



CSP Level Up In-Person Technical Training



Become Copilot Ready



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.

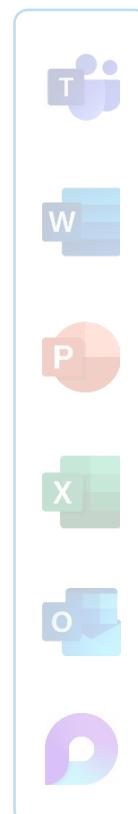
Govern access to Copilot

Microsoft Entra ID Premium P1

Users and Devices

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

- 2 Microsoft Entra ID P1



- 1 **Mitigate Device Risk** with Unified Endpoint management

- 2 Microsoft Intune 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

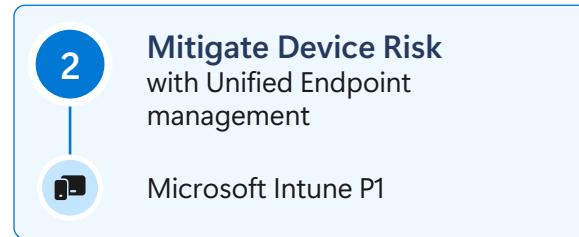
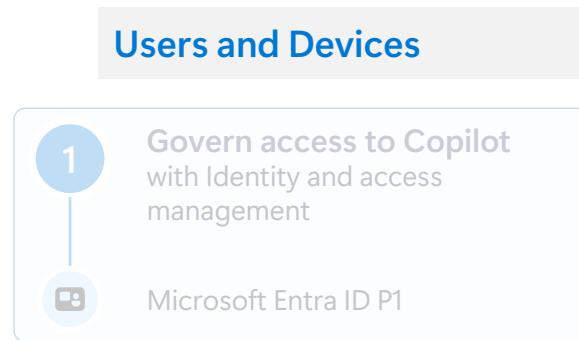


Password reset

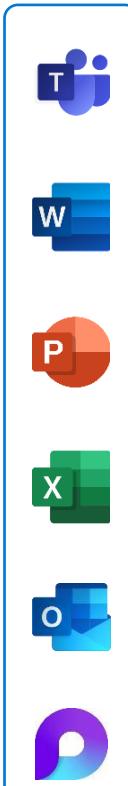
Monitor critical events and issue access tokens that can be revoked immediately.

Mitigate device and application risk

Microsoft Intune P1



Microsoft 365
Copilot



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:

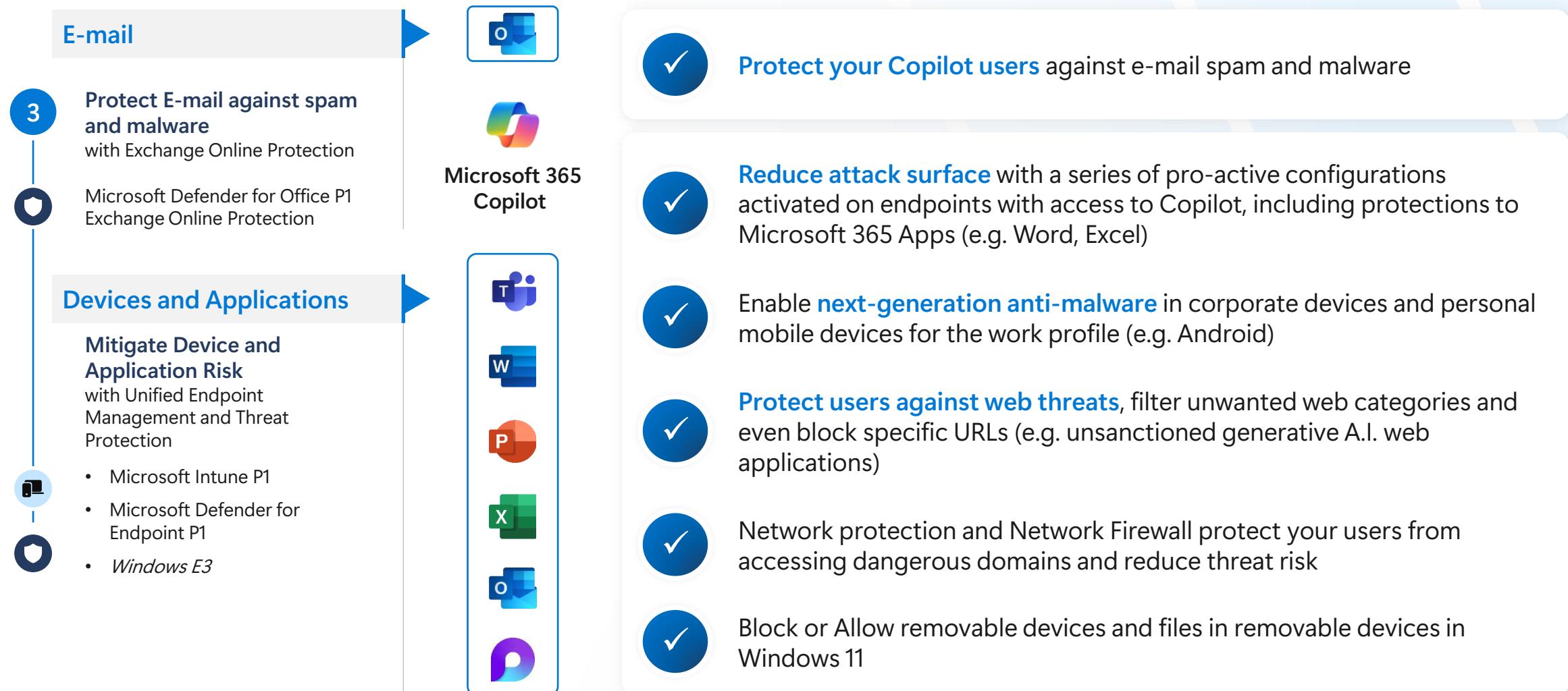
- Save generated files to unsecured apps
- Restrict copying and pasting to non-work apps
- DLP + Sensitivity Labels



Wipe all work content if the device is lost or disassociated with the company or the user.

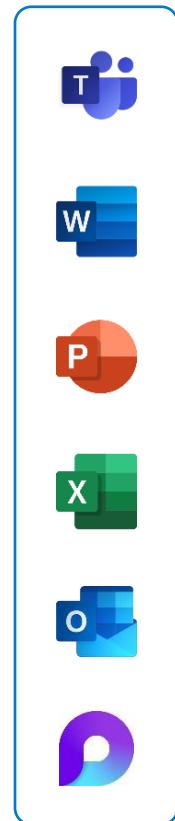
Protect E-mail, devices and apps against threats

Microsoft Defender for Endpoint P1, Exchange Online Protection



Secure and govern data in Copilot interactions

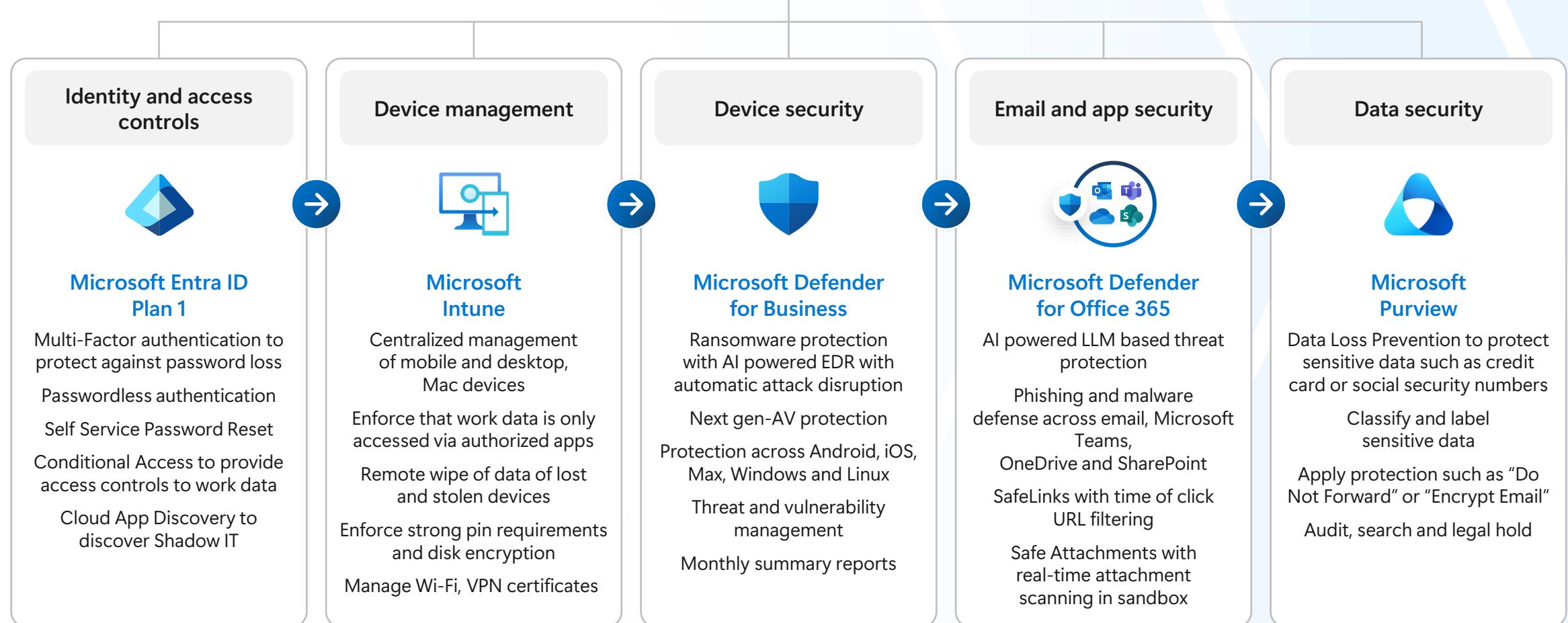
Microsoft Purview Information Protection P1



- 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

Additional offerings for small and medium businesses

Data protection add-ons



Information protection and governance

Discover, classify, and protect sensitive information wherever it lives or travels

\$7/user/month



Insider risk management

Detect, investigate, and act on malicious and inadvertent activities

\$6/user/month



eDiscovery and audit

Search and export content in Microsoft 365 and Office 365

\$6/user/month

Productivity add-ons



Clipchamp Premium

Video editing app with advanced features incl. brand kit, advanced 4K/60 fps output, generative AI

Intro. price:
\$5/user/month



Teams Phone Standard

Cloud-based telephony using VOIP or PSTN

\$8/user/month

Securing AI Environments from Threats



Copilot for Microsoft 365

Unlock productivity and unleash creativity



Natural Language



Large Language
Models

+



Microsoft Graph
- Your Data -

+



Microsoft 365
Apps

+



The
Web



Security

+



Compliance

+



Privacy

+



Responsible AI

Concerns we've heard from you...



Shadow AI use

78%
of AI users use BYOAI

75% of employees are using AI, which means ~58% of employees are bringing their own AI to work¹.



Lack of protection

97%
of organizations

have concerns about implementing AI due to the lack of controls to mitigate risks of data leakage².



Increased AI **regulations**

By
2027

at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation².

1. [2024 Work Trend Index Annual Report from Microsoft and LinkedIn: AI at Work Is Here. Now Comes the Hard Part](#)

2. [Securing data in an AI-first world with Microsoft Purview, Nov 15, 2023](#)

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

You are not alone.

Organizations worldwide are facing similar challenges



Over-burdened employees spending too much time on routine tasks

Find the right strategy to implement generative AI technology to boost productivity and automate tasks.



Complexity in managing endpoints (PCs, tablets, phones, etc.)

Balance employees using their own devices for work, while also controlling against unauthorized app/device use.



Concerns over accidental sharing and non-compliance from within the company

Establish the right data governance model to securely enable AI and avoid disjointed identity and access strategies and intrusive device experience.



Risks associated with external security threats and attacks

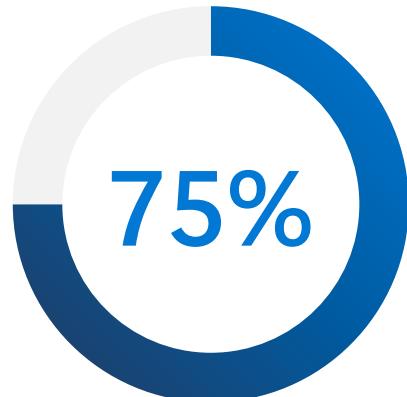
Protect your data and endpoints across the organization with Zero Trust security.



High IT costs and inefficiencies associated with using too many solutions from multiple vendors

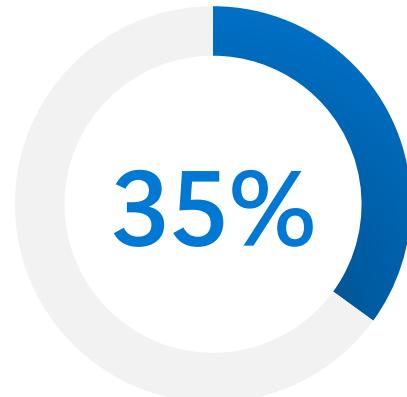
Minimize total cost of ownership (TCO) with vendor consolidation and navigate your migration to the cloud.

Enabling AI productivity while protecting organization data



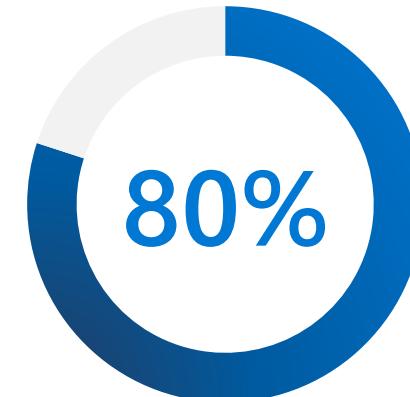
AI productivity expectations

75% of knowledge workers use AI at work today¹



Lack of controls to protect data shared in AI

35% of respondents are concerned about lack of tools to protect data that goes into generative AI²



Integrated security platform

80% agree that a comprehensive security platform with integrated solutions is superior to using multiple best-of-breed solutions that have to be manually integrated and managed³

1. [Work Trend Index](#), commissioned by Microsoft

2. Survey of 658 data security professionals, Mar 2023, commissioned by Microsoft

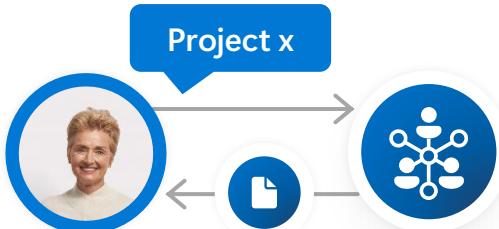
3. [Data Security Index](#) report, Oct 2023, commissioned by Microsoft

Security and compliance challenges

1

Data oversharing

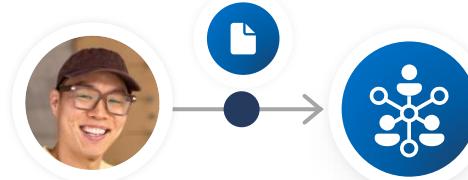
Users may access sensitive data via AI apps they're not authorized to view or edit



2

Data leak

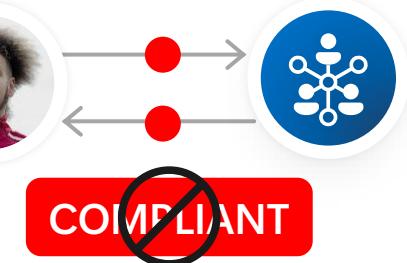
Users may inadvertently leak sensitive data to AI apps



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

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



"Internal threats, whether accidental or malicious, pose a significant risk to sensitive data and critical systems."

"Securing internal systems is the first step toward building a robust defense against external threats."

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

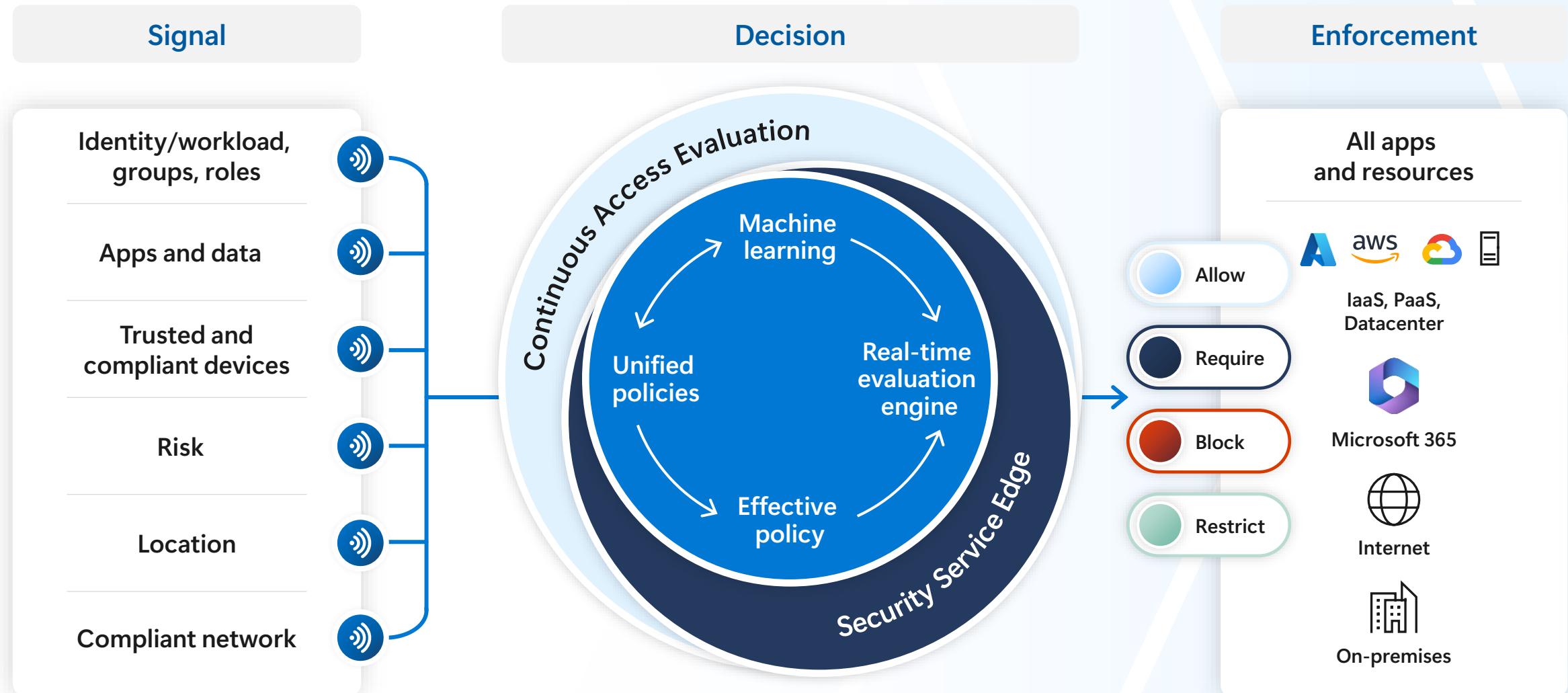
There are over **4,000 password attacks**
every second¹

**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

Enhance Conditional Access with new conditions and controls



Enforce real-time Conditional Access policies



Enforce access controls
with adaptive policies



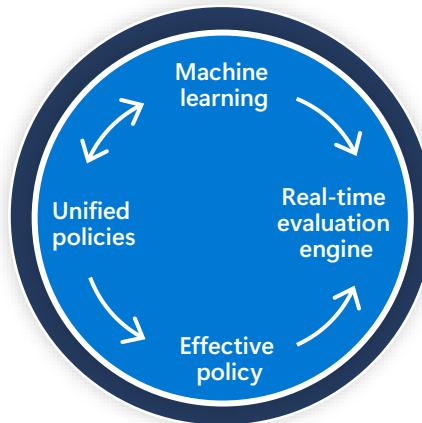
Protect data inside
applications



Restrict access for
vulnerable and
compromised devices

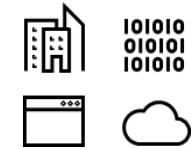
Signals

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.

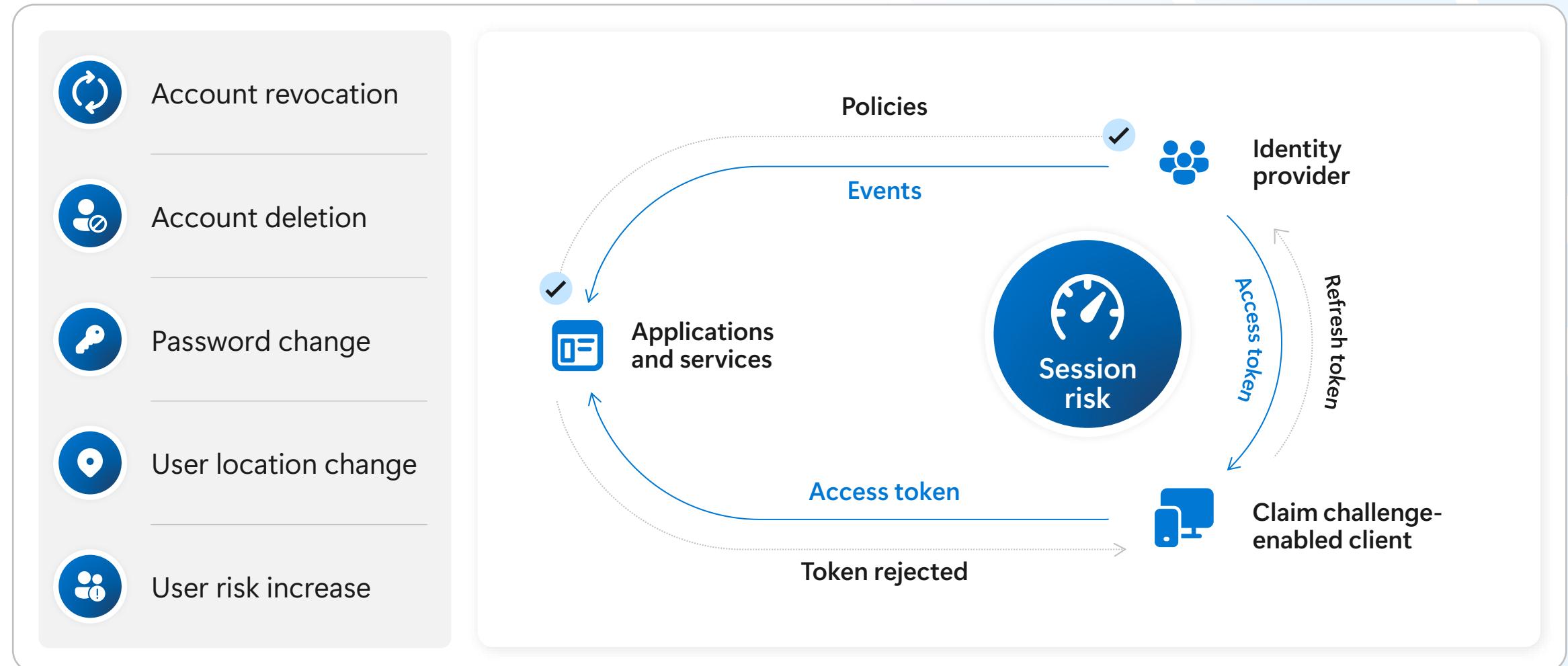
- Templates are grouped into scenario categories:
 - Secure foundation
 - Zero Trust
 - Remote work
 - Protect administrator
 - Emerging threats
 - All
- Templates can be reviewed and adapted before applying
- Ability to upload custom policy files to create your own policy templates

The screenshot shows the 'Create new policy from templates' page. At the top, there's a navigation bar with 'Select a template' and 'Review + Create' tabs, and a search bar. Below the navigation is a category filter bar with tabs: 'Secure foundation' (which is selected), 'Zero Trust', 'Remote work', 'Protect administrator', 'Emerging threats', and 'All'. The main area displays a grid of policy templates. Each template card includes a radio button, the template name, a brief description, and 'View' and 'Download JSON file (Preview)' buttons.

- Require multifactor authentication for admins**
Description: 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 \(Preview\)](#)
- Securing security info registration**
Description: Secure when and how users register for Azure AD multifactor authentication and self-service password.
[Learn more](#)
[View](#) [Download JSON file \(Preview\)](#)
- Block legacy authentication**
Description: Block legacy authentication endpoints that can be used to bypass multifactor authentication.
[Learn more](#)
[View](#) [Download JSON file \(Preview\)](#)
- Require multifactor authentication for all users**
Description: Require multifactor authentication for all user accounts to reduce risk of compromise.
[Learn more](#)
[View](#) [Download JSON file \(Preview\)](#)
- Require multifactor authentication for Azure management**
Description: Require multifactor authentication to protect privileged access to Azure resources.
[Learn more](#)
[View](#) [Download JSON file \(Preview\)](#)
- Require compliant or hybrid Azure AD joined device or multifactor authentication for all users**
Description: 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 views of the Microsoft 365 Defender platform. The top view shows the 'Incidents' dashboard with a list of recent alerts and their details. The bottom view is a detailed look at a specific 'Multi-stage incident on multiple endpoints'. This detailed view includes a summary of active alerts (73/73), MITRE ATT&CK tactics (1), and other alert categories (1). It also lists 20 impacted devices and 12 impacted users. A timeline on the left shows suspicious connection events. The right side provides a breakdown of impacted entities by risk level and a list of 187 entities found.

