your legacy applications

Only allow trusted applications to run

Attack surface reduction (ASR) rules



Minimize the attack surface

Signature-less, control entry vectors, based on cloud intelligence.

Attack surface reduction (ASR) controls, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware
- Block abuse of exploited vulnerable signed drivers

Lateral movement and credential theft

- Block process creations originating from PSEXEC and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

Network protection

Allow, audit and block

- Perimeter-less network protection (“SmartScreen in the box”) preventing users from accessing malicious or suspicious network destinations, **using any app on the device and not just Microsoft Edge**
- Customers can add their own TI in addition to trusting our rich reputation database

The screenshot shows the Microsoft 365 Defender interface under the 'Endpoints' section. On the left, a sidebar lists various settings: General, Advanced features, Licenses, Email notifications, Auto remediation, APIs, SIEM, Rules, Alert suppression, Indicators (which is selected), Web content filtering, Asset rule management, Configuration management, Enforcement scope, Device management, Onboarding, and Offboarding. The main pane displays the 'Indicators' tab, which lists IP addresses and their associated details. A summary at the bottom right indicates a connection was blocked by an IT administrator.

IP address	Application	Action	Alert severity	Scope	Expires on (UTC)
4.227.186.72		Block execution	High	All devices	
2001:0000:3238:dfe1:63:0000:0000:fefb		Warn	Not Applicable		
79.170.44.215		Block execution	Informational	All devices	
1.1.1.1		Block execution	High	All devices	
184.168.131.241		Block execution	Medium	chircho-test	
2.2.2.2		Allow	Not Applicable	All devices	

Virus & threat protection
Connection blocked
Your IT administrator caused Microsoft Defender Security Center to block this network connection. Contact your IT help desk.

Endpoint detection & response

Detect and investigate advanced persistent attacks



Correlated behavioral alerts



Investigation and hunting over six months of data



Rich set of response actions

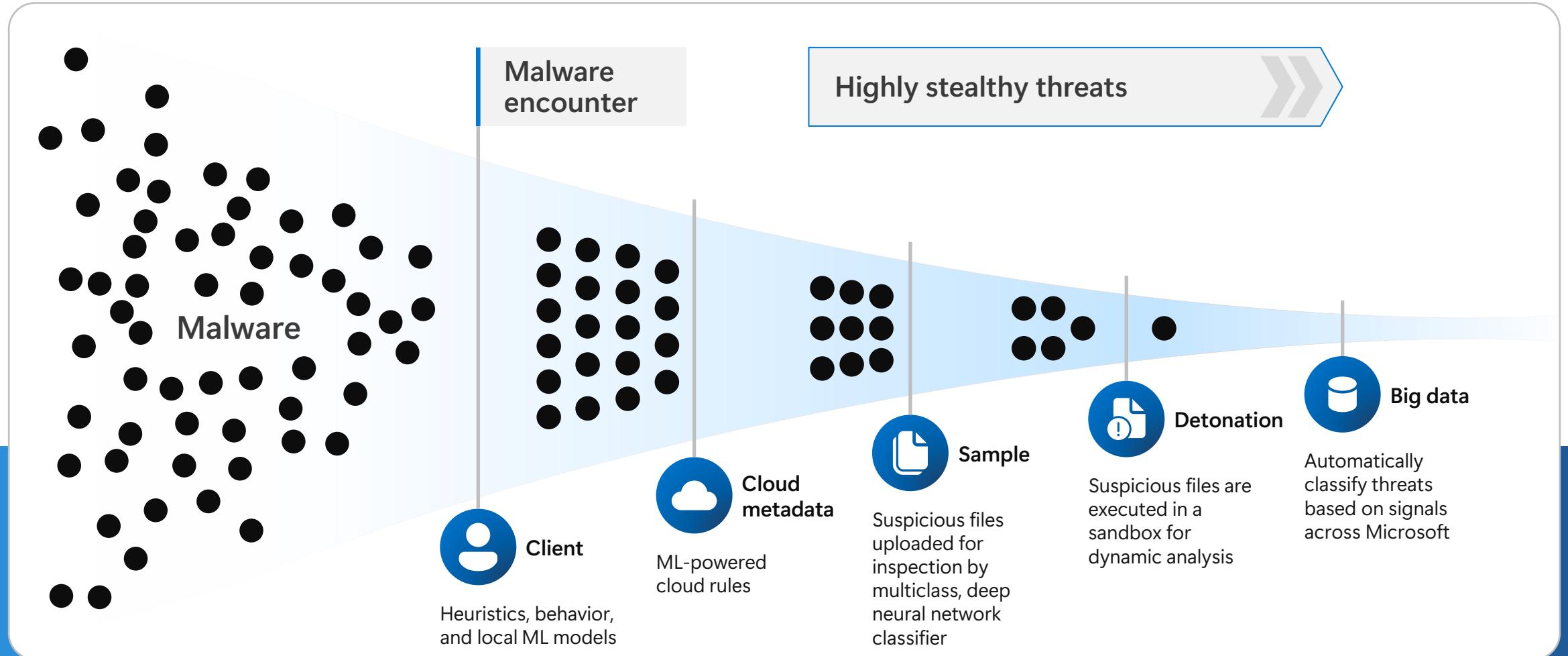


Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation

The screenshot shows the Microsoft 365 Defender Incidents page. The page title is "Incidents - Microsoft 365 security" and the URL is "https://security.microsoft.com". The main heading is "Incidents" with a subtitle "Most recent incidents and alerts". Below this is a table with columns: Incident name, Incident Id, Tags, Severity, Investigation state, Categories, Impacted assets, and Active. The table lists various incidents, such as "Multi-stage incident on multiple endpoints" (Incident Id 45367, Tags: BLAKEMO, Severity: High), "SensitiveFilesDiscovery" (Incident Id 50752, Tags: aamaini-np-test, Severity: Medium), and "Attempt to stop Microsoft Defender for Endpoint" (Incident Id 53279, Tags: aamaini-np-test, Severity: Medium). The table also includes filters for Status: New, Severity: High, and Service sources: EDR.

Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active
Multi-stage incident on multiple endpoints	45367	aamaini-np-test, BLAKEMO	High	2 investigation states	Persistence, Malware	20 Hosts, 12 Accounts	73/73
'SensitiveFilesDiscovery' detected on multiple endpoints	50752	aamaini-np-test	Medium	Unsupported OS	Exfiltration, Malware, Persistence	3 Hosts, azureuser	71/71
Attempt to stop Microsoft Defender for Endpoint	53279	aamaini-np-test	Medium	Partially investigated	Defense evasion	desktop-7vb403o, dipinternaluser	1/1
Suspicious launchctl tool activity on one endpoint	53868	aamaini-np-test	Medium	Unsupported OS	Execution	amigroot2s-Mac	1/1
Suspicious launchctl tool activity on one endpoint	53846	aamaini-np-test	Medium	Unsupported OS	Execution	Mac	1/1
Multi-stage incident involving Defense evasion	53297	aamaini-np-test	Medium	Unsupported alert type	Defense evasion, Discovery	mariyah-simcon1, TDPUser	2/2
Suspicious launchctl tool activity on one endpoint	53286	aamaini-np-test	Medium	Unsupported OS	Execution	Mac	1/1
Multi-stage incident involving Execution & Exfiltration	51560	aamaini-np-test	Medium	2 investigation states	Execution, Defense evasion	desktop-htae58, 2 Accounts	25/25
Possible exfiltration of archived data on one endpoint	50910	aamaini-np-test	Medium	Unsupported OS	Exfiltration	gargank-rhel82-asm-cli.voon2wwututjamf	2/2
Multi-stage incident including Ransomware on one endpoint	50073	Ransomware	High	Unsupported alert type	Discovery, Ransomware	DESKTOP-NO1GOOG, Blake	4/4
Multi-stage incident involving Initial access & Command and Control	47735	Ransomware, BLAKEMO	High	Unsupported alert type	Initial access, Command and Control	BLAKEMOWIN10VM, Blake	6/6
Suspicious launchctl tool activity on one endpoint	47773	aamaini-np-test	Medium	Unsupported OS	Execution	Mac	2/2
Multi-stage incident on one endpoint	48759	aamaini-np-test	High	Unsupported OS	Initial access, Malware	Mac	8/8
Multi-stage incident involving Execution & Late Bind	47719	aamaini-np-test	High	Unsupported alert type	Execution, Defense evasion	main0208x64, TDPUser	5/5
Suspicious client communication on one endpoint	47624	Telemetry spoofing	Medium	Unsupported alert type	Suspicious activity	desktop-460973	1/1
Microsoft Defender Antivirus protection turned off	47615	aamaini-np-test	Medium	Unsupported alert type	Defense evasion	main0208x64	1/1
Multi-stage incident involving Credential access	45599	Telemetry spoofing	Medium	3 investigation states	Credential access, Exfiltration	2 Hosts, 2 Accounts	674/674

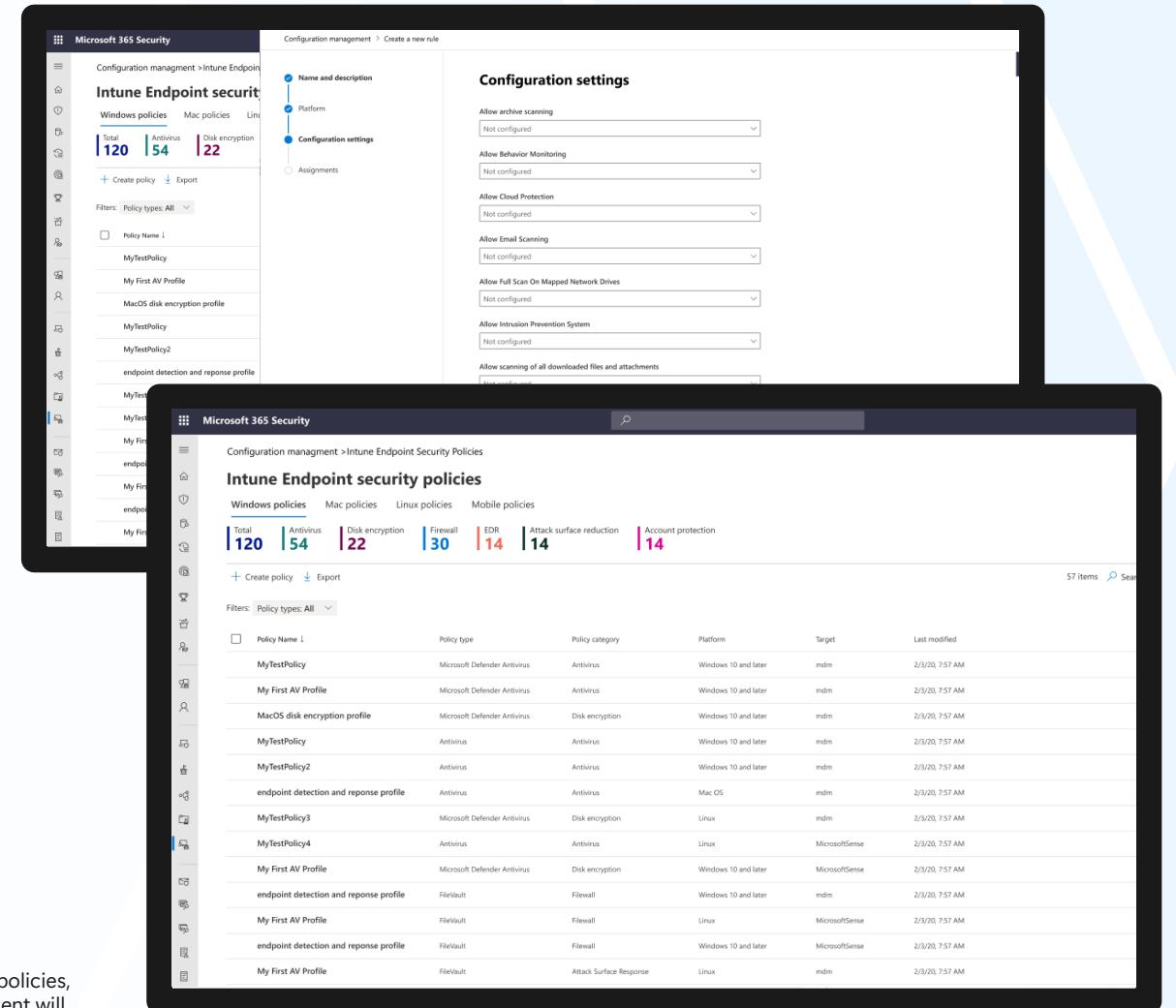
Microsoft Defender for Endpoint's NGP protection pipeline



Security settings management

Manage all security settings natively from Defender for Endpoint

- » **Use a single portal** to manage all security settings across your devices
- » **Secure your multiplatform enterprise seamlessly** with native support for Windows, macOS and Linux devices
- » **Enroll your devices with ease** using a simplified management experience that removed identify-based requirements
- » **Streamline policy management** by creating, modifying, and pushing policies directly from the Defender portal.
- » **Operate security and IT in lockstep** with a single source of truth for endpoint settings and policy management



Note: Only Microsoft Intune endpoint security policies will populate in the Defender portal. Mobile device policies, SCCM policies, GPO policies, manually configured policies (PowerShell scripts, etc.) and policies from third-party Mobile Device Management will not populate in the portal.

Endpoint security policies

Use security policies to manage security settings on devices.

Antivirus

Manage antivirus settings for devices.

Disk Encryption

Focus on settings for built-in encryption (BitLocker, FileVault).

Firewall

Configure built-in firewalls for macOS and Windows 10/11 devices.

Endpoint Detection and Response (EDR)

Manage EDR settings and onboard devices to Microsoft Defender for Endpoint.

Attack Surface Reduction

Manage settings for reducing attack surfaces on Windows 10/11 devices.

