Azure Developer Community

Navigating Cyber Threats With Microsoft Security Copilot

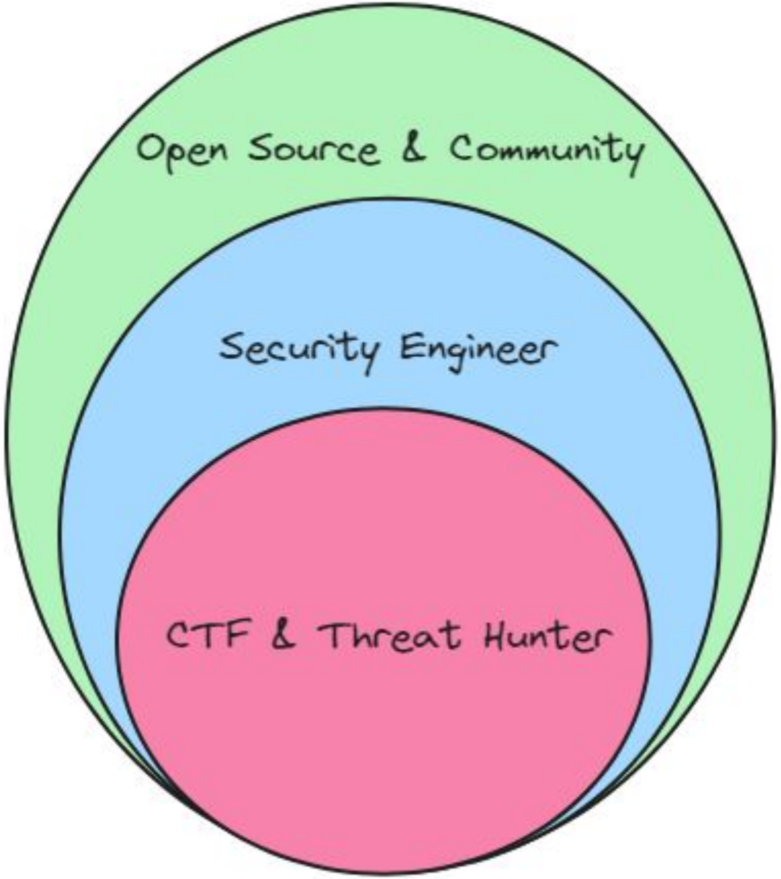
#blueteaming

$whoami

Shubhendu Shubham

“sudo rm -rf / problems”

