

Microsoft Security

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



Submit a prompt

Receives response



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

Responding Combines all data Response

Formats the data

and patterns to and context and provide intelligent the model will work insights out a response

technology that can augment these unique capabilities with the skill sets, processing speeds, and rapid learning of AI.

Human ingenuity and expertise will always be an irreplaceable component of defense. So we need

Build hunting queries from natural language

For Security Analysts

- Get threat intel insights
- related to specific incidents Analyze malicious scripts with
- one button click Get remediation guidance
- incident reports for leadership

Create comprehensive

Determine if a device is compliant with company's policies

For IT admins



- 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

Security advantage_ Hyperscale Security-specific Evergreen threat nfrastructure orchestrator intelligence Microsoft infrastructure

The Microsoft Copilot for

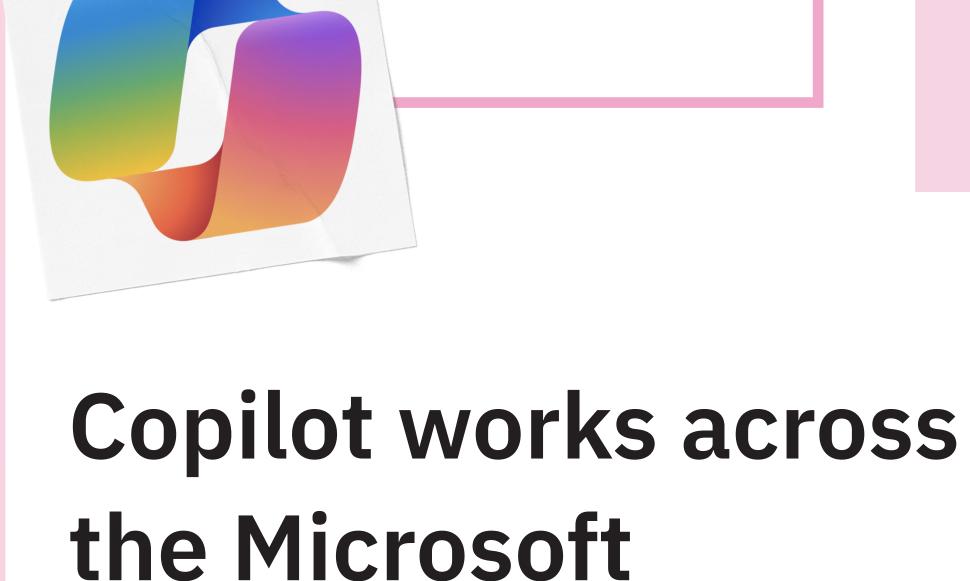


Most advanced

general models

OpenAI

Security



Security Stack_ Microsoft is in a unique position to transform security for our customers, not only because of our investments in AI, but also because we offer end-to-end security, identity,

compliance, and more across our

portfolio. We can cover more threat

vectors and deliver value with a coordinated experience.

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot for Security itself,

with all use cases in one place,

Experiences to meet you

where and how you work

enabling enriched cross-product guidance.

Standalone

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

familiar with.



Summarize an incident, assess its impact,

provide actionable recommendations for faster investigation and remediation, and, lastly, generate a post-response activity report.

Upskill security talent Unlock new skills that allow analysts at all

levels to complete complex tasks like

threat hunting, reverse engineering of malware, and more. Assess risks with AI-driven threat intelligence

Inquire in natural language about emerging

threats and your organization's exposure

and gain contextualized insights for rapid response to new and evolving threats.

Microsoft Purview

Copilot 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.

