Securing Copilot for Microsoft 365 Education

K12 SECURITY INFORMATION EXCHANGE (K12 SIX)
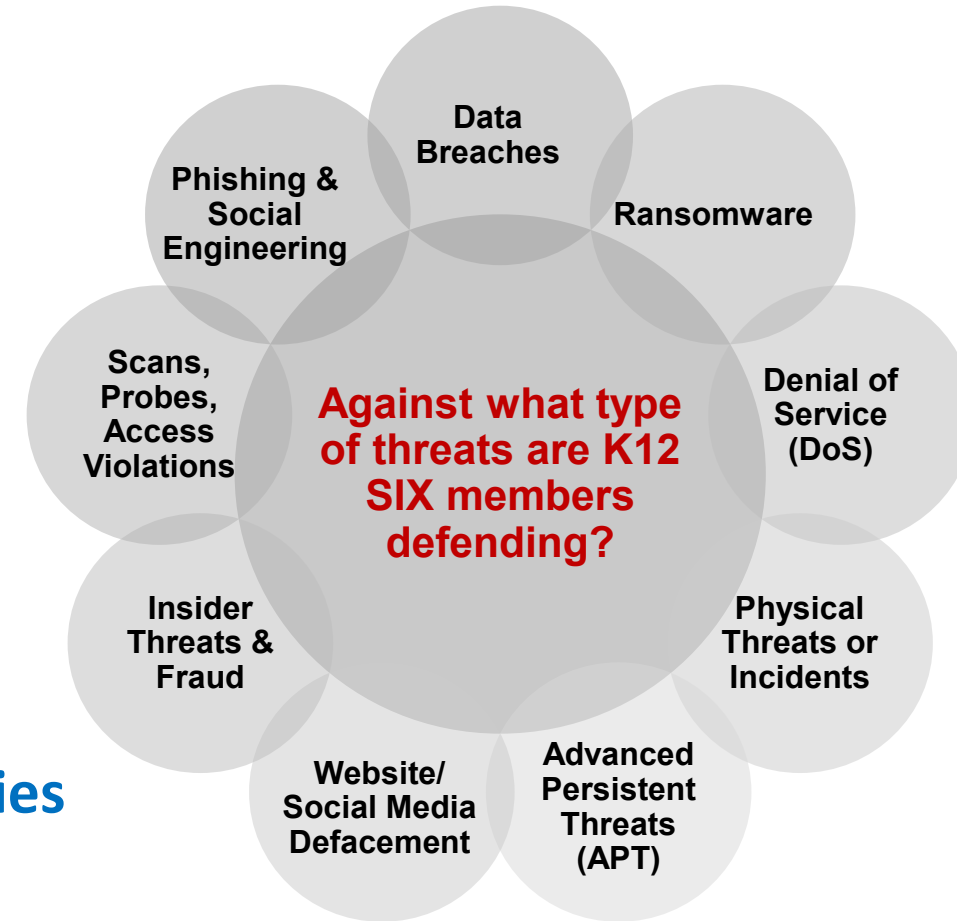
2024 WEBINAR SERIES

APRIL 2, 2024

Brought to you by:
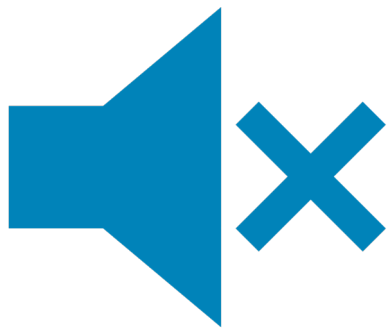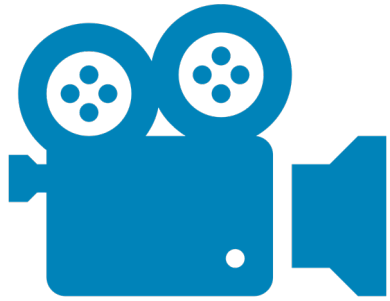
K12 Security Information eXchange (K12 SIX)

- A Global Resilience Federation (GRF) member community, K12 SIX is a real-time cyber threat intelligence sharing hub **exclusively for schools**, to aid in preventing and mitigating cyber threats.

