Microsoft Security

ATEA Security Days

Sikkerhed mod Cybertrusler i en AI-drevet verden

Nikolaj Laursen
Security Technology Specialist

Threats aren't slowing down. Attackers use AI to move faster, smarter

67% of all phishing attacks utilized some form of AI [1]

66 data security alerts faced by organizations per day, up from 52 in 2023 [2]

73% of cybersecurity experts admit they have missed, ignored, or failed to respond to high-priority security alerts [3]

→

Defenders need AI that can do even more for them

AI allows for a paradigm shift

Exponential gains in human expertise and efficiency to **defend at machine speed and scale**

Reactive → Proactive

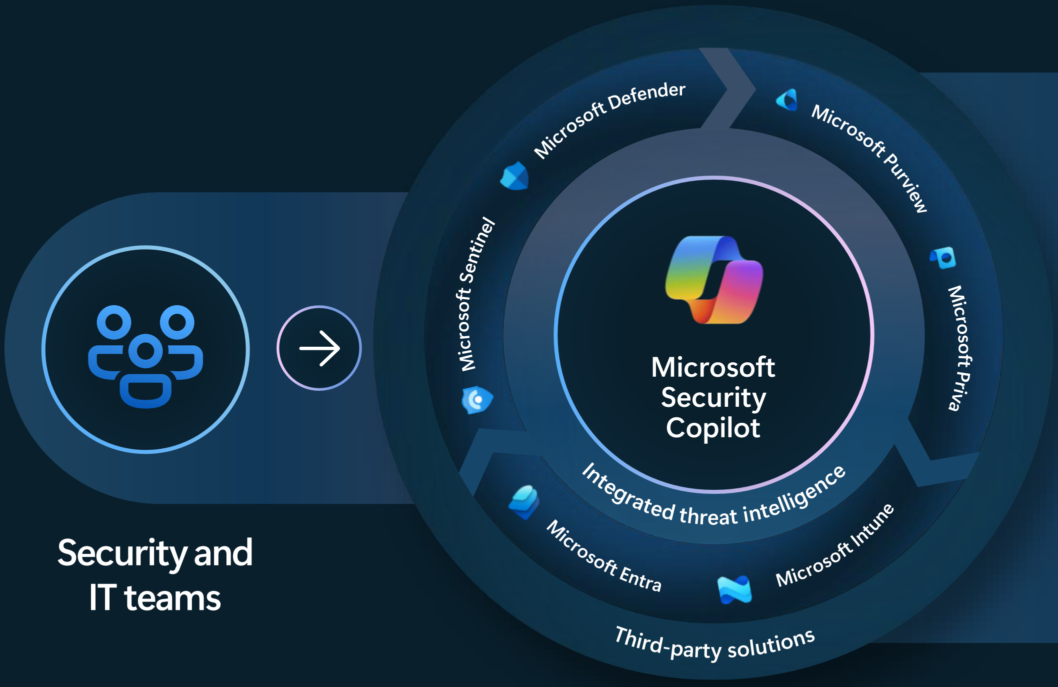
Siloed → Integrated

Static → Dynamic

Manual → Automated

Security Copilot is built to solve these challenges

A generative AI-powered assistant for daily operations in security and IT
that empowers teams to protect at the speed and scale of AI



Security and IT teams

Microsoft Security Copilot

Integrated threat intelligence

Microsoft Defender

Microsoft Purview

Microsoft Priva

Microsoft Intune

Microsoft Entra

Microsoft Sentinel

Third-party solutions

for many use cases like:

- Security investigation and remediation
- Building and reverse engineering scripts
- Risk exploration and posture management
- Troubleshooting IT issues
- Policy creation and management

Enhance security and IT operations

Security operations

CISO

- ✓ Get executive summary and detailed reporting

SOC analyst

- ✓ Accelerate investigation and remediation
- ✓ Reverse engineer malicious scripts

Threat intelligence (TI) analyst

- ✓ Enrich analysis with unified TI
- ✓ Accelerate threat hunting

Beyond the SOC

Data security admin

- ✓ Proactive data security posture management
- ✓ Discover protection gaps and streamline controls

IT admin

- ✓ Risk investigation
- ✓ Accelerate IT troubleshooting

Identity admin

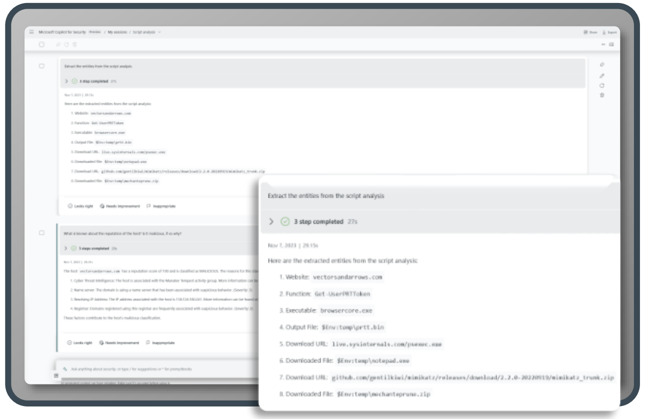
- ✓ Sign-in and risky user exploration
- ✓ Lifecycle workflow management

← Autonomous AI agents to automate tasks across your security and IT teams →

Security Copilot enhancements

Standalone

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot itself, with many use cases in one place, enabling enriched cross-product guidance



Extract the entities from the script analysis

3 step completed 27s

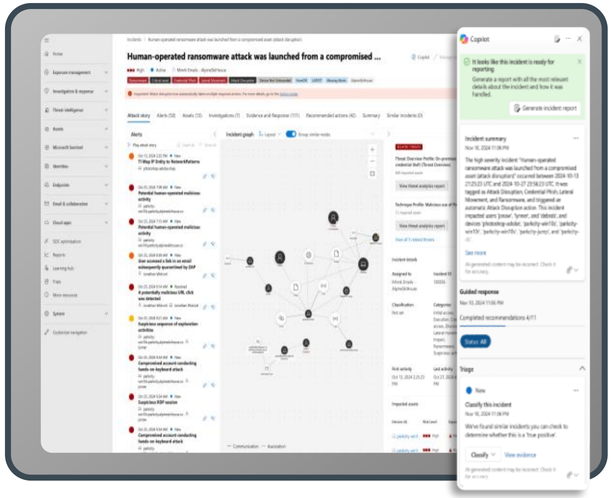
Nov 7, 2023 | 29.15s

Here are the extracted entities from the script analysis:

1. Website: `vectorsandarrows.com`
2. Function: `Get-UserPRTToken`
3. Executable: `browsercore.exe`
4. Output File: `$Env:temp\prtt.bin`
5. Download URL: `live.sysinternals.com/psexec.exe`
6. Downloaded File: `$Env:temp\notepad.exe`
7. Download URL: `github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip`
8. Downloaded File: `$Env:temp\mechanteprune.zip`

Embedded

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already work from and are familiar with



Human-operated ransomware attack was launched from a compromised ...

Copilot

It looks like this incident is ready for reporting

Generate a report with all the most relevant details about the incident and how it was handled.

Generate incident report

Incident summary

Nov 10, 2024 11:06 PM

The high severity incident "Human-operated ransomware attack was launched from a compromised asset (attack disruption)" occurred between 2024-10-13 21:25:23 UTC and 2024-10-27 23:56:23 UTC. It was tagged as Attack Disruption, Credential Phish, Lateral Movement, and Ransomware, and triggered an automatic Attack Disruption action. This incident impacted users 'jonaw', 'lyneer', and 'debrab', and devices 'photoshop-adobe', 'parkcity-win10s', 'parkcity-win10r', 'parkcity-win10v', 'parkcity-jump', and 'parkcity-dc'.

See more

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

Guided response

Nov 10, 2024 11:06 PM

Completed recommendations 4/11

Status: All

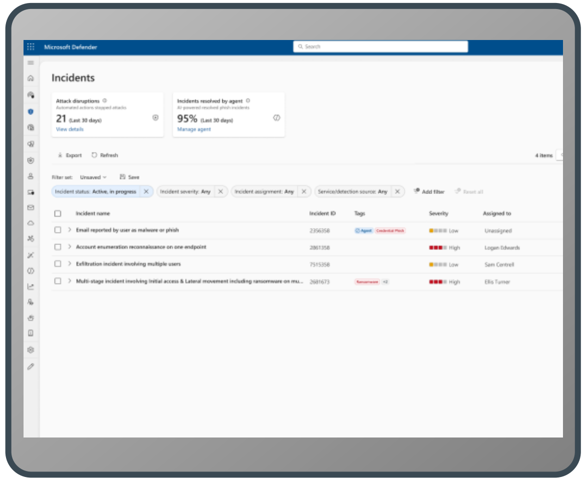
Triage

New

Classify this incident

Automation and agents

Helps teams accelerate response with built-in agents and custom promptbooks as well as integration with Logic Apps



Microsoft Defender

Incidents

Attack disruptions
Automated actions 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 4 items

Filter set: Unsaved Save

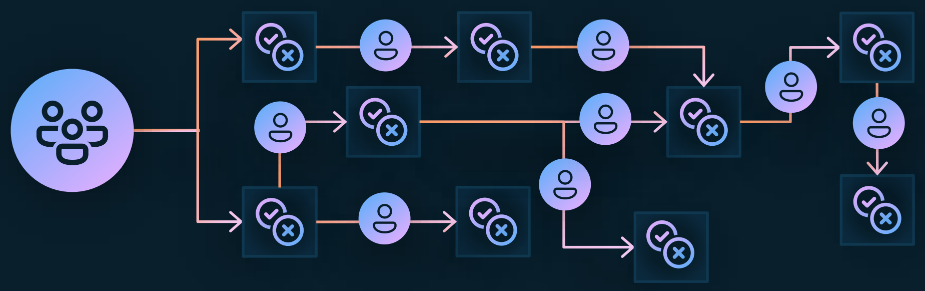
Incident status: Active, in progress | Incident severity: Any | Incident assignment: Any | Service/detection source: Any | Add filter | Reset all

Incident name	Incident ID	Tags	Severity	Assigned to
Email reported by user as malware or phish	2356358	Agent Credential Phish	Low	Unassigned
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

