



# What's New and Highlights in Security, Compliance and Identity

**Technical Presales & Deployment**

**<https://aka.ms/TPD>**

**Andre Barreiros**

**[abarreiros@microsoft.com](mailto:abarreiros@microsoft.com)**

**Daniela Magalhaes**

**[Daniela.Magalhaes@microsoft.com](mailto:Daniela.Magalhaes@microsoft.com)**

**Marco Carvalho Cardoso**

**[macardo@microsoft.com](mailto:macardo@microsoft.com)**

**November'25**

---

# Agenda

- 
- Intro
  - News & Updates:
    - Events, Learning & Training
    - Intune
    - Entra ID
    - Purview
    - Sentinel
    - Security Copilot
    - Defender
  - TP&D
  - Q&A

Intro

The background features a solid blue field. A large, smooth, orange wave-like shape curves from the bottom left towards the center. To its right, a darker blue, teardrop-shaped area is outlined by a thin pink line. In the bottom right corner, there are overlapping gradients of light blue and purple.

# What's New and Highlights in Security, Compliance and Identity

- Monthly News and Updates for all things related with Security, Compliance and Identity.
- Monthly, every third Thursday at 9:30am GMT
- Technical Presales & Deployment Team:
  - Andre Barreiros [abarreiros@microsoft.com](mailto:abarreiros@microsoft.com)
  - Daniela Magalhaes [Daniela.Magalhaes@microsoft.com](mailto:Daniela.Magalhaes@microsoft.com)
  - Marco Cardoso [Marco.Cardoso@microsoft.com](mailto:Marco.Cardoso@microsoft.com)

# What's New series

**18 December** — 09:30–10:30 GMT

<https://www.cloudchampion.co.uk/c/whats-new-in-security-compliance-and-identity-december>

**22 January** — 09:30–10:30 GMT

<https://www.cloudchampion.co.uk/c/whats-new-in-security-compliance-and-identity-january-2>

**19 February** — 09:30–10:30 GMT

<https://www.cloudchampion.co.uk/c/whats-new-in-security-compliance-and-identity-february-2>

**19 March** — 09:30–10:30 GMT

<https://www.cloudchampion.co.uk/c/whats-new-in-security-compliance-and-identity-march-2>

**16 April** — 09:30–10:30 GMT+1

<https://www.cloudchampion.co.uk/c/whats-new-in-security-compliance-and-identity-april-3>

**21 May** — 09:30–10:30 GMT+1

<https://www.cloudchampion.co.uk/c/whats-new-in-security-compliance-and-identity-may>

**Intune**

# Intune

## 1. Scope Tag Enforcement for Endpoint Privilege Management Elevation Requests

Scope tags now apply to elevation requests.

Admins can only view/manage requests within their assigned scope.

Strengthens security by maintaining proper administrative boundaries.

## 2. Windows Autopilot – Secure-by-Default Provisioning

Enrollment Status Page (ESP) installation of Windows security updates during OOBЕ now scheduled for **Jan 2026**.

Setting visible but not yet active; extra time ensures reliability.

Admins fully control update timing via ESP for both Intune and Autopilot devices.

Supports Microsoft's "Security starts with you" focus by reducing vulnerability during first sign-in.

## 3. PowerShell Script Installer for Win32 Apps

Win32 apps can now use a PowerShell script as the installer.

Enables richer workflows (prerequisites, config changes, post-install actions).

Intune tracks installation results based on script return code.



Unbox. Log in. Take off.



# Intune

Public Preview

## Soft-deleted Microsoft Entra groups now visible in Intune

This feature is in public preview.

Microsoft Intune now displays soft-deleted Microsoft Entra groups in the Intune admin center. When a group is soft-deleted, its assignments no longer apply. However, if the group is restored, its previous assignments are automatically reinstated.

For more information, see [Include and exclude app assignments in Microsoft Intune](#).

For more information, see [Public preview in Microsoft Intune](#).

## Windows 10 support in Intune

On October 14, 2025, [Windows 10 reached end of support](#) and won't receive quality and feature updates. Windows 10 is an **allowed** version in Intune. Devices running this version can still enroll in Intune and use eligible features, but functionality won't be guaranteed and can vary.

For more information, see [Support statement for Windows 10 in Intune](#).





**Entra ID**

# Entra ID

Public Preview

## Public Preview - Soft Delete & Restore for Conditional Access Policies and Named Locations

**Type:** New feature

**Service category:** Conditional Access

**Product capability:** Identity Security & Protection

We're thrilled to announce the **Public Preview of soft delete and restore for Conditional Access (CA) policies and Named Locations** in Microsoft Entra. This new capability extends our proven soft delete model to critical security configurations across **Microsoft Graph APIs (in beta) and the Microsoft Entra Admin Center**, helping admins recover from accidental or malicious deletions quickly and strengthen overall security posture.

With this feature, admins can:

- Restore deleted items to their exact prior state within 30 days
- Review deleted items before restoring
- Permanently delete when needed

Soft delete has already been proven at scale across Microsoft Entra (7M+ objects restored in the last 30 days). Bringing it to CA policies and Named Locations ensure quick disaster recovery, minimizes downtime, and maintains security integrity.

# Entra ID

Public Preview

## Public Preview - Conditional Access Optimization Agent in Microsoft Entra

**Type:** New feature

**Service category:** Conditional Access

**Product capability:** Identity Security & Protection

Conditional Access Optimization Agent in Microsoft Entra monitors for new users or apps not covered by existing policies, identifies necessary updates to close security gaps, and recommends quick fixes for identity teams to apply with a single selection. For more information, see: [Microsoft Entra Conditional Access optimization agent](#).