- This non-profit member community provides cost-effective collective defense by crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security team.

Collective defense | Best practices | Model policies
Professional development | Advocacy

https://www.k12six.org/member-benefits

Against what type of threats are K12 SIX members defending?

- Data Breaches
- Ransomware
- Denial of Service (DoS)
- Physical Threats or Incidents
- Advanced Persistent Threats (APT)
- Website/ Social Media Defacement
- Insider Threats & Fraud
- Scans, Probes, Access Violations
- Phishing & Social Engineering

Housekeeping

✓ **Yes! This webinar is being recorded.** You will receive a link to the recording and slides via email shortly after the webinar.

✓ **Questions for Presenters?** Please submit them via the Zoom Q&A panel.

✓ **Comments?** All attendees are muted. Feel free to ask questions and/or provide your insights to other attendees in the Zoom Chat panel.

✓ **We want your feedback!** Look for a quick post-webinar survey to share your thoughts.

Copilot for Microsoft 365

Microsoft 365 A3 and A5 security and compliance

Ash Sumer
Sr. Technical Specialist
Microsoft US Education

Jumpstart the creative process and generate ideas while writing

With Copilot in Word, transform writing with efficiency and creativity.

- Create first draft by referencing up to three documents

- Rewrite sections or an entire document, or change the tone to refine existing documents

- Receive suggestions to strengthen arguments, smooth inconsistencies

- Save time and summarize text in lengthy documents

- Discover information—for example, ask if there is a call to action
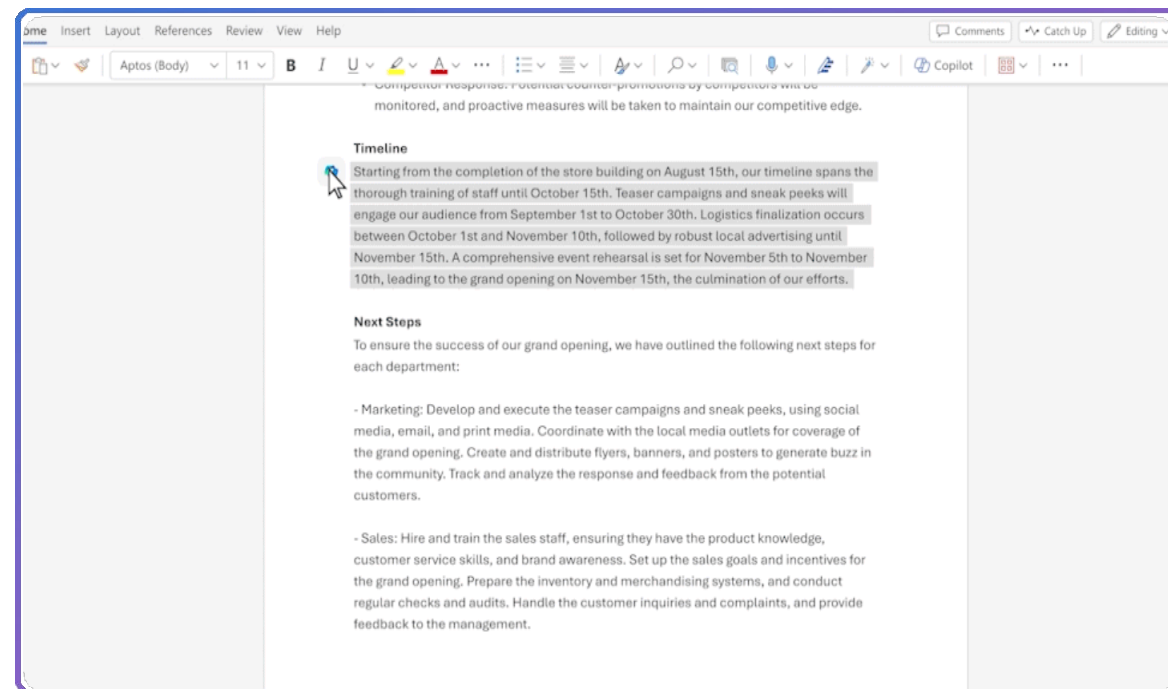
Copilot in Word