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 the Microsoft 365 Defender logo and a search bar. The main header is "Microsoft Defender Vulnerability Management dashboard".
Organization exposure score: A circular gauge shows an exposure score of 23/100, with a legend indicating Low (0-29), Medium (30-69), and High (70-100). Below the gauge is a line chart titled "Exposure score over time" showing fluctuations from February 5th to March 5th.
Top security recommendations: A table listing recommendations with columns for Recommendation, Exposed devices, Threats, Impact, and Tags. Examples include "Update Microsoft Edge Chromium-based" (213 devices, 10.69 impact) and "Update Ubuntu Tar for Linux" (94 devices, 2.64 impact).
Top events (7 days): A table showing events from February 27, 2023, such as "Ubuntu Curl for Linux has 3 new vulnerabilities, impacting 111 devices" (111 devices impacted).
Top remediation activities: A table listing activities like "Block Office communication application from creating 37/87 child processes".
Top vulnerable software: A table showing software vulnerabilities across OS platforms: Edge Chromium-based (Other), Tar for Linux (Linux), and Safari for Mac (MacOS).
Microsoft Secure Score for Devices: A summary section showing the overall secure score (49.2%), application, OS, network, accounts, and security controls scores, and a "Score for device" chart.

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



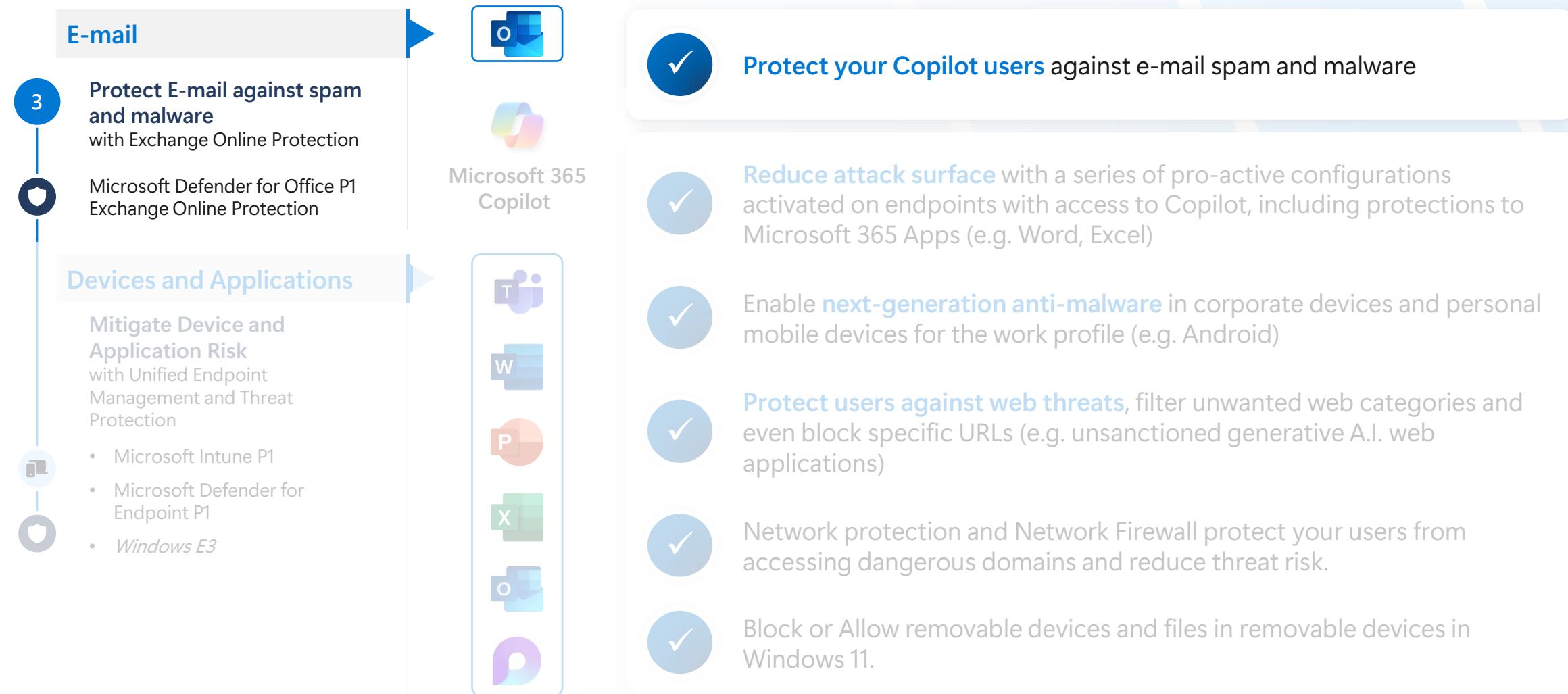
96% of phishing attacks arrive via email

3+ billion phishing emails are sent daily

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

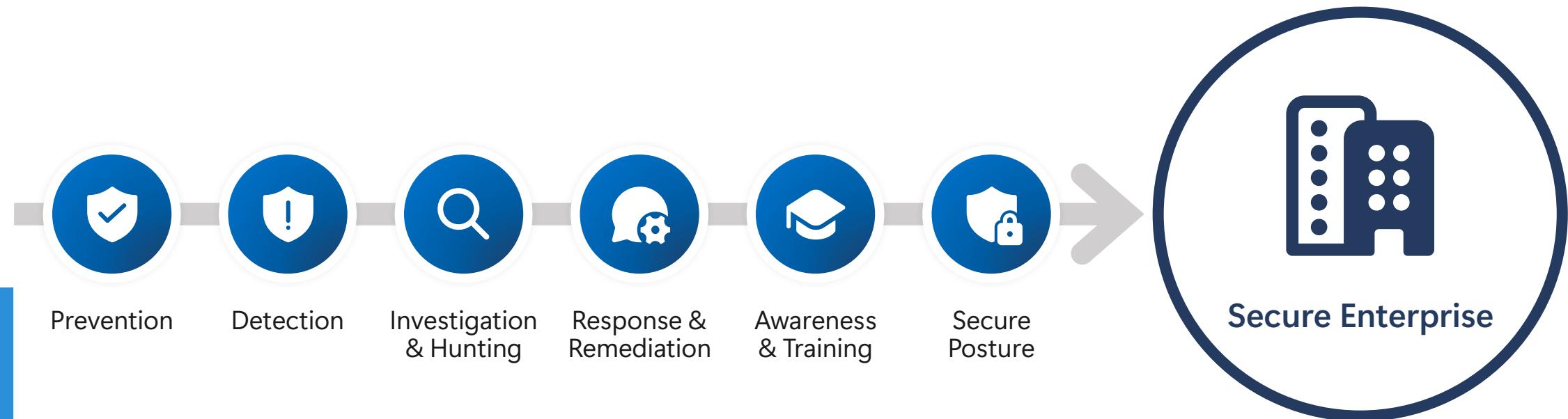
Protect E-mail, devices and apps against threats

Microsoft Defender for Endpoint P1, Exchange Online Protection



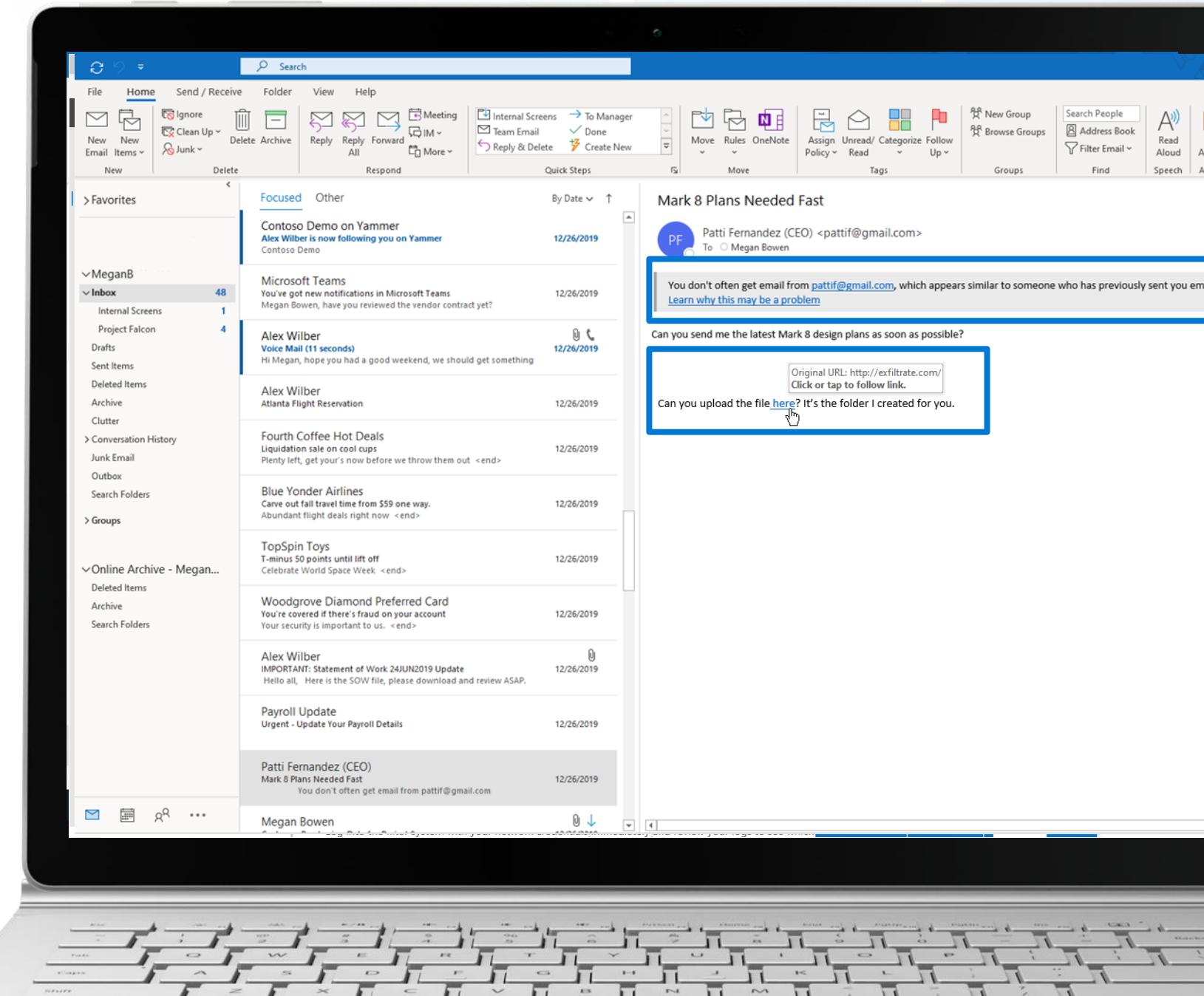
Microsoft Defender for Office 365

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 with a white shield icon containing a large white 'X'. To the right of the icon, the text "This website has been classified as malicious." is displayed. Below this, a message says "Opening this website might not be safe." followed by a URL link "http://spamlink.contoso.com". A blue button at the bottom right of the dialog box contains the text "X Close this page".

This website has been classified as malicious.

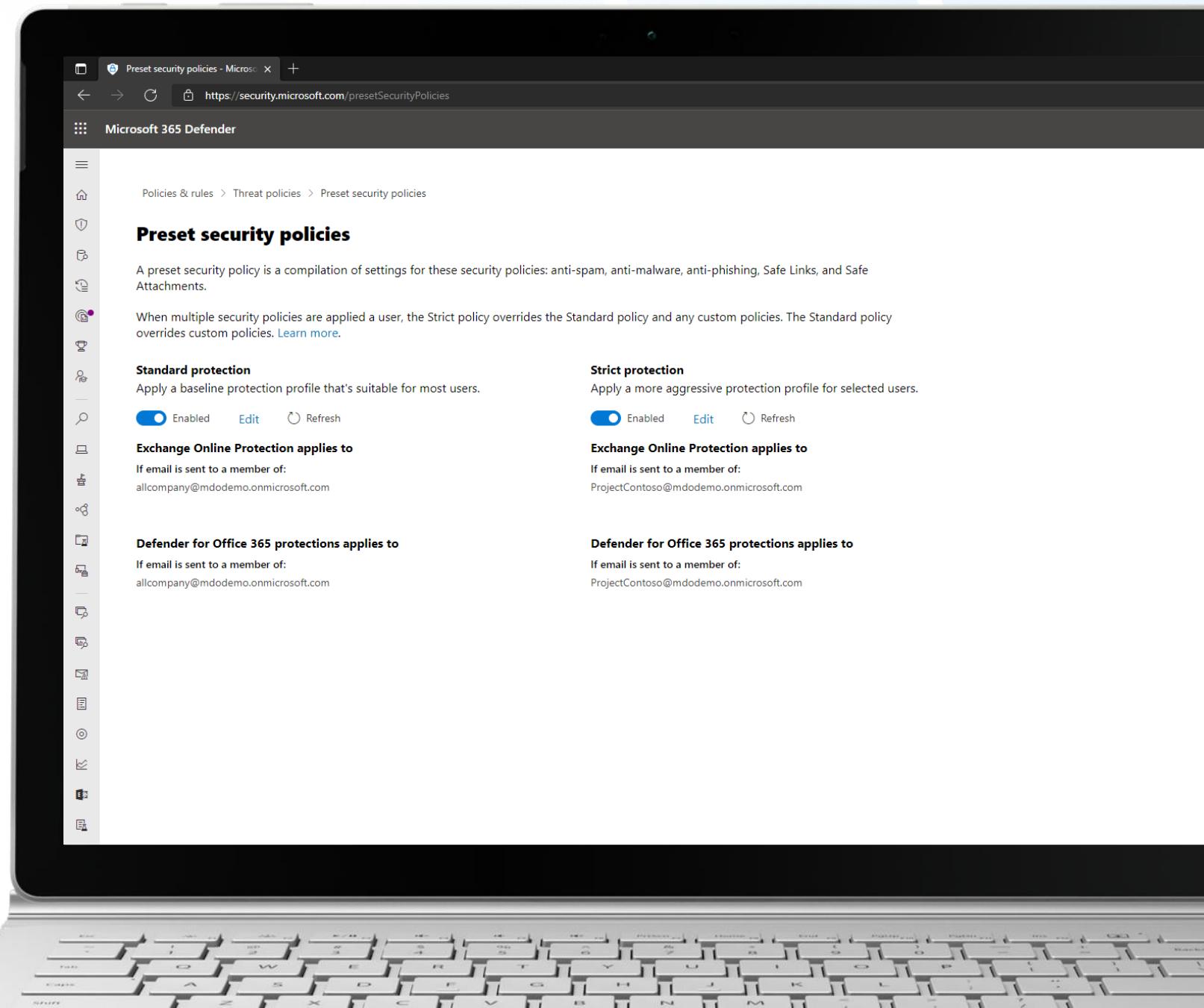
Opening this website might not be safe.

<http://spamlink.contoso.com>

X Close this page

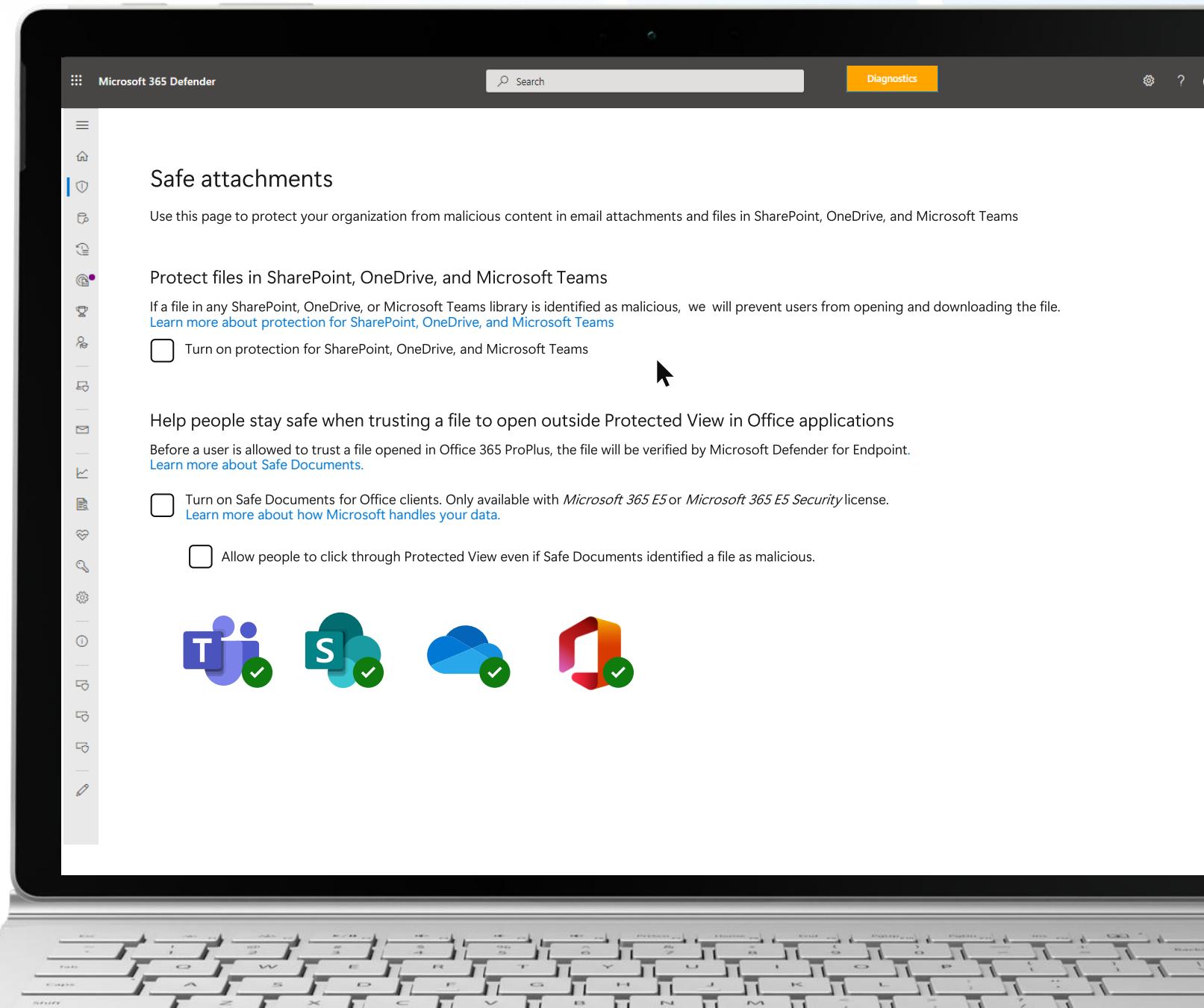
Defender for Office 365: Leveraging Preset Security Policies

- **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



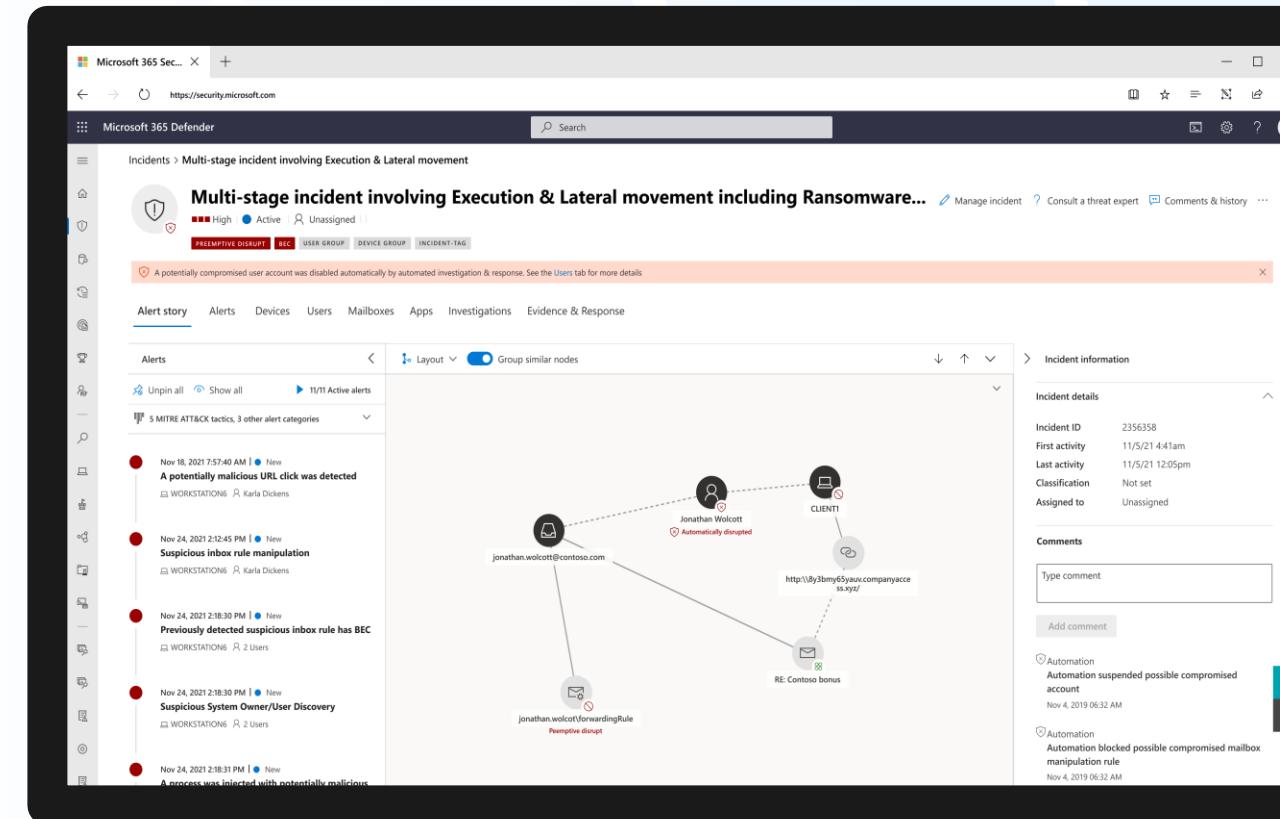
Industry first, AI-powered attack disruption to contain lateral movement of suspicious users and devices before they can act maliciously



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



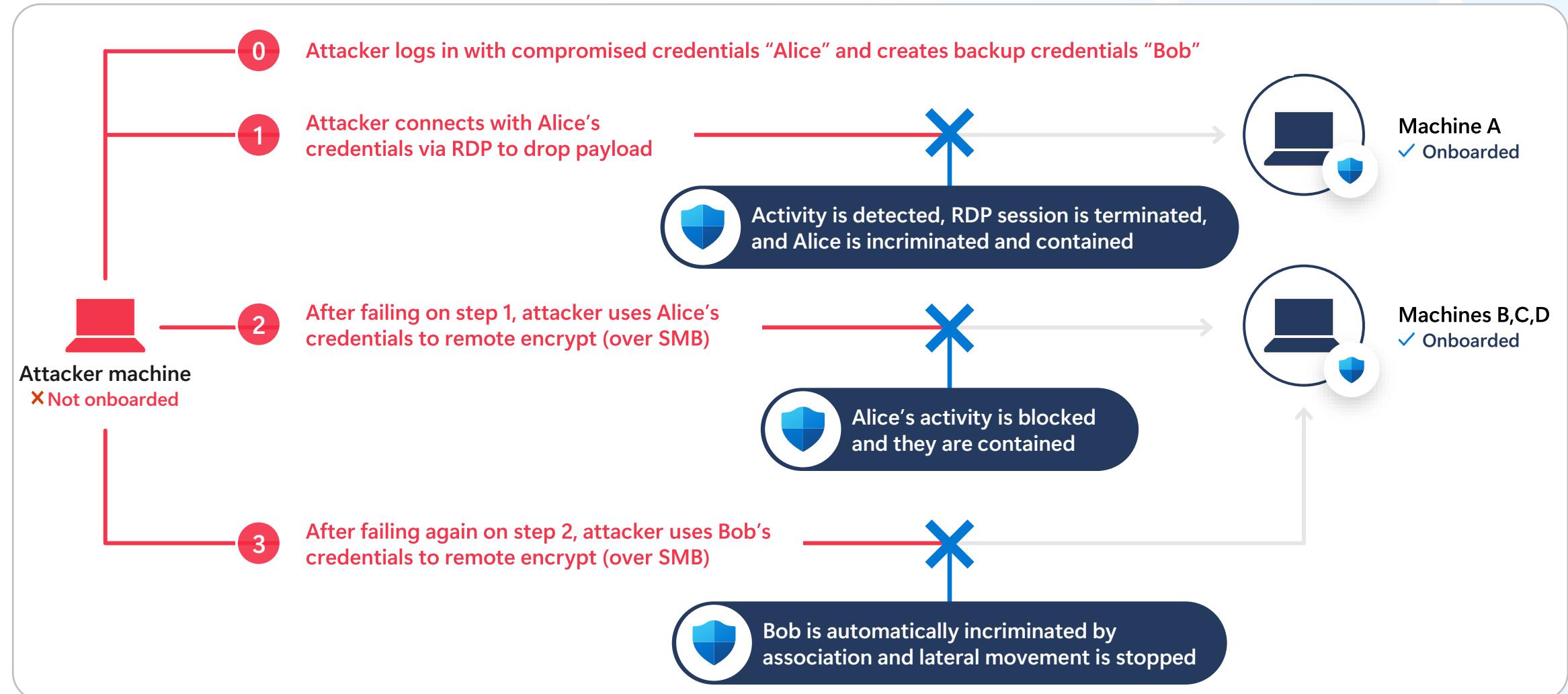
Threat and vulnerability management helps you discover, prioritize, and remediate software vulnerabilities