The screenshot shows the Microsoft 365 Defender portal interface. On the left, there is a navigation sidebar with various options like Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management, Dashboard, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, and Attack simulation training. The 'Endpoint security policies' option is highlighted with a red box. The main content area is titled 'Endpoint Security Policies' and shows a table of policies categorized by platform: Windows policies, Mac policies, and Linux policies. The 'Windows policies' tab is selected. The table includes columns for Policy Name, Policy type, Policy category, Assigned, and Platform. The data in the table is as follows:

Policy Name	Policy type	Policy category	Assigned	Platform
[Redacted]	Windows Security Experience	Antivirus	false	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	true	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	false	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	true	windows10
[Redacted]	Attack Surface Reduction Rules	Attack surface redu...	true	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	false	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	true	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	true	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	true	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	false	windows10
[Redacted]	Attack Surface Reduction Rules	Attack surface redu...	true	windows10
[Redacted]	Microsoft Defender Antivirus	Antivirus	false	windows10
[Redacted]	Windows Security Experience	Antivirus	false	windows10
[Redacted]	Attack Surface Reduction Rules	Attack surface redu...	false	windows10

Vulnerability management

A risk-based approach to prioritize and remediate your vulnerabilities



Continuous real-time discovery

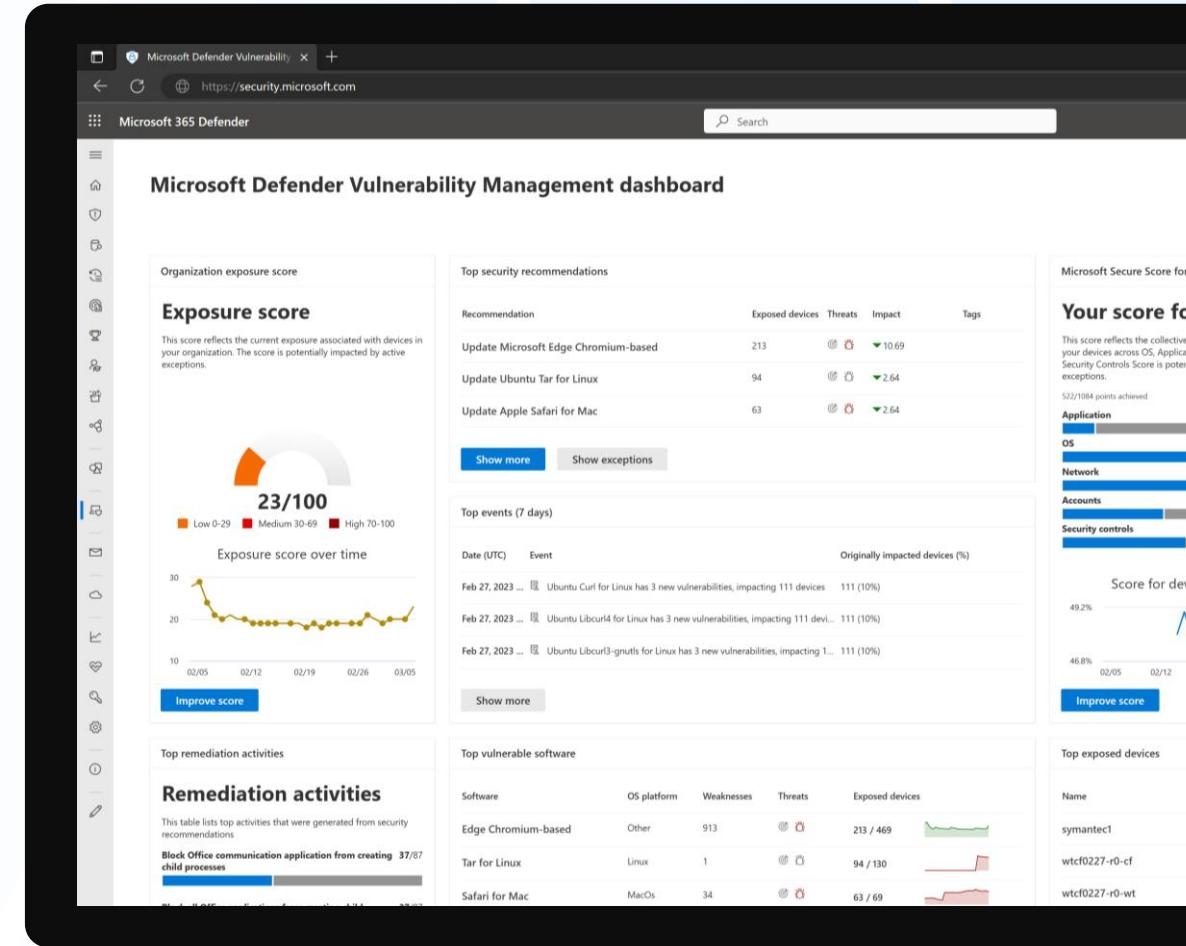


Context-aware prioritization



Built-in end-to-end remediation process

Powered by [Microsoft Defender Vulnerability Management \(core\)](#)



Incident Management and Response

End-to-end attack story

Reconstructing the story

The broader attack story is better described when relevant alerts and related entities are brought together

Incident scope

Analysts receive better perspective on the purview of complex threats containing multiple entities

Higher fidelity, lower noise

Effectively reduces the load and effort required to investigate and respond to attacks



For more details click [here](#).

The screenshot displays the Microsoft 365 Defender interface for managing incidents. At the top, a navigation bar includes 'Microsoft 365 Defender', 'Incidents', 'Alerts', 'Assets', 'Investigations', 'Evidence and Response (187)', and 'Summary'. The main area shows a list of incidents under the heading 'Most recent incidents and alerts'. One incident is expanded, titled 'Multi-stage incident on multiple endpoints' (ID: 45367), which details 73/73 active alerts, 1 MITRE ATT&CK tactics, and 1 other alert categories. Below this, a timeline shows suspicious connections from 'ubuntu01' and 'Venturas-Mac-3'. To the right, a detailed view of the incident information is shown, including sections for 'Scope' (20 impacted devices, 12 impacted users), 'Top impacted entities', and 'Evidence' (187 entities found). A sidebar on the right provides additional details like 'Incident Information', 'Tags summary', and 'Incident tags'.

Get rich reporting in Microsoft Defender for Endpoint

Microsoft 365 Defender

Search

Devices

ASR rule detections

0

07/11 07/14 07/17 07/20 07/23 07/26 07/29 08/01 08/04 08/07 08/10

Blocked

You have no ASR rule detections yet.

View detections Add exclusions

ASR rule configuration

99% of devices don't use standard protection

Deploy standard attack surface reduction (ASR) rules to proactively stop common attacks.

Block credential stealing from the Windows local security database

Block persistence through WMI event subscription

Block abuse of exploited vulnerable signed drivers

Protect devices

97% of devices are not blocking detections

Set ASR rules to block detections for better protection.

Block Win32 API calls from Office macro

Block all Office applications from creating child processes

Block JavaScript or VBScript from launching download...

Block process creations originating from PSExec and ...

Block Office applications from creating executable con...

Block Office applications from injecting code into othe...

Block mode Audit mode Warn Off Unknown Not Applicable

View configuration Add exclusions

Threat analytics

255 threats require action

High-impact threats

Threat overview: Exfiltration 4,874 / 4,922

Technique profile: Antivirus tampering 3,207 / 3,245

Active Alerts Resolved Alerts No Alerts

Highest exposure threats

Actor profile: Malware distributor Storm-0324 facilitated by 6

Actor profile: Storm-0241 6

High 70-100 Medium 30-69 Low 0-29

See more

Device compliance

83% noncompliant

Intune device compliance status

Compliant Noncompliant In grace period Not evaluated

View details

Devices with active malware

2 affected device(s)

Applies to Intune-managed devices. Devices with multiple malware detections may be counted more than once.

Updated Today at 8:41 AM

Active Malware remediated

View details

Types of malware on devices

Detections on Intune-managed devices

EnterpriseUnwantedSoftware 2

Malware on devices

Detections on Intune-managed devices

Malware name

EUS:Win32/Custom

EUS:Win32/CustomEnterpriseBlock

Trojan:Win32/Occamy.C7D

Virus:DOS/EICAR Test File

Devices with malware detections

Intune-managed devices with the most detections

Device	Detections
WebsiteDLP2	2
DESKTOP	1
DLP_AM	1
DLP_AM_WDATP_12	1

Users with malware detections

Users with the most detections on Intune-managed devices

User	Detections
DLPIInternal User	2
Tewang	2
Deepti	1

Detect & Respond: Cloud App Security



InPrivate Mail - admin@iddemo.onm... Manage advanced alerts - S Policy templates - Office X + ⌂

Cloud App Security Discover Investigate Control Alerts Protect more cloud apps Microsoft

Policy templates

TYPE	SEVERITY	NAME	CATEGORY	Advanced
Select type...	Yellow	Template name...	Select risk category...	

1 - 17 of 17 Templates

Template	Severity	Linked policies	Published	
New popular app Alert when new apps are discovered that are used by more than 500 users.	Red	0	Sep 17, 2017, 2:05 AM	+
Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.	Red	0	Sep 17, 2017, 2:05 AM	+
General anomaly detection Alert when an anomalous session is detected in one of the sanctioned apps, such as: impossible travel, log on pattern, inactive account.	Red	0	Sep 17, 2017, 2:05 AM	+
New high upload volume app Alert when new apps are discovered whose total daily upload traffic is more than 500 MB.	Red	0	Sep 17, 2017, 2:05 AM	+
Mass download by a single user Alert when a single user performs more than 50 downloads within 1 minute.	Red	0	Sep 17, 2017, 2:05 AM	+
New high volume app Alert when new apps are discovered that have total daily traffic of more than 500 MB.	Red	0	Sep 17, 2017, 2:05 AM	+
Logon from a risky IP address Alert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky IP	Red	0	Sep 17, 2017, 2:05 AM	+



MONITOR CLOUD APP USAGE

Advanced incident investigation tools

Investigate on users, file, activities, locations and managed apps, quantify exposure and risk

Cloud data visibility

Identify how data – both classified and not classified – is shared across cloud apps and identify risk

Cloud app risk assessment

Assess risk cloud apps based on ~60 security and compliance risk factors.

On-going analytics & anomaly detection

Get anomalous usage alerts, new app and trending apps alerts

The dashboard displays the following key metrics:

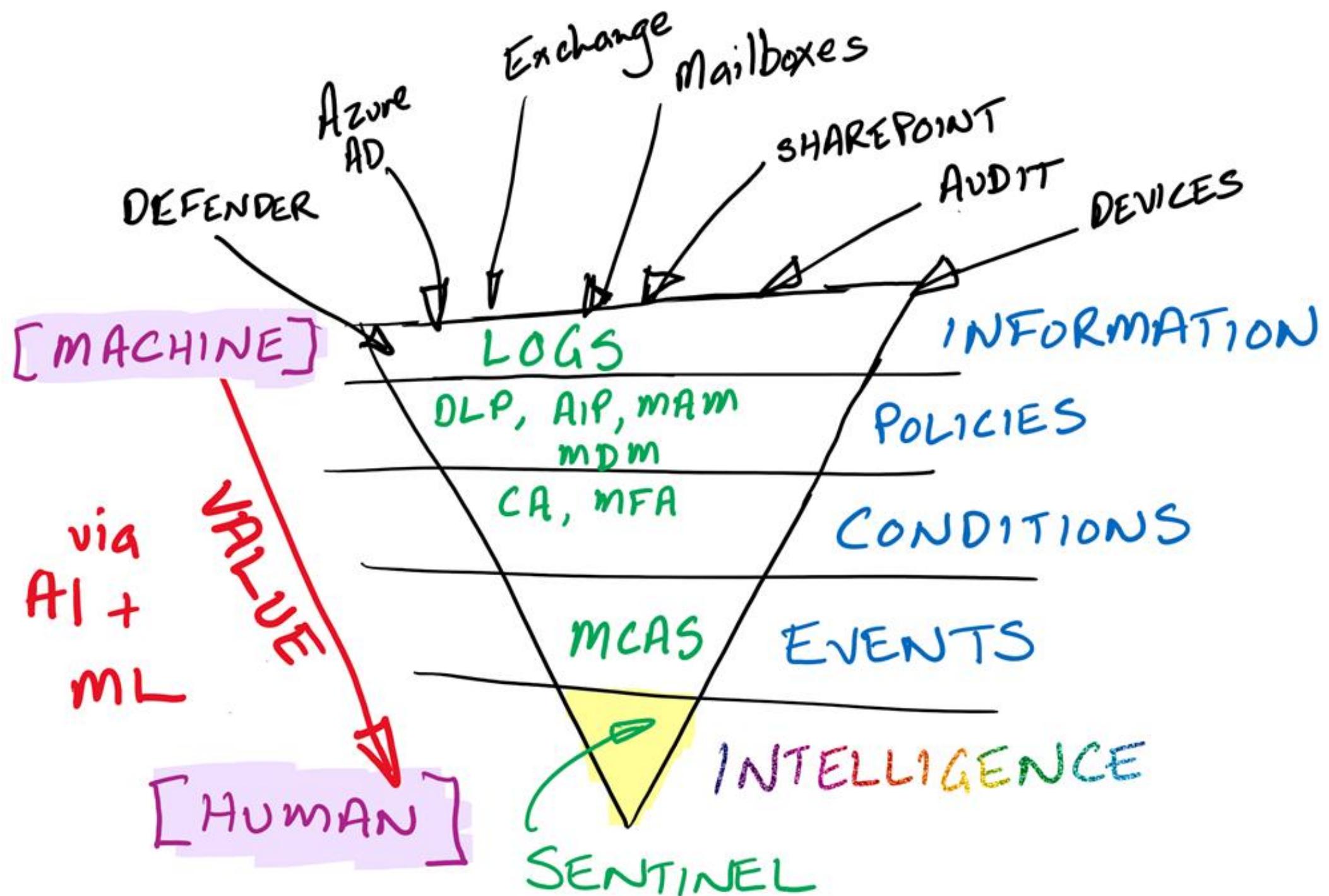
- Apps: 557
- Users: 1173
- IP addresses: 2540
- Traffic: 314.4 GB (60.4 GB Sanctioned, 232.5 GB Unsanctioned)

The 'Risk levels' section shows a total traffic volume of 314.4 GB.