Stay focused on closing deals with an AI assistant for email

With Copilot in Outlook, stay on top of your inbox, manage meeting follow-ups, and create impactful communication in a fraction of the time.

- Customize an email prompt with options for length and tone

- Include people's viewpoints in conversation summaries

- Summarize email threads to catch up quickly
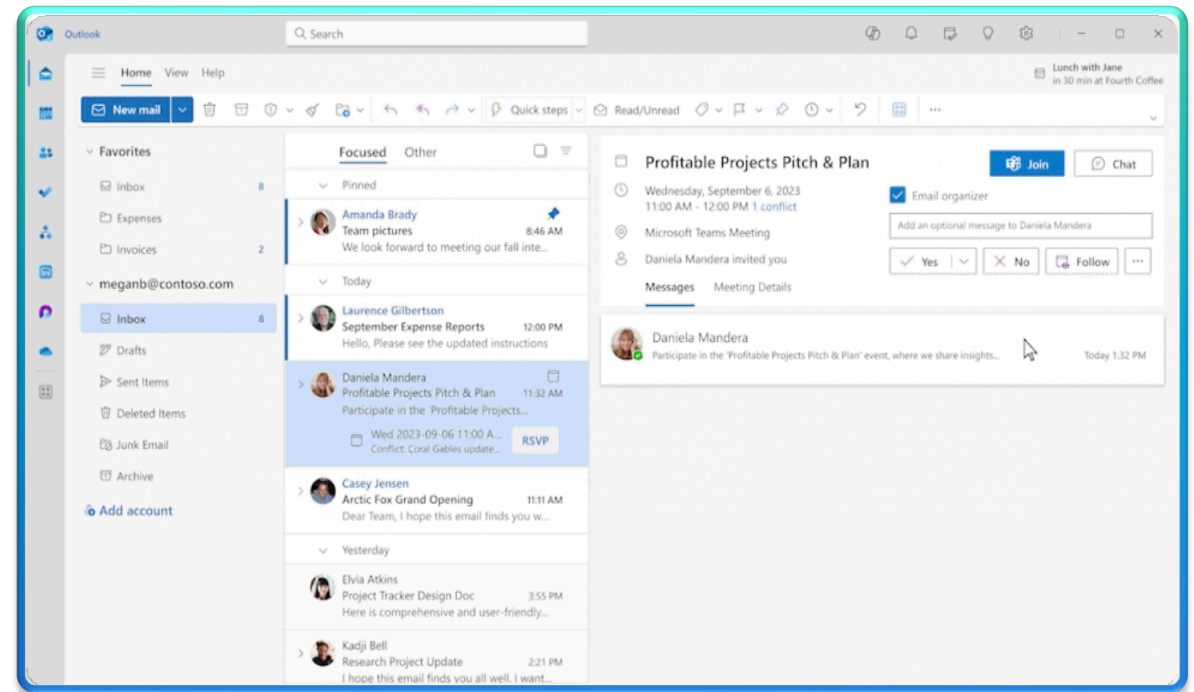
Copilot in Outlook

Simplify quality reporting and data validation

With Copilot in Excel, analyze, comprehend, and visualize data with ease.

