Microsoft Security

What's New in Security, Compliance and Identity

Technical Presales & Deployment
https://aka.ms/TPD

Ricardo Trigueiro
ritrigue@microsoft.com

Daniela Magalhães
daniela.magalhaes@microsoft.com

Marco Carvalho Cardoso
macardo@microsoft.com

February'25

Agenda

- Intro
- News & Updates:
  - General News and Highlights
  - Entra
  - Intune
  - Sentinel
  - Defender XDR
  - Defender for Cloud
  - Security Copilot
  - Purview
  - Zero Trust
- TP&D
- Q&A

Intro

What’s New in Security, Compliance and Identity

- Monthly News and Updates for all things related with Microsoft Security, Compliance and Identity with a partner focus.

- Monthly, every third Thursday at 11am GMT+1

- Technical Presales & Deployment Team:
  - André Barreiros - abarreiros@microsoft.com
  - Daniela Magalhães - daniela.magalhaes@microsoft.com
  - Marco Carvalho Cardoso – macardo@microsoft.com
  - Ricardo Trigueiro – ritrigue@microsoft.com

What’s New series:

What’s New in Security, Compliance and Identity – Cloud Champion

What’s New and Highlights in Business Applications – Cloud Champion

What’s New in Modern Work – Cloud Champion

General News and Highlights

8 Lessons from the front lines of AI Red Teaming

- Microsoft AI Red Team conduct more than 100 Gen AI red teaming operations since 2018
- 8 Lessons:

1. Understand system capabilities and applications
2. Complex attacks aren't always necessary
3. AIRT is not safety benchmarking
4. Leverage automation for scale
5. Human element remains crucial
6. Responsible AI risks are pervasive but complex
7. LLMs amplify existing security risks and add new ones
8. The work of security AI systems will never be complete

References:

- Enhancing AI safety: Insights and lessons from red teaming | The Microsoft Cloud Blog
- MS_AIRT_Lessons_eBook.pdf

Learning and Training

- Showcase your skills with this new Security Certification | Microsoft Community Hub
  - Introducing the Microsoft Certified: Information Security Administrator Certification
  - Validate critical information security skills with our new Certification | Microsoft Community Hub
  - Exam SC-401: Administering Information Security in Microsoft 365 (beta) - Certifications | Microsoft Learn

- Microsoft Learn Challenge – Security Applied Skills:
  - Implement information protection and data loss prevention by using Microsoft Purview
  - Implement retention, eDiscovery, and Communication Compliance in Microsoft Purview
  - Defend against threats using Microsoft Defender XDR

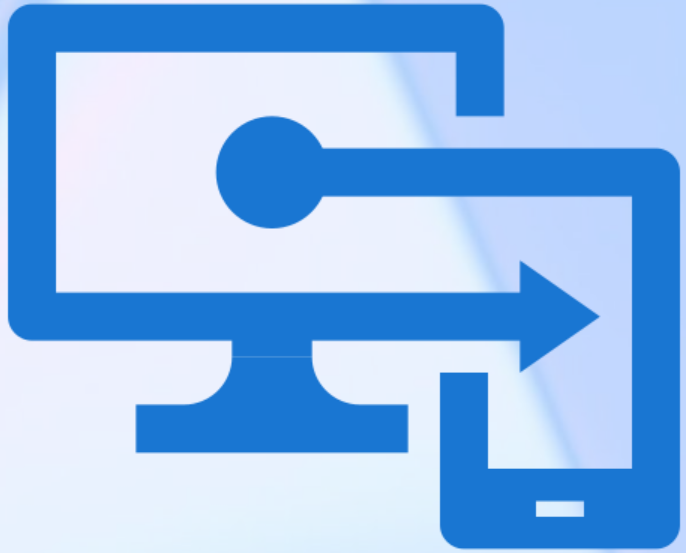
- Level Up your Security Skills with Microsoft Security Virtual Training Days
  - Feb 24-25, 2025: Defend Against Threats with Extended Detection and Response
  - Feb 27-28, 2025: Security, Compliance, and Identity Fundamentals
  - Mar 4-5, 2025: Implement Data Security with Microsoft Purview
  - Mar 10-11, 2025: Security, Compliance, and Identity Fundamentals
  - Mar 13-14, 2025: Modernize your Security Operations with Microsoft Sentinel
  - Mar 19-20, 2025: Security, Compliance, and Identity Fundamentals
  - Mar 24-25, 2025: Defend Against Threats with Extended Detection and Response
  - Mar 27-28, 2025: Security, Compliance, and Identity Fundamentals