aka Troubleshooter



CTF BADGES

Kusto Detective Gold Award

KUSTO
DETECTIVE AGENCY
2
CASE 9
AMD

KUSTO
DETECTIVE AGENCY
2
CASE 8
AMD

KUSTO
DETECTIVE AGENCY
2
CASE 7
AMD

KUSTO
DETECTIVE AGENCY
2
CASE 6
AMD

KUSTO
DETECTIVE AGENCY
2
CASE 5
AMD

KUSTO
DETECTIVE AGENCY
2
CASE 4
AMD

HACKTHEBOX
CERTIFIED BUG BOUNTY HUNTER
CBBH

TOP 30
WINNER
Azure Developer Stories
2021

HACKTHEBOX
Subject Matter Expert
SME

CERTIFICATIONS

Microsoft CERTIFIED
EXPERT

SC 100

Microsoft CERTIFIED
EXPERT

AZ 305

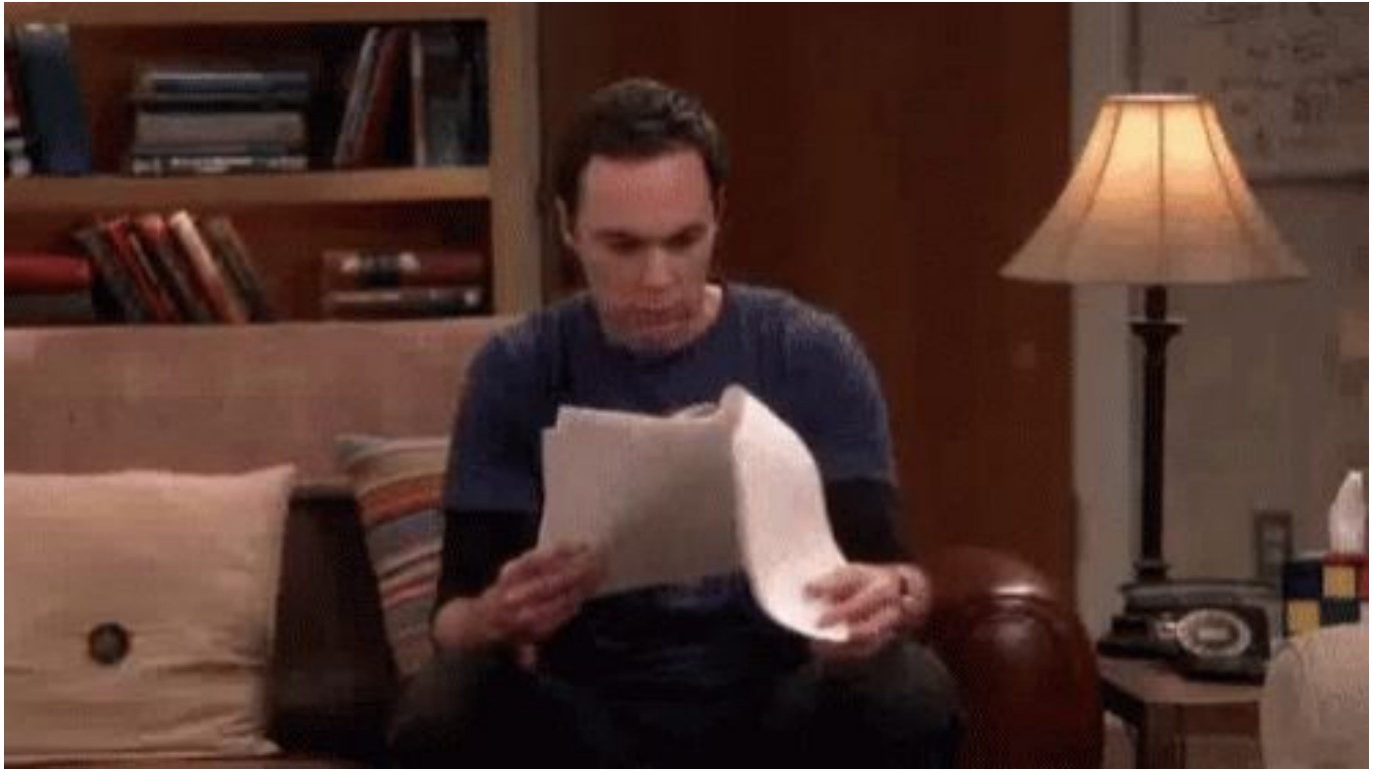
Microsoft CERTIFIED
ASSOCIATE

AZ 104

Disclaimer

"If you think technology can solve your security problems, then you don't understand the problems, and you don't understand the technology." – Bruce Schneier

Why AI in Cybersecurity?



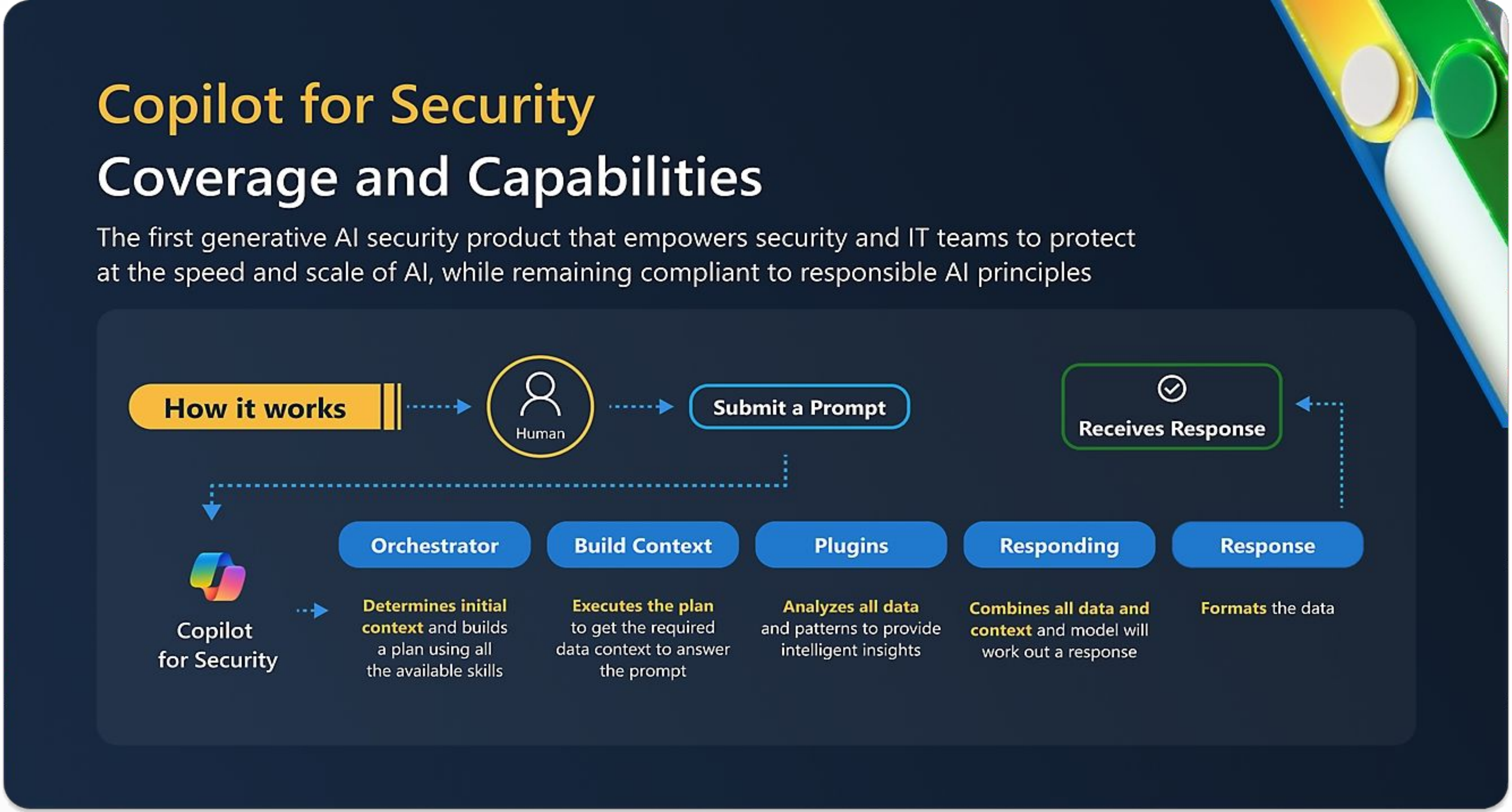
Statistics

- 4000 Password attacks per second (Year 2023) , 579(Year 2022)
- 72 minutes Median time for an attacker to access your private data if you open a phishing email
- 3.5 million Global shortage of skilled cybersecurity professionals

Source : Microsoft Digital Defence Report 2023

What is Microsoft Security Copilot ?