- Create new formula columns or insert charts

- Insert pivot tables into new a sheet

- Refine data by providing simple commands

- Identify trends, create visualizations, or ask for recommendations with natural language queries

Copilot in Excel

Copilot for Microsoft 365

Unlock productivity and unleash creativity

Natural Language

| Large Language Models | + | Microsoft Graph - Your Data - | + | Microsoft 365 Apps | + | The Web |
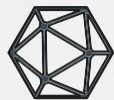
Microsoft 365 copilot basic architecture

Microsoft 365 Apps

Microsoft 365 Copilot

Microsoft 365 Service Boundary

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation models

Response + app commands

User prompt

Pre-processing

Grounding

Microsoft Graph

Post-processing

Semantic Index

Your context and content

emails, files, meetings, chats, calendars, and contacts

Customer Microsoft 365 Tenant

Modified prompt

LLM response

Large Language Model

Azure OpenAI instance is maintained by Microsoft. OpenAI has no access to the data or the model.

Azure OpenAI

RAI

RAI is performed on input prompt and output results

Data flow (🔒 = all requests are encrypted via HTTPS and wss://)

1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps

Copilot for Microsoft 365

Built on Microsoft's comprehensive approach

Security   +   Compliance   +   Privacy   +   Responsible AI

Microsoft's AI principles

Fairness

Reliability & Safety

Privacy & Security

Inclusiveness

Transparency

Accountability

Microsoft Cloud — AI you can trust

Your data is **your** data.

Your data is **not** used to train the OpenAI foundation models without permission.

Your data is **protected** by the most comprehensive enterprise compliance and security controls.

Copilot for Microsoft 365
inherits your security, compliance, and privacy policies

1

Manage overprivileged and risky users

Microsoft Entra ID

2

Mitigate Device Risk

Microsoft Intune

3

Secure and govern data

Microsoft Purview

4

Discover and control the use of AI apps

Microsoft Defender for Cloud Apps

Govern access to Copilot
Microsoft Entra ID

Users and Devices

1 **Manage overprivileged and risky users**
with Identity and access management

Microsoft Entra ID

2 Mitigate Device Risk
With Unified Endpoint management

Microsoft Intune

Copilot for Microsoft 365

✓ 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, risk detection.

✓ Decide access level with Conditional Access policies.

Allow access

Require MFA

Limit access

Password reset

Monitor access

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

Manage device estate
Microsoft Intune

Users and Devices

1. **Manage overprivileged and risky users**
   with Identity and access management

   Microsoft Entra ID

2. **Mitigate Device Risk**
   with Unified Endpoint management

   Microsoft Intune

Copilot for Microsoft 365
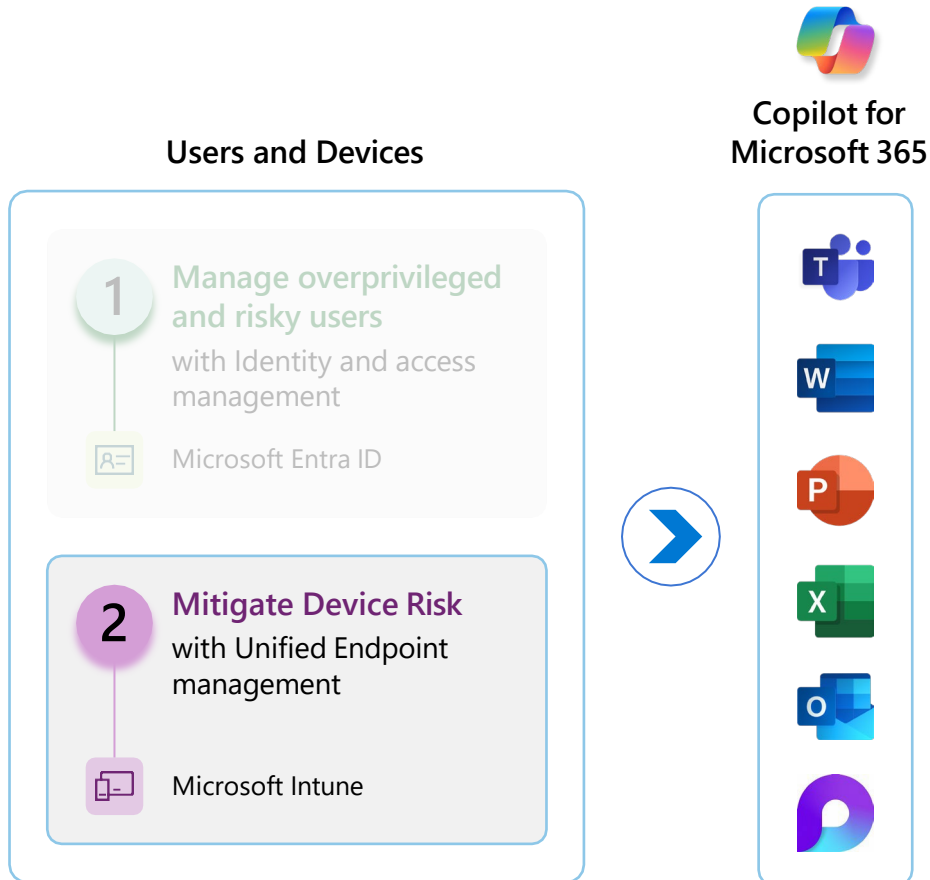
✓ Ensure the Microsoft 365 apps are securely installed on the user's device and kept up to date.