Entra

Entra Updates

- Improving visibility into downstream tenant sign-ins — General Availability
- Microsoft Entra releases and announcements - Microsoft Entra | Microsoft Learn — General Availability
- New Identity Secure Score recommendations in General Availability | Microsoft Community Hub — General Availability
- Provision custom security attributes from HR sources (preview) - Microsoft Entra ID | Microsoft Learn — Public Preview
- Bulk update user properties in Entra ID — Public Preview
- New webinar series: How to secure access for your employees with the Microsoft Entra Suite | Microsoft Community Hub — Learn

Intune



Intune updates

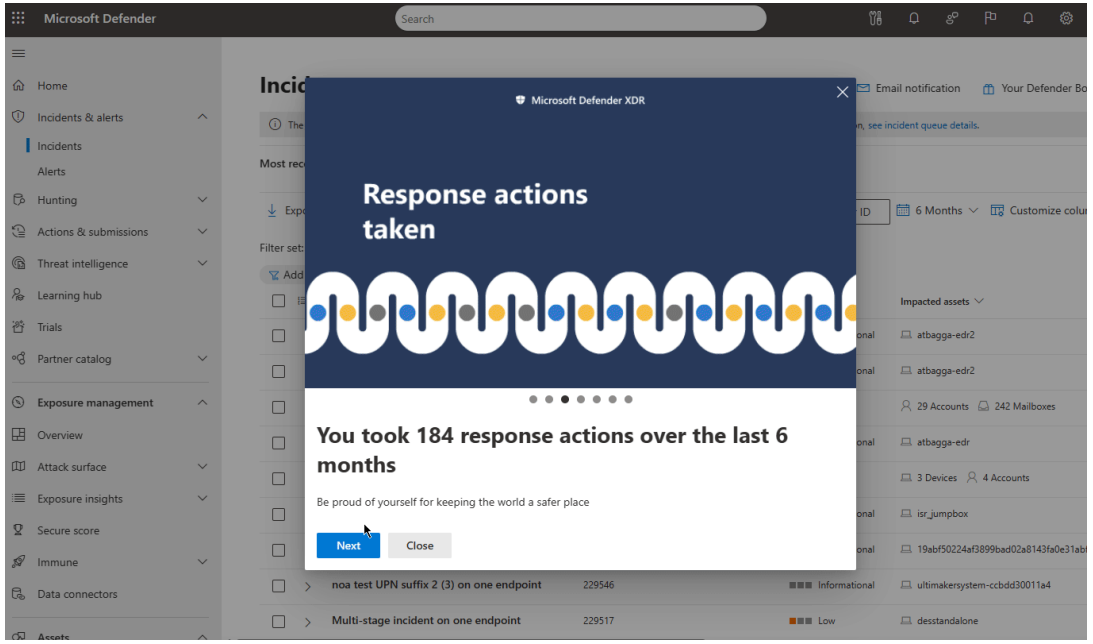
- Intune Plan 1
- New settings available in the Windows settings catalog to Configure multiple display mode — General Availability
- Updated security baseline for Microsoft Edge v128 — General Availability
- Updated security baseline for Windows version 24H2 — General Availability
- Intune Suite
- Use Microsoft Security Copilot with Endpoint Privilege Manager to help identify potential elevation risks — General Availability
- Device Query for Multiple Devices — General Availability
- What's new in Microsoft Intune: January 2025 - Microsoft Intune Blog — Learn
- In development - Microsoft Intune | Microsoft Learn — Learn

