



TORINO

#GlobalAzureTorino



Utilizzo dell'AI generativa nel campo della sicurezza

Marco Moioli
Cloud Solution Architect
Microsoft



Agenda

Subject A

Subject B

Subject C

AI technology is **here**

Forbes

What ChatGPT And Generative AI Mean For Your Business?

COMPUTERWORLD

Microsoft's new Teams Premium tier integrates with OpenAI's GPT-3.5

MARKETS INSIDER

Nuance and Microsoft Announce the First Fully AI-Automated Clinical Documentation Application for Healthcare

VentureBeat

Microsoft gives Businesses a GPT boost In Teams and Viva Sales

TheVerge

ChatGPT is now available in Microsoft's Azure OpenAI service

USA TODAY

New Bing with ChatGPT brings the power of AI to Microsoft's signature search engine

VentureBeat

Microsoft announces generative AI-powered Copilot 365 to 'change work as we know it'

CN BUSINESS.

Real estate agents say they can't imagine working without ChatGPT now

TechCrunch

Microsoft brings an AI-powered Copilot to its business app suite

And the
impact
is **real**



Carmax estimates an individual would take 11 years to do what Azure OpenAI Service was able to do in days



Progressive is saving \$10M annually with AI-powered chatbots



EY is saving 250K hours of manual work per client using intelligent document automation

A Copilot for every Microsoft Cloud experience

Microsoft 365 Copilot

Works alongside you in the apps you use every day

[Learn more](#)

Dynamics 365 Copilot

Turbocharge your workforce with a copilot for every job role

[Learn more](#)

Copilot in Power Platform

Imagine it, describe it, and Power Platform builds it

[Learn more](#)

Microsoft Copilot for Security

Defend at machine speed with Microsoft Security Copilot

[Learn more](#)

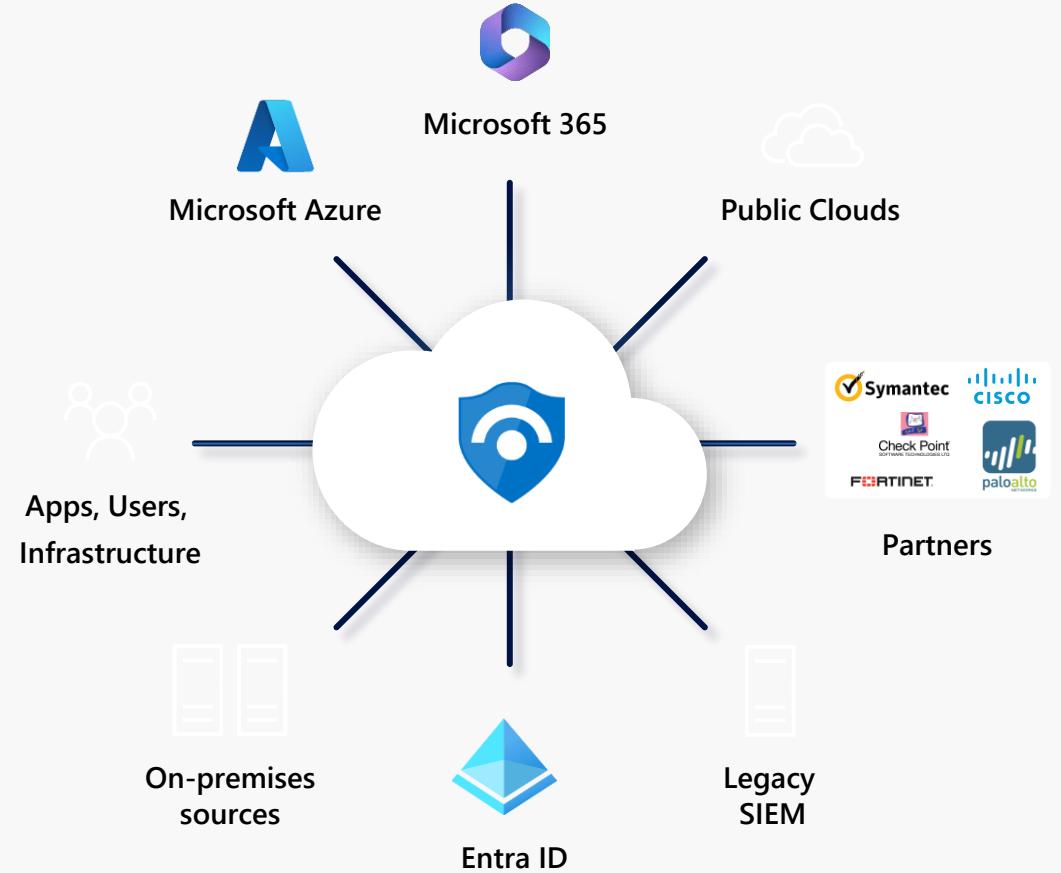
GitHub Copilot

Increase developer productivity to accelerate innovation

[Learn more](#)

Benefits of AI for security

- **Efficiency:** Prioritization and automation
- **Speed:** Ability to understand unique threats in real time
- **Scale:** Ability to process large volumes of data



The Microsoft Sentinel platform has more than 10 petabytes of daily ingestion

What makes Generative AI important for security?

Cybercrime and cyber warfare are still on the rise

The Washington Post

THE CYBERSECURITY 202

Think ransomware gangs won't thrive this year? Think again, experts say

Analysis by Tim Starks
with research by David DiMoffetta

March 30, 2023 at 6:52 a.m. EDT

Comment 4 Gift Article Share

Welcome to The Cybersecurity 202! And greetings from (just outside of) San Francisco, one of my favorite few cities. As I type this, I have a splendid view of the Golden Gate Bridge.

Reading this online? Sign up for The Cybersecurity 202 to get scoops and sharp analysis in your inbox each morning.

Below: The U.S. sends cybersecurity aid to Costa Rica, and a possible North Korean-linked cyberattack could have thousands of victims. First:

The Economist

Russian hackers are preparing for a new campaign in Ukraine

A spring cyber-offensive is about to be unleashed



FINANCIAL TIMES

& CAREERS LIFE & ARTS HTML

er 2008-style precipice?
tion.

Subscribe now

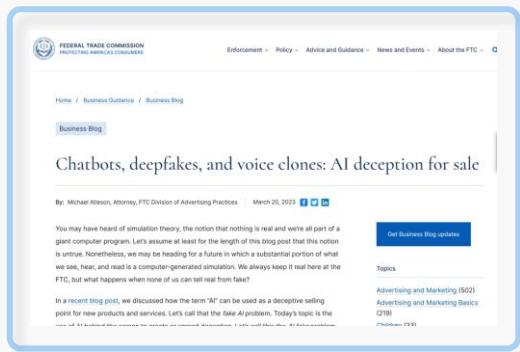
ber stress tests after

cant increase' in incidents since outbreak of

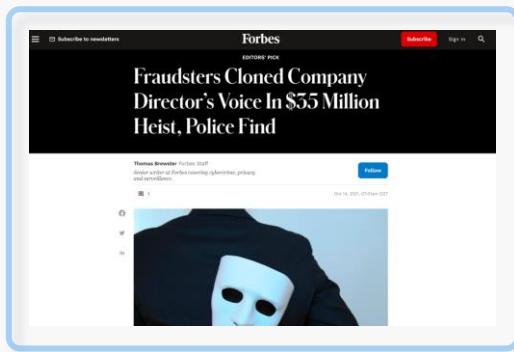


What we know already

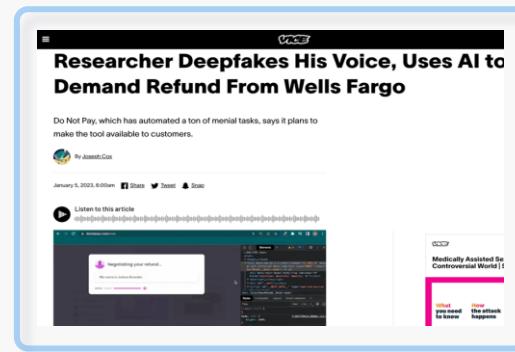
[Learn more](#)



