Microsoft Security

Microsoft Security Copilot

Safeguards for the Age of AI

Contents

Elevating security operations with generative AI

Cybersecurity has never been easy – especially now, when security and IT teams face the increasing speed and scale of cyberattacks, complicated by intensifying state-sponsored threats, continued regulatory uncertainty and a growing array of disparate tools and solutions for addressing it all.

On average, security organisations rely on 80 different tools to oversee their environments, leading to a deluge of data, alert fatigue and limited visibility across security solutions. Compounding these challenges is a significant skills gap, making it even harder for teams to effectively protect their systems and data.

Complex and fragmented tooling[1]

80

average number of tools used by an organisation to manage their cybersecurity

Immense data volume[2]

1K+

alerts received daily by an average security operations centre (SOC)

Shortage of security expertise[3]

92%

of organisations report having skills gaps

Despite such a daunting landscape, there is a reason for optimism. The possibilities offered by generative AI, embodied in Microsoft Security Copilot, provide a powerful opportunity to level the playing field.

[1] 'Microsoft Copilot for Security: The Right Tool at the Right Time', Microsoft, 2024
[2] 'Microsoft Copilot for Security: The Right Tool at the Right Time', Microsoft, 2024
[3] 'ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce 2023', page 20, ISC2, 2023

Security Copilot is a generative AI-powered assistant

It streamlines manual, labour-intensive processes and empowers even junior staff members with advanced capabilities. With this technology, organisations can operate more efficiently, respond more effectively and ultimately protect their environments with greater confidence and ease.

In the content that follows, we'll show how the advanced generative AI capabilities of Security Copilot empower teams to address some of the most pressing challenges in cybersecurity today by:

- Simplifying the **complex and fragmented tooling** problem by integrating and streamlining the security ecosystem.
- Addressing the **immense data volume** problem with intelligent data processing and analysis.
- Bridging the expertise gap by **empowering all levels of staff** with AI-assisted capabilities.

More than just a tool, Security Copilot is a comprehensive strategy for integrating AI into every facet of daily operations in security. This approach can transform how you manage security challenges, helping your organisation shift from a reactive stance to a proactive one, and helping you stay resilient in an increasingly complex threat environment.

Chapter 1

Catch what others miss

Threat signals and security alerts create noise that can conceal attackers. Security Copilot enables teams to analyse real-time threat signals and their organisation's data to cut through the noise, detect threats before they cause harm and reinforce security posture.

Improved threat detection

Security Copilot helps analysts identify and document more critical details during incident analysis tasks. With the assistance of AI, analysts can better capture essential information that might be hidden within large datasets, which directly enhances their ability to detect and understand threats.

49% higher content scores[4]

Security professionals achieve 49% higher content scores on incident summaries when working with Security Copilot.

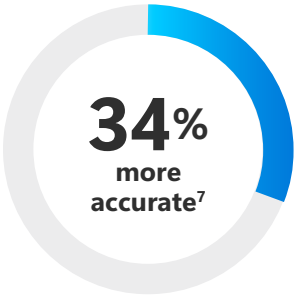
Security Copilot also helps analysts produce higher-quality writing – up to 10% better in terms of accuracy and inclusion of key facts.[5]
For example, in a test where summaries were evaluated for 15 essential facts, those written with Security Copilot included more of these critical details, leading to more accurate and actionable reports.

[4] 'Randomised Controlled Trial for Copilot for Security', page 5, Microsoft, January 2024
[5] 'Randomised Controlled Trial for Copilot for Security', page 5, Microsoft, January 2024

Outsmart sophisticated scripts

Traditional methods for analysing the complex scripts of a modern cyberattack require a high level of expertise. Security Copilot makes the process easier by using generative AI to analyse and reverse-engineer these scripts to identify malicious intent and provide step-by-step remediation guidance.

Experienced security professionals are 12% more accurate with script analysis when working with Security Copilot.



New-in-career security professionals are 34% more accurate with script analysis when working with Security Copilot.

This capability is crucial in bridging the skills gap, as it allows junior analysts to perform at a higher level without the need for extensive training.

Superior responses

Security Copilot leverages generative AI to offer step-by-step remediation guidance tailored to the specific context of an incident. This allows security teams to respond more accurately and swiftly, ensuring threats are addressed before they can escalate.

43% more accurate[8]

Security professionals are 43% more accurate on remediation tasks when working with Security Copilot.

[6] 'Randomised Controlled Trial for Copilot for Security', page 4, Microsoft, January 2024
[7] 'Randomised Controlled Trial for Copilot for Security', page 9, Microsoft, January 2024
[8] 'Randomised Controlled Trial for Copilot for Security', page 9, Microsoft, January 2024

Chapter 2

Outpace adversaries

During security incidents, every minute counts. Security Copilot puts critical guidance and context at security teams' fingertips so they can respond to incidents in minutes instead of hours or days.

Address security incidents swiftly

Without AI assistance, the process of triaging alerts and generating incident reports can be time consuming and prone to errors. An AI assistant quickens the process and makes outputs more accurate. Security Copilot integrates data from various sources and helps users present clear, actionable reports in a fraction of the time typically required.

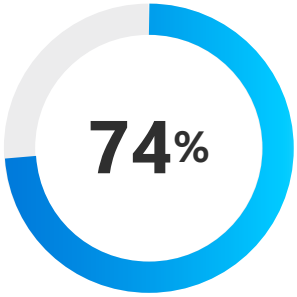
22% **faster overall task completion**[9]

Overall, security professionals complete tasks 22% faster when assisted by Security Copilot.*

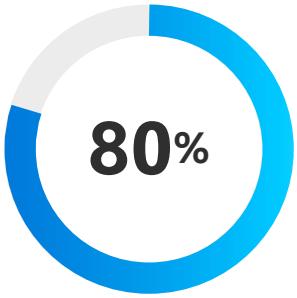
* This finding resulted in part from them finishing analysing scripts 14% faster, analysing incident reports 19% faster and completing incident summarisation tasks 39% faster, as detailed on the following page.