Microsoft Copilot for Security (Copilot for Security) is a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale.



Copilot for Security

Coverage and Capabilities

The first generative AI security product that empowers security and IT teams to protect at the speed and scale of AI, while remaining compliant to responsible AI principles

How it works → Human → **Submit a Prompt** → Copilot for Security →

Orchestrator: **Determines initial context** and builds a plan using all the available skills

Build Context: **Executes the plan** to get the required data context to answer the prompt

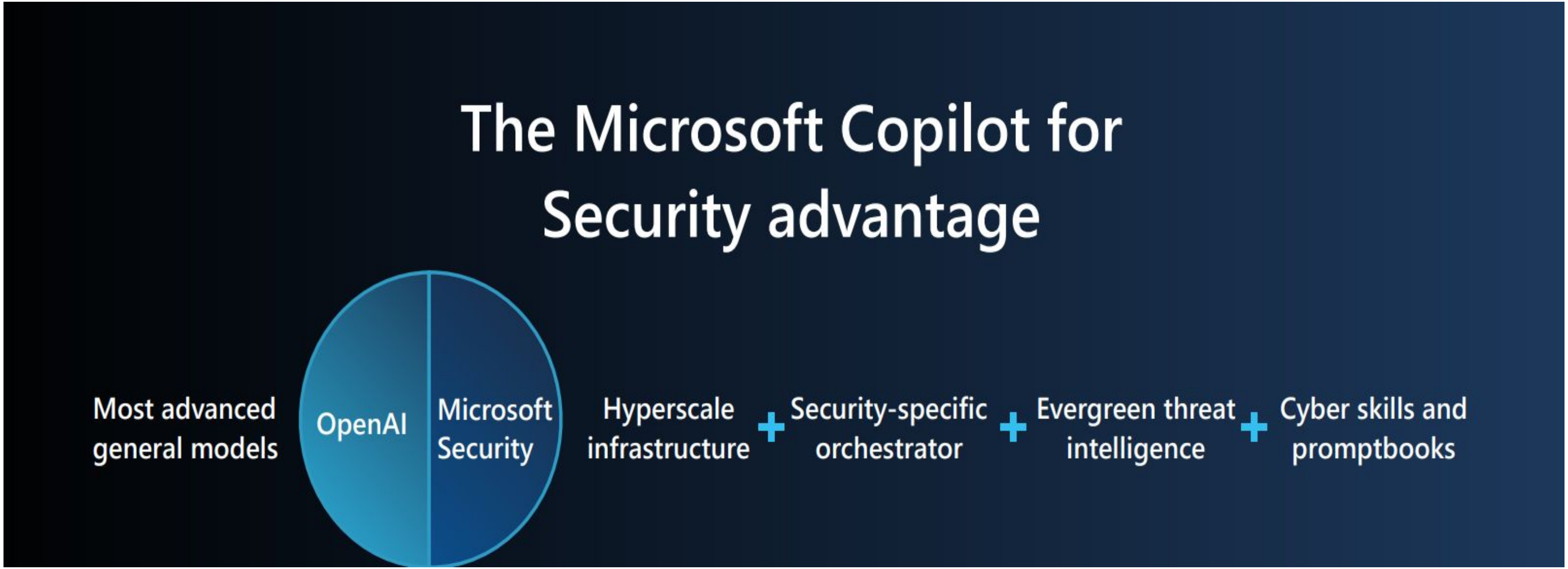
Plugins: **Analyzes all data** and patterns to provide intelligent insights

Responding: **Combines all data and context** and model will work out a response

Response: **Formats** the data

→ ✓ **Receives Response**

Source : Microsoft



The Microsoft Copilot for Security advantage

Most advanced general models

OpenAI | Microsoft Security

Hyperscale infrastructure + Security-specific orchestrator + Evergreen threat intelligence + Cyber skills and promptbooks

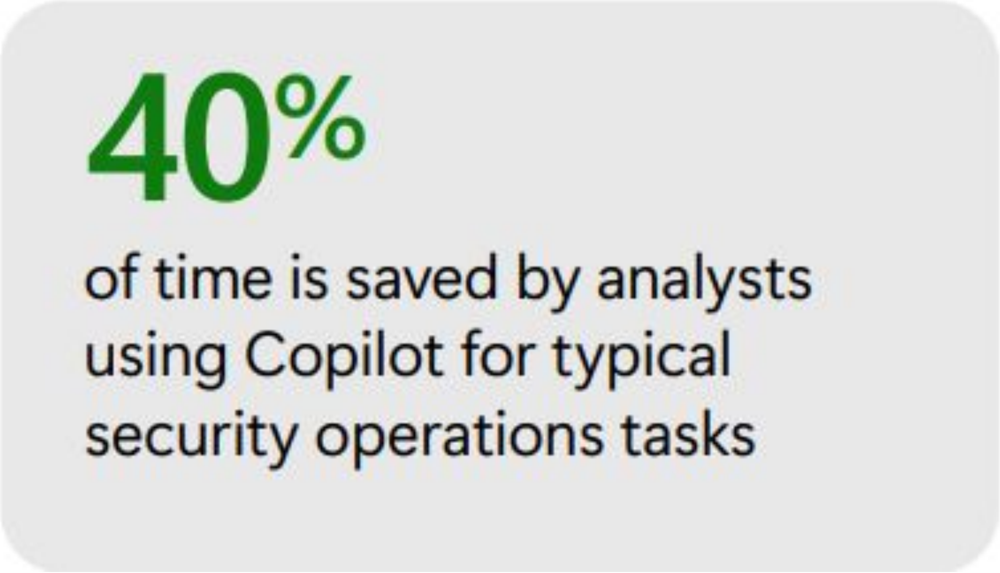
Human ingenuity and expertise will always be an irreplaceable component of defense. So we need technology that can augment these unique capabilities with the skill sets, processing speeds, and rapid learning of AI.