## Public Preview - Convert Source of Authority of synced Active Directory users to the cloud

**Type:** New feature

**Service category:** User Management

**Product capability:** Microsoft Entra Connect and Microsoft Entra Cloud Sync

The Source of Authority (SOA) at the object level allows administrators to convert specific users synced from Active Directory (AD) to Microsoft Entra ID into cloud-editable objects, which are no longer synced from AD and act as if originally created in the cloud. This feature supports a gradual migration process, decreasing dependencies on AD while aiming to minimize user and operational impact. Both Microsoft Entra Connect Sync and Cloud Sync recognize the SOA switch for these objects. The option to switch the SOA of synced users from AD to Microsoft Entra ID is currently available in Public Preview. For more information, see: [Embrace cloud-first posture: Transfer user Source of Authority \(SOA\) to the cloud \(Preview\)](#).

# Entra ID

## Microsoft Entra Sessions at Ignite:

- Microsoft Entra: What's New in Secure Access on the AI Frontier
- Secure access for AI agents with Microsoft Entra
- Microsoft Entra Suite: Accelerate Zero Trust and Secure AI Access (TODAY)
- Identity Under Siege: Modern ITDR from Microsoft
- Top Essentials for an Integrated, AI-Ready Security Foundation (TODAY)
- Move OFF Passwords: Passkeys in Microsoft Entra ID (TODAY)
- Modernize Identity Governance for SAP with Microsoft Entra (TODAY)
- Strengthen your identity security posture with Conditional Access
- Govern identities with confidence using Microsoft Entra

Purview

The image features a solid yellow background. A thick, curved line with a color gradient from purple to orange starts at the bottom left and extends towards the top right. In the bottom right corner, there is a large, rounded, teardrop-like shape with a color gradient from blue to purple.

# Purview

## General Availability

### Global Availability - Sensitivity labels support extended to 11 data sources

**Type:** New feature

**Service category:** Data governance

**Product capability:** Unified Catalog

Sensitivity labels can now be applied to 11 more [Data Map data sources](#): Azure Cosmos DB for SQL API, Azure Data Explorer, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Databricks Unity Catalog, Azure SQL Managed Instance, Azure Synapse Analytics (Workspace), Snowflake, SQL Server, Amazon S3, Microsoft Dataverse.

For more information: [Data sources that connect to Microsoft Purview Data Map](#) | [Microsoft Learn](#)

## Public Preview

### Public Preview - Create workflows to automate processes in Unified Catalog

**Type:** New feature

**Service category:** Data Governance

**Product capability:** Unified Catalog

Workflows in Microsoft Purview Unified Catalog provide a centralized, automated way to manage approval scenarios, such as granting access to data products and publishing data products and glossary terms.

Workflows are automated, repeatable sets of actions or business processes that users can establish to streamline operations in their organization. The available workflows can automate the approval processes for requesting access to, and publishing, data products. Governance teams can use the workflows to automate their desired approval processes. You can set customizable workflows for these processes:

- [Granting access to data products](#)
- [Publishing data products and glossary terms](#)

You can also use the [Unified Catalog API](#) to allow you to programmatically integrate and manage the Microsoft Purview Unified Catalog into your custom apps to automate operations, integrate custom workflows, and so on.

For more information: [Workflows in Unified Catalog \(preview\)](#) | [Microsoft Learn](#)

# Purview

Public Preview

## Public Preview - Block sensitive information to be shared with AI

**Type:** New feature

**Service category:** Data Loss Prevention

**Product capability:** Data Loss Prevention in AI

Data Loss Prevention now provides various abilities to block sensitive information to be found by AI.

- [Block specific sensitive information types from being used in prompts](#) to Microsoft 365 Copilot and Copilot Chat. When a user attempts to use sensitive information types that are blocked by the DLP policy, they will receive a notification informing them that the prompt cannot be completed. It's available in Microsoft 365 Copilot, Copilot Chat and Copilot in Word, Excel, PowerPoint.
- [Block files and emails with sensitivity labels from being used in response summaries](#) is released to general availability.
- [Get started with data loss prevention protections for Recall](#) helps protect against sensitive content being included in Recall snapshots on Copilot+ PCs.
- [Use Network Data Security to help prevent sharing sensitive information with unmanaged AI](#). You can enforce DLP protections on network traffic for Microsoft Entra GSA Internet Access to help prevent users from sharing sensitive information with unmanaged AI apps (files only).

For more information: [Learn about using Microsoft Purview Data Loss Prevention to protect interactions with Microsoft 365 Copilot and Copilot Chat | Microsoft Learn](#)



**Sentinel**



# Sentinel

## Call to Action - update queries and automation by July 1, 2026 - standardized account entity naming in incidents and alerts

**Type:** Call to Action

**Service category:** Security Information and Event Management (SIEM)

**Product capability:** Microsoft Sentinel

Microsoft Sentinel is updating how it identifies account entities in incidents and alerts. This change introduces a standardized naming logic to improve consistency and reliability across your analytics and automation workflows. Updated entity naming to prioritize **UPN prefix** for consistency across detections and queries.

Update your KQL queries and automation logic to follow the new precedence-aware pattern. Use the [coalesce\(\)\(/kusto/query/coalesce-function\)](#) function to ensure compatibility:

## Public Preview - Export STIX threat intelligence objects

**Type:** New feature

**Service category:** Security Information and Event Management (SIEM)

**Product capability:** Export STIX threat intelligence objects

Microsoft Sentinel now supports exporting STIX threat intelligence objects to other destinations, such as external platforms. If you've ingested threat intelligence to Microsoft Sentinel from an external platform, such as when using the Threat Intelligence - TAXII data connector, you can now export threat intelligence back to that platform, **enabling bi-directional intelligence sharing**. This new support provides direct and secure sharing, reducing the need for manual processes or custom playbooks to distribute threat intelligence.

