Microsoft 365
COMMUNITY CONFERENCE

Mission Readiness - Cybersecurity and Copilot in the Public Sector

Karuana Gatimu
Director, Customer Advocacy
AI & Collaboration
Microsoft

LinkedIn Profile

Microsoft

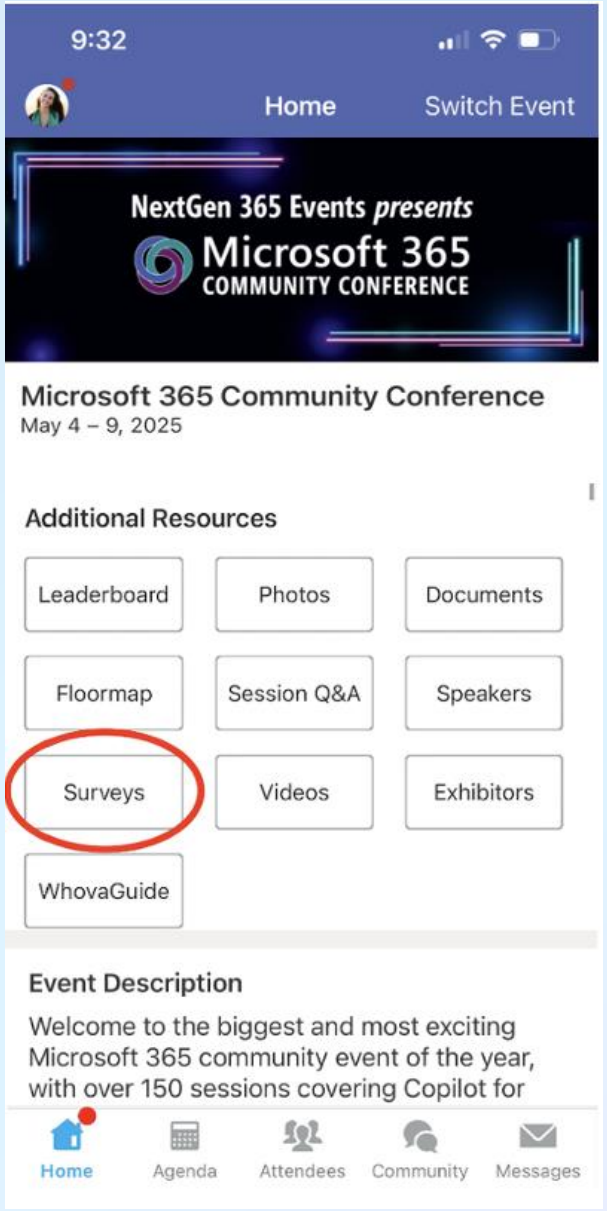
Whova

The official event app for the
Microsoft 365 Community Conference

Event invitation code: Orlando2026

Join the event app to access:

- Event announcements
- Personalized agenda, session details
- Speaker & attendee profiles
- Networking, meet-ups, messages
- Event documents



Session feedback surveys

We want to hear from YOU!

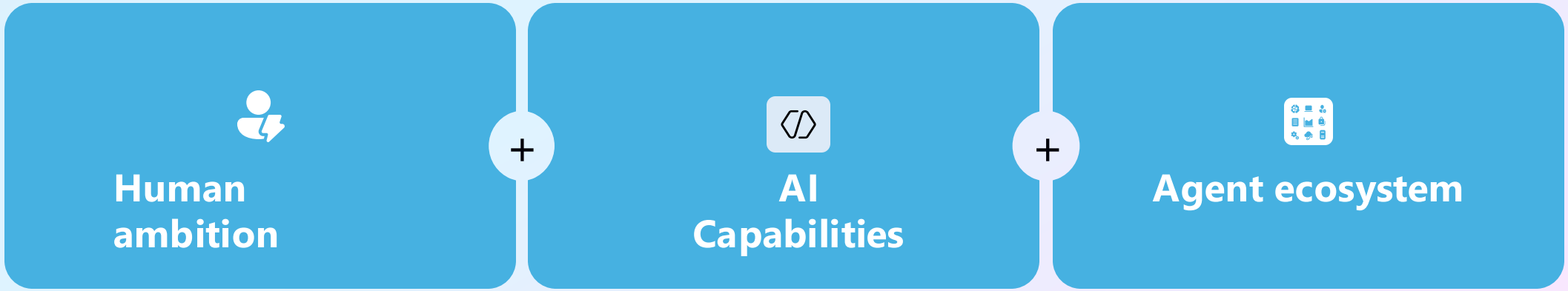
Share your feedback to make next years conference even better!

Here's how –

- Simply go to the Whova App on your smartphone.
- Scroll down on the M365 Community Conference Homepage to 'Additional Resources' to click "Surveys'.
- Click Session Feedback.
- Scroll down to find this session title.
- Complete the session feedback survey.
- Finally, click 'Submit'.

It's just that easy!

Democratizing intelligence



The AI challenge

AI needs execution

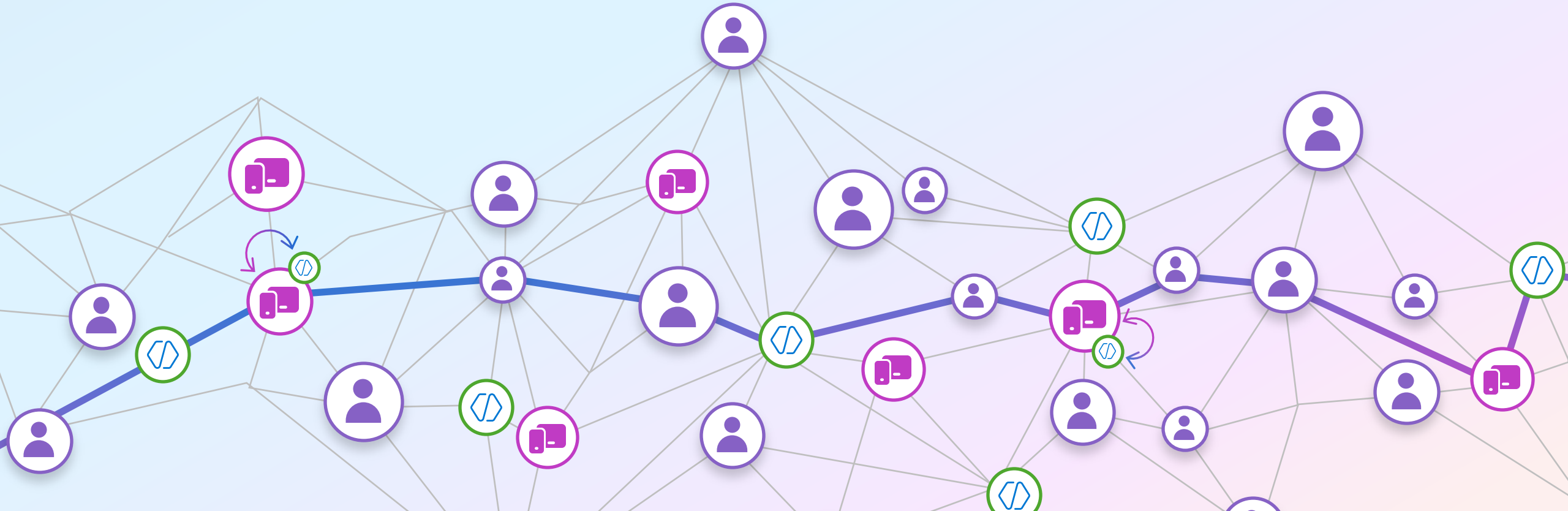
AI requires structured workflows to transform potential into performance.

