Microsoft Security

What’s New in Security, Compliance and Identity

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

Ricardo Trigueiro
ritrigue@microsoft.com

André Barreiros
abarreiros@microsoft.com

Agenda

Intros & What’s New Concept

News & Updates:

- General News and Highlights
- Intune
- Zero Trust
- Entra
- Sentinel
- Defender XDR
- Security Copilot
- Purview

Q&A

Intro and “What’s New” concept

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
  - Ricardo Trigueiro – ritrigue@microsoft.com
  - Daniela Magalhães - daniela.magalhaes@microsoft.com

General News and Highlights

Retirement of MSOnline And AzureAD Powershell Modules

- The **MSOnline** and **Azure AD PowerShell** modules were deprecated on March 30, 2024.
- The retirement for **MSOnline** PowerShell module starts in early **April 2025**. Customers must migrate any use of MSOnline PowerShell to Microsoft Graph PowerShell SDK or Microsoft Entra PowerShell to avoid impact after April 1, 2025.
- Support for **AzureAD** PowerShell ends on **March 30, 2025**, with its retirement starting after July 1, 2025. Organizations should prioritize migrating from MSOnline PowerShell. The shutdown of Azure AD PowerShell will begin after MSOnline PowerShell is retired.

References:

- Important update: Deprecation of Azure AD PowerShell and MSOnline PowerShell modules | Microsoft Community Hub
- Migrate from Azure AD PowerShell to Microsoft Graph PowerShell. | Microsoft Learn
- Azure AD PowerShell to Microsoft Graph PowerShell migration FAQ | Microsoft Learn
- Find Azure AD and MSOnline cmdlets in Microsoft Graph PowerShell | Microsoft Learn

Intune

Intune + Windows 365 update

Public Preview

- Intune support for Windows 365 Link is now available

References:
[Automatically enroll Windows 365 Link in Intune | Microsoft Learn]

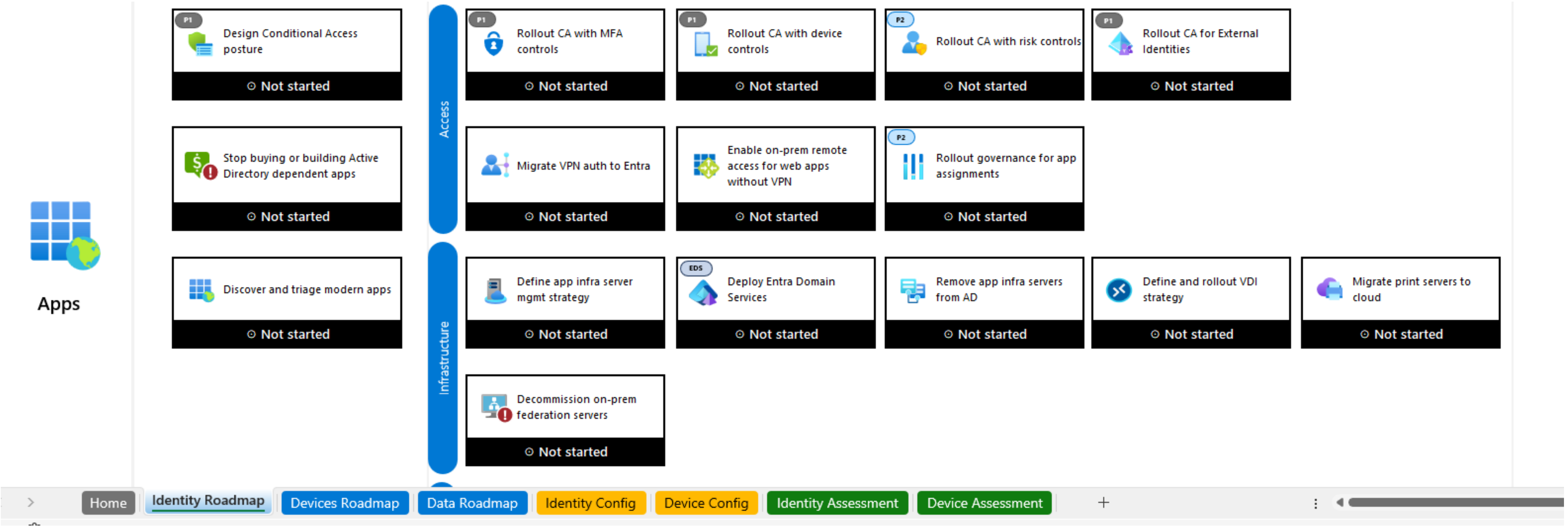
Intune updates

- Configure Intune to require multifactor authentication at device enrollment
- Store macOS certificates in user keychain
- Device Inventory for Windows
- Support for tamper protection in policies for Security settings management for Microsoft Defender for Endpoint (to be available on or around January 18th, 2025.)