The 'Files' section lists the following files:

File Name	Owner	Access Level	File Type	Last Modified
TeamNotebook(Shared)	MOD Administrator	Microsoft OneDrive for Bus...	Box	Apr 18, 2017
TeamNotebook(Shared).onetoc2	MOD Administrator	Microsoft OneDrive for Bus...	Box	Apr 18, 2017
Notebooks	MOD Administrator	Microsoft OneDrive for Bus...	Box	Apr 18, 2017
Attachments	MOD Administrator	Microsoft OneDrive for Bus...	Box	Apr 18, 2017
Screen Shot 2017-03-14 at 7:00:21 AM.png QUARANTINE.txt	demo	Box	Box	Apr 12, 2017
Quarantine	demo	Box	Box	Apr 12, 2017
casdemo2017@outlook.com	demo	Box	Box	Apr 12, 2017

Intelligence vs Information



Introducing Microsoft Sentinel

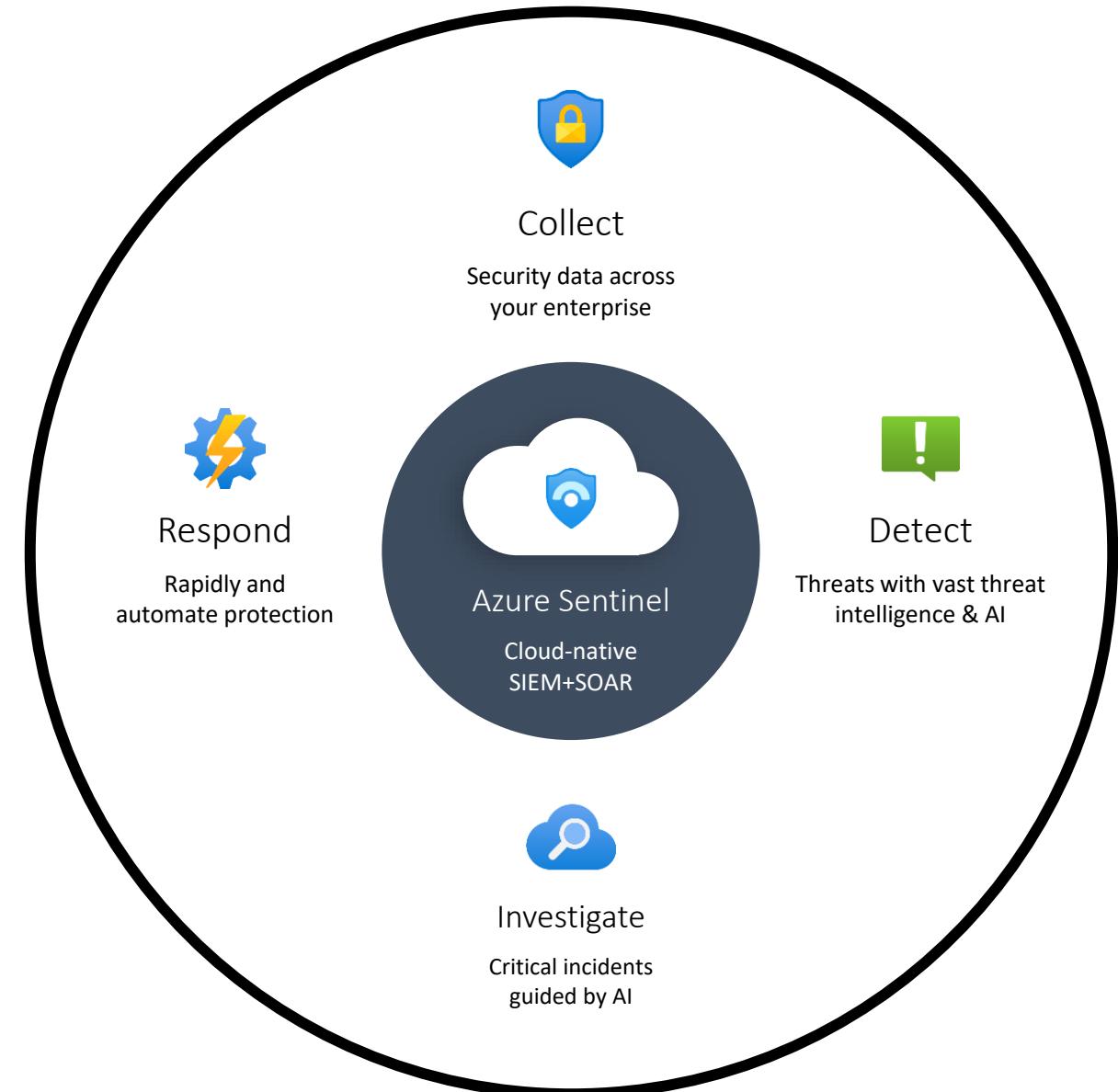
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your [Office 365 + M365 Alerts for Free](#)

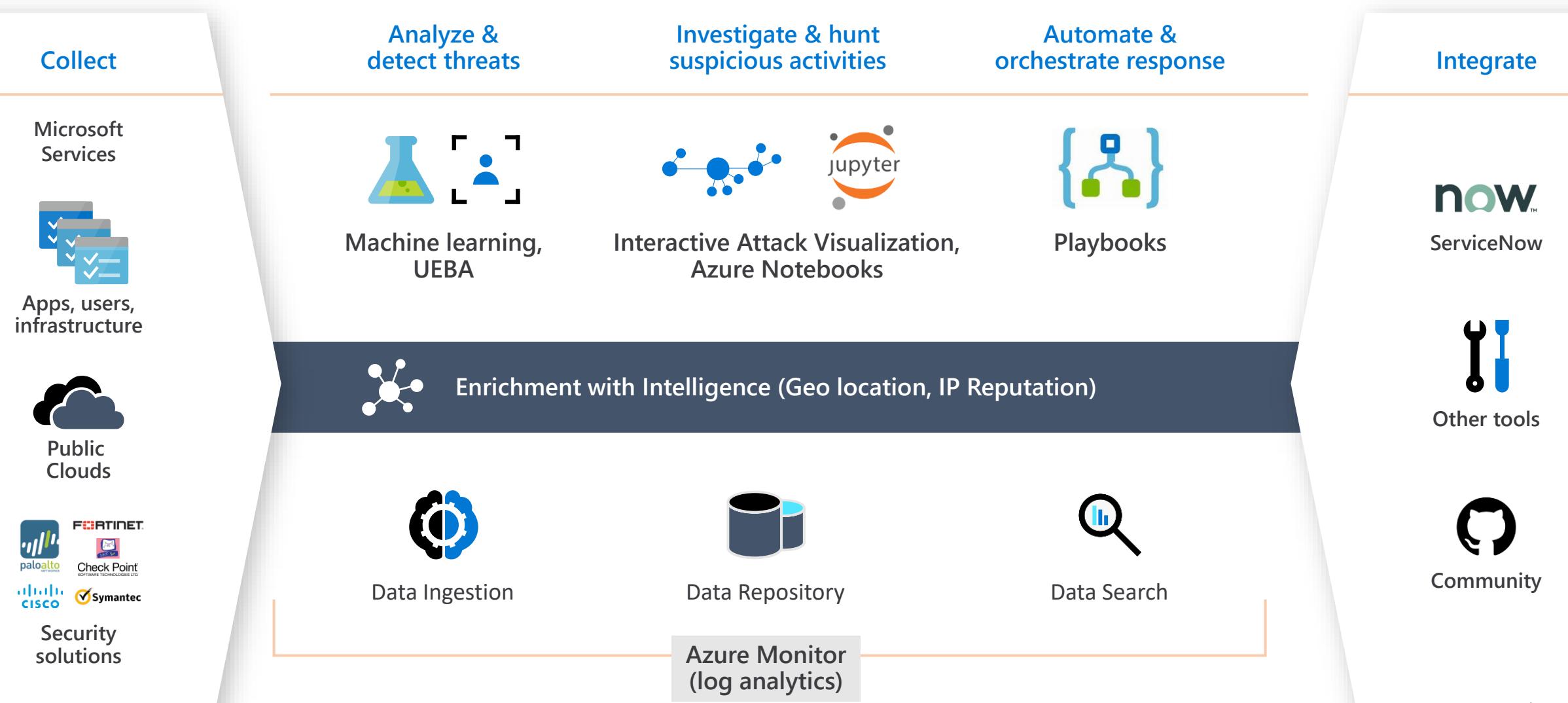
Easy integration with your [existing tools](#)

Faster threat protection with [AI by your side](#)





Core capabilities



Azure

And how it plays into the larger story...

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

**Proven log platform with more than
10 petabytes of daily ingestion**



Secure Data I: DLP & Sensitivity Labels



Securing Against Internal Threats

Reducing Risk Within Your Organization

Fortify Access
Identity & Access Management

Secure Internal Data
DLP & Sensitivity Labels

Shield Devices
Endpoint & Threat Protection



59 data security incidents experienced on average in the past year with **20%** of them being **severe**¹

Security and privacy are the top concerns for organizations to use generative AI tools²

1. Data Security Index, Microsoft, 2023

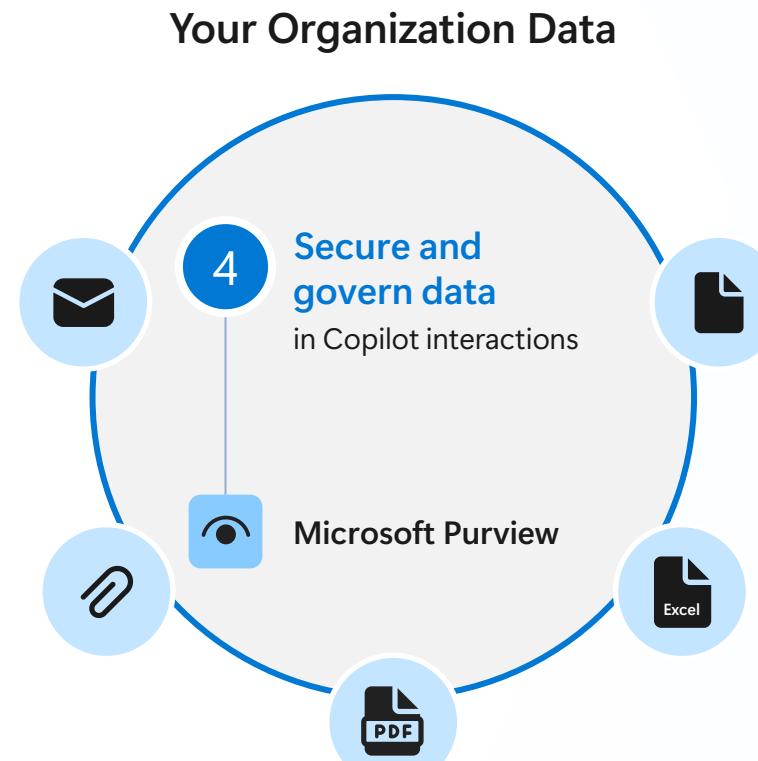
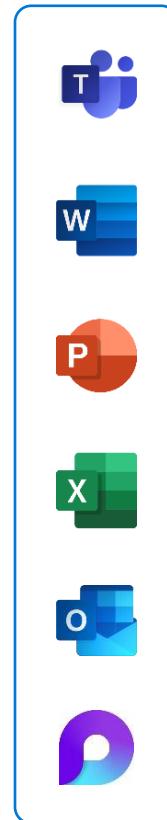
2. Security and privacy are the top concerns for organizations to use generative AI tools²

Secure and govern data in Copilot interactions

Microsoft Purview Information Protection P1



Microsoft 365
Copilot



- ✓ Data consumption and processing with Copilot is limited to the user's permissions
- ✓ Copilot respects sensitive documents' sensitivity labels
- ✓ If Copilot generates sensitive data and saves it in Microsoft 365, Data Loss Prevention policies will apply
- ✓ Interactions with Copilot are retained and logged for audits or search purposes. Detect business, or code of conduct violations
- ✓ Remove inactive data to reduce obsolete insights

Data security incidents can happen anytime, anywhere



Data at risk of misuse if organization has no visibility into their data estate

1

User falls prey to phishing attack,
compromises user credentials



Data compromise
by external threat

2

User copies file to a USB, then
uploads to a personal Dropbox



Data theft by
malicious insider

3

User negligently shares sensitive
data in generative AI apps



Data exposure by
negligent insider

Fortify data security with Microsoft Purview



Information Protection

- Discover, classify, and protect data at scale, using automation and ML
- Productivity tools with built-in user-selectable sensitivity labels for precise controls
- Data is protected (encrypted) across environments, throughout its lifecycle



Insider Risk Management

- Leverage analytics, machine learning, sequencing to understand user context and intent
- Investigate potential incidents with curated, high-quality, and enriched alerts and evidence
- Ensure user privacy while identifying highest risk users



Data Loss Prevention

- Prevent unauthorized use, like improperly saving, storing or printing sensitive data
- Create, deploy, and manage DLP policies across all cloud, apps, and devices from a single location
- Leverage data classification, labeling, and user insights to finetune and adapt DLP policies

Adaptive Protection

Dynamically adjust data security controls based on user risk level

Secure by Default with Microsoft Purview and Protect Against Oversharing



Foundational

Start with recommended labels

- Start with default labels and protection at file and site level.
- Turn on data security pre-requisites and advanced analytics.
- Train users on managing exceptions.
- Turn on DLP for labeled content.

M365 new/updated content protected

1 week



Managed

Address files with highest sensitivity

- Manually configure priority sites default library labeling.
- Auto labeling for credentials and contextual conditions.
- Turn on DLP for content that is not labeled.
- Turn on Adaptive Protection and data leak behavioral rules.

M365 priority content protected

2 week



Optimized

Expand to your entire M365 data estate

- Auto-label sensitive files on clients (low thresholds).
- Simulate auto-labeling sensitive files at rest.
- Reduce false positives with advanced classifiers.
- Automate and improve M365 protection to historical and in-use data.

M365 historical content protected

2 weeks iteration



Strategic

Operate, expand, and retroactive actions

- Operational review of user labeling behaviors.
- Iterate with new labeling scenarios.
- Set up accountability chain and lifecycle management.
- Extend protection to Azure SQL and non-M365 storage.