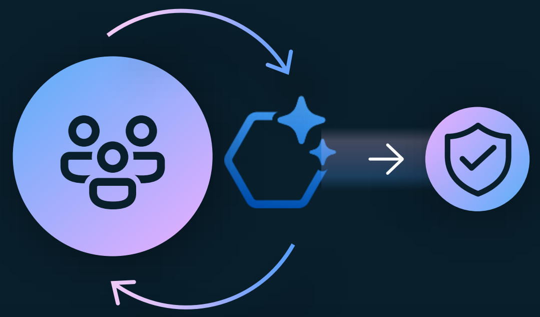
Security Copilot platform

Agents go further than traditional automation

Traditional automation

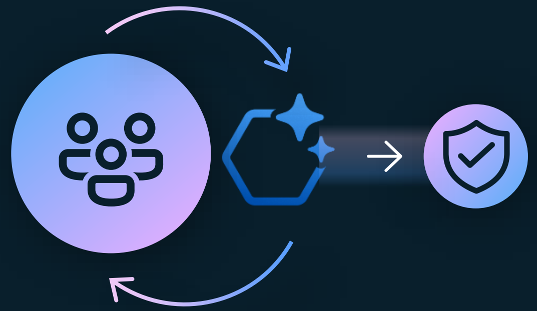


Agentic AI

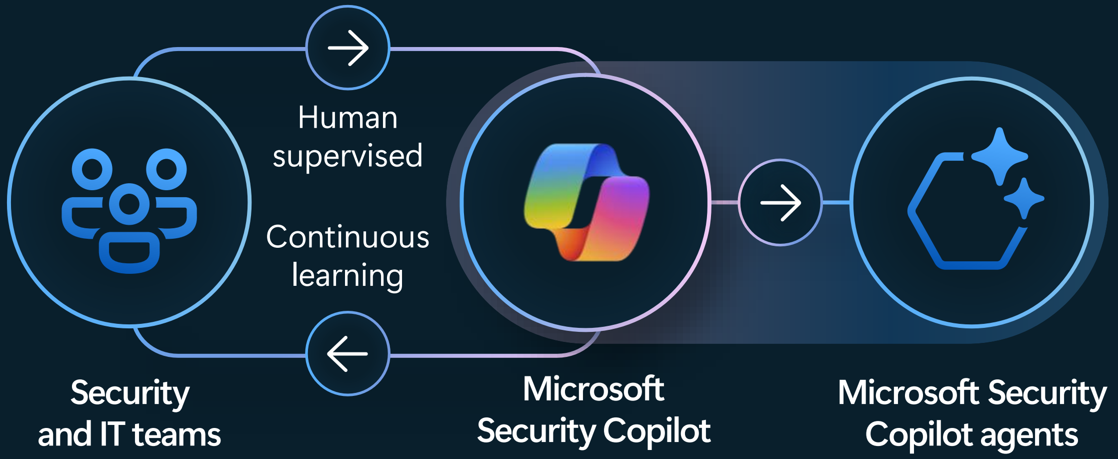


Rigid	→	Adaptive
Static	→	Dynamic
Manual updates	→	Continuous learning
Pre-defined	→	Context-aware
Easily broken	→	Highly resilient

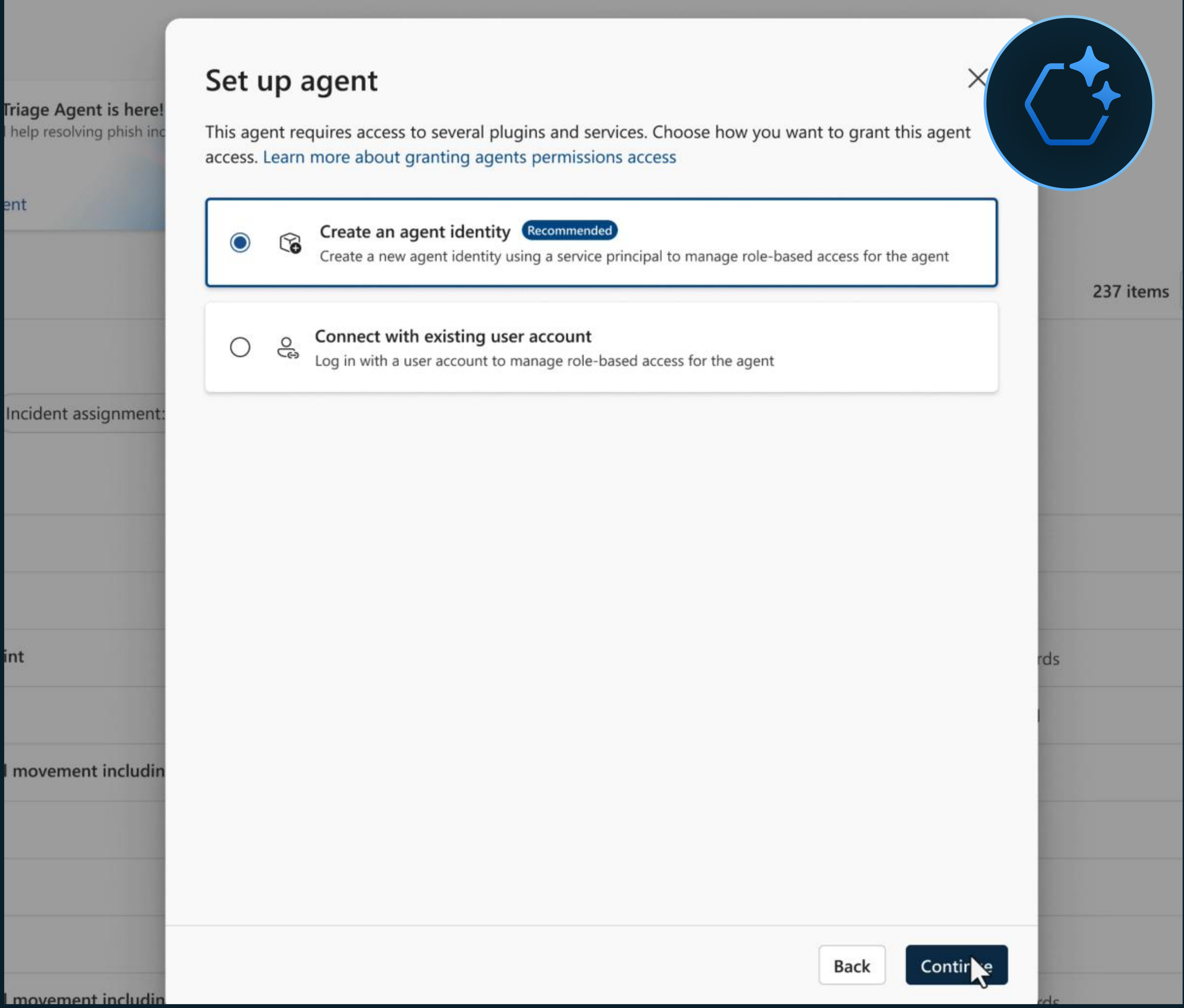
Agentic AI



But What Makes the Agents Unique?



Configure the Agent with its own Identity



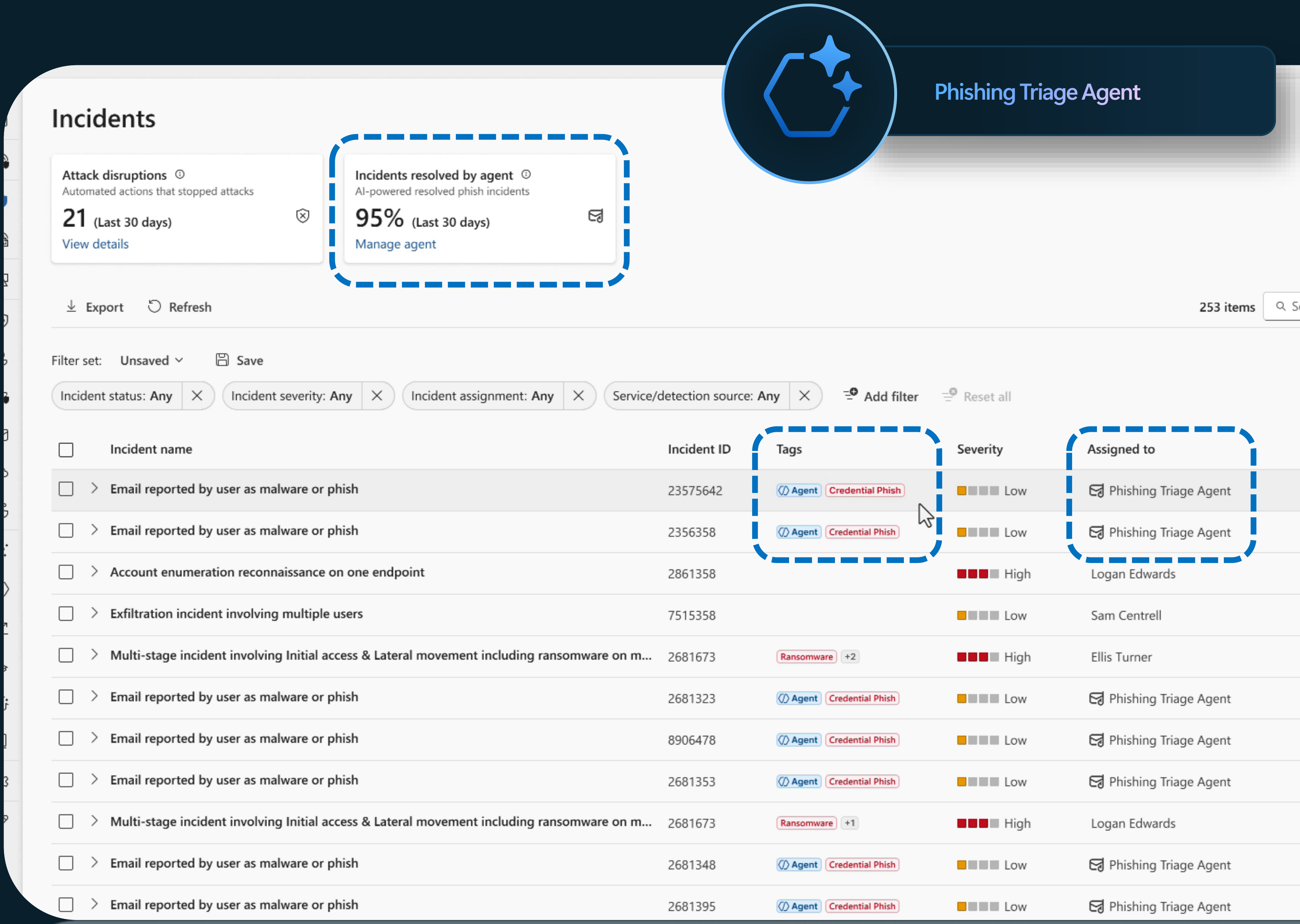
Set up agent

This agent requires access to several plugins and services. Choose how you want to grant this agent access. Learn more about granting agents permissions access

