Microsoft Security

Phishing Triage

Alert Triage in DLP and IR

Conditional

AgentCon Milan

Espandere Microsoft Security Copilot con agenti AI

Mario Serra

MW & Security Specialist @ Overnet

Microsoft MVP Security

Michele Sensalari

CTO @Overnet

Microsoft MVP Security

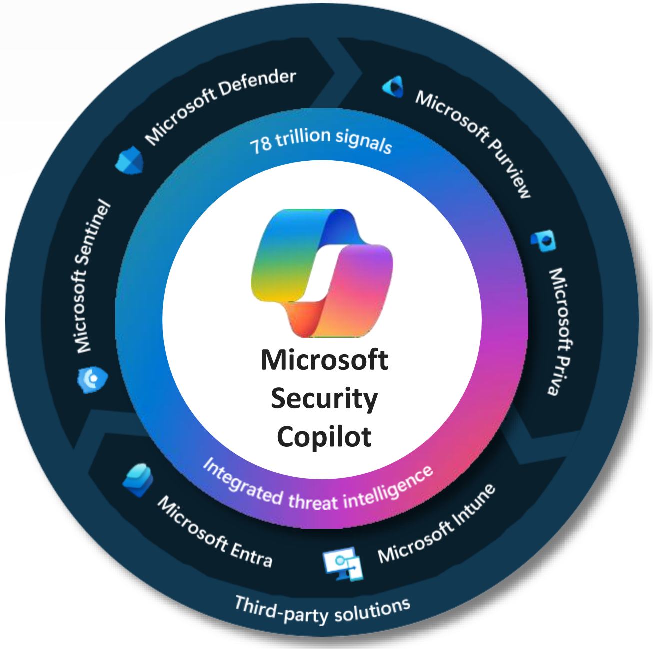
WindowServer.it

global AI community

Security Copilot

Microsoft Security Copilot

Microsoft Security Copilot is an advanced cybersecurity tool that leverages artificial intelligence to enhance the detection, analysis, and response to cyber threats. It integrates various security data sources, including system logs, network events, and vulnerability information, to offer a comprehensive view of an organization's IT infrastructure security status.



Use cases include:

- Incident Summaries
- Guided Response
- Threat Intelligence
- Script Analysis
- Incident Reporting

Microsoft Security Copilot

Primary use cases

Incident Response — Summarize incidents, assess impact, and receive tailored remediation guidance, including for triage, investigation, and containment.

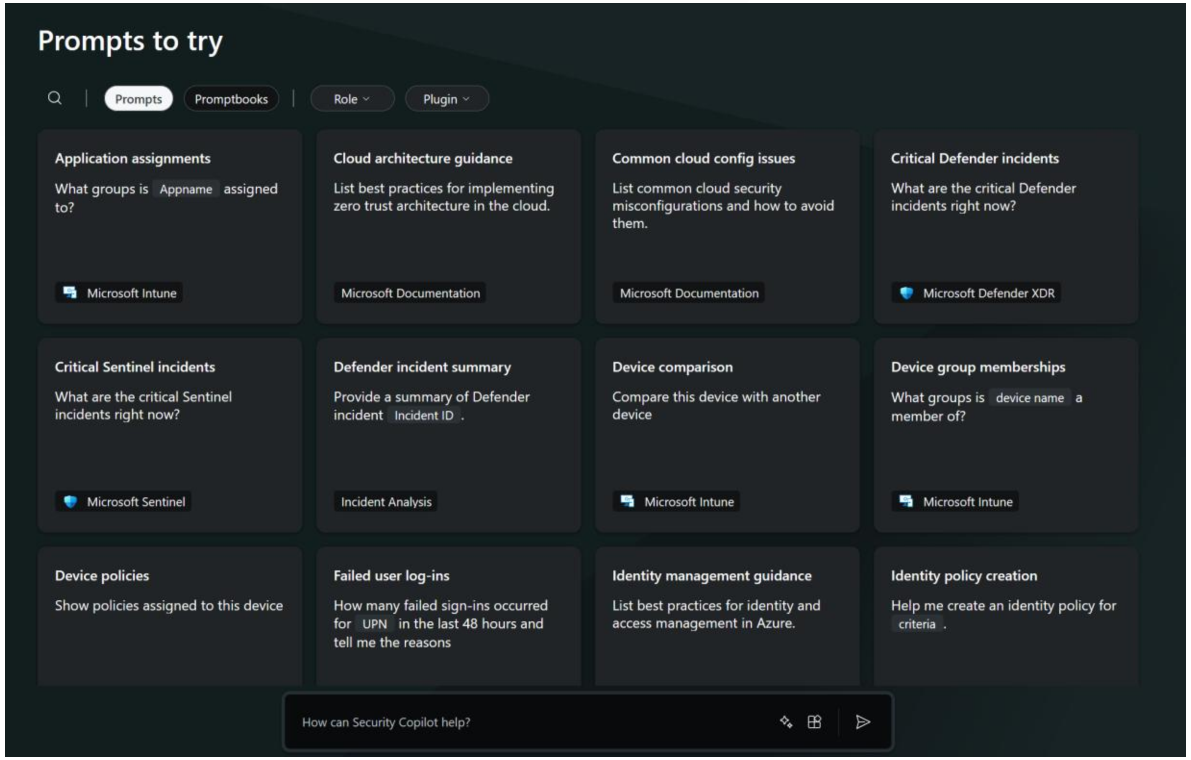
Security Reports — Summarize investigations, incidents, vulnerabilities, or threats in minutes and prepare the information in ready-to-share reports.

Reverse Script Engineering — Analyze complex command line scripts and translate them into natural language with clear explanations of actions.

Security Posture Management — Learn if your organization is at risk from vulnerabilities and examine resources in your environment for signs of a breach.

Standalone Copilot Security Experiences

The Standalone experience is best when you need a centralized, immersive portal for security operations.



Prompts to try

Application assignments
What groups is Appname assigned to?
Microsoft Intune

Cloud architecture guidance
List best practices for implementing zero trust architecture in the cloud.
Microsoft Documentation

Common cloud config issues
List common cloud security misconfigurations and how to avoid them.
Microsoft Documentation

Critical Defender incidents
What are the critical Defender incidents right now?
Microsoft Defender XDR

Critical Sentinel incidents
What are the critical Sentinel incidents right now?
Microsoft Sentinel

Defender incident summary
Provide a summary of Defender incident Incident ID .
Incident Analysis

Device comparison
Compare this device with another device
Microsoft Intune

Device group memberships
What groups is device name a member of?
Microsoft Intune

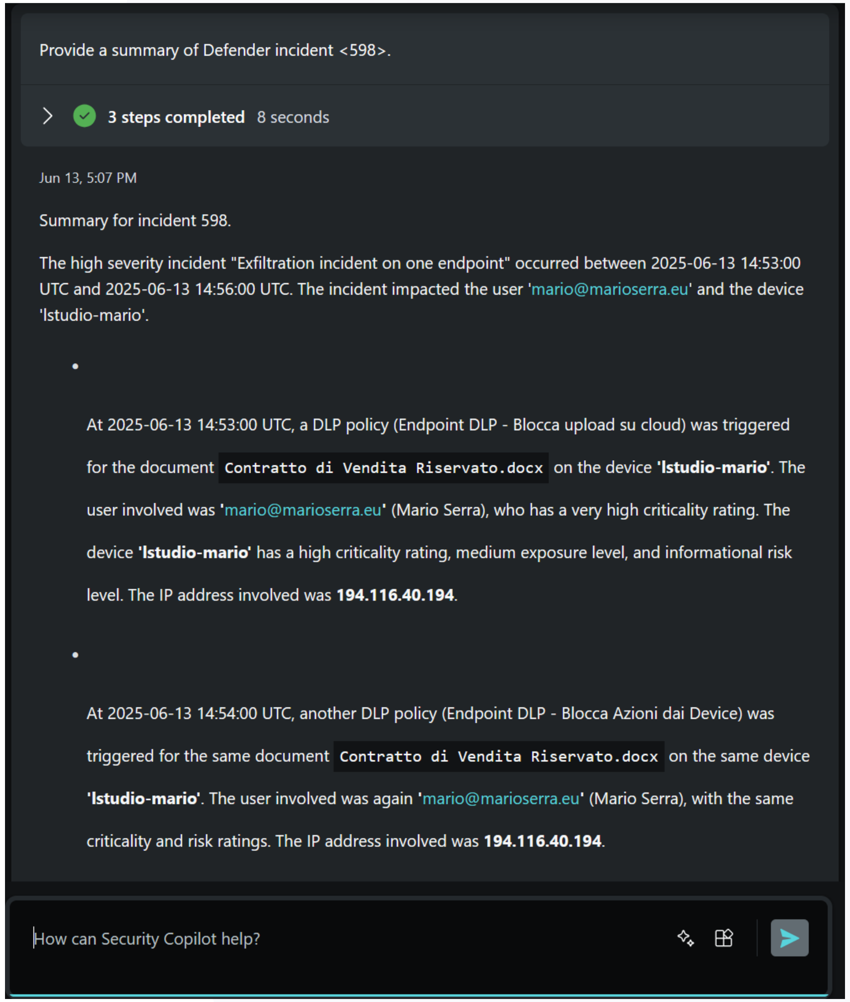
Device policies
Show policies assigned to this device

Failed user log-ins
How many failed sign-ins occurred for UPN in the last 48 hours and tell me the reasons

Identity management guidance
List best practices for identity and access management in Azure.

Identity policy creation
Help me create an identity policy for criteria .

How can Security Copilot help?



Provide a summary of Defender incident <598>.

3 steps completed 8 seconds

Jun 13, 5:07 PM

Summary for incident 598.

The high severity incident "Exfiltration incident on one endpoint" occurred between 2025-06-13 14:53:00 UTC and 2025-06-13 14:56:00 UTC. The incident impacted the user 'mario@marioserra.eu' and the device 'lstudio-mario'.