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

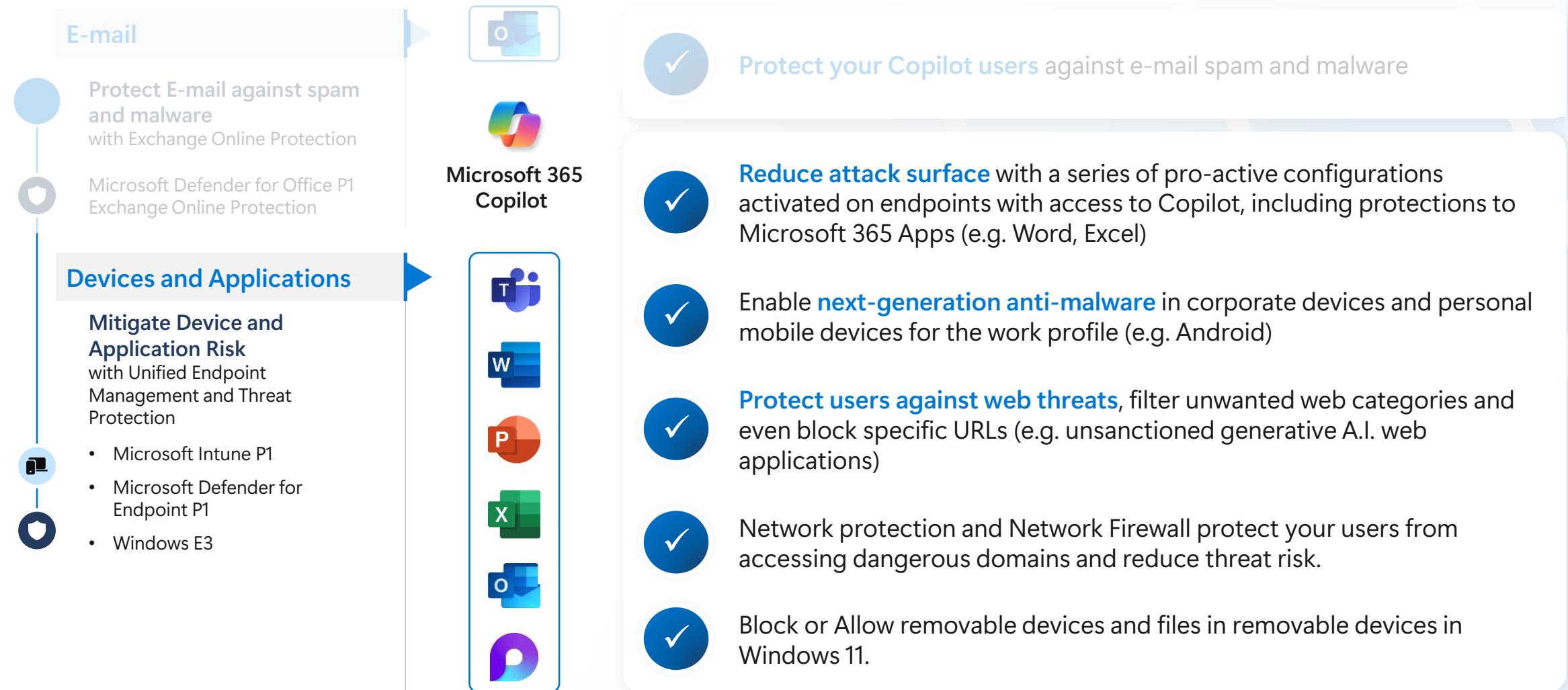


46% of compromised systems had
no malware on them

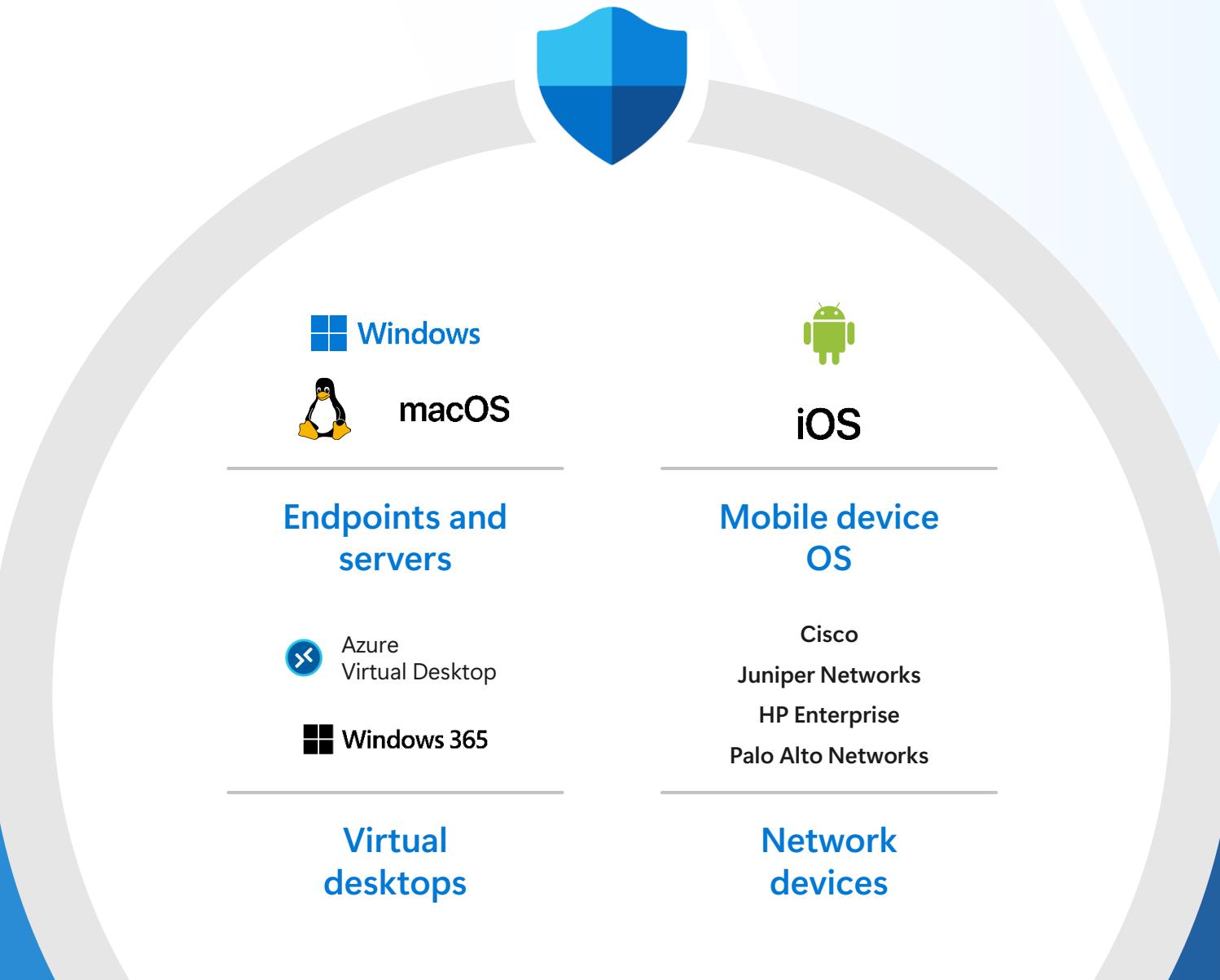
Collecting **evidence**
and alerts, even from one infected
device, can be a long **time-consuming**
process

Protect E-mail, devices and apps against threats

Microsoft Defender for Endpoint P1, Exchange Online Protection



Delivering endpoint security across platforms

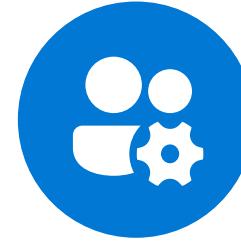


Historical roles and friction



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

Customer needs



Simple, cross-platform,
unified endpoint security
management console



Intuitive, advanced policy
management capabilities



Security controls
granularity and
completeness



Continuous assessment
and reporting of
endpoint state

Seamless and frictionless

Setup Wizard & Onboarding with Microsoft Defender for Business

Set up Copilot for Microsoft 365

Use the new Microsoft 365 Copilot setup guide, a wizard-based experience in the Microsoft 365 admin center, to help prepare your organization for Copilot for Microsoft 365:

Review the [list of prerequisites](#) and make sure they are met for your organization

Assign licenses to your users or groups

Promote Microsoft 365 Copilot features to your users with the email announcement template provided in the setup wizard

- Find this wizard in the admin center
> Home > Setup page >
- Apps and Email > Get ready for Microsoft 365 Copilot



The screenshot shows two pages of the Microsoft 365 Admin Center setup guide for Microsoft Copilot.

Top Page: The title is "Set up Microsoft Copilot for Microsoft 365". It includes a brief description of Copilot's purpose and a note that it doesn't need to be installed. It also lists "What to expect" steps: preparing the organization, assigning licenses, and sending an email announcement.

Bottom Page: The title is "Prepare your organization for Copilot". It discusses prerequisites, mentions some features are coming soon, and provides sections for adding users and viewing a readiness report. It also includes a "Prerequisites per service" section for Microsoft 365 Apps.

Attack surface reduction

Eliminate risks by reducing the surface area of attack



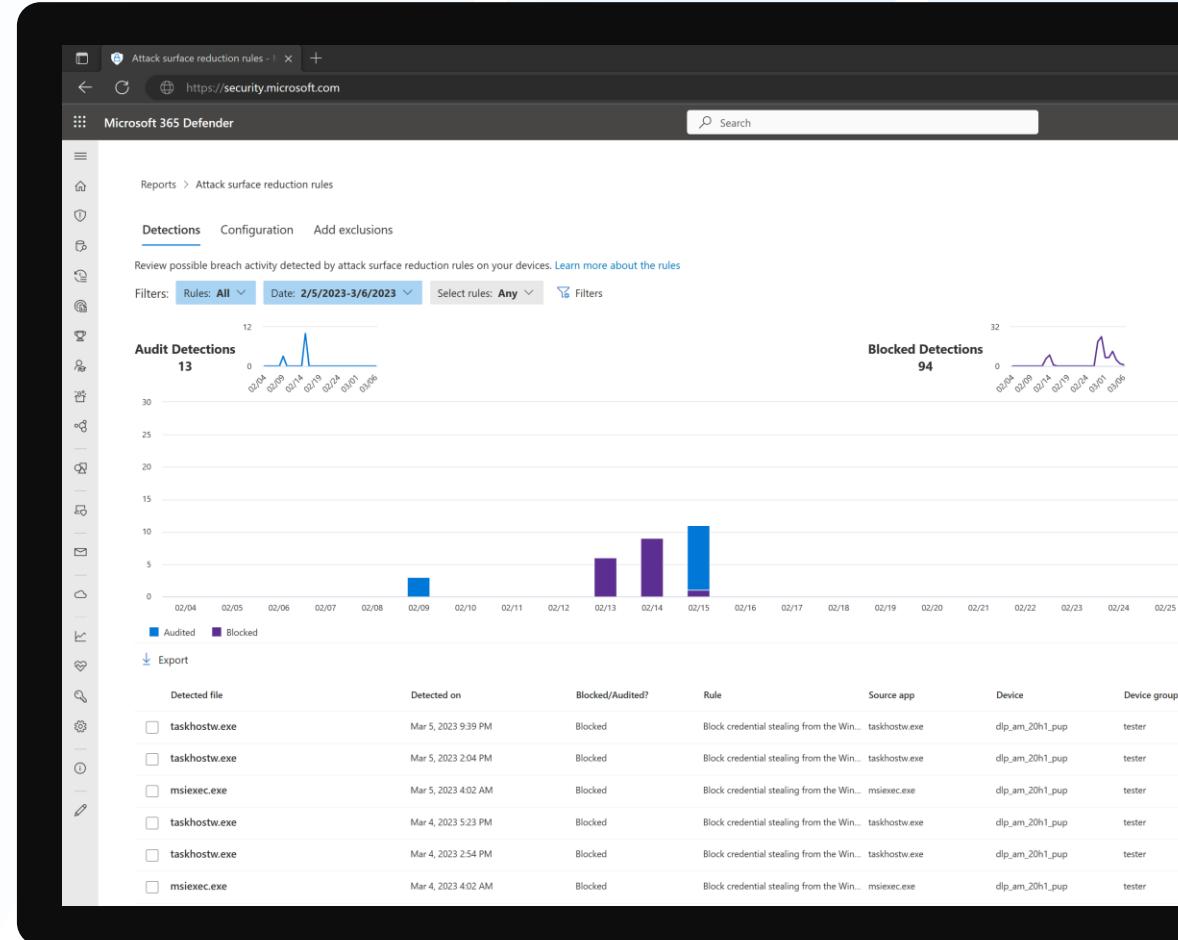
System hardening without disruption



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 for managing network endpoints. On the left, a sidebar lists various settings like 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 is titled 'Endpoints' and shows a table of 'Indicators'. The table has columns for IP address, Application, Action, Alert severity, Scope, and Expires on (UTC). It lists several entries, including some from a rich reputation database and some added by the user. A message box at the bottom right states 'Virus & threat protection' and 'Connection blocked', explaining that the IT administrator caused Microsoft Defender Security Center to block this network connection.

IP address	Application	Action	Alert severity	Scope	Expires on (UTC)
4.227.186.72		Block execution	High		
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	

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 the following columns: Incident name, Incident Id, Tags, Severity, Investigation state, Categories, Impacted assets, and Active. The table lists numerous incidents, each with a brief description and status. For example, the first incident is "Multi-stage incident on multiple endpoints" with Incident Id 45367, tags "aamaini-np-test" and "BLAKEMO", severity "High", and investigation state "2 investigation states". Other categories listed include Persistence, Malware, Unsupported OS, Defense evasion, Execution, and Ransomware. The table also includes filters for Status (New), Severity (High), and Service sources (EDR). The bottom right corner of the screenshot shows the number "674/6".

Endpoint detection & response



Correlated post-breach detection
Investigation experience
Incidents
Deception techniques
Advanced hunting

Response actions (+EDR blocks)
Deep file analysis
Live response
Threat analytics

Next generation protection

Blocks and tackles sophisticated threats and malware



Behavioral based real-time protection



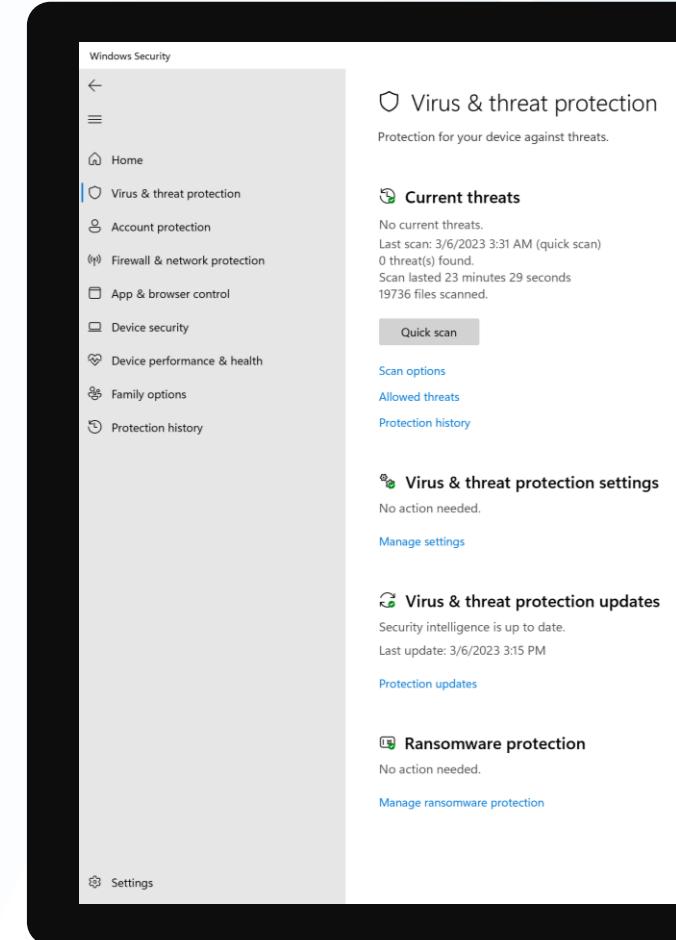
Blocks file-based and fileless malware



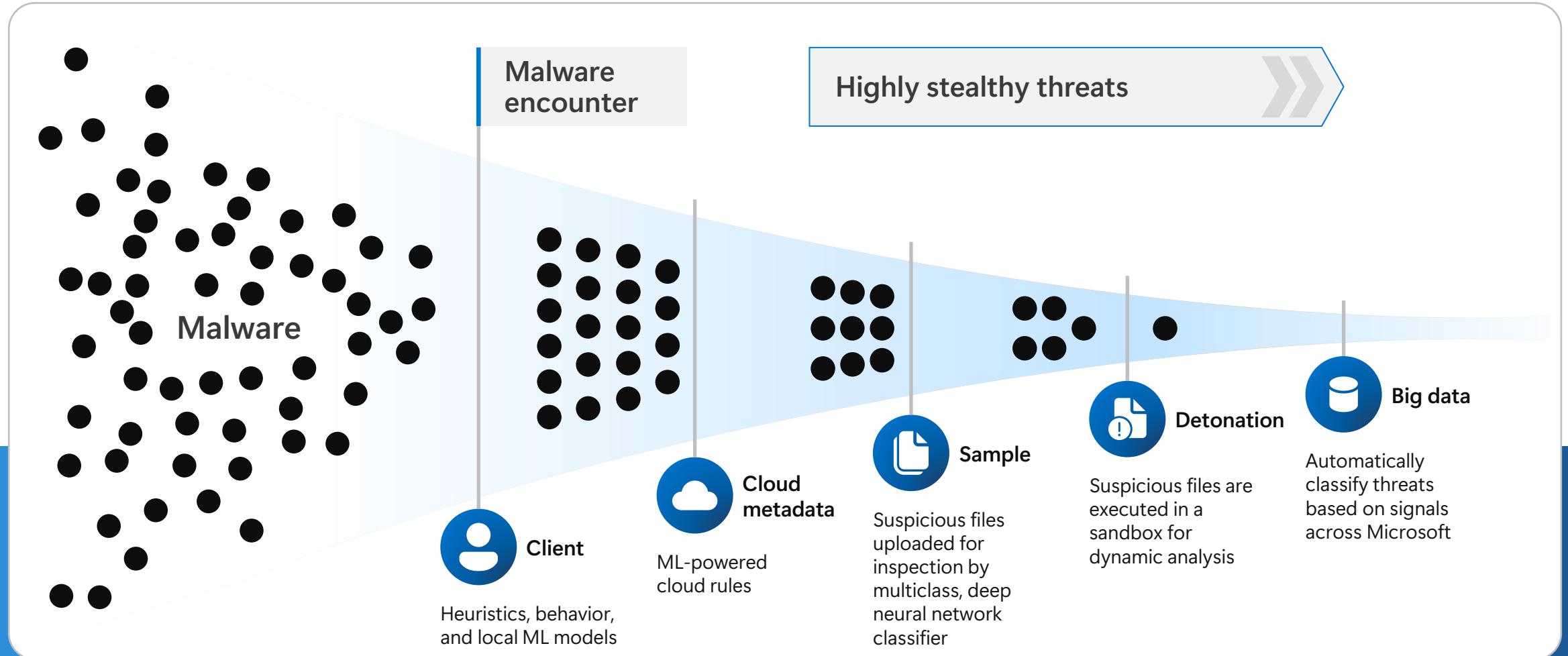
Stops malicious activity from trusted and untrusted applications



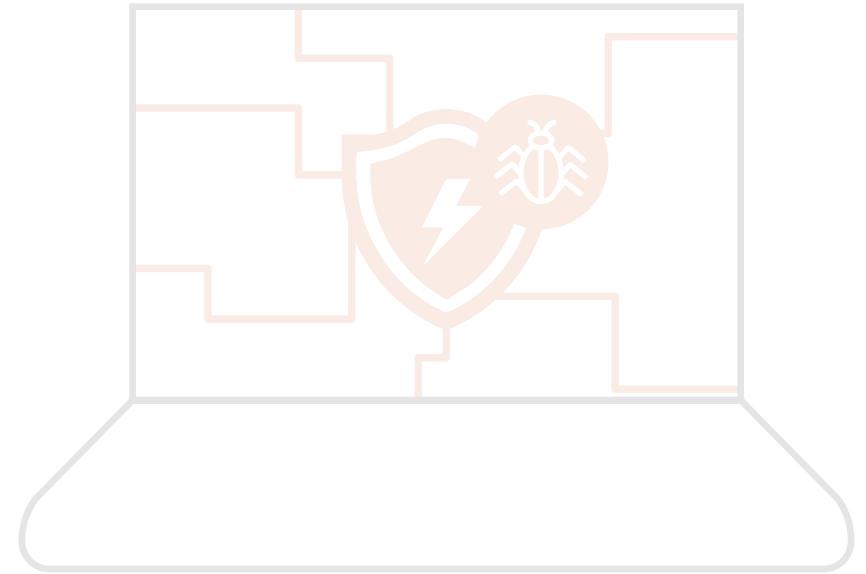
"Aced protection tests 12 months in a row." Proven protection in the field, backed up by consistent top rankings on industry comparison tests (AV-TEST, SE Labs).



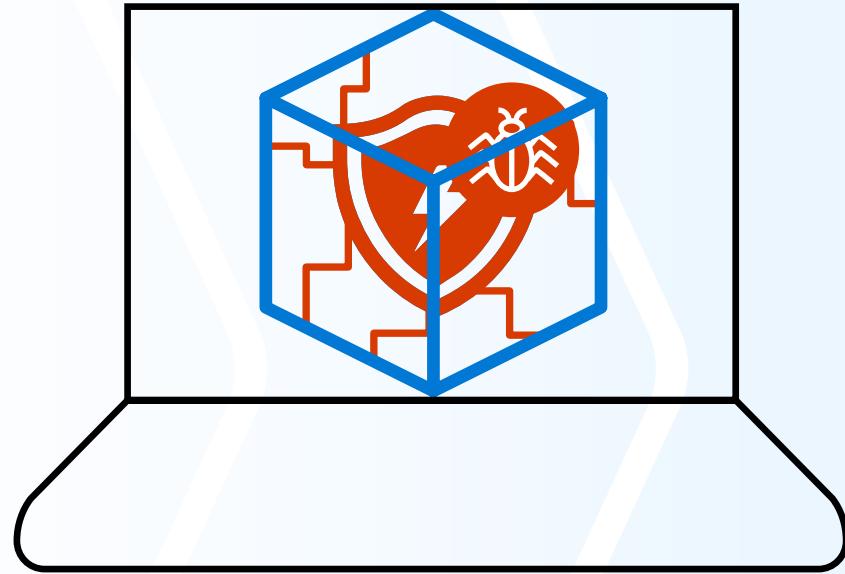
Microsoft Defender for Endpoint's NGP protection pipeline



Sandboxing of the antivirus engine



Then



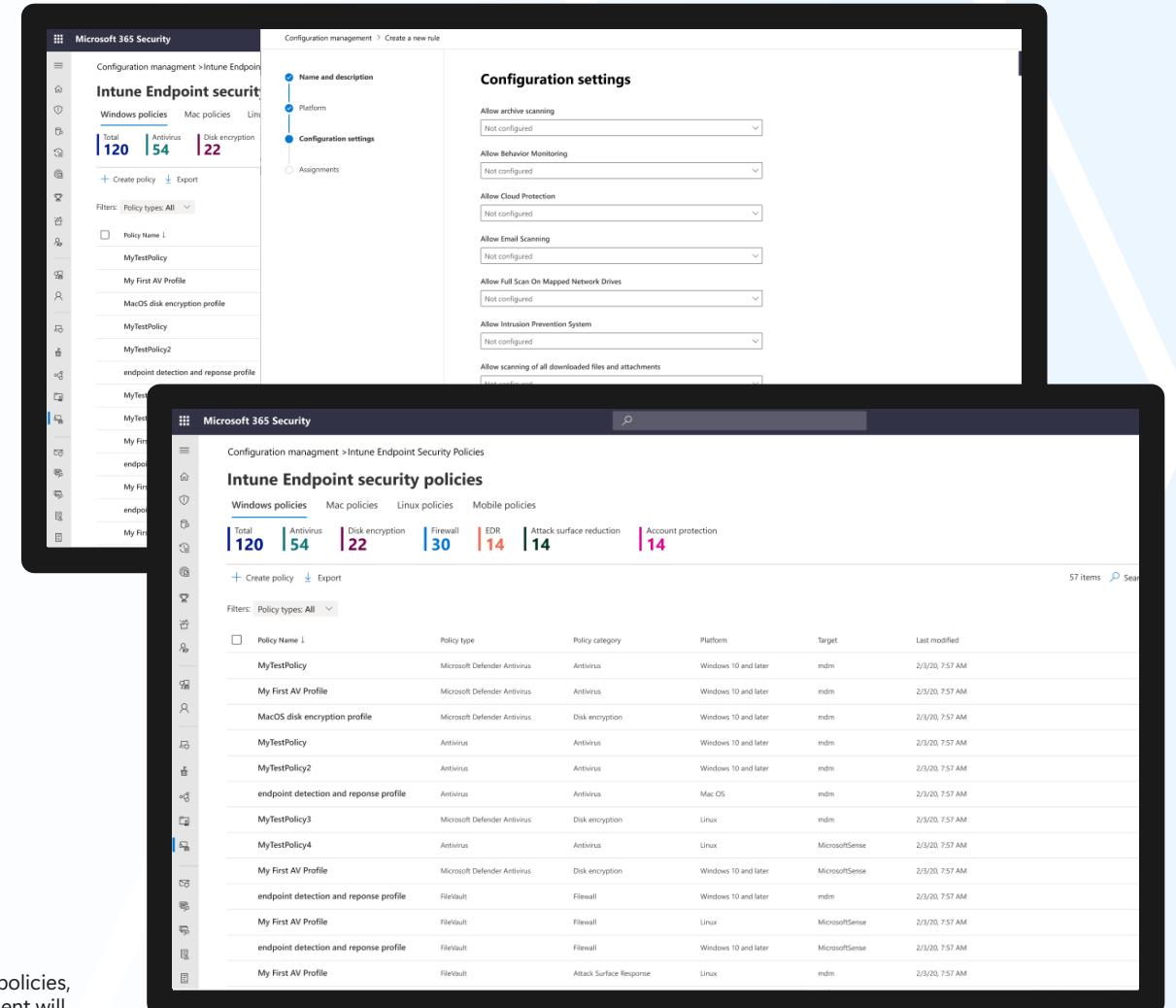
Now



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 has tabs for Windows policies, Mac policies, and Linux policies. Under the Windows policies tab, there is a table listing various security policies. The columns include Policy Name, Policy type, Policy category, Assigned, and Platform. The table lists items such as Windows Security Experience, Microsoft Defender Antivirus, Attack Surface Reduction Rules, and Microsoft Defender Antivirus entries for windows10 and windows11 platforms.