● **Create an agent identity** Recommended
Create a new agent identity using a service principal to manage role-based access for the agent

○ **Connect with existing user account**
Log in with a user account to manage role-based access for the agent

Incidents Proactively Resolved by Agent



Incidents

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

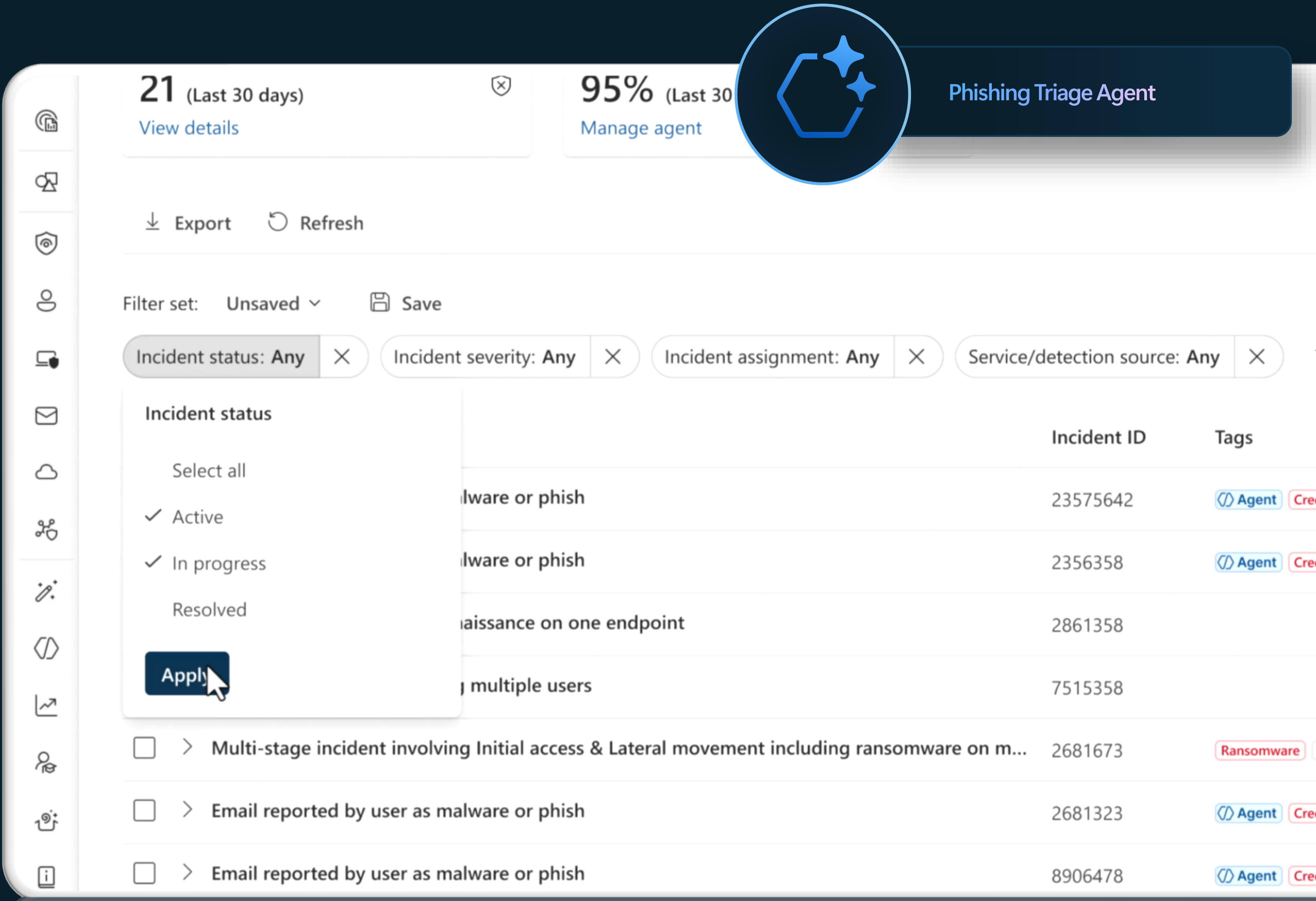
Incidents resolved by agent
AI-powered resolved phish incidents
95% (Last 30 days)
Manage agent

Filter set: Unsaved

Incident status: Any | Incident severity: Any | Incident assignment: Any | Service/detection source: Any

Incident name	Incident ID	Tags	Severity	Assigned to
Email reported by user as malware or phish	23575642	Agent Credential Phish	Low	Phishing Triage Agent
Email reported by user as malware or phish	2356358	Agent Credential Phish	Low	Phishing Triage Agent
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 m...	2681673	Ransomware +2	High	Ellis Turner
Email reported by user as malware or phish	2681323	Agent Credential Phish	Low	Phishing Triage Agent
Email reported by user as malware or phish	8906478	Agent Credential Phish	Low	Phishing Triage Agent
Email reported by user as malware or phish	2681353	Agent Credential Phish	Low	Phishing Triage Agent
Multi-stage incident involving Initial access & Lateral movement including ransomware on m...	2681673	Ransomware +1	High	Logan Edwards
Email reported by user as malware or phish	2681348	Agent Credential Phish	Low	Phishing Triage Agent
Email reported by user as malware or phish	2681395	Agent Credential Phish	Low	Phishing Triage Agent

Remove the Noise



Phishing Triage Agent

21 (Last 30 days)
View details

95% (Last 30
Manage agent

Export Refresh

Filter set: Unsaved ⌄ Save

Incident status: **Any** ✕ | Incident severity: **Any** ✕ | Incident assignment: **Any** ✕ | Service/detection source: **Any** ✕

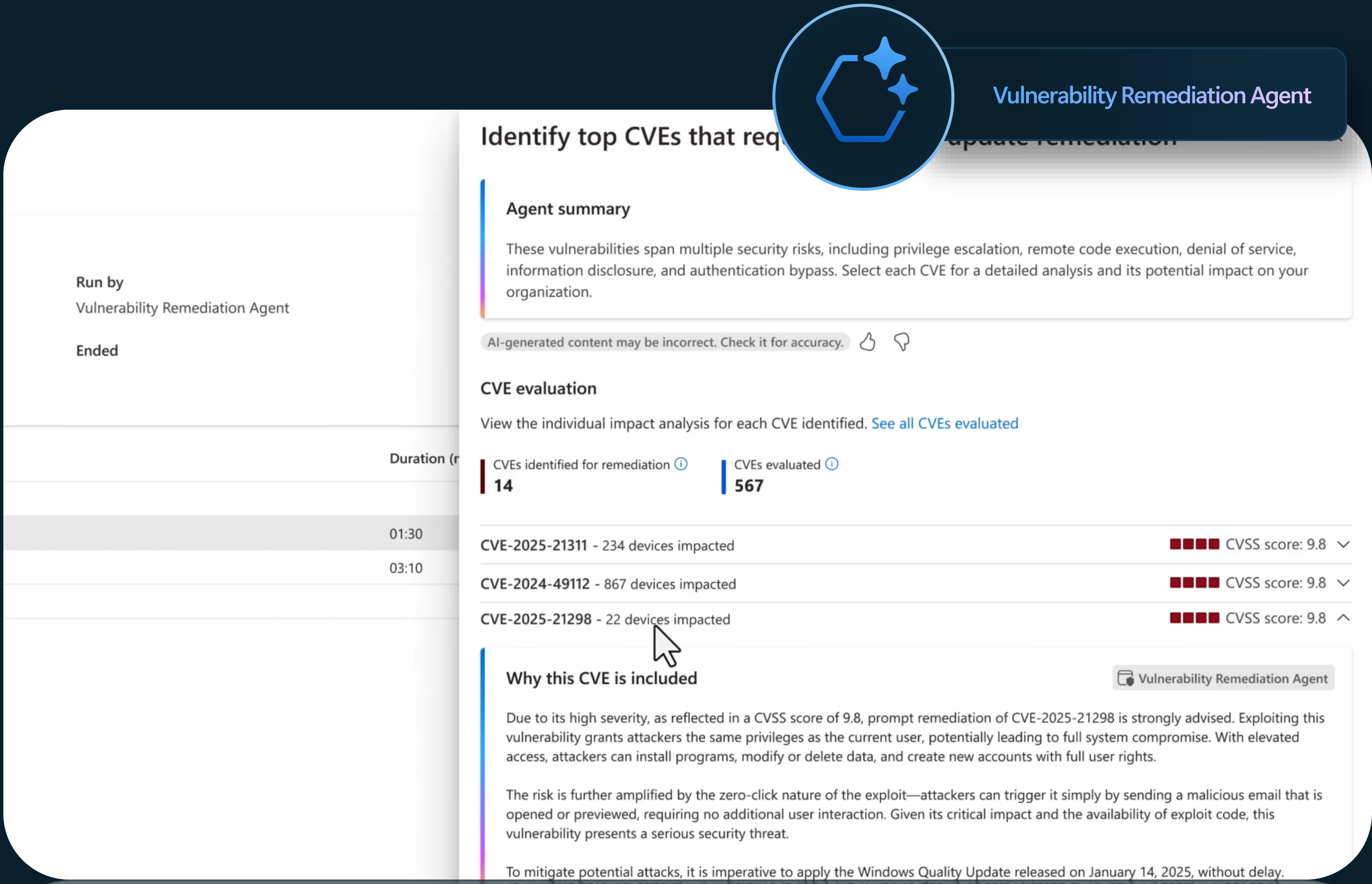
Incident status

Select all
✓ Active
✓ In progress
Resolved

Apply

	Incident ID	Tags
lware or phish	23575642	Agent Cre
lware or phish	2356358	Agent Cre
aissance on one endpoint	2861358	
multiple users	7515358	
□ › Multi-stage incident involving Initial access & Lateral movement including ransomware on m...	2681673	Ransomware
□ › Email reported by user as malware or phish	2681323	Agent Cre
□ › Email reported by user as malware or phish	8906478	Agent Cre

Get rich context writing in Natural Language



Vulnerability Remediation Agent

Run by
Vulnerability Remediation Agent

Ended

Duration (r
01:30
03:10

Identify top CVEs that req

update remediation

Agent summary

These vulnerabilities span multiple security risks, including privilege escalation, remote code execution, denial of service, information disclosure, and authentication bypass. Select each CVE for a detailed analysis and its potential impact on your organization.