For more information: [Connect to STIX/TAXII threat intelligence feeds - Microsoft Sentinel | Microsoft Learn](#)

# Sentinel

**General Availability – Enriched advanced hunting and custom detections queries with behavior insights**

**Type:** Update

**Service category:** Security Information and Event Management (SIEM)

**Product capability:** Hunting

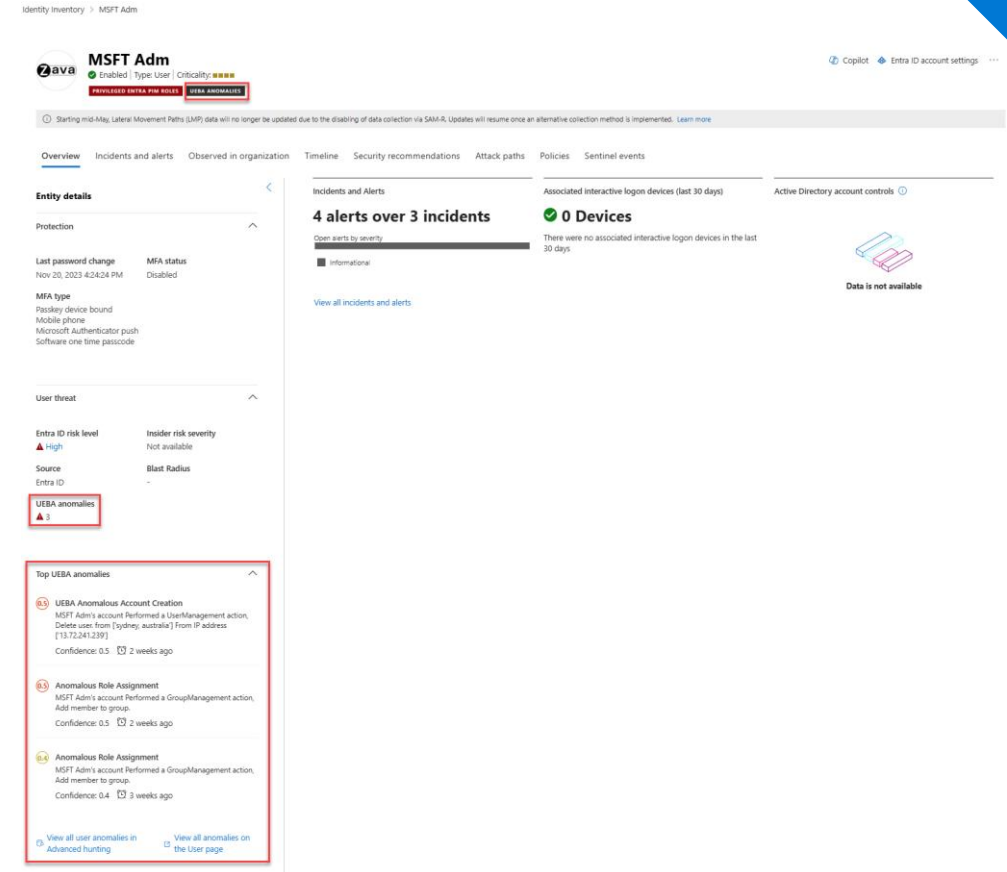
Advanced hunting and custom detection experiences now include a contextual banner that prompts analysts to join the UEBA Anomalies table to queries that include UEBA data sources.

- Users with behavioral anomalies are automatically tagged with **UEBA Anomalies**, helping analysts quickly identify which users to prioritize.

All features require UEBA to be enabled and are workspace-scoped to the currently selected workspace.

- For more information, see [How UEBA empowers analysts and streamlines workflows](#).  
[Agentless data connector](#) for Sentinel Solution for SAP now generally available. Learn more from our [Tech Community blog](#).
- Deprecation: Containerized SAP data connector will be out of support by September 30th 2026. [Migrate to our Agentless SAP data connector](#) today.

**Learn more:** [Advanced threat detection with User and Entity Behavior Analytics \(UEBA\) in Microsoft Sentinel | Microsoft Learn](#)



# Security Copilot

The background of the slide features abstract, flowing shapes in various shades of green and blue, creating a modern and dynamic visual effect.

# Security Copilot

Public Preview

## Public Preview – Security Copilot inclusion in Microsoft 365 E5 subscription

**Type:** Update

**Service category:** Security Copilot

**Product capability:** Security Copilot

We are excited to announce that Security Copilot will be included for all Microsoft 365 E5 customers in the upcoming months - bringing agentic AI in the daily workflow. Customers will receive a 30-day advanced notification before activation. If you're already a Microsoft 365 E5 customer using Security Copilot, you can access this benefit at no additional cost.

Customers with Microsoft 365 E5 will have 400 Security Compute Units (SCU) each month for every 1,000 paid user license, up to 10,000 SCUs each month at no additional cost. This is scalable.

**Learn more:** [Security Copilot inclusion](#)



# Security Copilot

## Public Preview – Security Copilot Agents

**Type:** Update

**Service category:** Security Copilot

**Product capability:** Security Copilot agents

We're not only making these agents more easily accessible, we're extending the ecosystem even further. Adding to the [37 Security Copilot agents already available](#), we're introducing more than 40 new Microsoft and partner-built agents. 12 new Microsoft-built agents across Microsoft Defender, Entra, Intune, and Purview are available today in preview. Additionally, more than 30 new partner-built agents extend protection end-to-end. These agents automate large-scale tasks, which allows security teams to dedicate more time to strategic initiatives.