For Security Analysts

- ✓ Build hunting queries from natural language
- ✓ Get threat intel insights related to specific incidents
- ✓ Analyze malicious scripts with one button click
- ✓ Get remediation guidance
- ✓ Create comprehensive incident reports for leadership

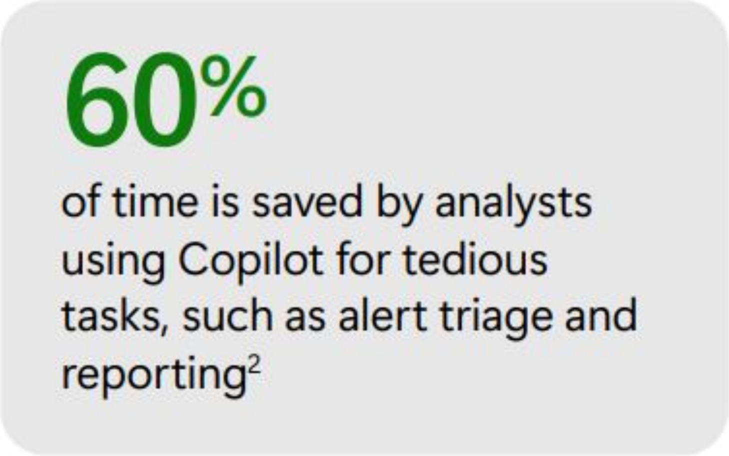
For IT admins

- ✓ Determine if a device is compliant with company's policies
- ✓ Get advice on configuring and managing new platforms
- ✓ Build new policies and test them to see how they would impact users
- ✓ Proactively identify devices that are not up to date
- ✓ Understand why MFA was triggered for a user



40%

of time is saved by analysts using Copilot for typical security operations tasks



60%

of time is saved by analysts using Copilot for tedious tasks, such as alert triage and reporting[2]

Microsoft Copilot for Security early customer data, 2023.

Platform Integration

Copilot in
Microsoft Defender XDR

Copilot in
Unified SOC Platform

Copilot in
Microsoft Purview

Copilot in
Microsoft Entra

Copilot in
Microsoft Intune

Copilot works across the Microsoft Security Stack

Debunk
Cybersecurity
AI Myths

Myth 1 : Unauthorised Data Access

Answer: No.

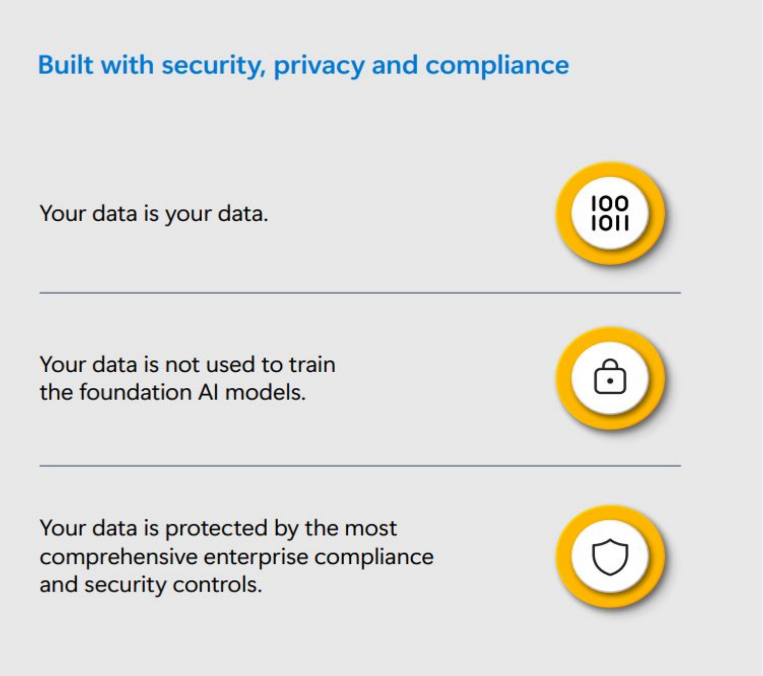
This won’t happen with Copilot because it uses ‘admin on behalf of’ rights for the user logged in. This means the rights are limited to that specific user and that user only. Copilot runs queries as the user, so it never has elevated privileges beyond what the user has.

Myth 2 : Data Privacy and Ownership

Will my customer data be used to train language models in Copilot?

Answer: No

When it comes to data, unlike ChatGPT, Copilot is grounded in the unique context of your organisation. That means when you ask Copilot any question, the answer will be based on what's happening in your organisation at that moment. Your data isn't used to train the foundation AI models. It's a closed learning loop that continuously improves based on your use



Built with security, privacy and compliance

Your data is your data.