Protection beyond M365

Situational



Address internal oversharing concerns for M365 Copilot deployment

	Pilot	Deploy (at scale)	Operate
Activities	<ul style="list-style-type: none">Identify most popular sites & assess oversharingGrant Copilot access to popular, low risk sitesTurn on proactive audit and protection	<ul style="list-style-type: none">Discover oversharing risksRestrict sensitive info from Copilot access and/or processingIncrease site privacy	<ul style="list-style-type: none">Further reduce risk and simplify oversightFurther secure sensitive dataImprove Copilot responses
Outcomes	 Deploy copilot to sub-set of users with up to 100 sites	 Copilot fully deployed in your organization	 Continuous improvement of data security practices
Effort*	 2–4 days	 2–4 weeks	 More than one month

*Suggested efforts should be reviewed into timelines based on your tenant size and organizational complexity

Adaptive Protection in Microsoft Purview

Optimize data security automatically

Context-aware detection

Identify the most critical risks with ML-driven analysis of both content and user activities

Dynamic controls

Enforce effective controls on high-risk users while others maintain productivity

Automated mitigation

Minimize the impact of potential data security incidents and reduce admin overhead

Insider Risk Management

Detect risky users and assign risk levels



Elevated risk



Data Loss Prevention

Dynamically apply preventative controls

DLP Policy 1

Block



Moderate risk



DLP Policy 2

Block with override



Minor risk



DLP Policy 3

Policy tips

Data Loss Prevention

Prevent unauthorized use of data across apps, services, and devices



Cloud native

Cloud managed and delivered with **built-in protection** in Microsoft 365 apps, services, and Windows endpoints



Unified

Balance productivity and protection with **granular policy controls** and manage multi-scoped policies from a **single location**



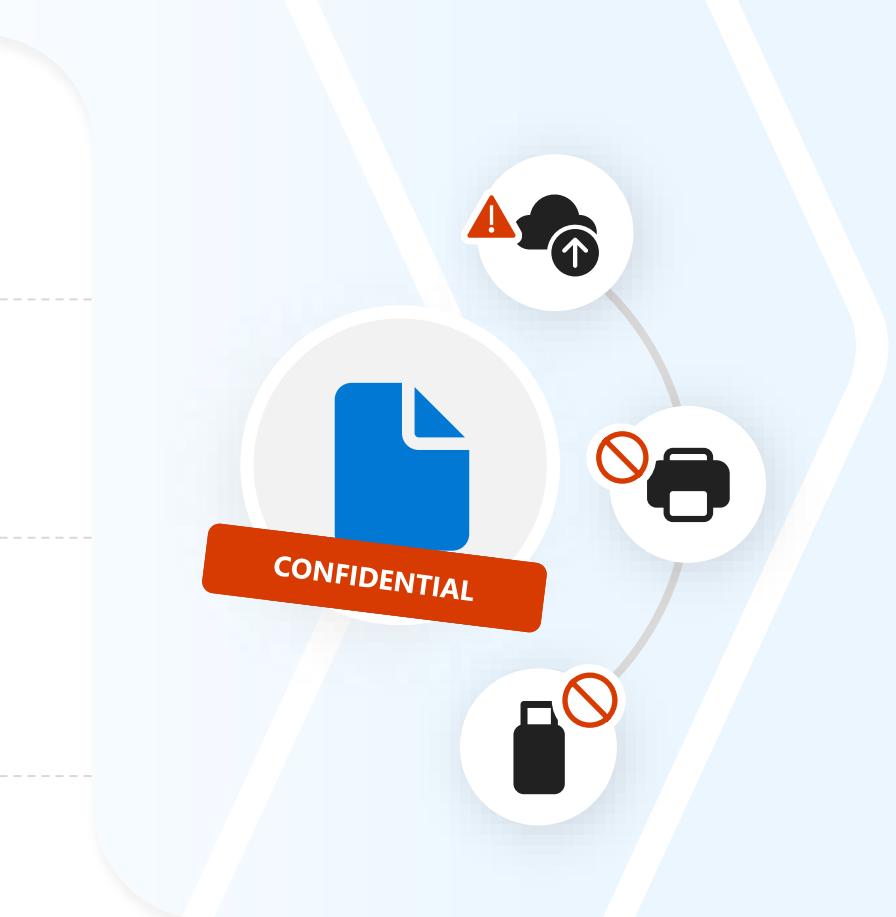
Integrated

Leverage **classification** and **user activity insights** to better inform DLP policies and benefit from **integrated incident management**



Easy

Get started quickly with **default policies** and **migration tool**



Data Loss Prevention



Cloud apps and services

- Exchange
- SharePoint
- OneDrive
- Teams
- PowerBI

Non-Microsoft applications:
Salesforce | Workday | Box | Dropbox

Devices

- Windows
- macOS
- Virtual environments: *Citrix | Windows Virtual Desktop | Hyper-V | Amazon workspaces*
- Network share location
- Removable storage
- Printers
- Service domains
- Browsers: *Chrome | Firefox | Edge*

Network

HTTP/HTTPS FTP/SFTP

Cloud native with built-in protection

Save cost and scale effectively

- Cloud managed and delivered, no on-premise infrastructure or agents needed
- Built-in experiences in Microsoft 365 apps and services, Windows endpoints, On-premises
- Extend protection to non-Microsoft applications and platforms

Data classification service

Sensitive Info Types (SITs)
Trainable Classifiers
Context-based Classification
Coming to Private Preview Jan 2023



Microsoft 365



Endpoints



Sensitivity Labels

Public
Confidential
General
...



Non-Microsoft apps



On-premises

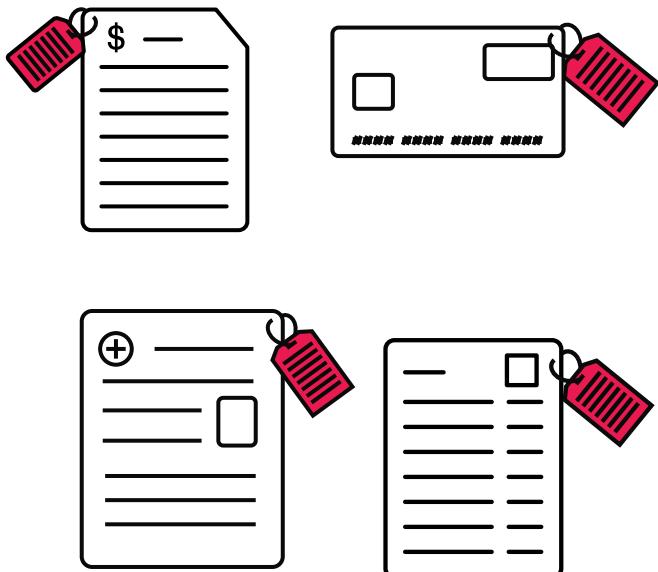


Integrated insights and alerting

Enrich policy and investigation with rich signals

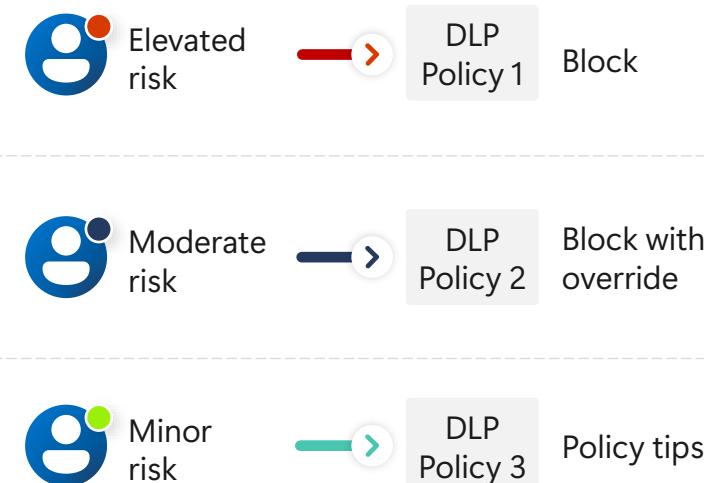
Know the context

Leverage classification and labeling on sensitive data from Information Protection



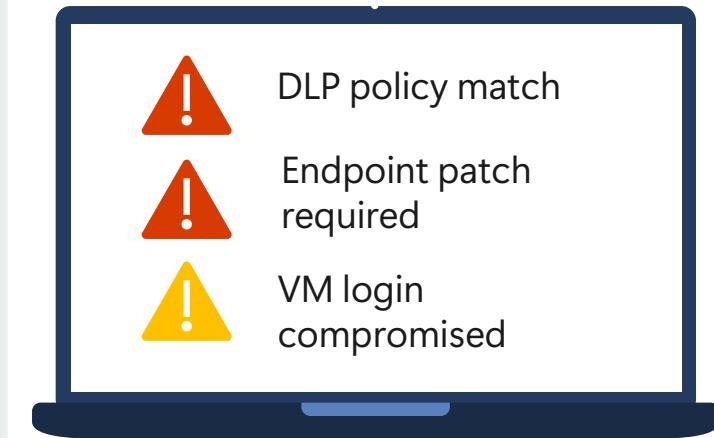
Understand the intent

Automatically apply risk insights from Insider Risk Management to DLP policies



Integrate alert investigation

Integrate DLP alerts with Microsoft Defender XDR and Sentinel for richer investigation experience



Shield Devices: Endpoint & Threat Protection



Securing Against Internal Threats

Reducing Risk Within Your Organization

Fortify Access

Identity & Access Management



Secure Internal Data

DLP & Sensitivity Labels



Shield Devices

Endpoint & Threat Protection



Microsoft Threat Intelligence is actively tracking more than **300 unique threat actors**, including more than 160 nation states and 50 ransomware actors.¹

The number of password attacks Microsoft has detected increased to more than **7,000 per second in 2024**, due to unmanaged devices.²

1. [Microsoft Security Blog 2024](#)

2. Microsoft Digital Defense Report 2024

Today | Imperatives for IT and security teams



Protect data and access to corporate resources.



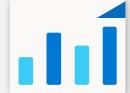
Adapt to evolving threats quickly.



Manage app updates and vulnerabilities.



Gain complete visibility and control.



Keep overhead and costs down.



Govern compliance protocols.

Cloud native is the definitive approach to modern endpoint management

Microsoft Intune

Cloud-native endpoint management enlightened by generative AI

Simplify and consolidate endpoint management

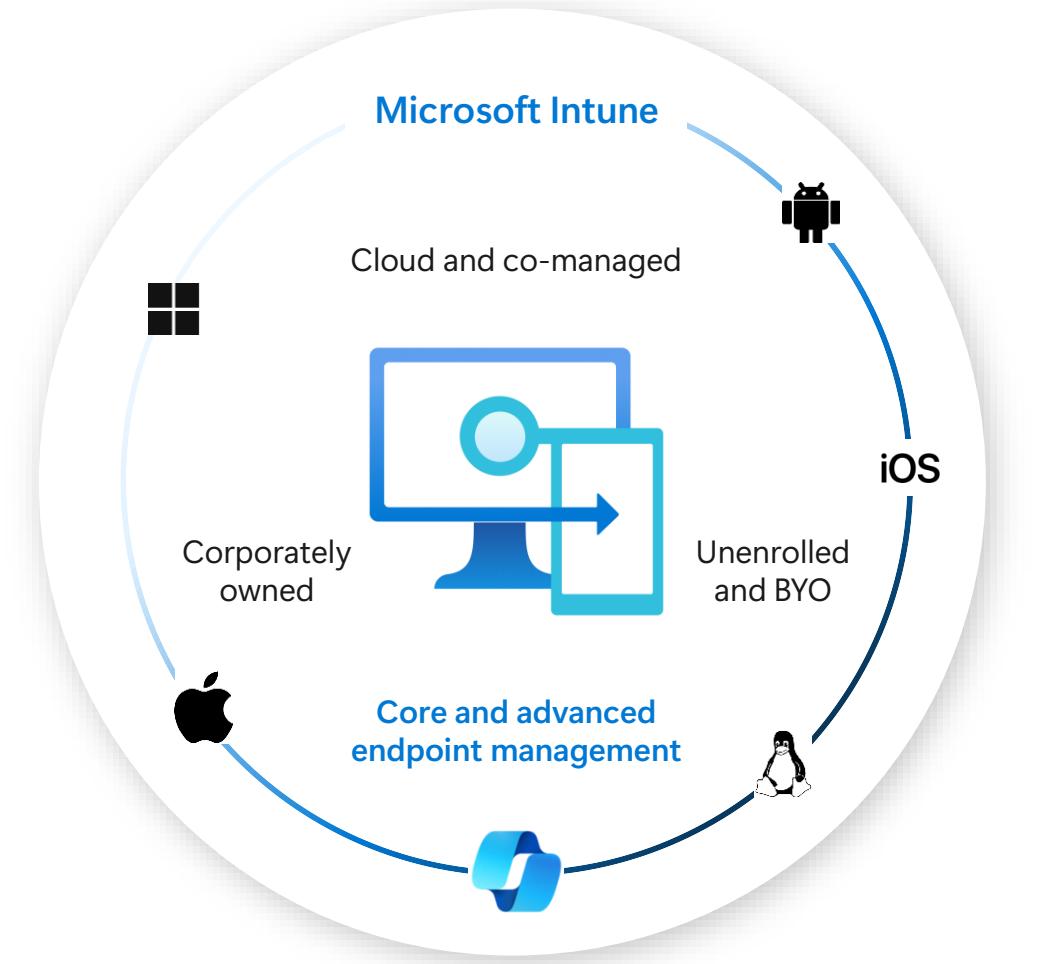
Cut cost and complexity by shifting to the cloud, unifying endpoint management and security tools in one place.

Fortify Zero Trust security

Mitigate threats and improve compliance across all devices by protecting users, devices, apps, and data.

Power better experiences

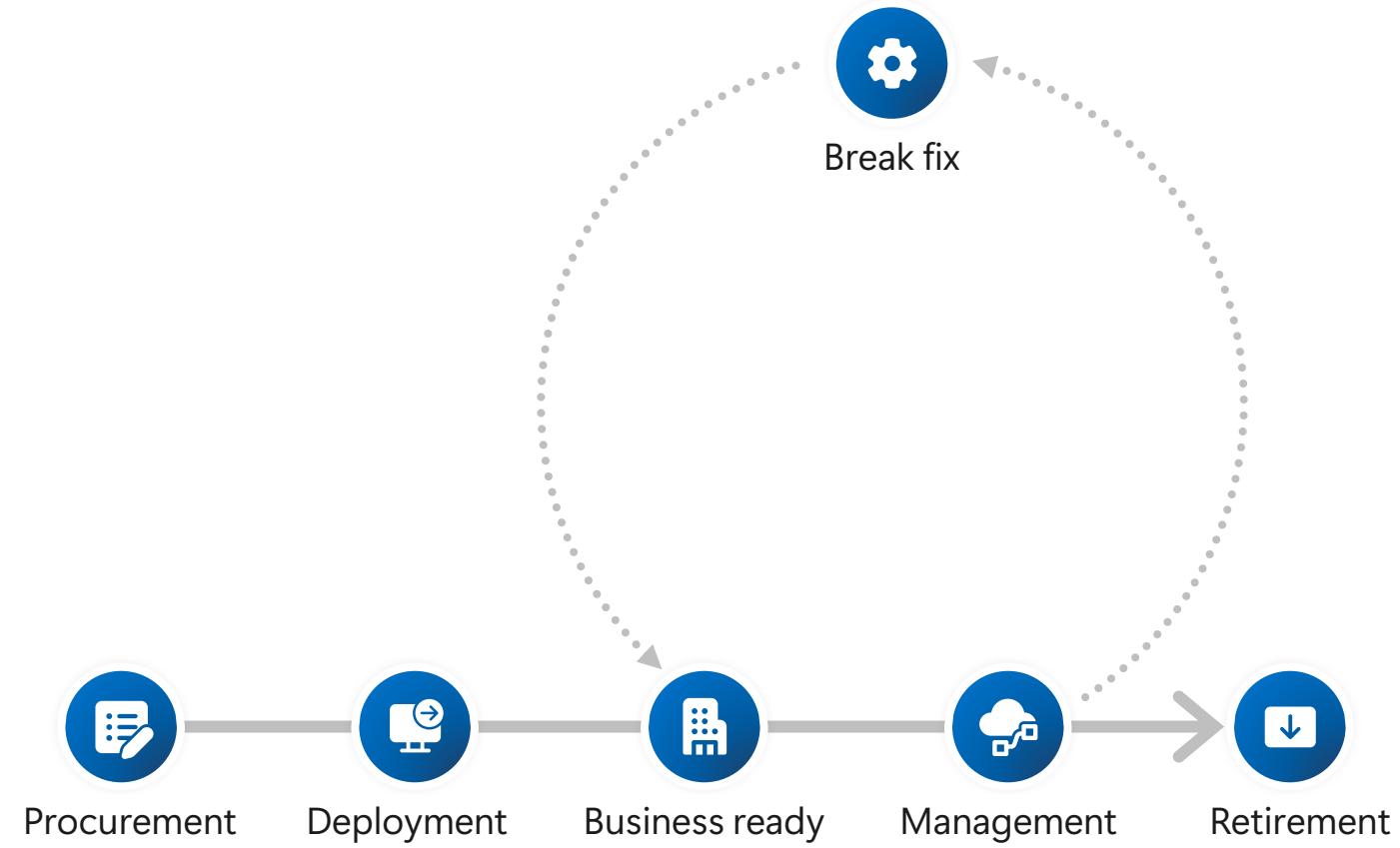
Proactively manage better user experiences while driving operational excellence with AI and automation.