Insights need action

AI insights remain dormant until deployed through applications.

AI needs boundaries

Governance controls secures AI within business parameters.



Common Challenges facing Public Sector Executives

- **Accelerating AI adoption while modernizing aging infrastructure** — Many rank AI as a top priority, but infrastructure modernization lags behind executive support, creating a gap that threatens mission execution.
- **Budget pressures and mandated cost reductions** — Most face significant cost-cutting requirements and tighter operating budgets, forcing consolidation, automation, and enterprise service adoption.
- **Strengthening cybersecurity amid evolving threats** — Rising cyber risks and hybrid infrastructure complexity require agencies to improve resilience, adopt zero-trust, and secure AI while navigating fragmented oversight and regulatory demands.
- **Managing workforce disruption and talent shortages** — Workforce downsizing and increasing demand for digital services leave CIOs balancing modernization with fewer staff.
- **Navigating compliance, data governance, and cross-agency interoperability** — Organizations must deliver secure, compliant, data-driven services while aligning to stringent federal data standards and improving interagency collaboration.

The Sovereignty Challenge

Digital sovereignty has increasingly played a critical role in global affairs amidst a swiftly changing global landscape.

The digital sovereignty landscape is evolving, driven by growing consideration for data security, compliance, global trade and geopolitical issues.

Digital sovereignty goes beyond just privacy. It includes:

- Ensuring control and visibility over access to data
- Protecting data from security breaches and malicious activity
- Meeting the evolving regulatory and compliance requirements

Organizations must balance strategic goals with sovereignty considerations. Microsoft offers a comprehensive suite of solutions to help meet your sovereignty needs.

The promise of AI: A national imperative

Economic growth and competitiveness

AI is projected to have a cumulative global economic impact of **$19.9 trillion** through 2030 and **drive 3.5% of global GDP** in 2030.

Source: The Global Impact of Artificial Intelligence on the Economy and Jobs: AI will Steer 3.5% of GDP in 2030, Document number:# US51057924, August 2024

Transformational impact across industries

From healthcare and education to manufacturing and national security, AI is driving unprecedented **efficiency, innovation, and new business models.**

Public service and social prosperity

AI can **streamline government operations, enhance citizen engagement, and improve public service delivery**, creating more inclusive and responsive governance.

As AI adoption accelerates, it is crucial to balance national strategic objectives with sovereign considerations.

Harnessing AI to drive economic transformation, innovation, and global competitiveness

Safeguarding national sovereignty, security, and regulatory compliance in an increasingly hyperscale world

Becoming Frontier | Government

Enrich employee experiences

by automating daily tasks, employees can focus on agency missions, leading to faster and more informed decisions

Reinvent citizen engagement

by enhancing citizen services with 24–7 autonomous self-service portals

Reshape government processes

through AI-powered data management and collaboration, to make agency operations more efficient

Bend the curve on innovation

through human-led, agent orchestrated government-as-a-platform to unlock agility, speed and scale

Next Step: Schedule an Agentic Workshop

Safeguard government systems with AI security

1. Detect and disrupt threats in real-time using AI algorithms to protect sensitive data.
2. Strengthen cybersecurity posture of government systems.
3. Prevent cyber attack disruptions from nation state and cyber criminal organizations.
4. Shift cyber defense paradigm from manually-driven detections to automated-scalable remediations.
5. Improve collective cyber defense and threat intelligence across national government.
6. Enhance cyber-resiliency by continuous monitoring to protect against evolving threats.
7. Unified SecOps Experience.
8. Quick Triaging and Attack Disruption.

Consistent infrastructure management and development platform

Configuration management and governance

- Azure Update Manager
- Configuration Management
- Azure Policy
- Inventory Management

Resiliency and observability

- Azure Monitor
- Chaos Studio
- Site Recovery

Built-in security and control

- Microsoft Defender for Cloud

Universal AI assistant, portal and tools

- Copilot in Azure
- Azure Portal
- Powershell and CLI

Azure Services across your infrastructure

Azure

- Windows Server
- SQL
- Kubernetes
- Linux

Multi-cloud

- aws
- Google Cloud
- ORACLE

On-premises

- vmware by Broadcom
- NUTANIX
- Azure Local
- Microsoft Hyper-V

Enabled by Azure Arc

AI Enabled Enterprise Capabilities

Base LLM Chat

Secure generative AI chat allowing employees to ideate, draft content, analyze documents, generate images, leverage enterprise agents

M365 Copilot Chat

AI Enhanced Automation

User, group, and enterprise workflows, scheduled and event-based automations that can leverage generative AI

Power Automate

Knowledge Bots/Agents

Unlock organization knowledge providing self service solutions. Enable business groups to quickly build knowledge solutions

Copilot Studio
Power Apps

Governed LLM & API Access

Enterprise level LLM access, catalog, control. Focal point for enterprise API access. Enabling groups to build solutions and leverage APIs seamlessly

Azure Foundry

Agentic AI

Framework and services for enabling end user and organization level Agents and Agentic Orchestrations