**Learn more:** [Agents built into your workflow: Get Security Copilot with Microsoft 365 E5 | Microsoft Security Blog](#)

Public Preview



Defender

# Defender for Cloud

Public Preview

## Public Preview – Microsoft Cloud Security Benchmark (MCSB) v2

**Type:** New feature

**Service category:** Cloud Security Posture Management (CSPM)

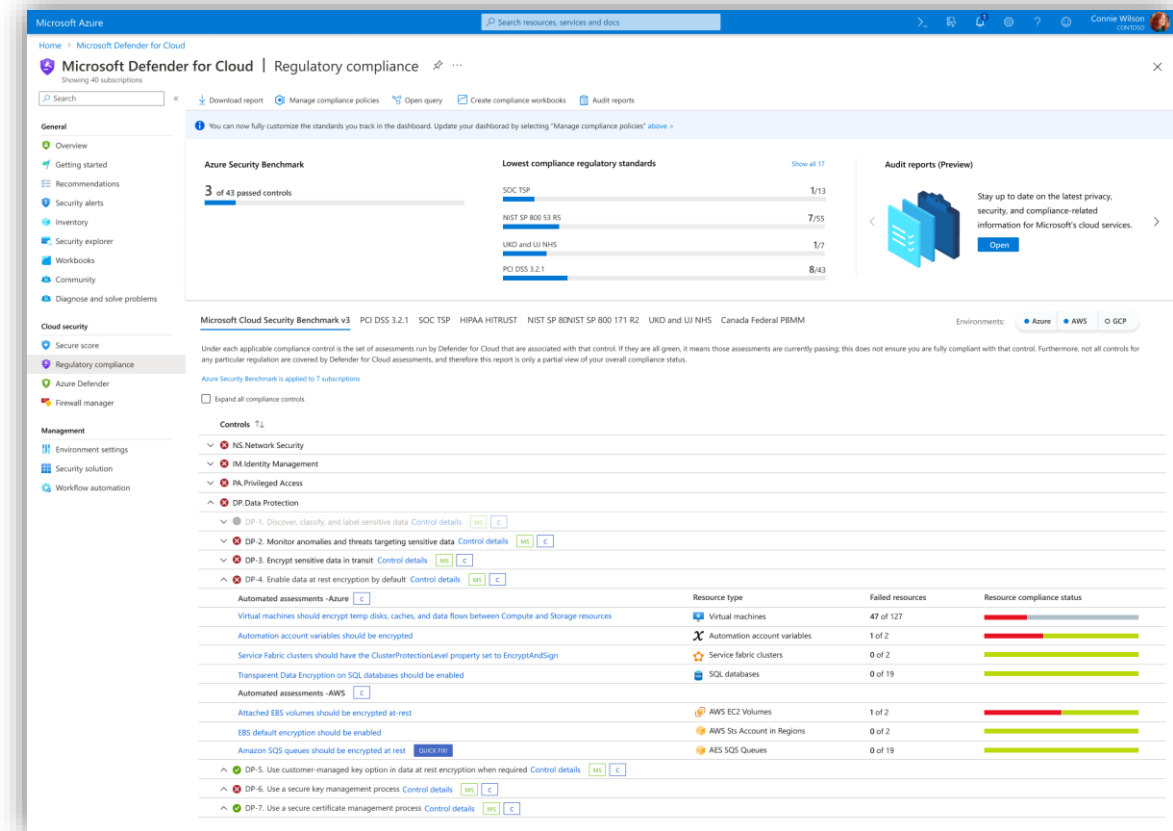
**Product capability:** Compliance & Governance

We're excited to announce the **Public Preview of MCSB v2** in Microsoft Defender for Cloud. This update introduces a risk-based compliance framework with expanded Azure Policy controls and AI workload guidance, helping organizations secure multi-cloud environments more effectively.

With this feature, customers can:

- Assess compliance posture using risk-based scoring
- Apply AI-driven recommendations for workload hardening
- Align with industry benchmarks across Azure and hybrid environments

**Learn more:** [Defender for Cloud Release Notes](#)



# Defender for Cloud

## Public Preview – Restrict Pod Access Response Action

**Type:** New feature

**Service category:** Kubernetes Security

**Product capability:** Threat Containment

We're thrilled to announce the **Public Preview of Restrict Pod Access** in Microsoft Defender for Cloud. This feature enables Kubernetes response actions via Defender XDR to block sensitive interfaces within compromised pods, reducing lateral movement risk.

**Learn more:** [Defender for Cloud Release Notes](#)

Public Preview





# Defender for Cloud

## General Availability – Continuous Vulnerability Re-scan for Container Images

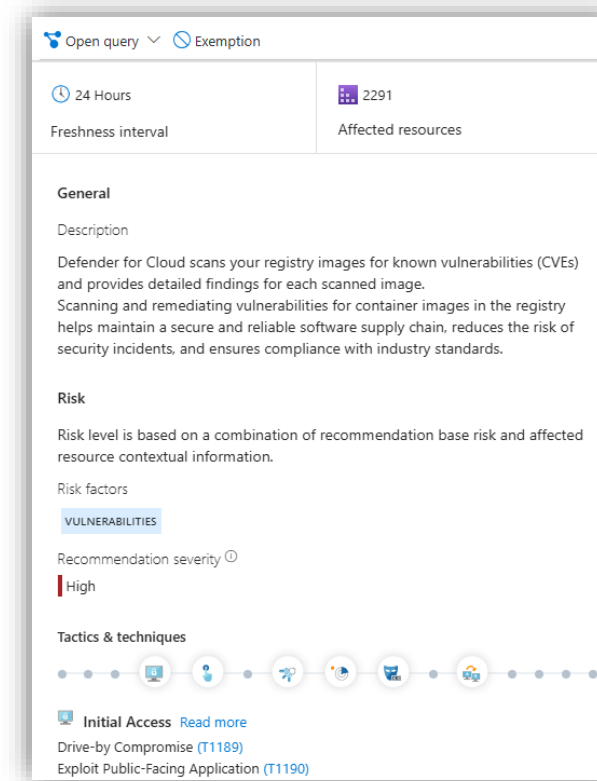
**Type:** Enhancement

**Service category:** Container Security

**Product capability:** Vulnerability Management

We're pleased to announce **GA of continuous vulnerability re-scanning** for container images in Microsoft Defender for Cloud.