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

CVE evaluation

View the individual impact analysis for each CVE identified. See all CVEs evaluated

CVEs identified for remediation	CVEs evaluated
14	567

CVE-2025-21311 - 234 devices impacted	CVSS score: 9.8
CVE-2024-49112 - 867 devices impacted	CVSS score: 9.8
CVE-2025-21298 - 22 devices impacted	CVSS score: 9.8

Why this CVE is included

Vulnerability Remediation Agent

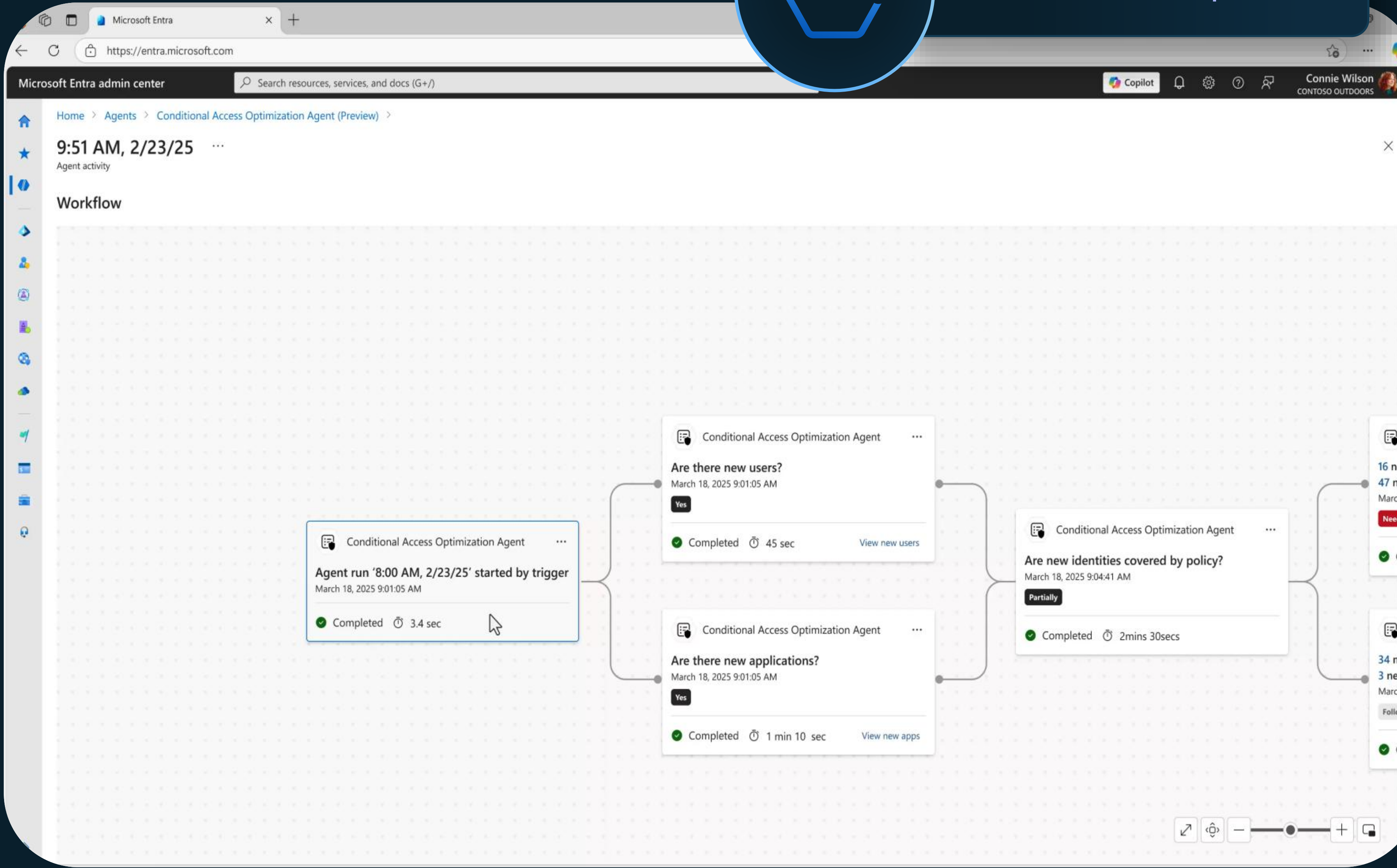
Due to its high severity, as reflected in a CVSS score of 9.8, prompt remediation of CVE-2025-21298 is strongly advised. Exploiting this vulnerability grants attackers the same privileges as the current user, potentially leading to full system compromise. With elevated access, attackers can install programs, modify or delete data, and create new accounts with full user rights.

The risk is further amplified by the zero-click nature of the exploit—attackers can trigger it simply by sending a malicious email that is opened or previewed, requiring no additional user interaction. Given its critical impact and the availability of exploit code, this vulnerability presents a serious security threat.

To mitigate potential attacks, it is imperative to apply the Windows Quality Update released on January 14, 2025, without delay.

Conditional Access Optimization

Full Transparency, Collection and Reasoning Behind the Decision



Microsoft Entra

https://entra.microsoft.com

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Connie Wilson
CONTOSO OUTDOORS

Home > Agents > Conditional Access Optimization Agent (Preview) >

9:51 AM, 2/23/25 ···
Agent activity

Workflow

Conditional Access Optimization Agent ···
Agent run '8:00 AM, 2/23/25' started by trigger
March 18, 2025 9:01:05 AM
Completed 3.4 sec

Conditional Access Optimization Agent ···
Are there new users?
March 18, 2025 9:01:05 AM
Yes
Completed 45 sec View new users

Conditional Access Optimization Agent ···
Are there new applications?
March 18, 2025 9:01:05 AM
Yes
Completed 1 min 10 sec View new apps

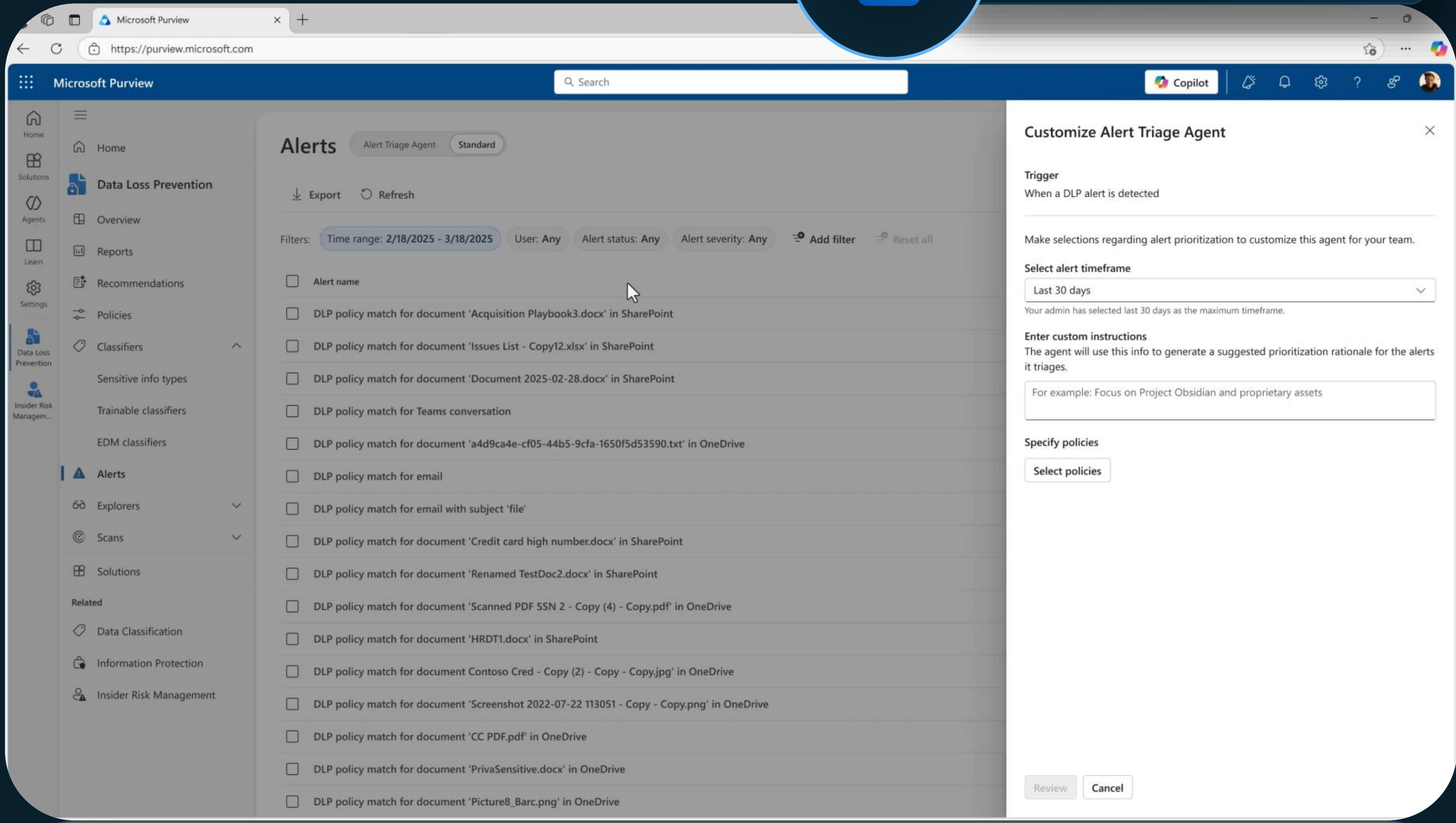
Conditional Access Optimization Agent ···
Are new identities covered by policy?
March 18, 2025 9:04:41 AM
Partially
Completed 2mins 30secs

16 n
47 n
Marc
Nee

34 n
3 ne
Marc
Foll

Customize and Train Your Agent by providing Instructions and Feedback

Alert Triage in DLP and IRM



Alerts

Alert Triage Agent | Standard

Export | Refresh

Filters: Time range: 2/18/2025 - 3/18/2025 | User: Any | Alert status: Any | Alert severity: Any | Add filter | Reset all

	Alert name
□	DLP policy match for document 'Acquisition Playbook3.docx' in SharePoint
□	DLP policy match for document 'Issues List - Copy12.xlsx' in SharePoint
□	DLP policy match for document 'Document 2025-02-28.docx' in SharePoint
□	DLP policy match for Teams conversation
□	DLP policy match for document 'a4d9ca4e-cf05-44b5-9cfa-1650f5d53590.txt' in OneDrive
□	DLP policy match for email
□	DLP policy match for email with subject 'file'
□	DLP policy match for document 'Credit card high number.docx' in SharePoint
□	DLP policy match for document 'Renamed TestDoc2.docx' in SharePoint
□	DLP policy match for document 'Scanned PDF SSN 2 - Copy (4) - Copy.pdf' in OneDrive
□	DLP policy match for document 'HRDT1.docx' in SharePoint
□	DLP policy match for document Contoso Cred - Copy (2) - Copy - Copy.jpg' in OneDrive
□	DLP policy match for document 'Screenshot 2022-07-22 113051 - Copy - Copy.png' in OneDrive
□	DLP policy match for document 'CC PDF.pdf' in OneDrive
□	DLP policy match for document 'PrivaSensitive.docx' in OneDrive
□	DLP policy match for document 'Picture8_Barc.png' in OneDrive

Customize Alert Triage Agent

Trigger
When a DLP alert is detected

Make selections regarding alert prioritization to customize this agent for your team.