Zero Trust

Microsoft Zero Trust Workshop

Guidance



Apps

Access

P1 Design Conditional Access posture — Not started

P1 Rollout CA with MFA controls — Not started

P1 Rollout CA with device controls — Not started

P2 Rollout CA with risk controls — Not started

P1 Rollout CA for External Identities — Not started

Stop buying or building Active Directory dependent apps — Not started

Migrate VPN auth to Entra — Not started

Enable on-prem remote access for web apps without VPN — Not started

P2 Rollout governance for app assignments — Not started

Infrastructure

Discover and triage modern apps — Not started

Define app infra server mgmt strategy — Not started

EDS Deploy Entra Domain Services — Not started

Remove app infra servers from AD — Not started

Define and rollout VDI strategy — Not started

Migrate print servers to cloud — Not started

Decommission on-prem federation servers — Not started

References:

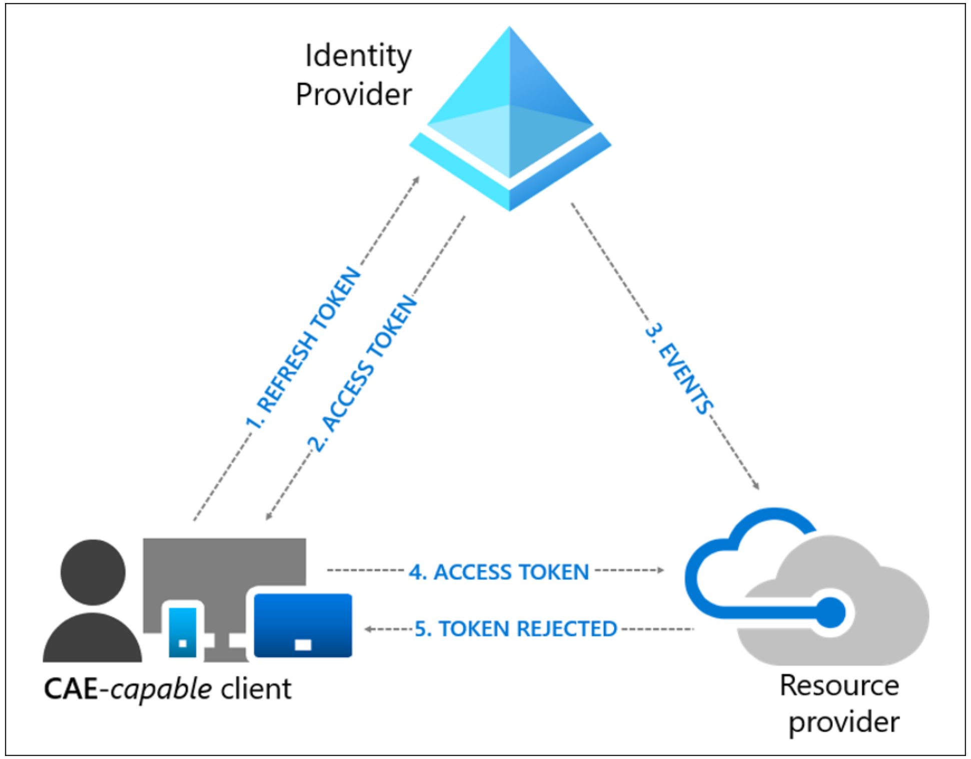
- [Microsoft Zero Trust Assessment | Microsoft Zero Trust Workshop]
- [Agile Business, agile security: How AI and Zero Trust work together | Microsoft Security Blog]
- [New Microsoft guidance for the CISA Zero Trust Maturity Model | Microsoft Security Blog]

Entra

Public Preview

Universal Continuous Access Evaluation

- Part of Global Secure Access
- Revokes and validates network access
- Give CAE capabilities to non-CAE apps through Global Secure Access.
- Protects against token theft and replay



References:

- Learn about Universal Continuous Evaluation (Preview) - Global Secure Access | Microsoft Learn
- Continuous access evaluation in Microsoft Entra - Microsoft Entra ID | Microsoft Learn
- What’s new in Microsoft’s Security Service Edge solution | Microsoft Community Hub

