

Protect at the speed and scale of AI



While navigating the ever-changing cyberthreat landscape is difficult, organizations also face security challenges from within:

90%

of organizations report having one or more skills gaps on their cybersecurity team¹

4400+

alerts received daily by an average security operations center (SOC)²

76

average number of tools used by an organization to manage their cybersecurity³

Leverage generative AI for cybersecurity

Microsoft Security Copilot is a generative AI-powered assistant for daily operations in security and IT. Security Copilot empowers teams to manage and protect at the speed and scale of AI by turning global threat intelligence, industry best practices, and organizations' data from Microsoft and partner tools into tailored insights to respond faster, catch what others miss, and strengthen team expertise.

Catch what others miss

Security Copilot not only summarizes security and IT data, but it also offers guidance and analysis to help teams detect risks via the Microsoft Threat Intelligence plugin that might otherwise be missed.

Respond faster

Security Copilot reduces time to resolution by putting critical guidance and context at teams' fingertips to respond in minutes instead of hours or days.

Strengthen team expertise

Security Copilot's natural language interface enables junior staff to perform more advanced tasks and streamlines work for expert staff to focus on the hardest challenges.

Explore how Security Copilot saves time and improves your team's effectiveness—no matter their skill level

30%

reduction in mean time to resolution with Security Copilot⁴

- ✓ **Write Kusto Query Language (KQL) queries with natural language**
Save time by eliminating the need to manually write or translate queries into complex coding language.
- ✓ **Generate incident reports in minutes**
Summarize security incidents and investigations in shareable, customizable reports.
- ✓ **Troubleshoot IT issues efficiently**
Synthesize relevant information rapidly and receive actionable insights to identify and resolve IT issues quickly.
- ✓ **Outsmart sophisticated scripts**
Gain context for incidents to quickly triage complex security alerts into actionable summaries and remediate quicker with step-by-step response guidance.
- ✓ **Accelerate cyberthreat hunting**
Build hunting queries in natural language to quickly identify and investigate suspicious behavior or compromised devices.
- ✓ **Explore risks and manage posture**
Get a broad picture of your environment with prioritized risks to uncover opportunities to improve security posture easily.

Reduce burnout and retain skilled talent

Free your team to concentrate on strategic, high-impact work when you automate tedious, menial tasks.

From	To
Overwhelmed	Strategic
Reacting to threats	Anticipating threats
Slow, manual tasks	Streamlined, automated tasks
Alert and data fatigue	Real-time analysis and triage
Steep learning curve for new analysts	Guided instructions for complex tactics
Ambiguity across complex security stacks	Clarity and actionable insights

A recent Forrester study⁵ surveyed SecOps decision makers and found significant improvements in security operations. Respondents reported significantly increased productivity in their SecOps teams, with average time savings of:

47%

in suspicious script analysis

41%

in summarizing alerts and incidents

39%

in preparing reports

Here's what Security Copilot customers are saying:

"I'm finding that I can ask Microsoft Security Copilot about attack factors that I've never seen before and get answers much faster. That helps me to make a better decision and respond faster to an attacker."

-David Yates, Senior Cybersecurity Analyst, Eastman

"As early adopters of Microsoft Security Copilot, we can report up to 40 percent time savings and 60 percent increased efficiency for our security teams, regardless of their level of expertise."

-James Eduard Andaya, Security Operations Team Lead, QNet

"We once had the ability to detect incidents in the timescale of weeks. Now, we detect things in a matter of minutes."

-David McMorries, Chief Information Security Officer, Oregon State University

Maximize your IT team's impact

In addition to security teams, IT teams are also challenged with protecting organizations from increasingly sophisticated cyberattacks across a variety of tools and devices. In a study⁶ of the impact of Security Copilot for IT administrators, users experienced:

47%

increase in accuracy for sign-in troubleshooting

36%

increase in accuracy for device policy management

25%

increase in accuracy for device troubleshooting

[Learn more about Security Copilot >](#)

Get ready to protect with Security Copilot

Learn more and access resources to unify your security operations (SecOps) across prevention, detection, and response with an AI-powered platform.

[Explore AI-powered Unified SecOps Platform | Microsoft Security >](#)

¹2024 ISC2 Cybersecurity Workforce Study

²Research Report: 2023 State of Threat Detection

³Organizations Now Have an Average 76 Security Tools to Manage - Infosecurity Magazine

⁴Generative AI and Security Operations Center Productivity: Evidence from Live Operations

⁵New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot - Forrester

⁶Randomized Controlled Trials for Security Copilot for IT Administrators