Defender XDR

Defender Boxed

Limited time

- Defender Boxed is available for a limited time in **January** and **July** of each year.
- This series of slides highlights your organization's security successes, improvements, and response actions in the Microsoft Defender portal for the past six months/year.
- You can do the following actions:
  - Download a detailed summary
  - Change the frequency of how often Defender Boxed will appear. You can choose between once (every January) or twice (every January and July) per year.
  - Share your achievement to your social media networks, email, and other forums by saving the slide as an image.
-



References:

- [Prioritize incidents in the Microsoft Defender portal - Microsoft Defender XDR | Microsoft Learn]
- [What's new in Microsoft Defender XDR - Microsoft Defender XDR | Microsoft Learn]

Defender XDR Updates

- IP addresses can now be excluded from automated responses in attack disruption. This feature allows you to exclude specific IPs from automated containment actions triggered by attack disruption. — Public Preview
- You can now view how Security Copilot came up with the query suggestion in its responses in Microsoft Defender advanced hunting. Select See the logic behind the query below the query text to validate that the query aligns with your intent and needs, even if you don't have an expert-level understanding of KQL. — General Availability
- The Link to incident feature in Microsoft Defender advanced hunting now allows linking of Microsoft Sentinel query results. In both the Microsoft Defender unified experience and in Defender XDR advanced hunting, you can now specify whether an entity is an impacted asset or related evidence. — General Availability
- Device activity events from Microsoft Sentinel's device entity pages are now visible in the *Timeline* tab on the Device entity page in the Defender portal, in addition to remaining visible on the *Sentinel events* tab.
  The device activity events now include blocked, dropped or denied network traffic originating from a given device. — Public Preview
-

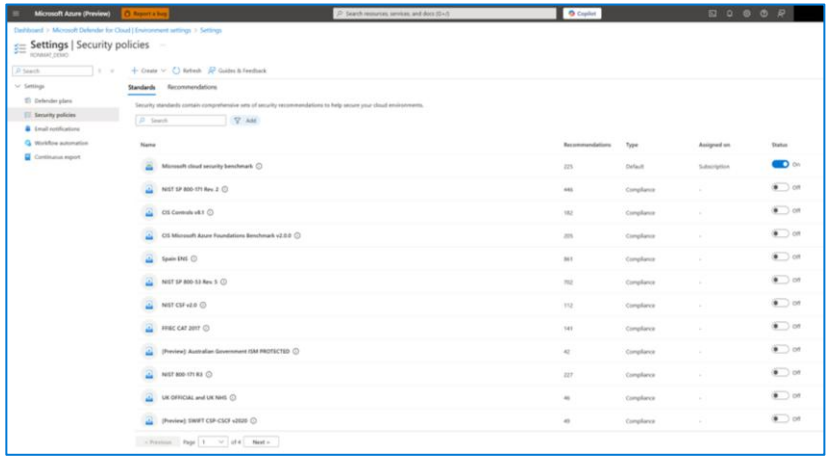
Defender for Cloud

New multicloud regulatory compliance standards in Defender for Cloud

Public Preview

- More than 30 new and enhanced regulatory compliance standards available with expanded support across Azure, AWS and GCP. Including:
  - E.U. Network and Information Security Directive 2 (NIS2)
  - CIS GCP Foundations v3.0
  - U.S. Criminal Justice Information Services (CJIS) Security Policy, Version 5.9.5
  - U.S. Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT)
  - U.K. National Cyber Security Centre (NCSC) Cyber Essentials v3.1
  - U.K. National Cyber Security Centre (NCSC) Cyber Assurance Framework (CAF) v3.2

- Enhancements to existing regulatory compliance standards expanded to Azure, AWS and GCP:
  - SWIFT Customer Security Controls Framework (2024)
  - E.U. General Data Protection Regulation (GDPR)
  - ISO IEC 27002:2022
  - NIST CSF v2.0
  - PCI DSS v4.0.1
  - NIST SP 800 53 R5.1.1