✓ 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

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

Secure and govern data in Copilot interactions
Microsoft Purview Information Protection

✓ Data consumption and processing with Copilot is limited to the user's permissions.

✓ Copilot inherits sensitive documents' sensitivity labels and applies them to its output and references.

✓ 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

Copilot for Microsoft 365

Your Organization Data

3 **Secure and govern data** in Copilot interactions

Microsoft Purview

Discover and control the use of AI apps
Microsoft Defender for Cloud Apps

Users and Devices

Microsoft 365 Apps

Your Organization Data

1 **Manage overprivileged and risky users**
with Identity and access management

Microsoft Entra ID

2 **Mitigate Device Risk**
With Unified Endpoint management

Microsoft Intune

Copilot for Microsoft 365

3 **Secure and govern data**
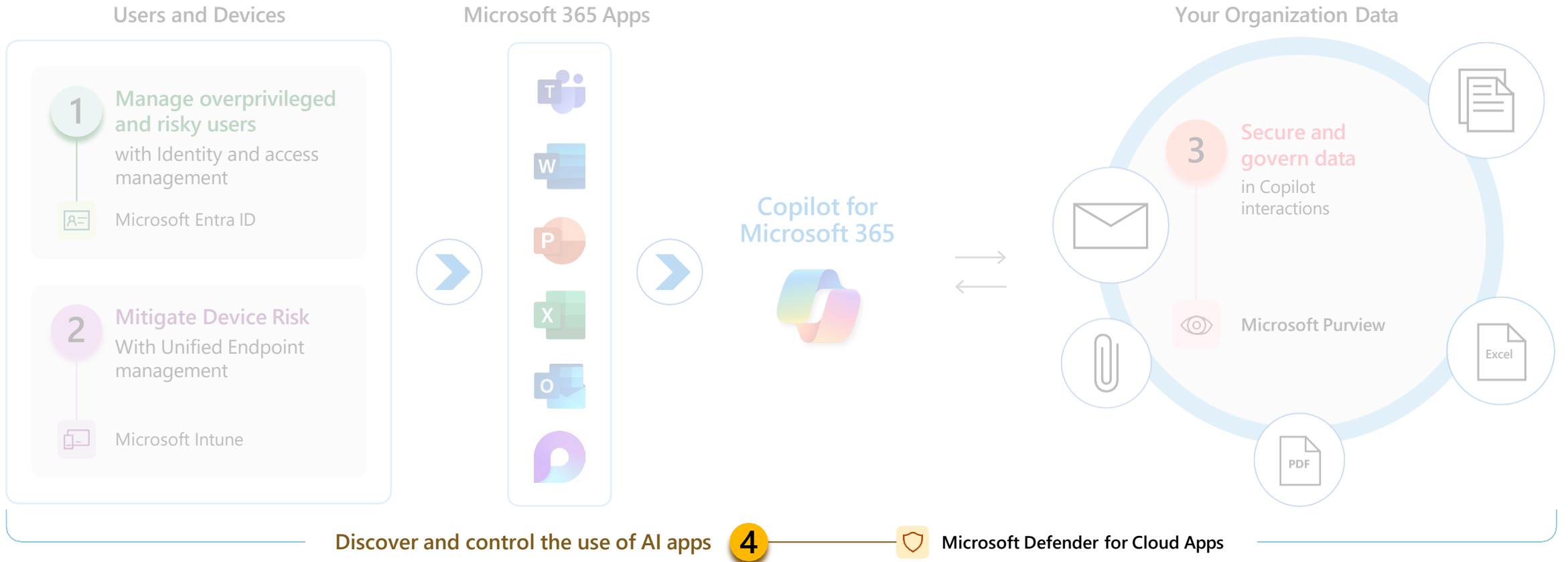in Copilot interactions