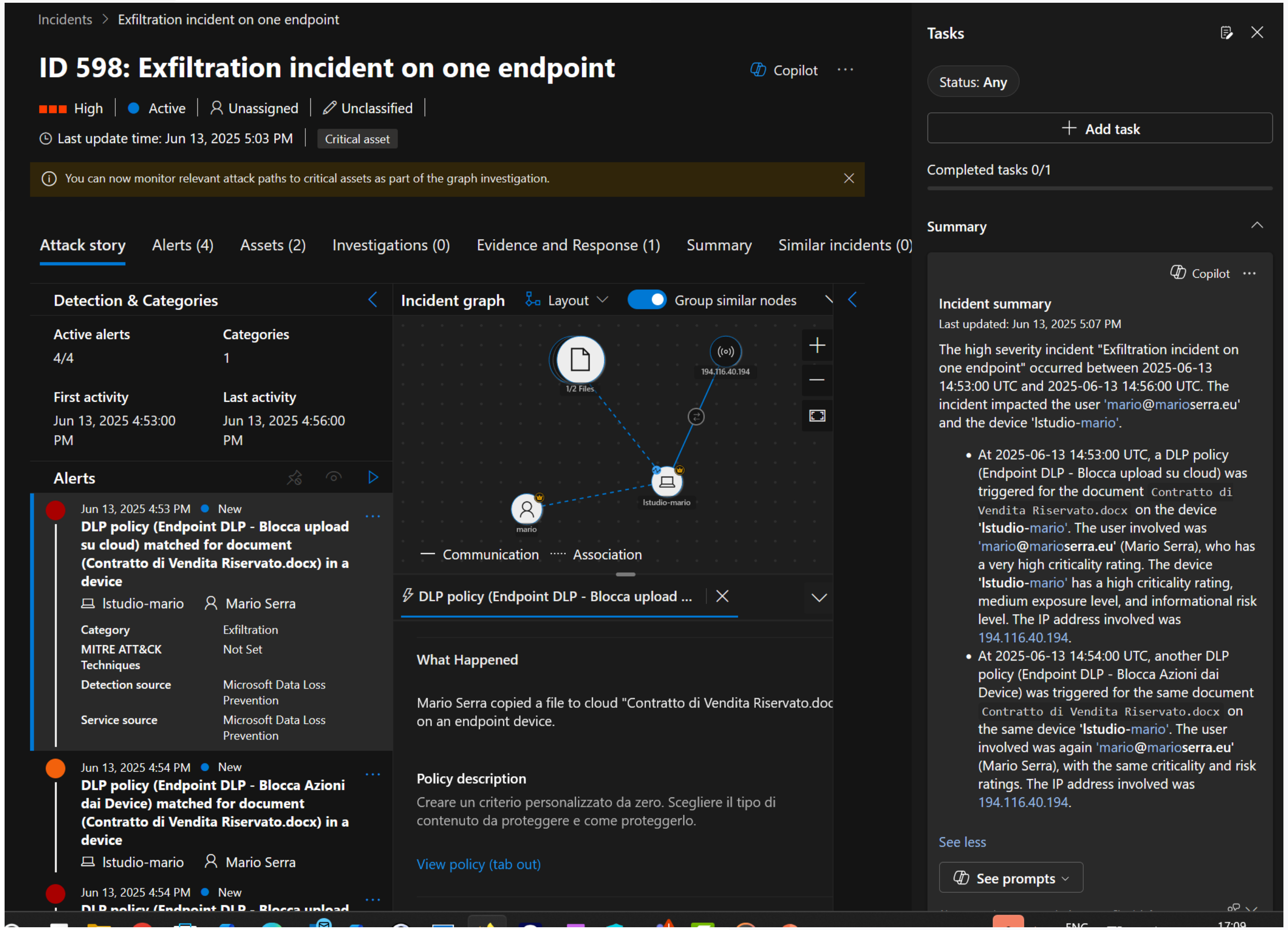
- At 2025-06-13 14:53:00 UTC, a DLP policy (Endpoint DLP - Blocca upload su cloud) was triggered for the document `Contratto di Vendita Riservato.docx` on the device **'lstudio-mario'**. The user involved was 'mario@marioserra.eu' (Mario Serra), who has a very high criticality rating. The device **'lstudio-mario'** has a high criticality rating, medium exposure level, and informational risk level. The IP address involved was **194.116.40.194**.

- At 2025-06-13 14:54:00 UTC, another DLP policy (Endpoint DLP - Blocca Azioni dai Device) was triggered for the same document `Contratto di Vendita Riservato.docx` on the same device **'lstudio-mario'**. The user involved was again 'mario@marioserra.eu' (Mario Serra), with the same criticality and risk ratings. The IP address involved was **194.116.40.194**.

How can Security Copilot help?

Embedded Copilot Security Experiences

The Embedded experience may be used when you want to enhance your workflow within existing Microsoft security products with Copilot's AI capabilities.



ID 598: Exfiltration incident on one endpoint

High | Active | Unassigned | Unclassified

Last update time: Jun 13, 2025 5:03 PM | Critical asset

You can now monitor relevant attack paths to critical assets as part of the graph investigation.

Detection & Categories

Active alerts	Categories
4/4	1
First activity	**Last activity**
Jun 13, 2025 4:53:00 PM	Jun 13, 2025 4:56:00 PM

Alerts

Jun 13, 2025 4:53 PM ● New

DLP policy (Endpoint DLP - Blocca upload su cloud) matched for document (Contratto di Vendita Riservato.docx) in a device

Istudio-mario   Mario Serra

Category	Exfiltration
MITRE ATT&CK Techniques	Not Set
Detection source	Microsoft Data Loss Prevention
Service source	Microsoft Data Loss Prevention

Jun 13, 2025 4:54 PM ● New

DLP policy (Endpoint DLP - Blocca Azioni dai Device) matched for document (Contratto di Vendita Riservato.docx) in a device

Istudio-mario   Mario Serra

Jun 13, 2025 4:54 PM ● New

DLP policy (Endpoint DLP - Blocca upload

DLP policy (Endpoint DLP - Blocca upload ...

What Happened

Mario Serra copied a file to cloud "Contratto di Vendita Riservato.doc
on an endpoint device.

Policy description

Creare un criterio personalizzato da zero. Scegliere il tipo di contenuto da proteggere e come proteggerlo.

View policy (tab out)

Completed tasks 0/1

Summary

Incident summary

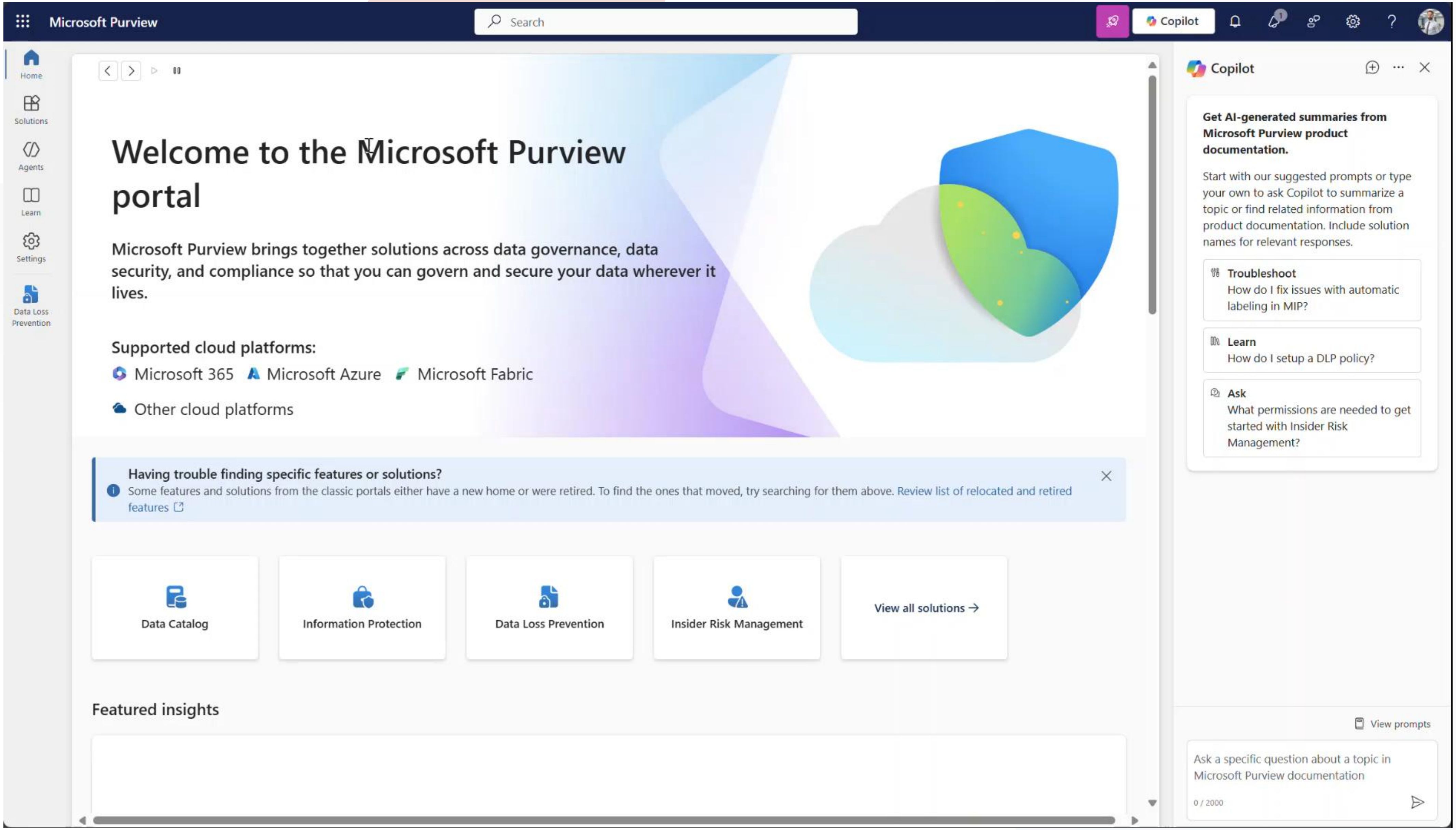
Last updated: Jun 13, 2025 5:07 PM

The high severity incident "Exfiltration incident on one endpoint" occurred between 2025-06-13 14:53:00 UTC and 2025-06-13 14:56:00 UTC. The incident impacted the user 'mario@marioserra.eu' and the device 'Istudio-mario'.

- At 2025-06-13 14:53:00 UTC, a DLP policy (Endpoint DLP - Blocca upload su cloud) was triggered for the document `Contratto di Vendita Riservato.docx` on the device **'Istudio-mario'**. The user involved was 'mario@marioserra.eu' (Mario Serra), who has a very high criticality rating. The device **'Istudio-mario'** has a high criticality rating, medium exposure level, and informational risk level. The IP address involved was 194.116.40.194.
- At 2025-06-13 14:54:00 UTC, another DLP policy (Endpoint DLP - Blocca Azioni dai Device) was triggered for the same document `Contratto di Vendita Riservato.docx` on the same device **'Istudio-mario'**. The user involved was again 'mario@marioserra.eu' (Mario Serra), with the same criticality and risk ratings. The IP address involved was 194.116.40.194.

Demo

Microsoft Security Copilot Users Experience



Welcome to the Microsoft Purview portal

Microsoft Purview brings together solutions across data governance, data security, and compliance so that you can govern and secure your data wherever it lives.

Supported cloud platforms:

Microsoft 365 Microsoft Azure Microsoft Fabric

Other cloud platforms

Having trouble finding specific features or solutions?
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features

Featured insights

Copilot

Get AI-generated summaries from Microsoft Purview product documentation.

Start with our suggested prompts or type your own to ask Copilot to summarize a topic or find related information from product documentation. Include solution names for relevant responses.

Troubleshoot
How do I fix issues with automatic labeling in MIP?

Learn
How do I setup a DLP policy?

Ask
What permissions are needed to get started with Insider Risk Management?