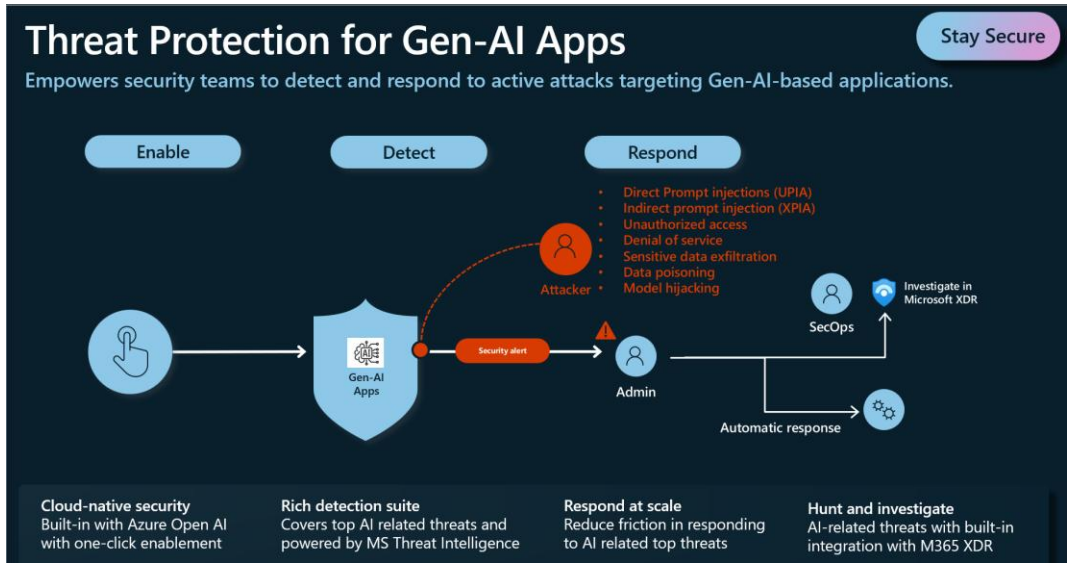
References:

- [New and enhanced multicloud regulatory compliance standards in Defender for Cloud]

Protecting Azure AI Workloads using Threat Protection for AI in Defender for Cloud

Limited Preview

- Threat protection for AI workloads in Microsoft Defender for Cloud protects AI workloads on an Azure subscription by providing insights to threats that might affect your generative AI applications.
- Defender XDR Integration
- Sign Up for the limited public preview:
  - Registration form: Threat protection for AI workloads limited preview (Page 1 of 4)



References:

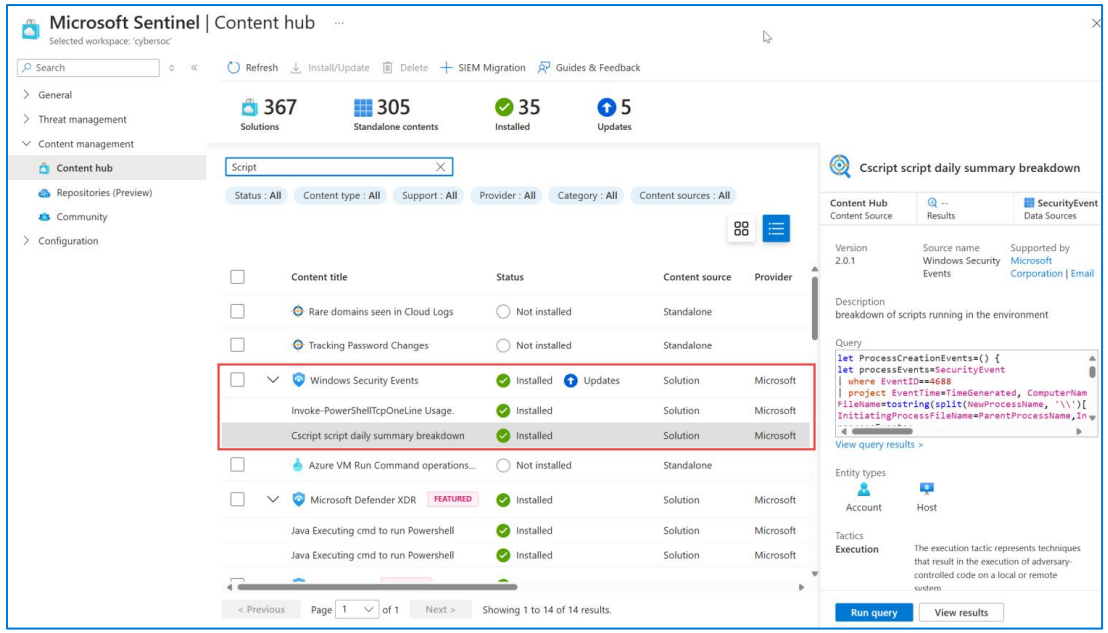
- Protecting Azure AI Workloads using Threat Protection for AI in Defender for Cloud | Microsoft Community Hub
- Overview - AI threat protection - Microsoft Defender for Cloud | Microsoft Learn
- Enable threat protection for AI workloads (preview) - Microsoft Defender for Cloud | Microsoft Learn
- Securing Multi-Cloud Gen AI workloads using Azure Native Solutions | Microsoft Community Hub