Device lifecycle management with Windows Autopilot and Intune

Key Benefits:

- No more maintenance of images and drivers
- No need for IT to touch the devices
- Simple process for users and IT
- Integration in the device supply chain
- Reset device back to a business ready state



Automate Windows deployment using Autopilot



Drop-ship management-ready devices



Significant cost and time savings in OS deployment



Bypass traditional image-based deployment



Ongoing ability to do automated provisioning of apps, configurations and user settings



Easy new device experience for end-users

Learn more:

aka.ms/WinAutopilot >>



Enable remote desktop access with Azure Virtual Desktop



Deliver the only multi-session Windows 10 experience that's highly scalable and stays up to date



Enable optimizations for Office



Migrate RDS desktops and apps and simplify licensing and reduce costs



Deploy and scale in minutes. Manage with unified admin interface in Azure Portal



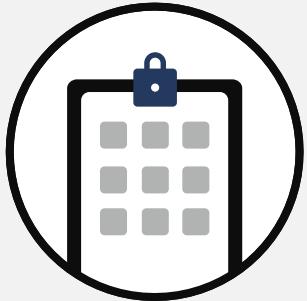
Support any end-user device platform including Windows, Android, Mac, iOS, and HTML 5

Learn more:

aka.ms/AzureVD >>



Manage work data on mobile devices with Microsoft Intune



Mobile Device Management (MDM)

Conditional Access:
Manage access to company owned devices



Enroll devices for management



Provision settings, certs, profiles



Report and measure device compliance



Remove corporate data from devices remotely



Mobile Application Management (MAM)

Conditional Access:
Manage which apps can be used to access work email or files on personal devices



Publish mobile apps to users



Configure and update apps



Enforce that work data cannot be saved on personal apps



Secure and remove corporate data within mobile apps

Learn more:

<https://Aka.ms/IntuneLearn>



Example: Managing work data on personal devices

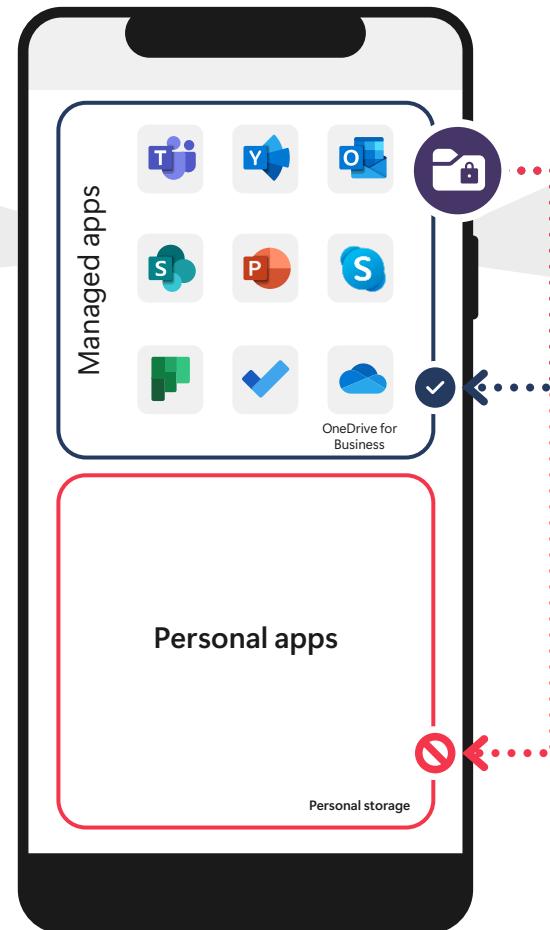
MAM policy to secure work data



Corporate data



Personal data



Email attachment



OneDrive for Business



Copy



Paste to personal app



Save to personal storage



Save

Microsoft Intune empowers you to specify access controls for work data

Separate company managed apps from personal apps, and set policies on how work data is accessed from managed apps

Intune app helps ensure corporate data can't be copied and pasted to personal apps within the device

Handling Oversharing





Oversharing Agenda

- 1 Intro to Oversharing
- 2 Oversharing Blueprint
- 3 Restricted SharePoint Search (Temporary)
- 4 SharePoint Advanced Management (SAM)
- 5 Microsoft Purview



Oversharing Agenda

1

Intro to Oversharing

2

Oversharing Blueprint

3

Restricted SharePoint Search (Temporary)

4

SharePoint Advanced Management (SAM)

5

Microsoft Purview



Search



Work

Web



Copilot

To get started, try one of the suggested prompts, type your own, or just select the content you want to work with.

All

People

Files

Meetings

Emails

Prompts



Help me learn about
topic

Draft email notes for
meeting

Help me improve my
writing based on file

View prompts

Are there any ORG changes happening next month?

Add content

|



Search



Work Web



11:10 AM

Are there any ORG changes happening next month

Home

Copilot

Create

OneDrive

Feed

Pages

Apps

Yes, there are some organizational changes happening next month. Here are a few updates:

1. **BWS Organizational Update:** Kristin Patterson has joined the BWS leadership team to lead the Customer Voice & Health Team. Kadji Bell will transition manager responsibilities to Kristen and take on a critical IC role focused on the execution of the center of excellence, change management, and scaling processes. This change will be effective from August 26 [1](#).
2. **Changes to the BWS Design team:** Mona Kane, Ray Tanaka, and Sarah Evans will move to Sarah Perez's team. Mona will report directly to Sarah, and Ray and Sarah will report to Robyn. Sara Kiani will remain in BWGD and will report to Robin Counts' team. This change is effective immediately [2](#).
3. **Confidential Q2 CY24 ReOrg:** There are org changes coming up on September 4th based on this report [3](#) [4](#).

1

[BWS Org Update](#)

2

[Changes to the BWS D...](#)

3

[Confidential Q2 CY...](#)

+1

[Copy](#)[Share](#)

1

of 20 responses

AI-generated content may be incorrect

[View prompts](#)

Are there any ORG changes happening next month?

[Add content](#)



Search



Work

Web



11:10 AM

Are there any ORG changes happening next month

Yes, there are some organizational changes happening next month. Here are a few updates:

1. **BWS Organizational Update:** Kristin Patterson has joined the BWS leadership team to lead the Customer Voice & Health Team. Kadji Bell will transition manager responsibilities to Kristen and take on a critical IC role focused on the execution of the center of excellence, change management, and scaling processes. This change will be effective from August 26 [1](#).
2. **Changes to the BWS Design team:** Mona Kane, Ray Tanaka, and Sarah Evans will move to Sarah Perez's team. Mona will report directly to Sarah, and Ray and Sarah will report to Robyn. Sara Kiani will remain in BWGD and will report to Robin Counts' team. This change is effective immediately [2](#).
3. **Confidential Q2 CY24 ReOrg:** There are org changes coming up on September 4th based on this report [3](#) [4](#).

[1](#) BWS Org Update[2](#) Changes to the BWS D...[3](#) Confidential Q2 CY...[+1](#)

Copy

Share



1 of 20 responses

AI-generated content may be incorrect



View prompts

Are there any ORG changes happening next month?

Add content



How Copilot gets access to content

Copilot retrieves only the information you have access to

The process is called “retrieval augmented generation”

1

You submit a prompt

2

Orchestrator determines what it needs to answer the prompt

3

Orchestrator uses Graph to find relevant info you **are allowed to access**

4

Orchestrator appends info to your prompt to enhance it

5

LLM uses additional that information to generate a response

Internal oversharing: Too much access and too few controls

1

Over-permissioning too much internal access

Bias towards overly broad access
for permissions and links

2

Under-enforcement too few internal controls

Content looks the same without
labeling and content-aware policies
to follow its use

Implications

Risk of exposure in search and AI tools

| Hard to get started with AI and solve without the right tools

Oversharing is a biproduct of collaboration

Individual user permissions



Exchange mailbox



Teams chats



OneDrive for Business

Group based permissions



Teams channels

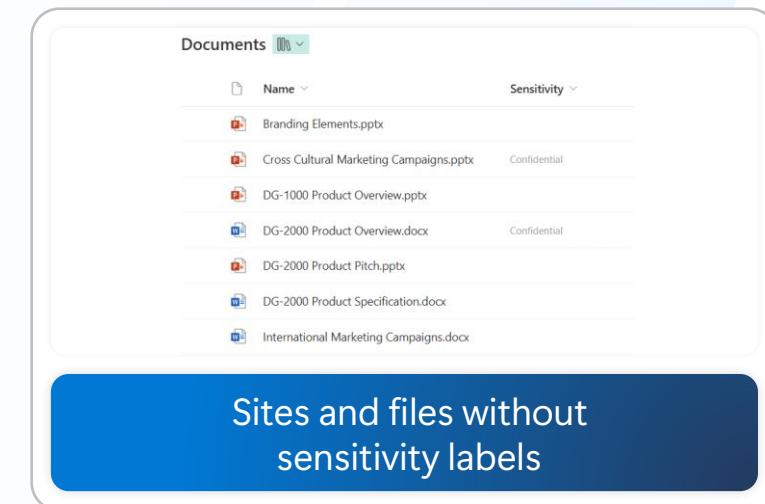
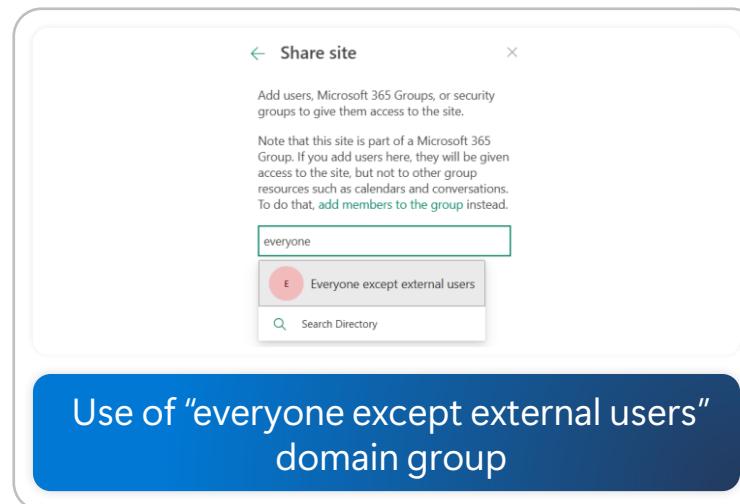
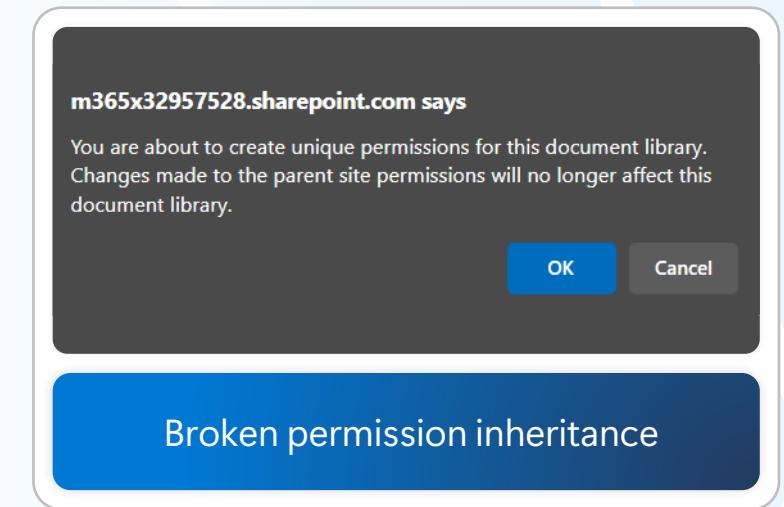
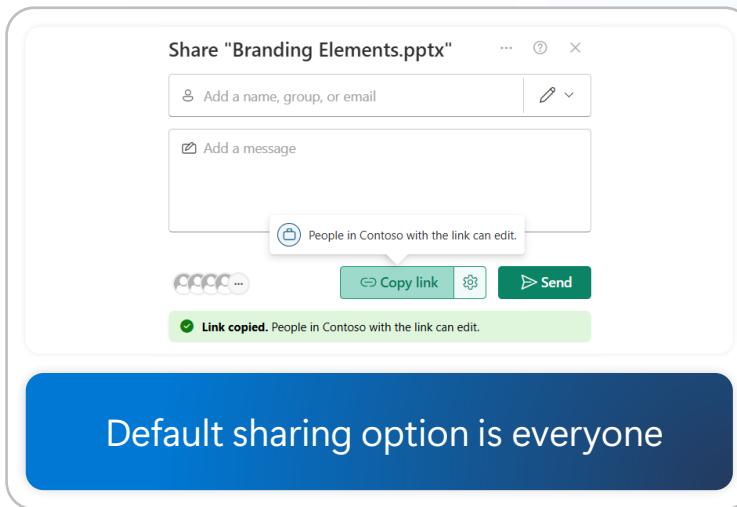
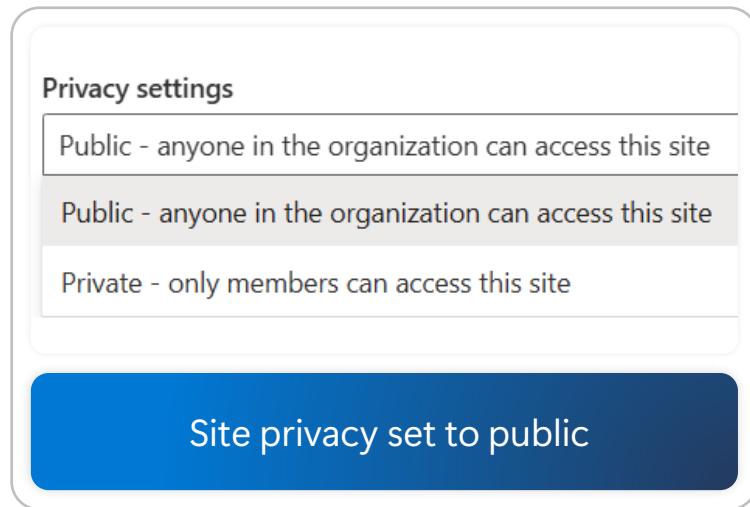