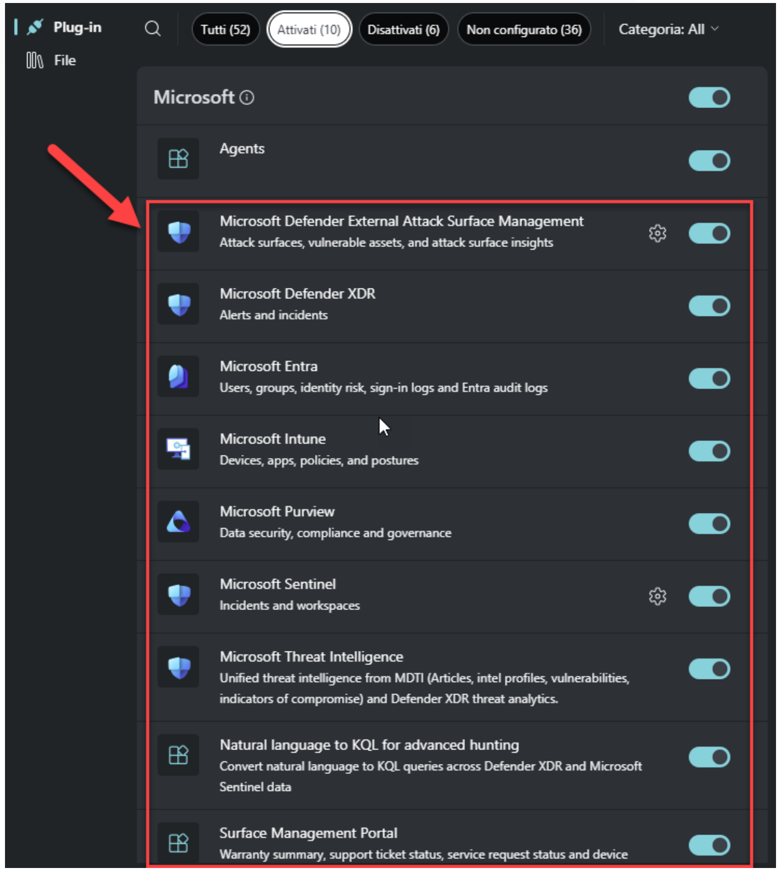
View prompts

Ask a specific question about a topic in Microsoft Purview documentation

0 / 2000

Plugin

Copilot for Security comes with many default plugins and supports several non-Microsoft plugins. You can also extend Copilot for Security's capabilities by adding or creating your own plugin. The Copilot for Security platform enables developers and users to write plugins that can be invoked to perform specialized tasks.



Agents

Microsoft Defender External Attack Surface Management
Attack surfaces, vulnerable assets, and attack surface insights

Microsoft Defender XDR
Alerts and incidents

Microsoft Entra
Users, groups, identity risk, sign-in logs and Entra audit logs

Microsoft Intune
Devices, apps, policies, and postures

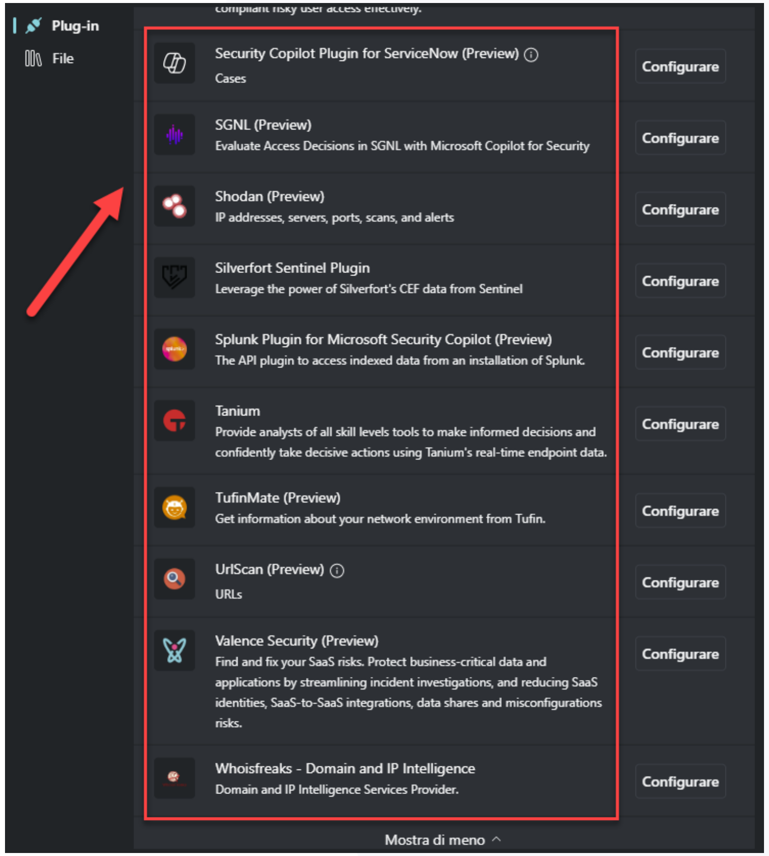
Microsoft Purview
Data security, compliance and governance

Microsoft Sentinel
Incidents and workspaces

Microsoft Threat Intelligence
Unified threat intelligence from MDTI (Articles, intel profiles, vulnerabilities, indicators of compromise) and Defender XDR threat analytics.

Natural language to KQL for advanced hunting
Convert natural language to KQL queries across Defender XDR and Microsoft Sentinel data

Surface Management Portal
Warranty summary, support ticket status, service request status and device



compliant risky user access effectively.

Security Copilot Plugin for ServiceNow (Preview)
Cases

SGNL (Preview)
Evaluate Access Decisions in SGNL with Microsoft Copilot for Security

Shodan (Preview)
IP addresses, servers, ports, scans, and alerts

Silverfort Sentinel Plugin
Leverage the power of Silverfort's CEF data from Sentinel

Splunk Plugin for Microsoft Security Copilot (Preview)
The API plugin to access indexed data from an installation of Splunk.

Tanium
Provide analysts of all skill levels tools to make informed decisions and confidently take decisive actions using Tanium's real-time endpoint data.

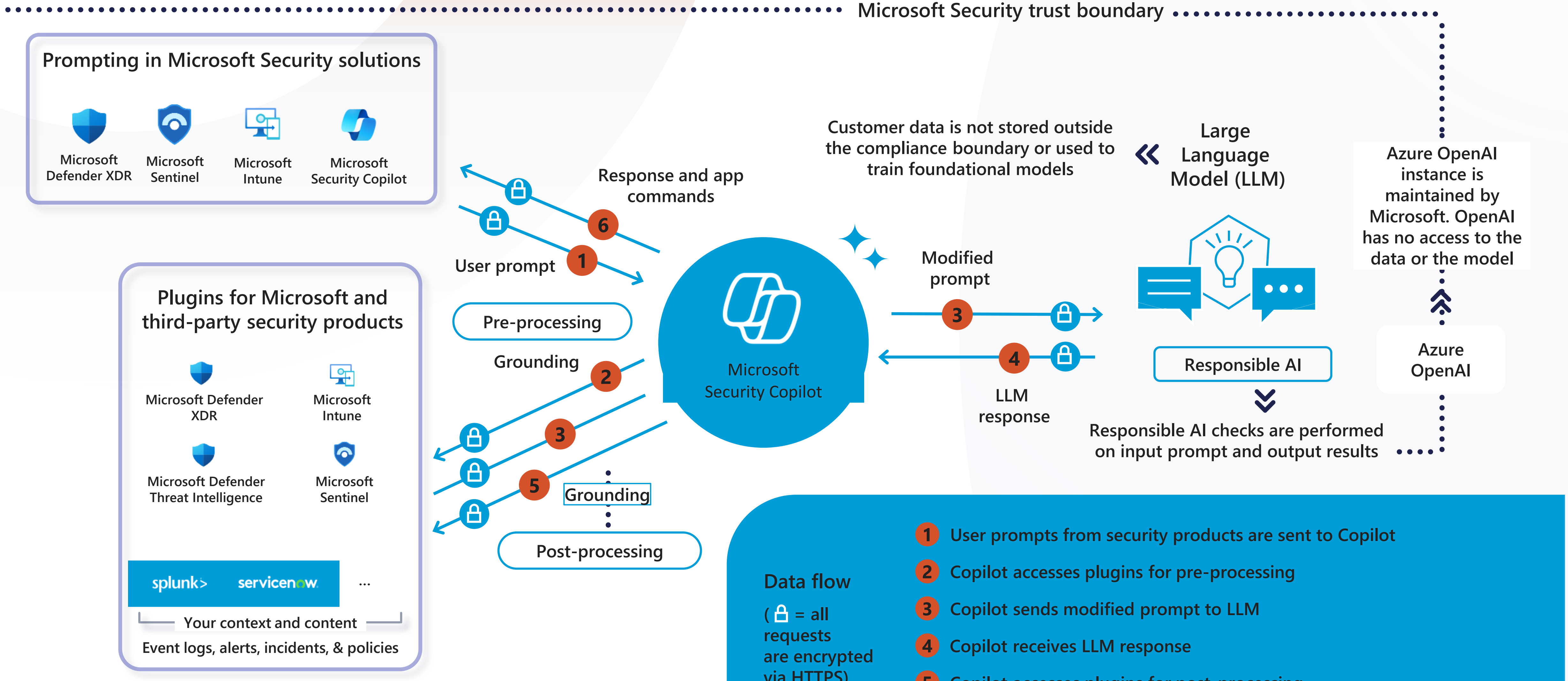
TufinMate (Preview)
Get information about your network environment from Tufin.

UrlScan (Preview)
URLs

Valence Security (Preview)
Find and fix your SaaS risks. Protect business-critical data and applications by streamlining incident investigations, and reducing SaaS identities, SaaS-to-SaaS integrations, data shares and misconfigurations risks.

Whoisfreaks - Domain and IP Intelligence
Domain and IP Intelligence Services Provider.

Data flow for Microsoft Copilot for Security



Microsoft Security trust boundary

Prompting in Microsoft Security solutions

Microsoft Defender XDR

Microsoft Sentinel

Microsoft Intune

Microsoft Security Copilot

Response and app commands

6

User prompt

1

Plugins for Microsoft and third-party security products

Microsoft Defender XDR

Microsoft Intune

Microsoft Defender Threat Intelligence

Microsoft Sentinel

splunk> servicenow ...

Your context and content

Event logs, alerts, incidents, & policies

Pre-processing

Grounding

2

3

5

Grounding

Post-processing

Microsoft Security Copilot

Customer data is not stored outside the compliance boundary or used to train foundational models

Modified prompt

3

4

LLM response

Large Language Model (LLM)

Responsible AI

Responsible AI checks are performed on input prompt and output results

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

Azure OpenAI

Data flow

(🔒 = all requests are encrypted via HTTPS)