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	true	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 \(core\)](#)

Microsoft Defender Vulnerability Management dashboard

Organization exposure score
Exposure score
This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

Exposure score
23/100

Top security recommendations

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	

Top events (7 days)

Date (UTC)	Event	Originally impacted devices (%)
Feb 27, 2023 ...	Ubuntu Curl for Linux has 3 new vulnerabilities, impacting 111 devices	111 (10%)
Feb 27, 2023 ...	Ubuntu Libcurl4 for Linux has 3 new vulnerabilities, impacting 111 devices	111 (10%)
Feb 27, 2023 ...	Ubuntu Libcurl3-gnutls for Linux has 3 new vulnerabilities, impacting 111 devices	111 (10%)

Top remediation activities
Remediation activities
This table lists top activities that were generated from security recommendations

Activity	Count
Block Office communication application from creating child processes	37/87

Top vulnerable software

Software	OS platform	Weaknesses	Threats	Exposed devices
Edge Chromium-based	Other	913	0	213 / 469
Tar for Linux	Linux	1	0	94 / 130
Safari for Mac	MacOS	34	0	63 / 69

Top exposed devices

Name	Score
symantec1	49.2%
wtcf0227-r0-cf	46.8%
wtcf0227-r0-wt	49.2%

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 platform. The top half shows a list of incidents, each with a summary, severity (e.g., High, Medium), investigation state, categories, impacted assets, active alerts, service sources, and detection details. One incident is selected, shown in a detailed view below. The detailed view includes sections for Alerts and categories (73/73 active alerts, 1 MITRE ATT&CK tactics, 1 other alert categories), Scope (20 impacted devices, 12 impacted users), Top impacted entities (listing various user and device accounts with risk levels), and Evidence (listing 187 entities found). On the right side, there is an Incident Information panel with various metadata fields.

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 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	Red	0	Sep 17, 2017, 2:05 AM	+
Multiple failed user log on attempts to an app	Red	0	Sep 17, 2017, 2:05 AM	+
General anomaly detection	Red	0	Sep 17, 2017, 2:05 AM	+
New high upload volume app	Red	0	Sep 17, 2017, 2:05 AM	+
Mass download by a single user	Red	0	Sep 17, 2017, 2:05 AM	+
New high volume app	Red	0	Sep 17, 2017, 2:05 AM	+
Logon from a risky IP address	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

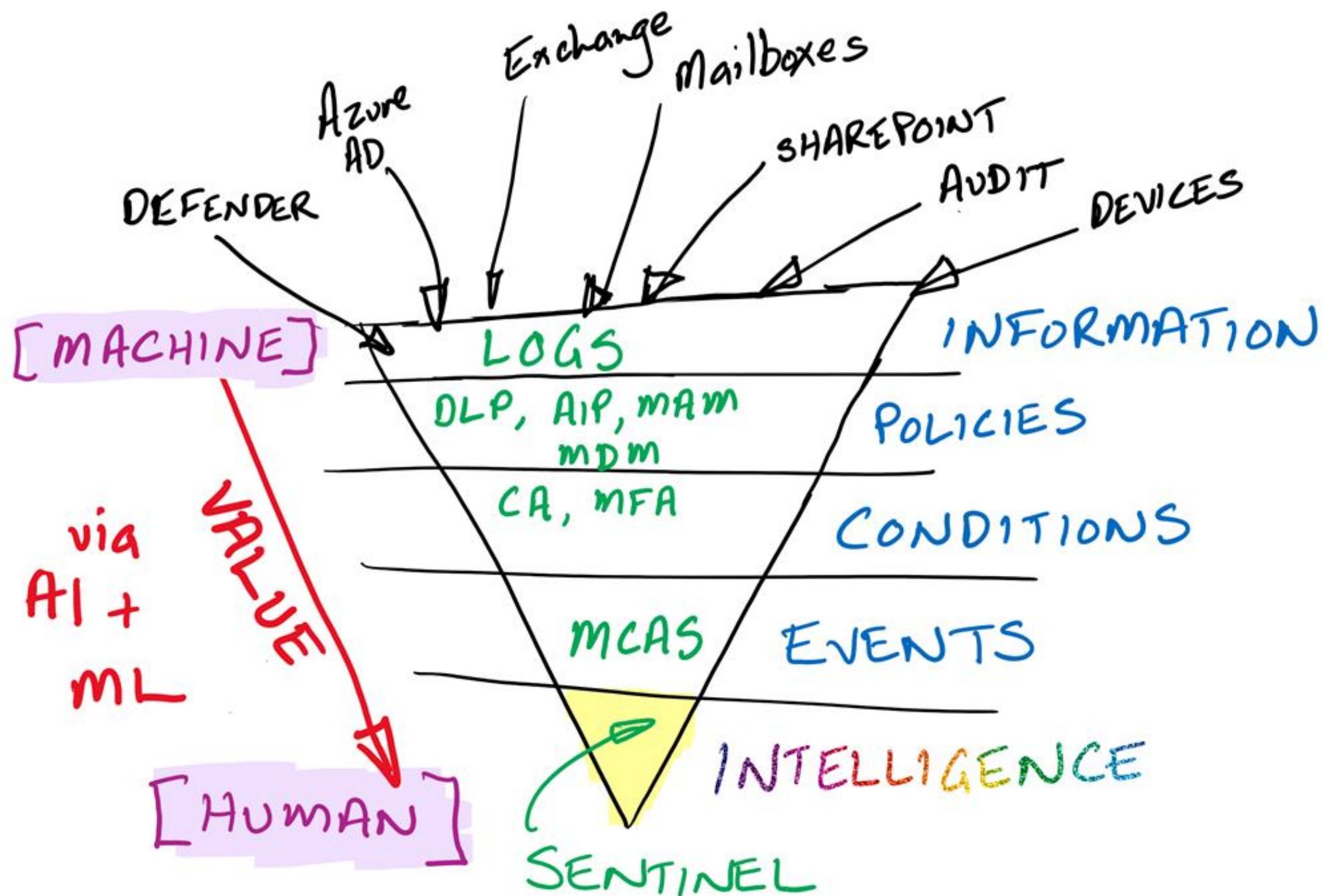
Assess risk cloud apps based on ~60 security and compliance risk factors.

On-going analytics & anomaly detection

Get anomalous usage alerts, new app and trending apps alerts

The image displays two devices showing the Microsoft Cloud App Security interface. The top device is a monitor showing the 'Cloud Discovery' dashboard. Key statistics include 557 Apps, 1173 Users, 2540 IP addresses, and 314.4 GB Traffic (with 60.4 GB highlighted in red). Below these are charts for App categories (e.g., Collaboration, Online meetings, CRM, Cloud storage, Social network) and Discovered apps (e.g., Office 365, Microsoft Skype for Business, Microsoft Dynamics, Notion, Zapier, Facebook, Giphy, Twinkl, SendGrid, Oxygen Cloud, Drive). The bottom device is a tablet showing the 'Files' section, listing various files and their details such as owner, access level, and last modified date.

Intelligence vs Information



Introducing Microsoft Sentinel

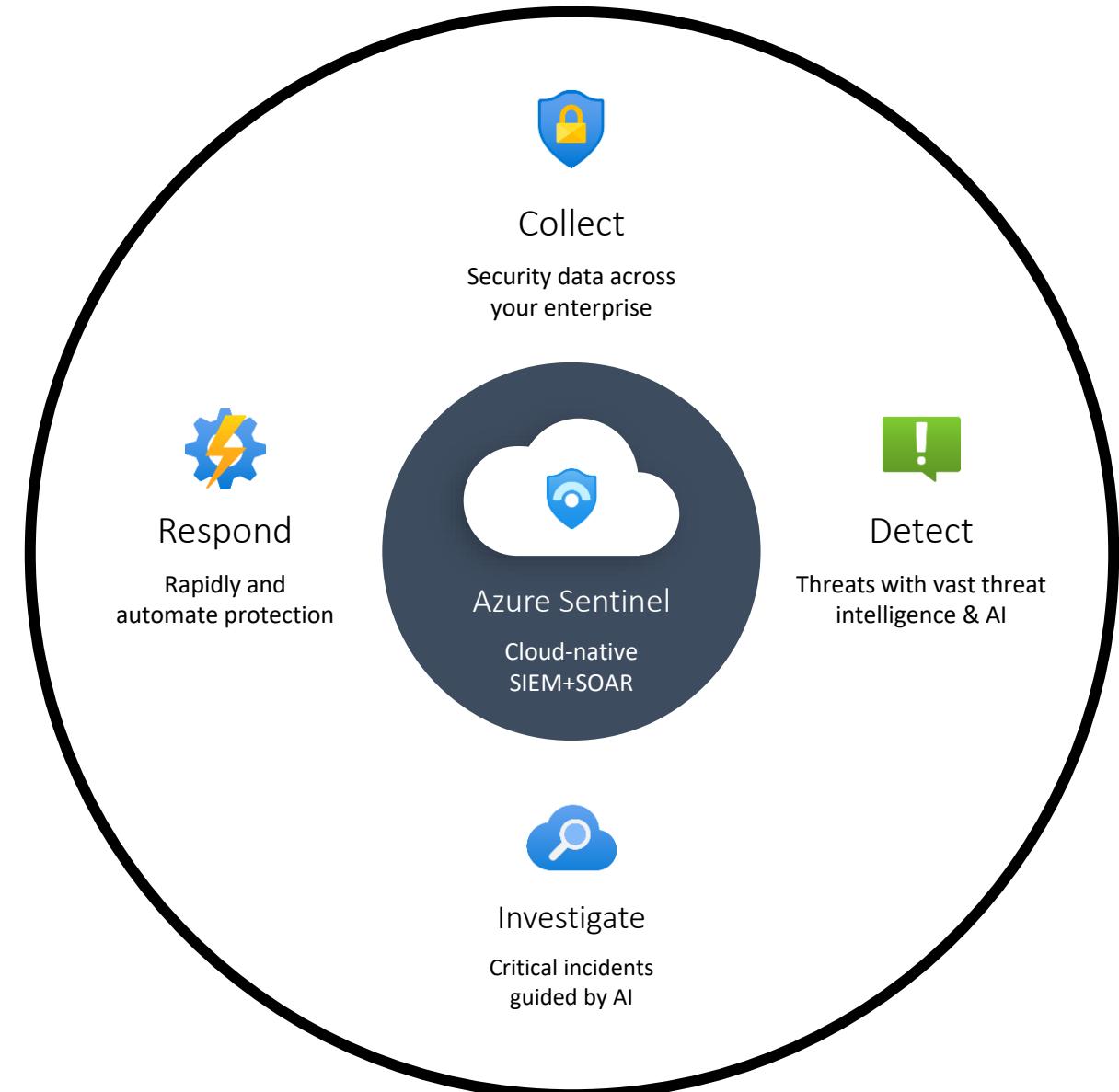
Cloud-native SIEM for intelligent security analytics for your entire enterprise

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](#)



Search (Ctrl+F)

General

Overview

Logs

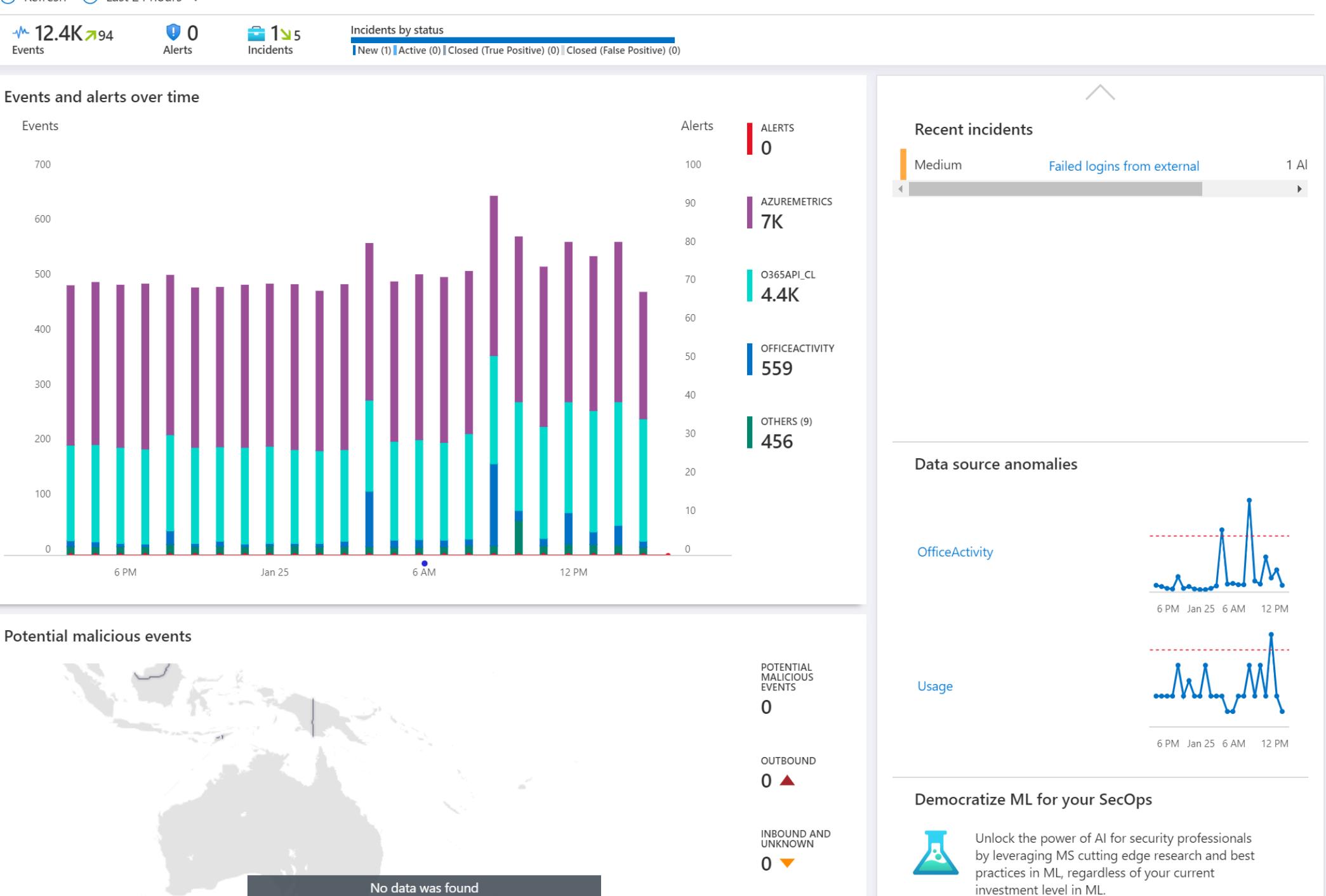
News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior
- Threat intelligence (Preview)

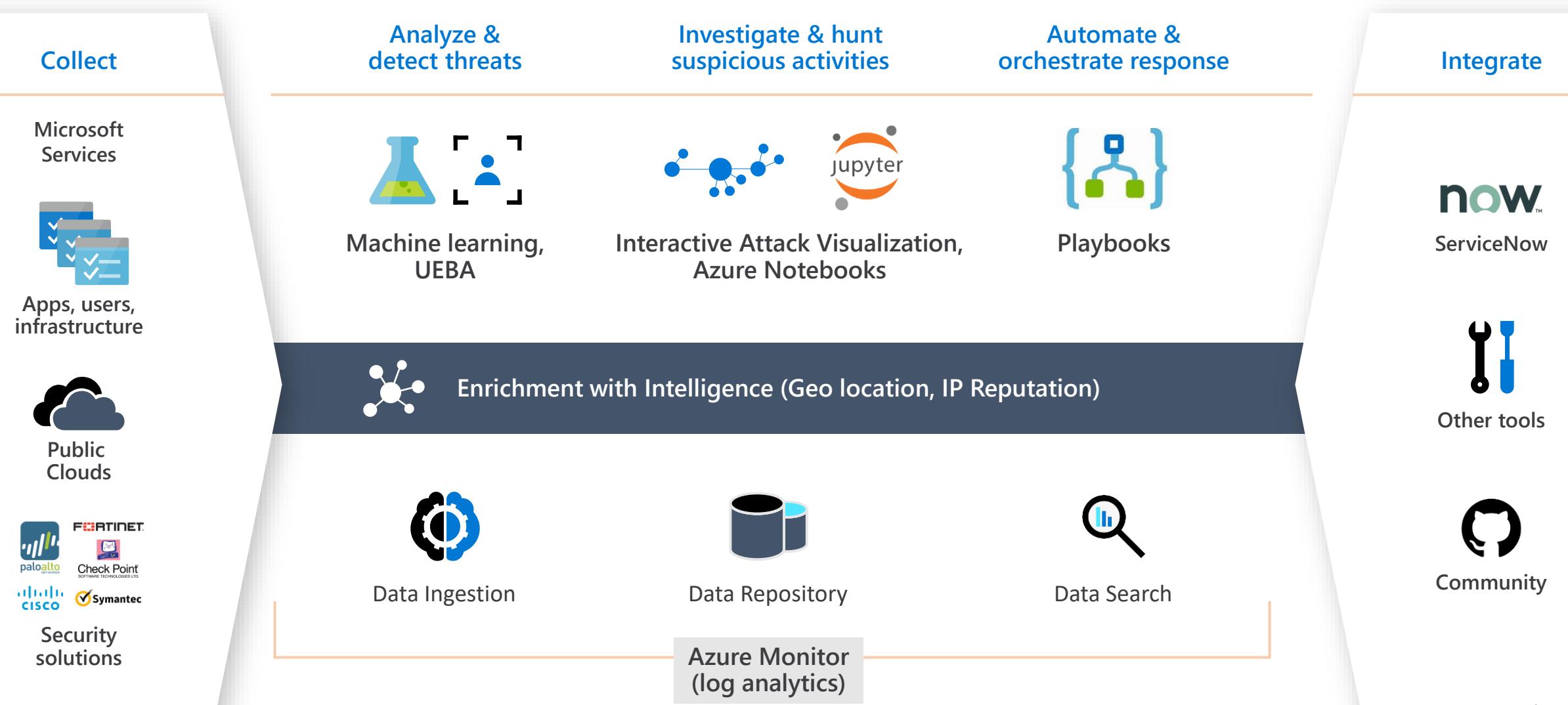
Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings





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**



Microsoft Azure Search resources, services, and docs (G+) 1 ? ? admin@ciaops365.com CIAOPS (CIAOPS365.COM)

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Data connectors

Selected workspace: 'ciaops'

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings

74 Connectors 8 Connected 0 Coming soon

Search by name or provider Providers: All Data Types: All Status: All

Status ↑ Connector name ↑

	AI Vectra Detect (Preview) Vectra AI
	Alcide kAudit (Preview) Alcide
	Amazon Web Services Amazon
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Azure DDoS Protection Microsoft
	Azure Defender Microsoft
	Azure Defender for IoT Microsoft
	Azure Firewall Microsoft

Azure Active Directory

Connected Status	Microsoft Provider	Last Log Received
		2 hours ago Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received
01/25/21, 02:00 PM

Related content

- 6 Workbooks
- 2 Queries
- 36 Analytic rules templates

Data received

Go to log analytics

Legend: SigninLogs AuditLogs

Total data received

January 17 January 24

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics**
- Watchlist (Preview)
- Playbooks
- Community
- Settings

Search

Severity : All Rule Type : All Status : All Tactics : All

SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓	STATUS ↑↓	TACTICS
High	Known Strontium group domains	Scheduled	Enabled	Command and Control
High	Known IRIDIUM IP	Scheduled	Enabled	Command and Control
High	Known Phosphorus group domains/IP	Scheduled	Enabled	Command and Control
High	Create incidents based on Azure Security Center al...	Microsoft Security	Enabled	
High	Create incidents based on Azure Active Directory l...	Microsoft Security	Enabled	
High	Advanced Multistage Attack Detection	Fusion	Enabled	Collection, Command and Control, Data Exfiltration
High	Create incidents based on Azure Advanced Threat ...	Microsoft Security	Enabled	
High	Create incidents based on Microsoft Defender Adv...	Microsoft Security	Enabled	
High	Create incidents based on Microsoft Cloud App Se...	Microsoft Security	Enabled	
High	Known Manganese IP and UserAgent activity	Scheduled	Enabled	Defense
High	Create incidents based on Office 365 Advanced Th...	Microsoft Security	Enabled	
High	Suspicious application consent similar to O365 Att...	Scheduled	Enabled	Credential Access
High	First access credential added to Application or Ser...	Scheduled	Enabled	Credential Access
Medium	Failed AzureAD logons but success logon to host	Scheduled	Enabled	Defense
Medium	Malware in the recycle bin	Scheduled	Enabled	Defense
Medium	CIAOPS - URL detonation	Scheduled	Enabled	
Medium	Suspicious number of resource creation or deploy...	Scheduled	Enabled	Impact
Medium	SSH Potential Brute Force	Scheduled	Enabled	Credential Access
Medium	Rare high NXDomain count	Scheduled	Enabled	Command and Control
Medium	SharePointFileOperation via devices with previousl...	Scheduled	Enabled	Exfiltration
Medium	Process executed from binary hidden in Base64 en...	Scheduled	Enabled	Collection, Credential Access
Medium	Brute force attack against Azure Portal	Scheduled	Enabled	Credential Access
Medium	SSH newly internet-exposed endpoints	Scheduled	Enabled	Initial Access
Medium	Multiple users email forwarded to same destination	Scheduled	Enabled	Collection, Data Exfiltration
Medium	User account created and deleted within 10 mins	Scheduled	Enabled	Collection, Command and Control
Medium	Sign-in from IP that attempt to gain initial access	Scheduled	Enabled	Collection, Command and Control

High Severity Enabled Status

Id: d0fe6fe9-d84d-4186-aab1-f05ca5c32994

Description: Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents, OfficeActivity and VMConnection dataTypes. References: <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/>.