Power Apps

End User AI Productivity Tools

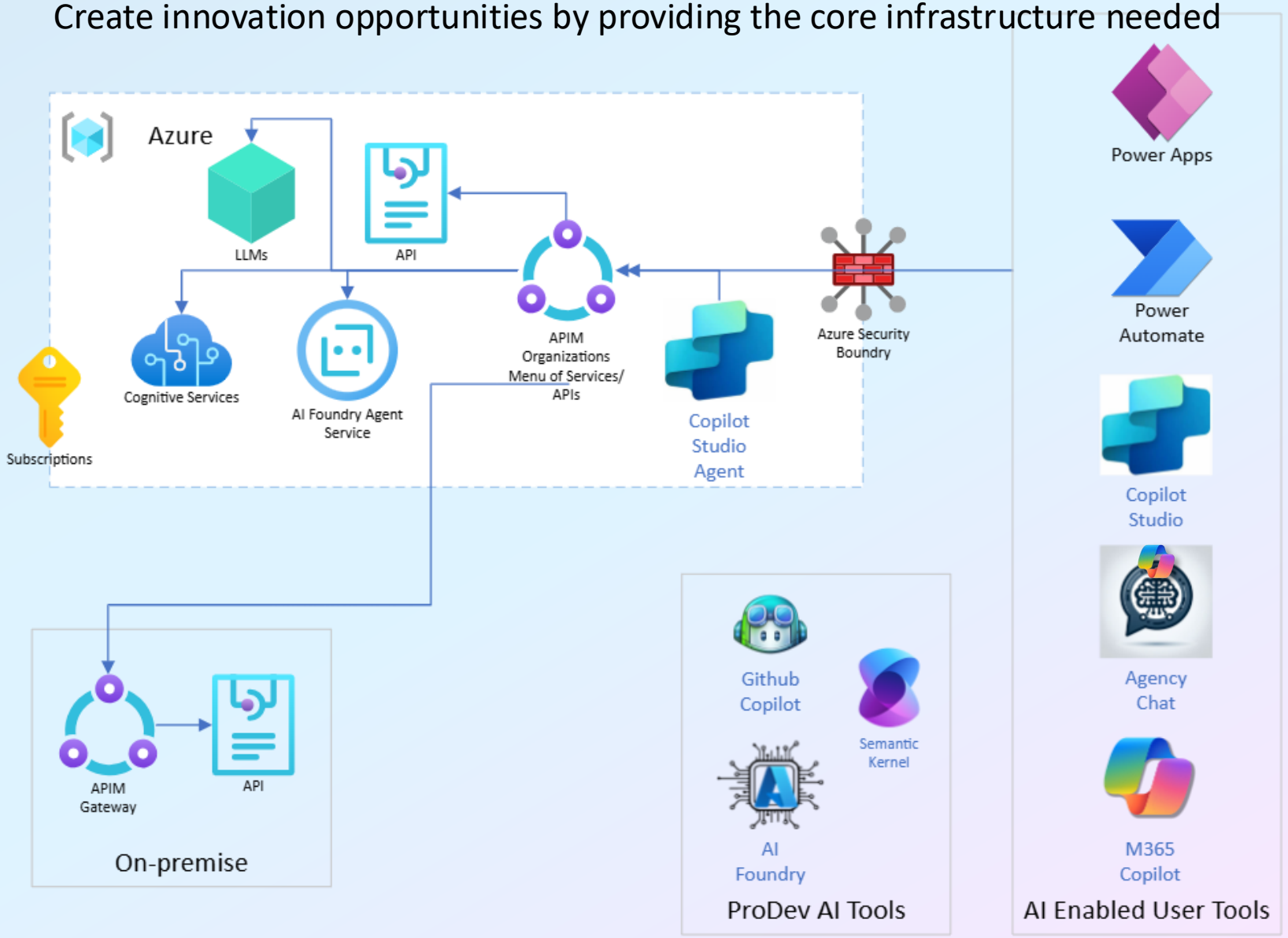
Increase user productivity in the applications they leverage throughout the day and on the go

M365 Copilot

What capabilities do you want to provide to empower the mission? These are our recommended capabilities to move towards an established AI Enabled Frontier Enterprise.

AI Enabled Enterprise

Create innovation opportunities by providing the core infrastructure needed

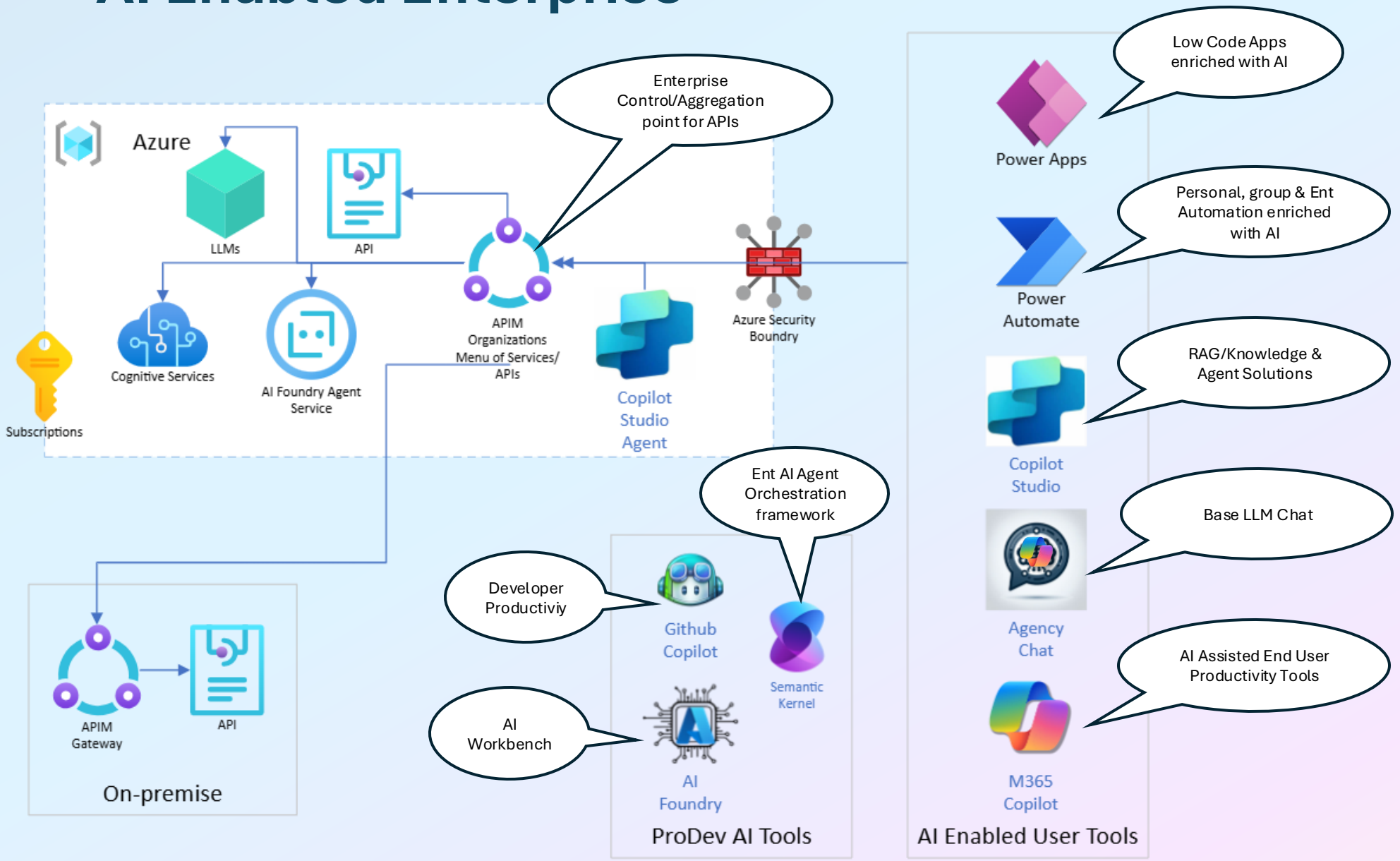


Securely operationalize AI at scale by providing integrated governance, compliance, and performance analytics across apps and agents.

It accelerates innovation and delivers measurable ROI through productivity gains, cost efficiency, and enhanced customer experience.