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

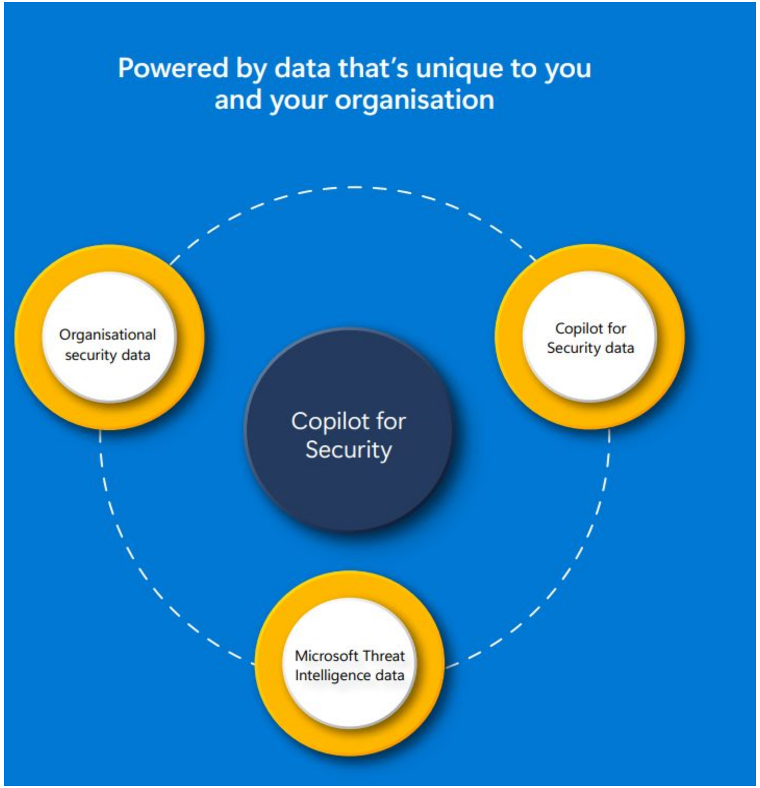
Your data is protected by the most comprehensive enterprise compliance and security controls.

Is transferred data protected from unauthorised access?

Answer: Yes.

When using Copilot for Security, your data:

- Is your data.
- Is stored where you choose and always encrypted at rest.
- Isn't used for sales or shared with third parties.
- Is housed in systems governed by Microsoft SOC and International Organisation for Standardisation-certified processes.
- Isn't used to train foundation AI models.
- Is never shared with OpenAI.
- Is protected by the most comprehensive enterprise compliance and security controls


Powered by data that's unique to you and your organisation
Organisational security data
Copilot for Security data
Copilot for Security
Microsoft Threat Intelligence data

Myth 3 : Data Leakage and Exposure

Could Copilot expose my data to others using the tool?

Answer: No

Copilot for Security was designed based on responsible AI. It includes the same security, privacy and compliance controls as other trusted Microsoft products, as well as AI-specific safety mechanisms. Your data is analysed within the Copilot system and doesn’t leave the Microsoft Azure production tenant. Per Microsoft standards, your data is encrypted in transit and at rest

Myth 4 : Compliance Issues

Does Copilot for Security meet industry or regional compliance requirements?

Answer: Yes

Copilot meets General Data Protection Regulation (GDPR) requirements for EU markets by implementing the Azure Public Preview requirements. It stores all EU customer data within the EU Data Boundary and is available in multiple languages. Copilot also provides compliance controls to help you meet business and regulatory requirements

Myth 5 : Hallucinations

Does Copilot for Security help detect hallucinations?

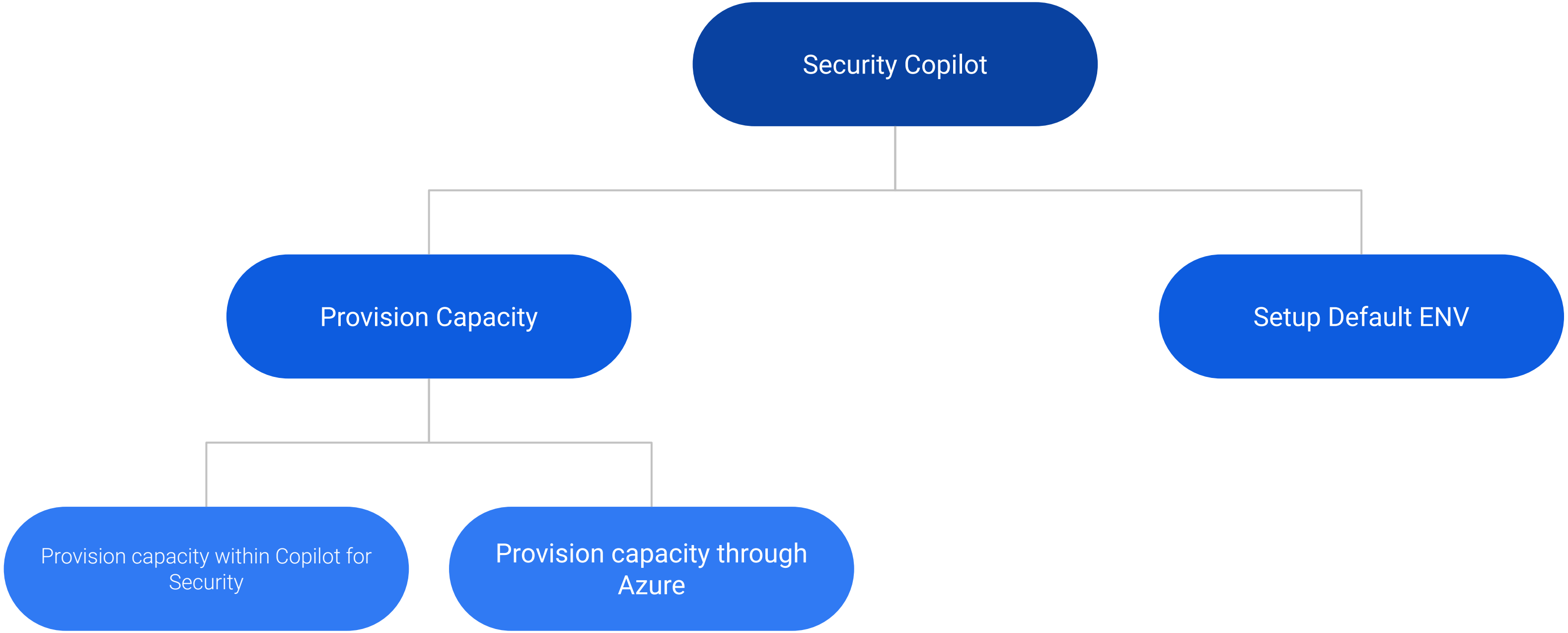
Answer : Yes

Trust is paramount in security. If you can't trust security data and insights, you can't achieve the right outcomes. For humans to confidently work with AI-powered tools such as Copilot, it's critical to build trust in the technology.