[Chatbots, deepfakes and voice clones](#)
Federal Trade Commission Article



[Fraudsters Cloned Company Directors Voice](#)
Forbes Article



[Researcher Deepfakes His Voice](#)
Vice Article



[WithSecure-Creatively Malicious](#)
PDF



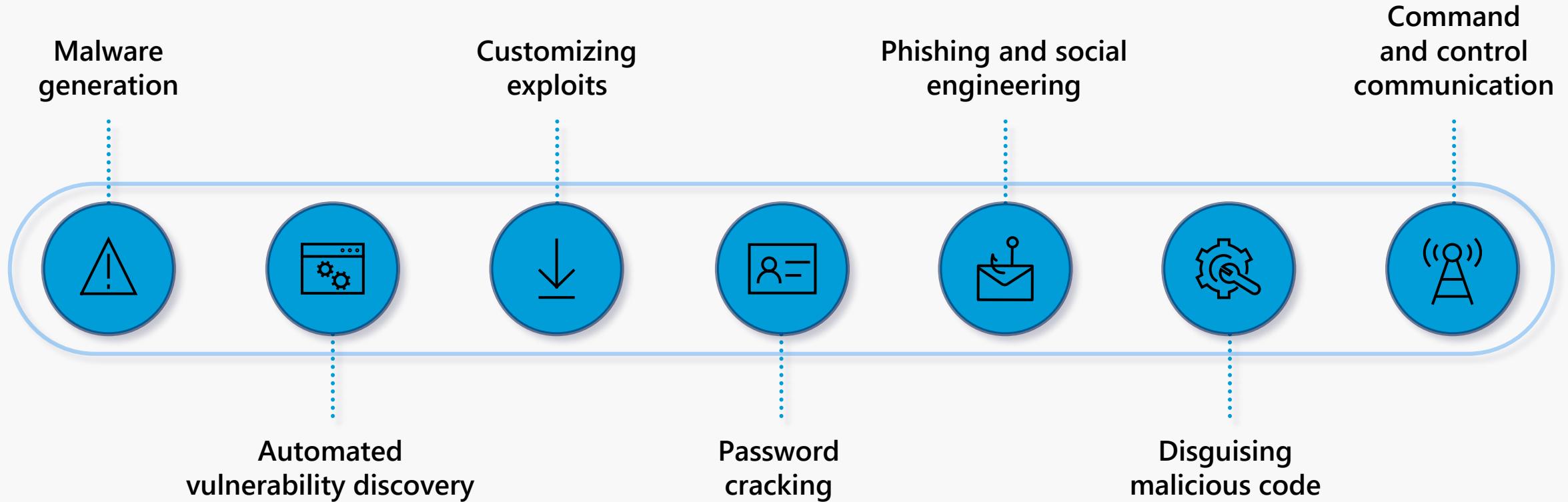
[How Hackers Use Generative AI](#)
Article



[Blackmamba Chatgpt polymorphic](#)
Blog post

What to expect from adversaries

AI-empowered attacks



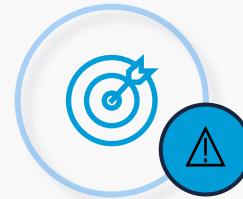
LLM for adversarial activity

AI-empowered attacks



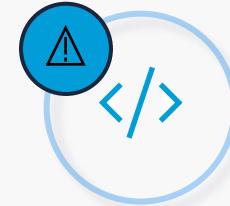
Disinformation

- Generative images
- Generative text, fake news stories
- Fake online personas, crafting a conversation narrative



Spear phishing

- High-quality personalized messaging
- Automated conversation, trust building
- Fake voice, phone interaction



Democratization of cybercrime

- Code-gen lowers the technical barrier to entry
- Malware—for more sophisticated actors, we may see GenAI used to modify existing malware to bypass detection



Impersonation fraud

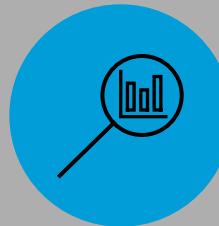
- Fake voice messages, even video
- Fake text