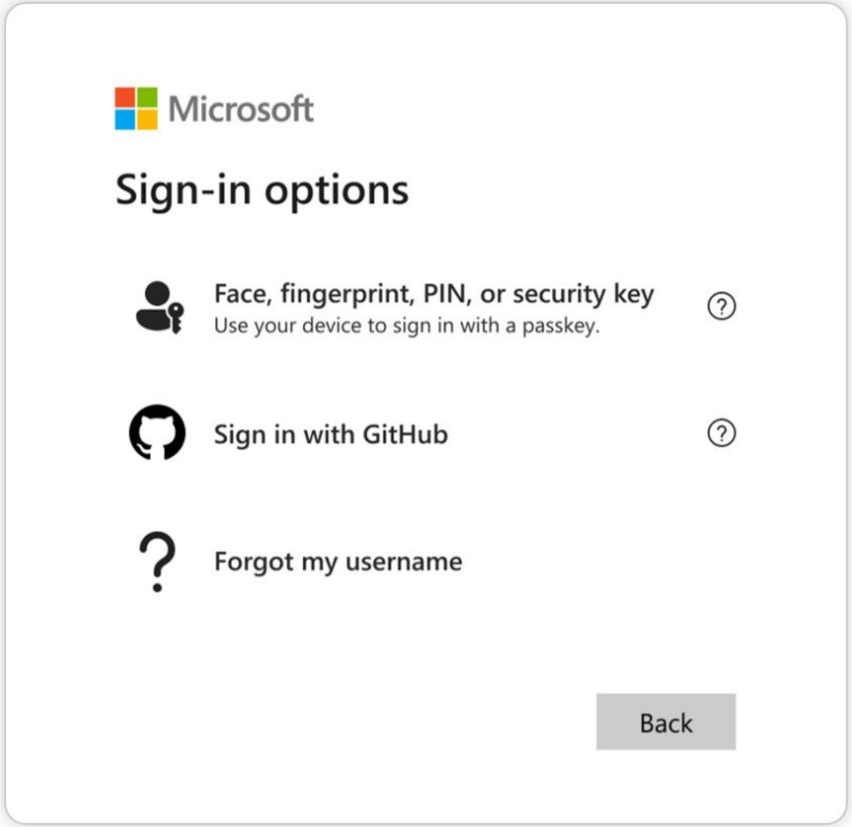
Guidance

Convincing a billion users to love passkeys

- 7000 password attacks per second blocked
- AitM attacks rising 146% year over year

- Passkeys can protect against these attacks

- Invite users to enroll passkeys



Microsoft

Sign-in options

Face, fingerprint, PIN, or security key
Use your device to sign in with a passkey.

Sign in with GitHub

Forgot my username

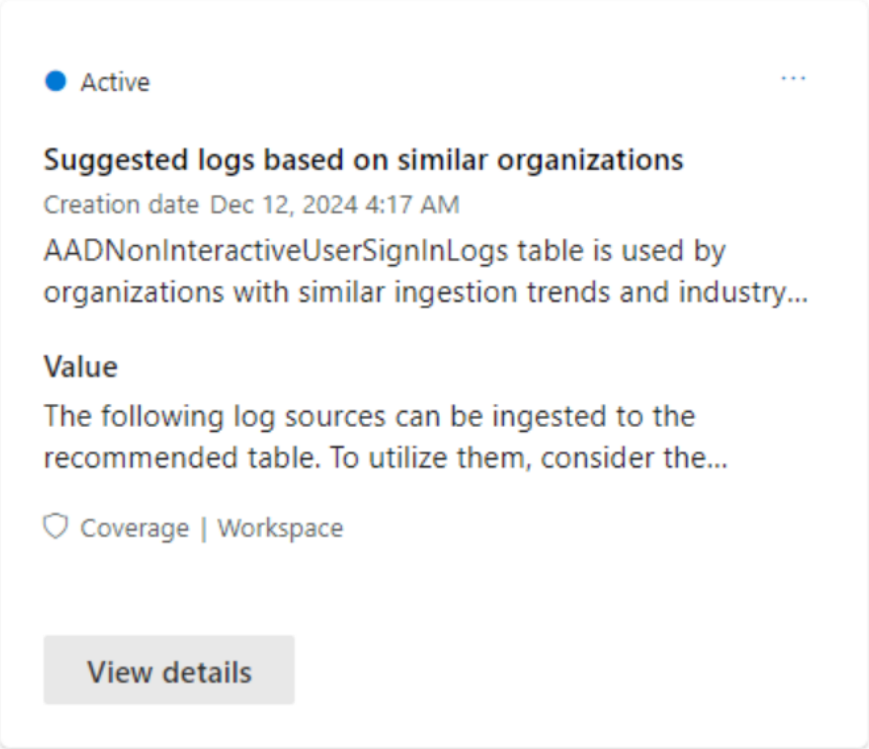
References:
- Convincing a billion users to love passkeys: UX design insights from Microsoft to boost adoption and security | Microsoft Security Blog
- Passwordless authentication | Microsoft Security
- What is a Passkey? Secure Signins | Microsoft Security

Sentinel

SOC Optimization Recommendations based on similar organizations

Public Preview

- Struggling to find which data sources should be onboarded on Sentinel?
- Recommendations based on similar organizations use advanced machine learning to suggest which data to ingest, based on organizations with similar ingestion patterns.
- Get actionable recommendations to help cover against specific threats



● Active

Suggested logs based on similar organizations

Creation date Dec 12, 2024 4:17 AM

AADNonInteractiveUserSignInLogs table is used by organizations with similar ingestion trends and industry...