SharePoint sites

Option to share more broadly via link

Highest risk of oversharing in Microsoft 365 Copilot

Common causes of Copilot oversharing in SharePoint



Two powerful tools to oversharing



Microsoft 365 Copilot

Now powered by SharePoint Advanced Management

Provides SharePoint site management and content governance capabilities



Microsoft Purview

Provides security, compliance, and governance across data and files



Oversharing Agenda

1

Intro to Oversharing

2

Oversharing Blueprint

3

Restricted SharePoint Search (Temporary)

4

SharePoint Advanced Management (SAM)

5

Microsoft Purview

Microsoft deployment blueprint to address internal oversharing in Microsoft 365 Copilot

Customers with E3 or Business Premium Foundational

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2-4 days	2-4 weeks	1+ months
Deployment steps	<ul style="list-style-type: none"> Identify the most popular sites & assess oversharing Grant Copilot access to popular, low risk sites Turn on proactive audit and protection 	<ul style="list-style-type: none"> Discover oversharing risks Restrict sensitive info from Copilot access and/or processing Increase site privacy Further secure sensitive data Improve Copilot responses 	<ul style="list-style-type: none"> Further reduce risk and simplify oversight Discover oversharing risks Restrict sensitive info from Copilot access and/or processing Increase site privacy Turn on proactive audit and protection Further secure sensitive data Improve Copilot responses

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel
Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: <https://aka.ms/E3PrepareYourDataForCopilot>

Customers with E5 Optimized

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2-4 days	2-4 weeks	1+ months
Deployment steps	<ul style="list-style-type: none"> Identify the most popular sites & assess oversharing Grant Copilot access to popular, low risk sites Turn on proactive audit and protection 	<ul style="list-style-type: none"> Discover oversharing risks Restrict sensitive info from Copilot access and/or processing Increase site privacy Further secure sensitive data Improve Copilot responses 	<ul style="list-style-type: none"> Further reduce risk and simplify oversight Discover oversharing risks Restrict sensitive info from Copilot access and/or processing Increase site privacy Turn on proactive audit and protection Further secure sensitive data Improve Copilot responses

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel
Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: <https://aka.ms/E3PrepareYourDataForCopilot>

Get the blueprint:
<https://aka.ms/Copilot/OversharingBlueprintLearn>

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	<p>1. Identify the most popular sites & assess oversharing</p> <ul style="list-style-type: none"> Export the top 100 most used sites from SPO admin center Run SAM permission state report¹ Use Purview Content Explorer to view which sites contain sensitive information types (SITs)² <p>2. Grant Copilot access to popular, low risk sites</p> <ul style="list-style-type: none"> Cross reference the report results from SAM and Content Explorer with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery^{1,2} Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified¹ <p>3. Turn on proactive audit and protection</p> <ul style="list-style-type: none"> Turn Off EEEU (everyone except external users) at the tenant level² Turn on Audit and view Copilot interaction activity reports and charts^{1,2} Turn on audit-mode oversharing SPO DLP policy to detect anyone sharing links for labeled and unlabeled data² 	<p>1. Discover oversharing risks</p> <ul style="list-style-type: none"> Use permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)¹ Identify Copilot agent insights & take actions¹ <p>2. Restrict sensitive info from Copilot access and/or processing</p> <ul style="list-style-type: none"> Initiate Access Review for all sites that are overshared¹ Apply restricted access control (RAC) on business-critical sites¹ Exclude critical sites from Copilot reasoning over them¹ <p>3. Increase site privacy</p> <ul style="list-style-type: none"> Publish labels to Office apps, Container/Sites, Outlook for manual data protection by user² Use site labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members² Turn on enforce-mode oversharing SPO DLP policy to restrict access to sensitive data exposure & starting remediating them² Disable RSS (if enabled) to allow full Copilot experience¹ 	<p>1. Further reduce risk and simplify oversight</p> <ul style="list-style-type: none"> Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹ Automate SAM permission state report to maintain permissions hygiene¹ <ul style="list-style-type: none"> Automate permission reports and actions to maintain permission hygiene¹ Regularly review oversharing reports and restrict access as needed¹ Proactively avoid oversharing by applying RAC at site provisioning¹ Periodically review inactive sites and take necessary action¹ Control site provisioning by allowing creation for users that complete training¹ Use change history to identify site changes that may cause oversharing¹ Continuously manage all your oversharing DLP alerts via the Microsoft Purview Portal² <p>2. Further secure sensitive data</p> <ul style="list-style-type: none"> Reduce risk by remediating alerts for overshared documents from the SPO DLP policy and applying sensitive labels² <p>3. Improve Copilot responses</p> <ul style="list-style-type: none"> Setup retention/deletion policies for SharePoint to reduce data surface² Identify inactive sites, then restrict access, archive or delete¹

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: <https://aka.ms/E3PrepareYourDataForCopilot>



Oversharing Agenda

1

Intro to Oversharing

2

Oversharing Blueprint

3

Restricted SharePoint Search (Temporary)

4

SharePoint Advanced Management (SAM)

5

Microsoft Purview

Restricted SharePoint Search

Temporary mitigation for customers where oversharing of data is a concern



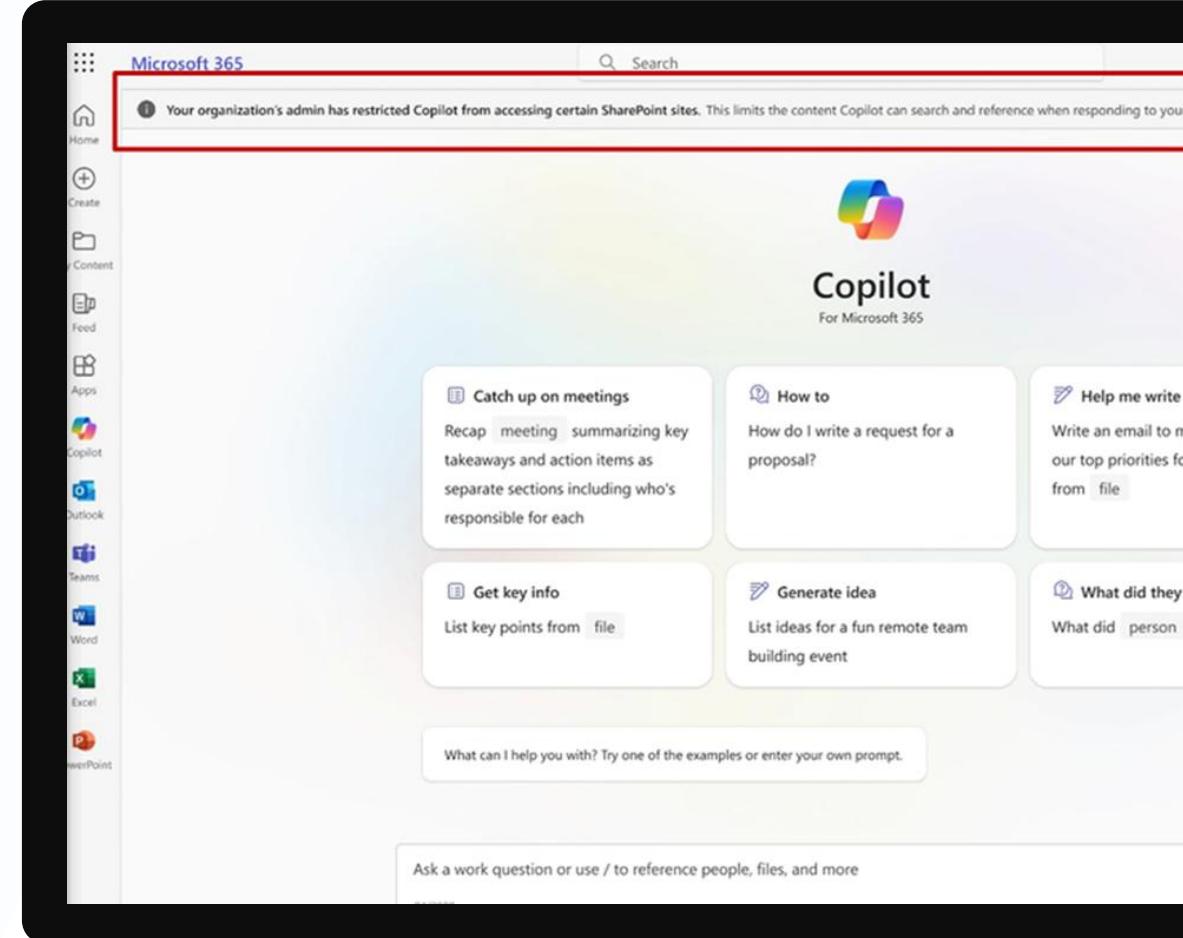
Impacts Copilot and **organization-wide** Search



Restricts the scope of search to site whitelist



Workaround to **unlock** Copilot deployment



Which data can Copilot still retrieve & use with RSS enabled?



Allowed list of curated SharePoint sites setup by admin



Files that were shared directly with the user



User's content such as OneDrive files, chats, emails and calendar



Files that the user viewed, edited or created



Files from their frequently visited SharePoint sites

Plan your RSS Allow List

Get an initial list of sites

The “Known” sites
The top active and shared sites



Review site permissions

Work with your site admins and stakeholders to assess permissions



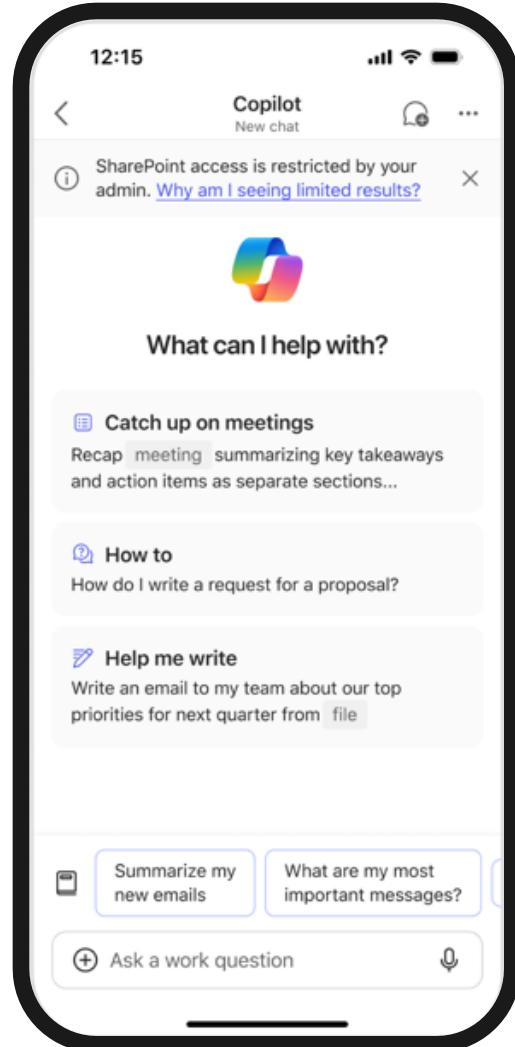
Apply the allowed list

Turn on Restricted SharePoint Search, add, and remove sites.

Enable SharePoint Restricted Search

Step	Description	Example
1	Get the current mode that is set for Restricted Search	<code>Get-SPOTenantRestrictedSearchMode</code>
2	Enable Restricted Search	<code>Set-SPOTenantRestrictedSearchMode -Mode Enabled</code>
3a	Add sites using a list	<code>Add-SPOTenantRestrictedSearchAllowedList -SitesList @("https://contoso.sharepoint.com/sites/Marketing", "https://contoso.sharepoint.com/sites/Benefits")</code>
3b	Add sites using a CSV file	<code>Add-SPOTenantRestrictedSearchAllowedList -SitesListFileUrl C:\Users\admin\Downloads\UrlList.csv</code>

End-User Experience

The Microsoft 365 web interface showing the Copilot extension. The top navigation bar includes 'Microsoft 365', a search bar, and various settings icons. A red box highlights a message in the top left corner: 'Your organization's admin has restricted Copilot from accessing certain SharePoint sites. This limits the content Copilot can search and reference when responding to your prompts. [Learn more](#)' followed by a close button. The main content area features the Copilot logo and 'Copilot For Microsoft 365'. It displays six cards with prompts: 'Catch up on meetings' (Recap meeting summarizing key takeaways and action items as separate sections including who's responsible for each), 'How to' (How do I write a request for a proposal?), 'Help me write' (Write an email to my team about our top priorities for next quarter from file), 'Get key info' (List key points from file), 'Generate idea' (List ideas for a fun remote team building event), and 'What did they say?' (What did person say about...). Below these cards is a text input field with placeholder text: 'What can I help you with? Try one of the examples or enter your own prompt.' and a 'View prompts' button. At the bottom, there is a text input field with placeholder text: 'Ask a work question or use / to reference people, files, and more' and a character count indicator '84/2000'.

End-User Support Article



<https://support.microsoft.com/en-us/office/why-am-i-seeing-limited-results-29c9d8da-30d0-4ec2-a41f-5f2d93b509e4>

Why am I seeing limited results?