Sentinel

View granular solution content in the Microsoft Sentinel content hub and

General Availability

- View the individual content available in a specific solution directly from the Content hub
- This new visibility helps you understand the content available to you, and more easily identify, plan, and install the specific solutions you need.



References:

- What's new in Microsoft Sentinel | Microsoft Learn
- Discover and deploy Microsoft Sentinel out-of-the-box content from Content hub | Microsoft Learn

Sentinel Updates

- Find the Sentinel content you need using AI search | Microsoft Community Hub — Public Preview
- Introducing Threat Intelligence Ingestion Rules | Microsoft Community Hub — Public Preview
- Threat intelligence management interface has moved — General Availability
- Microsoft Defender Threat Intelligence data connectors now generally available (GA) — General Availability
- Improve SecOps collaboration with **case management** — Public Preview
  Manage cases natively in Microsoft's unified SecOps platform

Security Copilot

Security Copilot Updates

- Use Microsoft Security Copilot with Endpoint Privilege Manager to help identify potential elevation risks — Public Preview
- Integrating API data into Microsoft Security Copilot using custom logs and KQL plugins — Guidance
- Boost SOC automation with AI: Speed up incident triage with Security Copilot and Microsoft Sentinel | Microsoft Community Hub — Guidance

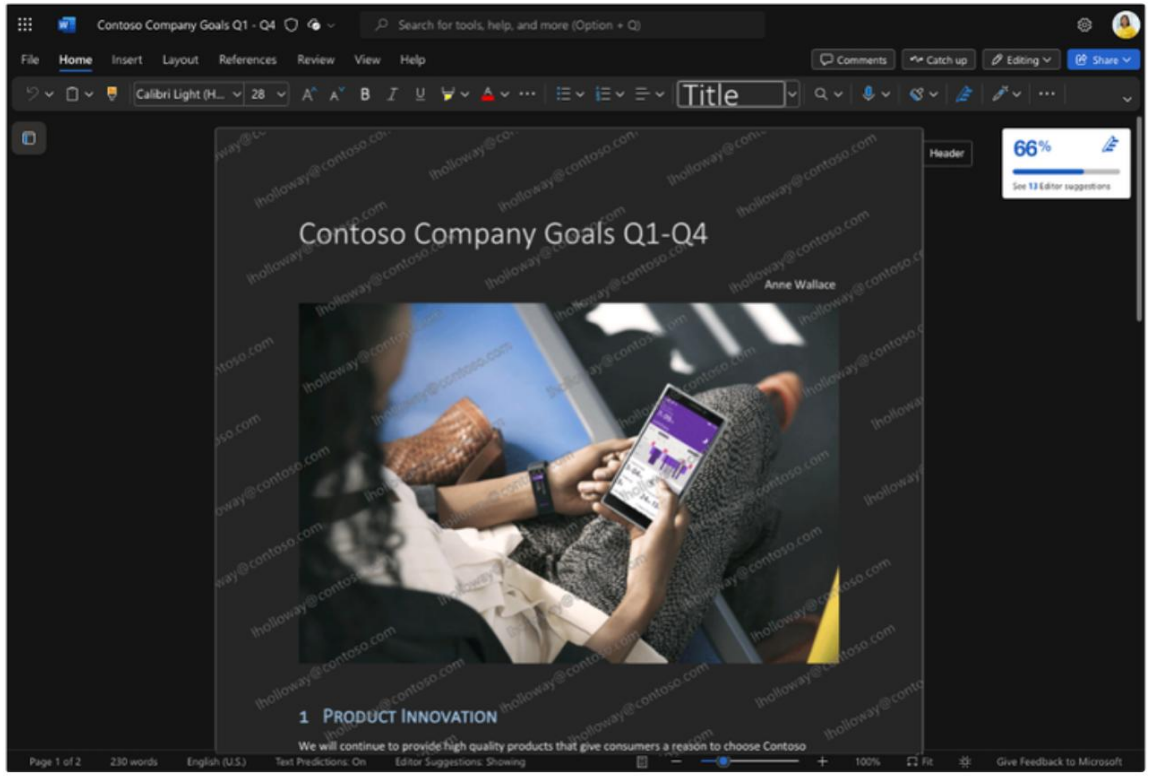
Purview

Dynamic Watermarks

General Availability

- Dynamic watermarking for sensitivity labels in Word, Excel, and PowerPoint

- Key Features:
  - User-Specific Watermarks
  - Watermark Customizability
  - Cross-Platform Support
  - Seamless Integration
  - Enhanced Security



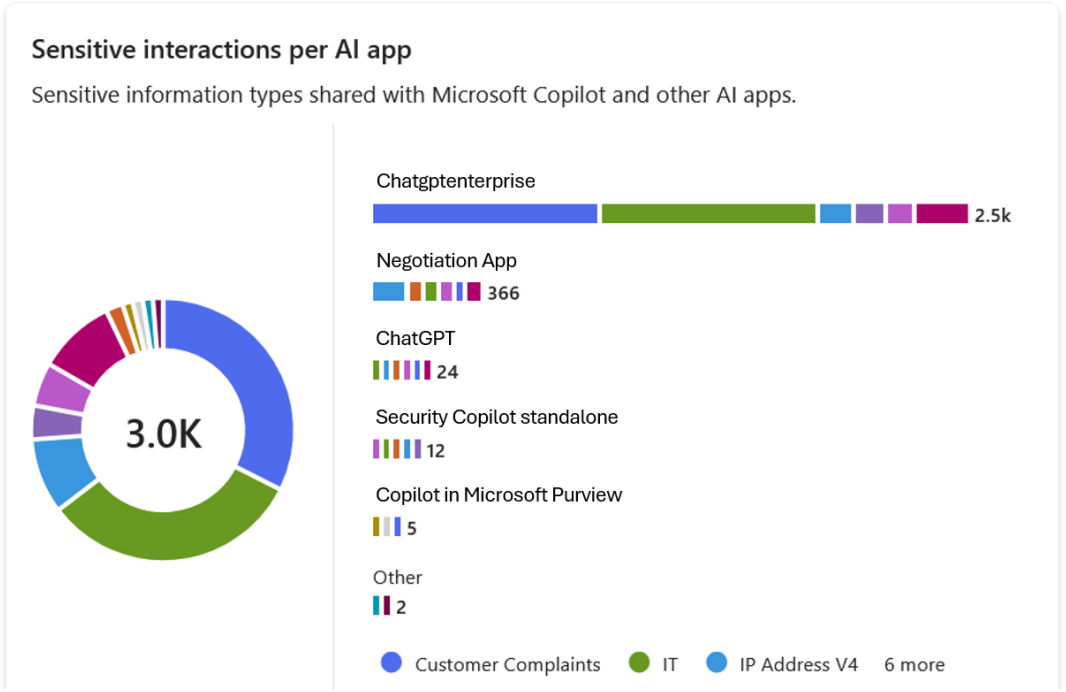
References:

- General Availability: Dynamic watermarking for sensitivity labels in Word, Excel, and PowerPoint | Microsoft Community Hub
- What's new in Microsoft Purview | Microsoft Learn
- Apply encryption using sensitivity labels | Microsoft Learn

Unlocking the Power of Microsoft Purview for ChatGPT Enterprise

Public Preview

- Benefits of Integrating ChatGPT Enterprise with Microsoft Purview:
  - Enhanced Data Security
  - Compliance and Governance
  - Customizable Detection
  - Seamless Integration