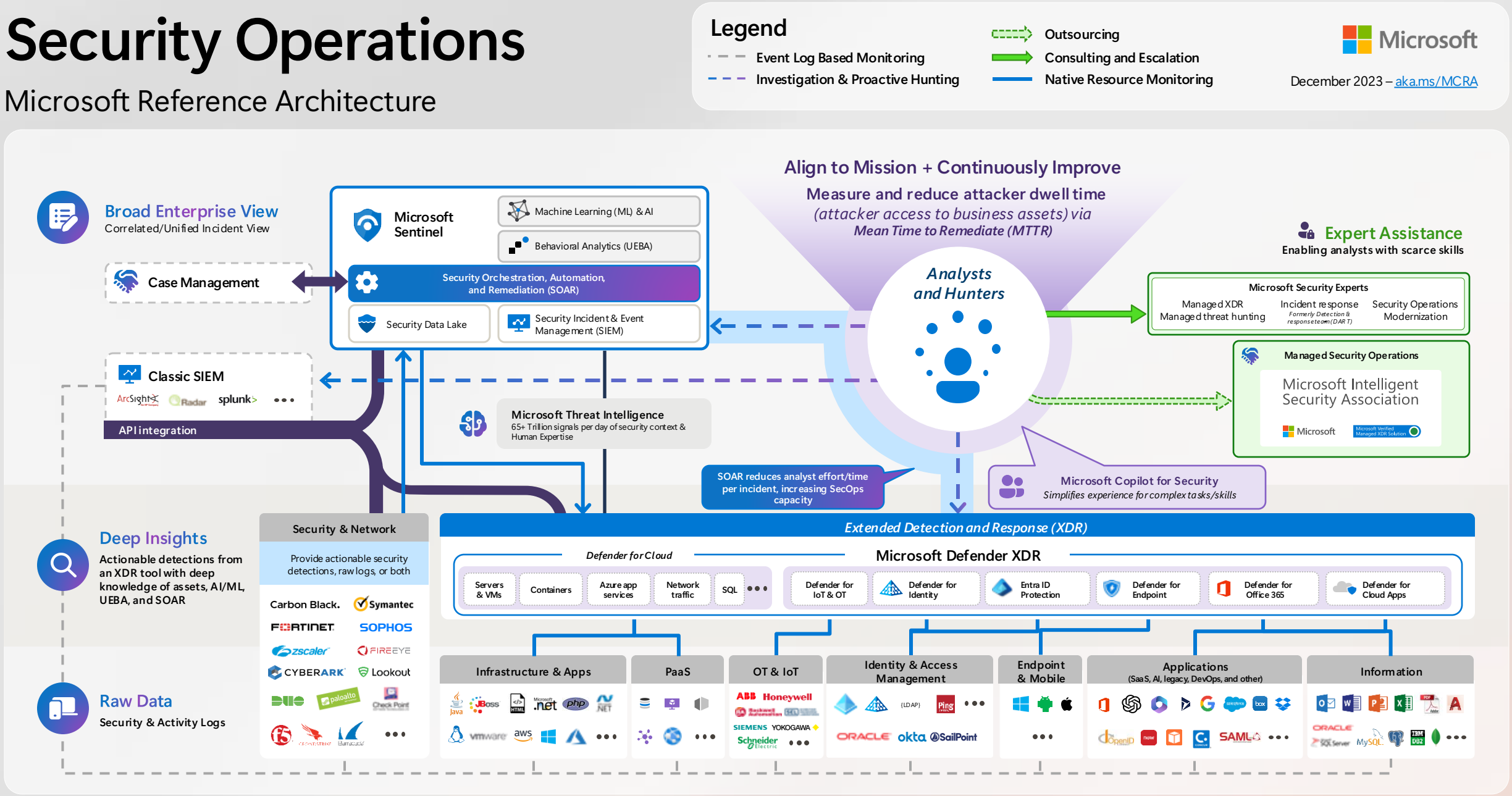
Ask about having an AI Enabled Enterprise discussion!

AI Enabled Enterprise



Security Operations

Microsoft Reference Architecture



Implement AI with confidence, at scale

AI operationalization done right – secure by design, integrated by default

Secure execution

Enforce safe logic execution across agents by embedding business logic rules safely and preventing data leaks and insider threats.

Govern usage

Codify policies, enforce compliance, and ensure agents and apps behave ethically and consistently.

Operate efficiently

Ensure consistency and precision, at scale, with centralized deployment, management, and optimization of AI apps and agents from a single, secure control point.

Monitor performance

Track AI impact and KPIs in real-time, and use performance analytics to uncover trends, guide improvements, and drive smarter decisions.

Enable secure, enterprise-grade AI at scale with a fully managed platform

AI Enabled Enterprise Capabilities

Base LLM Chat

Secure generative AI chat allowing employees to ideate, draft content, analyze documents, generate images, leverage enterprise agents

AI Enhanced Automation

User, group, and enterprise workflows, scheduled and event-based automations that can leverage generative AI

Knowledge Bots/Agents

Unlock organization knowledge providing self service solutions. Enable business groups to quickly build knowledge solutions

Governed LLM & API Access

Enterprise level LLM access, catalog, control. Focal point for enterprise API access. Enabling groups to build solutions and leverage APIs seamlessly

Agentic AI

Framework and services for enabling end user and organization level Agents and Agentic Orchestrations

End User AI Productivity Tools

Increase user productivity in the applications they leverage throughout the day and on the go

AI is transforming ~~technology~~

the human experience

While products mature
now is the time to

Applying Zero Trust Principles to Microsoft 365 Copilot

Building a Security Foundation Before, During, and After Copilot Deployment

April 2026

Why Security Before Copilot?

Copilot inherits whatever permissions and data exposure already exist in your tenant -- if your security foundation is weak, Copilot amplifies the risk.

- Copilot accesses the same data a user can see via Microsoft Graph -- emails, documents, chats, SharePoint sites, and OneDrive files
- If sensitive files are overshared or mislabeled, Copilot will surface them in responses
- The Zero Trust strategy -- "never trust, always verify" -- treats every connection and resource request as though it originated from an uncontrolled network
- Building a Zero Trust foundation is not just a Copilot prerequisite; it strengthens your entire M365 security posture