Tactics: Command and Control

Rule query:

```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org", "accounts-web-mail.com", "customer-certificate.com", "yahoo-verification.net", "yahoo-verify.net", "outlook.com-identifier-service.log.name", "microsoft-update.b", "confirm-session-identifier.info", "session-managemen
```

Rule frequency: Run query every **1 day**

Rule period: Last **1 day** data

Rule threshold: Trigger alert if query returns **more than 0** results

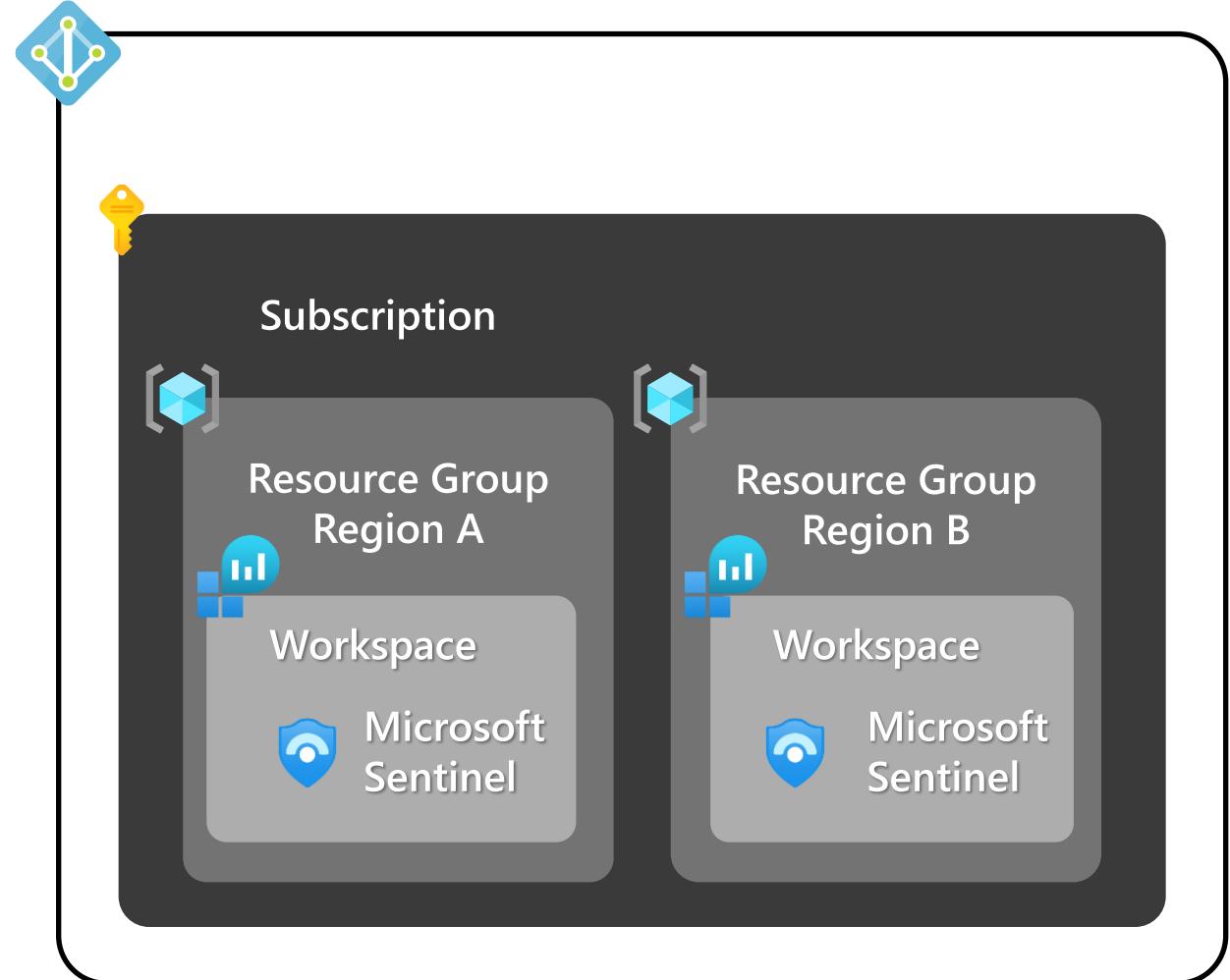
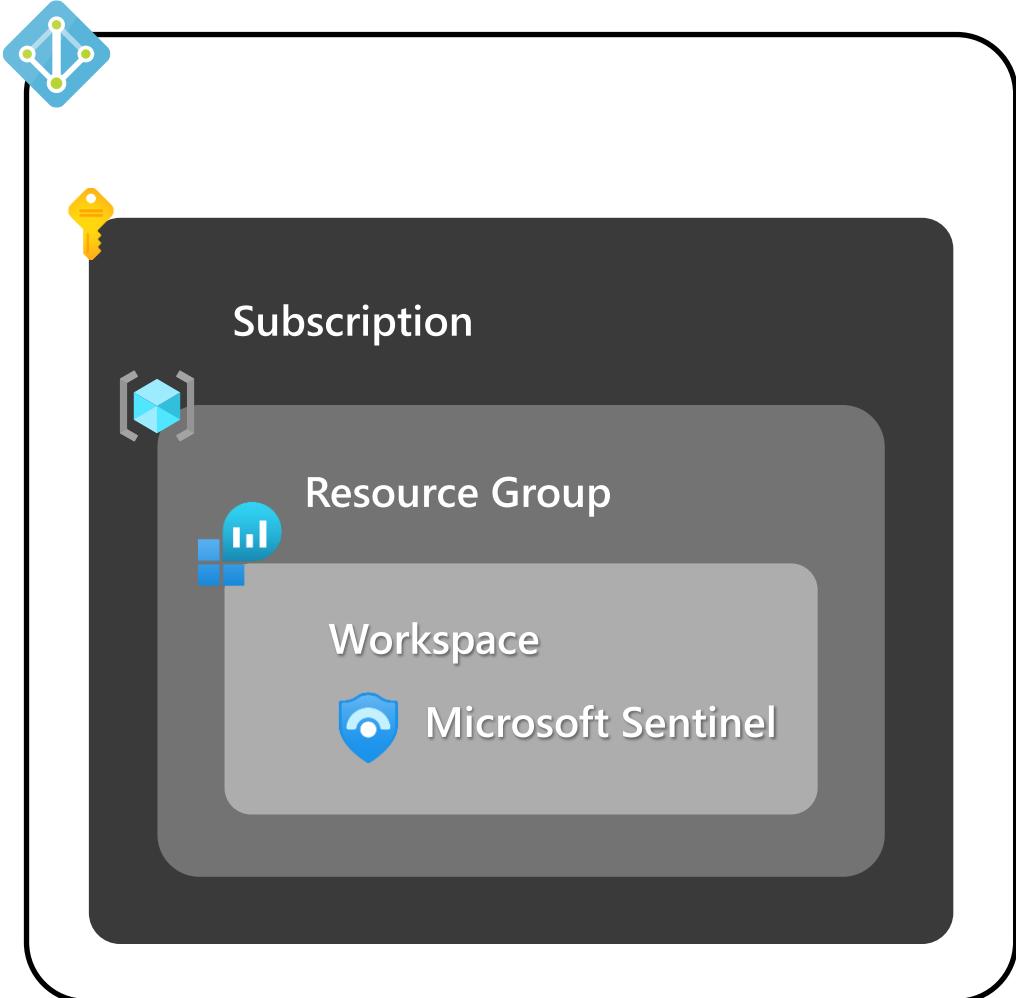
Event grouping: Group all events into a single alert

Suppression: Not configured

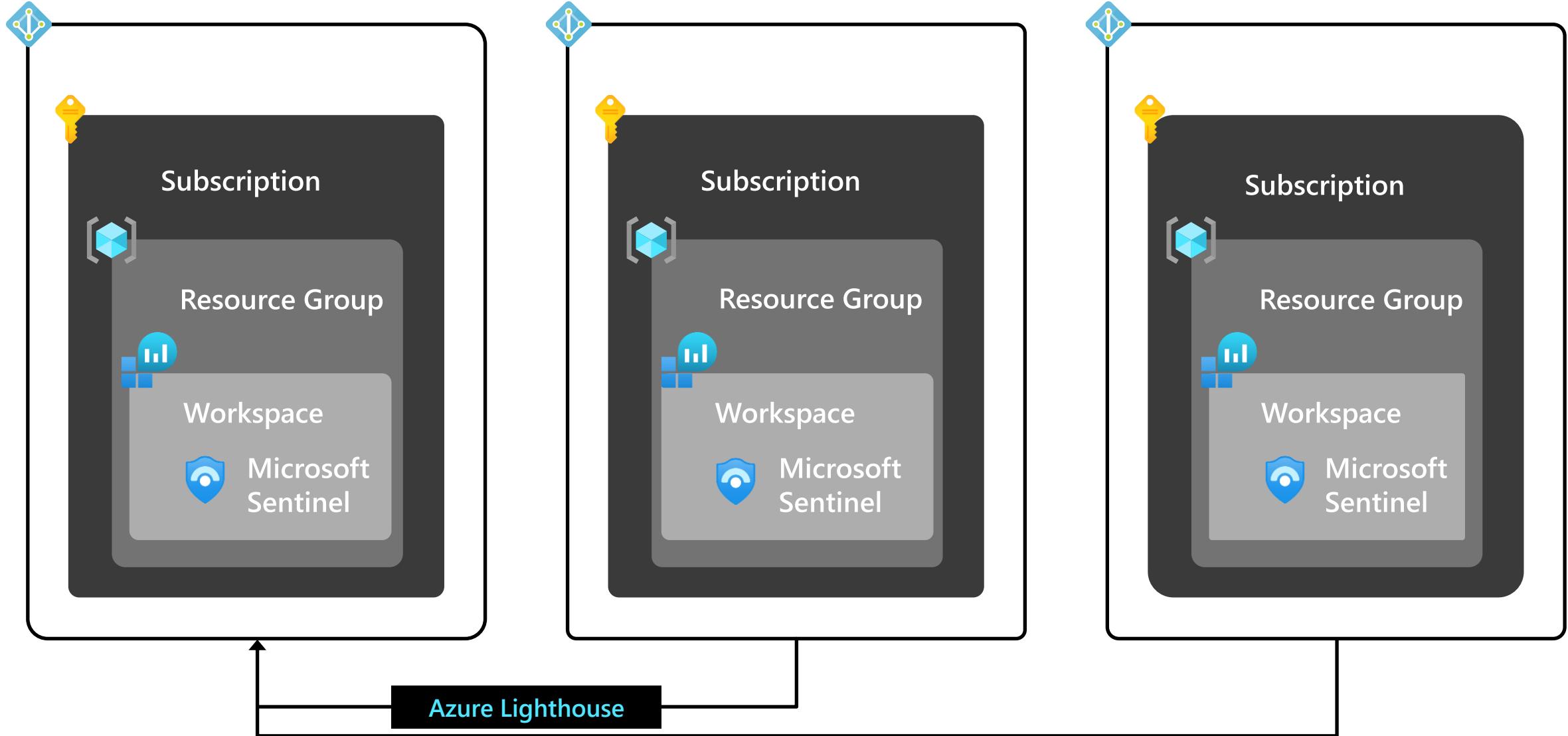
Create incidents from this rule: Enabled

Alert grouping: Disabled

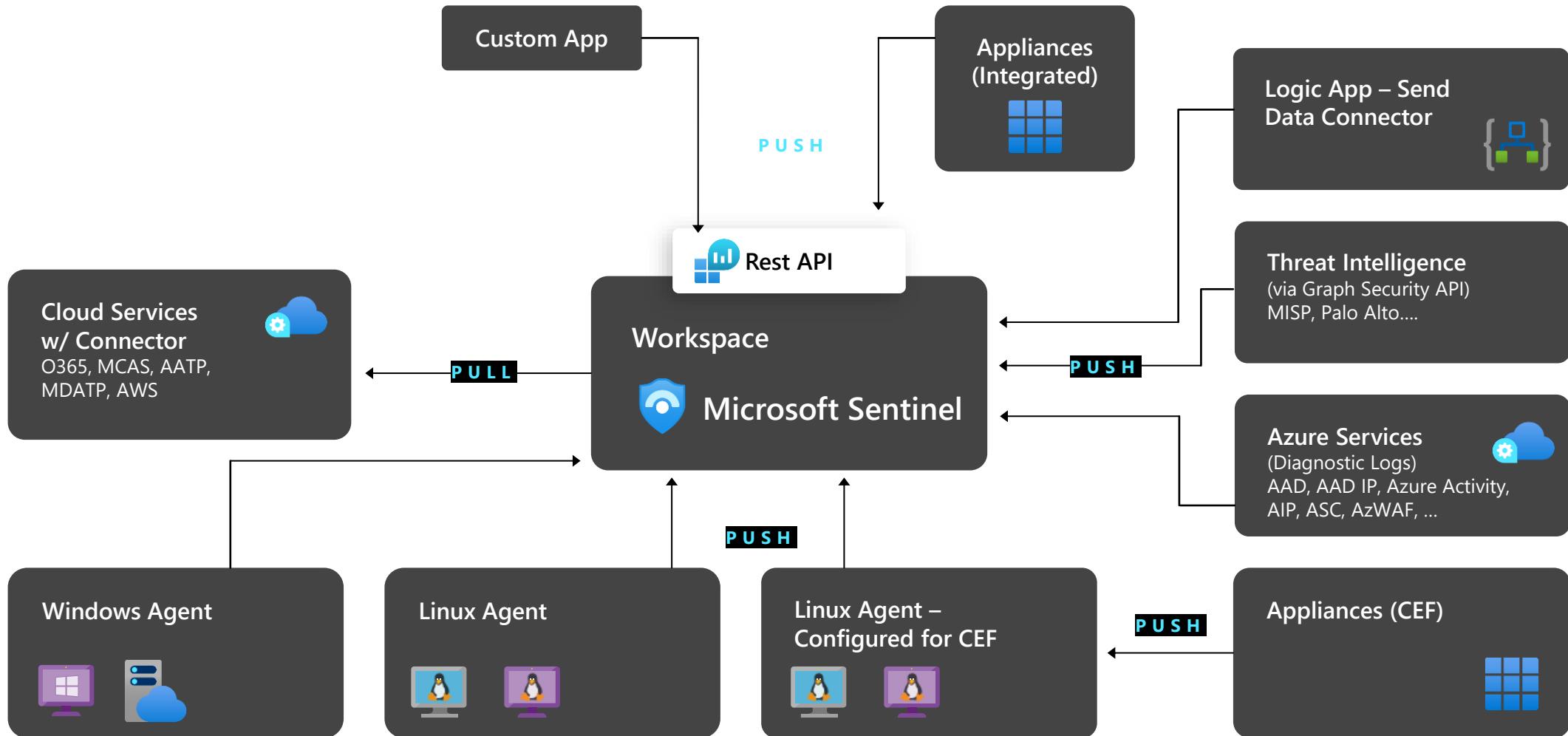
Workspace Design (Single Tenant)



Workspace Design (Multi-Tenant)



All the ways data gets in



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

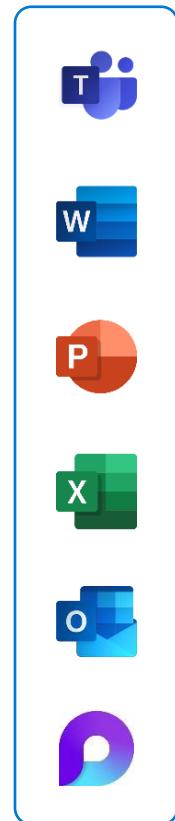
Security and privacy are the top concerns for organizations to use generative AI tools²

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



- ✓ 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 weeks



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**



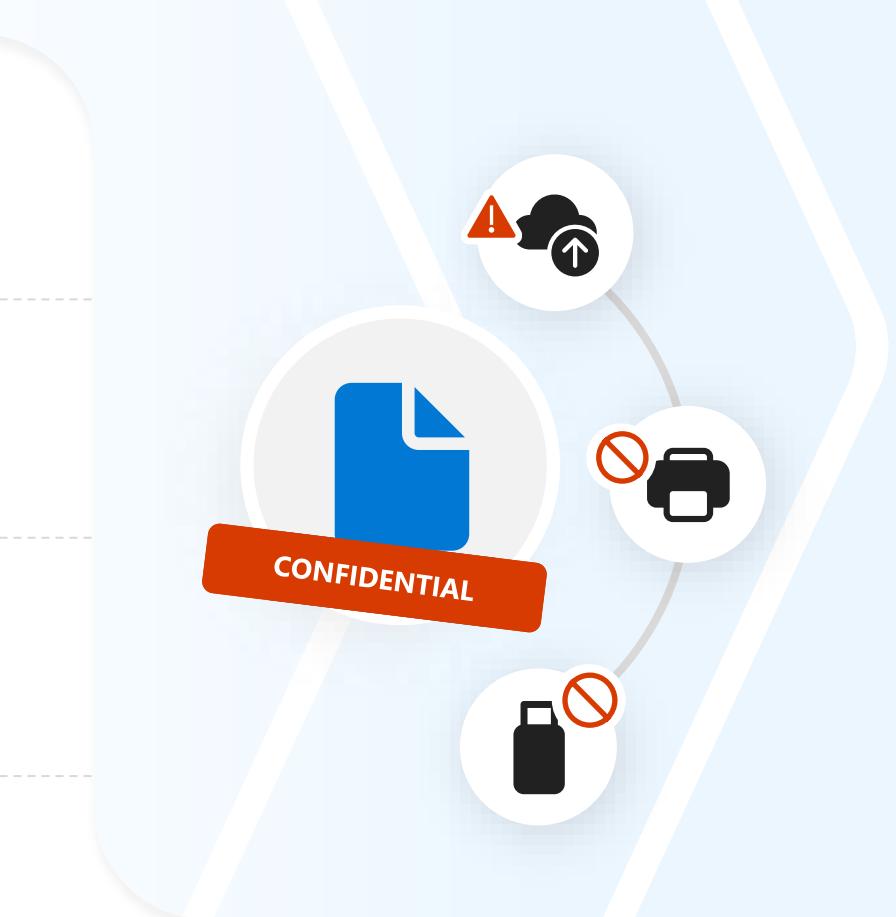
Integrated

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

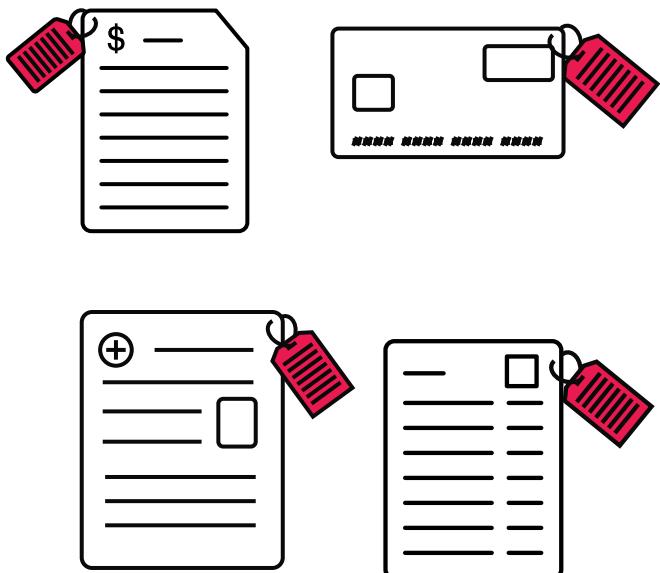


Integrated insights and alerting

Enrich policy and investigation with rich signals

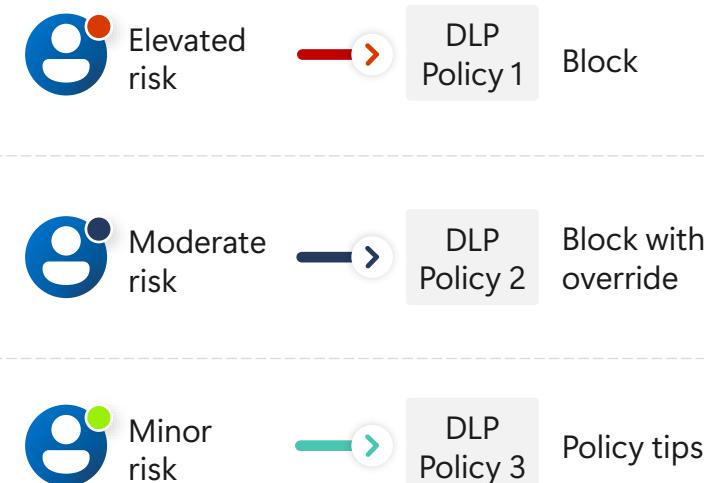
Know the context

Leverage classification and labeling on sensitive data from Information Protection



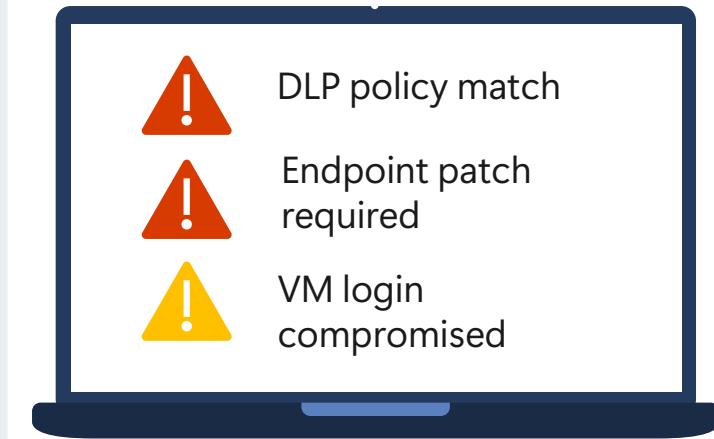
Understand the intent

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

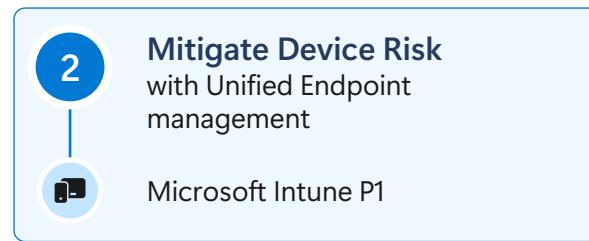
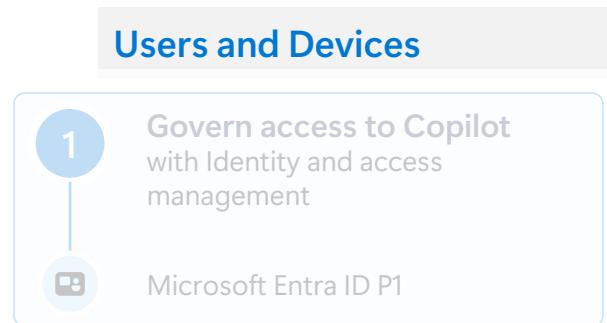
The number of password attacks Microsoft has detected increased to more than **7,000 per second in 2024**, due to unmanaged devices.²

1. [Microsoft Security Blog 2024](#)

2. Microsoft Digital Defense Report 2024

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.

Traditional Windows deployment | The legacy way



Build a custom image,
gathering everything else
that's necessary to deploy



Deploy image to a new
computer, overwriting what
was originally on it

Time means money, making
this an expensive
proposition

Modern Windows deployment | The new way



Un-box and turn on
off-the-shelf Windows PC

Transform with minimal
user interaction

Device is ready
for productive use

Endpoint management has evolved to address the world's trends for today

Disjointed management
of mobile and desktop
devices

Integrated security
solutions for endpoints

Leverage AI and analytics
to prevent, detect and
respond

A cloud-native approach powers your AI-enabled future.

Unified management
across all devices

Migration to cloud-based
management

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

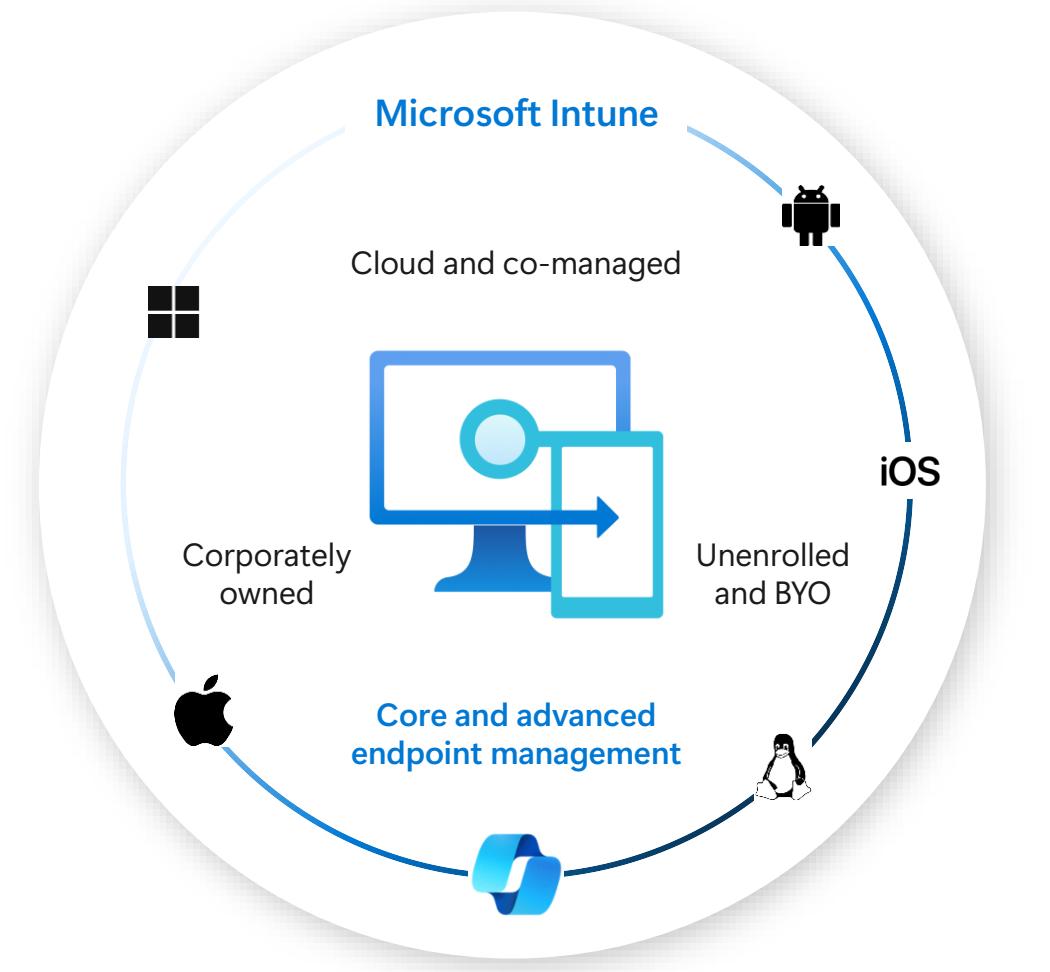
Cut cost and complexity by shifting to the cloud, unifying endpoint management and security tools in one place.