How Copilot for Security works

Primary use cases



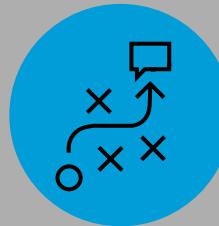
Incident summarization



Impact analysis

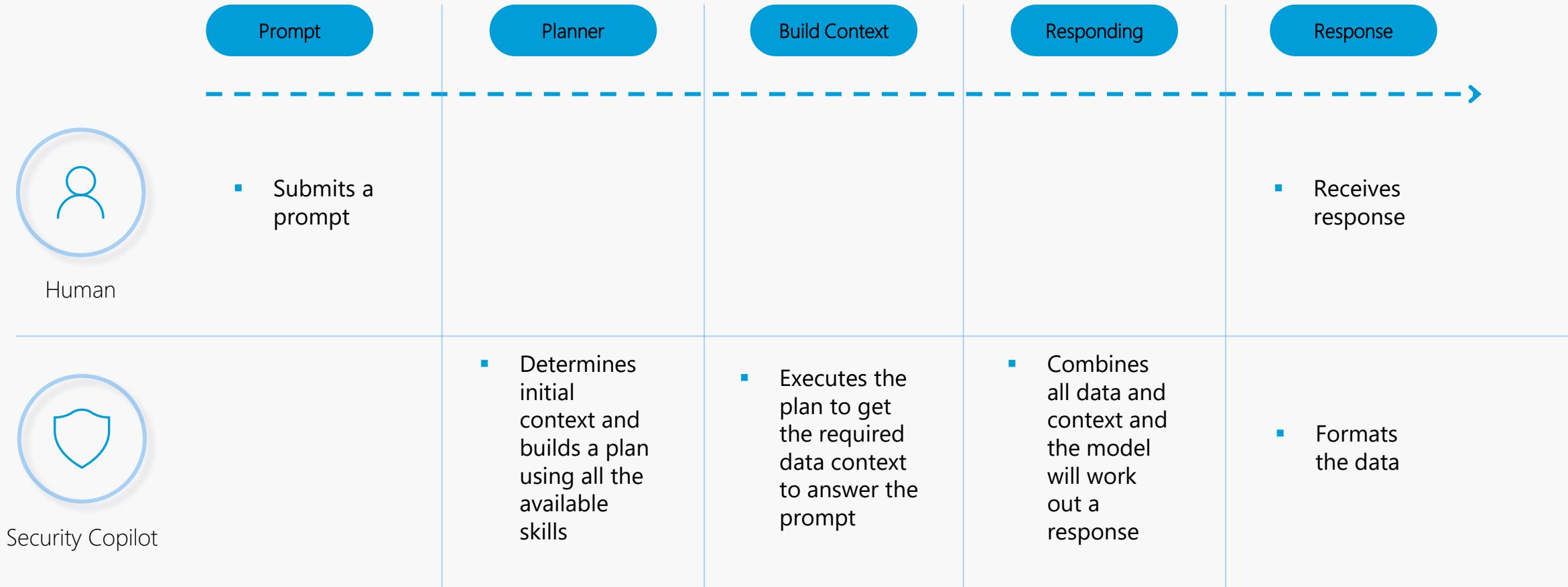


Reverse engineering of scripts

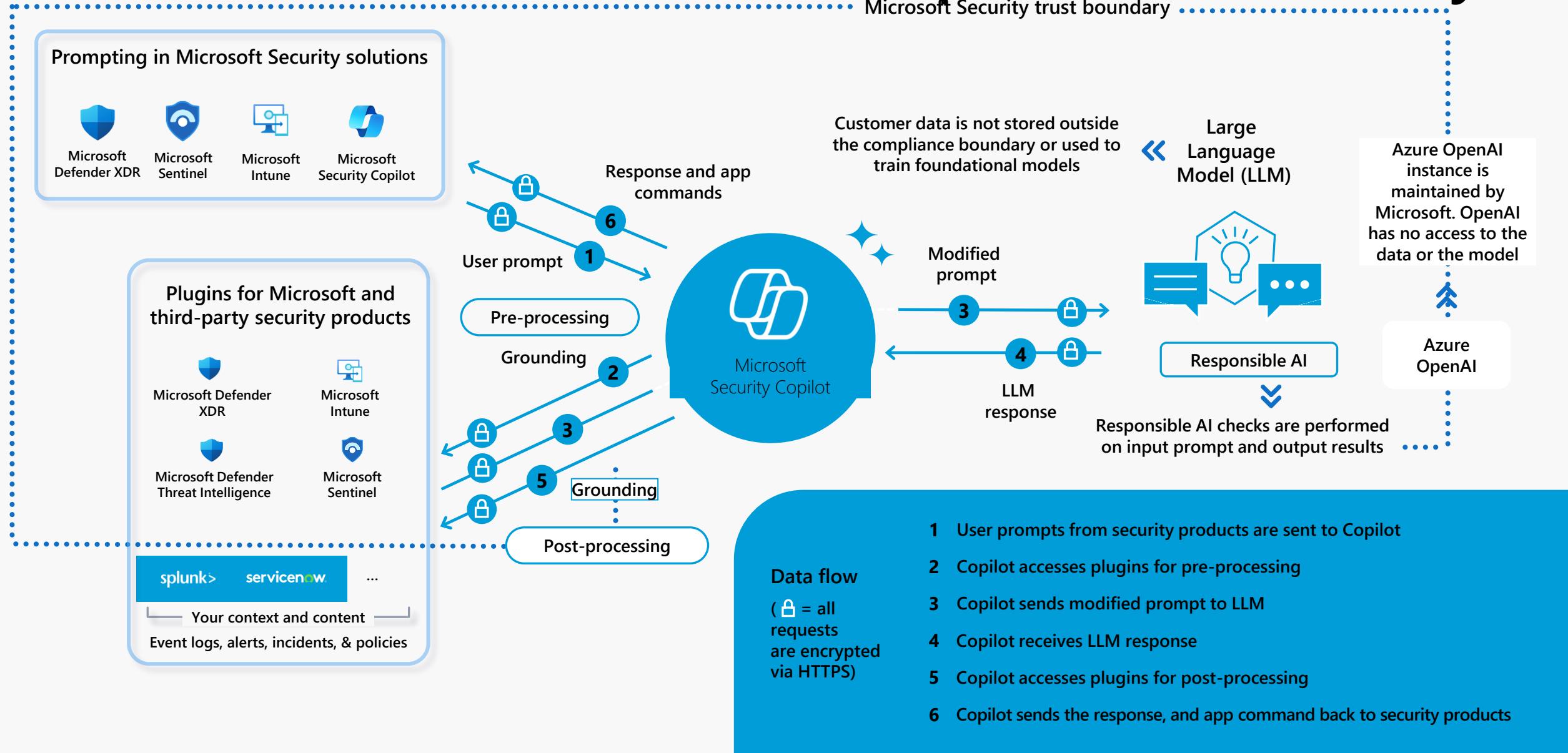


Guided response

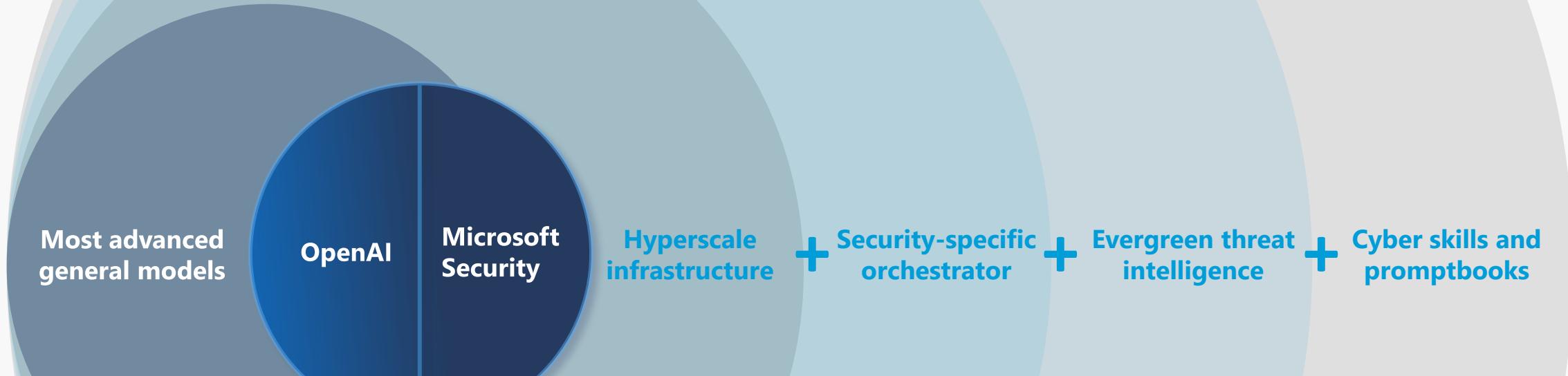
How it works



Data flow for Microsoft Copilot for Security



The Microsoft Copilot for Security advantage



Built with security, privacy, and compliance.

Your data is **your** data



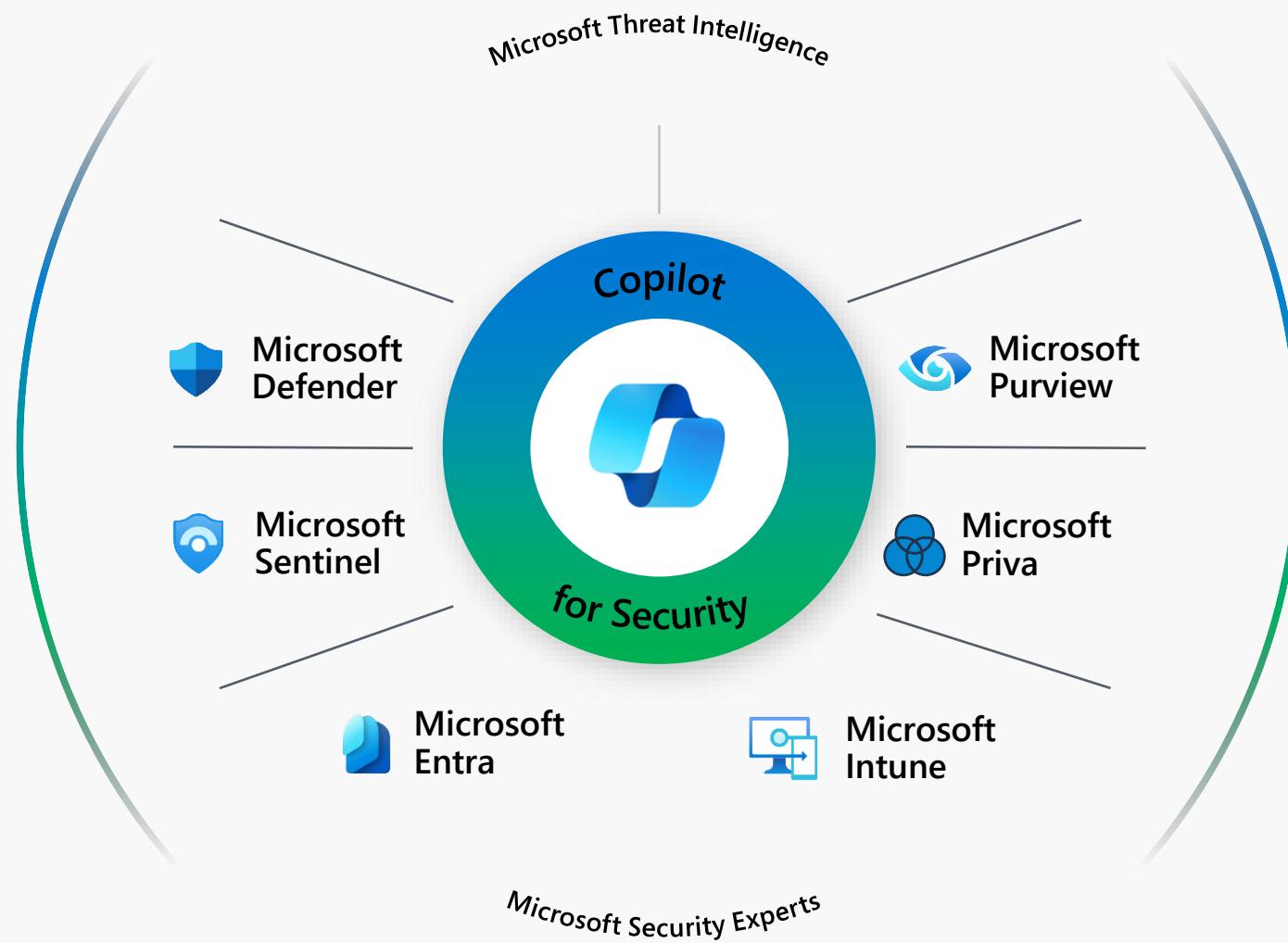
Your data is **not** used to train
the foundation AI models