► Applies To

Your search and your Copilot experience are showing you limited results because your organization's administrator has decided to restrict the SharePoint sites that appear in the organization-wide search results and Copilot experiences. When your administrator makes this decision, only the following organization content will show up in your organization-wide search and your Copilot experiences:

- A curated list of SharePoint sites set up by your organization's administrator
- Content from SharePoint sites you frequently visit
- Your files from OneDrive, chats, emails, and calendars you have access to
- Files that were shared directly with you
- Files you've viewed, edited, or created

To have more results included in search and Copilot experiences, please get in touch with your administrator to provide access to additional sites.

If you're not sure who your administrator is see [How do I find my Microsoft 365 admin?](#)



Need more help?



Restricted SharePoint Search – Key Takeaways

Not a “Copilot” Feature

Should only be considered if your Copilot deployment is blocked due to file oversharing concerns

A temporary solution: Allows full Copilot deployment, and in parallel, implementation of security controls as needed (SAM/Purview) to address oversharing concerns

Does not modify permissions or sharing controls on content

Will impact other org-wide search experiences in Microsoft 365



Restricted SharePoint Search – Limitations

Restricted SharePoint Search can't be scoped to specific group of users.

The restricted SharePoint search experience affects all users, both those with Copilot licenses and those without.

The limit of 100 allowed SharePoint sites is not expandable.

Any file shared explicitly with a user are still included in Copilot experience, irrespective of RSS.

Frequent SharePoint sites for users are part of Copilot experience.

Resources



[Introducing Restricted SharePoint Search](#)



[Data, Privacy, and Security for Copilot for Microsoft 365](#)



[Restricted SharePoint Search - SharePoint in Microsoft 365 | Microsoft Learn](#)



Oversharing Agenda

1

Intro to Oversharing

2

Oversharing Blueprint

3

Restricted SharePoint Search (Temporary)

4

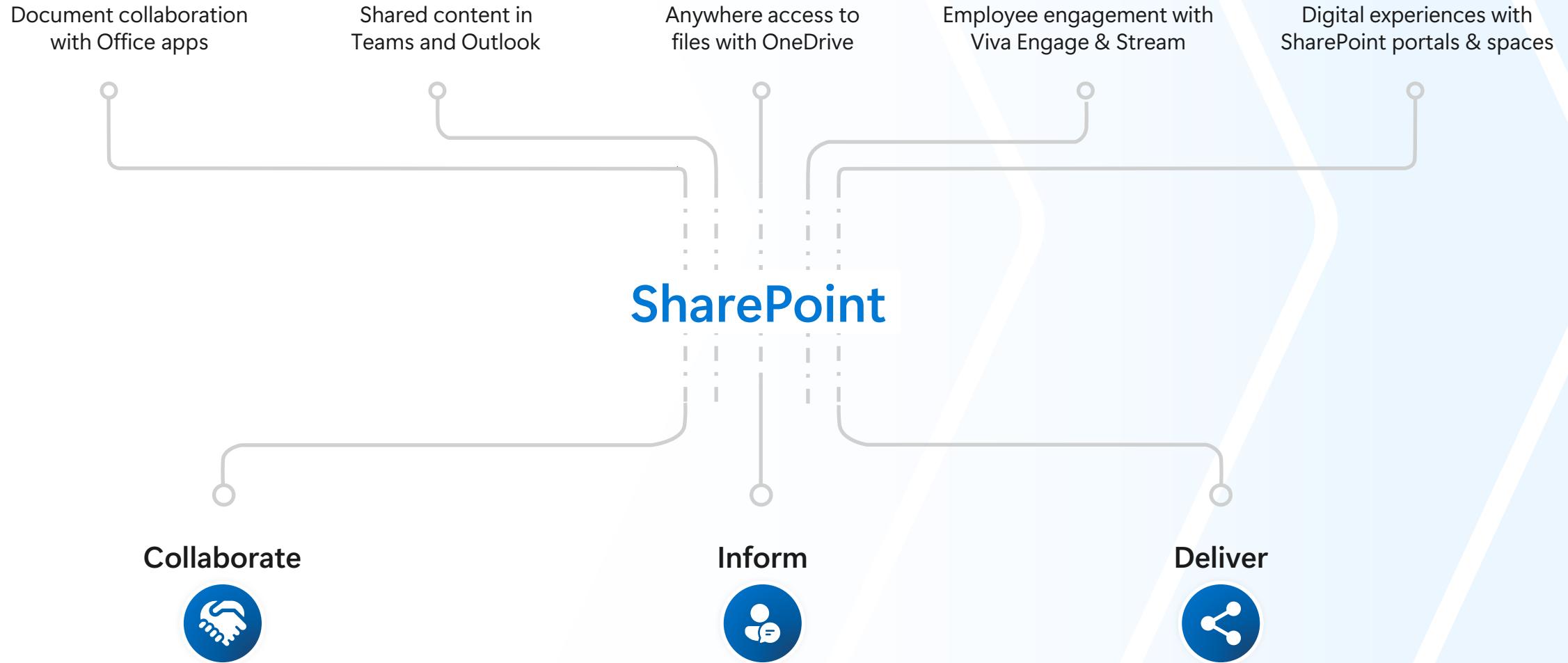
SharePoint Advanced Management (SAM)

5

Microsoft Purview

SharePoint | Content collaboration in the Microsoft cloud

SharePoint is at the center of content collaboration in the Microsoft cloud and empowers you to collaborate, inform, and deliver with dynamic sites, personalized news, and secure file sharing.



Govern Copilot content access and quality with SAM

SharePoint Advanced Management enhances content governance for SharePoint and OneDrive, streamlining content management and preventing content sprawl and oversharing



Content Sprawl



Content Oversharing
prevention



Site Lifecycle

SharePoint Advanced Management capabilities

	SAM Capabilities
Oversharing and accidental sharing Lack of built-in tools and access policies puts content at risk.	SharePoint data access governance (DAG) insights Quickly identify overshared sites and request sites access review by site owners. Restricted access control (RAC) for SharePoint sites Limit access to specific SharePoint sites and stop oversharing in seconds. Restricted access control (RAC) for OneDrives Limit access to OneDrive's across the tenant to specific users (e.g., full-time employees) in seconds. Conditional access policies for SharePoint and OneDrive sites (CAPS) Add conditions like MFA or Managed device to access sites with business-critical content. Block download policy for SharePoint and OneDrive sites Block download of content to prevent accidental oversharing or data loss. Block the download of Teams meeting recording files from SharePoint or OneDrive Block download of Teams recording for anyone in the company
Sprawl of SharePoint sites content Governing ever-increasing digital content is critical for every SharePoint or IT admins.	SharePoint data access governance (DAG) insights Quickly identify most important sites to your organization Inactive SharePoint sites policy Automatically identify and take control of inactive sites. Recent admin actions Find a list of recent site actions as well as status of those actions. Change history Audit / review changes to site settings by any anyone with access to SharePoint Admin Center. Collaboration Insights Optimize workflows, enhance communication, and drive data-driven decisions for increased productivity, efficiency, and success in your organization.
Content lifecycle management Lack of advanced management tools to continuously monitor and govern inactive/active SharePoint sites content make it hard to meet various access and regulatory requirements, such as GDPR, FINRA.	SharePoint data access governance (DAG) insights Quickly identify sites that need your attention. Block download policy for SharePoint and OneDrive sites Block download of content to prevent accidental oversharing or data loss. Inactive SharePoint sites policy Automatically handle stale sites.

Oversharing control: Permission State Report with Actions

Gain Control Over Site Permissions and Overshared Content

Identify Overshared content:

- Customizable and comprehensive permission reports across all sites
- Detect root causes of oversharing (broken inheritance, sharing links, EEEUs, site privacy and more)
- Focus on critical permissions by user count and extended groups
- Integrates with sensitivity labels for enhanced security
- Downloadable, with insights from AI analytics

Scalable Actions:

- Site Access Review with site owner file review dashboard
- Restricted Access Control – limit access to high-risk areas
- Restricted Content Discovery – lock down content from Copilot

Generally available

The screenshot shows a Microsoft SharePoint interface. At the top, there's a header bar with the site name 'Contoso Finance' and various navigation links like Home, News, Team directory, Patents, Files, FAQs, and Edit. To the right, there are buttons for Private, Top secret, Follow, and a search bar. Below the header, a banner says 'Snapshot till March' with a link to 'Download detailed report'. Underneath, there are buttons for '+ Initiate site access review', 'View all reviews', and 'Restrict site access'. The main content area is titled 'Site reviews > Permissions to many users'. It displays a table with columns: Name, Scope, Total number of Permisioned users, Total number of groups, Count of Anyone' links, Count of 'People in your org' links, Has EEEU, Has Everyone, Action, and Final status. The table lists several items, including 'Contoso Finance' (SharePoint Site, 6804 users), 'Finance_projections_FY23.xlsx' (File, 7142 users), 'Vendor Bills' (Folder, 7524 users), 'ProfitabilityPlan.pptx' (File, 7945 users), 'Flow map.jpg' (File, 8580 users), and 'Confidential Q2 CY24 ReOrg' (File, 9092 users). Each row has a 'Manage access' button with a dropdown menu showing options: 'Select', 'Retained all permissions', 'Modified existing permissions', and 'Removed permissions completely'. A callout box highlights the 'Broken inheritance, Sharing links, EEEU domain group' column. At the bottom of the table, there are buttons for 'Complete review', 'Save as draft', and 'Cancel'.

Data access governance

Reports My review requests

This page provides reports to help you maintain the security and compliance of your data in SharePoint.

[Learn more about data access governance](#)

Sharing links

Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint.

[View reports](#)

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites.

[View reports](#)

Shared with 'Everyone except external users'

Make sure files, folders, and lists aren't being overshared by reviewing sites that have the most items shared with "Everyone except external users."

[View reports](#)

Content accessible to 'Permissioned users'

[PREVIEW](#)

Review sites with a high number of users across all permission scopes (inherited and broken).

[View reports](#)

Data access governance > Content accessible to 'Permissioned users'

Content accessible to 'Permissioned users' PREVIEW

Review sites with a high number of users across all permission scopes (inherited and broken).



No reports right now

Create a new report using filters.

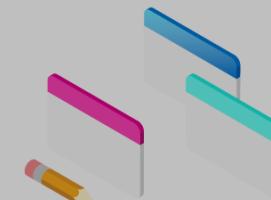
[Create report](#)

Data access governance > Content accessible to 'Permissioned users'

X

Content accessible to 'Permissioned users' PREVIEW

Review sites with a high number of users across all permission scopes (inherited and broken).



No reports right now

Create a new report using filters.

[Create report](#)

Create a report

Discover sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold

Report name ***Scope *** SharePoint OneDrive For Business**Template *****Privacy (Team sites only)****Sensitivity****Sensitivity Info Type****Report type *** Snapshot till date

Generated based on latest permissions, as of report generation date

 Recent activity for last 28 days**Count of permissioned users**[Create and run](#)[Cancel](#)

Data access governance > Content accessible to 'Permissioned users'

Content accessible to 'Permissioned users' PREVIEW

Review sites with a high number of users across all permission scopes (inherited and broken).

[Learn more about content accessible to 'Permissioned users'](#)

Add a report Run all Refresh status

<input type="checkbox"/>	Report name	Status	Scope	Permissioned users count	Date range	Sites found	Privacy (Team sites only)	Sensitivity	Template
<input type="checkbox"/>	Snapshot till March	Running (this might take a few hours)	SharePoint	Over 1,000	As of Mar 3, 2023	-	Private	All	Communication sites, Team sites
<input type="checkbox"/>	View for Feb	Updated in the last 24 hours	SharePoint	Over 2,500	As of Feb 3, 2023	198	Private	Highly confidential	-



Snapshot till March

This displays list of sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold
Download detailed .csv report for up to 10,000 sites.

[Download detailed report](#)[+ Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

Filters: Site sensitivity: All External sharing: All

Filters: Site sensitivity: All External sharing: All

These are labelled files and unlabelled files where a sensitive info type was detected

Name	URL	Site access review status	Files	No. of sensitive files ⓘ	Total permissioned users ↓	Count of EEEU permissions	Count of 'Anyone' lin
Contoso HR	../teams/contosohr	—	44869	4814	22334	2	312
Contoso Marketing	../teams/contosomar	—	41839	4423	15698	1	296
Contoso Finance	../sites/contosofin	—	38286	4178	11237	3	167
Contoso Giving	../sites/contosogiv	—	35310	3987	10245	6	145
Contoso team	../sites/contosoteam	—	31498	3546	8530	2	124
Contoso Vac	../sites/contosovac	—	30764	3215	6054	1	72
Contoso HRA	../teams/contosohra	—	28187	2895	3998	5	2416
Contoso Media	../sites/contosomedia	—	22396	2564	2804	8	38
Contoso in house	../sites/contosoinh	—	20189	2489	1890	3	32
Contoso infra	../sites/contosoinfra	—	19374	2341	1487	4	23
Contoso design	../sites/contosodesign	—	13298	2287	1329	1	21
Contoso leaders	../teams/contosolead	—	9450	2135	1127	5	21
Contoso data	../teams/consolidata	—	8800	2039	1038	7	647
Contoso BI	—	8126	1983	1024	2	721	

Initiate site access review

An email will be sent to all site owners, with a request for them to review the sites for potential oversharing.

Add a comment for site owners

E.g. Check these sites for number of users or permissions or sharing events etc.

Sites added

CS Contoso Finance
...com/sites/contosofin

CS Contoso Giving
...com/sites/contosogiv

[Send](#)[Cancel](#)



Site reviews > Permissions to many users

The list below details inherited and unique permissions which have the highest number of users and possible contributing factors such as links, groups or Everyone Except External Users (EEEU) claims. Remove permissions where they are no longer required to prevent oversharing.

	Name	Scope	Number of Permissioned users	Sensitivity Info Type	Sensitivity Label	Number of groups	Number of 'Anyone' links	Number of 'People in your org' links	Has EEUU	Action	Final status
>	Contoso Finance	SharePoint Site	6804	US Passport Number +2	Top secret	4	-	-	-	Manage access	Select
>	Finance_projections_FY23.xlsx	File	7142	US SSN Number + 4	Confidential	5	2	2	-	Manage access	Select
>	Vendor_bills	Folder	7524	US SSN Number + 1	Highly confidential	7	1	2	-	Manage access	Select
>	ProfitabilityPlan.pptx	File	7945	US SSN Number	-	6	1	3	Yes	Manage access	Select
>	Flow map.jpg	File	8580	US Passport Number	General	3	2	1	Yes	Manage access	Select
>	Confidential Q2 CY24 ReOrg	File	9092	ABA Routing Number	-	4	3	3	Yes	Manage access	Select



Site reviews > Permissions to many users

The list below details inherited and unique permissions which have the highest number of users and possible contributing factors such as links, groups or Everyone Except External Users (EEEU) claims. Remove permissions where they are no longer required to prevent oversharing.