Microsoft, is committed to responsible AI, which is why Copilot is designed to:

- Show reasoning, sources, debug and runtime.
- Ensure data is compliant, secure and private.
- Address harms and hallucinations.
- Be transparent and allow for an open dialogue

Onboarding



Security Copilot

Provision Capacity

Setup Default ENV

Provision capacity within Copilot for Security

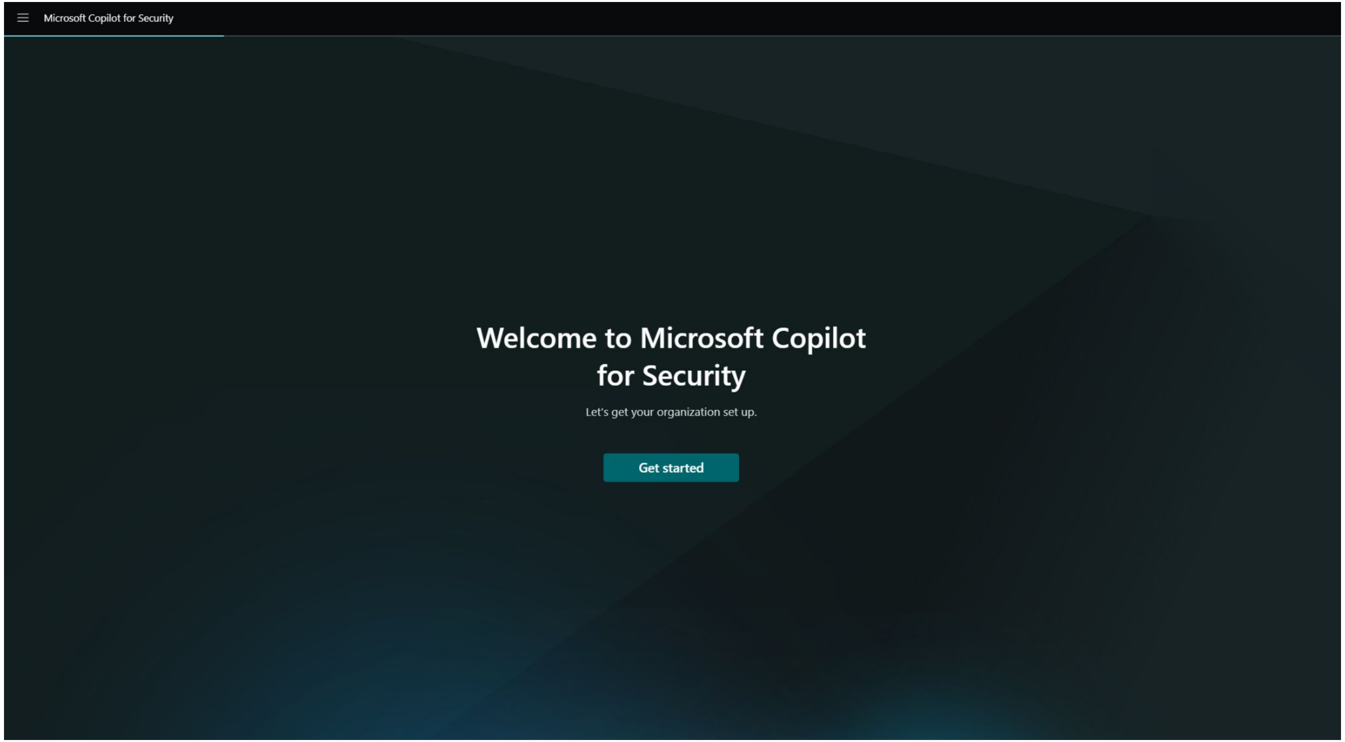
Provision capacity through Azure

Demo

Prerequisite

- Azure Subscription
- Azure subscription owner or contributor to create capacity