Your data is protected by the
most comprehensive enterprise
compliance and security controls



Microsoft's End-to-End Security



End-to-end security at machine speed and scale

Microsoft Security Solutions	Available in the standalone experience	Available as an embedded experience	
 Microsoft Defender XDR	✓	✓	
 Microsoft Sentinel	✓	✓ *	
 Microsoft Intune	✓	✓	
 Microsoft Entra	✓	✓	
 Microsoft Purview	✓	✓	

Rapid investigation and response

Investigate with AI-assisted insights and quickly pivot to remediation with actionable, prioritized recommendations

Scaled visibility

Quickly assess security posture, threats and policy or compliance gaps. Access summaries with context to understand the potential impacts.

Faster troubleshooting

Get deep understanding of device, user, access, and app status to resolve issues quickly. Find and remediate policy issues faster with natural language prompts.

Advanced skills unlocked

Script analysis and natural language to KQL and KeyQL empower any team member to complete complex tasks with confidence.

*Available as part of the unified security operations platform.

Copilot standalone experience

The screenshot shows the Microsoft Security Copilot interface in a dark mode theme. At the top, there's a navigation bar with three horizontal lines, the text "Microsoft Security Copilot", and a "Preview" button.

Below the navigation bar, a button says "Continue your last session".

The main content area contains three cards:

- Tell me about Defender incident 20259.**

The customer inquired about the Defender incident 20259 with Medium severity. The incident involved a medium-severity alert for an unfamiliar sign-in attempt from IP address '136.49.226.136' in the United States. The incident was detected on 2023-11-02 18:36:24 UTC and involved an user named 'lvandenende'. The incident was at the Initial Access stage of the kill chain. The user was affected by the attempted sign-in and the incident is still ongoing. The incident was reported to the customer by the agent. The customer was asked to provide a summary of the incident. The agent provided a summary of the security incident.

Updated less than a minute ago
- Tell me more about Cobalt Strike.**

Cobalt Strike is a penetration testing and adversary emulation framework that was first released in 2012. It was initially designed to...
- Tell me about my latest incidents.**

These include unfamiliar sign-in properties, multiple failed user logon attempts, threat intelligence session, attack using AiTM...

At the bottom left, there's a section titled "Explore with Copilot" with buttons for "Featured prompts" (selected) and "Promptbooks".

Below that are three cards:

- Threat actor profile**

Get a report profiling a known actor with suggestions for protecting against common tools and tactics.

Microsoft Security · 5 ↗
- Vulnerability impact assessment**

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security · 6 ↗
- Microsoft Sentinel incident investigation**

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

Microsoft Security · 7 ↗

At the bottom center, there's a search bar with the placeholder "Ask anything about security, or type / for suggestions or * for promptbooks" and a "View all sessions →" link.

Icons for a file, a question mark, and a refresh/circular arrow are located at the bottom corners.



How can I improve my security posture?



Are any of my machines affected?



Summarize this incident in bullets.



Which alerts are being triggered the most?



What is log4shell?



Tell me about Defender incident 20259.

Tell me about Defender incident 20259.



> 3 steps completed 25s

Nov 2, 3:14 PM | 26.94s

Defender incident 20259 with Medium severity has a total of 1 alerts. 1 alerts were selected for summarizing the incident.

Some alerts from the incident include:

1. Severity: Medium Start time: 2023-11-02 18:36:24 Description: Unfamiliar sign-in properties relating to attempted sign-in, IP '136.49.226.136' impacting User 'lvandenende'

Here's a short summary of the incident:

The security incident occurred on 2023-11-02 18:36:24 UTC and involved a medium-severity alert. An unfamiliar sign-in attempt was detected, originating from IP address '136.49.226.136' in the United States, impacting user 'lvandenende'. The incident is at the Initial Access stage of the kill chain.

Sources

[Incident Page](#)



Looks right



Needs improvement



Inappropriate



Manage sources

Plugins

Files

Plugins

Turn on or create your own plugins to give Copilot access to the security services and websites you use. [Learn more](#)



All (22)

On (7)

Off (15)

Microsoft i



Azure AI Search (Preview)

Indexed data

Set up



Microsoft Defender External Attack Surface

Management



Attack surfaces, vulnerable assets, and attack surface insights



Microsoft Defender Threat Intelligence

Articles, intelligence profiles, vulnerabilities, indicators of compromise, hosts, and threat analytics



Microsoft Defender XDR

Alerts and incidents



Microsoft Entra

Alerts, users, groups, access reviews, and risky services



Microsoft Intune

Devices, apps, policies, and postures



Microsoft Purview Not available i

Purview alerts, Insights, and Risk details



Microsoft Sentinel (Preview)

Incidents and workspaces



Add a plugin



Complete the info to add a new plugin. [Learn more](#)

Who can use this plugin? i *

Just me



Select an upload format i *



Copilot for Security plugin

Custom .yaml or .json



OpenAI plugin

manifest.json

Cancel

Add

My sessions

[+ New session](#)
 All
 Recent

 Delete

Name	Last updated	Created
Device summary for avd-0	4:43 PM	4:43 PM
show me active alerts in my environment	4:41 PM	4:41 PM

Promptbook library

Promptbooks contain one or more prompts that run in sequence automatically. They quickly produce custom reports and analysis using your plugins and permissions. [Learn more](#)

 All
 My promptbooks
 Contoso
 Microsoft

Name	Inputs	Plugins	Tags	Prompts	Owner
Microsoft 365 Defender incident investigation Get a report about a specific incident, with related alerts, reputation scores, users, and devices.	DEFENDER INCIDENT ID			7	Microsoft
Microsoft Sentinel incident investigation Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.	SENTINEL INCIDENT ID			7	Microsoft
Suspicious script analysis Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.	SNIPPET	Script		6	Microsoft
Threat actor profile Get a report profiling a known actor with suggestions for protecting against common tools and tactics.	THREATACTORNAME	Threat Actor		5	Microsoft
Vulnerability impact assessment Get a report summarizing the intelligence for a known vulnerability and how to address it.	CVEID	cveid		4	Microsoft



Can you summarize sentinel incident 29088 contained in workspace woodgrove-loganalyticsworkspace?

> 3 steps completed 1 min

2:09 PM

Incident 29088 in the Woodgrove-LogAnalyticsWorkspace has the title "SAP - (Preview) File Downloaded From a Malicious IP Address" and is described as a user downloading a file from an SAP system using an IP address known to be malicious. The incident has a severity of "High" and is currently in "New" status. The incident was first detected on 2023-06-21T18:38:41.103Z and last updated on 2023-06-22T18:43:44.4744196Z.

The incident has 1 associated alert with the same title and description. The alert was generated on 2023-06-22T18:43:44.1397144Z and has a tactic of "Exfiltration".

There are 3 entities associated with this incident:

1. IP: 185.82.217.3
2. Host: CPC-mscot-S0C0S (Windows, FQDN: cpc-mscot-s0c0s)
3. Account: [mscott@woodgrove.ms](#) (AzureAD domain, DisplayName: [mscott@woodgrove.ms](#))

Please note that this is a summary of the available information, and further investigation may be required to fully understand the incident.