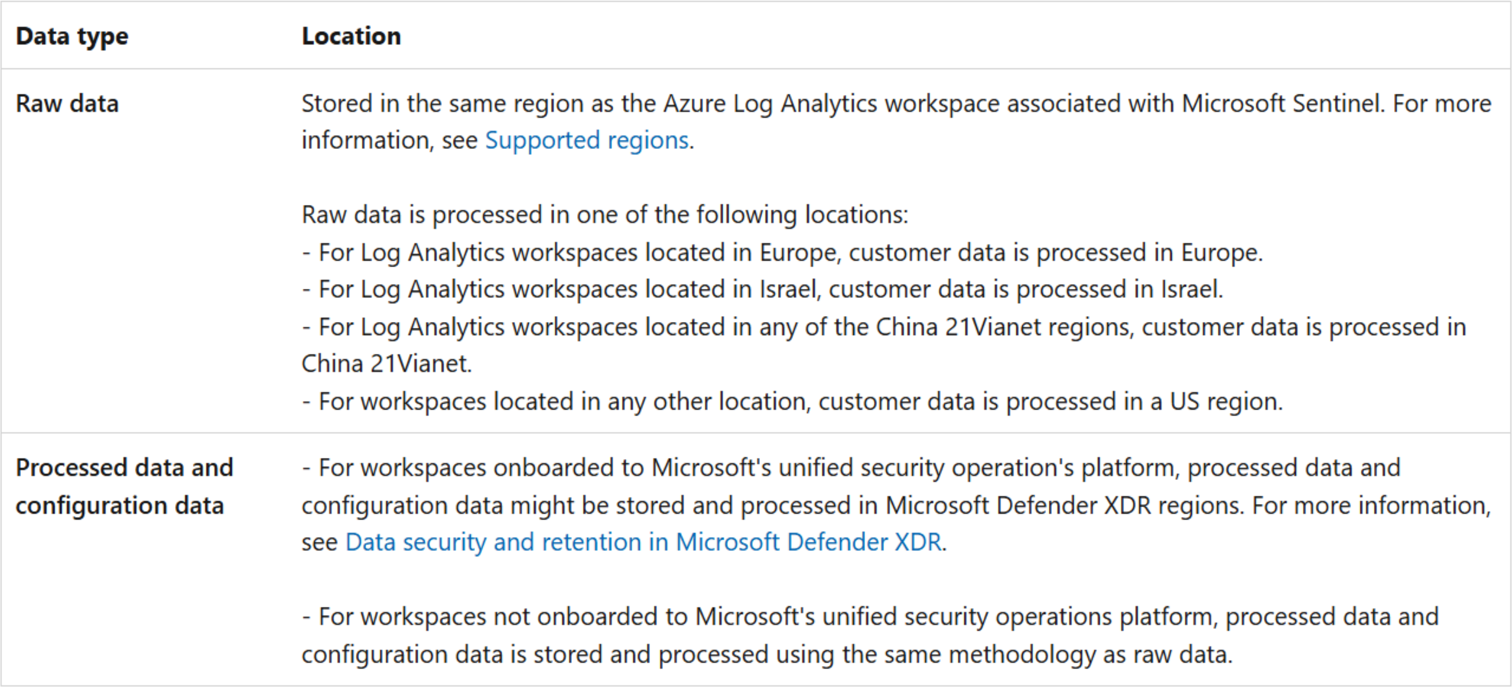
Value

The following log sources can be ingested to the recommended table. To utilize them, consider the...

References:
- [Introducing SOC Optimization Recommendations Based on Similar Organizations | Microsoft Community Hub]
- [Optimize security operations | Microsoft Learn]
- [Optimizing your SOC's threat coverage and data value | Virtual Ninja Training]

General Availability

Geographical availability and data residency in Sentinel and Microsoft Defender XDR



Data type	Location
Raw data	Stored in the same region as the Azure Log Analytics workspace associated with Microsoft Sentinel. For more information, see Supported regions. Raw data is processed in one of the following locations: - For Log Analytics workspaces located in Europe, customer data is processed in Europe. - For Log Analytics workspaces located in Israel, customer data is processed in Israel. - For Log Analytics workspaces located in any of the China 21Vianet regions, customer data is processed in China 21Vianet. - For workspaces located in any other location, customer data is processed in a US region.
Processed data and configuration data	- For workspaces onboarded to Microsoft's unified security operation's platform, processed data and configuration data might be stored and processed in Microsoft Defender XDR regions. For more information, see Data security and retention in Microsoft Defender XDR. - For workspaces not onboarded to Microsoft's unified security operations platform, processed data and configuration data is stored and processed using the same methodology as raw data.

References:

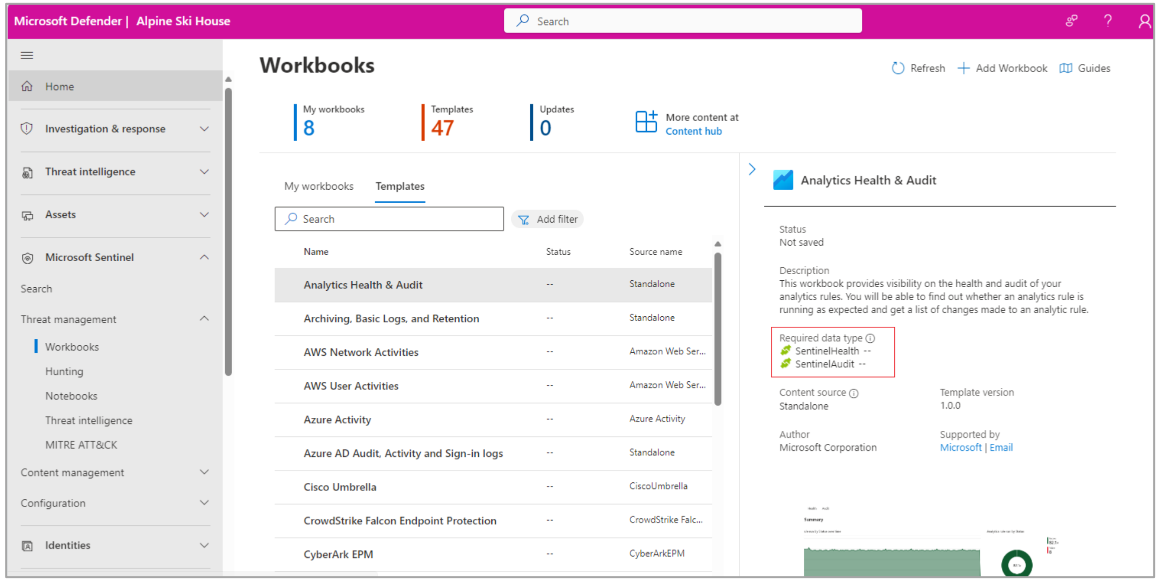
- Geographical availability and data residency in Microsoft Sentinel \| Microsoft Learn
- Data retention and data security in Microsoft Defender XDR - Microsoft Defender XDR \| Microsoft Learn

Defender XDR

General Availability

Sentinel Workbooks now available to view directly in the Microsoft Defender Portal

- Microsoft Sentinel workbooks are now available for viewing directly in the Defender portal with Microsoft's unified security operations (SecOps) platform.
- Workbook edition is done in Azure Portal.



Workbooks

My workbooks 8 | Templates 47 | Updates 0

Name	Status	Source name
Analytics Health & Audit	--	Standalone
Archiving, Basic Logs, and Retention	--	Standalone
AWS Network Activities	--	Amazon Web Ser...
AWS User Activities	--	Amazon Web Ser...
Azure Activity	--	Azure Activity
Azure AD Audit, Activity and Sign-in logs	--	Standalone
Cisco Umbrella	--	CiscoUmbrella
CrowdStrike Falcon Endpoint Protection	--	CrowdStrike Falc...
CyberArk EPM	--	CyberArkEPM

Analytics Health & Audit

Status
Not saved

Description
This workbook provides visibility on the health and audit of your analytics rules. You will be able to find out whether an analytics rule is running as expected and get a list of changes made to an analytic rule.

Required data type
SentinelHealth --
SentinelAudit --

Content source
Standalone

Template version
1.0.0

Author
Microsoft Corporation

Supported by
Microsoft | Email

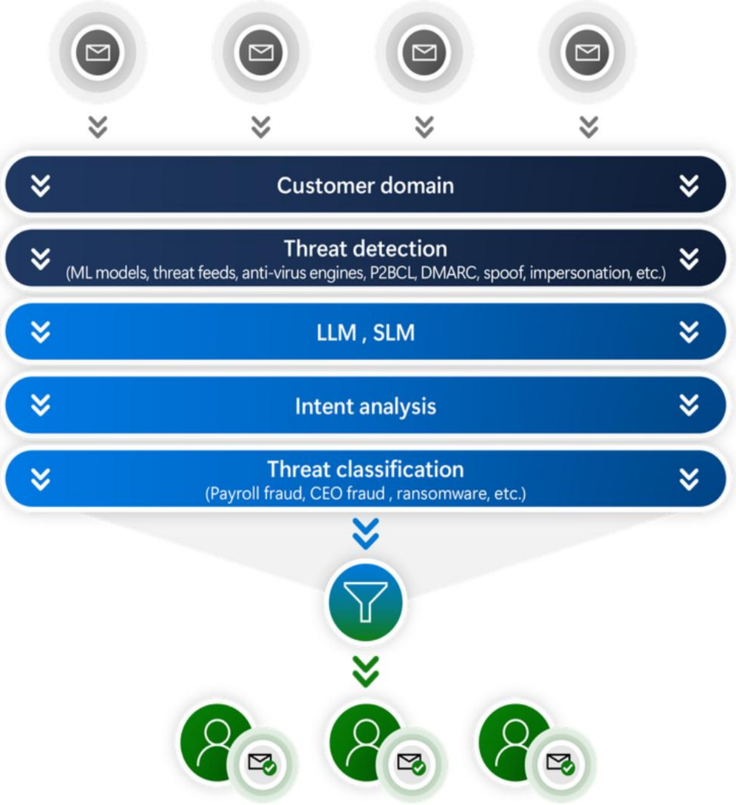
References:

- [What's new in Microsoft Sentinel | Microsoft Learn]
- [Visualize your data using workbooks in Microsoft Sentinel | Microsoft Learn]