Microsoft Purview

Excel

PDF

Discover and control the use of AI apps 4 — 🛡 **Microsoft Defender for Cloud Apps**

✓ Discover & assess the risk across 400+ AI apps in an organization

✓ Block or approve the use of discovered AI apps in the organization

Security and compliance controls for Copilot for Microsoft 365

Users and Devices

1 **Manage overprivileged and risky users** with Identity and access management

Microsoft Entra ID

2 **Mitigate Device Risk** With Unified Endpoint management

Microsoft Intune

Microsoft 365 Apps

Copilot for Microsoft 365

Your Organization Data

3 **Secure and govern data** in Copilot interactions

Microsoft Purview

4 Discover and control the use of AI apps — Microsoft Defender for Cloud Apps

Microsoft 365 Security and Compliance controls for Copilot

Baseline security

Copilot + Office 365 A3

Multi-factor Authentication with security defaults

Manual sensitivity and retention labels for content that can be processed by Copilot (Office only)

Core security controls

Copilot + Microsoft 365 A3

Conditional Access policies based on identity, device, location, and network

Manual sensitivity and retention labels for content that can be processed by Copilot (Office + non-Office files, e.g., pdf)

Unified Endpoint management capabilities
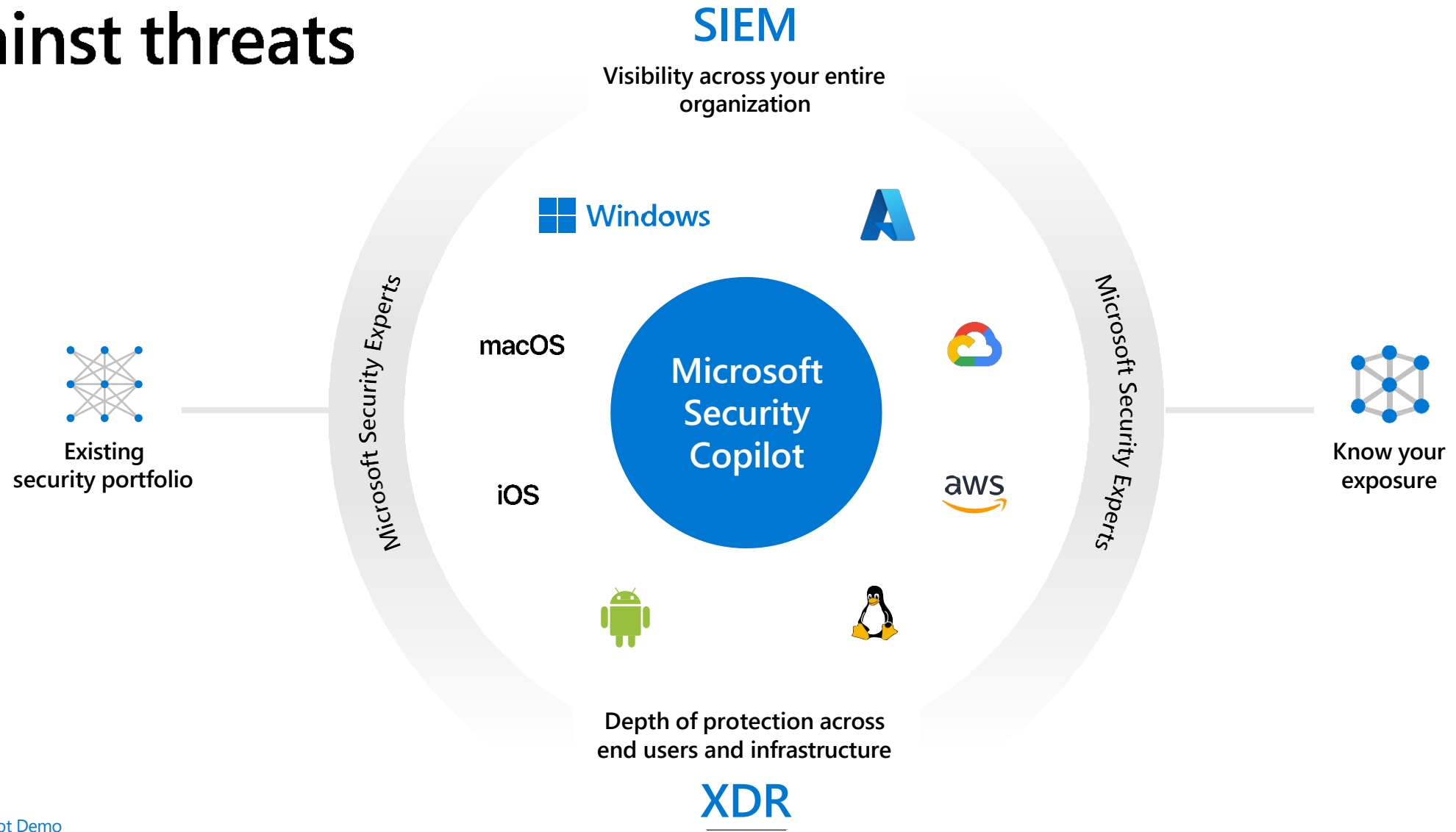
Best in class security controls