Confirm Off-target Report Pin

❖ Ask anything about security, or type / for suggestions

Severity: Link: None

These rules indicate that the IP address is associated with known cyber threat intelligence profiles and suspicious behavior.

Confirm Off-target Report Pin

Tell me more about cobalt strike and silk typhoon.

>  3 steps completed 1 min  +2

2:14 PM

Here's more information about Cobalt Strike and Silk Typhoon:

1. Cobalt Strike
Cobalt Strike is a commercial, full-featured penetration testing tool that allows an attacker to deploy an agent named "Beacon" on the victim's machine. Beacon includes a wealth of functionality to the attacker, including command execution, keylogging, file transfer, SOCKS proxying, privilege escalation, and more. It is often used by advanced persistent threat (APT) groups and cybercriminals for post-exploitation activities. Cobalt Strike has been observed in various cyber attacks, including those taking advantage of the Exchange Server vulnerabilities. You can read more about it in this [article](#).

2. Silk Typhoon (HAFNIUM)
Silk Typhoon is a threat actor group that has been observed exploiting the Exchange Server vulnerabilities. They are known for their sophisticated attacks and have targeted various organizations worldwide. Microsoft researchers have observed a steady increase in signals indicating exploitation by threat actors other than Silk Typhoon. Numerous other attackers have been seen adopting the exploit into their toolkits. You can read more about Silk Typhoon and their activities in this [article](#).

Confirm Off-target Report Pin

❖ Ask anything about security, or type / for suggestions

these devices compliant.

> 3 steps completed 1 min

2:15 PM

Here are the devices associated with the user [mscott@woodgrove.ms](#) and their compliance status:

Device Name	Manufacturer	Model
MSCOTT-SURFACE2	Microsoft Corporation	Surface Laptop 2
DESKTOP-LDLSMJL	Microsoft Corporation	Virtual Machine
CPC-mscot-S0C0S	Microsoft Corporation	Cloud PC Enterprise 2vCPU/8GB/128GB

To make these devices compliant, follow these steps:

- 1. Remain in contact**
Ensure that the devices remain in contact with the Intune service. Devices that do not remain in contact may be considered noncompliant. Check the device's network connectivity and ensure it can communicate with the Intune service.
- 2. Defender for Endpoint - Device Risk**
For the device CPC-mscot-S0C0S, ensure that the required security level for Device Threat Protection is met. This can be achieved by updating the device's security software, applying security patches, and ensuring that the device is protected against known threats.

After addressing these issues, the devices should become compliant. Keep in mind that it may take some time for the compliance status to update in Intune.

Confirm Off-target Report Pin

❖ Ask anything about security, or type / for suggestions



If there was suspicious activity or an alert, explain it in more detail. Give each section a short heading, provide a one-sentence description for each point, and link any items that can be branching points for further investigation.

12:37 PM

LDAP Alert

The LDAP alert indicates that a suspicious LDAP query was executed by the user dtorres on the workstation8.contoso.com device, using the ONENOTE.EXE process. The alert suggests that this could be a sign of reconnaissance activity by an attacker who is trying to learn the organization's structure and find valuable targets.

WMI Alert

The alert about WMI indicates that a malicious process named DoorBreach.exe was created on the machine workstation8 by a PowerShell script that downloaded and imported a module from a suspicious URL. The PowerShell script was executed by the user dtorres, who had full elevation token and domain credentials. The process used WMI to spawn new processes, which is a common technique used by malware to evade detection and persistence. The alert occurred multiple times between 2023-02-28 and 2023-03-02, suggesting a persistent infection.

A further investigation of the WMI activity and the DoorBreach.exe process is needed to determine the scope and impact of the infection.

Sources

1. Microsoft Sentinel

Confirm Off-target Report Unpin

Reverse-engineer exploits Containment: Preserving exist...

Type "/" or ask anything about security

Alert on compromised account and device on Contoso.com

OneNote WMI PowerShell AMSI Kinsing Muhsitic
Sabsik Wacatac

Summary Pinned items (5)

Alert Summary

This alert indicates that a device belonging to Devon Torres, a user of the contoso.com domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (ONENOTE.EXE) that was launched from a downloaded file (SalesLeads (1).onepkg) and its parent process (explorer.exe), as well as the device's hostname (workstation8), OS version (Windows 21H2), and risk score (High). The alert also shows the device's last seen time, external and internal IP addresses, and antivirus status. The device has a user-defined tag (ContosoDemo) and is onboarded to Microsoft Defender for Endpoint (MDATP).

Attack Steps

The account dtorres@contoso.com was involved in a series of suspicious actions on the workstation8 host, indicating a possible compromise by a malware campaign.

The following attack steps were observed:

- Malicious OneNote package file downloaded
- Malicious scripts executed via WScript.exe
- Attempted AMSI tampering and process injection
- Suspicious Microsoft Defender Antivirus exclusion and startup folder addition
- Suspicious LDAP query and process discovery
- Suspicious WMI process creation
- Suspicious PowerShell command line and script execution

Attack Details

Malicious OneNote package file downloaded



12:47 PM

Based on the queries and results, it is possible that the given user has been compromised or targeted by an attacker. Some indicators of compromise or suspicious activity are:

- The user had **two failed logon attempts** from the same IP address (172.174.4.116) using Office 365 login service, before successfully logging in with the same IP address and service. This could indicate a brute force or credential stuffing attack, or a typo by the user.
 - The user had a **logon success** from a different IP address (20.231.126.12) using Office 365 cmsi service, which is a conditional access policy that requires additional verification. This could indicate a phishing or spoofing attempt, or a legitimate logon from a different device or location.
 - The user had a **logon failed** from the same IP address (20.231.126.12) using Office 365 login reprocess service, which is a service that reprocesses failed logon attempts. This could indicate a persistent or repeated attack, or a technical issue.
 - The user had **multiple logon successes** from the same IP address (172.174.4.116) using Office 365 OAuth2 authorize service, which is a service that grants access to third-party applications. This could indicate a consent phishing or malicious app attack, or a legitimate use of authorized apps.
- > How to verify

Sources

1. Microsoft Defender

 Confirm Off-target Report Pin

Summarize the incident and plot the attack chain.

Retrieving threat intelligence and summarizing ...

Type "/" or ask anything about security



Alert on compromised account and device on Contoso.com

[OneNote](#) [WMI](#) [PowerShell](#) [AMSI](#) [Kinsing](#) [Muhsitic](#)
[Sabsik](#) [Wacatac](#)
[Summary](#) [Pinned items \(5\)](#)

Alert Summary

This alert indicates that a device belonging to Devon Torres, a user of the contoso.com domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (ONENOTE.EXE) that was launched from a downloaded file (SalesLeads (1).onepkg) and its parent process (explorer.exe), as well as the device's hostname (workstation8), OS version (Windows 21H2), and risk score (High). The alert also shows the device's last seen time, external and internal IP addresses, and antivirus status. The device has a user-defined tag (ContosoDemo) and is onboarded to Microsoft Defender for Endpoint (MDATP).

Attack Steps

The account dtorres@contoso.com was involved in a series of suspicious actions on the workstation8 host, indicating a possible compromise by a malware campaign.

The following attack steps were observed:

- Malicious OneNote package file downloaded
- Malicious scripts executed via WScript.exe
- Attempted AMSI tampering and process injection
- Suspicious Microsoft Defender Antivirus exclusion and startup folder addition
- Suspicious LDAP query and process discovery
- Suspicious WMI process creation
- Suspicious PowerShell command line and script execution

Attack Details

Malicious OneNote package file downloaded

Copilot for Security in Unified SOC Platform

Intelligent context for alerts and incidents

Quickly assess emerging threats and your organization's exposure. Respond with enriched, AI-driven insights.

Rapid investigation and response

Security Copilot provides end-to-end support of analysts. From summaries of incidents and response, to assessment of incident impact, to actionable recommendations for faster investigation and remediation.

Unlock advanced SOC skills

Unlock new skills that allow analysts at all levels to complete complex tasks translating natural language to KQL or analyzing malicious scripts.