Select alert timeframe
Last 30 days
Your admin has selected last 30 days as the maximum timeframe.

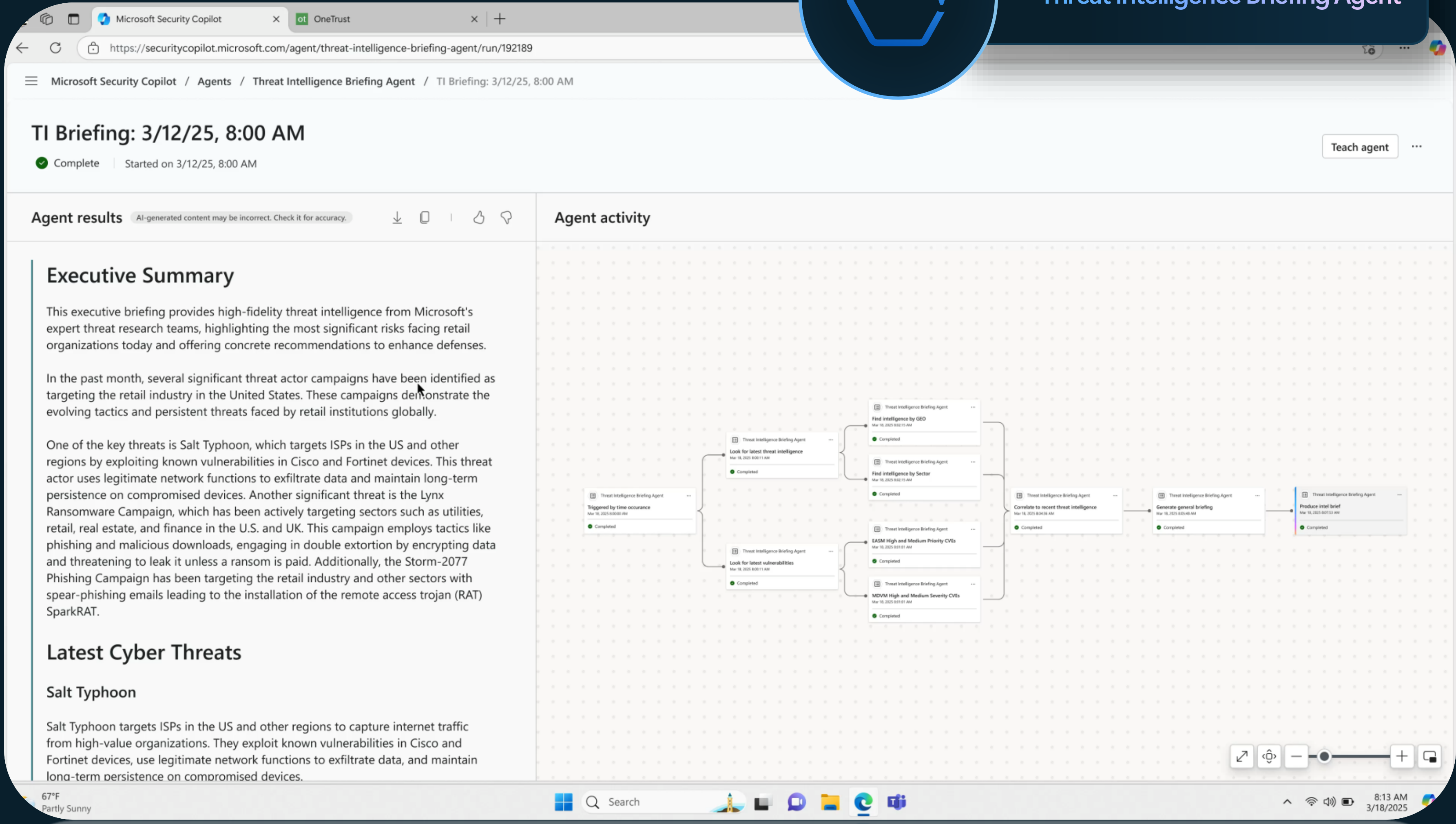
Enter custom instructions
The agent will use this info to generate a suggested prioritization rationale for the alerts it triages.
For example: Focus on Project Obsidian and proprietary assets

Specify policies
Select policies

Review | Cancel

Proactive Reports and Threat insights mapped to you

Threat Intelligence Briefing Agent



Microsoft Security Copilot
OneTrust
https://securitycopilot.microsoft.com/agent/threat-intelligence-briefing-agent/run/192189
Microsoft Security Copilot / Agents / Threat Intelligence Briefing Agent / TI Briefing: 3/12/25, 8:00 AM
Teach agent
Agent results
AI-generated content may be incorrect. Check it for accuracy.
Agent activity
Threat Intelligence Briefing Agent
Triggered by time occurance
Mar 18, 2025 8:00:00 AM
Completed
Look for latest threat intelligence
Mar 18, 2025 8:00:11 AM
Look for latest vulnerabilities
Mar 18, 2025 8:00:11 AM
Find intelligence by GEO
Mar 18, 2025 8:02:15 AM
Find intelligence by Sector
Mar 18, 2025 8:02:15 AM
EASM High and Medium Priority CVEs
Mar 18, 2025 8:01:01 AM
MDVM High and Medium Severity CVEs
Mar 18, 2025 8:01:01 AM
Correlate to recent threat intelligence
Mar 18, 2025 8:04:36 AM
Generate general briefing
Mar 18, 2025 8:05:48 AM
Produce intel brief
Mar 18, 2025 8:07:53 AM
Search
67°F
Partly Sunny
8:13 AM
3/18/2025

TI Briefing: 3/12/25, 8:00 AM

Complete | Started on 3/12/25, 8:00 AM

Executive Summary

This executive briefing provides high-fidelity threat intelligence from Microsoft's expert threat research teams, highlighting the most significant risks facing retail organizations today and offering concrete recommendations to enhance defenses.

In the past month, several significant threat actor campaigns have been identified as targeting the retail industry in the United States. These campaigns demonstrate the evolving tactics and persistent threats faced by retail institutions globally.

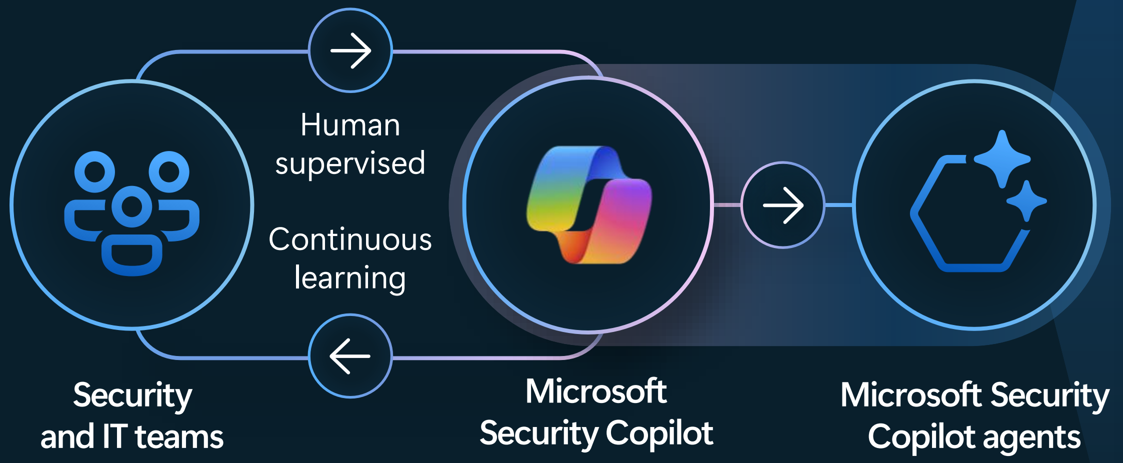
One of the key threats is Salt Typhoon, which targets ISPs in the US and other regions by exploiting known vulnerabilities in Cisco and Fortinet devices. This threat actor uses legitimate network functions to exfiltrate data and maintain long-term persistence on compromised devices. Another significant threat is the Lynx Ransomware Campaign, which has been actively targeting sectors such as utilities, retail, real estate, and finance in the U.S. and UK. This campaign employs tactics like phishing and malicious downloads, engaging in double extortion by encrypting data and threatening to leak it unless a ransom is paid. Additionally, the Storm-2077 Phishing Campaign has been targeting the retail industry and other sectors with spear-phishing emails leading to the installation of the remote access trojan (RAT) SparkRAT.

Latest Cyber Threats

Salt Typhoon

Salt Typhoon targets ISPs in the US and other regions to capture internet traffic from high-value organizations. They exploit known vulnerabilities in Cisco and Fortinet devices, use legitimate network functions to exfiltrate data, and maintain long-term persistence on compromised devices.