1 User prompts from security products are sent to Copilot

2 Copilot accesses plugins for pre-processing

3 Copilot sends modified prompt to LLM

4 Copilot receives LLM response

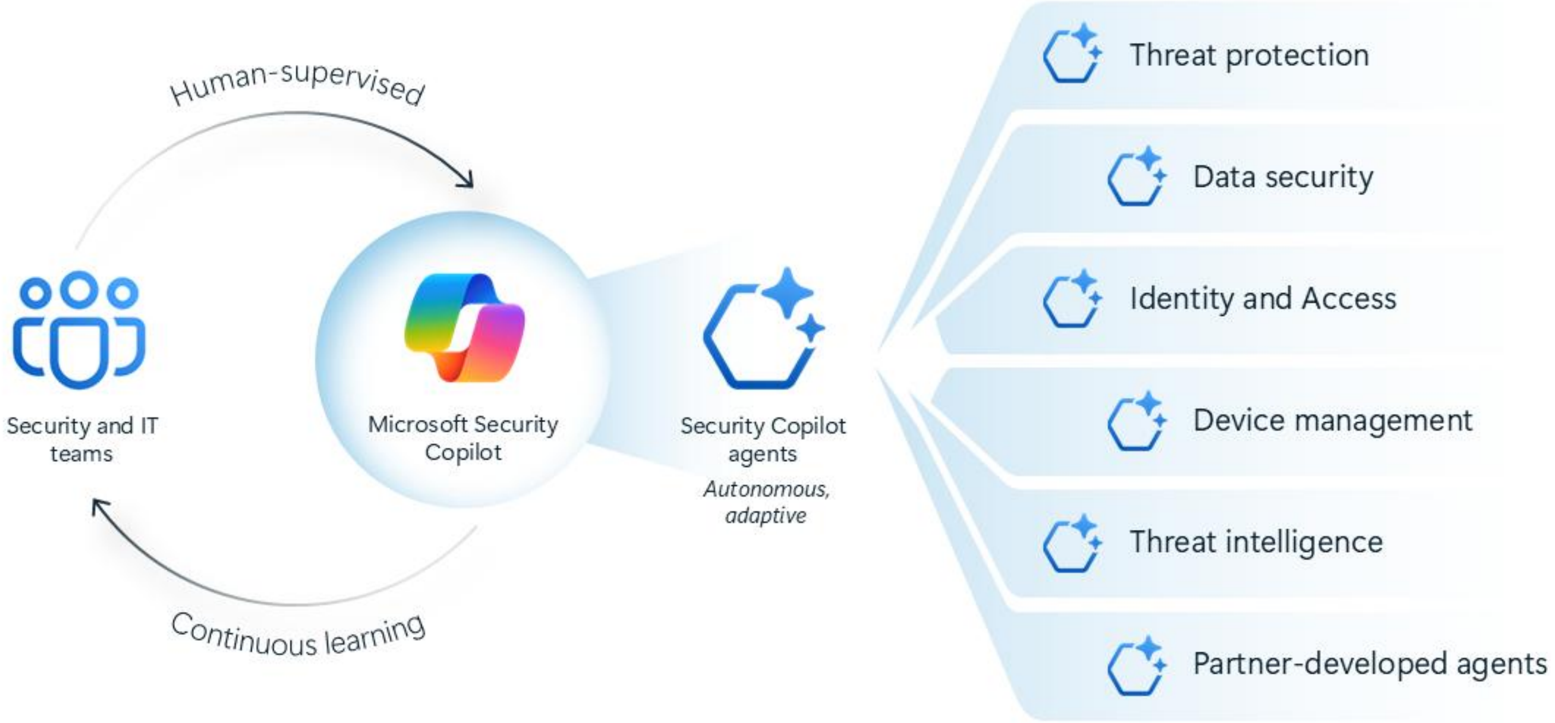
5 Copilot accesses plugins for post-processing

6 Copilot sends the response, and app command back to security products

Security Copilot AI Agent

Security Copilot Agents

- Microsoft Security Copilot agents automate repetitive tasks and reduce manual workloads
- These agents handle high-volume, time-consuming tasks by pairing data and code with an AI language model.
- Agents utilize SCUs to operate just like other features in the product.



Available Agent in Security Copilot

Microsoft Entra ID

Conditional Access Optimization Agent. 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

Microsoft Purview

These Data Loss Prevention(DLP) and Insider Risk Management (IRM) alert triage agents provide an agent-managed alert queue where the alerts about the highest risk activities are identified and prioritized.

Microsoft Defender XDR

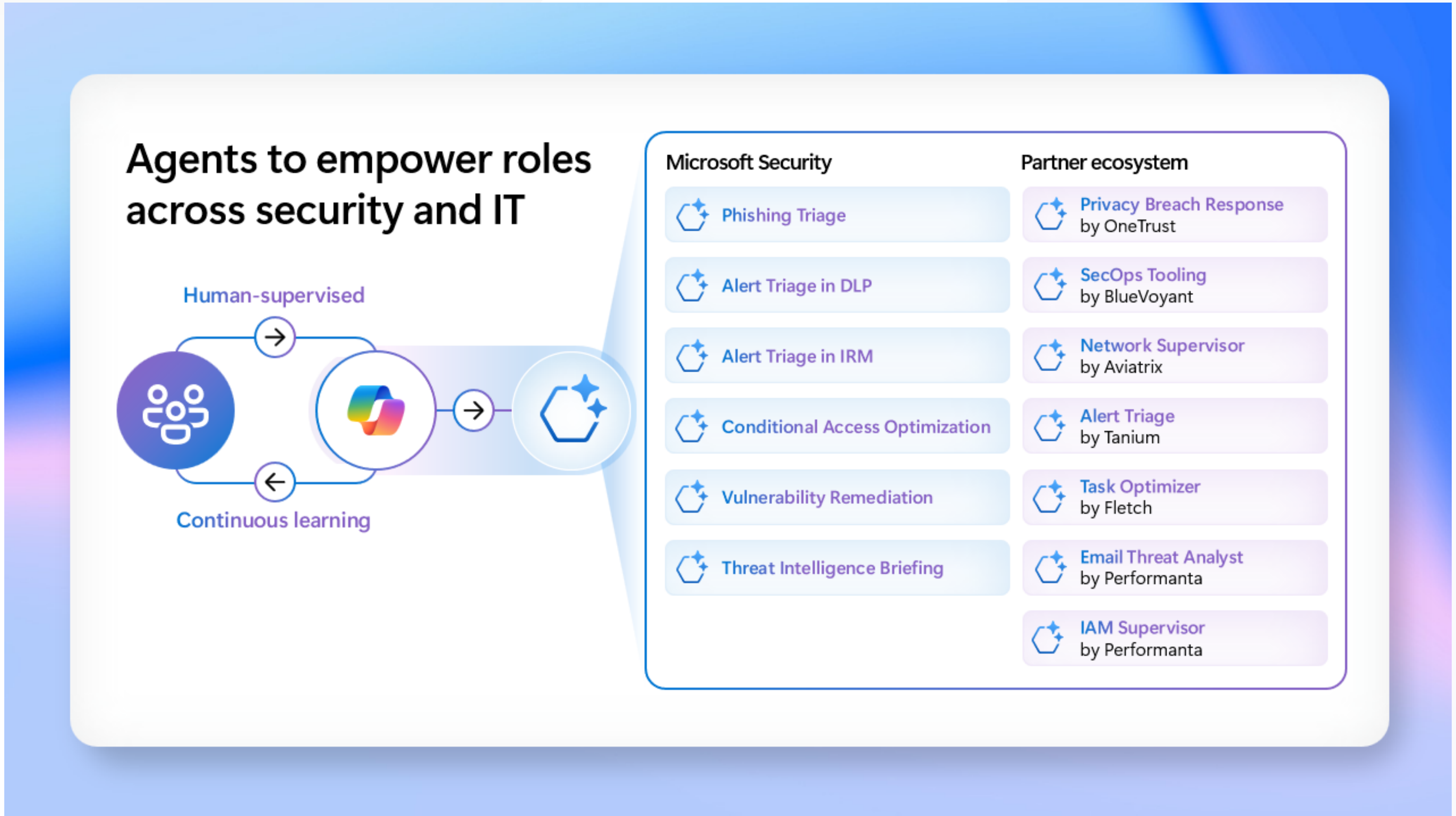
Designed to scale security teams' response in triaging and classifying user-submitted phishing incidents, allowing organizations to improve their efficiency by reducing manual effort and streamlining their phishing response.

Microsoft Intune

Identify top vulnerabilities, understand their impact, and get step-by-step remediation guidance to fix vulnerabilities using Intune capabilities.

Standalone experience - **Threat Intelligence Briefing** Agent in Security Copilot: generates threat intelligence briefings based on the latest threat actor activity

Partner ecosystem

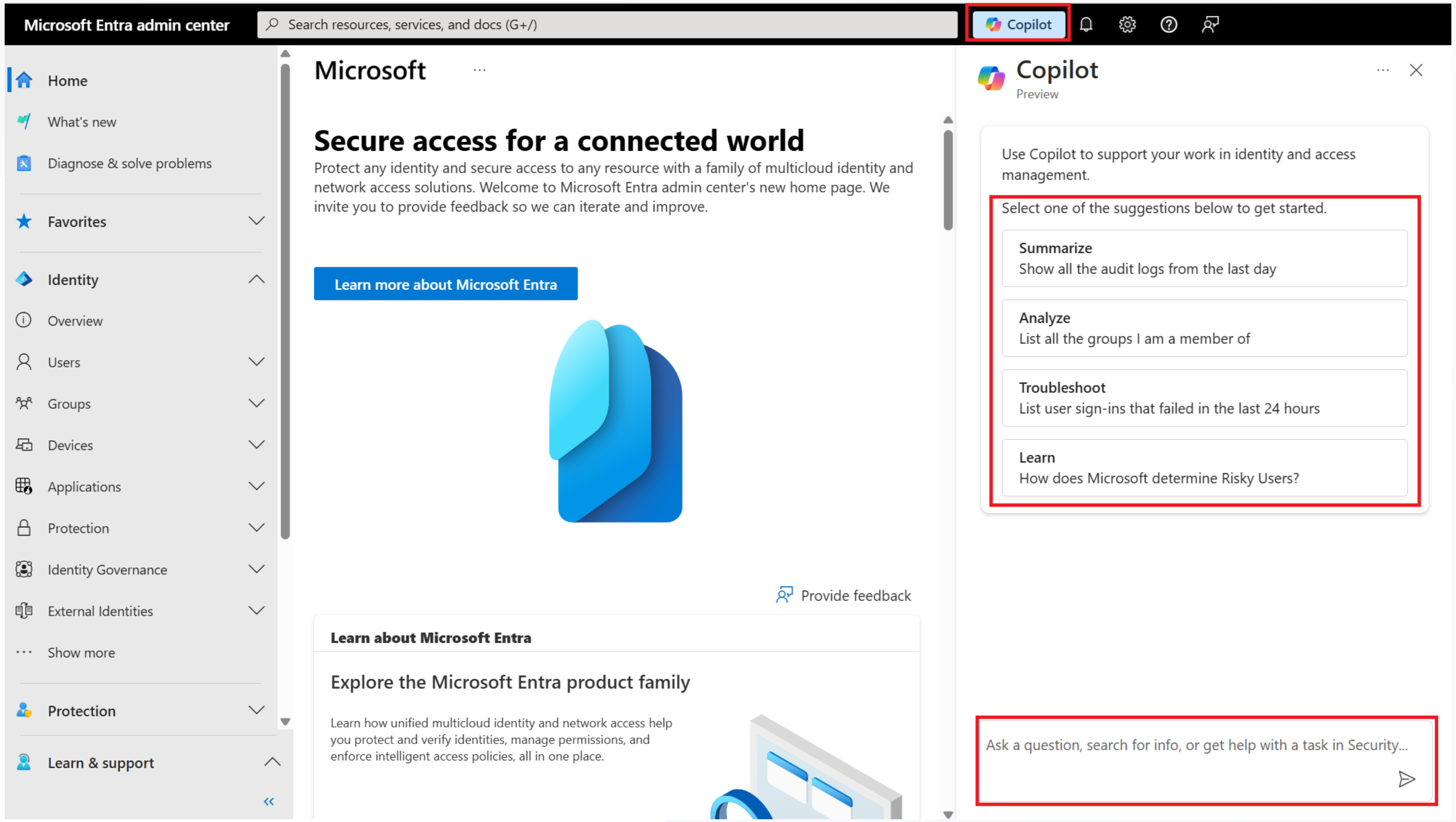


Agents to empower roles across security and IT

Microsoft Security	Partner ecosystem
Phishing Triage	Privacy Breach Response by OneTrust
Alert Triage in DLP	SecOps Tooling by BlueVoyant
Alert Triage in IRM	Network Supervisor by Aviatrix
Conditional Access Optimization	Alert Triage by Tanium
Vulnerability Remediation	Task Optimizer by Fletch
Threat Intelligence Briefing	Email Threat Analyst by Performanta
	IAM Supervisor by Performanta

Microsoft Security Copilot scenarios in Microsoft Entra

- Investigate recommendations
- Summarize a user's risk level
- Investigate access reviews
- Investigate insights within entitlements management
- Investigate alerts in Scenario Health Monitoring
- Microsoft Entra Role Based Access Control (RBAC)
- License Usage
- etc



Secure access for a connected world

Protect any identity and secure access to any resource with a family of multicloud identity and network access solutions. Welcome to Microsoft Entra admin center's new home page. We invite you to provide feedback so we can iterate and improve.