**Learn more:** [Defender for Cloud Release Notes](#)



General Availability

## General Availability – Additional Compliance Frameworks

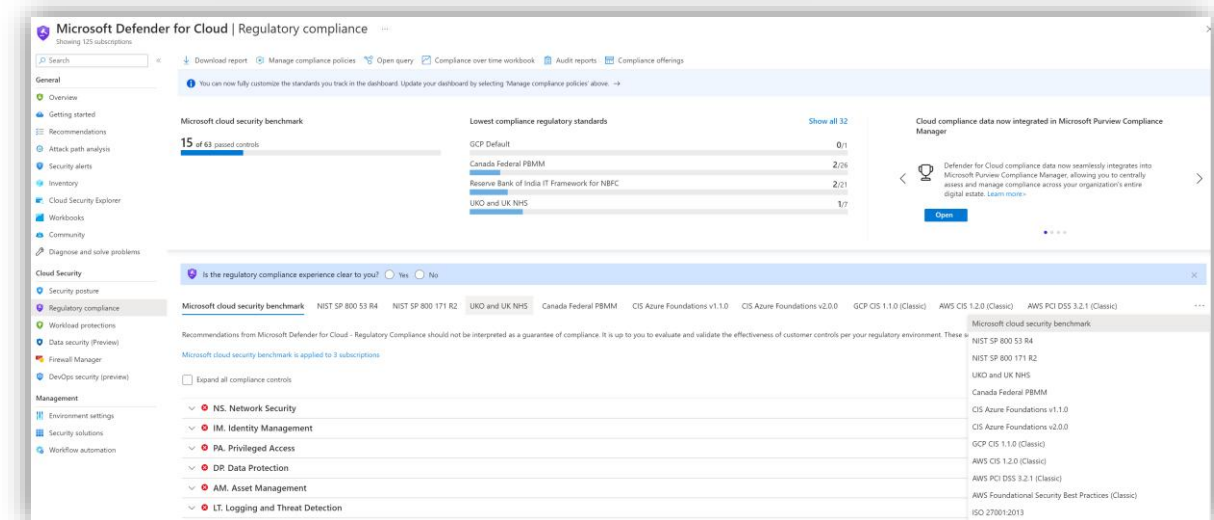
**Type:** Enhancement

**Service category:** Compliance Management

**Product capability:** Regulatory Alignment

We're pleased to announce **GA of additional compliance frameworks** in Microsoft Defender for Cloud.

**Learn more:** [Defender for Cloud Release Notes](#)



# Defender XDR

## Public Preview – Threat Intelligence Briefing Agent

Type: New feature

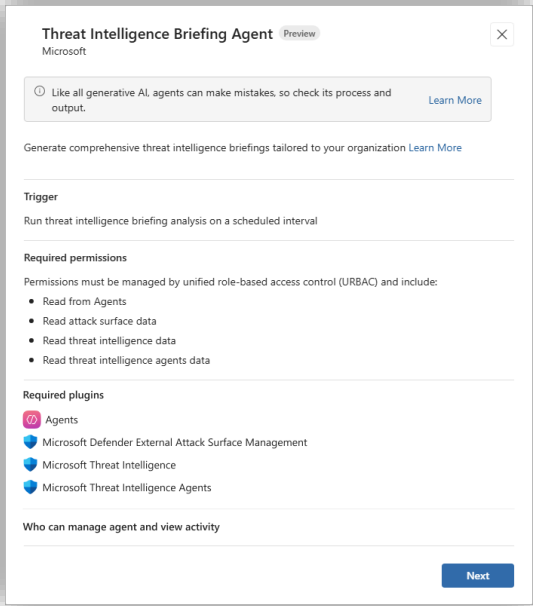
Service category: Threat Intelligence

Product capability: Advisory Services

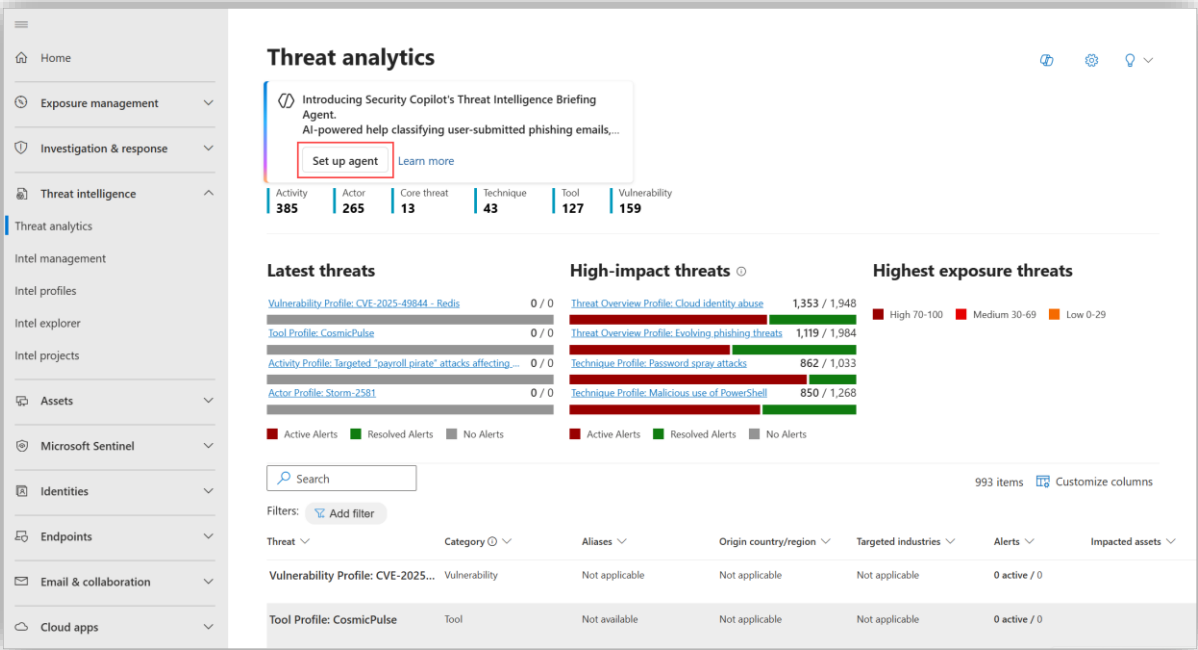
We’re thrilled to announce the **Threat Intelligence Briefing Agent (Public Preview)** in Microsoft Defender XDR. This agent delivers **daily customized threat briefings**, real-time intelligence feeds, and integrates with **Threat Analytics dashboards**. Benefits include:

- Proactive **threat awareness** for customers.
- Enhanced **advisory and consulting opportunities**.
- Strengthened **customer trust and engagement**.  
Partners can use this to offer **retainer-based advisory services**.