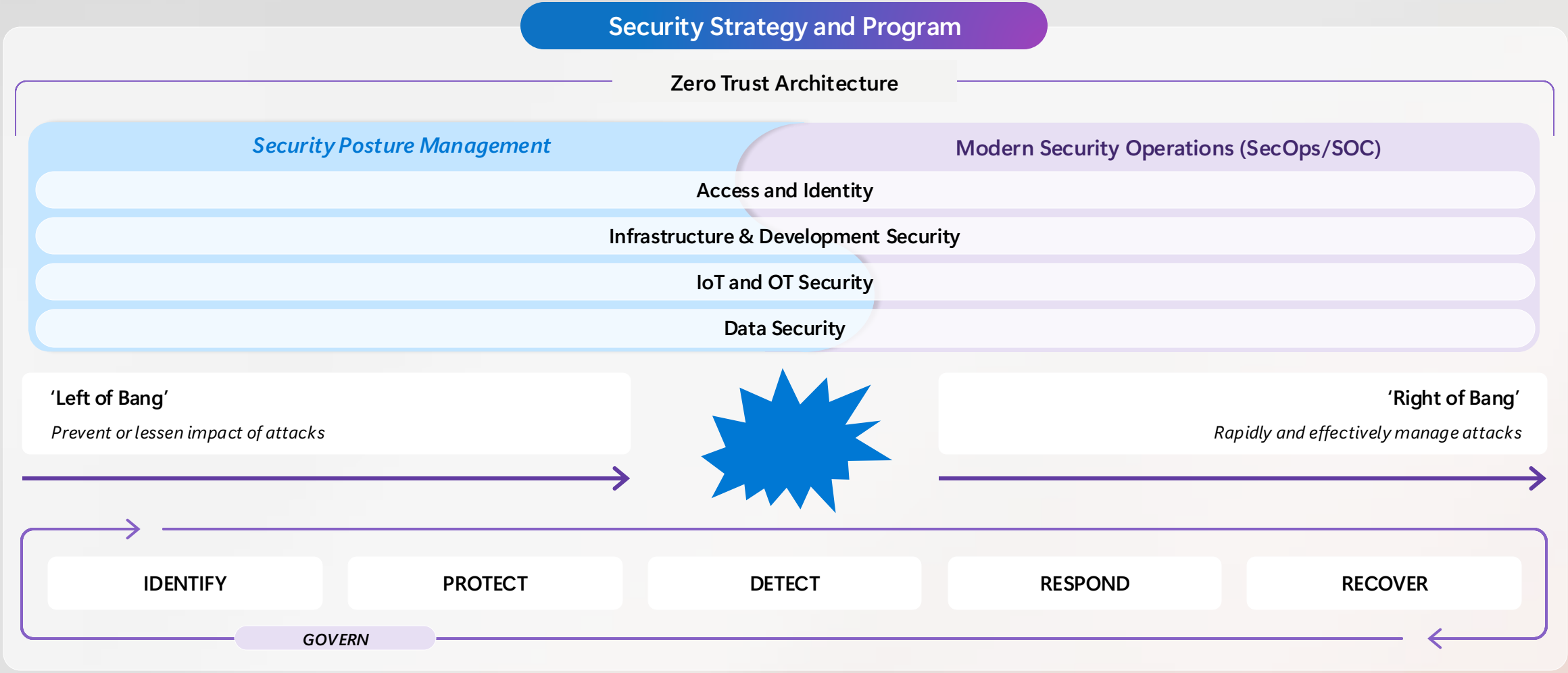
Seven Layers of Protection

Microsoft recommends seven distinct protection layers to secure your M365 tenant before enabling Copilot. [1]

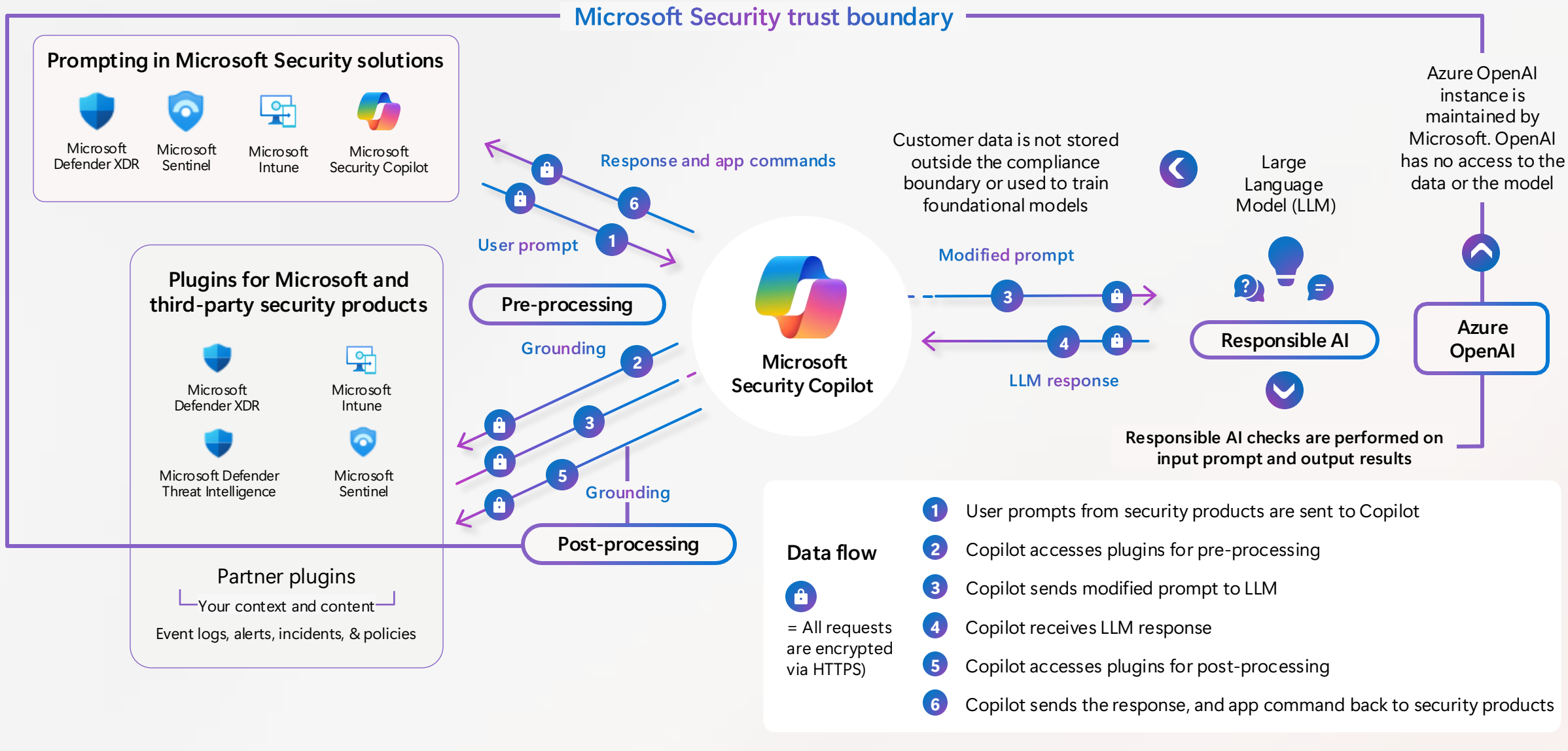
1. **Data Protection**
   Sensitivity labels, DLP policies, content classification
2. **Identity and Access**
   MFA, Conditional Access, risk-based authentication
3. **App Protection**
   Intune App Protection policies for managed apps
4. **Device Management and Protection**
   Device enrollment, compliance, endpoint DLP
5. **Threat Protection**
   Defender for Office 365, Defender for Endpoint, Defender XDR
6. **Secure Collaboration with Teams**
   Baseline, sensitive, and highly sensitive tiers
7. **User Permissions to Data**
   Least privilege access, site-level audits, oversharing reviews

End to End Security

Enable business mission and increasing security assurances with intentional approach



Data flow for Security Copilot (GCC)



Data Protection in Depth

Data classification and labeling are the most critical controls because Copilot respects sensitivity labels and DLP policies when generating responses. [2]

Classify and Label

Use Microsoft Purview Information Protection to classify and label documents and emails based on sensitivity [2]

Sensitivity Labels

Assign labels representing your sensitivity levels -- applied manually or automatically via auto-labeling policies