Name	Scope	Number of Permissioned users	Sensitivity Info Type	Sensitivity Label	Number of groups	Number of 'Anyone' links	Number of 'People in your org' links	Has EEEU	Action	Final status
> Contoso Finance	SharePoint Site	6804	US Passport Number +2	Top secret	<u>4</u>	-	-	-	Manage access	Select
> Finance_projections_FY23.xlsx	File	7142	US SSN Number + 4	Confidential	<u>5</u>	2	2	-	Manage access	Select
> Vendor_bills	Folder	7524	US SSN Number + 1	Highly confidential	<u>7</u>	1	2	-	Manage access	Select
> ProfitabilityPlan.pptx	File	7945	US SSN Number	-	<u>6</u>	1	3	Yes	Manage access	Select
> Flow map.jpg	File	8580	US Passport Number	General	<u>3</u>	2	1	Yes	Manage access	Select
> Confidential Q2 CY24 ReOrg	File	9092	ABA Routing Number	-	<u>4</u>	3	3	Yes	Manage access	Select

Broken permission inheritance

Files containing sensitive data

Default sharing option is everyone

Use of "everyone except external users" domain group

Restricted Access Control (RAC)

for SharePoint & OneDrive



RAC (Restricted access control) policy can be set at the site level. Even if individual files/folders have broken inheritance and over-shared, only RAC allowed users can access

Copilot honors RAC policy!

Microsoft 365 group-connected sites,
Non-group SharePoint sites, Teams sites,
Shared channel sites, OneDrive sites

Generally available

The screenshot shows the SharePoint admin center interface. On the left, there's a navigation pane with various options like 'Data access governance', 'Content accessible to 'Permissioned users'', and 'Snapshot till March'. The main area displays a table titled 'Snapshot till March' showing a list of sites across different teams and their permission status. On the right, a modal window titled 'Restricted site access' is open, explaining the setting allows only users in specific security groups to access the site. It includes a checkbox for 'Restrict SharePoint site access to only users in specified groups' and a dropdown menu for 'Add group' containing several Microsoft 365 groups: Contoso Financial Council, Contoso Tech, Contoso Marketing, and Contoso HR.

Restricted Content Discovery (RCD)

Advanced access control to exclude sites from Copilot

1

Use this **site-level setting Restricted Content Discoverability** to restrict content discoverability via Copilot and Org-wide search

2

SharePoint Admin sets this property to a site via PS cmdlet

3

There is no change to the site's permissions! > Users continue to have physical access

4

Contents of the site gets reindexed** – as a result contents are security trimmed and **not discoverable via Copilot and tenant-wide search**

```
>Set-SPOSite -Identity <site-url> -RestrictContentOrgWideSearch $true
```

Public preview

**Standard indexing delays apply, especially with site with large number of files

```
PS C:\WINDOWS\system32> Set-SPOSite -Identity https://contosoenergyusa40.sharepoint.com/sites/ContosoFin -RestrictContentOrgWideSearch $true
```



Search



Work

Web



11:10 AM

Are there any ORG changes happening next month



Without SAM

Yes, there are some organizational changes happening next month. Here are a few updates:

1. **BWS Organizational Update:** Kristin Patterson has joined the BWS leadership team to lead the Customer Voice & Health Team. Kadji Bell will transition manager responsibilities to Kristen and take on a critical IC role focused on the execution of the center of excellence, change management, and scaling processes. This change will be effective from August 26 [1](#).
2. **Changes to the BWS Design team:** Mona Kane, Ray Tanaka, and Sarah Evans will move to Sarah Perez's team. Mona will report directly to Sarah, and Ray and Sarah will report to Robyn. Sara Kiani will remain in BWGD and will report to Robin Counts' team. This change is effective immediately [2](#).
3. **Confidential Q2 CY24 ReOrg:** There are org changes coming up on September 4th based on this report [3](#) [4](#).

[1 BWS Org Update](#)[2 Changes to the BWS D...](#)[3 Confidential Q2 CY...](#)[+1](#)[Copy](#)[Share](#)

1 of 20 responses

AI-generated content may be incorrect

[View prompts](#)

Are there any ORG changes happening next month?

[+ Add content](#)



Search



Work

Web



11:10 AM

Are there any ORG changes happening next month



With SAM

Yes, there are some organizational changes happening next month. Here are a few updates:

1. **BWS Organizational Update:** Kristin Patterson has joined the BWS leadership team to lead the Customer Voice & Health Team. Kadji Bell will transition manager responsibilities to Kristen and take on a critical IC role focused on the execution of the center of excellence, change management, and scaling processes. This change will be effective from August 26 [①](#).
2. **Changes to the BWS Design team:** Mona Kane, Ray Tanaka, and Sarah Evans will move to Sarah Perez's team. Mona will report directly to Sarah, and Ray and Sarah will report to Robyn. Sara Kiani will remain in BWGD and will report to Robin Counts' team. This change is effective immediately [②](#).

1 [BWS Org Update](#)2 [Changes to the BWS D...](#)[Copy](#)[Share](#)

1 of 20 responses

AI-generated content may be incorrect

[View prompts](#)

Are there any ORG changes happening next month?

[+ Add content](#)



Oversharing Agenda

1

Intro to Oversharing

2

Oversharing Blueprint

3

Restricted SharePoint Search (Temporary)

4

SharePoint Advanced Management (SAM)

5

Microsoft Purview



Addressing oversharing at file level with Purview

1

Identify overshared files and sites with new [Oversharing assessments](#) surfaced in Data Security Posture Management for AI

2

Keep Copilot from using labeled files in prompts responses with [Data Loss Prevention](#) for M365 Copilot and [Information Protection](#) sensitivity labels

Identify and mitigate risks related to AI usage

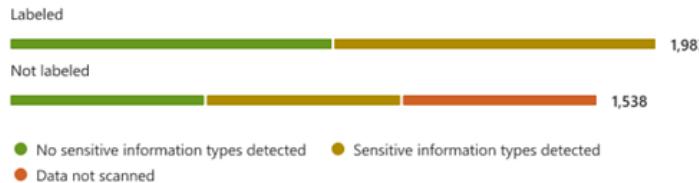
Oversharing assessment in Data Security Posture Management (DSPM) for AI

Proactively strengthen data security to help prevent incidents like data oversharing, leakage, or unethical use

Protect your data from potential oversharing risks

Data assessments provide you with insights on potential oversharing risks in your organizations, along with fixes to limit access to sensitive data.

Data coverage of top 100 SharePoint sites



Obsidian Merger

Overview Protect Monitor

Sensitive information auto-labeling policy

Use auto-labeling policies based on sensitive content or keywords.

Sensitive information types

12

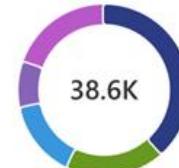
[View all](#)



Create auto-labeling policy for sensitive information
Microsoft Purview Information Protection

Top unethical use in AI interactions

Potentially unethical behavior detected in prompts and responses in Microsoft 365 Copilot.



● Targeted harassment ● Threat ● Money laundering ● Stock manipulation ● Unauthorized disclosure

[View details](#) [View recommendation](#)

Discover data security, safety, and compliance risks in reports and oversharing assessments

Protect sensitive data from overexposure with suggested policies and **one click application of sensitivity labels**

Govern AI usage for non-compliant or unethical usage and get recommendations on enforcing compliance policies

Now in public preview

Exclude sensitive files from Copilot processing

Microsoft Purview Data Loss Prevention (DLP) for Microsoft 365 Copilot

Prevent Microsoft 365 Copilot Business Chat from creating summaries or responses for Office or PDF files with specified sensitivity labels

Choose where to apply the policy

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

Location	Scope	Actions
<input type="checkbox"/> Exchange email	Turn on location to scope	
<input type="checkbox"/> SharePoint sites	Turn on location to scope	
<input type="checkbox"/> OneDrive accounts	Turn on location to scope	
<input type="checkbox"/> Teams chat and channel messages	Turn on location to scope	
<input checked="" type="checkbox"/> Microsoft 365 Copilot	All users & groups	Edit

[Back](#)[Next](#)[Cancel](#)

Granular options for policy targeting

Configure restrictions at an item level, group/site level, or for specific Entra user groups.

[Create group](#)[+ Add condition](#) [Add group](#)

Actions

Use actions to protect content when the conditions are met.

Prevent Copilot from processing content

Content that matches your conditions won't be used by Copilot to generate responses.

[Learn more about this action](#)

ⓘ Currently, this action is supported only for labeled files in SharePoint and OneDrive that are processed in Microsoft 365 Chat experiences.

Exclude content from processing in Copilot ⓘ

[+ Add an action](#)[Save](#)[Cancel](#)

Prevent Copilot from processing file contents

Ensure that sensitive content within labeled documents is not processed and responses are not available to copy and paste into other applications

Links to learn more (1 of 2)

[Copilot Readiness Hub](#)

What is Copilot?

- [Introducing Copilot for Microsoft 365](#)
- [The Copilot System](#)
- [ChatGPT vs. Copilot for Microsoft 365: What's the difference?](#)

How Copilot works

- [How Copilot for Microsoft 365 works: Microsoft Mechanics video](#)
- [Semantic Index for Copilot](#)
- [Microsoft Graph](#)
- [Microsoft Graph connectors](#)
- Additional copilot experiences across the Microsoft Cloud
 - [Microsoft Dynamics 365 Copilot](#)
 - [Copilot in Power Platform](#)
 - [Microsoft Security Copilot](#)
 - [GitHub Copilot](#)
 - [Copilot in Microsoft Stream](#)

Privacy

- [Microsoft's privacy policy](#)
- [Microsoft Privacy Statement](#)
- [Trust Center data protection and privacy](#)
- [Data, privacy, and security for Copilot for Microsoft 365](#)
- [Data, privacy, and security for Azure OpenAI Service](#)
- [Role-based access control](#)
- [User permissions and permission levels in SharePoint Server](#)
- [Customer Lockbox requests](#)
- [Microsoft 365 isolation controls](#)
- [Data Protection Addendum](#)

Links to learn more (2 of 2)

Data residency and storage

EU Data Boundary

- [Website](#)
- [Blog](#)
- [Documentation](#)

Compliance

- [Microsoft Compliance](#)
- [Service Trust Portal](#)
- [Compliance offering definitions](#)
- General Dat Protection Regulation (GDPR)
 - [Full summary](#)
 - [Short summary](#)

How to prepare for Copilot for Microsoft 365

- [Learn about Microsoft feedback for your organization](#)
- [Manage Microsoft feedback for your organization](#)
- [How to manage Microsoft Search](#)
- [Microsoft 365 Product Terms](#)
- [Content management and security in SharePoint, OneDrive, and Teams](#)

Security

- [Configure usage rights for Azure Information Protection \(AIP\)](#)
- [Universal Licensing Terms for Online Services](#)
- [Data Protection Addendum](#)
- [Isolation and Access Control in Microsoft 365](#)

Responsible AI

- Responsible AI core principles
 - [Videos](#)
 - [Documentation](#)
- [Microsoft Responsible AI Standard](#)
- [Governing AI: A Blueprint for the Future](#)

New security managed services partner kit

- 1 Grow recurring revenue and profitability with security managed services
- 2 Use AI driven sales insights and M365 Lighthouse multitenant management to increase success
- 3 Increase customer loyalty and partner share of wallet



Step by step guidance on how to begin with services



Practical guidance on expanding from IT management to security



Integration with security frameworks and key partner tools

<https://aka.ms/SMBManagedServices>

Learn more



Get started with [Microsoft 365 Business Premium](#)



Discover how Hollen boosts security with Microsoft 365 Business Premium in this [customer story](#)



[Learn the top 5 benefits](#) of Microsoft 365 Business Premium



Read all about AI-powered [Copilot for Microsoft 365](#)



Links to learn more (1 of 2)

[Copilot Readiness Hub](#)

What is Copilot?

- [Introducing Copilot for Microsoft 365](#)
- [The Copilot System](#)
- [ChatGPT vs. Copilot for Microsoft 365: What's the difference?](#)

How Copilot works

- [How Copilot for Microsoft 365 works: Microsoft Mechanics video](#)
- [Semantic Index for Copilot](#)
- [Microsoft Graph](#)
- [Microsoft Graph connectors](#)
- Additional copilot experiences across the Microsoft Cloud
 - [Microsoft Dynamics 365 Copilot](#)
 - [Copilot in Power Platform](#)
 - [Microsoft Security Copilot](#)
 - [GitHub Copilot](#)
 - [Copilot in Microsoft Stream](#)

Privacy

- [Microsoft's privacy policy](#)
- [Microsoft Privacy Statement](#)
- [Trust Center data protection and privacy](#)
- [Data, privacy, and security for Copilot for Microsoft 365](#)
- [Data, privacy, and security for Azure OpenAI Service](#)
- [Role-based access control](#)
- [User permissions and permission levels in SharePoint Server](#)
- [Customer Lockbox requests](#)
- [Microsoft 365 isolation controls](#)
- [Data Protection Addendum](#)

Links to learn more (2 of 2)

Data residency and storage

EU Data Boundary

- [Website](#)
- [Blog](#)
- [Documentation](#)

Compliance

- [Microsoft Compliance](#)
- [Service Trust Portal](#)
- [Compliance offering definitions](#)
- General Dat Protection Regulation (GDPR)
 - [Full summary](#)
 - [Short summary](#)

How to prepare for Copilot for Microsoft 365

- [Learn about Microsoft feedback for your organization](#)
- [Manage Microsoft feedback for your organization](#)
- [How to manage Microsoft Search](#)
- [Microsoft 365 Product Terms](#)
- [Content management and security in SharePoint, OneDrive, and Teams](#)

Security

- [Configure usage rights for Azure Information Protection \(AIP\)](#)
- [Universal Licensing Terms for Online Services](#)
- [Data Protection Addendum](#)
- [Isolation and Access Control in Microsoft 365](#)

Responsible AI

- Responsible AI core principles
 - [Videos](#)
 - [Documentation](#)
- [Microsoft Responsible AI Standard](#)
- [Governing AI: A Blueprint for the Future](#)

Learn more



Get started with [Microsoft 365 Business Premium](#)



Discover how Hollen boosts security with Microsoft 365 Business Premium in this [customer story](#)



[Learn the top 5 benefits](#) of Microsoft 365 Business Premium



Read all about AI-powered [Copilot for Microsoft 365](#)





<https://bit.ly/ciacopilottech>