References:

- [Unlocking the Power of Microsoft Purview for ChatGPT Enterprise | Microsoft Community Hub]
- [Microsoft Purview data security and compliance protections for Microsoft 365 Copilot and other generative AI apps | Microsoft Learn]

Purview Updates

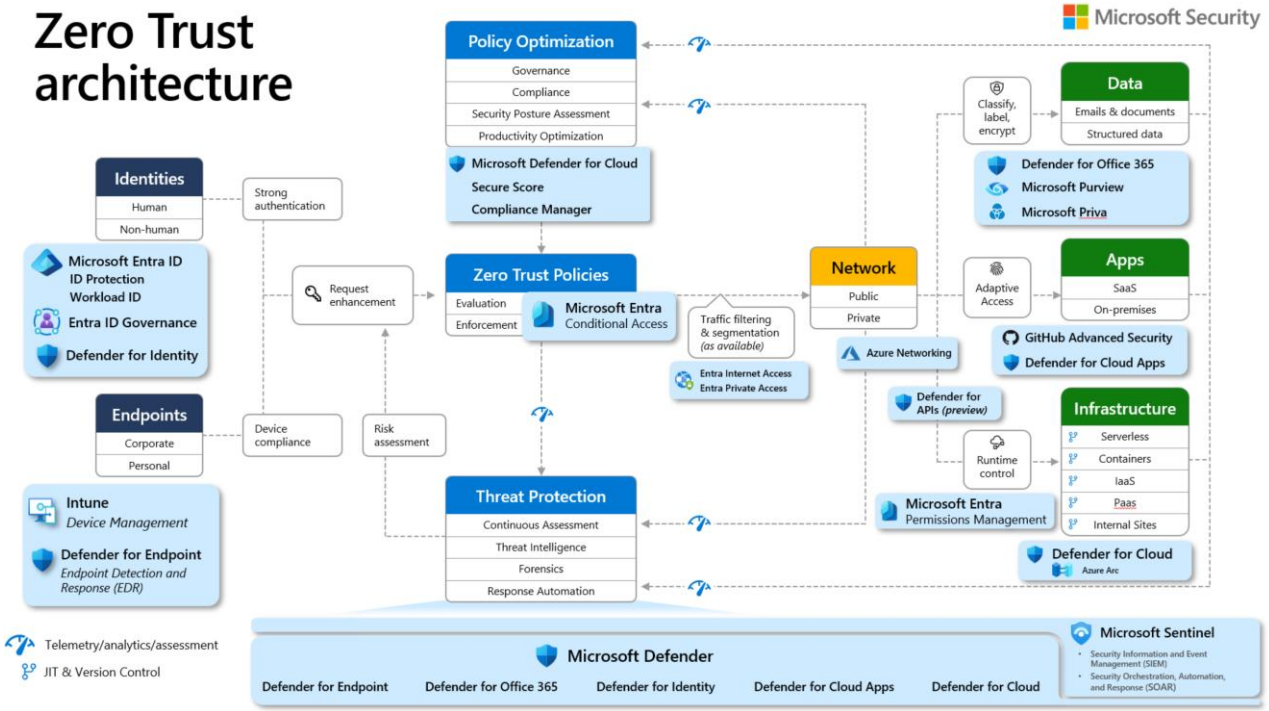
- Protect Teams meeting with Sensitivity label
  Use sensitivity labels to protect calendar items, Teams meetings, and chat — Public Preview
- Extending prevent copying chat to clipboard — General Availability
- Purview Webinars | Microsoft Community Hub — Learn

Zero Trust

Microsoft Security in Action: Zero Trust Deployment Essentials for Digital Security

Guidance

- Implementing Zero Trust requires a strategic approach.
- Learn how to get started with deploying Microsoft's Zero Trust pillars with step-by-step guidance on securing identity, data, applications, infrastructure, and networks.