Agents to empower roles across security and IT



Human supervised

Continuous learning

Security and IT teams

Microsoft Security Copilot

Microsoft Security Copilot agents

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

Phishing Triage Agent in the Microsoft Defender portal

Autonomously triages phishing alerts

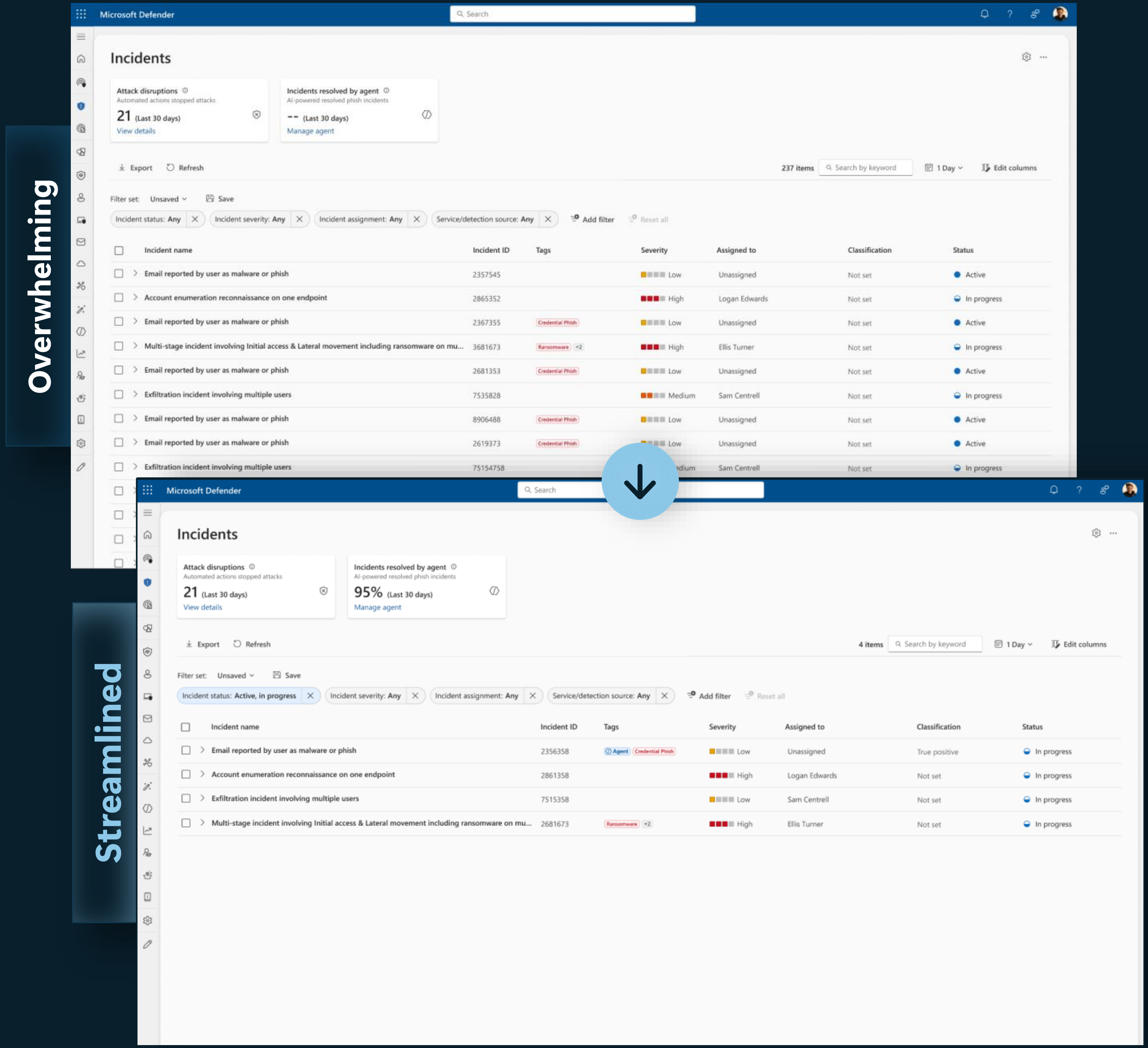
Conduct sophisticated assessments to determine whether an incident is a genuine threat or a false alarm with exceptional precision.

Evolves behavior based on feedback

Learns and evolves behavior through feedback provided in natural language, ensuring increased accuracy and nuance, with your team in control.

Provides full transparency into verdicts

Provides natural language explanations for verdicts and visually maps steps taken to reach each conclusion. Your team can adjust decisions as-needed.



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

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

237 items | Search by keyword | 1 Day

Filter set: Unsaved

Incident status: Any | 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	2357545		Low	Unassigned	Not set	Active
Account enumeration reconnaissance on one endpoint	2865352		High	Logan Edwards	Not set	In progress
Email reported by user as malware or phish	2367355	Credential Phish	Low	Unassigned	Not set	Active
Multi-stage incident involving Initial access & Lateral movement including ransomware on mu...	3681673	Ransomware +2	High	Ellis Turner	Not set	In progress
Email reported by user as malware or phish	2681353	Credential Phish	Low	Unassigned	Not set	Active
Exfiltration incident involving multiple users	7535828		Medium	Sam Centrell	Not set	In progress
Email reported by user as malware or phish	8906488	Credential Phish	Low	Unassigned	Not set	Active
Email reported by user as malware or phish	2619373	Credential Phish	Low	Unassigned	Not set	Active
Exfiltration incident involving multiple users	75154758		Medium	Sam Centrell	Not set	In progress

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

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

4 items | Search by keyword | 1 Day

Filter set: Unsaved

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	Logan Edwards	Not set	In progress
Exfiltration incident involving multiple users	7515358		Low	Sam Centrell	Not set	In progress
Multi-stage incident involving Initial access & Lateral movement including ransomware on mu...	2681673	Ransomware +2	High	Ellis Turner	Not set	In progress

Vulnerability Remediation Agent in Microsoft Intune

Continuously detect evolving threats

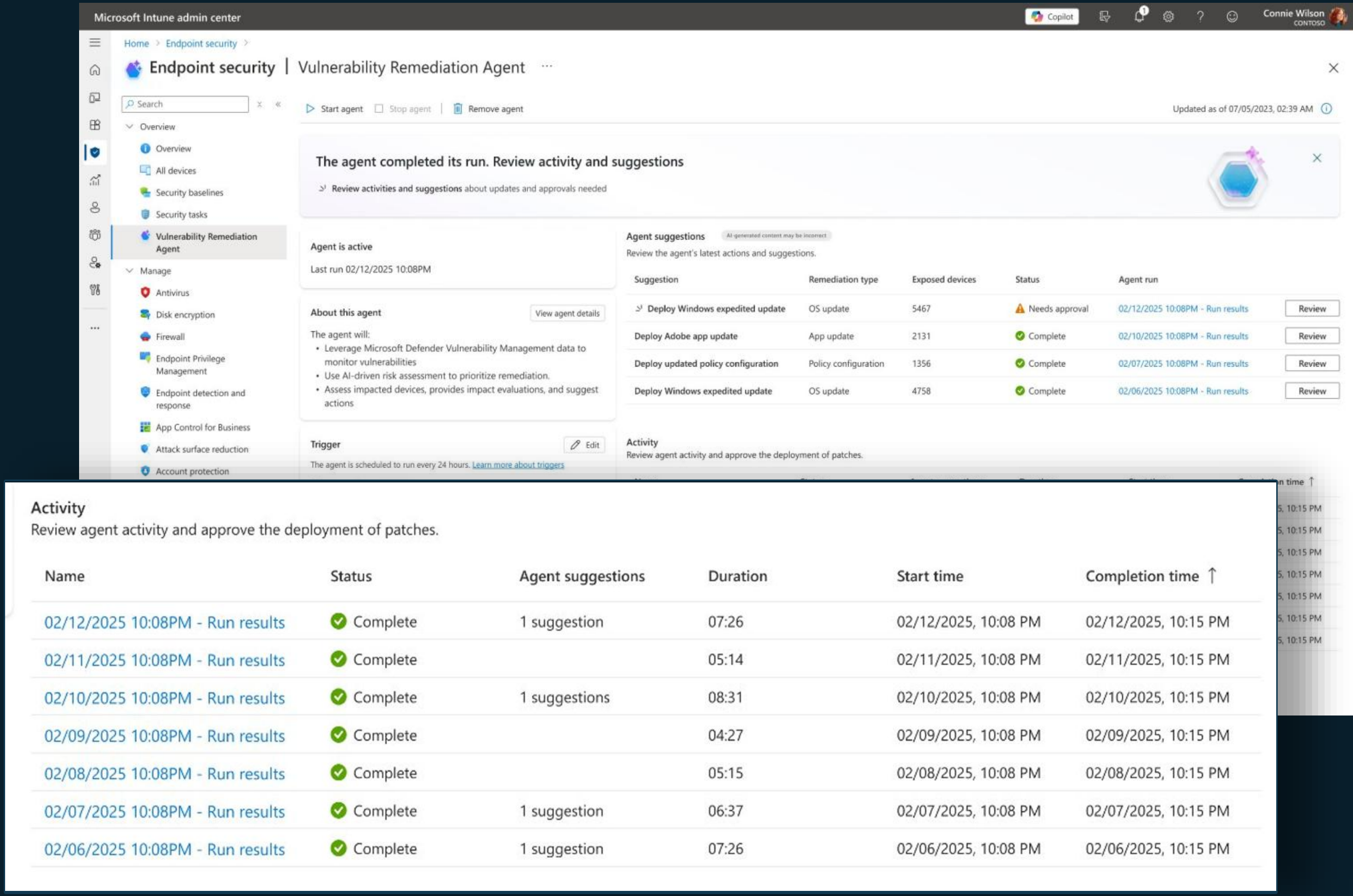
Monitors and reevaluates vulnerabilities over 90 days, identifying newly emerging threats.

Prioritize and expedite critical patches

Uses AI-driven analysis to analyze impact and determine which vulnerabilities need immediate attention.

Remediate faster with full context

Provides clear reasoning for urgency, enabling faster, informed remediation without unnecessary disruptions.



Updated as of 07/05/2023, 02:39 AM

The agent completed its run. Review activity and suggestions

Review activities and suggestions about updates and approvals needed

Agent is active

Last run 02/12/2025 10:08PM

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

Trigger

The agent is scheduled to run every 24 hours. Learn more about triggers

Agent suggestions AI-generated content may be incorrect

Review the agent's latest actions and suggestions.

Suggestion	Remediation type	Exposed devices	Status	Agent run	
Deploy Windows expedited update	OS update	5467	⚠ Needs approval	02/12/2025 10:08PM - Run results	Review
Deploy Adobe app update	App update	2131	✓ Complete	02/10/2025 10:08PM - Run results	Review
Deploy updated policy configuration	Policy configuration	1356	✓ Complete	02/07/2025 10:08PM - Run results	Review
Deploy Windows expedited update	OS update	4758	✓ Complete	02/06/2025 10:08PM - Run results	Review

Activity

Review agent activity and approve the deployment of patches.