Learn about Microsoft Entra

Explore the Microsoft Entra product family

Learn how unified multicloud identity and network access help you protect and verify identities, manage permissions, and enforce intelligent access policies, all in one place.

Use Copilot to support your work in identity and access management.

Select one of the suggestions below to get started.

Summarize
Show all the audit logs from the last day

Analyze
List all the groups I am a member of

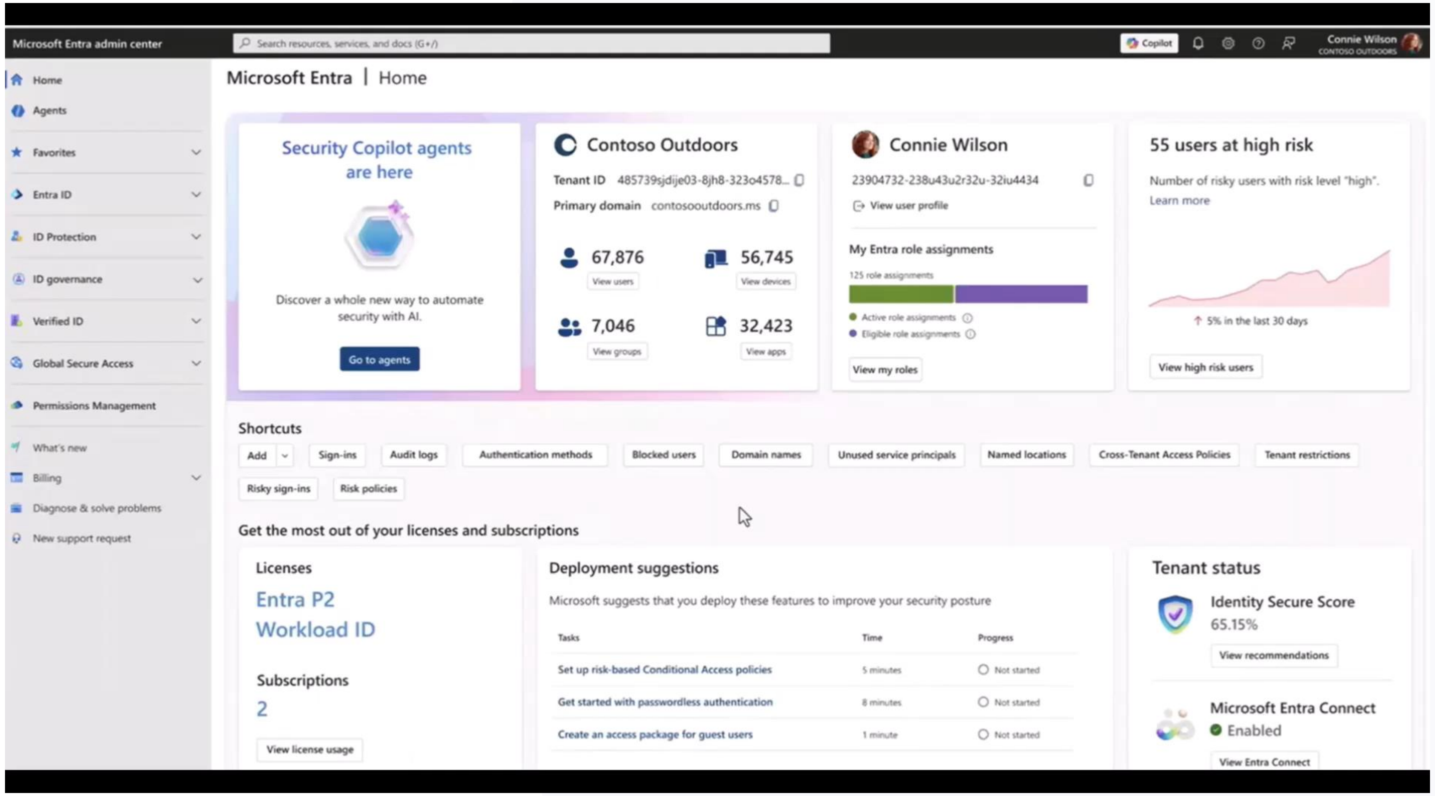
Troubleshoot
List user sign-ins that failed in the last 24 hours

Learn
How does Microsoft determine Risky Users?

Ask a question, search for info, or get help with a task in Security...

Microsoft Entra Conditional Access optimization agent

- The Conditional Access optimization agent ensures all users are protected by policy. It recommends policies and changes based on best practices aligned with Zero Trust and Microsoft's learnings. In preview, the agent evaluates policies requiring multifactor authentication (MFA), enforces device-based controls (device compliance, app protection policies, and Domain Joined Devices), and blocks legacy authentication and device code flow.
- The agent runs every 24 hours but can also run manually.
- It runs in the context of the administrator who configured the agent.



Discover a whole new way to automate security with AI.

Tenant ID 485739sjdije03-8jh8-323o4578...

Primary domain contosooutdoors.ms

23904732-238u43u2r32u-32iu4434

Number of risky users with risk level "high".

Get the most out of your licenses and subscriptions

Deployment suggestions

Microsoft suggests that you deploy these features to improve your security posture

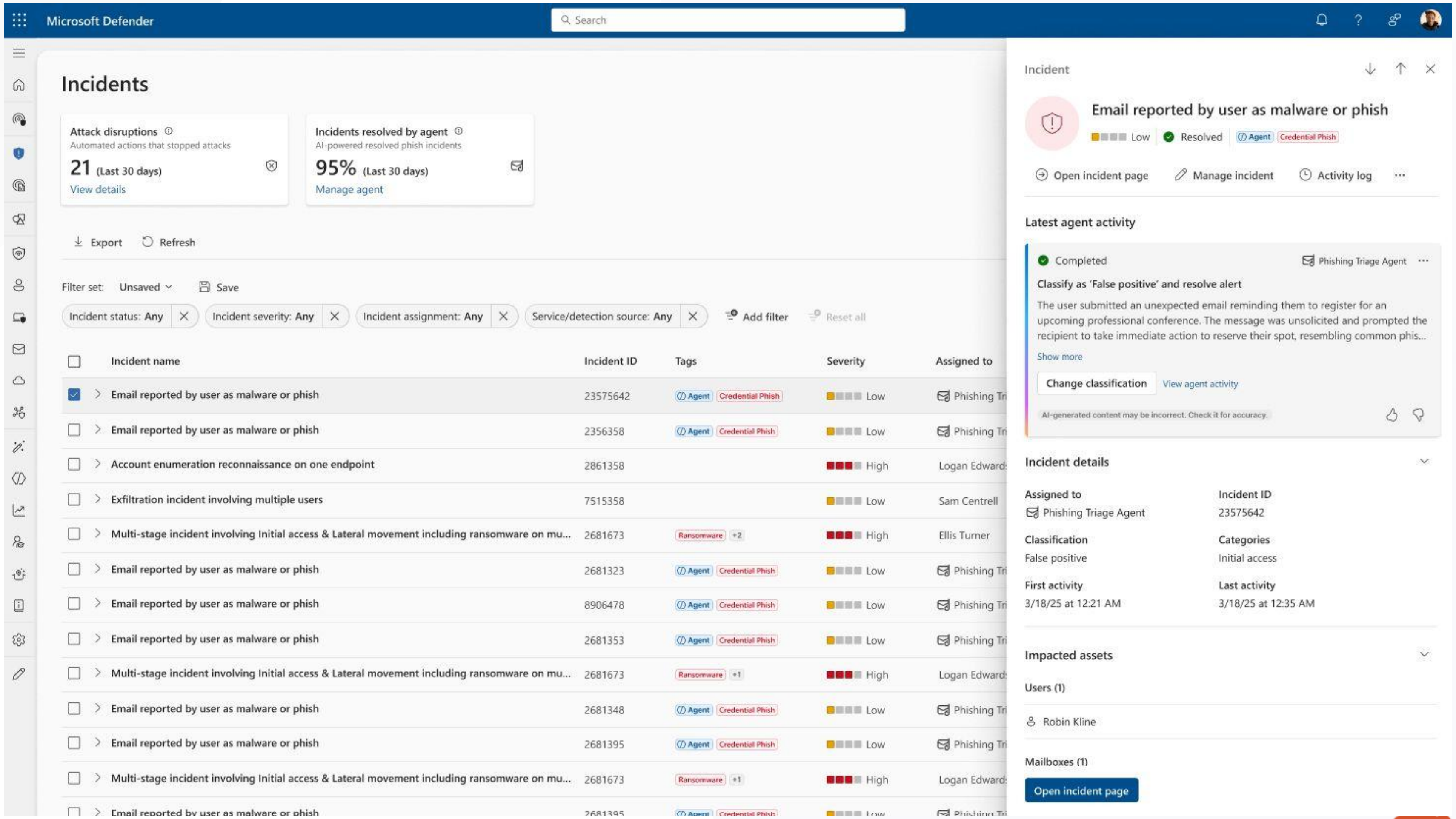
Tasks	Time	Progress
Set up risk-based Conditional Access policies	5 minutes	○ Not started
Get started with passwordless authentication	8 minutes	○ Not started
Create an access package for guest users	1 minute	○ Not started

Phishing remains one of the most persistent cybersecurity threats

- 91% of cyberattacks start with a phishing email, according to Microsoft Report
- Threat actors constantly refine their tactics: reviving old techniques or inventing new owns to bypass detection
- Attackers use creative phishing techniques to move faster, smarter and more persistently.
- New vectors:
  - QR code phishing
  - Collaborative tools as Teams
- In Microsoft 365 organizations with mailboxes in Exchange Online, users can report phishing and suspicious email in Outlook.
- SOC analyst are overwhelmed

Microsoft Security Copilot Phishing Triage Agent in Microsoft Defender

This AI-powered virtual agent is designed to scale security teams' response in **triaging and classifying user-submitted phishing incidents**, allowing organizations to improve their efficiency by reducing manual effort and streamlining their phishing response.



Microsoft Defender

Search

Incidents

Attack disruptions
Automated actions that stopped attacks
21 (Last 30 days)
View details

Incidents resolved by agent
AI-powered resolved phish incidents
95% (Last 30 days)
Manage agent

Export Refresh

Filter set: Unsaved Save

Incident status: Any ✕ Incident severity: Any ✕ Incident assignment: Any ✕ Service/detection source: Any ✕ Add filter Reset all

	Incident name	Incident ID	Tags	Severity	Assigned to
☑	Email reported by user as malware or phish	23575642	Agent Credential Phish	Low	Phishing Tri
□	Email reported by user as malware or phish	2356358	Agent Credential Phish	Low	Phishing Tri
□	Account enumeration reconnaissance on one endpoint	2861358		High	Logan Edwards
□	Exfiltration incident involving multiple users	7515358		Low	Sam Centrell
□	Multi-stage incident involving Initial access & Lateral movement including ransomware on mu...	2681673	Ransomware +2	High	Ellis Turner
□	Email reported by user as malware or phish	2681323	Agent Credential Phish	Low	Phishing Tri
□	Email reported by user as malware or phish	8906478	Agent Credential Phish	Low	Phishing Tri
□	Email reported by user as malware or phish	2681353	Agent Credential Phish	Low	Phishing Tri
□	Multi-stage incident involving Initial access & Lateral movement including ransomware on mu...	2681673	Ransomware +1	High	Logan Edwards
□	Email reported by user as malware or phish	2681348	Agent Credential Phish	Low	Phishing Tri
□	Email reported by user as malware or phish	2681395	Agent Credential Phish	Low	Phishing Tri
□	Multi-stage incident involving Initial access & Lateral movement including ransomware on mu...	2681673	Ransomware +1	High	Logan Edwards
□	Email reported by user as malware or phish	2681395	Agent Credential Phish	Low	Phishing Tri

Incident

Email reported by user as malware or phish
Low | Resolved | Agent Credential Phish

Open incident page Manage incident Activity log

Latest agent activity

Completed — Phishing Triage Agent

Classify as 'False positive' and resolve alert

The user submitted an unexpected email reminding them to register for an upcoming professional conference. The message was unsolicited and prompted the recipient to take immediate action to reserve their spot, resembling common phis...

