

Microsoft Security Copilot 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



Security Copilot

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

Security Copilot offers AI-driven guidance and analysis across identities, devices, data, clouds, and apps. It helps teams across the entire security stack catch what others miss, respond faster, and strengthen team expertise.

For security analysts



- ✓ Distill complex security alerts into concise, actionable summaries
- ✓ Receive actionable step-by-step guidance for incident response
- ✓ Analyze malicious scripts quickly and translate them to natural language with clear explanations
- ✓ Use AI-driven analytics to assess the potential impacts of security incidents

For IT admins



- ✓ Leverage assisted troubleshooting and root cause mapping
- ✓ Identify policy conflicts
- ✓ Drafting KQL queries to get real time device insights
- ✓ Policy creation guidance and summarization
- ✓ Optimize cloud PC performance
- ✓ Streamline update management

For data security admins



- ✓ Uncover, manage and act on hidden risk
- ✓ Analyze incidents deeper and more efficiently
- ✓ Discover protection gaps and streamline controls
- ✓ Expedite data security investigations
- ✓ Explore AI-powered guidance to empower teams

For identity admins



- ✓ Get AI-driven risk detection, insights, and mitigation
- ✓ Troubleshoot access failures during critical access attempts
- ✓ Manage least-privileged access for enhanced security
- ✓ Assisted incident investigation and troubleshooting

For TI analysts



- ✓ Summarize and contextualize threat intelligence
- ✓ Map threat intelligence to MITRE ATT&CK® framework
- ✓ Understand the threats most critical to your organization
- ✓ Find all threat intelligence related to an indicator or artifact
- ✓ Use promptbooks for a guided experience with common investigation workflows

For CISOs



- ✓ Summarize and contextualize threat intelligence
- ✓ Create a report on the state of your organization's security posture
- ✓ Build custom security plans optimized for the organization
- ✓ Prioritize critical security incidents
- ✓ Assess team performance

The Security Copilot advantage



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 Security Copilot 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.

Security Copilot product integrations



Unified SOC platform

Outpace cyberthreats with XDR and SIEM, all in one platform.



Microsoft Sentinel

Collect security data and correlate alerts from virtually any source with intelligent security analytics.



Microsoft Intune

Mitigate cyberthreats to devices, protect data, and improve compliance across clouds.



Microsoft Defender Threat Intelligence

Understand cyberthreats and expose suspicious infrastructure with threat intelligence—including with Copilot.



Microsoft Entra

Help protect any identity and secure access to any resource with one family of solutions.



Microsoft Purview

Secure and govern your data at machine speed and scale of AI.



Microsoft Defender External Attack Surface Management

See your rapidly changing, global external cyberattack surface in real time.



Microsoft Defender for Cloud

Understand multicloud risk and get remediation recommendations.



Microsoft Defender XDR

Help prevent and detect cross-domain cyberattacks at the speed of AI.



Security Copilot randomized controlled trial (RCT) with experienced security analysts conducted by Microsoft Office of the Chief Economist, January 2024.

Ideas on how to measure your own ROI

Measure your team metrics for the six months prior to using Copilot against the metrics for your first six 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)."