References:

- Microsoft Security in Action: Zero Trust Deployment Essentials for Digital Security | Microsoft Community Hub
- Microsoft Zero Trust Assessment | Microsoft Zero Trust Workshop
- Zero Trust Guidance Center | Microsoft Learn

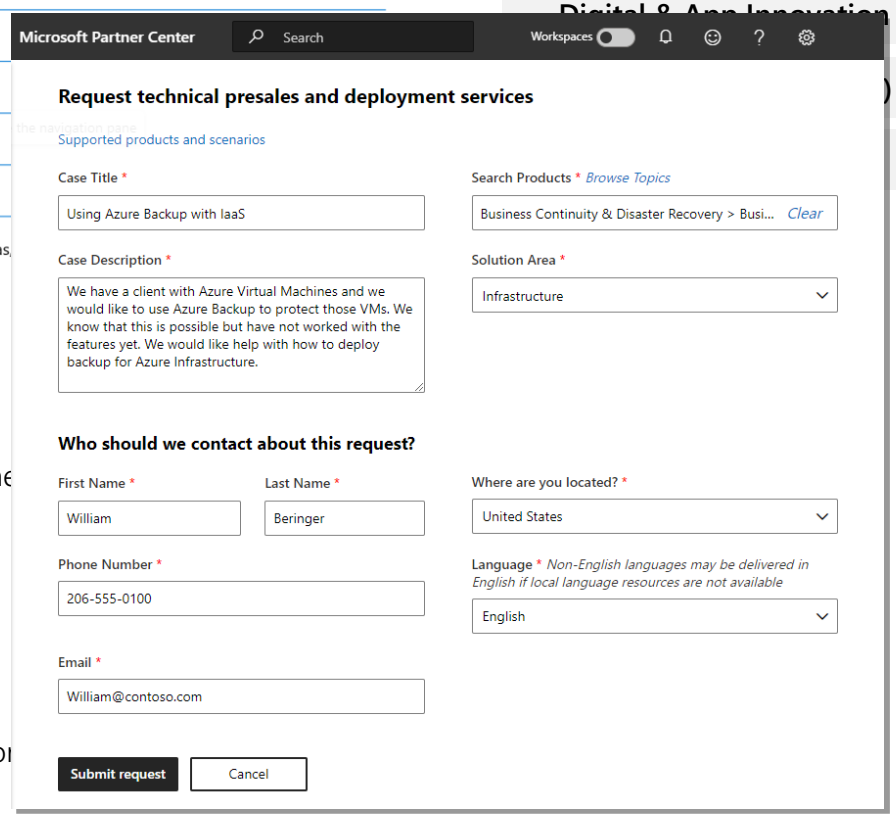
Leverage your MCAIPP benefits and engage TP&D Services

Technical presales and deployment services to help you deliver services and applications faster.

	Advisory hours	Technical sales preparation & deal enablement
Partner Launch Benefits	Not available	Not available
Partner Success Core Benefits	5	
Partner Success Expanded Benefits	10	
Solutions Partner	50	
Specialization / Expert*	50	

*Specialization and Expert MSP designation and TPD benefits shown are the same as Partner designation benefits.

Infrastructure (Azure)	Modern Work
Digital & App Innovation (Azure)	Security
	Business Applications
	ISV



Technical consultations scope:

- Delivered remotely
- Consultation service to help plan, build and grow partne technical capabilities
- Provides technical resources, recommendations and deliverables
- Focuses on common partner questions and technical scenarios
- Packaged as a Microsoft Cloud Partner Program adviso benefit

Examples

- Help analyze customer/partner architecture and how to respond with Microsoft capabilities
- Discuss product features, clarify doubts about technical capabilities
- Perform demos/PoCs of Microsoft products
- Provide best practices and recommendations
- Check usage scenarios:

Visit http://aka.ms/TPDMSForm and select 'Create a new TPD request' towards the top of the page, or log into your Partner Center dashboard and select the Benefits tile > Technical benefits.

Q&A

- Ask your questions
- Deep level and complex scenarios? Reach out to our team: https://aka.ms/TPDMSForm
- Reach out to us:
  - ritrigue@microsoft.com
  - abarreiros@microsoft.com
  - daniela.magalhaes@microsoft.com
  - macardo@microsoft.com

Microsoft Security

Thank you!