Fortify Zero Trust security

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

Power better experiences

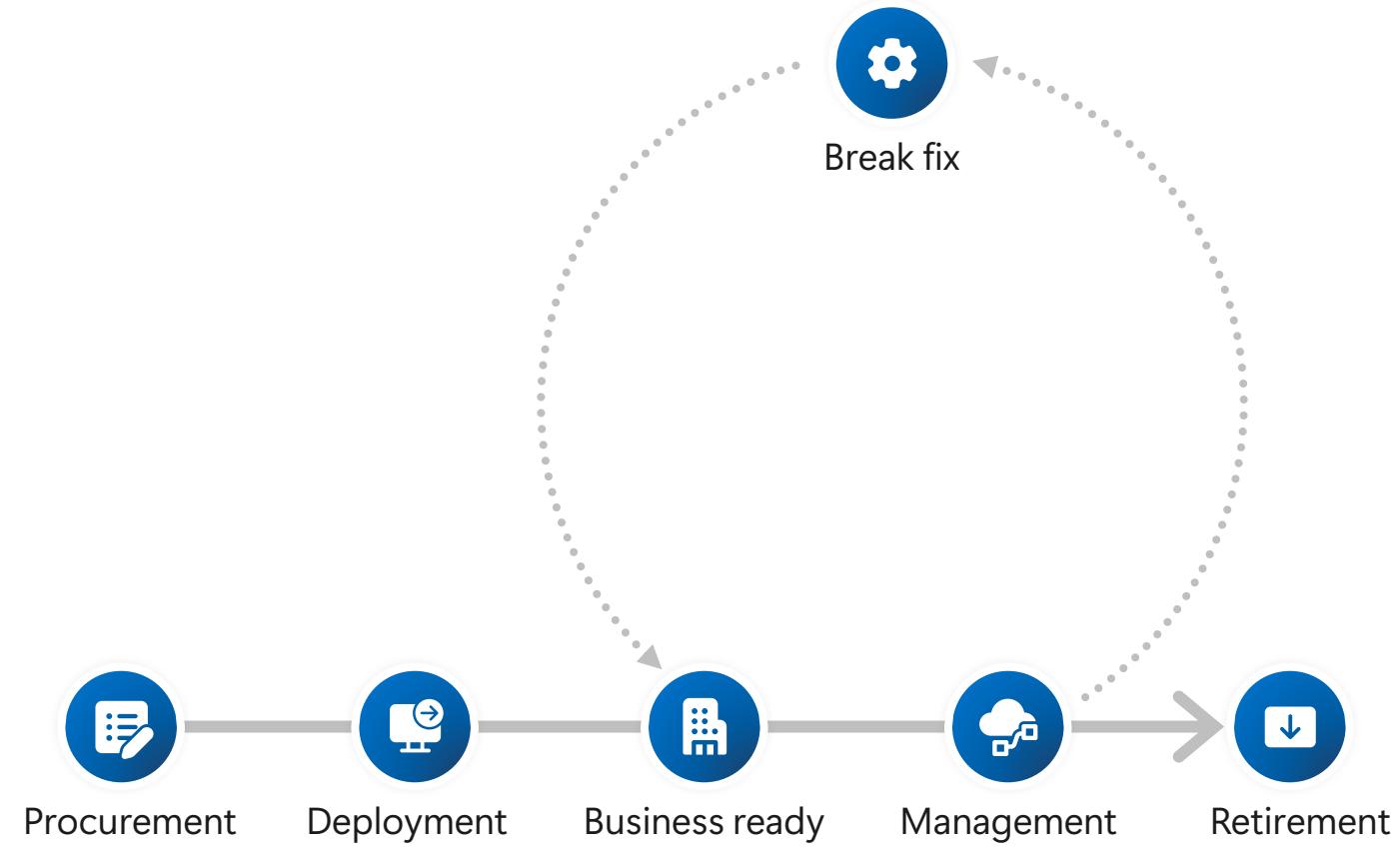
Proactively manage better user experiences while driving operational excellence with AI and automation.



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 >>



How: Modernize all workloads by moving them to Intune

Fastest path to a single pane of glass in the cloud

Existing Windows Endpoints

Enroll into co-management, Entra hybrid join, configure with all Intune modernized workloads.

As devices get refreshed move to full cloud-native as a new Windows endpoint.

New Windows Endpoints

Provision new devices using Autopilot user-driven mode into Intune and Entra joined. Migrate personas wholesale to accelerate.



Deploy using
Windows Autopilot



Join to
Microsoft Entra



Automatically enroll in
Microsoft Intune

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



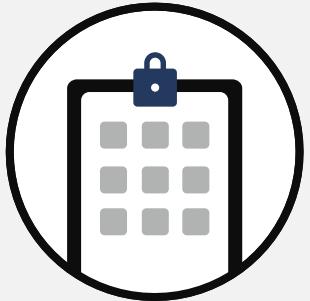
Support any end-user device platform including Windows, Android, Mac, iOS, and HTML 5

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



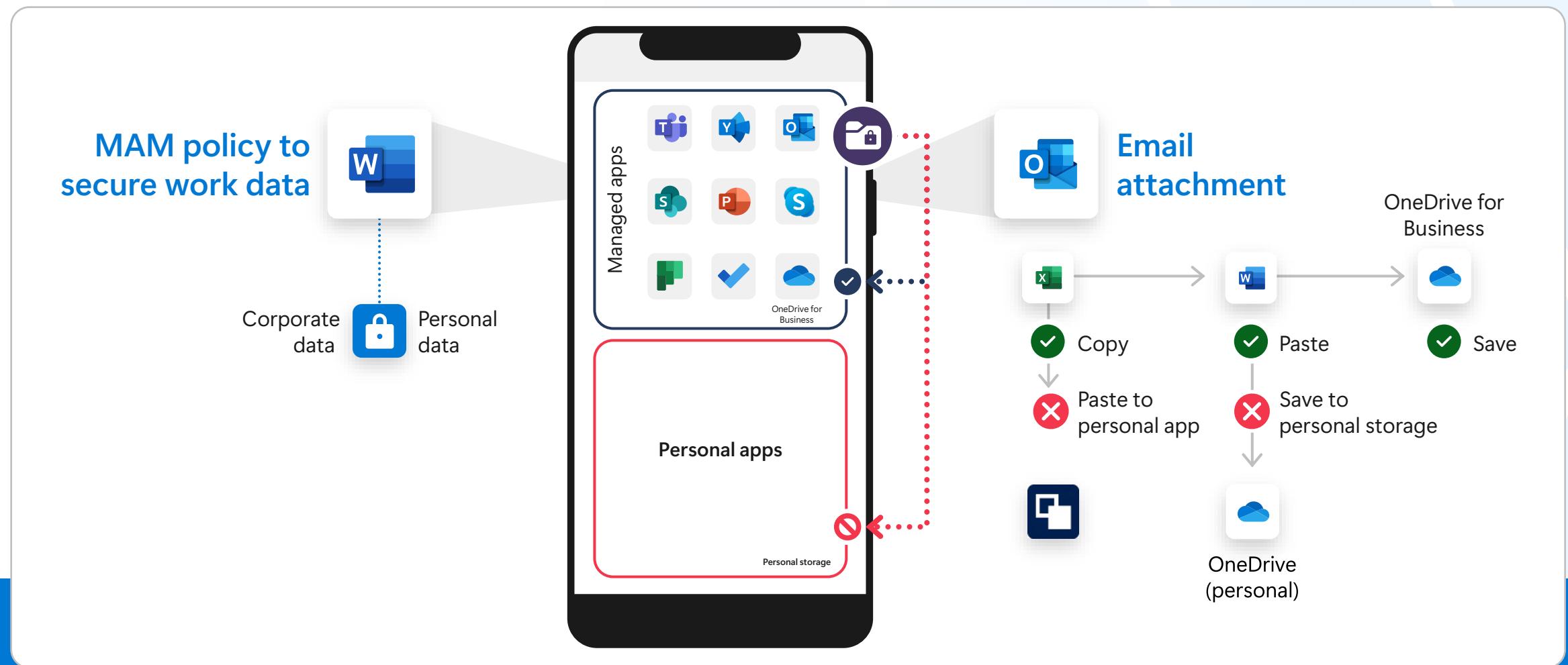
Secure and remove corporate data within mobile apps

Learn more:

<https://Aka.ms/IntuneLearn>



Example: Managing work data on personal devices



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



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**

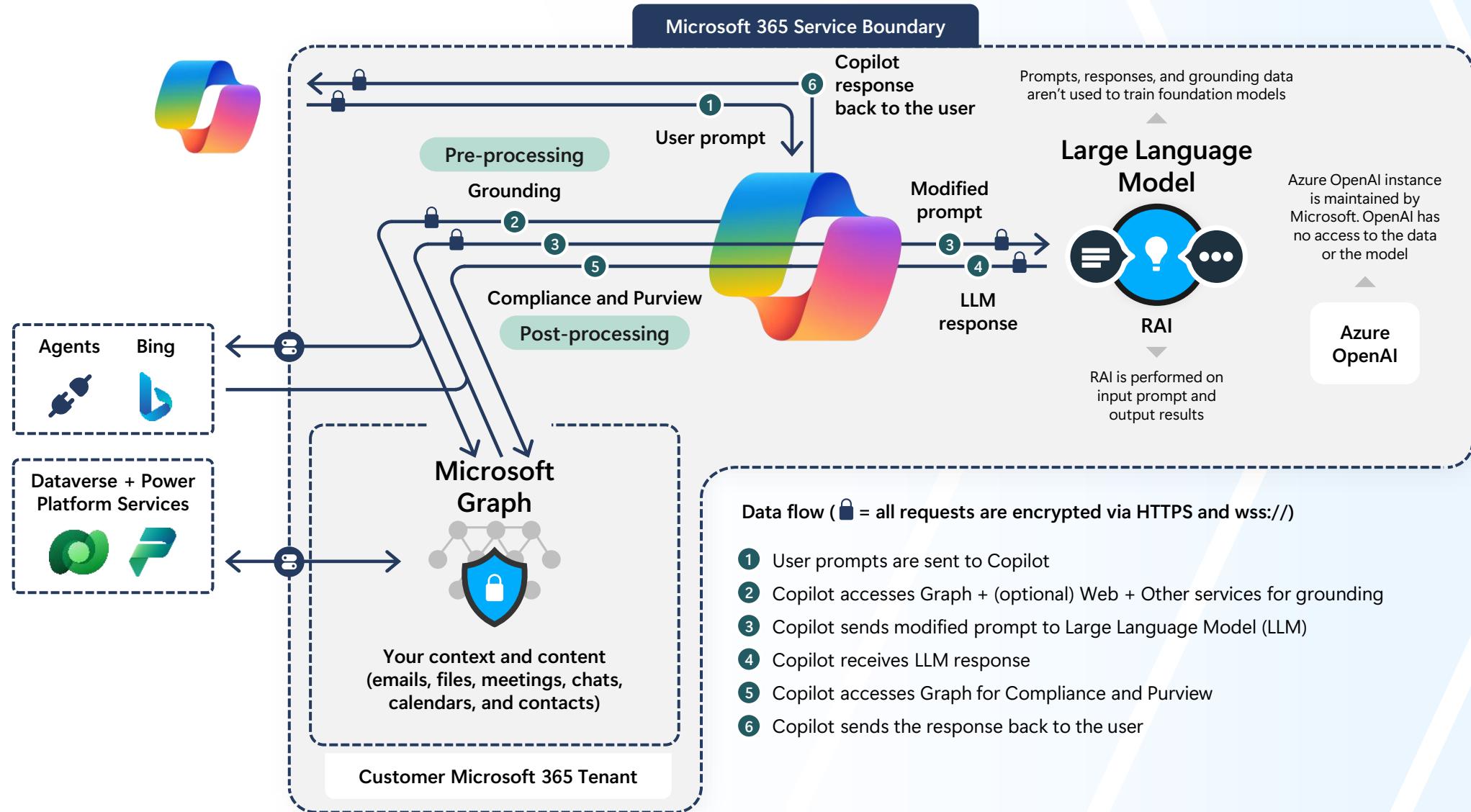
4

Orchestrator appends info to your prompt to enhance it

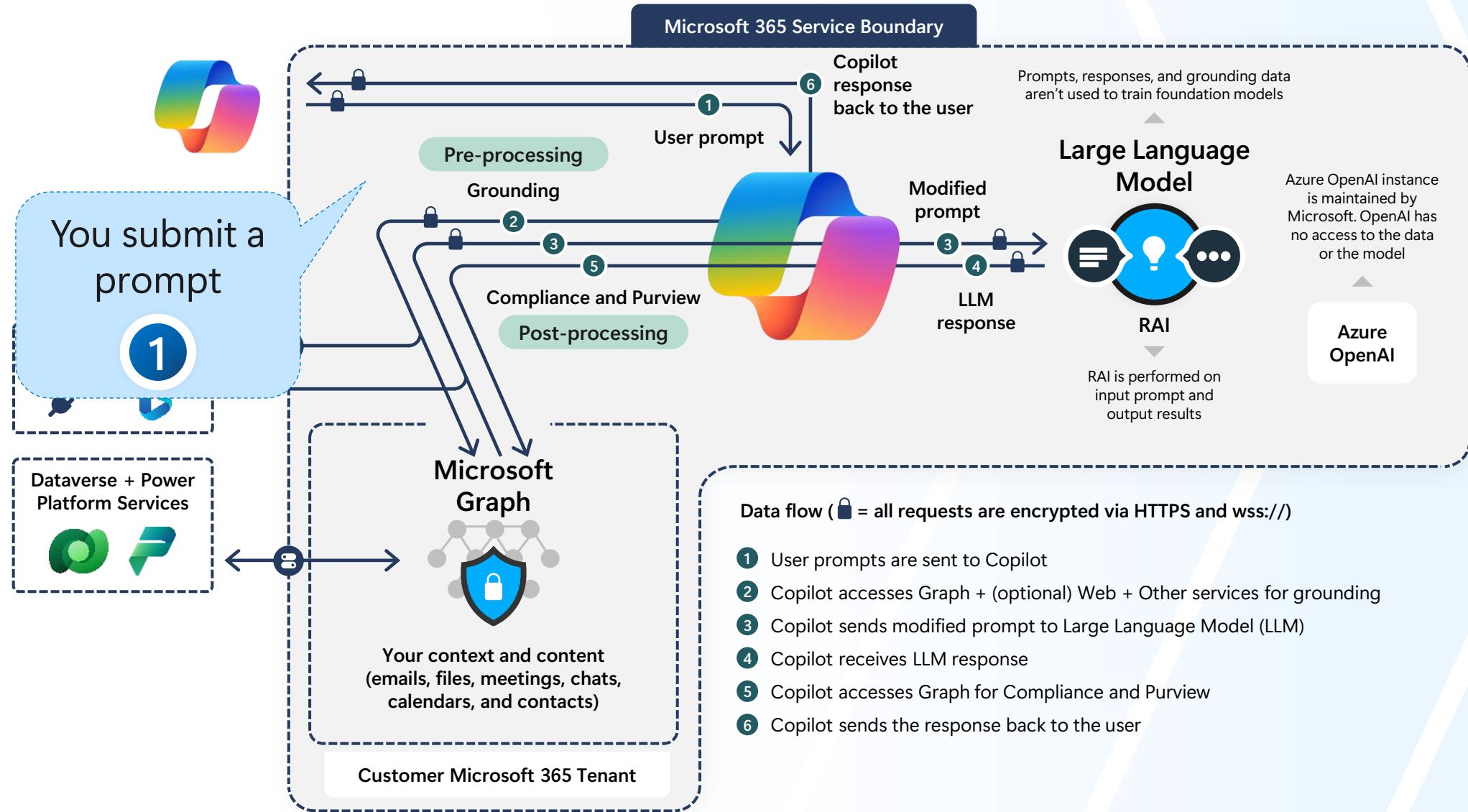
5

LLM uses additional that information to generate a response

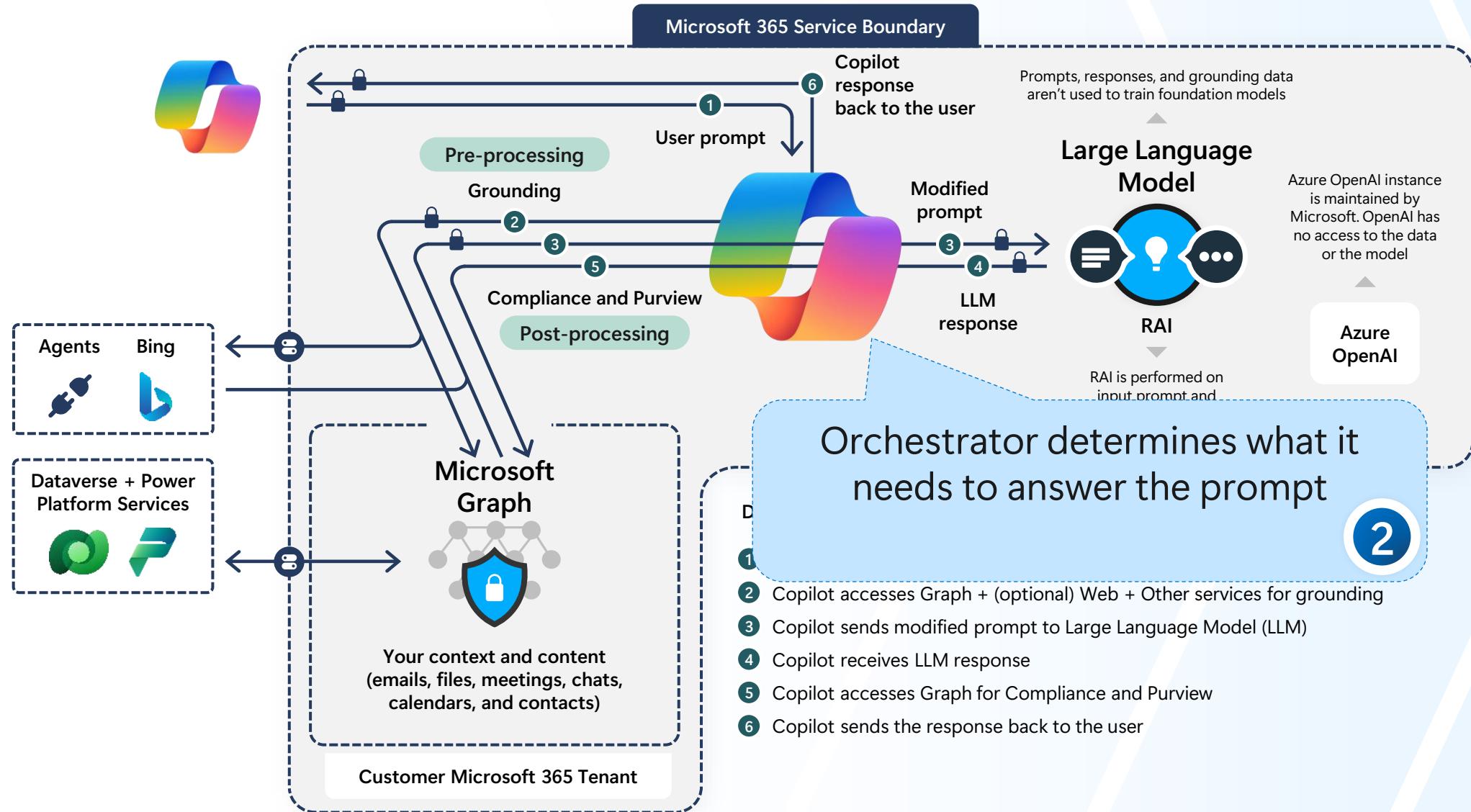
Microsoft Copilot for Microsoft 365 architecture and content retrieval



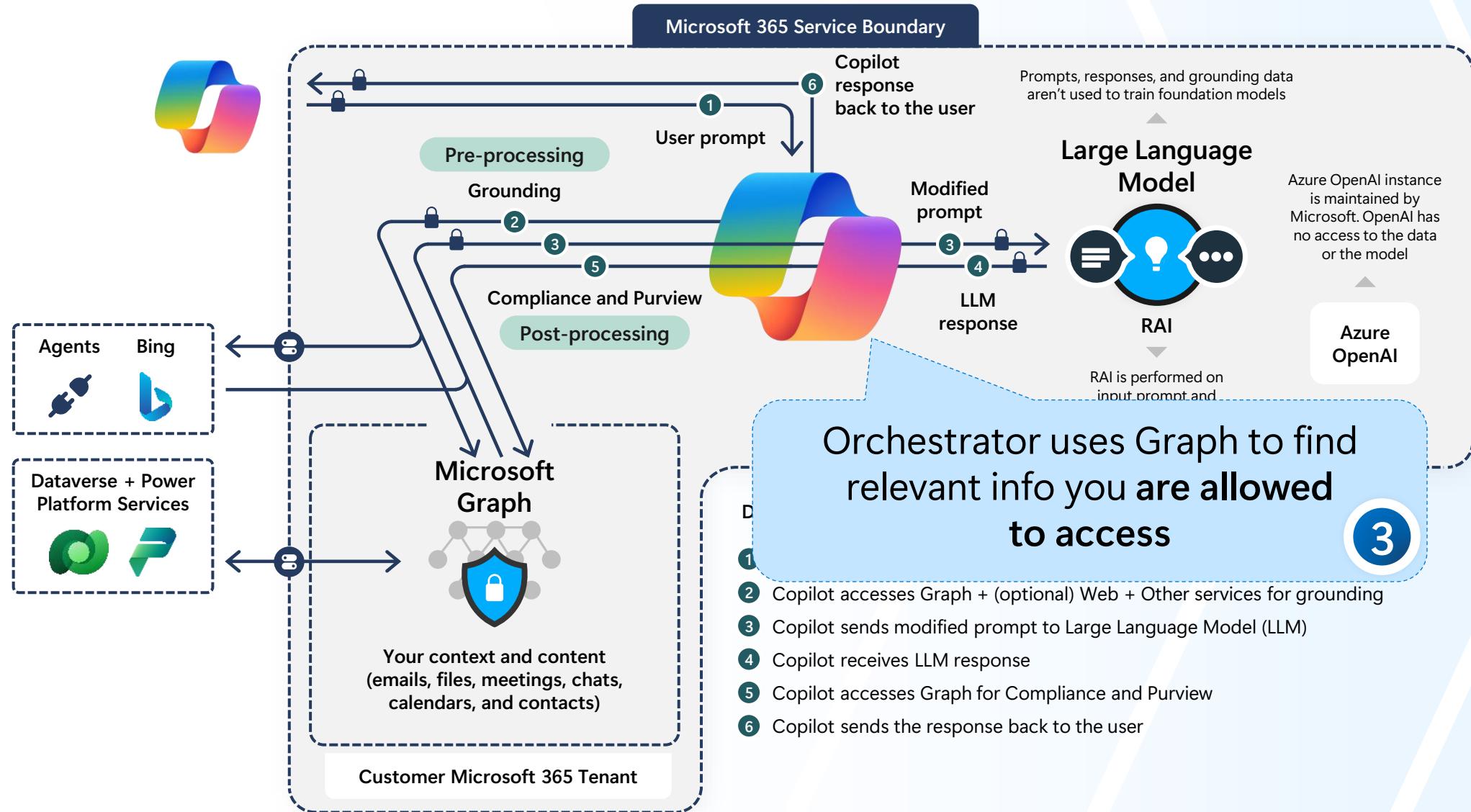
Microsoft Copilot for Microsoft 365 architecture and content retrieval



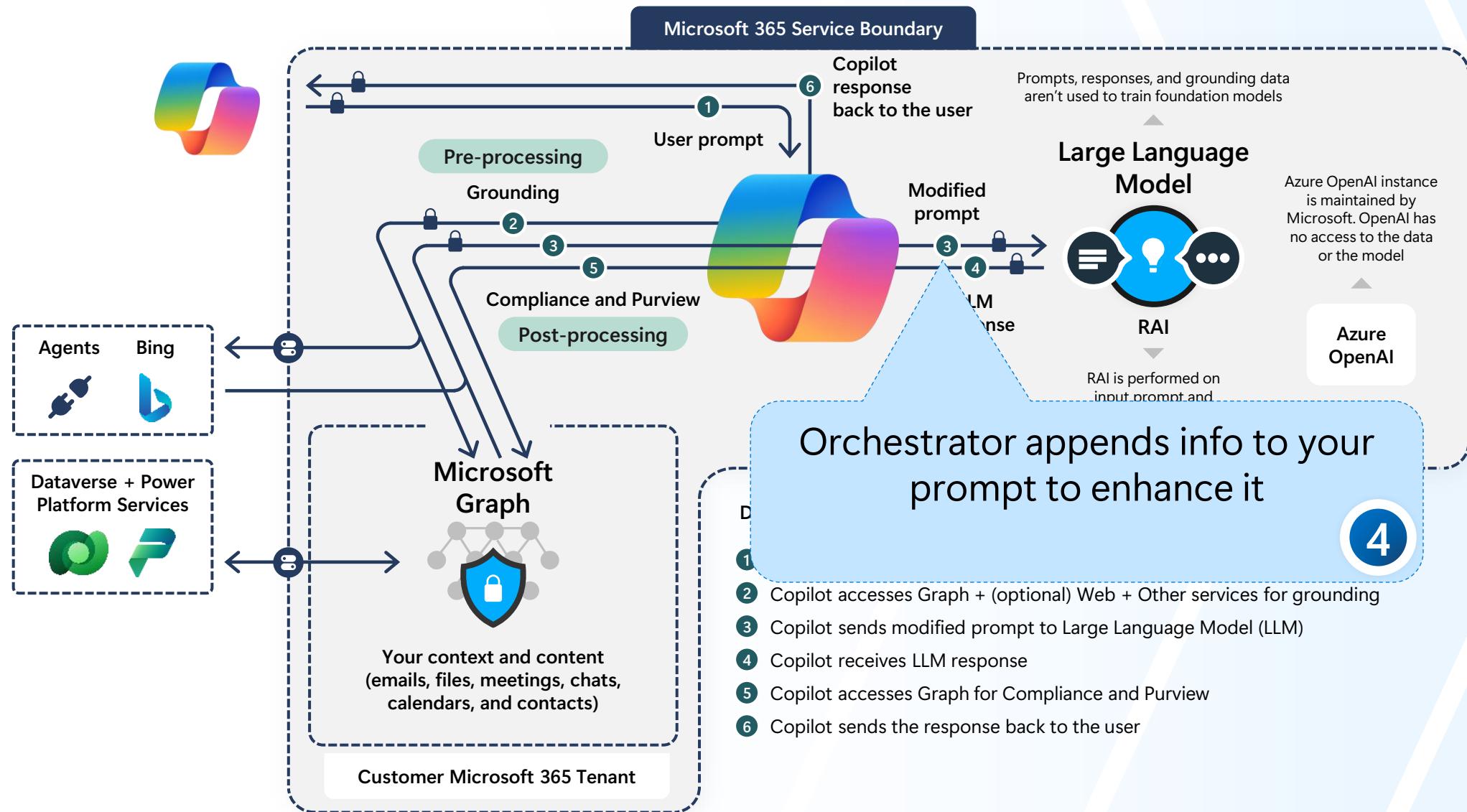
Microsoft Copilot for Microsoft 365 architecture and content retrieval