The screenshot shows the Microsoft Defender Advanced Hunting interface. The left sidebar lists various Microsoft Defender services: AlertEvidence, AlertInfo, Anomalies, ASimDnsActivity, AWSCloudTrail, AWSGuardDuty, AWSPVCFlow, EmailEvents, CloudAppEvents, DeviceFileEvents, DeviceImageLoadEvents, Change Tracking, DNS Analytics (Preview), Azure Monitor for VMs (VMConnection, Network Performance Monitor, SQL Advanced Threat Protection, SQL Vulnerability Assessment, Update Management). The main pane displays an Advanced Hunting query titled "Advanced Hunting". The query is:let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);search in (EmailUrlInfo, UrlClickEvents, DeviceNetworkEvents, DeviceFileEvents, BehaviorEntities)Timestamp between (ago(180d) .. now())and (RemoteUrl in ('domains'))or FileOriginUrl in ('domains')or FileOriginRefererUrl in ('domains')or Url in ('domains'))| project \$table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort, InitiatingProcessSHA1, InitiatingProcessAccountNameThe results table shows 8 items found, all being DeviceNetworkEvents of type ConnectionFailure from device karla.d-pc to intranet-host.cc. The timestamp for all entries is Aug 01, 2023 3:36 AM. The right side of the interface includes a "Security Copilot" panel with a query history, a status message "AI generated. Verify for accuracy.", and a "Generating query..." progress bar. A search bar at the bottom says "Describe the data you are looking for...".

Copilot for Security in Microsoft Intune

Faster response

Swiftly respond to threats, incidents and vulnerabilities with full device context and AI assisted insights and actions.

More informed outcomes

Proactively apply targeted policies and remediate endpoint issues with what-if analysis, actionable guidance and deep understanding of device, user and app status.

Simplified posture management

Quickly translate business intent into recommended and compliant configurations and policies using natural language.

The screenshot shows the Microsoft Intune interface. On the left, there's a navigation sidebar with options like Home, Dashboard, Devices (which is selected), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Devices | Configuration' and shows a table of 128 policies. The columns in the table are Policy name ↑, Platform, Policy type, and Scope tags. Below the table, there's a 'Help and support' section with links to Help and support. On the right side, there's a 'Security Copilot' sidebar. It has a header 'Sherrod DeGrippo CONTOSO' and a timestamp 'November 15, 3:55 PM'. The sidebar contains a message: 'Create a policy that blocks users from using any removable storage devices on Windows 11 laptops'. It shows the policy details: 'Here is the Intune configuration policy that blocks users from plugging in any removable storage devices on Windows 11 laptops:'. Under 'Setting ↑', it lists 'Administrative Templates' and 'System > Removable Storage Access'. It also includes a 'Create policy' button and a note 'AI-generated content may be incorrect'. At the bottom of the sidebar, there's a link 'Ask about policies ...'.

Devices | Configuration profiles

Policies Import ADMX

① Overview

+ Create ⏪ Refresh ⏴ Export ⏷ Columns Copilot

81 policies

All devices

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

Chrome OS (preview)

Linux

Device enrollment

Enroll devices

Provisioning

Windows 365

Policy

Compliance policies

Conditional access

Configuration profiles

Scripts

Remediations

Group Policy analytics

Update rings for Windows 10 and later

Feature updates for Windows 10 and later

Search ⏵ Add filters

Policy name ↑	Platform	Policy type	Last modified	Scope tags	...
[BF] HSL	iOS/iPadOS	Device features	10/23/2023, 5:50:41 AM	DEFAULT	...
Android PKCS	Android Enterprise	PKCS certificate	5/28/2023, 5:11:33 PM	DEFAULT	...
Android SCEP	Android Enterprise	SCEP certificate	5/28/2023, 5:06:43 PM	DEFAULT	...
Android Trust	Android Enterprise	Trusted certificate	5/28/2023, 4:59:38 PM	DEFAULT	...
Android VPN	Android Enterprise	VPN	5/28/2023, 5:15:30 PM	DEFAULT	...
Corp WiFi macs	macOS	Wi-Fi	5/1/2021, 6:30:25 AM	DEFAULT	...
COSU AAD Shared mode Gartner demo	Android Enterprise	Device restrictions	7/27/2021, 11:28:35 AM	DEFAULT	...
Critical OS updates	macOS	Software updates	8/30/2023, 7:57:18 AM	DEFAULT	...
Defender for Endpoint	Windows 10 and later	Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)	2/24/2022, 11:06:09 AM	DEFAULT	...
Demo BIOS Config	Windows 10 and later	BIOS configurations	4/22/2022, 12:34:38 PM	DEFAULT	...
Demo BIOS Config 1	Windows 10 and later	BIOS configurations	4/22/2022, 12:30:38 PM	DEFAULT	...
DFE Protection	macOS	Endpoint protection	4/3/2022, 10:16:56 AM	DEFAULT	...
Endpoint Analytics Data Collection	Windows 10 and later	Windows health monitoring	10/12/2022, 5:48:25 PM	DEFAULT	...
FileVault encryption	macOS	Endpoint protection	4/12/2022, 3:30:40 PM	DEFAULT	...
Hide Shutdown Button on Start Menu	Windows 10 and later	Settings catalog	9/21/2023, 4:32:29 PM	DEFAULT	...
Hide Shutdown Button on Start Menu - Amit	Windows 10 and later	Settings catalog	9/21/2023, 4:33:57 PM	DEFAULT	...
Intune data collection policy	Windows 10 and later	Windows health monitoring	8/28/2023, 4:12:33 PM	DEFAULT	...

Woodgrove

- [!\[\]\(1a4acf473171943dce648052d3e007b3_img.jpg\) Home](#)
- [!\[\]\(1c2c90de50dc63e35daef54f6124b890_img.jpg\) Dashboard](#)
- [!\[\]\(ffc95c04e6187abb17ed8a678e8b607a_img.jpg\) All services](#)
- [!\[\]\(c3d5bb317ffa2d716538e6468b3e983a_img.jpg\) Devices](#)
- [!\[\]\(47a5dad0c18bb9e9a183a82482139698_img.jpg\) Apps](#)
- [!\[\]\(a4d68b07ae2c2081a8d6a97aa658706d_img.jpg\) Endpoint security](#)
- [!\[\]\(02e631022941299c9daa6f19e7021587_img.jpg\) Reports](#)
- [!\[\]\(abb299caccc27181729264adbe10a6c3_img.jpg\) Users](#)
- [!\[\]\(caeafa4a30b89dfe5963a31b56a2a1ed_img.jpg\) Groups](#)
- [!\[\]\(b611ae3ea6b49e655a9278885782f906_img.jpg\) Tenant administration](#)
- [!\[\]\(12d5266dfb7162a7216850705b4211ca_img.jpg\) Troubleshooting + support](#)

Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

[Give us your feedback](#)

Status

Devices not in compliance

35

Configuration policies with error or conflict

10

Client app install failure

4

Connector errors

1

Service health

Healthy

Account status

Active

Spotlight



Introducing the Microsoft Intune Suite

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

[Explore](#)

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

[Explore](#)

Get more out of Intune



Microsoft Intune Blog

Discuss best practices, get the latest news, and engage in conversations around Microsoft Intune.

What's new in Microsoft Intune (2310) October edition

Security Copilot with Microsoft Intune: Early Access Program

Microsoft Intune Endpoint Privilege Management for Windows 365



Intune Customer Success

Get the deep technical knowledge to help you be successful using Intune.

Known issue: Incorrect count for onboarded Microsoft Defender for Endpoint devices report

Resolved: Intune MAM applications unresponsive on Samsung SM-G990E devices

Day zero support for iOS/iPadOS 17 and macOS 14

Documentation and training



What's new in Microsoft Intune



Features in development



Learning path: Microsoft Intune fundamentals

Copilot for Security in Microsoft Entra

Rapid identity risk investigation

Explore sign-ins and risky users, understand the 'why' and get contextualized insights on what to do to protect the accounts, all in natural language.