Copilot + Microsoft 365 A5

User/session risk and access control

Automatic sensitivity and retention labels for content that can be processed by Copilot

Discover and evaluate the risk of 400+ **AI apps** & implement **controls for their use** at work

Defending against threats

SIEM

Visibility across your entire organization

Microsoft Security Experts

Windows

macOS

iOS

Microsoft Security Copilot

aws

Microsoft Security Experts

Existing security portfolio

Know your exposure

Depth of protection across end users and infrastructure

XDR

Security Copilot Demo

Microsoft 365

Thank you.

K12 SIX Wants Your Feedback on Today's Webinar

K12 SIX Webinar Feedback

Follow the QR code or visit
https://forms.office.com/r/qipifEfkzb

to provide K12 SIX with your feedback on today's webinar.

K12 SIX Public Resources

- **The K-12 Cyber Incident Map:** https://www.k12six.org/map **and "State of K-12 Cybersecurity: Year in Review" report series** https://www.k12six.org/the-report

- **K12 SIX 'Essentials' Series:** https://www.k12six.org/essentials-series
  - Cybersecurity Frameworks: What K-12 Leaders Need to Know
  - K-12 Essential Cybersecurity Protections Series for 23-24 SY
  - K-12 Cyber Incident Response Runbook

- **Webinar Series:** https://www.k12six.org/webinars
  - 4/16: "Balancing Cybersecurity with Learning" (Clever)

Questions? Contact us at info@k12six.org