Public Preview

Redefining email security with LLMs to tackle a new era of social engineering

- Phishing emails have evolved from poorly written messages to sophisticated, AI-generated content that appears more legitimate and tailored to each recipient. Adversaries are now using generative AI to craft these emails, making them harder to detect and more effective in building trust relationships with targets.
- Increasing sophistication of BEC campaigns, where attackers use AI to engage in long-term conversations with targets to extract money or gather personal information.
- Microsoft Defender for Office 365 now uses Large Language Models (LLMs) to provide AI-powered email and collaboration security, parsing language to understand and identify attacker intentions.
- The initial rollout of LLM-based detection has shown significant success, with a **99.995%** accuracy in detecting attacker intent and blocking **140,000** BEC emails daily!
- The new LLM-native protection strengthens defenses by detecting, classifying, and mitigating threats in real-time, providing security operations teams with better insights into attacker techniques.


Customer domain
Threat detection
(ML models, threat feeds, anti-virus engines, P2BCL, DMARC, spoof, impersonation, etc.)
LLM , SLM
Intent analysis
Threat classification
(Payroll fraud, CEO fraud , ransomware, etc.)

References:

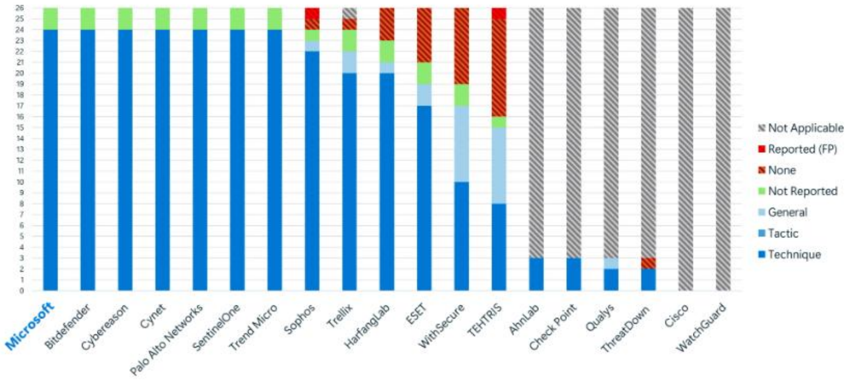
- Microsoft Ignite: Redefining email security with LLMs to tackle a new era of social engineering | Microsoft Community Hub

Report

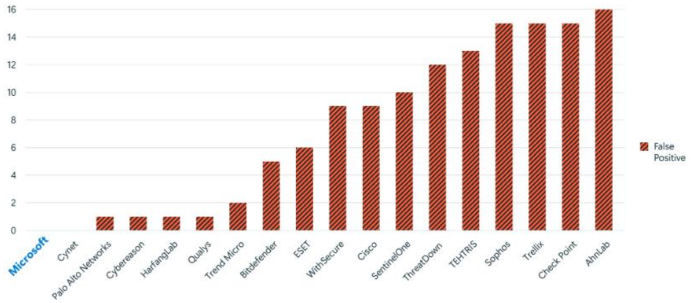
Defender XDR demonstrates 100% detection coverage across all cyberattack stages in the 2024 MITRE ATT&CK® Evaluations: Enterprise

- Microsoft Defender XDR achieved **100% technique-level detections** across all attack stages for both Linux and macOS threats.
- **Zero False Positives**, ensuring that only malicious activities were alerted and blocked, allowing the SOC to focus on real cyberthreats.
- **Cross-Platform Capabilities:** Key capabilities include remote encryption detection and macOS behavioral monitoring, providing deep visibility into attacker activities.
- **Microsoft Security Copilot**, the industry's **first generative AI for security**, enhances threat detection and response with features like script analysis.
- **Defender XDR** is a natively integrated platform spanning endpoints, hybrid identities, email, collaboration tools, SaaS apps, and data, offering centralized visibility and powerful analytics