Show more

Change classification View agent activity

AI-generated content may be incorrect. Check it for accuracy.

Incident details

Assigned to Phishing Triage Agent	Incident ID 23575642
Classification False positive	Categories Initial access
First activity 3/18/25 at 12:21 AM	Last activity 3/18/25 at 12:35 AM

Impacted assets

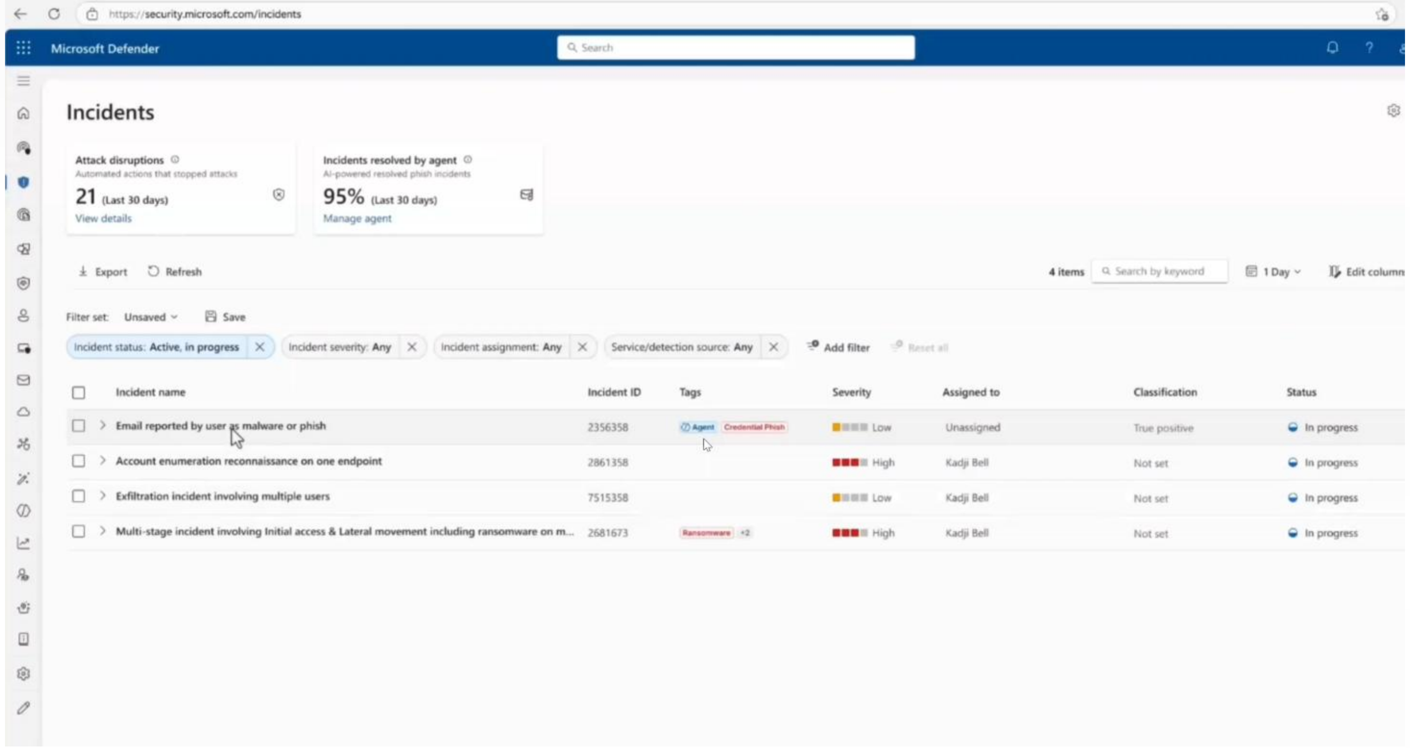
Users (1)

Robin Kline

Mailboxes (1)

Open incident page

Phishing Triage Agent in the Defender XDR Portal



https://security.microsoft.com/incidents

Incidents

Attack disruptions
Automated actions that stopped attacks
21 (Last 30 days)
View details

Incidents resolved by agent
AI-powered resolved phish incidents
95% (Last 30 days)
Manage agent

Incident status: Active, in progress ✕ | Incident severity: Any ✕ | Incident assignment: Any ✕ | Service/detection source: Any ✕

Incident name	Incident ID	Tags	Severity	Assigned to	Classification	Status
Email reported by user as malware or phish	2356358	Agent, Credential Phish	Low	Unassigned	True positive	In progress
Account enumeration reconnaissance on one endpoint	2861358		High	Kadji Bell	Not set	In progress
Exfiltration incident involving multiple users	7515358		Low	Kadji Bell	Not set	In progress
Multi-stage incident involving Initial access & Lateral movement including ransomware on m...	2681673	Ransomware +2	High	Kadji Bell	Not set	In progress

Autonomously triages phishing alerts

Leveraging generative AI, the agent perform advanced analyses to identify even the most sophisticated phishing attempts with high accuracy

Learn from feedback

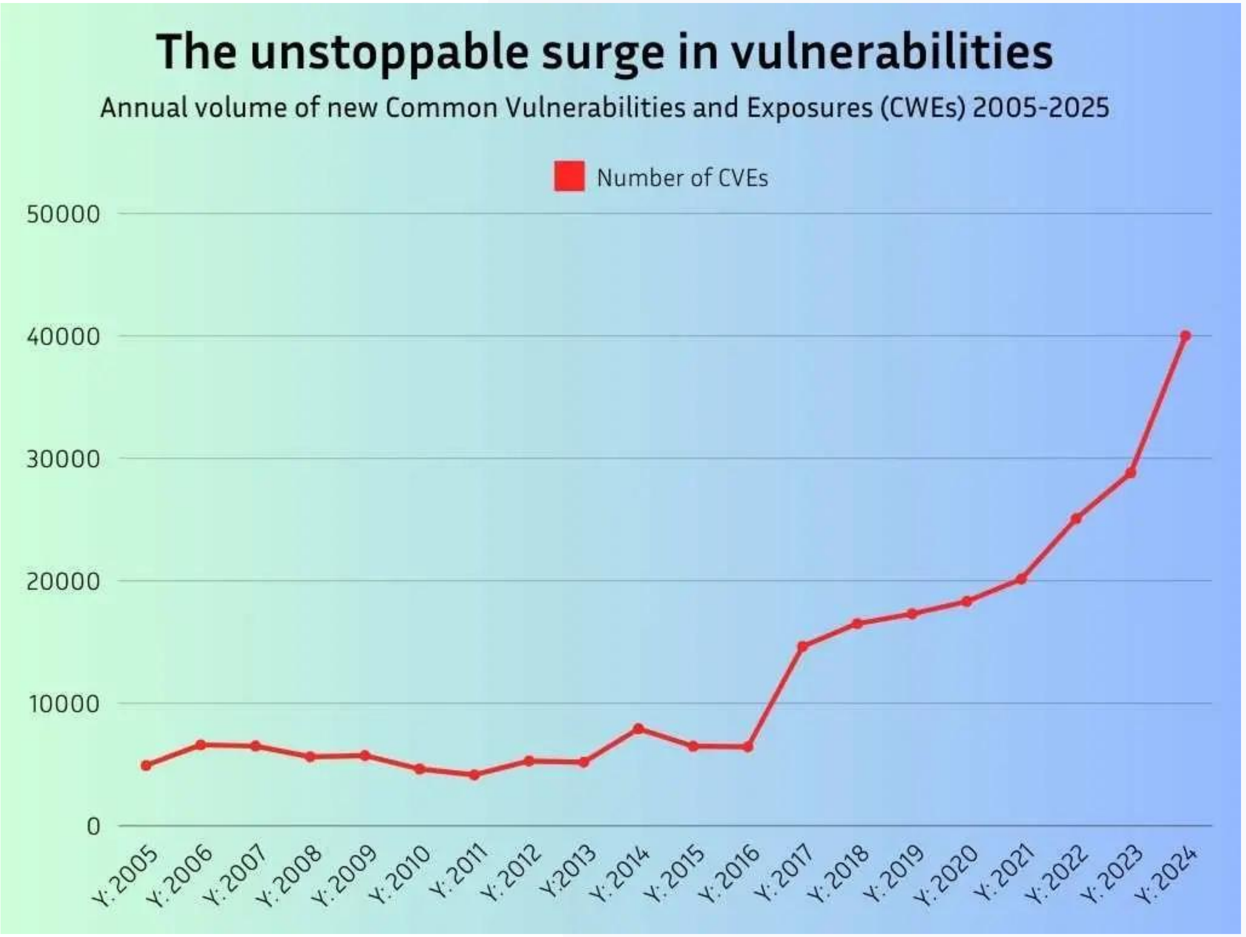
The agent learns and evolves its behavior through feedback provided by analysts in natural language, ensuring it becomes increasingly accurate and tailored to the organization's specific context