Learn more: [Defender XDR What's New & Microsoft Security Copilot Threat Intelligence Briefing Agent](#)



Public Preview



# Defender XDR

Public Preview

## Public Preview – IdentityAccountInfo Table in Advanced Hunting

**Type:** New feature

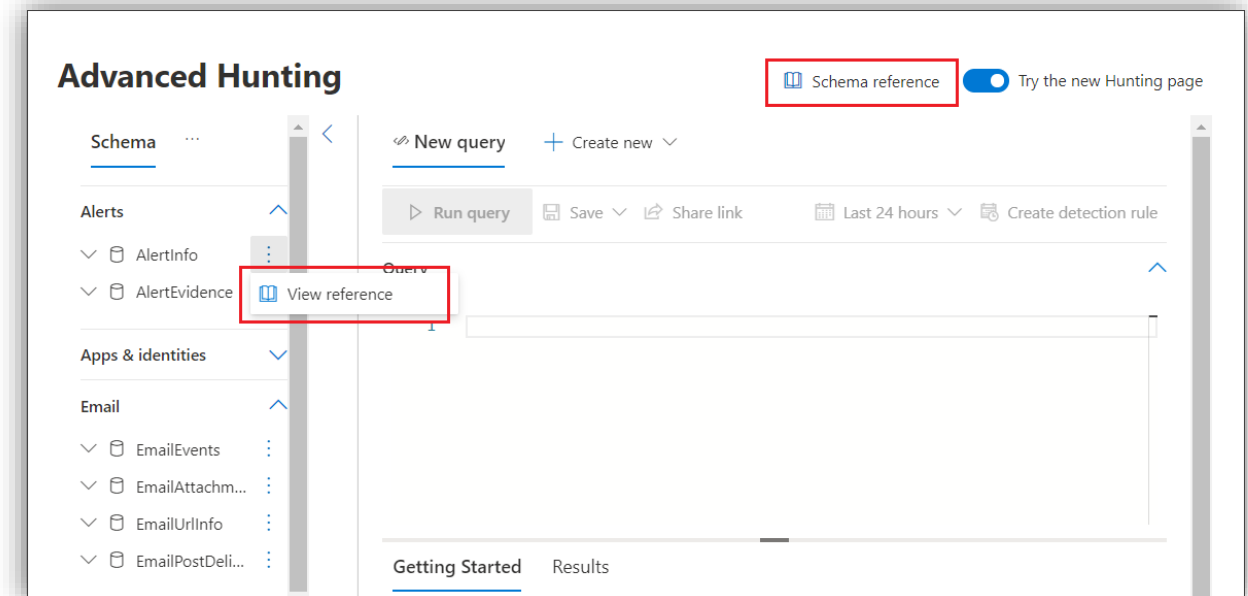
**Service category:** Threat Hunting

**Product capability:** Identity Security

We're excited to announce the **Public Preview of IdentityAccountInfo table** in Microsoft Defender XDR.

This table contains information about account information from various sources, including Microsoft Entra ID. It also includes information and link to the identity that owns the account.

**Learn more:** [Defender XDR What's New](#)



# Defender XDR

Public Preview

## Public Preview – Threat Analytics Indicators Tab

**Type:** Enhancement

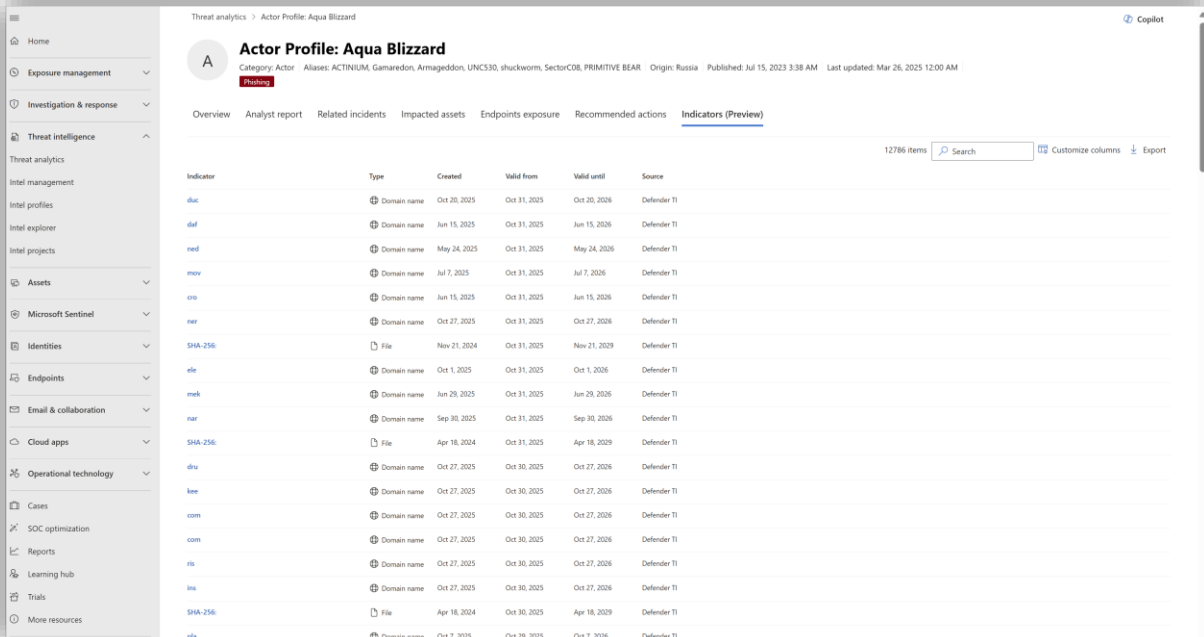
**Service category:** Threat Intelligence

**Product capability:** Incident Response

We're thrilled to announce the **Indicators tab in Threat Analytics** for Microsoft Defender XDR.