1. Sign in to Copilot for Security (https://securitycopilot.microsoft.com).
2. Select Get started.

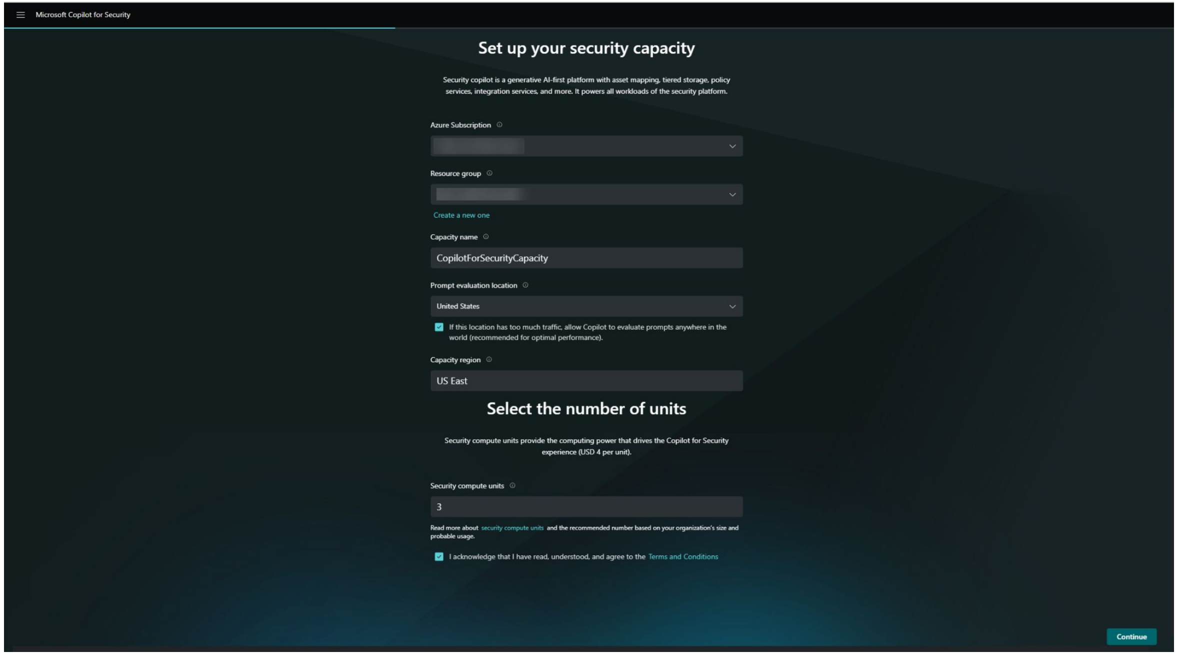


Welcome to Microsoft Copilot for Security

Let's get your organization set up.

3.Set up your security capacity:

Select the Azure subscription, associate capacity to a resource group, add a name to the capacity, select the prompt evaluation location, and specify the number of Security Compute Units (SCUs). Data is always stored in your home tenant geo.



Set up your security capacity

Security copilot is a generative AI-first platform with asset mapping, tiered storage, policy services, integration services, and more. It powers all workloads of the security platform.

Azure Subscription: [redacted]

Resource group: [redacted]

Create a new one

Capacity name: CopilotForSecurityCapacity

Prompt evaluation location: United States

☑ If this location has too much traffic, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region: US East

Select the number of units

Security compute units provide the computing power that drives the Copilot for Security experience (USD 4 per unit).

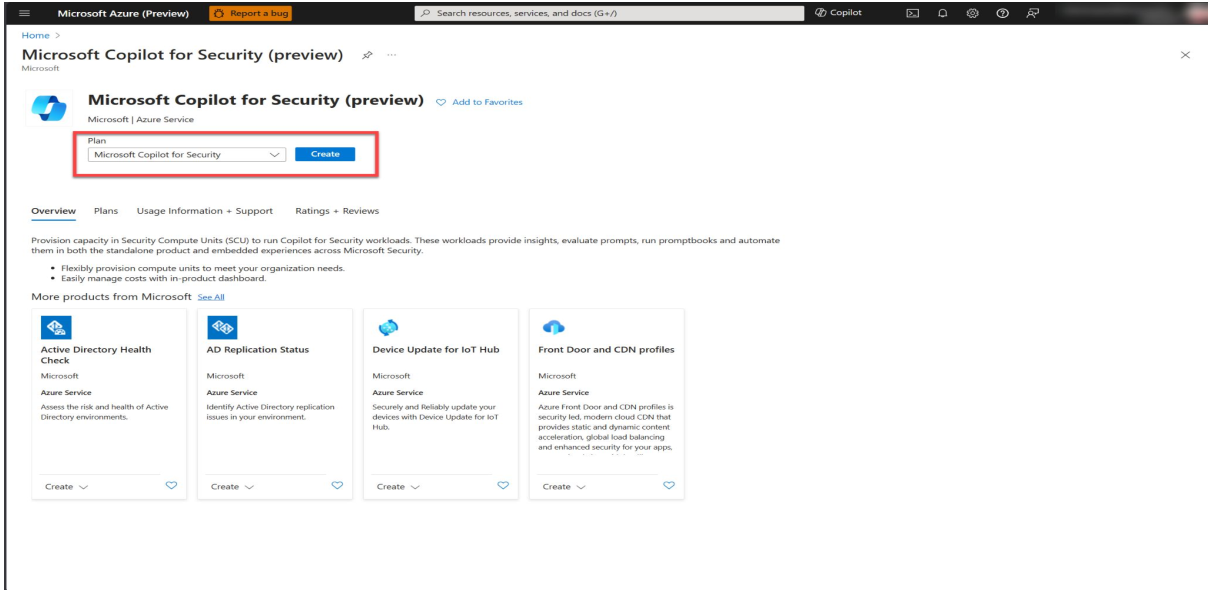
Security compute units: 3

Read more about security compute units and the recommended number based on your organization's size and probable usage.

☑ I acknowledge that I have read, understood, and agree to the Terms and Conditions

Provision capacity in Azure

1. Sign in to the Azure portal.
2. Search for Copilot for Security in the list of services, then select Copilot for Security.
3. Select Resource groups.
4. Under Plan, select Microsoft Copilot for Security. Then select Create.



Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Copilot
Home >

Microsoft Copilot for Security (preview)

Microsoft

Microsoft Copilot for Security (preview)

Microsoft | Azure Service

Plan: Microsoft Copilot for Security

Create
Overview
Plans
Usage Information + Support
Ratings + Reviews

Provision capacity in Security Compute Units (SCU) to run Copilot for Security workloads. These workloads provide insights, evaluate prompts, run promptbooks and automate them in both the standalone product and embedded experiences across Microsoft Security.

- Flexibly provision compute units to meet your organization needs.
- Easily manage costs with in-product dashboard.