ER6 Linux and MacOS detection comparison



ER6 False positive comparison

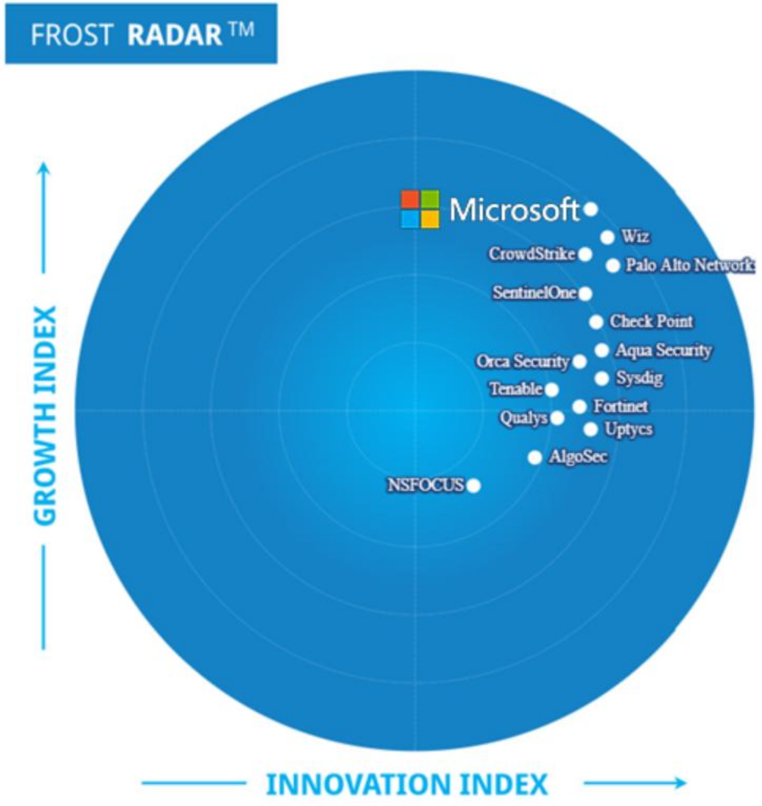


References:

- [Microsoft Defender XDR demonstrates 100% detection coverage across all cyberattack stages in the 2024 MITRE ATT&CK® Evaluations: Enterprise | Microsoft Security Blog]

Microsoft Defender for Cloud Named a Leader in Frost Radar™ for CNAPP for the Second Year in a Row!

- “With significant investments in cloud security, a strong partner network, and strategic positioning as a multicloud security provider, Microsoft has a solid foundation for sustained growth in the next few years to maintain its lead in the cloud security industry as competition increases.“
- Unified Security Platform
- Seamless Integration
- Data-Aware Security
- Multicloud Support



References:

- [Microsoft Defender for Cloud Named a Leader in Frost Radar™ for CNAPP for the Second Year in a Row! | Microsoft Community Hub]

Security Copilot

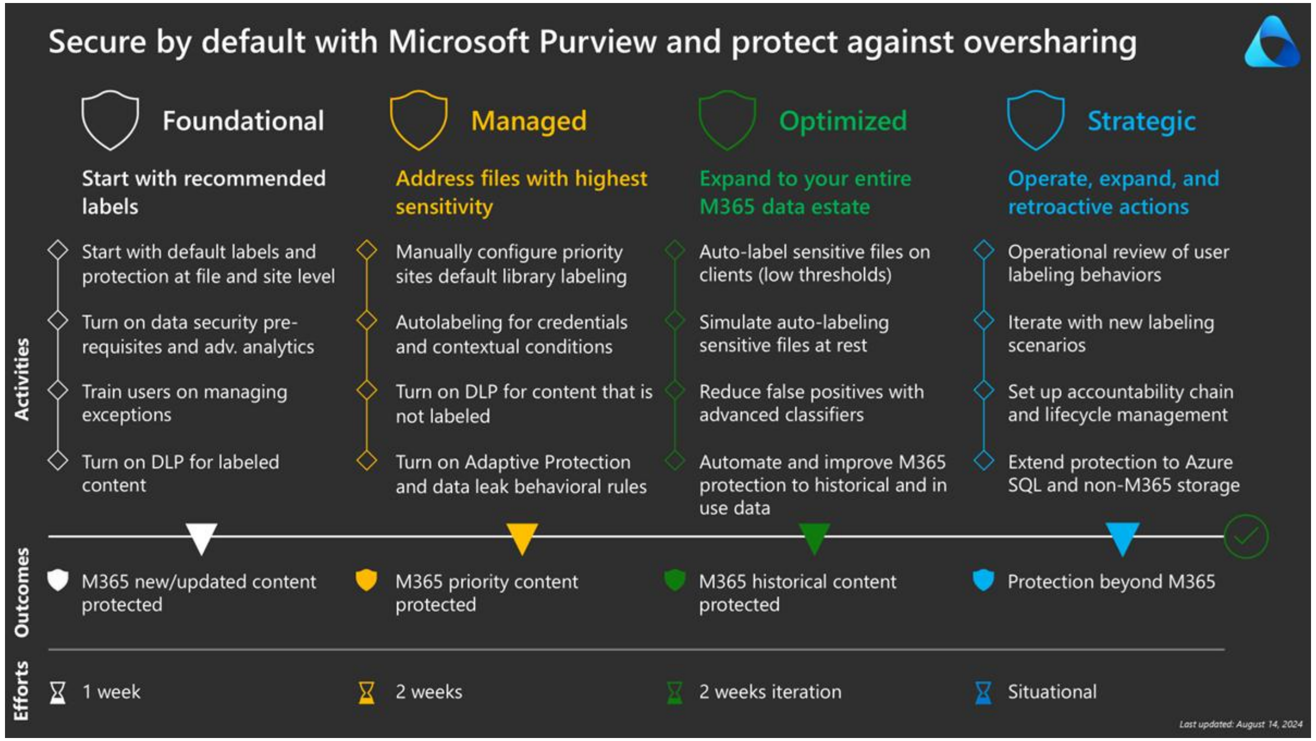
Security Copilot Updates

- KQL Migrator powered by Microsoft Security Copilot | Microsoft Community Hub General Availability
- Investigate app risk in Microsoft Security Copilot - Microsoft Entra | Microsoft Learn Public Preview
- The Projected Total Economic Impact Of Microsoft Security Copilot Report
- Microsoft Security Copilot – Microsoft Adoption General Availability

