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

Human → Submit a prompt → Copilot for Security → Orchestrator → Build Context → Plugins → Responding → Response → Receives response

- **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 the model will work out a response
- **Response**: Formats the data

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

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

Copilot works across the Microsoft 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.

Experiences to meet you where and how you work

Standalone

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

Embedded

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

Copilot in Microsoft Defender XDR

Investigate and respond to threats in a guided experience

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.

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.

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.

Copilot 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.

Copilot 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.

Copilot 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.

Subjects with Copilot were **25%** faster

97% of participants said they want Copilot next time they do the same task.

Analysts using Copilot for Security were **7%** more accurate across all tasks

Microsoft Copilot for Security commissioned a survey of 38 US cyber professionals (security analysts, analysts, security engineers, security officers, and chief information officers), January 2024.

Ideas on how to measure your own ROI

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

- Mean time to respond (MTTR)
- Incidents worked per day
- Average incident resolution time

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 a quick snapshot of Copilot gains.

Ask a new hire to use copilot and your integrated knowledge base to ramp up and provide an assessment of value at 90 days on the job.

Measuring the quality of work is hard. Are you finding more attack details and documenting them more accurately in the incident? You can sample work output on similar cases with/without Copilot and score them for quality. If the sample size is big enough, you can start to look at trends.

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)."

Learn more: aka.ms/CopilotForSecurity

© Copyright Microsoft Corporation. All rights reserved.