Security Copilot provides end-to-end support of analysts. From summaries of

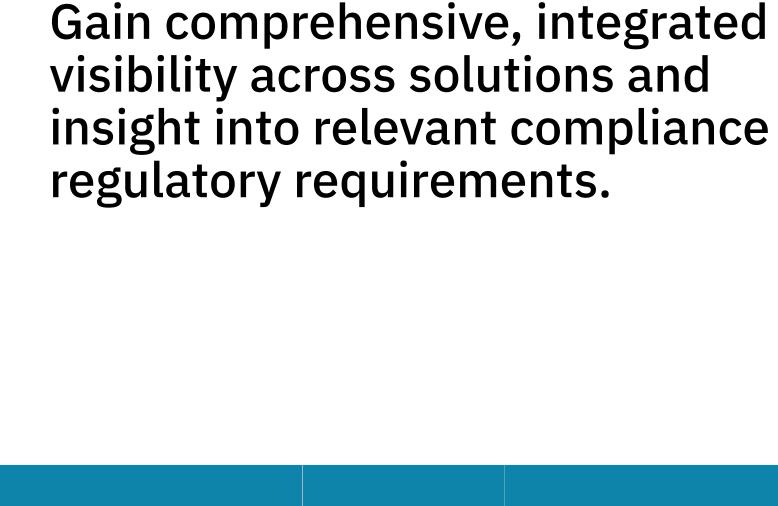
Unlock advanced SOC skills

Rapid investigation and response

incidents and response, to assessment of incident impact, to actionable recommendations for faster investigation and remediation.

all levels to complete complex tasks translating natural language to KQL or analyzing malicious scripts.

Unlock new skills that allow analysts at



Copilot in

Scaled visibility

language.

Copilot in

Rapid identity risk investigation Explore sign-ins and risky users,

protect the accounts, all in natural

contextualized insights on what to do to

Microsoft Entra_

understand the 'why' and get

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

such as incident investigations. Sign-in log analysis eliminates the need for manual inspection.

Subjects with

Copilot were

New levels of efficiency

problem faster.