Transparency for verdicts

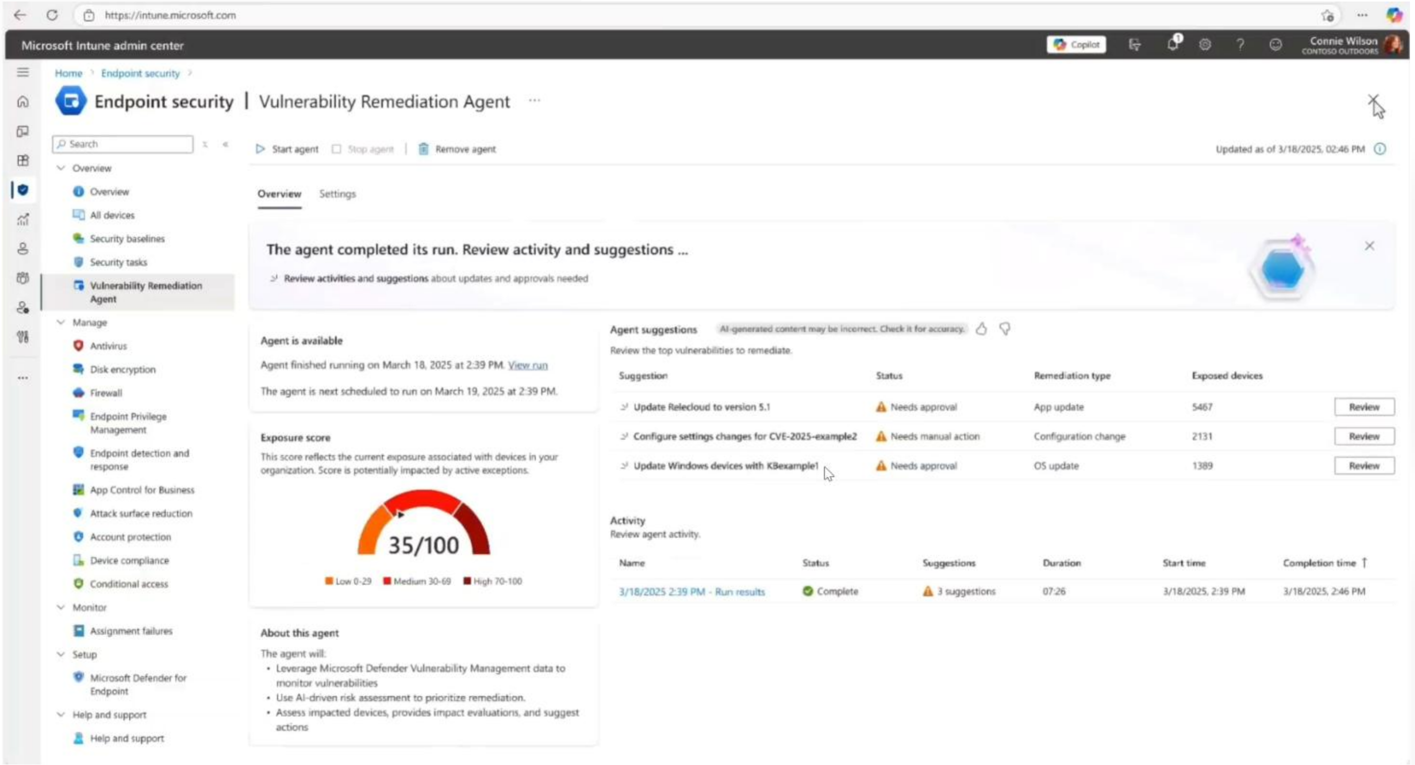
The agent offers full transparency in its decision-making, providing explanations for its verdicts in clear, natural language, as well as a flow diagram that visually outlines the steps taken to reach a conclusion

Threat actors are exploiting vulnerabilities faster than ever

- 40.000 common vulnerability and exposures were published in 2024
- Threat actors constantly exploiting vulnerabilities reviving old techniques or inventing new ones to bypass detection
- Time to exploit vulnerabilities is falling significantly



Intune Agent – Intelligent, end to end Vulnerability Remediation



The agent completed its run. Review activity and suggestions ...

Review activities and suggestions about updates and approvals needed

Agent is available

Agent finished running on March 18, 2025 at 2:39 PM. View run

The agent is next scheduled to run on March 19, 2025 at 2:39 PM.

Exposure score

This score reflects the current exposure associated with devices in your organization. Score is potentially impacted by active exceptions.

35/100

🟧 Low 0-29 🟥 Medium 30-69 🟥 High 70-100

About this agent

The agent will:
- Leverage Microsoft Defender Vulnerability Management data to monitor vulnerabilities
- Use AI-driven risk assessment to prioritize remediation.
- Assess impacted devices, provides impact evaluations, and suggest actions

Agent suggestions AI-generated content may be incorrect. Check it for accuracy.

Review the top vulnerabilities to remediate.

Suggestion	Status	Remediation type	Exposed devices	
Update Relecloud to version 5.1	⚠ Needs approval	App update	5467	Review
Configure settings changes for CVE-2025-example2	⚠ Needs manual action	Configuration change	2131	Review
Update Windows devices with KBexample1	⚠ Needs approval	OS update	1389	Review

Activity

Review agent activity.

Name	Status	Suggestions	Duration	Start time	Completion time ↑
3/18/2025 2:39 PM - Run results	✓ Complete	⚠ 3 suggestions	07:26	3/18/2025, 2:39 PM	3/18/2025, 2:46 PM

Discovery of vulnerability data

The agent analyzes vulnerability data from Microsoft Defender Vulnerability Management (MDVM) to help IT pros discover the vulnerabilities in their environment

AI generated analysis to streamline remediation

The agent priorities the remediation of high impact vulnerabilities by leveraging MDVM and Copilot for an impact analysis, providing explanations for its recommendations in clear natural language & offering full transparency in its decision making

Step by Step remediation guide

The agent provides a step-by-step remediation guide, equipping admins with both the critical insights needed to assess high-impact vulnerabilities and the actionable steps to take in Intune to resolve them

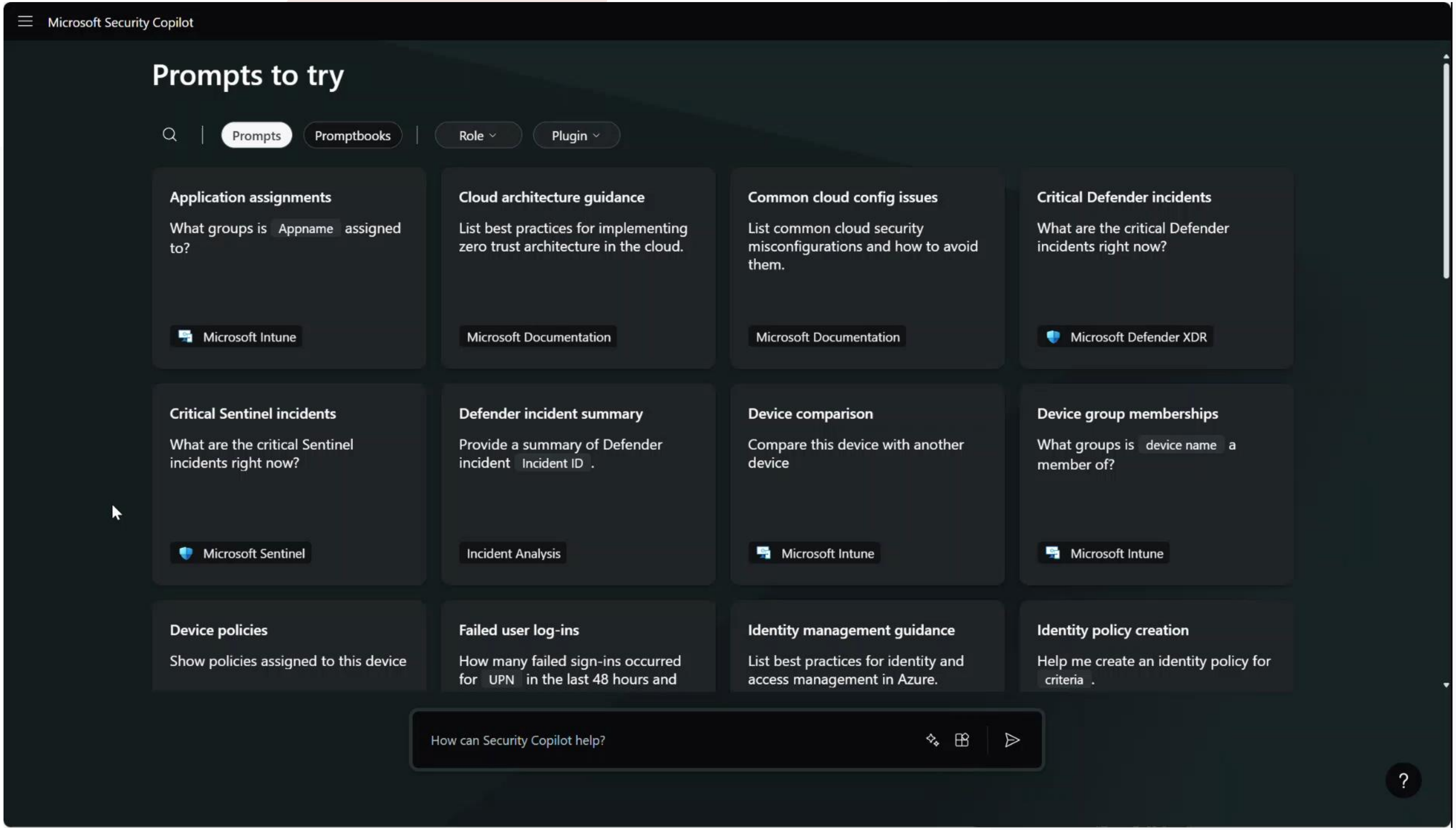
Alert triage in Microsoft Purview

The data loss prevention agent helps security teams by evaluating alerts based on the **sensitivity risk, exfiltration risk,** and **policy risk**. The agent then sorts the triaged alerts into four categories. These categories are presented in the DLP solution on the Alerts page.

- **All**: Which contains all alerts the agent is working on or has fully triaged.
- **Needs attention**: These are the alerts that the agent has triaged and determined that they should be assigned top priority in your review process.
- **Less urgent**: These are the alerts that the agent has triaged and determined that they should be assigned a lower priority in your review process.
- **Not triaged**: These are the alerts that the agent has yet to triage or the agent unsuccessfully attempted to triage.

Demo

Deploy Agent



Microsoft Security Copilot

Prompts to try

Application assignments
What groups is Appname assigned to?
Microsoft Intune

Cloud architecture guidance
List best practices for implementing zero trust architecture in the cloud.
Microsoft Documentation

Common cloud config issues
List common cloud security misconfigurations and how to avoid them.
Microsoft Documentation

Critical Defender incidents
What are the critical Defender incidents right now?
Microsoft Defender XDR

Critical Sentinel incidents
What are the critical Sentinel incidents right now?
Microsoft Sentinel

Defender incident summary
Provide a summary of Defender incident Incident ID .
Incident Analysis

Device comparison
Compare this device with another device
Microsoft Intune

Device group memberships
What groups is device name a member of?
Microsoft Intune

Device policies
Show policies assigned to this device

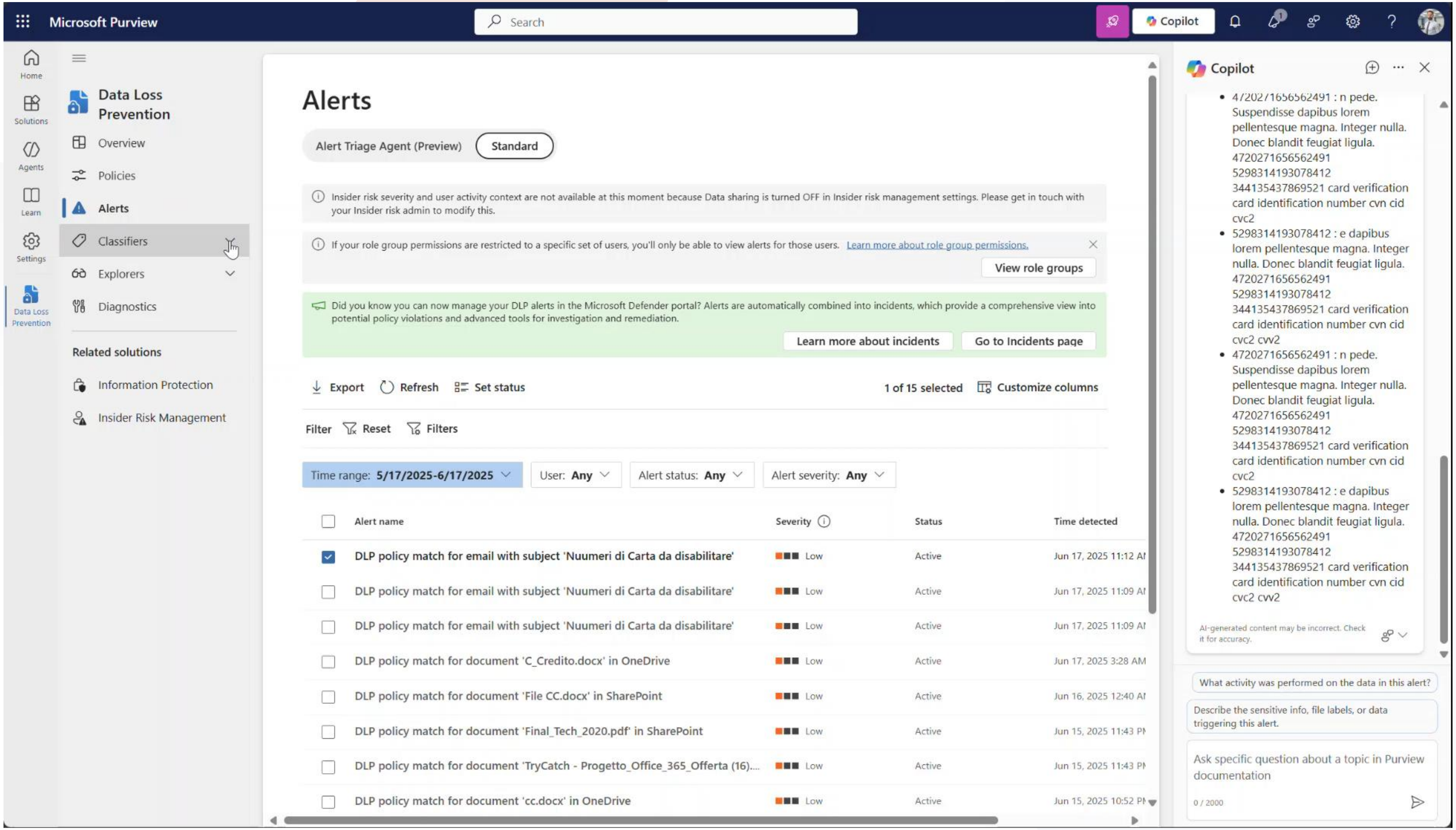
Failed user log-ins
How many failed sign-ins occurred for UPN in the last 48 hours and