DLP Policies

Detect and block sensitive information (PII, PHI, financial data) to prevent Copilot from accessing protected content [4]

Encryption Settings

Configure encryption on sensitivity labels to prevent external sharing or unauthorized access

Retention Policies

Keep what you need and delete what you do not -- reducing stale content that Copilot might surface

Content Explorer

Use Content Explorer and Activity Explorer to verify classification coverage across your tenant

Identity, Access, and App Protection

Strong authentication and conditional access ensure that only verified users on compliant devices can trigger Copilot, while app protection keeps data contained within managed applications. [2]

Identity

Require MFA for all users via Conditional Access; evaluate sign-in risk and enforce step-up authentication when anomalies are detected. [2]

Access

Perform regular access reviews using Microsoft Entra ID Governance to prevent oversharing; use Privileged Identity Management (PIM) for just-in-time admin access. [2]

App Protection

Deploy Intune App Protection policies to ensure organizational data remains safe within managed apps; block data transfer to unmanaged apps. [2]

Device and Threat Protection

Enrolled and compliant devices paired with advanced threat detection create the perimeter that prevents compromised endpoints from misusing Copilot. [2]

Device Management

- Enroll devices in Microsoft Intune and enforce health and compliance requirements before granting access [2]
- Integrate Microsoft Defender for Endpoint with Intune for deeper device insights and risk-based compliance
- Extend DLP to endpoints using endpoint data loss prevention policies

Threat Protection

- Deploy Microsoft Defender for Office 365 and Defender for Endpoint to automatically prevent common attacks [2]
- Pilot and deploy Microsoft Defender XDR for unified, cross-domain threat protection
- Optionally integrate Microsoft Sentinel for SIEM-level detection and response across your environment

Secure Collaboration and Permissions

Copilot works within Teams, SharePoint, and OneDrive -- configuring tiered collaboration security and enforcing least-privilege access ensures Copilot only surfaces content people are authorized to see. [1]

Baseline

All teams: standard sharing and access controls applied organization-wide

Sensitive

Restricted sharing with limited guest access and tighter permissions

Highly Sensitive

Encryption and strict access controls for critical content

- Review external sharing policies to limit accidental data exposure to outside collaborators
- Audit access to shared content in SharePoint and Teams at the site and container level; enforce restrictions on information discovery [2]
- Use SharePoint Advanced Management to identify and remediate potential oversharing of files and sites
- Ensure sensitivity labels and DLP policies govern what Copilot can access at the file level

Data Hygiene and Readiness

Before enabling Copilot, clean up your data estate -- redundant, outdated, and trivial content will pollute Copilot responses and erode user trust. [2]

- Clean out ROT (redundant, outdated, trivial) content through an extensive audit of documents, emails, chats, and wikis [2]
- Consolidate multiple file versions and retain only the final, current version
- Standardize file naming conventions and add metadata to improve search relevance
- Assign a data steward to oversee ongoing data governance, access rules, and Copilot data utilization [2]
- Promote data hygiene habits through organization-wide training and change management
- Perform monthly permission audits, quarterly oversharing scans, and annual policy reviews [2]

From Strategy to Deployment

A successful mission-readiness journey follows a clear path -- from Zero Trust foundations through Copilot enablement to autonomous security operations.

Step 1

Assess

Run the Microsoft Zero Trust Assessment against your Entra tenant to measure current posture and identify gaps across Identity, Devices, Data, and Network.

Step 2

Secure

Deploy Zero Trust controls across all pillars using CISA Maturity Model guidance, prioritizing phishing-resistant MFA, endpoint protection, and data classification.

Step 3

Enable

Activate Microsoft 365 Copilot for productivity and Security Copilot for SOC operations within your government cloud tier (GCC, GCC-High, or DoD).

Step 4

Scale

Build custom agents with Agent Builder and Copilot Studio, extend agentic capabilities to Teams and Microsoft 365, and leverage the OneGov pricing advantage.

Parallel Rollout Strategy

You do not have to finish all protections before starting Copilot -- deploy protections and Copilot licenses in parallel, phasing in users as each layer is validated. [2]

1. **Deploy Foundational Protections**

   Identity (MFA, Conditional Access), data protection (sensitivity labels, DLP), and device enrollment

2. **Pilot Copilot Licenses**

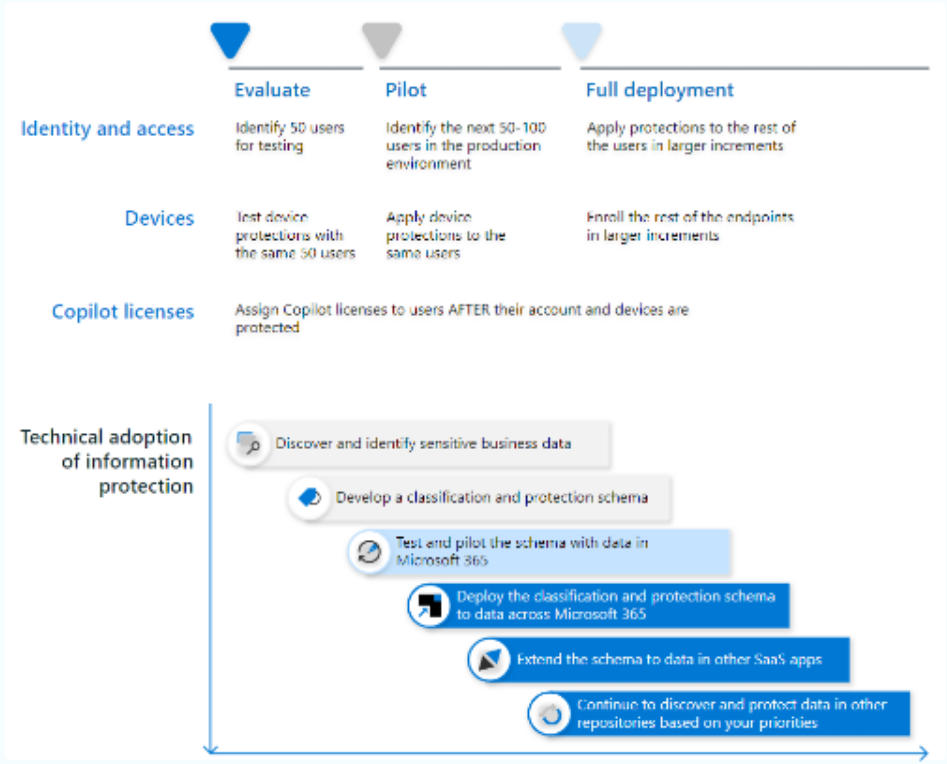
   Assign Copilot licenses to early adopters on fully protected accounts and devices [2]

3. **Expand Protections and Users**

   Add threat protection (Defender XDR), secure collaboration tiers, and permissions reviews; expand Copilot to additional groups

4. **Enterprise-Wide Rollout**

   Full monitoring via Copilot Dashboard in Viva Insights and Microsoft Purview Audit to track usage and detect anomalies [4]



Source: Get Ready for M365 Copilot Checklist

Your Mission Starts Now

The window to act is open -- leverage the tools, the pricing, and the momentum to transform your agency's security posture and operational readiness.