Faster troubleshooting

With context at your fingertips, find gaps in access policies, generate identity workflows, and get to the root of the problem faster.

New levels of efficiency

Guided recommendations allow admins at all levels to complete complex tasks such as incident investigations. Sign-in log analysis eliminates the need for manual inspection.

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation sidebar with options like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, Monitor & health, Sign-in logs (which is selected), Audit Logs, and Learn & support. The main content area is titled "Sign-in events" under "Contoso". It displays a table of sign-in logs for the last 24 hours, filtered by "User contains: Adriana Giorgi" and "Authentication requirement: Multifactor authentication". The table columns include Date, Request ID, User, Application, Status, IP address, and Location. A modal window titled "Copilot can help troubleshoot" is open over the table. In the bottom right corner of the main content area, there is a "Copilot" sidebar with a user profile for "Connie Wilson CONTOSO". The sidebar includes sections for "Security Copilot" (Preview), a question "Why was Adriana Giorgi forced to MFA?", and a list of generated content. At the bottom of the sidebar, there are buttons for "View sign-ins", "Ask a question or type / for suggestions", and a "Copilot" button.

Why was Adriana Giorgi prompted for MFA?

Copilot for Security in Microsoft Entra

Rapid identity risk investigation

Explore sign-ins and risky users, understand the 'why' and get contextualized insights on what to do to protect the accounts, all in natural language.

Faster troubleshooting

With context at your fingertips, find gaps in access policies, generate identity workflows, and get to the root of the problem faster.

New levels of efficiency

Guided recommendations allow admins at all levels to complete complex tasks such as incident investigations. Sign-in log analysis eliminates the need for manual inspection.

Create a workflow called "Government Sales Employee Onboarding" for new hire employees in the "US Government Sales" department that gives them access to the "Gov Sales" group and access package

The screenshot shows a Microsoft Copilot for Security window titled "Security Copilot Preview". The timestamp is March 16, 3:55 PM. A blue line from the text above points to the "Create a workflow" section. The workflow summary is for "Onboard new hire employees" in the "US Government Sales" department. It includes triggers on employee hire date, enabling user accounts, sending welcome emails, adding users to the "Government Sales employees" group, and requesting the "Gov sales" access package using the "Onboarding" policy. Additional customizations available include welcome emails with company branding and up to 8 additional tasks. Buttons for "Create draft" and "Customize email" are shown. Below, there's a note about AI-generated content being incorrect, a reference section (1 reference), and a section for customizing the welcome email subject header ("Welcome <username> to <tenant>"). A checkbox for "Use company branding" is present, along with a "Submit" button. Another note says the welcome email has been customized with company branding and a custom message. Finally, a section asks if the user wants to continue customizing the workflow with buttons for "Generate workflow" and "Keep customizing".

Copilot for Security in Microsoft Purview

Scaled visibility

Gain comprehensive, integrated visibility across solutions and insight into relevant compliance regulatory requirements.

Summarization for speed

Quickly summarize alerts containing a breadth of signals and lengthy content to review in the lens of data security and compliance policies.

Unlock expert skills

Receive step-by-step guidance, conduct searches in natural language, and conduct advanced investigations without keyword query language.

The image displays two screenshots of Microsoft Purview's security interface. The top screenshot shows the 'Alerts' section of the 'Insider Risk Management' blade in the Microsoft Purview portal. It details an alert titled '(7bbc3040) Data theft by departing users' with a risk score of 87/100 and a 'Confirmed' status. The alert summary indicates it was triggered on September 25, 2023, by an HR connector importing a resignation date for a user (Jane Doe). The bottom screenshot shows the 'Security Copilot' interface, which provides natural language prompts and generates Keyword Query Language (KQL) results. A prompt asks to find documents and emails where 'Reader' is within 2 words of '1.0' or 'MS Reader', or within 10 words of 'Microsoft'. The generated KQL result is: '(Author:"Mona Kane" OR Author:"Anne Keetings") OR (Sender:"Mona Kane" OR Sender:"Anne Keetings") OR (Recipients:"Mona Kane" OR Recipients:"Anne Keetings") AND ((Reader NEAR(2) "1.0") OR "MS Reader" OR (Reader NEAR(10) Microsoft) z'. A note at the bottom says 'KQL copied. Paste in the text box below'.

Copilot for Security in Microsoft Defender for Cloud

Quick understanding of posture

Identify risks faster leveraging contextual insights across sensitive data, critical vulnerabilities, lateral movement, and more.

Guided remediation

Drill down into critical risks and receive guided recommendations to prioritize remediation actions faster, all in natural language

Work smarter

Get contextual risk insights, summarized breakdowns, step-by-step guidance throughout the course of an investigation. Quickly identify key users and delegate remediation.

The screenshot displays the Microsoft Defender for Cloud Recommendations interface. On the left, a sidebar lists various security features: General (Overview, Getting started, Recommendations), Security alerts, Inventory, Security explorer, Workbooks, Community, Diagnose and solve problems, Cloud security (Secure score, Regulatory compliance, Workload protection, Data governance (Purview/Maui), Firewall manager), Management (Settings, Security solutions, Workflow automation). The main area shows 'Active recommendations by risk' with counts: Critical (48), High (55), Medium (180), Low (1297), N/A (3448). Below this is a table of recommendations:

Risk level	Title	Affected resource	Risk factors	Attack paths	Status
Critical	Management ports should be closed on your virtual machine	mdc-demo-w2022	Exposure to the internet	4	Overdue
Critical	All network ports should be restricted on network security group...	mdc-demo-w2022	Exposure to the internet	2	Overdue
Critical	API endpoints in Azure API Management should be authenticated	modify-resource	Exposure to the internet	3	Overdue
Critical	SQL databases should have vulnerability findings resolved	samplemedesdemo1	Exposure to the internet	2	Overdue
Critical	API endpoints in Azure API Management should be authenticated	submitsession	Exposure to the internet	3	Overdue
Critical	EC2 instance should use IMDSv2	mdc-demo-w2022	Exposure to the internet	1	Unassigned
Critical	EC2 instance should not have a public IP address	i-09e4cb65a0f5675ec1	Exposure to the internet	3	Unassigned
Critical	EC2 instance should not have a public IP address	i-0465c8f12mz75ec1	Exposure to the internet	3	Unassigned
Critical	EC2 instance should not have a public IP address	i-02e65438b0f5675ec1	Exposure to the internet	2	Unassigned
Critical	EC2 instance should not have a public IP address	i-03e6123ct0f5675ec1	Exposure to the internet	2	Unassigned
Critical	EC2 instance should not have a public IP address	i-15e7438d15675ec1	Exposure to the internet	3	Unassigned
Critical	EC2 instance should not have a public IP address	i-06e24380f5675ec1	Exposure to the internet	1	Unassigned
Critical	EC2 instance should use IMDSv2	i-07e65ht560f5675ec1	Exposure to the internet	3	Unassigned
Critical	Management ports of EC2 instances should be protected with...	i-01e6ty560f5675ec1	Exposure to the internet	3	Unassigned
Critical	Management ports of EC2 instances should be protected with...	i-06e34w856a5i75es3	Exposure to the internet	2	Unassigned
Critical	EC2 instance should not have a public IP address	i-01e6k3u6erf5675ec1	Exposure to the internet	2	Unassigned

The right side of the interface shows a summary of publicly exposed resources: Aug 01, 2023 11:14 AM, 13 publicly exposed resources require attention, and a detailed breakdown of specific resources at risk, including 9 VMs with internet exposure and high severity vulnerabilities, 1 AWS S3 bucket that's publicly accessible, housing sensitive data, 1 SQL with excessive internet exposure, allowing basic authentication and containing sensitive data, and 2 API endpoints lacking authentication, transmitting sensitive information. It also includes sections for 'Show results', 'AI generated. Verify for accuracy.', and 'Focus on risks to sensitive data', 'Focus on risks to critical vulnerability', and 'Focus on risks to lateral movement'.