Name	Status	Agent suggestions	Duration	Start time	Completion time ↑
02/12/2025 10:08PM - Run results	✓ Complete	1 suggestion	07:26	02/12/2025, 10:08 PM	02/12/2025, 10:15 PM
02/11/2025 10:08PM - Run results	✓ Complete		05:14	02/11/2025, 10:08 PM	02/11/2025, 10:15 PM
02/10/2025 10:08PM - Run results	✓ Complete	1 suggestions	08:31	02/10/2025, 10:08 PM	02/10/2025, 10:15 PM
02/09/2025 10:08PM - Run results	✓ Complete		04:27	02/09/2025, 10:08 PM	02/09/2025, 10:15 PM
02/08/2025 10:08PM - Run results	✓ Complete		05:15	02/08/2025, 10:08 PM	02/08/2025, 10:15 PM
02/07/2025 10:08PM - Run results	✓ Complete	1 suggestion	06:37	02/07/2025, 10:08 PM	02/07/2025, 10:15 PM
02/06/2025 10:08PM - Run results	✓ Complete	1 suggestion	07:26	02/06/2025, 10:08 PM	02/06/2025, 10:15 PM

Conditional Access Optimization Agent in Microsoft Entra

Quickly identify security gaps

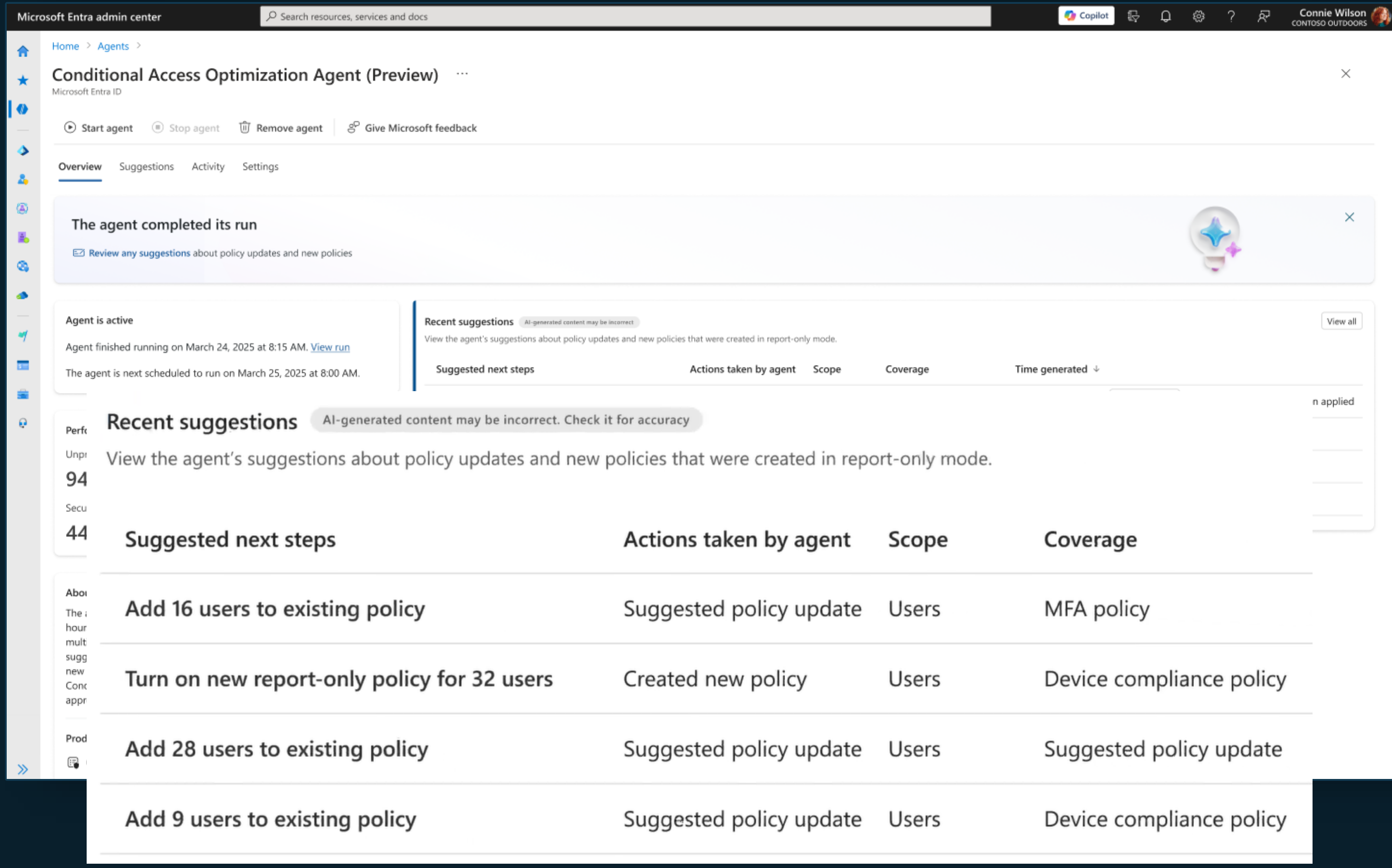
The agent continuously monitors for new users and apps to detect misalignments with Conditional Access policies, reducing unnoticed vulnerabilities.

One-click fixes

Get actionable recommendations with easy one-click remediation, streamlining CA policy updates and enhancing security with minimal effort.

Secure access as conditions change

The agent continually responds to changes in the environment, enhancing protection and reducing manual audits.



Conditional Access Optimization Agent (Preview)

Microsoft Entra ID

The agent completed its run

Review any suggestions about policy updates and new policies

Agent is active

Agent finished running on March 24, 2025 at 8:15 AM. View run

The agent is next scheduled to run on March 25, 2025 at 8:00 AM.

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

View the agent's suggestions about policy updates and new policies that were created in report-only mode.

Suggested next steps	Actions taken by agent	Scope	Coverage
Add 16 users to existing policy	Suggested policy update	Users	MFA policy
Turn on new report-only policy for 32 users	Created new policy	Users	Device compliance policy
Add 28 users to existing policy	Suggested policy update	Users	Suggested policy update
Add 9 users to existing policy	Suggested policy update	Users	Device compliance policy

Alert Triage Agents in Microsoft Purview Data Loss Prevention (DLP) and Insider Risk Management (IRM)

Prioritizes high-risk alerts

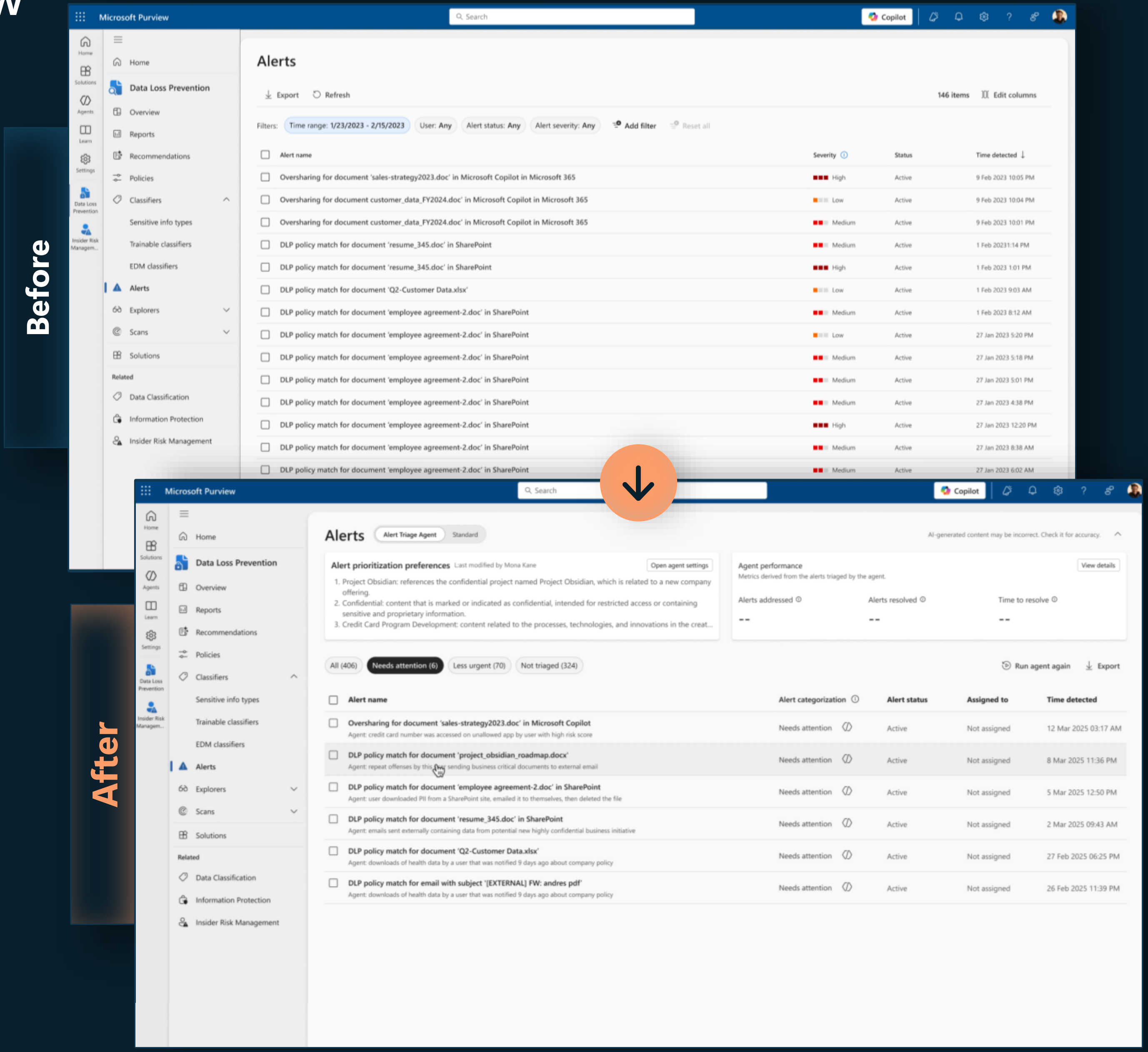
Intelligently identifies the riskiest DLP and IRM alerts based on organizational priorities, ensuring critical threats receive immediate attention.

Customize agent criteria

Learns and fine-tunes alert triage criteria from admin-provided natural language customizations within hours.

Improve efficiency and coverage

Automates alert triage and provides comprehensive summaries so data security teams can focus on critical threats.