Purview

Guidance

Secure by default with Microsoft Purview and protect against oversharing



Secure by default with Microsoft Purview and protect against oversharing

	Foundational	Managed	Optimized	Strategic
	Start with recommended labels	Address files with highest sensitivity	Expand to your entire M365 data estate	Operate, expand, and retroactive actions
Activities	Start with default labels and protection at file and site level	Manually configure priority sites default library labeling	Auto-label sensitive files on clients (low thresholds)	Operational review of user labeling behaviors
	Turn on data security pre-requisites and adv. analytics	Autolabeling for credentials and contextual conditions	Simulate auto-labeling sensitive files at rest	Iterate with new labeling scenarios
	Train users on managing exceptions	Turn on DLP for content that is not labeled	Reduce false positives with advanced classifiers	Set up accountability chain and lifecycle management
	Turn on DLP for labeled content	Turn on Adaptive Protection and data leak behavioral rules	Automate and improve M365 protection to historical and in use data	Extend protection to Azure SQL and non-M365 storage
Outcomes	M365 new/updated content protected	M365 priority content protected	M365 historical content protected	Protection beyond M365
Efforts	1 week	2 weeks	2 weeks iteration	Situational

Last updated: August 14, 2024

References:

- Secure by default with Microsoft Purview and protect against oversharing | Microsoft Learn
- Microsoft 365 Copilot blueprint for oversharing | Microsoft Learn
- The Microsoft Azure Security Podcast

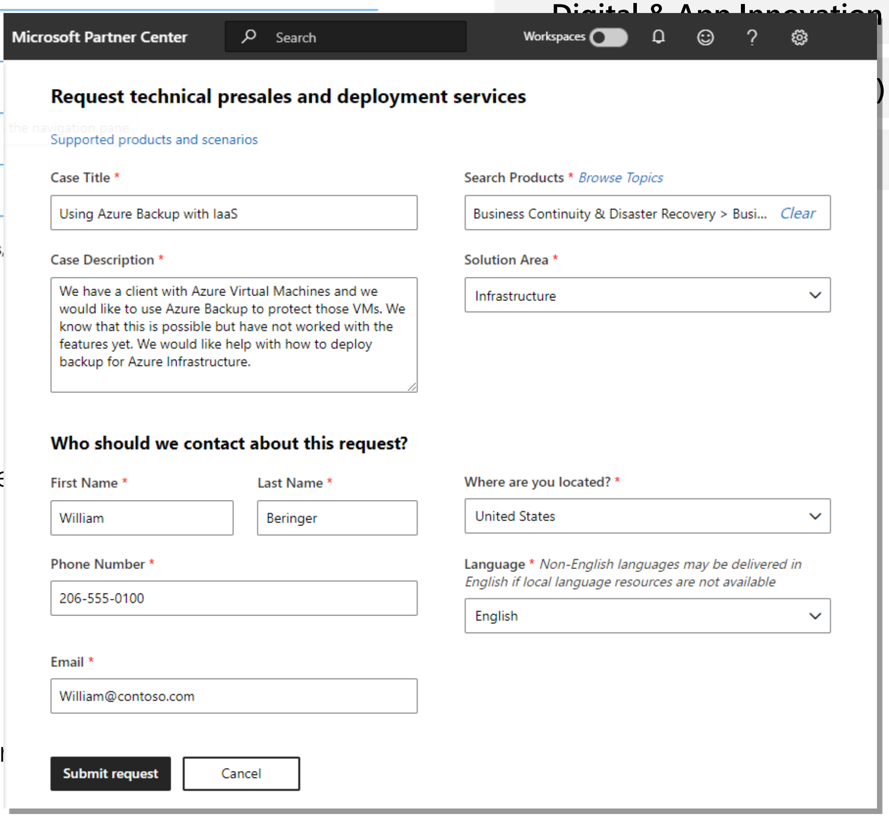
Leverage your MCAIPP benefits and engage TP&D Services

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


Microsoft Partner Center

Request technical presales and deployment services

Supported products and scenarios

Case Title *
Using Azure Backup with IaaS

Search Products * *Browse Topics*
Business Continuity & Disaster Recovery > Busi... *Clear*

Case Description *
We have a client with Azure Virtual Machines and we would like to use Azure Backup to protect those VMs. We know that this is possible but have not worked with the features yet. We would like help with how to deploy backup for Azure Infrastructure.

Solution Area *
Infrastructure

Who should we contact about this request?

First Name *
William

Last Name *
Beringer

Where are you located? *
United States

Phone Number *
206-555-0100

Language * *Non-English languages may be delivered in English if local language resources are not available*
English

Email *
William@contoso.com

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 advisor 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

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

Microsoft Security

Thank you!