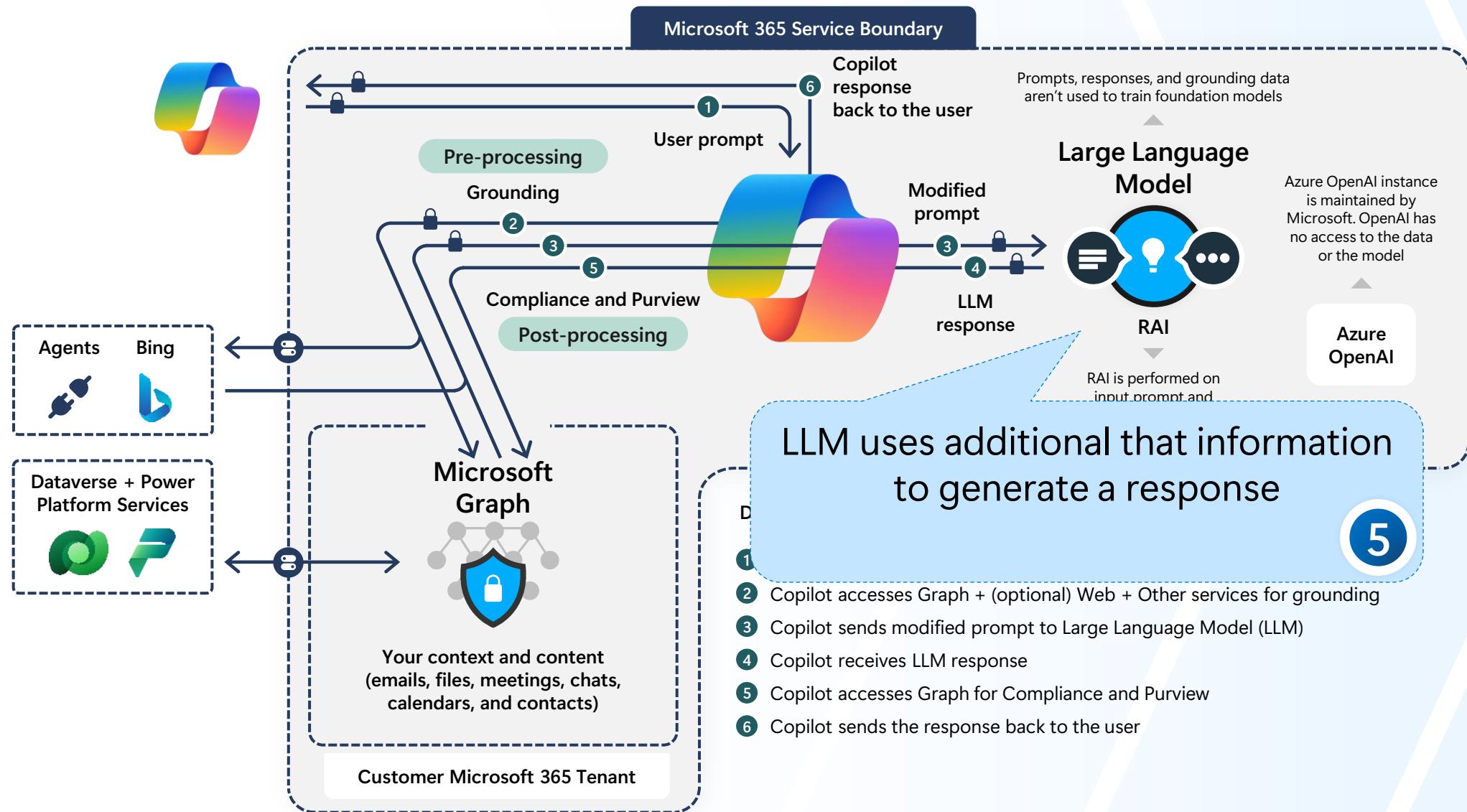
Microsoft Copilot for Microsoft 365 architecture and content retrieval



Microsoft Copilot for Microsoft 365 architecture and content retrieval



Microsoft Copilot for Microsoft 365 architecture and content retrieval



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

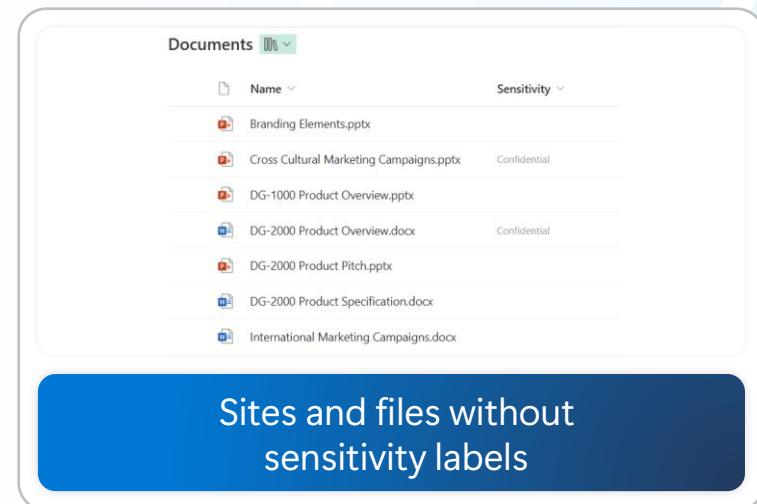
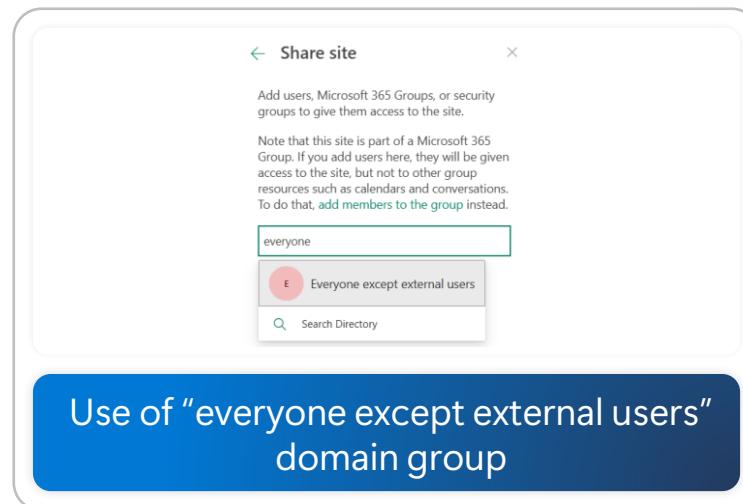
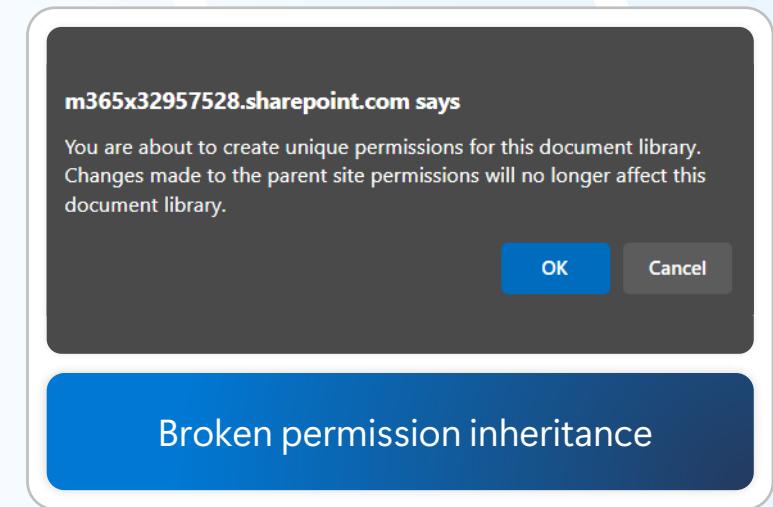
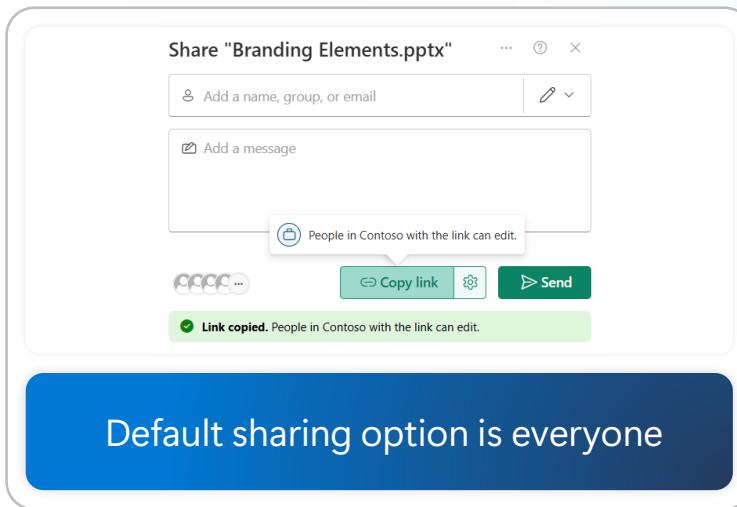
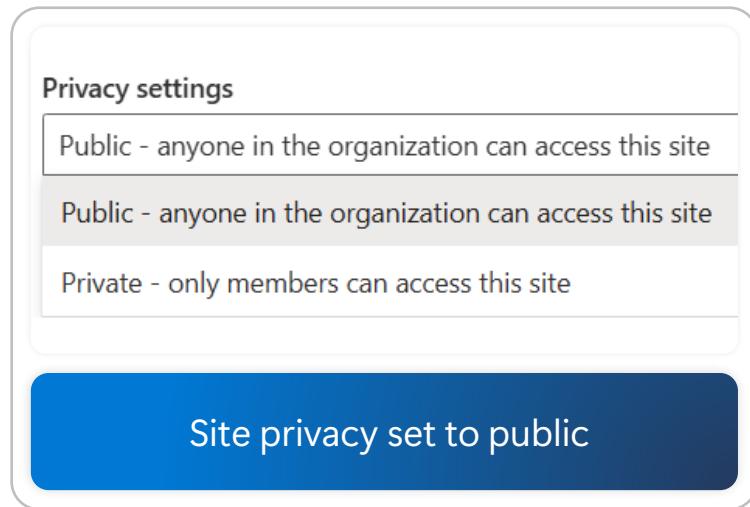


SharePoint sites

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

Address internal user oversharing concerns for M365 Copilot deployment

	Pilot (optional)	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

Last updated: Oct 24, 2024

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>

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 Run the Purview DSPM for AI Oversharing posture assessment to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types³ <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 Purview DSPM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery^{1,3} 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 Purview Audit and view Copilot interaction activity reports and charts^{1,2,3} Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³ Turn on audit-mode oversharing SPO Purview 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 DAG 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 Create customized Purview DSPM for AI Oversharing posture assessments to scale out data security actions, pivoted on labels and sensitive information types³ <p>2. Restrict sensitive info from Copilot access and/or processing</p> <ul style="list-style-type: none"> Initiate SAM Access Review for all sites that are overshared¹ Apply SAM restricted access control (RAC) on business-critical sites¹ Exclude critical sites from Copilot reasoning over them with SAM Restricted Content Discovery (RCD)¹ Publish sensitivity labels with Purview Information Protection to Office apps, Container/Sites, Outlook for manual data protection by user² Exclude Copilot from summarizing sensitive content via sensitivity labels³ <p>3. Increase site privacy</p> <ul style="list-style-type: none"> Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members² Apply default site library sensitivity labels to protect new and modified unlabeled documents³ Turn on enforce-mode oversharing SPO Purview 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 needed.¹ Proactively avoid oversharing by applying RAC at site provisioning.¹ Periodically review ownerless 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 Routinely run Purview DSPM for AI Oversharing assessment report to scale out data security actions, pivoted on labels and sensitive information types³ Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue² View risky user activity in context of oversharing Purview DLP incidents³ <p>2. Further secure sensitive data</p> <ul style="list-style-type: none"> Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies³ Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access² <p>3. Improve Copilot responses</p> <ul style="list-style-type: none"> Setup Purview retention/deletion policies for SharePoint to reduce data surface² Identify inactive sites with SAM, then restrict access 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/E5PrepareYourDataForCopilot>



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



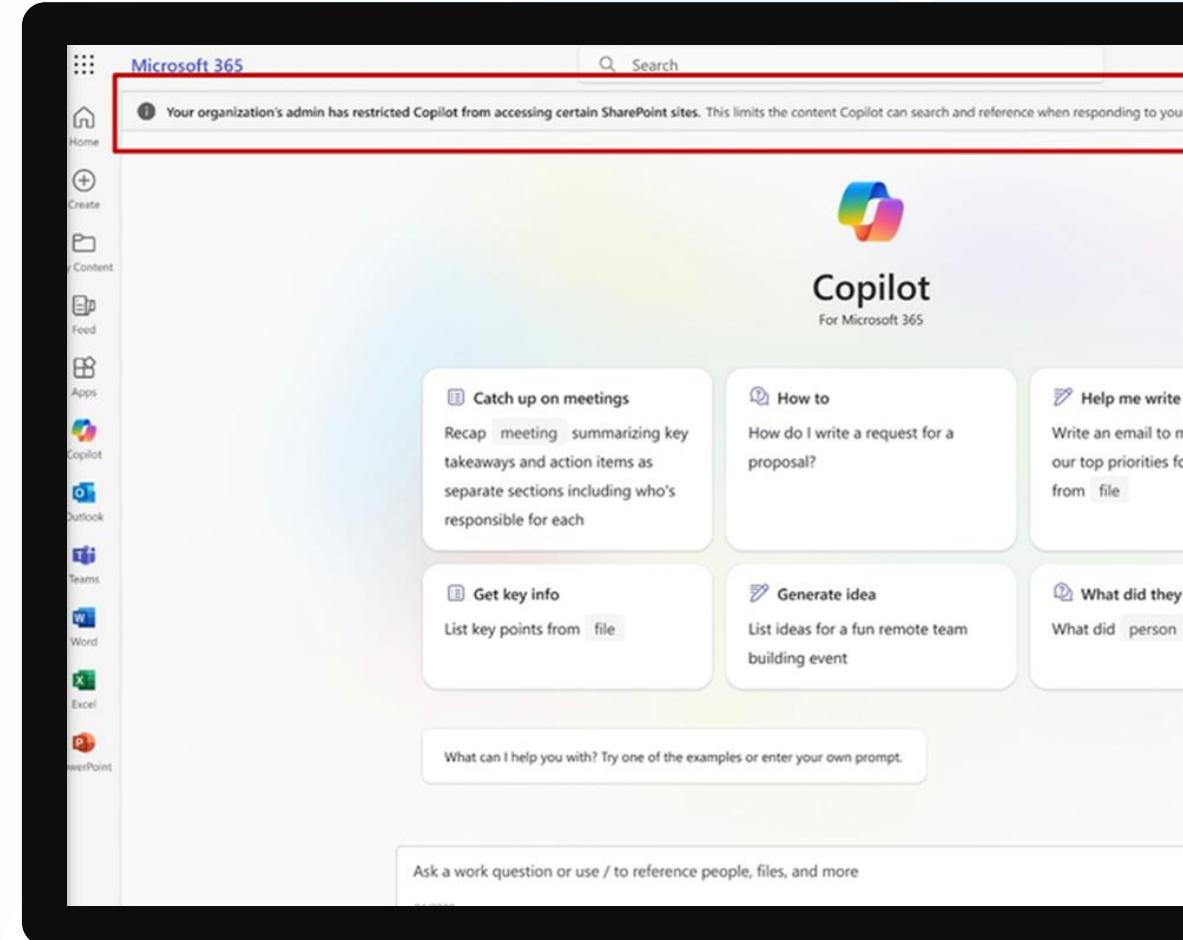
Impacts Copilot and **organization-wide** Search



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



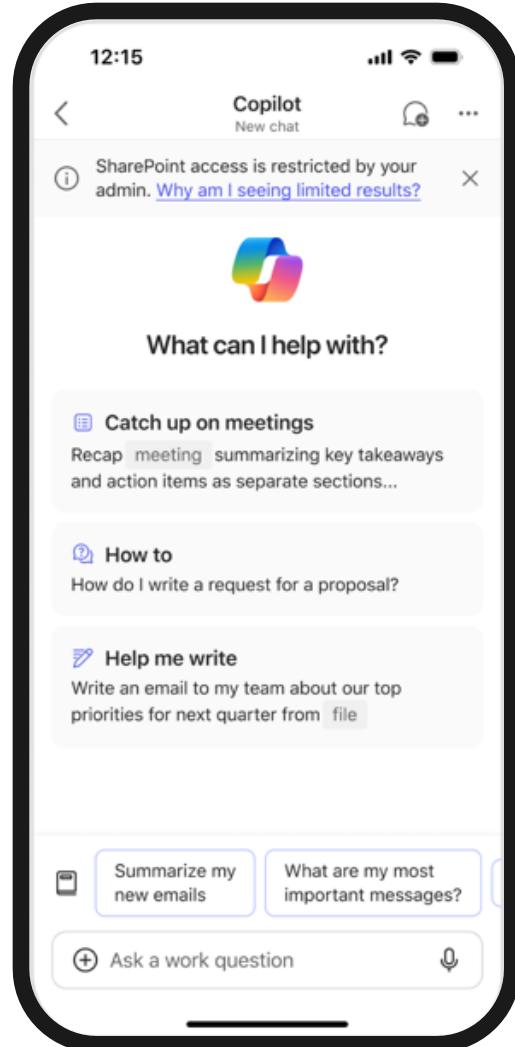
Apply the allowed list

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 tagline 'For Microsoft 365'. It displays six cards arranged in a grid: '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 is a message 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

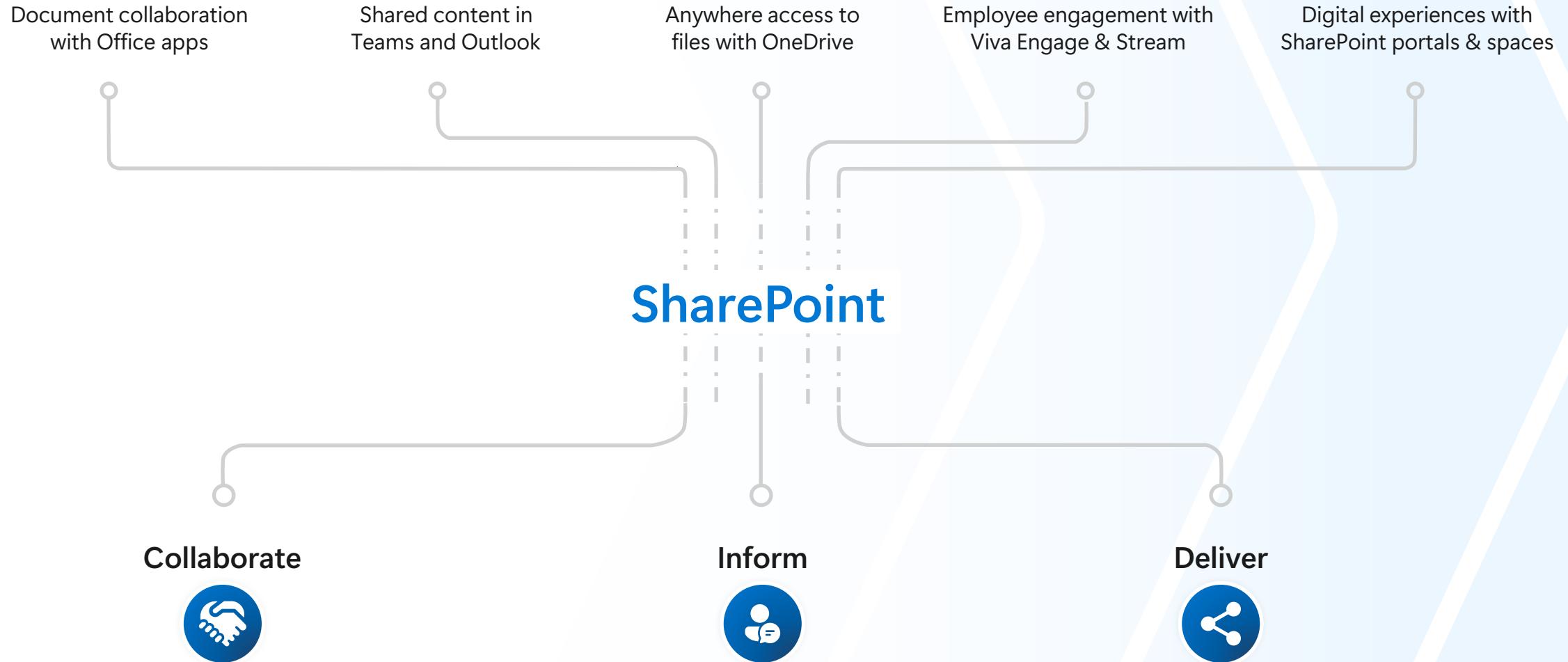
SharePoint Advanced Management (SAM)

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

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 SharePoint site review interface. At the top, a summary box titled "Snapshot till March" provides an overview of sites with high user counts across permission scopes. It includes a "Download detailed report" button and navigation links for "Initiate site access review", "View all reviews", and "Restrict site access". Below this, the main content area displays a table titled "Permissions to many users" under the heading "Site reviews > Permissions to many users". The table lists various items with their names, scopes, user counts, and group counts. To the right of the table, a sidebar shows three status categories: "Retained all permissions" (1 item), "Modified existing permissions" (1 item), and "Removed permissions completely" (1 item). A blue callout box highlights the "Broken inheritance, Sharing links, EEEU domain group" row, which corresponds to the "Confidential Q2 CY24 ReOrg" file. At the bottom of the page, there are buttons for "Complete review", "Save as draft", and "Cancel".

Name	Scope	Total number of Permisioned users	Total number of groups	Count of Anyone' links	Count of 'People in your org' links	Has EEU	Has Everyone	Action	Final status
Contoso Finance	SharePoint Site	6804	4	-	-	-	-	Manage access	Select
Finance_projections_FY23.xlsx	File	7142	5	2	2	-	-	Manage access	Select
Vendor Bills	Folder	7524	2	1	2	-	-	Manage access	Select
ProfitabilityPlan.pptx	File	7945	6	1	3	Yes	-	Manage access	Select
Flow map.jpg	File	8580	3	2	1	Yes	-	Manage access	Select
Confidential Q2 CY24 ReOrg	File	9092	4	3	3	Yes	-	Manage access	Select

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.

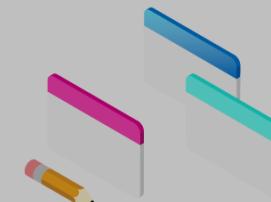
[Create report](#)

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

As of March 3, 2024

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

Download a detailed .csv report for up to 1M sites.

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

100 items

Search

Filters: Site sensitivity: All External sharing: All

Name	URL	Site access review	Total permissioned users ↓	Files	Sensitive Files ⓘ	Items with unique permissions	EEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
Contoso HR	../teams/contosohr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
Contoso Marketing	../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
Contoso Finance	../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
Contoso Team	../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
Contoso Vac	../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
Contoso in house	../teams/contosoin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
Contoso infra	../teams/contosoin	-	3998	28187	2890	5	2	21	21	Public	General	On
Contoso leaders	../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
Contoso design	../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
Contoso BI	../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
Contoso HR	../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
Contoso Give	../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
Contoso Sesh	../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
Contoso Sesh	../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On

Snapshot till March

As of March 3, 2024

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

Download a detailed .csv report for up to 1M sites.

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

Filters: Site sensitivity: All External sharing: All

Name	URL	Site access review	Total permissioned users ↓	Files	Sensitive Files ⓘ	Items with unique permissions	EEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
Contoso HR	../teams/contosohr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
Contoso Marketing	../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
Contoso Finance	../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
Contoso Team	../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
Contoso Vac	../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
Contoso in house	../teams/contosoin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
Contoso infra	../teams/contosoin	-	3998	28187	2890	5	2	21	21	Public	General	On
Contoso leaders	../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
Contoso design	../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
Contoso BI	../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
Contoso HR	../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
Contoso Give	../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
Contoso Sesh	../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
Contoso Sesh	../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On

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

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

Contoso Finance
...com/sites/contosofin

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 EEEU	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	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

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 right, a modal window titled 'Restricted site access' is open. It contains a description of the feature, a checkbox for 'Restrict SharePoint site access to only users in specified groups', and a 'Add group' input field with a dropdown menu showing four security groups: Contoso Financial Council, Contoso Tech, Contoso Marketing, and Contoso HR. On the left, there's a 'Snapshot till March' report card with a summary of site access review status and a detailed table below it. The table lists various SharePoint sites along with their URLs, access review status (Pending or Completed), Teams count, total permissioned users, and a 'Count of' column. Some rows are highlighted in blue.