- **FastTrack Partners** -- Engage for technical expertise and deployment support: aka.ms/Microsoft/FastTrack [10]
- **Copilot Readiness Hub** -- Access role-based content and adoption planning: adoption.microsoft.com [10]
- **Public Sector Skilling** -- Leverage resources at aka.ms/PublicSectorCybersecurity and aka.ms/PubSec_ZeroTrust
- **Microsoft Account Team** -- Connect to align AI priorities and business outcomes to your agency's mission

We have an exciting future ahead.

Next Steps

The Chief Information Security Officer (CISO) Workshop

https://learn.microsoft.com/en-us/security/adoption/the-ciso-workshop

Microsoft Cybersecurity Reference Architectures

https://learn.microsoft.com/en-us/security/adoption/mcra

Microsoft Unified Engagements

https://learn.microsoft.com/en-us/security/adoption/adoption#microsoft-unified-engagements

Expertise and tools for your journey

Technical expertise via our FastTrack partners

aka.ms/Microsoft/FastTrack

Tools, resources & training on our Adoption Hub

adoption.microsoft.com

Events and real-world knowledge in our community

aka.ms/TechCommunity

appendix

Security Resources

Microsoft

Security Adoption Framework
aka.ms/saf

Security Hub
aka.ms/SecurityDocs

Security Strategy and Program
- CISO Workshop – aka.ms/CISOworkshop | -videos

End to End Security Architecture
- Microsoft Cybersecurity Reference Architectures (MCRA) – aka.ms/MCRA | -videos
- Ransomware and Extortion Mitigation – aka.ms/humanoperated
- Backup and restore plan to protect against ransomware – aka.ms/backup

Driving Business Outcomes Using Zero Trust
- Rapidly modernize your security posture for Zero Trust
- Secure remote and hybrid work with Zero Trust
- Identify and protect sensitive business data with Zero Trust
- Meet regulatory and compliance requirements with Zero Trust

- Zero Trust Workshop – aka.ms/ztworkshop
- Zero Trust Deployment Guidance – aka.ms/ztguide | aka.ms/ztramp

Secure Access and Identities

- Securing Privileged Access (SPA) Guidance aka.ms/SPA
- Access Control Discipline
- Ninja Training
  - Microsoft Defender for Identity aka.ms/mdininja
- MCRA Video
  - Zero Trust User Access
- Microsoft Entra Documentation aka.ms/entradocs

Modern Security Operations (SecOps/SOC)

- Incident Response – aka.ms/IR
- CDOC Case Study – aka.ms/ITSOC
- Ninja Training
  - Microsoft 365 Defender aka.ms/m365dninja
  - Microsoft Sentinel aka.ms/sentinelninja
  - Microsoft Defender for Office 365 aka.ms/mdoninja
  - Microsoft Defender for Endpoint aka.ms/mdeninja
  - Microsoft Cloud App Security aka.ms/mcasninja
- MCRA Videos
  - Security Operations
  - SecOps Integration

Infrastructure & Development Security

- Security Development Lifecycle (SDL)
  - Security Controls
- Microsoft Cloud Security Benchmark aka.ms/benchmarkdocs
- Well Architected Framework (WAF)
  - aka.ms/wafsecure
- Azure Security Top 10
  - aka.ms/azuresecuritytop10
- Ninja Training
  - Defender for Cloud
- MCRA Video
  - Infrastructure Security
- Defender for Cloud Documentation

Data Security

- Secure data with Zero Trust
- Ninja Training
  - Microsoft Purview Information Protection aka.ms/MIPNinja
  - Microsoft Purview Data Loss Prevention aka.ms/DLPNinja
  - Microsoft Purview Insider Risk Management
  - Insider Risk Management
  - Data Security for SOC aka.ms/NinjaDSforSOC
- Microsoft Purview Documentation aka.ms/purviewdocs

IoT and OT Security

- Ninja Training
  - Defender for IoT Training
- MCRA Videos
  - MCRA Video OT & IIoT Security
- Defender for IoT Documentation aka.ms/D4IoTDocs

Product Capabilities
www.microsoft.com/security/business

Security Product Documentation
Azure | Microsoft 365

Microsoft Security Response Center (MSRC)
www.microsoft.com/en-us/msrc

Key Industry References and Resources

The Open Group

- Zero Trust Commandments Standard – https://publications.opengroup.org/c247
- Zero Trust Reference Model – https://publications.opengroup.org/s232
- Security Principles for Architecture – https://publications.opengroup.org/c246

US National Institute of Standards and Technology (NIST)

- Cybersecurity Framework – https://www.nist.gov/cyberframework
- Zero Trust Architecture – https://www.nist.gov/publications/zero-trust-architecture
  - NCCoE Zero Trust Project – https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
- Secure Software Development Framework (SSDF) – https://csrc.nist.gov/pubs/sp/800/218/final

Cybersecurity and Infrastructure Security Agency (CISA)

- Zero Trust Maturity Model – https://www.cisa.gov/zero-trust-maturity-model

Center for Internet Security (CIS)

- CIS Benchmarks – https://www.cisecurity.org/cis-benchmarks/

Security Copilot Agents

Learn more about Security Copilot agents in the video overview:
aka.ms/SecurityCopilotAgentsVideo

Already using Security Copilot?

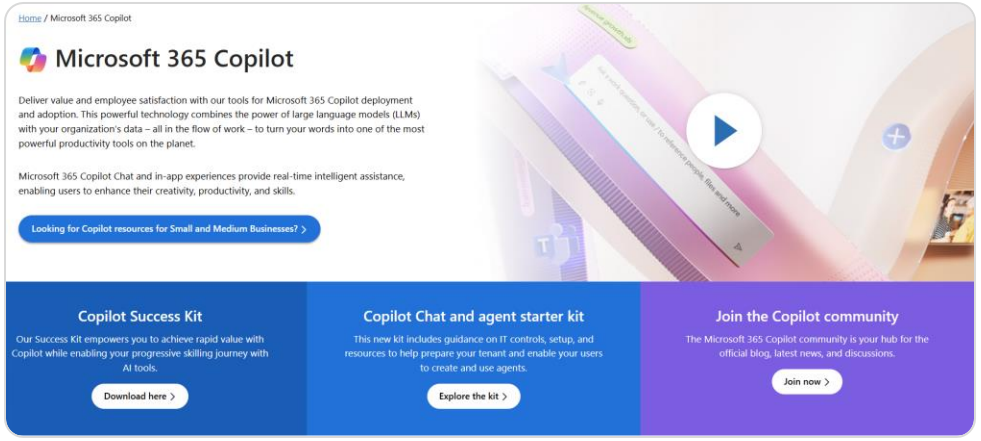
Make sure to join the Security Copilot CCP for the most updated information:
aka.ms/JoinCCP