faster

Analysts using

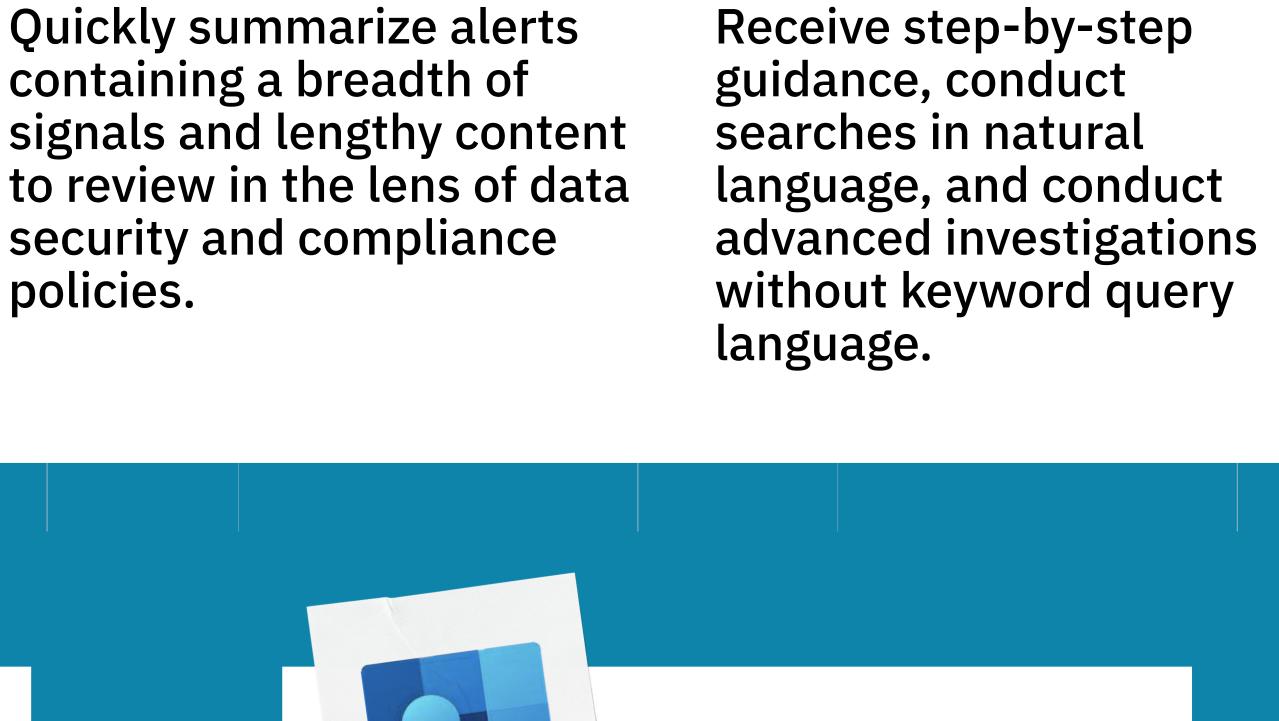
Security were

Copilot for

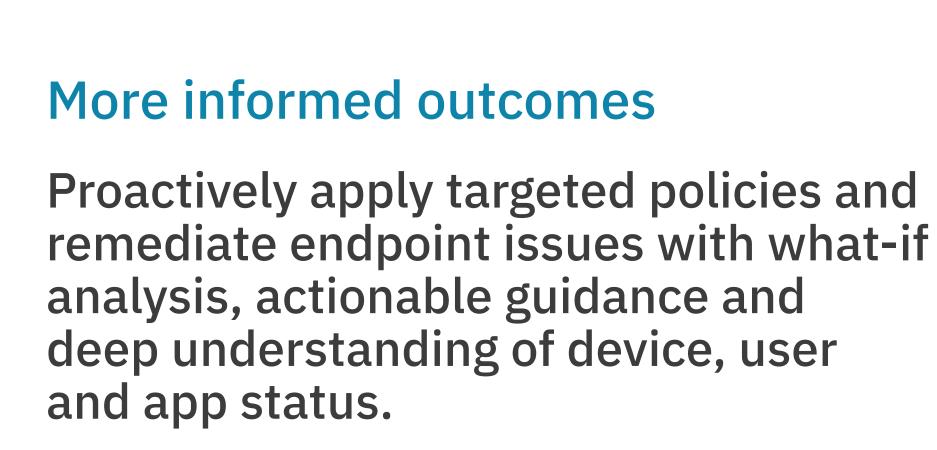
job.

Guided recommendations allow admins

at all levels to complete complex tasks



Unlock expert skills



Copilot in

Faster response

Microsoft Intune_

Swiftly respond to threats, incidents and

vulnerabilities with full device context

and AI assisted insights and actions.

Summarization for speed

containing a breadth of

security and compliance

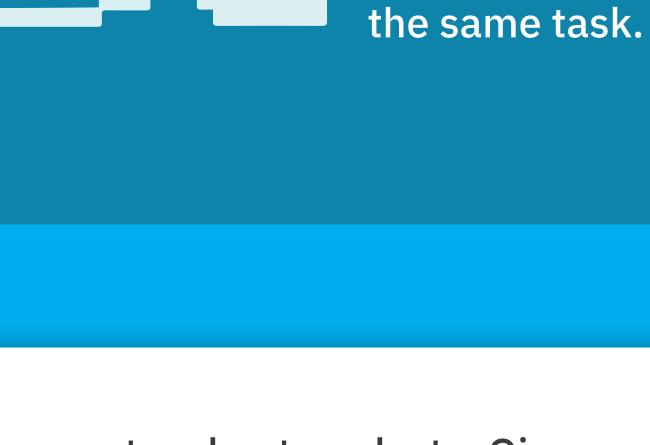
policies.

Simplified posture management Quickly translate business intent into

language.

configurations and policies using natural

recommended and compliant



of participants said

they want Copilot

next time they do

a quick snapshot of Copilot gains.

more acurate across all tasks Do a side by side challenge with your two best analysts. Give one

of them Copilot and compare results for time and accuracy to get

Ask a new hire to use copilot and your integrated knowledge base

incident? You can sample work output on similar cases with/

big enough, you can start to look at trends.

without Copilot and score them for quality. If the sample size is

to measure your own ROI Measure your team metrics for the 6 months prior to using

Ideas on how

Copilot against the metrics for your first 6 months of full team usage. Top metrics to Compare would be:

- Incidents worked per day **Average incident**
- resolution time

(MTTR)

to ramp up and provide an assessment of value at 90 days on the Measuring the quality of work is hard. Are you finding more attack details and documenting them more accurately in the

Measure the joy Copilot gives your analysts and admins. It won't have an immediate effect on your ROI, but if they like using Copilot better and are more satisfied with their work experience, the long-term benefits to your team can be considerable (Happy analysts=better work environment=less attrition and better long-term success)."