Alerts

146 items

Filters: Time range: 1/23/2023 - 2/15/2023 | User: Any | Alert status: Any | Alert severity: Any

Alert name	Severity	Status	Time detected ↓
Oversharing for document 'sales-strategy2023.doc' in Microsoft Copilot in Microsoft 365	High	Active	9 Feb 2023 10:05 PM
Oversharing for document customer_data_FY2024.doc' in Microsoft Copilot in Microsoft 365	Low	Active	9 Feb 2023 10:04 PM
Oversharing for document customer_data_FY2024.doc' in Microsoft Copilot in Microsoft 365	Medium	Active	9 Feb 2023 10:01 PM
DLP policy match for document 'resume_345.doc' in SharePoint	Medium	Active	1 Feb 20231:14 PM
DLP policy match for document 'resume_345.doc' in SharePoint	High	Active	1 Feb 2023 1:01 PM
DLP policy match for document 'Q2-Customer Data.xlsx'	Low	Active	1 Feb 2023 9:03 AM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Medium	Active	1 Feb 2023 8:12 AM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Low	Active	27 Jan 2023 5:20 PM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Medium	Active	27 Jan 2023 5:18 PM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Medium	Active	27 Jan 2023 5:01 PM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Medium	Active	27 Jan 2023 4:38 PM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	High	Active	27 Jan 2023 12:20 PM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Medium	Active	27 Jan 2023 8:38 AM
DLP policy match for document 'employee agreement-2.doc' in SharePoint	Medium	Active	27 Jan 2023 6:02 AM

Alerts

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

Alert prioritization preferences Last modified by Mona Kane

1. Project Obsidian: references the confidential project named Project Obsidian, which is related to a new company offering.
2. Confidential: content that is marked or indicated as confidential, intended for restricted access or containing sensitive and proprietary information.
3. Credit Card Program Development: content related to the processes, technologies, and innovations in the creat...

Agent performance

Metrics derived from the alerts triaged by the agent.

Alerts addressed	Alerts resolved	Time to resolve
--	--	--

All (406) | Needs attention (6) | Less urgent (70) | Not triaged (324)

Alert name	Alert categorization	Alert status	Assigned to	Time detected
Oversharing for document 'sales-strategy2023.doc' in Microsoft Copilot Agent: credit card number was accessed on unallowed app by user with high risk score	Needs attention	Active	Not assigned	12 Mar 2025 03:17 AM
DLP policy match for document 'project_obsidian_roadmap.docx' Agent: repeat offenses by this user sending business critical documents to external email	Needs attention	Active	Not assigned	8 Mar 2025 11:36 PM
DLP policy match for document 'employee agreement-2.doc' in SharePoint Agent: user downloaded PII from a SharePoint site, emailed it to themselves, then deleted the file	Needs attention	Active	Not assigned	5 Mar 2025 12:50 PM
DLP policy match for document 'resume_345.doc' in SharePoint Agent: emails sent externally containing data from potential new highly confidential business initiative	Needs attention	Active	Not assigned	2 Mar 2025 09:43 AM
DLP policy match for document 'Q2-Customer Data.xlsx' Agent: downloads of health data by a user that was notified 9 days ago about company policy	Needs attention	Active	Not assigned	27 Feb 2025 06:25 PM
DLP policy match for email with subject '[EXTERNAL] FW: andres pdf' Agent: downloads of health data by a user that was notified 9 days ago about company policy	Needs attention	Active	Not assigned	26 Feb 2025 11:39 PM

Threat Intelligence Briefing Agent in Security Copilot standalone

Threat insights mapped to you

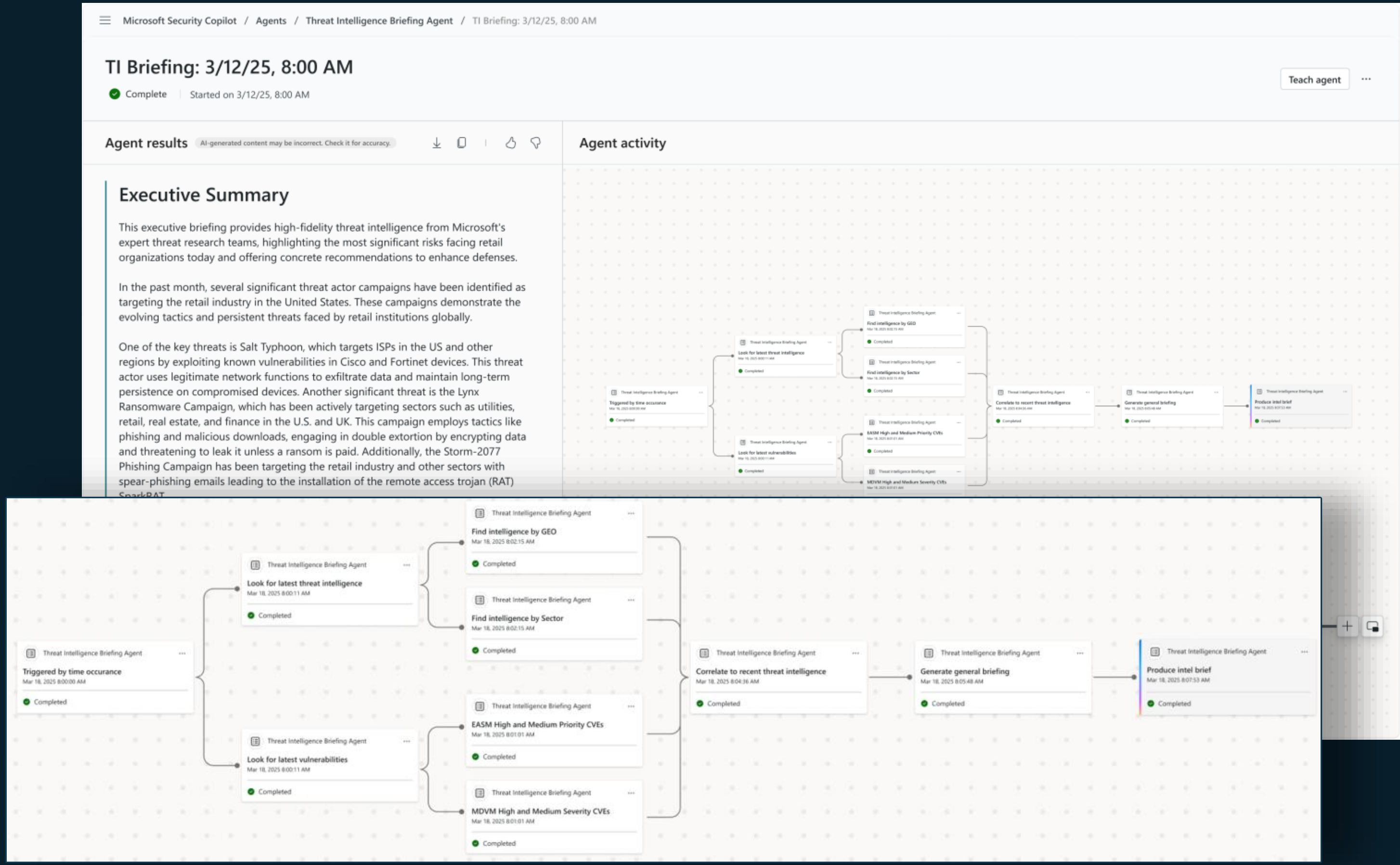
Provides the latest threat intelligence related to your organization's unique profile, including geolocation, IT infrastructure, and threat exposure.

Real-time situational awareness

Continuously learns from evolving attack landscapes and IT environments to provide the most relevant security updates.

Rapid reporting

Generates reports in minutes, eliminating the need for manual intelligence gathering and ongoing maintenance, which can take hours to days.



Microsoft Security Copilot / Agents / Threat Intelligence Briefing Agent / TI Briefing: 3/12/25, 8:00 AM

TI Briefing: 3/12/25, 8:00 AM

Complete | Started on 3/12/25, 8:00 AM

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

Executive Summary

This executive briefing provides high-fidelity threat intelligence from Microsoft's expert threat research teams, highlighting the most significant risks facing retail organizations today and offering concrete recommendations to enhance defenses.

In the past month, several significant threat actor campaigns have been identified as targeting the retail industry in the United States. These campaigns demonstrate the evolving tactics and persistent threats faced by retail institutions globally.

One of the key threats is Salt Typhoon, which targets ISPs in the US and other regions by exploiting known vulnerabilities in Cisco and Fortinet devices. This threat actor uses legitimate network functions to exfiltrate data and maintain long-term persistence on compromised devices. Another significant threat is the Lynx Ransomware Campaign, which has been actively targeting sectors such as utilities, retail, real estate, and finance in the U.S. and UK. This campaign employs tactics like phishing and malicious downloads, engaging in double extortion by encrypting data and threatening to leak it unless a ransom is paid. Additionally, the Storm-2077 Phishing Campaign has been targeting the retail industry and other sectors with spear-phishing emails leading to the installation of the remote access trojan (RAT) SparkRAT.

Teach agent
Agent activity
Threat Intelligence Briefing Agent
Triggered by time occurance
Mar 18, 2025 8:00:00 AM
Completed
Threat Intelligence Briefing Agent
Look for latest threat intelligence
Mar 18, 2025 8:00:11 AM
Completed
Threat Intelligence Briefing Agent
Look for latest vulnerabilities
Mar 18, 2025 8:00:11 AM
Completed
Threat Intelligence Briefing Agent
Find intelligence by GEO
Mar 18, 2025 8:02:15 AM
Completed
Threat Intelligence Briefing Agent
Find intelligence by Sector
Mar 18, 2025 8:02:15 AM
Completed
Threat Intelligence Briefing Agent
EASM High and Medium Priority CVEs
Mar 18, 2025 8:01:01 AM
Completed
Threat Intelligence Briefing Agent
MDVM High and Medium Severity CVEs
Mar 18, 2025 8:01:01 AM
Completed
Threat Intelligence Briefing Agent
Correlate to recent threat intelligence
Mar 18, 2025 8:04:36 AM
Completed
Threat Intelligence Briefing Agent
Generate general briefing
Mar 18, 2025 8:05:48 AM
Completed
Threat Intelligence Briefing Agent
Produce intel brief
Mar 18, 2025 8:07:53 AM
Completed

"Lessons Learned" de sidste 12 måneder

- Lav en plan inden du starter.
- Forvent ikke bare, at "AI-magi sker".
- Vælge 2 eller 3 Use Cases og få dem til at fungere for at kunne vise værdien af Security Copilot og før man går videre

- Forstå prissætningen, dimensionering, overvågning og optimering for at forstå værdien i din organisation.

- Uddannelse – Det er et nyt product!
- Forstå Standalone, Embedded og Automatiserings mulighederne og hvordan de kan passe til dine Use Cases og hvordan.

- Brug Security Copilot Github. Der er guides, Logic Apps, Plugins, Promptsbooks og meget mere – Gør det nemt for dig selv!

- Use Cases: Hvad skal Security Copilot gøre for dig?
- Analyser måden du arbejder på og se om der er gode kandidater til at blive automatiseret eller udvidet med Security Copilot

- Tag en beslutning på et oplyst grundlag og hvor kan det gøre den største forskel.

Microsoft Security

Tak!