More products from Microsoft

Active Directory Health Check
Microsoft
Azure Service
Assess the risk and health of Active Directory environments.

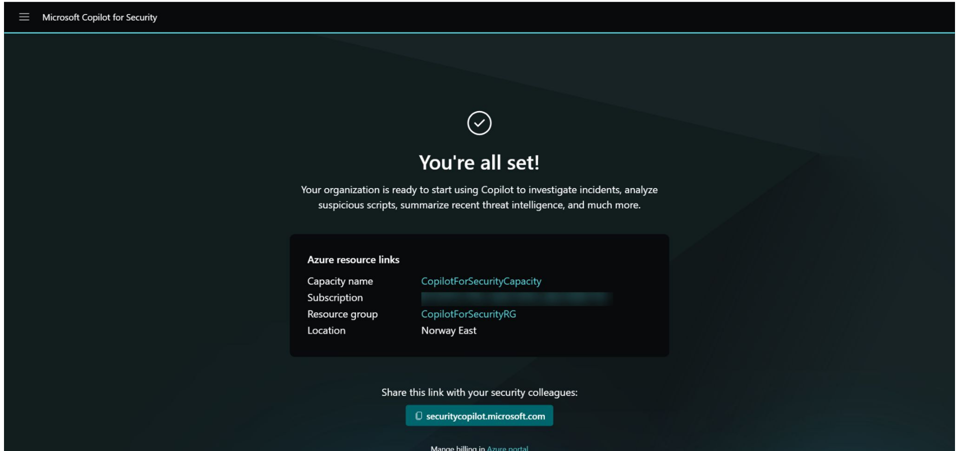
AD Replication Status
Microsoft
Azure Service
Identify Active Directory replication issues in your environment.

Device Update for IoT Hub
Microsoft
Azure Service
Securely and Reliably update your devices with Device Update for IoT Hub.

Front Door and CDN profiles
Microsoft
Azure Service
Azure Front Door and CDN profiles is security led, modern cloud CDN that provides static and dynamic content acceleration, global load balancing and enhanced security for your apps,

Set up Default environment

1. Associate your capacity to the Copilot for Security environment if the capacity was created in the Azure portal.
2. You're informed where your Customer Data will be stored. Select Continue.
3. Select among the data sharing options. Select Continue. For more information on data sharing, see Privacy and data security.
4. You'll be informed of the default roles that can access Copilot for Security. Select Continue.
5. A confirmation page is displayed. Select Finish



You're all set!

Your organization is ready to start using Copilot to investigate incidents, analyze suspicious scripts, summarize recent threat intelligence, and much more.

Azure resource links

Capacity name	CopilotForSecurityCapacity
Subscription	[redacted]
Resource group	CopilotForSecurityRG
Location	Norway East

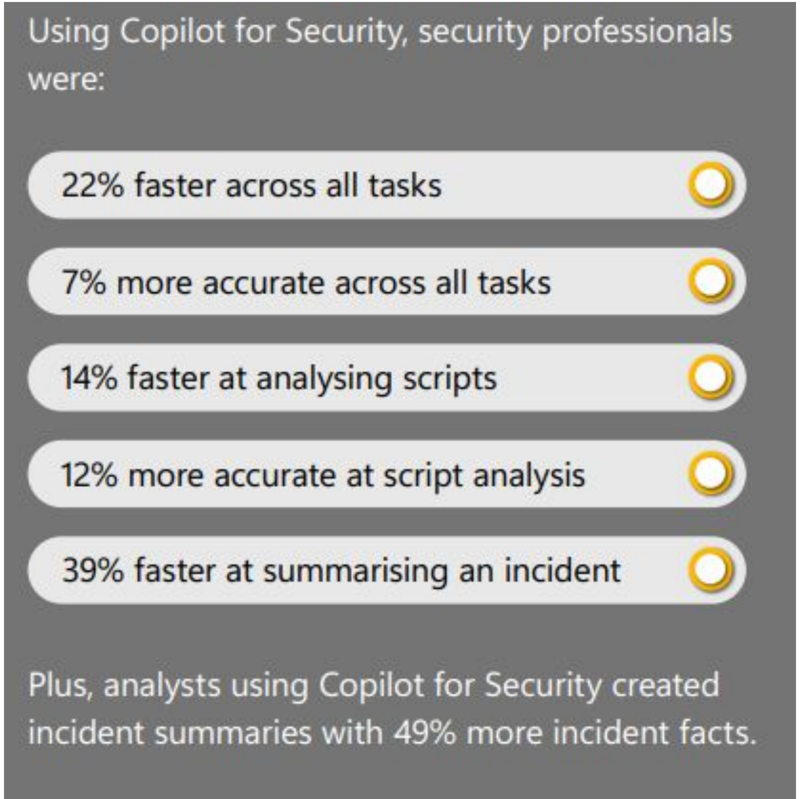
Share this link with your security colleagues:

Mange billing in Azure portal

Wanna become Security Copilot Ninja

How to Become a Microsoft Copilot for Security Ninja: The Complete Level 400 Training

Give your security team an edge with Industry-leading Generative AI



Using Copilot for Security, security professionals were:

- 22% faster across all tasks
- 7% more accurate across all tasks
- 14% faster at analysing scripts
- 12% more accurate at script analysis
- 39% faster at summarising an incident

Plus, analysts using Copilot for Security created incident summaries with 49% more incident facts.

References

1. **aka.ms/CopilotForSecurityGithub**
2. Microsoft Copilot for Security | Microsoft Security

What's Next ?

MITRE's D3FEND

This is not Phishing QR , It's my Linkedin

Don't Trust

Always verify

Thank You !

Azure Developer Community

Microsoft

ReskillI