Threat analytics now has an Indicators tab that provides a list of all indicators of compromise (IOCs) associated with a threat. Microsoft researchers update these IOCs in real time as they find new evidence related to the threat. This information helps your security operations center (SOC) and threat intelligence analysts with remediation and proactive hunting

**Learn more:** [Defender XDR What's New](#)



The screenshot displays the 'Actor Profile: Aqua Blizzard' page in the Microsoft Defender XDR Threat Analytics interface. The page is divided into a left-hand navigation pane and a main content area. The navigation pane includes links to Home, Exposure management, Investigation & response, Threat intelligence, Intel profiles, Intel explorer, Intel projects, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Operational technology, Cases, SOC optimization, Reports, Learning hub, Trials, and More resources. The main content area shows the 'Actor Profile: Aqua Blizzard' with a category of 'Actor' and aliases including ACTINIUM, Gamaredon, Armageddon, UNC330, shuckworm, SectorC0B, and PRIMITIVE BEAR. The origin is listed as Russia, published on Jul 15, 2023, and last updated on Mar 26, 2025. The 'Indicators (Preview)' tab is selected, showing a table of 12786 items. The table has columns for Indicator, Type, Created, Valid from, Valid until, and Source. The indicators listed include domain names, files, and domain names with various valid from and until dates.

Indicator	Type	Created	Valid from	Valid until	Source
dlc	Domain name	Oct 20, 2025	Oct 31, 2025	Oct 20, 2026	Defender TI
dlf	Domain name	Jun 15, 2025	Oct 31, 2025	Jun 15, 2026	Defender TI
ned	Domain name	May 24, 2025	Oct 31, 2025	May 24, 2026	Defender TI
now	Domain name	Jul 7, 2025	Oct 31, 2025	Jul 7, 2026	Defender TI
cro	Domain name	Jun 15, 2025	Oct 31, 2025	Jun 15, 2026	Defender TI
ner	Domain name	Oct 27, 2025	Oct 31, 2025	Oct 27, 2026	Defender TI
SHA-256:	File	Nov 21, 2024	Oct 31, 2025	Nov 21, 2029	Defender TI
ele	Domain name	Oct 1, 2025	Oct 31, 2025	Oct 1, 2026	Defender TI
mek	Domain name	Jun 29, 2025	Oct 31, 2025	Jun 29, 2026	Defender TI
nar	Domain name	Sep 30, 2025	Oct 31, 2025	Sep 30, 2026	Defender TI
SHA-256:	File	Apr 18, 2024	Oct 31, 2025	Apr 18, 2029	Defender TI
dlu	Domain name	Oct 27, 2025	Oct 30, 2025	Oct 27, 2026	Defender TI
lee	Domain name	Oct 27, 2025	Oct 30, 2025	Oct 27, 2026	Defender TI
com	Domain name	Oct 27, 2025	Oct 30, 2025	Oct 27, 2026	Defender TI
com	Domain name	Oct 27, 2025	Oct 30, 2025	Oct 27, 2026	Defender TI
rs	Domain name	Oct 27, 2025	Oct 30, 2025	Oct 27, 2026	Defender TI
iss	Domain name	Oct 27, 2025	Oct 30, 2025	Oct 27, 2026	Defender TI
SHA-256:	File	Apr 18, 2024	Oct 30, 2025	Apr 18, 2029	Defender TI
pla	Domain name	Oct 7, 2025	Oct 29, 2025	Oct 7, 2026	Defender TI

# Defender XDR

## Unified Custom Detections

**Type:** New feature

**Service category:** Detection Engineering

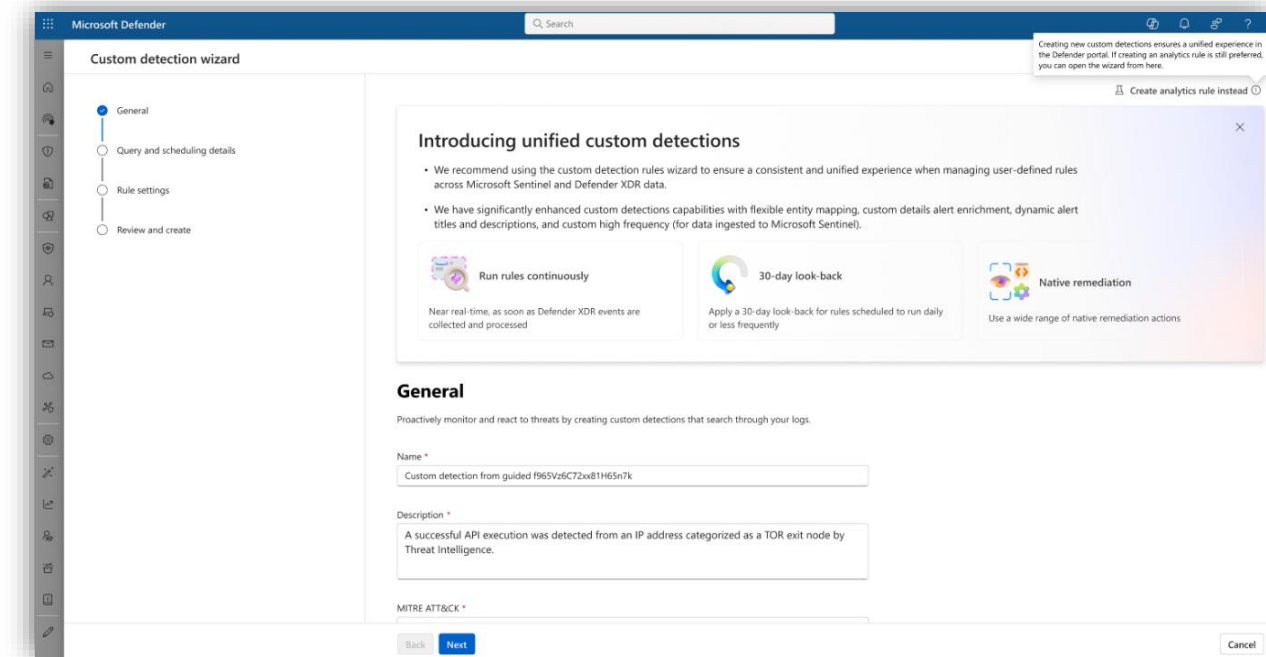
**Product capability:** Cross-Platform Security