38 **minutes saved on average**

Security Copilot users say working with generative AI assistance helps them save 38 minutes on average.



say using Copilot makes them feel more effective.[10]



say using Copilot makes them feel more productive.[11]

[9] 'Randomised Controlled Trial for Copilot for Security', page 14, Microsoft, January 2024
[10] 'Randomised Controlled Trial for Copilot for Security', page 14, Microsoft, January 2024
[11] 'Randomised Controlled Trial for Copilot for Security', page 14, Microsoft, January 2024

Minimise the time adversaries have to exploit vulnerabilities

Analysing scripts is tiresome work. After reviewing line after line of code, an analyst might miss a detail that could reveal a potential threat. Security Copilot streamlines this task by using AI to quickly identify malicious elements within scripts.

14% **faster overall task completion**[12]

Security professionals analyze scripts 14% faster when assisted by Security Copilot.

Providing critical information to speed decision-making and response

Comprehensive and precise incident reports are essential for understanding the nature, impact and response to security incidents, but the process of preparing them can be time consuming. Security Copilot helps analysts with data, formatting and organisation so they can create this essential documentation more efficiently.

19% **faster incident reports**[13]

Security professionals complete incident reports 19% faster when assisted by Security Copilot.

[12] 'Randomised Controlled Trial for Copilot for Security', page 6, Microsoft, January 2024
[13] 'Randomised Controlled Trial for Copilot for Security', page 6, Microsoft, January 2024

Quicker transitions from detection to action

Incident summarisation is a critical step in incident response, but without AI, it can be slow and prone to oversight. Security Copilot accelerates this process by integrating data from multiple sources, allowing users to generate comprehensive and clear summaries much faster.

39% **faster incident summaries[14]**

Security professionals complete incident summarisation essays 39% faster when assisted by Security Copilot.

[14] 'Randomised Controlled Trial for Copilot for Security', page 6, Microsoft, January 2024

Chapter 3

Strengthen team expertise

Security teams must continuously elevate their expertise to stay ahead in an evolving threat landscape. Security Copilot enables junior staff to perform more advanced capabilities and redirects expert staff to the hardest challenges, elevating the proficiency of the entire team.

Empower junior analysts

Proactive threat hunting often requires deep expertise in complex query languages. With Security Copilot, security teams can process queries using natural language, eliminating the need for specialised knowledge. Security Copilot further enhances team expertise with the advanced capabilities, processing speed and rapid learning of generative AI.

For security analysts

- Build hunting queries from natural language
- Get threat intelligence insights related to specific incidents
- Analyse malicious scripts with one 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

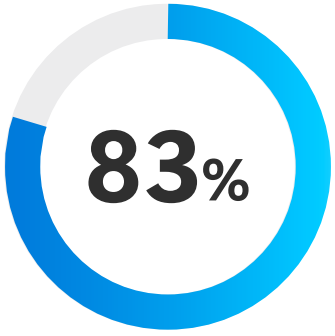
Security Copilot empowers less experienced team members to join threat-hunting activities by allowing them to build and execute Kusto Query Language (KQL) hunting queries in natural language, to help them quickly identify and investigate suspicious behaviour and compromised devices.

Because Security Copilot interoperates with all Microsoft Security products* and Microsoft Threat Intelligence, security teams can use it as a standalone or embedded experience to uncover greater insights on incidents.

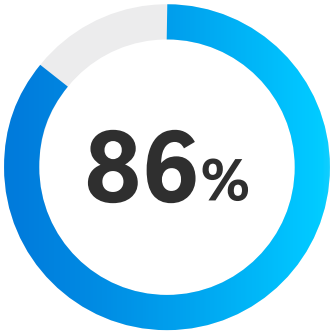
* Microsoft Defender, Microsoft Entra, Microsoft Intune, Microsoft Priva, Microsoft Purview, Microsoft Sentinel

Reduce tedium and increase focus

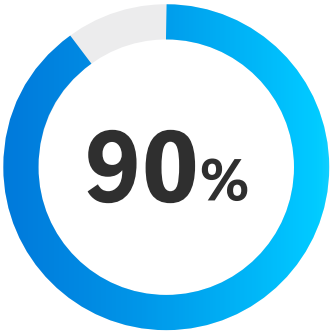
Security Copilot automates tedious tasks such as alert triage and report generation, allowing team members to concentrate on more strategic high-impact work.



said Copilot reduced the effort needed to complete a task.[15]



said Copilot helped improve their quality of work.[16]



want to use Copilot the next time they perform the same task.[17]

[15] 'Randomised Controlled Trial for Copilot for Security', page 13, Microsoft, January 2024
[16] 'Randomised Controlled Trial for Copilot for Security', page 13, Microsoft, January 2024
[17] 'Randomised Controlled Trial for Copilot for Security', page 13, Microsoft, January 2024

Conclusion

Because threat actors are constantly evolving and increasing the sophistication of their attacks, security organisations need to seek every opportunity to see more, move faster and increase the capabilities of team members.

As a generative AI-powered assistant for daily operations in security and IT, Security Copilot empowers teams to protect at the speed and scale of AI. Beyond just improving day-to-day tasks, Security Copilot helps teams adopt a more proactive stance, where they can anticipate threats rather than just react to them.

We encourage you to see how Security Copilot can fit into your current operations and help support your long-term goals. It offers a practical way to enhance your security efforts and stay resilient in a rapidly changing digital landscape.

Learn more about Security Copilot