Copilot for Security Pricing



- Provision capacity in Security Compute Units (SCU) to run Copilot for Security workloads
- 4\$ per hour per SCU
- Provisioned through Azure Portal
- Azure Subscription required

[Microsoft Copilot for Security - Pricing](#)

Usage monitoring

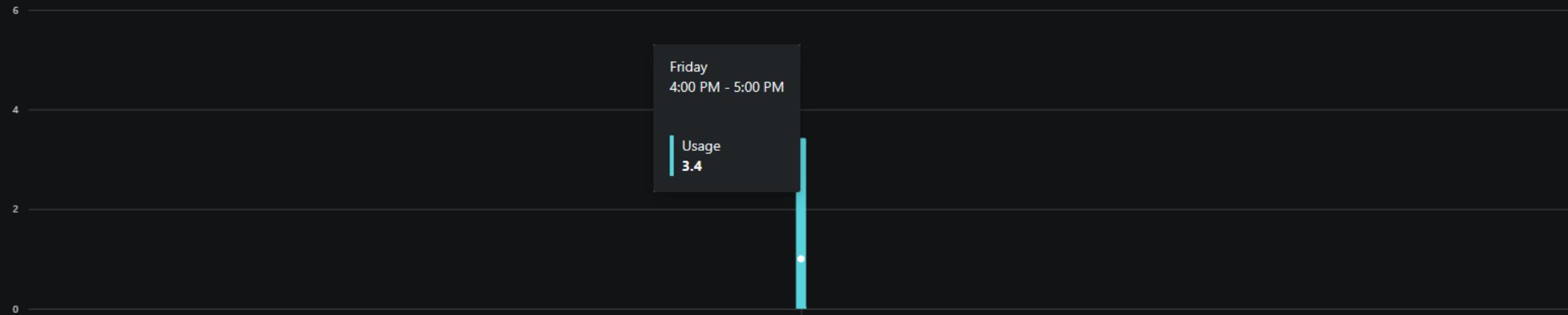
Last updated 4:59 PM

The number of security compute units available to your organization is determined by the units you have purchased per hour. Some usage beyond what you've purchased might be allowed at times. [Learn more about usage](#).

Units per hour
1 unit

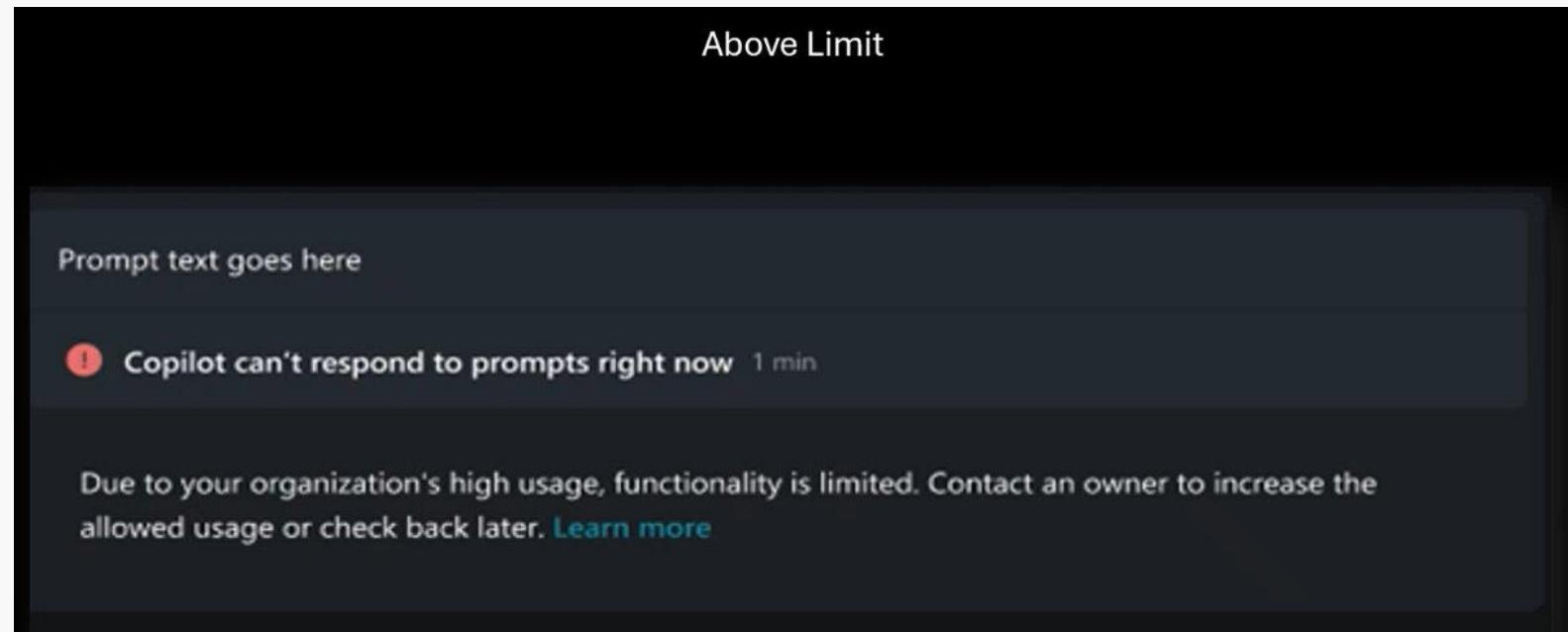
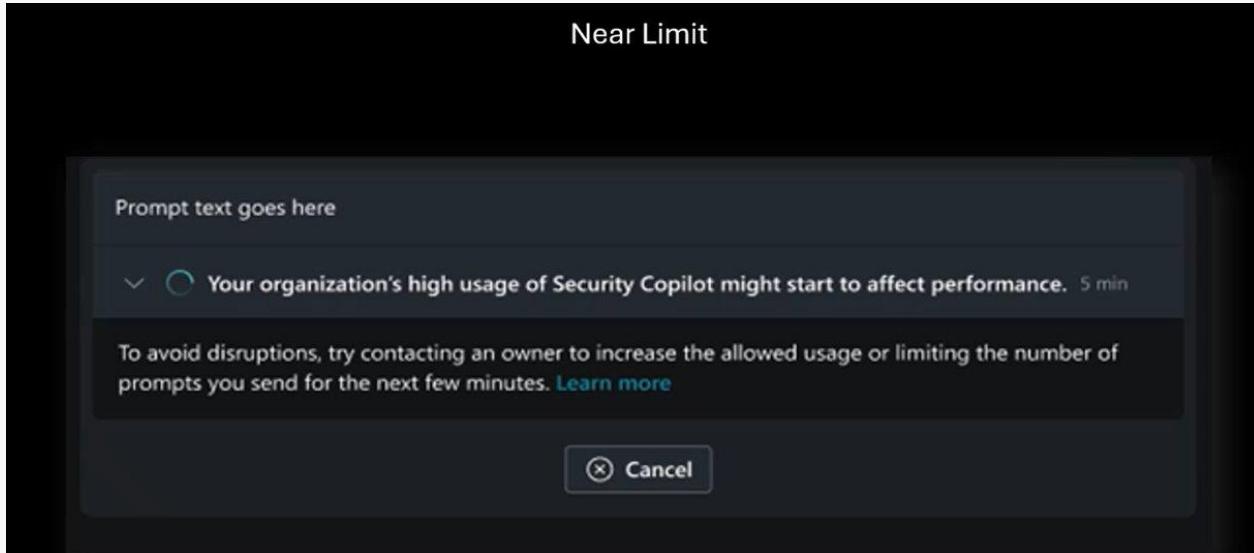
[Change](#)

Date: Last 24 hours ▾



Date	Unit usage	Unit status
Apr 12, 04:00 PM	3.4	

Near and above max capacity notifications



[**Microsoft Security Italian User Group**](#)

[**Microsoft Copilot for Security Community**](#)

[**Microsoft Copilot for Security - Github repository**](#)

[**Microsoft Copilot for Security YouTube playlist**](#)





#GlobalAzureTorino



TD SYNNEX

INTR3

PA EXPERTISE
RETELIT GROUP

TORINO