We're pleased to announce **Unified Custom Detections** in Microsoft Defender XDR. This feature allows **single-pane authoring** of detection rules across endpoints, email, identity, and cloud apps.

Benefits include:

- Simplified **rule management** for SOC teams.
- Consistent detection logic across multiple domains.
- Reduced operational complexity for MSSPs.  
Partners can position this as a **SOC optimization capability**.

**Learn more:** [Defender XDR What's New](#) & [Custom detections are now the unified experience for creating detections in Microsoft Defender](#)



# Defender XDR

## Defender Experts Reports: Trends & Emerging Threats

**Type:** Enhancement

**Service category:** Managed Detection & Response

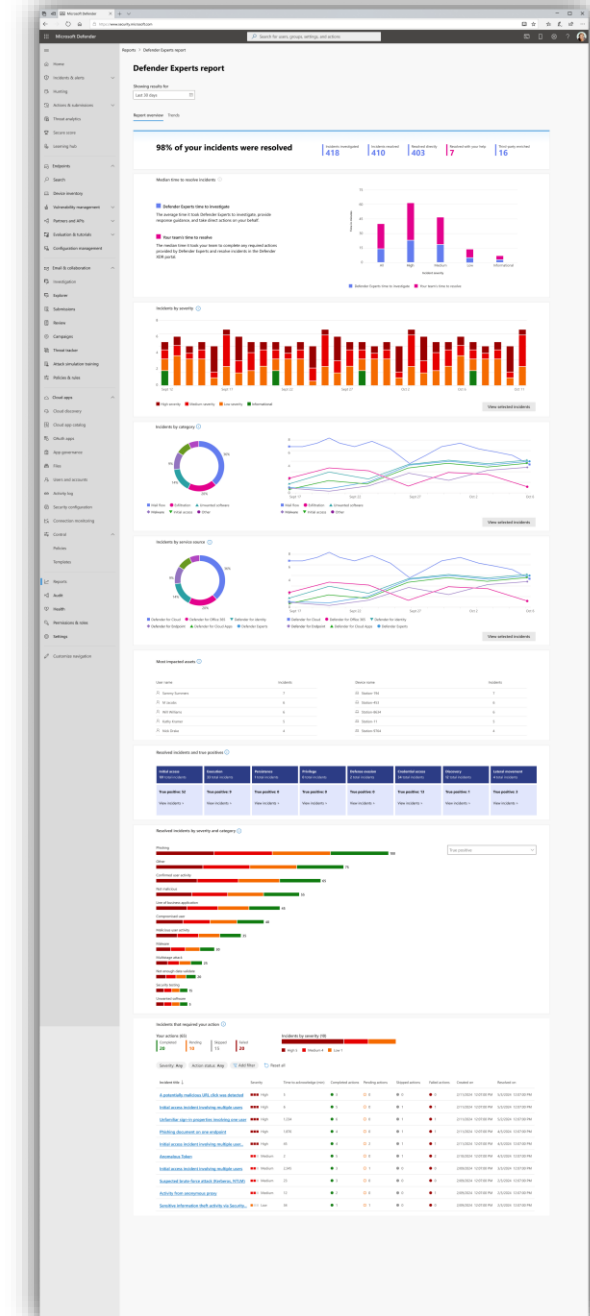
## Product capability: Reporting & Analytics

We're pleased to announce **expanded Defender Experts Reports** in Microsoft Defender XDR. These reports now include **trend analysis, emerging threat insights, and MITRE tactic mapping**.

Benefits include:

- Improved **customer reporting** and transparency.
- Actionable insights for **proactive defense**.
- Demonstrated MDR value for renewals and upsell. Partners can leverage this for **premium MDR offerings**.

**Learn more:** [Defender Experts for XDR reports](#)



# TP&D Services

# 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.

## Technical consultations scope:

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

The screenshot shows the Microsoft Partner Center interface for requesting technical services. The form is titled 'Request technical presales and deployment services' and includes a search bar at the top. Below the title, there are sections for 'Case Title', 'Case Description', 'Solution Area', and 'Who should we contact about this request?'. The 'Case Title' field contains 'Using Azure Backup with IaaS'. The 'Case Description' field contains a paragraph about a client using Azure Virtual Machines and needing help with Azure Backup. The 'Solution Area' dropdown is set to 'Infrastructure'. The 'Who should we contact about this request?' section includes fields for 'First Name' (William), 'Last Name' (Beringer), 'Phone Number' (206-555-0100), and 'Email' (William@contoso.com). There is also a 'Where are you located?' dropdown set to 'United States' and a 'Language' dropdown set to 'English'. At the bottom, there are 'Submit request' and 'Cancel' buttons.

Infrastructure (Azure)

Modern Work

Digital & App Innovation (Azure)

Security

Business Applications

ISV

## 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>

Or directly to:

- Andre Barreiros [abarreiros@microsoft.com](mailto:abarreiros@microsoft.com)
- Daniela Magalhaes [Daniela.Magalhaes@microsoft.com](mailto:Daniela.Magalhaes@microsoft.com)
- Marco Cardoso [Marco.Cardoso@microsoft.com](mailto:Marco.Cardoso@microsoft.com)



Thank you