Identity management guidance
List best practices for identity and access management in Azure.

Identity policy creation
Help me create an identity policy for criteria .

How can Security Copilot help?

Triage DLP Alert by Agent



Data Loss Prevention

Alerts

Alert Triage Agent (Preview) | Standard

Insider risk severity and user activity context are not available at this moment because Data sharing is turned OFF in Insider risk management settings. Please get in touch with your Insider risk admin to modify this.

If your role group permissions are restricted to a specific set of users, you'll only be able to view alerts for those users. Learn more about role group permissions.

View role groups

Did you know you can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically combined into incidents, which provide a comprehensive view into potential policy violations and advanced tools for investigation and remediation.

Learn more about incidents | Go to Incidents page

1 of 15 selected

Time range: **5/17/2025-6/17/2025** | User: **Any** | Alert status: **Any** | Alert severity: **Any**

	Alert name	Severity	Status	Time detected
☑	DLP policy match for email with subject 'Nuumeri di Carta da disabilitare'	■■■ Low	Active	Jun 17, 2025 11:12 A
□	DLP policy match for email with subject 'Nuumeri di Carta da disabilitare'	■■■ Low	Active	Jun 17, 2025 11:09 A
□	DLP policy match for email with subject 'Nuumeri di Carta da disabilitare'	■■■ Low	Active	Jun 17, 2025 11:09 A
□	DLP policy match for document 'C_Credito.docx' in OneDrive	■■■ Low	Active	Jun 17, 2025 3:28 AM
□	DLP policy match for document 'File CC.docx' in SharePoint	■■■ Low	Active	Jun 16, 2025 12:40 A
□	DLP policy match for document 'Final_Tech_2020.pdf' in SharePoint	■■■ Low	Active	Jun 15, 2025 11:43 P
□	DLP policy match for document 'TryCatch - Progetto_Office_365_Offerta (16)....	■■■ Low	Active	Jun 15, 2025 11:43 P
□	DLP policy match for document 'cc.docx' in OneDrive	■■■ Low	Active	Jun 15, 2025 10:52 P

Copilot

- 4720271656562491 : n pede. Suspendisse dapibus lorem pellentesque magna. Integer nulla. Donec blandit feugiat ligula. 4720271656562491 5298314193078412 344135437869521 card verification card identification number cvn cid cvc2
- 5298314193078412 : e dapibus lorem pellentesque magna. Integer nulla. Donec blandit feugiat ligula. 4720271656562491 5298314193078412 344135437869521 card verification card identification number cvn cid cvc2 cvv2
- 4720271656562491 : n pede. Suspendisse dapibus lorem pellentesque magna. Integer nulla. Donec blandit feugiat ligula. 4720271656562491 5298314193078412 344135437869521 card verification card identification number cvn cid cvc2
- 5298314193078412 : e dapibus lorem pellentesque magna. Integer nulla. Donec blandit feugiat ligula. 4720271656562491 5298314193078412 344135437869521 card verification card identification number cvn cid cvc2 cvv2

AI-generated content may be incorrect. Check it for accuracy.

What activity was performed on the data in this alert?

Describe the sensitive info, file labels, or data triggering this alert.

Ask specific question about a topic in Purview documentation

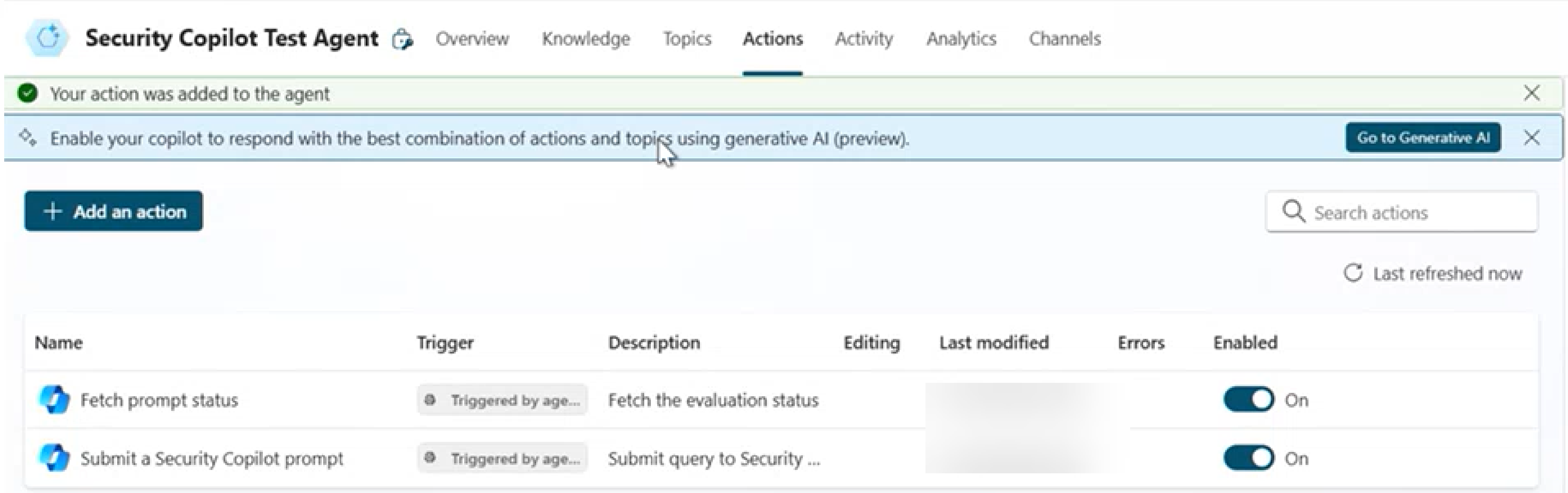
0 / 2000

Microsoft Security Copilot - Copilot Studio connector

The Copilot Studio connector enables you to access Security Copilot

The connector exposes the following connector actions:

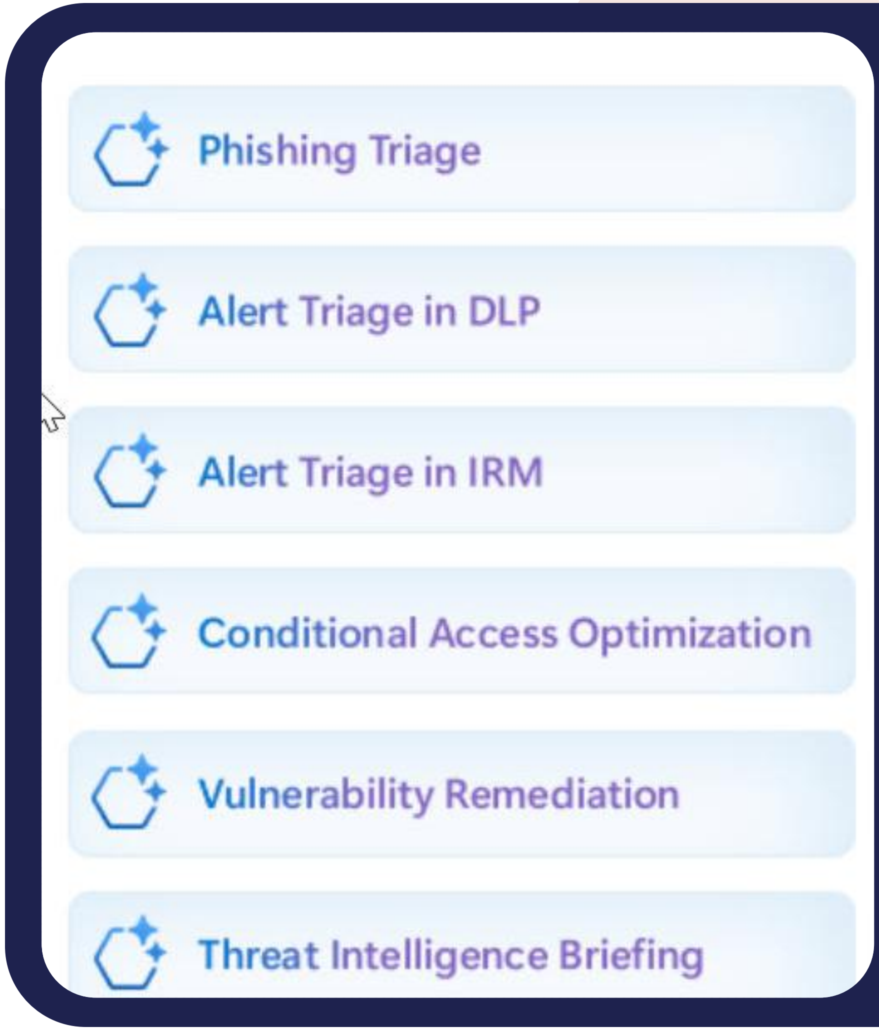
- **Submit a Security Copilot prompt** - Submit a natural language prompt to create a new Security Copilot investigation. After completion, the evaluation result will then be returned to your workflow.
- **Fetch a Security Copilot prompt status** - Submit a natural language prompt to pull the status of a Security Copilot evaluation. After completion, the evaluation result will then be returned to your workflow.



Your action was added to the agent

Enable your copilot to respond with the best combination of actions and topics using generative AI (preview).

Name	Trigger	Description	Editing	Last modified	Errors	Enabled
Fetch prompt status	Triggered by age...	Fetch the evaluation status		[redacted]		On
Submit a Security Copilot prompt	Triggered by age...	Submit query to Security ...		[redacted]		On



- Phishing Triage
- Alert Triage in DLP
- Alert Triage in IRM
- Conditional Access Optimization
- Vulnerability Remediation
- Threat Intelligence Briefing

Grazie!

Q&A