References

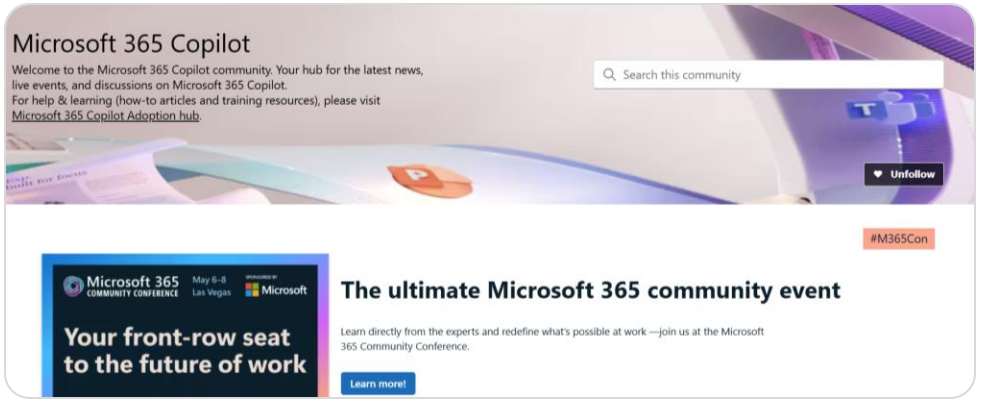
[1] Cybersecurity | Microsoft Public Sector Center of Exp...
[2] U.S. Public Sector Under Siege: Threat Intelligence f...
[3] Government & Public Sector Cybersecurity Market
[4] Continuing our momentum: Expanding Microsoft 365 Copi...
[5] Security Copilot in Defender: empowering the SOC with...
[6] Multi-Billion Dollar GSA OneGov Agreement with Micros...
[7] A strategic blueprint for zero trust standardization ...
[8] Zero Trust Implementation Guideline Primer
[9] Microsoft expands Copilot agentic tools in government...

News & community content

Microsoft Community Learning
aka.ms/Community/LearningChannel
Community led expert content on all your favorite Microsoft services.

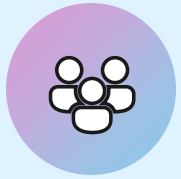


Start your week with live news and event updates aka.ms/MondaysatMicrosoft
Watch live or on-demand & share our blog.



Stay Connected!

Engage with the best community in tech… There's something for everyone!



Microsoft Tech Community

The community platform for Microsoft 365 – forums, blogs, and events

https://aka.ms/joinMTC

CommunityDays.org

Find or host a local event in your area or to match your interests

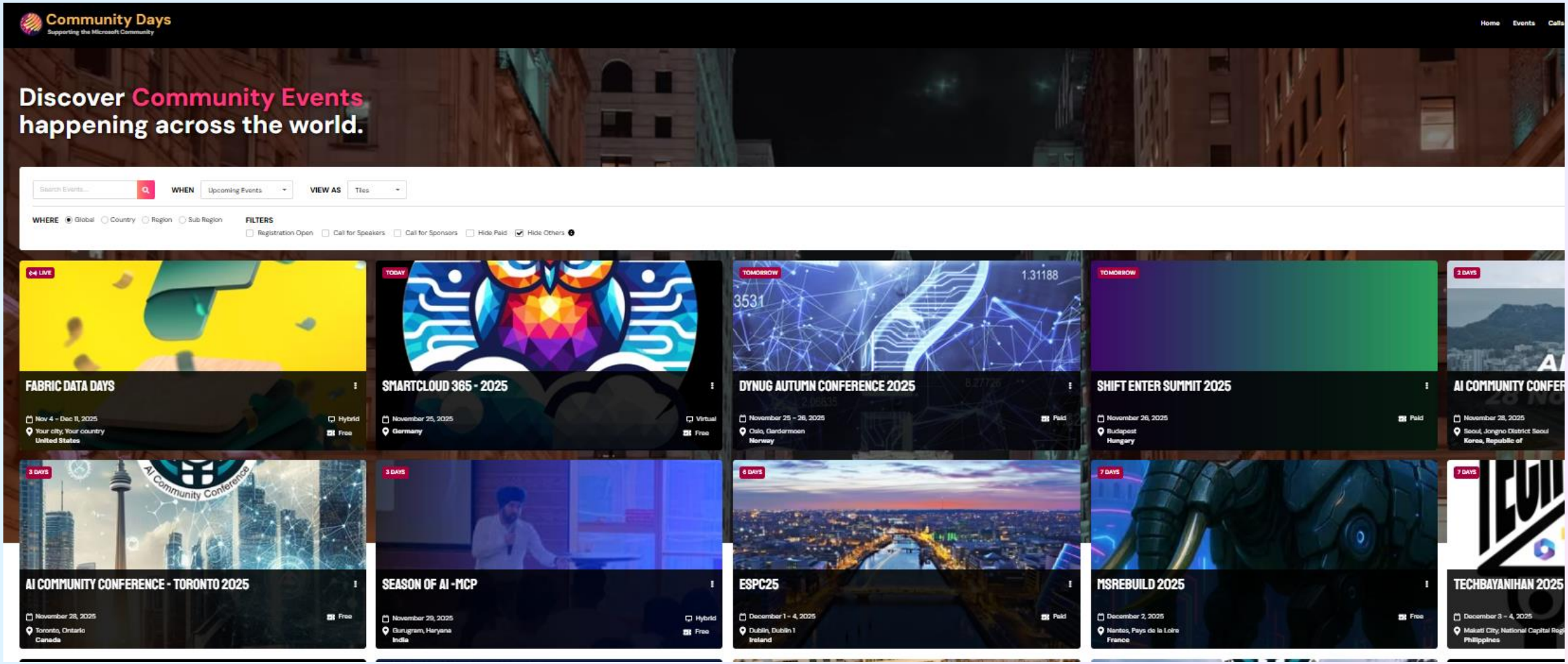
www.communitydays.org

Microsoft Community on LinkedIn

News, announcements and training delivered to your news feed

https://aka.ms/microsoftcommunitylinkedin

The one stop shop for Microsoft ecosystem community events

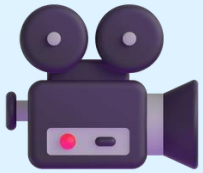


www.communitydays.org

SharePoint at 25 short film: *More than Code*

In honor of SharePoint's 25th birthday, *More Than Code* is a short film that explores the people, passion, and innovation behind one of the most transformative platforms in modern work. This film captures the stories of builders, leaders, and community champions who helped shape SharePoint into the knowledge backbone for collaboration, Copilot, and the next generation of agents.

SharePoint is more than code—it's 25 years of connection, innovation and impact.



Watch the digital premiere

Stream the documentary online globally in late April and celebrate SharePoint's 25-year journey from anywhere.

Watch the SharePoint at 25 digital event

Prepare for the film with a special digital event featuring insights, stories, and what's next for SharePoint in the era of AI.

Join MGCI – Learn, Share, Grow.

The Microsoft Global Community Initiative (MGCI) - Empowering global Microsoft communities with the tools, training, and resources to create impactful events and amplify diverse voices.

Learn, Share, Grow.

Event producers unite!

Join MGCI today!
https://aka.ms/MGCI

Thank you to our
Microsoft
Most Valuable
Professionals (MVP)
and Regional Directors!