Name	URL	Site access review status	Teams	Total permissioned users	Count of
Contoso HR	/teams/contosohr	—	1	22134	312
Contoso Marketing	/teams/contosomar	Pending	1	15698	296
Contoso Finance	/sites/contosofin	Completed	—	11227	167
Contoso Giving	/sites/contosogiv	—	—	10245	145
Contoso team	/sites/contosoteam	—	—	8530	124
Contoso Vac	/sites/contosovac	—	—	6654	72
Contoso HRA	/teams/contosohra	—	1	3998	2416
Contoso Media	/sites/contosocomedia	—	—	2804	38
Contoso in house	/sites/contosoinh	—	—	1890	32
Contoso infra	/sites/contosoinfra	—	—	1487	23
Contoso design	/sites/contosodesign	—	—	1329	21
Contoso leaders	/teams/contosolead	—	1	1127	647
Contoso data	/teams/contosodata	—	1	1038	721

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

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 users
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

[Save](#)

Restricted site access

Use this setting to allow only users in specific security groups to access this SharePoint site. You can add up to 10 security groups. Users not in these security groups will lose access to all this SharePoint site.

[Learn more about Restricted access control for SharePoint sites](#) Restrict SharePoint site access to only users in specified groups

Add group

- CF Contoso Financial Council
- CT Contoso Tech
- CM Contoso Marketing
- CH 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)

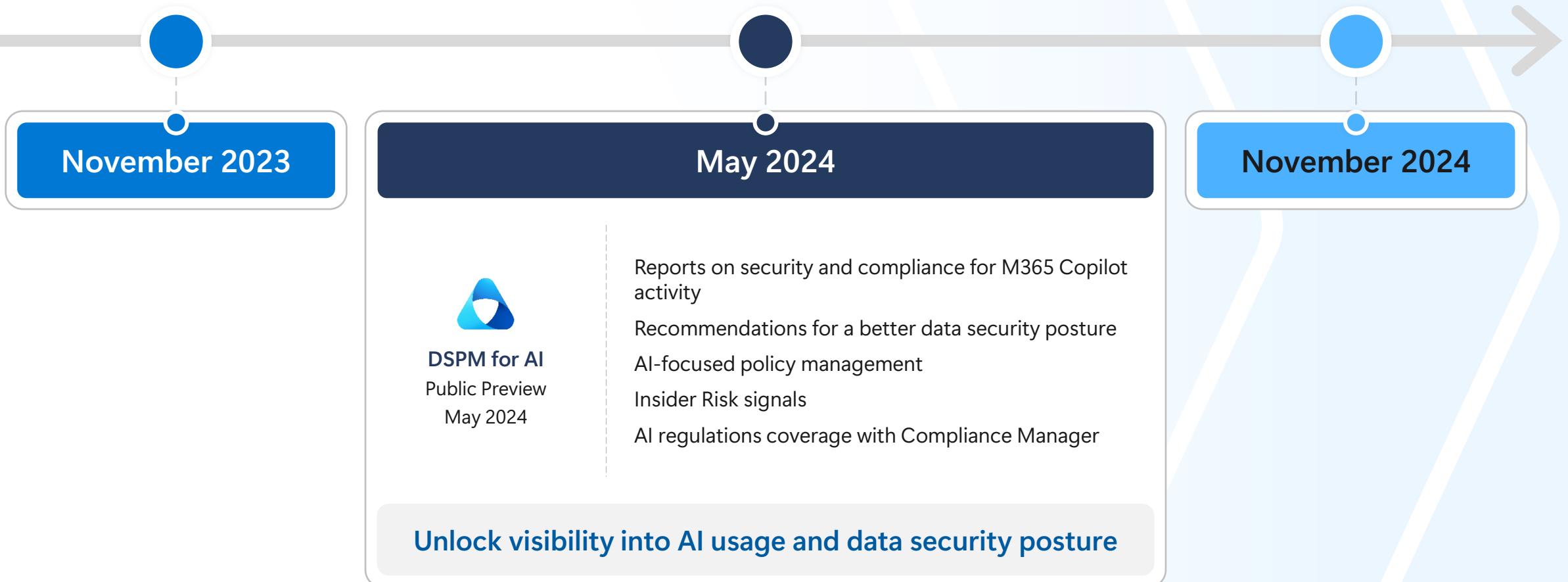
4

SharePoint Advanced Management (SAM)

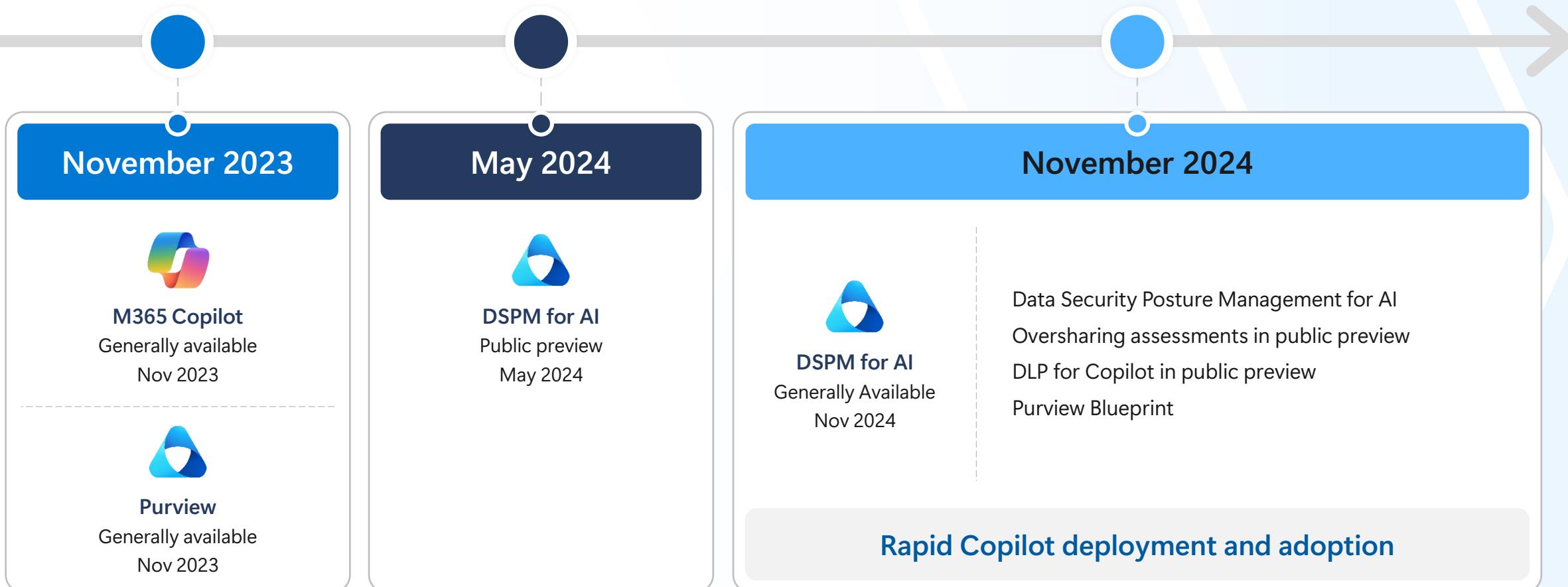
5

Microsoft Purview

Microsoft Purview's solutions help you secure your AI data like never before



Microsoft Purview's solutions help you secure your AI data like never before





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

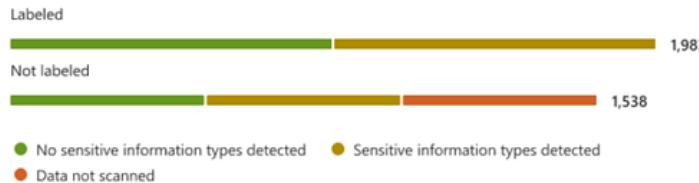
Oversharing assessment in Data Security Posture Management (DSPM) for AI

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

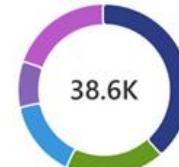
[View all](#)



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](#)

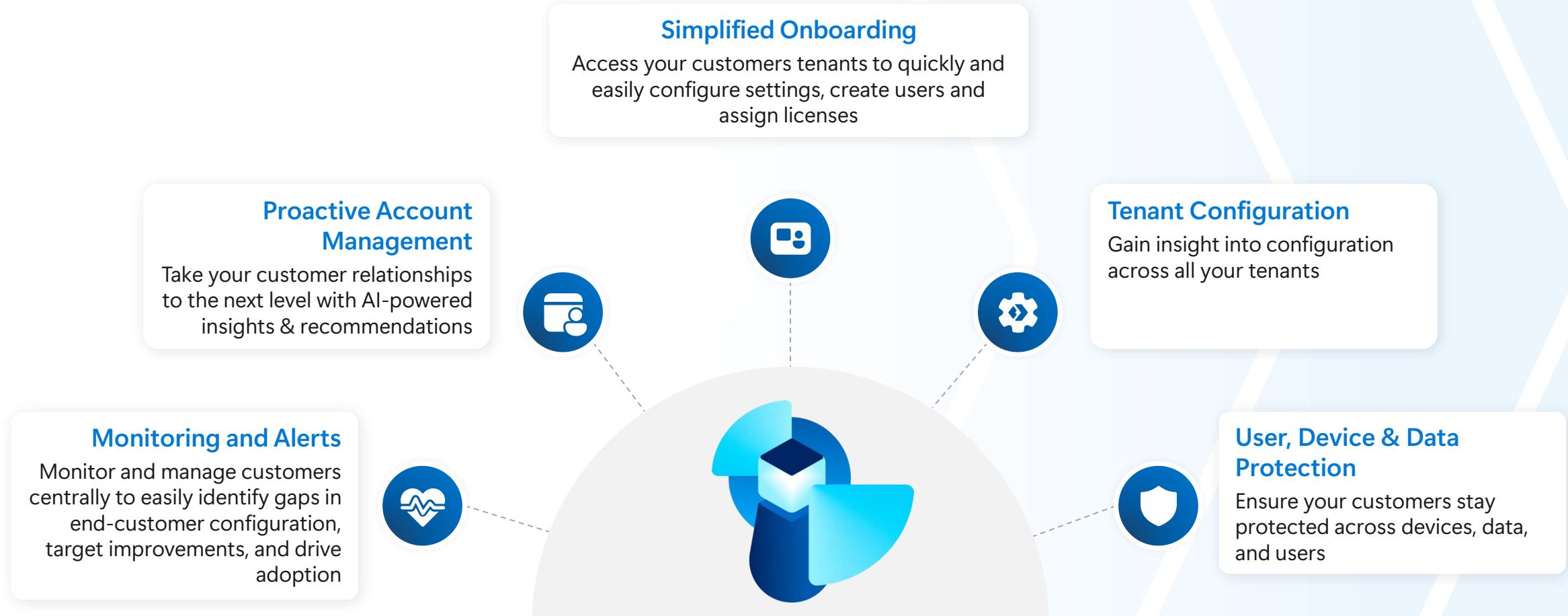
Prevent Copilot from processing file contents

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

Simplify Management: **Microsoft Lighthouse**



Microsoft 365 Lighthouse



Simple. Secure. AI-powered.

Enabling end-to-end success of Copilot with Lighthouse¹



Purchase Readiness

Use AI-driven insights to identify customers with propensity to buy Copilot for Microsoft 365

Targeted Assignment

Identify the best set of users to get started with and assign Copilot licenses in-line

Expansion Readiness

Identify customers ready to move from pilot to departmental or org wide rollout

Simple. Secure. AI-powered.

¹Coming soon

Manage your customer's Copilot journey with

Lighthouse Copilot Insights



1

Know which customers are ready

Propensity scoring to help you identify which customers are ready for Copilot. With this data at your fingertips, you know who to reach out to first, saving valuable time.

2

Track deployment tasks

Pinpoint customers who may need Copilot setup guidance or training. Use the insights to ensure all Copilot licenses are assigned to the right users and Copilot deployment tasks are complete.

3

View usage and license assignments

Easily monitor which customers are actively using Copilot, and quickly assign unused licenses, ensuring they get the most out of their AI investment.

A screenshot of the Microsoft 365 Lighthouse Copilot insights dashboard. The left sidebar shows navigation links for Home, Alerts, Copilot insights (which is selected), Tenants, Users, Devices, Data protection, Apps, Deployment, Permissions, Service health, Audit logs, and Sales advisor. The main content area has a title 'Copilot insights' with a 'Tenants: All' dropdown. Below it are two tabs: 'Opportunities' (disabled) and 'Adoption' (selected). A section titled 'Adoption trends' contains a bar chart comparing 'Assigned Copilot licenses' (blue bars) and 'Active license usage' (purple bars) across months from Jan to June. To the right, there's a 'Resources for your customers' section with links to 'Get started with Microsoft 365 Copilot', 'Adoption guides', 'Microsoft Copilot video tutorials', 'Connect to the Copilot dashboard', and 'Extend Microsoft 365 Copilot'. At the bottom, a table titled 'Tenant details and deployment tasks' lists two tenants: 'Liberty's Delightful Sinful Bakery & Cafe' and 'WingTip Toys', showing active user rates, copilot licenses, unassigned licenses, deployment task progress, and recommended actions. The top right corner shows a user profile for 'Connie Wilson'.



Baselines

Baselines provide a repeatable and scalable way to manage Microsoft 365 across multiple tenants. Baselines provide standard tenant configurations that deploy core security policies and compliance standards that keep your tenants' users, devices, and data secure and healthy.





Microsoft's default baseline

The default baseline is a set of pre-configured deployment tasks recommended by Microsoft to automate the setup and configuration of policies and settings to keep managed tenants safe, secure, and productive.



The screenshot shows the Microsoft 365 Lighthouse interface with the URL https://lighthouse.microsoft.com/?Microsoft_Intune_MTM=TestProd&Microsoft_Intune_DeviceSettings=TestProd&feature.msajs=true#view/Microsoft_Intune_MTM/BenchmarkCollection.ReactView/collection%7B%40odata.etag%3A%65C55.... The page title is "Default Baseline". The left sidebar includes links for Home, Alerts, Tenants, Users, Devices, Apps, Data protection, Deployment (with sub-links for Deployment insights, Baselines, Service health, Audit logs, Permissions, and Delegated access), Sales Advisor (Project Orlando), and Opportunities. The main content area displays the "Default Baseline" tasks:

Tasks	Category	Management portal	Required services	Priority
Require MFA for admins	Identity	Azure Active Directory	Microsoft Entra ID	P1
Require MFA for users	Identity	Azure Active Directory	Microsoft Entra ID	P1
Block legacy authentication	Identity	Azure Active Directory	Microsoft Entra ID	P1
Set up device enrollment	Devices	Azure Active Directory	Intune	
Configure Azure Active Directory for joining devices	Devices	Microsoft Intune	Intune	
Enable Intune Endpoint Analytics	Devices	Microsoft Intune	Intune	
Collect Windows event logs	Device Remediations		Intune	
Set up Microsoft Defender for Business	Devices	Microsoft Defender for Business	Intune, Microsoft Defend	
Provision Microsoft Defender	Devices	Microsoft Defender for Business	Intune, Microsoft Defend	
Automatically onboard devices to Microsoft Defender using Micros...	Devices	Microsoft Defender for Business	Intune, Microsoft Defend	
Configure app protection policies	Microsoft Endpoint Manager		Intune	
Configure application management for iOS				

At the bottom of the screen, there is a taskbar with icons for File Explorer, Task View, Edge browser, File, Mail, OneDrive, OneNote, Power BI, and others. The system tray shows a weather icon for "Light rain" and the date and time as "5:00 PM 12/5/2023".



Detect drift

Lighthouse continuously scans customer tenants to ensure they remain compliant and provides a graphical view of each time scan from the previous 30 days, providing the deployment status for the task and the assigned users.



The screenshot shows the Microsoft 365 Lighthouse interface for the tenant "City Power & Light". The main dashboard displays the following information:

- Compliance Summary:** Compliant (13), Not compliant (3), Dismissed (3), Not licensed (0).
- Deployment Plan:** A table showing tasks grouped by category and their status (Compliant or Not compliant) across 6 users.
- Users:** A chart showing the number of users in different compliance states over time (11/12 to 12/03).
- Scan History:** A table listing scan times, statuses, and counts for Not targeted, Excluded, Not licensed, Not compliant, and Compliant users.

The interface includes navigation menus for Home, Tenants, and City Power & Light, and tabs for Overview, Deployment plan, Deployment progress by user, Secure score, and Detection history.



Deployment insights

Microsoft 365 Lighthouse provides deployment insights within and across the tenants you manage. The single view lets you:

- Understand the deployment status across all tenants, users, and tasks.
- Review deployment exceptions such as Dismissed tasks and Excluded users.
- Review regressions such as tasks that change from a Compliant or Dismissed status to a status of Not compliant or Not licensed.
- Quantify threats based on user- and task-level deployment progress.
- Prioritize deployment activities based on risk.



The screenshot shows the Microsoft 365 Lighthouse Deployment insights dashboard. At the top, it displays two main progress metrics: "Deployment plans are not complete for 100.0% of tenants" and "Deployment tasks are not complete for 97.6% of users". Below these are two horizontal bar charts, one for Tenant progress (Complete vs. Not Complete) and one for User progress (Complete vs. Not Complete). The main area of the dashboard is a table listing 14 tenants, each with its baseline, deployment plan status, task progress, and various threat metrics like Dismissed tasks, Not licensed tasks, Regressed tasks, and User progress. The table also includes columns for Excluded users and Exclusions. The tenant names listed are Allure Bays Corp, Blue Yonder Airlines, City Power & Light, Contoso, Fourth Coffee, FusionTomo, Graphic Design Institute, and Parnell Aerospace. The dashboard has a sidebar with navigation icons and a bottom navigation bar with various application icons.

Tenant ↑	Baseline	Deployment plan status	Task progress ⓘ	Dismissed tasks	Not licensed tasks	Regressed tasks	User progress ⓘ	Excluded users	Exclusions ⓘ
Allure Bays Corp	Financial Services Baseline	Not complete	0/31	0	0	0	--	0	0
Blue Yonder Airlines	Default Baseline	Not complete	6/19	0	0	0	0/2	1	1
City Power & Light	Default Baseline	Not complete	14/19	3	0	0	0/6	1	1
Contoso	Premium Customers	Not complete	2/19	0	0	0	0/234	0	0
Fourth Coffee	Default Baseline	Not complete	3/19	0	0	0	0/8	0	0
FusionTomo	Default Baseline	Not complete	16/19	3	0	0	0/8	0	0
Graphic Design Institute	Default Baseline	Not complete	2/19	0	1	0	0/9	0	0
Parnell Aerospace	Default Baseline	Not complete	4/19	0	0	0	0/7	0	0



Delegated access

Delegated access management helps partners make sure the right people have the right access to the right stuff at the right time to do the right work





Set up GDAP

You can now set up all your customers with GDAP through Microsoft 365 Lighthouse, regardless of their licenses or size.

Lighthouse lets you quickly transition your organization to GDAP and begin the journey to least-privilege for your delegated access to customers.



The screenshot shows the Microsoft 365 Lighthouse dashboard. On the left is a navigation sidebar with options like Home, Alerts, Tenants, Users, Devices, Apps, Quarantined messages, Deployment, Service health, Audit logs, Permissions, and Sales Advisor (Project Orland). The main content area has a header with 'Tenants: All' and links for Add user, Reset password, Offboard users, and Manage tags. A 'Guided tour (2 of 4 done)' link is also present. The central focus is a 'GDAP Setup' box with the message '1 of your customers doesn't have a GDAP relationship'. It explains that to manage customer tenants, a GDAP relationship needs to be created. A blue 'Set up GDAP' button is at the bottom of this box. Below this are three cards: 'What's new & learning resources' (Interactive guides, What's new, Blog), 'Sales advisor' (2 subscriptions with upcoming renewals in 90 days, 0 Auto-renew off, 2 Auto-renew on, 410 new license requests), and 'Microsoft Defender Antivirus threat landscape' (0 threats blocked across all devices and tenants, a chart showing threat status over the past 30 days, and a 'View all active threats' button).



Manage delegated access

Lighthouse provides the status of all your customers' delegated relationships, including whether GDAP is set up, if a GDAP template has been assigned, and the next upcoming GDAP relationship expiration date for a customer tenant.



Microsoft 365 Lighthouse

Home > Delegated access

Delegated access

Tenants: All

Set up granular delegated administrative privileges (GDAP) for the customer tenants you manage. With GDAP templates, you can give users in your organization the permissions they need and keep your customer tenants secure.

[Learn more about GDAP management](#)

GDAP templates Relationships

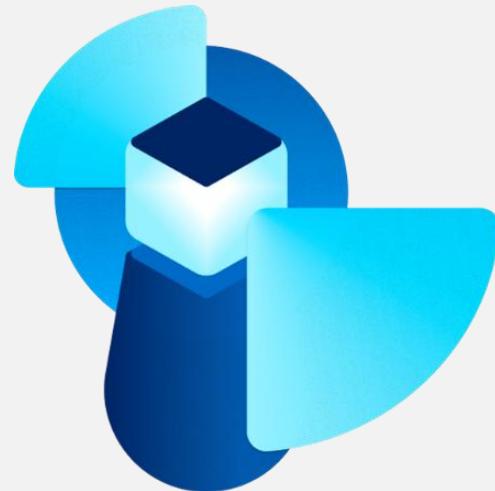
Track settings across the granular delegated admin privileges (GDAP) relationships that you've set up with all your customers. Select a tenant in the list to view delegated relationship details.

Export Refresh 8 tenants Search

Filters: Templates: All

Tenant and relationship	Status	Templates	Security groups	Start date	Expiration date	Tags
Contoso SH 2406_TM :SHAMSAU01	Active	Testing Rahul, Creati...	9	6/11/2024	6/1/2026	112 HEALTHCARE TEST HIT TAH
MTM Delegated Access 3_TM :SHAMSAU01	Active	Creating Template	0	7/1/2024	6/21/2026	112 NEW CUSTOMERS FINANCIAL SERVICES
MTM Delegated Access 4_TM :SHAMSAU01	Active	Creating Template	6	7/29/2024	7/19/2026	NEW CUSTOMERS
MTM Delegated Access 5_TM :SHAMSAU01	Active	Creating Template	1	7/22/2024	7/12/2026	112 NEW CUSTOMERS
Prakhar Selfhost_TM :SHAMSAU01	Active	Creating Template	1	8/14/2024	8/14/2026	

Microsoft 365 Lighthouse – What's new



What's new

Copilot
Insights

Delegated
access
management

Tenant 360
insights

Unified user
onboarding

Coming soon

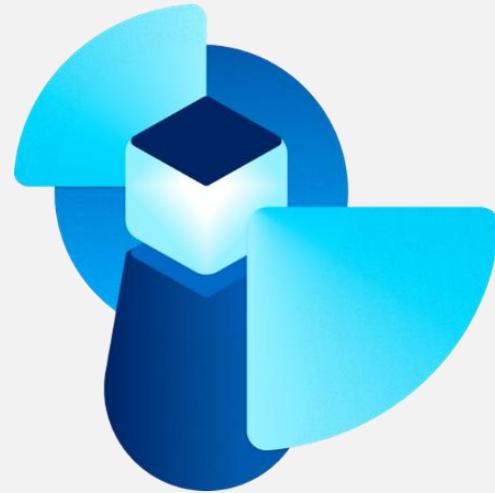
Role-based
access

Expanded
default
baseline

Promotional
visibility
in Sales Advisor

Lighthouse
Demo
Experiences

Microsoft 365 Lighthouse Requirements



Partner

Must be enrolled
in **CSP** program¹

Must have
delegated
access²

Customer

In same region
as partner

<2500
Users

At least one
eligible SKU³

¹MSPs must be enrolled in the Cloud Solution Provider (CSP) program as an Indirect Reseller or Direct Bill partner

²Either granular delegated admin privileges (GDAP) or a delegated admin privileges (DAP) relationship is required to onboard customers to Lighthouse

³Microsoft 365, Office 365, Exchange Online (commercial), EDU subscription, or Microsoft Defender for Business

Resources



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](#)



Session resources



[**Microsoft 365 Lighthouse Demo**](#)

[**Sales Advisor Demo**](#)

Get started:
aka.ms/M365Lighthouseonboard

Learn more:
aka.ms/M365Lighthouse

Microsoft 365 Lighthouse FAQ:
aka.ms/M365LighthouseFAQ

Sales Advisor demo video:
aka.ms/M365SalesAdvisorWalkthrough

Microsoft 365 Lighthouse datasheet:
aka.ms/M365LHDatasheet

Microsoft 365 Lighthouse blog:
aka.ms/Microsoft365LighthouseBlog

Access technical documentation:
aka.ms/M365LighthouseDocs

Share your feedback:
aka.ms/M365LighthouseFeedback

Copilot for Microsoft 365

Monthly updates for partners!



<https://aka.ms/WhatsNewCopilot>

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](#)

