Microsoft Security

Security Copilot

Delivering a Unified, AI-First Defense

A new approach to security

For years, security leaders have been promised a "single pane of glass," yet the reality remains a collection of disparate shards. To meet this moment, Microsoft is ushering in the era of the agentic workforce with Microsoft Security Copilot agents—autonomous agents that work side by side with security and IT teams, transforming how they protect, detect, and respond at machine speed.

By including Security Copilot with Microsoft 365 E5, we are making this agentic AI broadly accessible for defenders. Studies from live operations and randomized controlled trials show that these agents deliver immediate, integrated value across roles and workflows, with outcomes including:

These agentic capabilities transform security operations, empowering your team to:

- **Catch what others miss** by applying Microsoft's vast threat intelligence—distilled from over 100 trillion daily signals—to autonomously identify threats that others miss.
- **Respond faster** with AI-guided response to accelerate resolution time across your entire security and IT estate.
- **Strengthen team** expertise by turning every analyst into a high-performing expert, regardless of experience level.

This is the new partnership between human expertise and agentic AI, scaling your defense through intelligent action.

For the SOC analyst

Up to

550%

faster malicious email detection[1]

Accelerate your SOC's threat detection, enabling analysts to identify malicious emails 550% faster with Defender and Security Copilot.

For the identity admin

Up to

204%

more accurate in spotting missing Zero Trust policies[2]

Transform identity administration by proactively spotting and fixing missing Zero Trust policies.

For the security leader

40+

security agents available now[3]

Scale your team's capacity by automating routine work with a growing ecosystem of specialized agents from Microsoft and our partners.

Chapter 1

Catch what others miss

To catch what others miss, defenders first need a unified picture of their security landscape. This is the role of a modern SIEM, which provides the comprehensive data foundation for analysis. Security Copilot then applies threat intelligence—distilled from over 100 trillion daily signals—to that unified data, surfacing hidden attack patterns and cutting through the noise.

Gain unified visibility to reduce risk*

To truly catch what others miss, it's essential to unify your platform, thereby reducing financial exposure and overall risk. By consolidating fragmented systems, organizations gain the visibility to proactively harden defenses and limit the potential blast radius of an attack. According to a commissioned study by Forrester Consulting on behalf of Microsoft, The Total Economic Impact™ Of Microsoft Defender (June 2025), this integrated approach can reduce exposure to breach-related costs by up to 75%.

up to 75%

reduction in breach-related cost exposure[4]

Cut through the noise of alerts

The latest evolution in threat resolution, Security Copilot agents, are specifically designed to cut through noise. These agents work autonomously to manage high-volume security and IT tasks like alert and phishing triage. By correlating signals and handling routine alerts, they help resolve incidents earlier in the kill chain. This enables teams to catch malicious activity sooner and with greater confidence, demonstrating a dramatic improvement in signal clarity and operational efficiency.

22.88%

fewer alerts per incident[5]

Generate more accurate, actionable reports

A unified view and reduced noise empower analysts to produce more thorough and accurate work. In a randomized controlled trial, security professionals using Copilot created incident summaries that were significantly more complete, ensuring critical details were not missed. With AI assistance, professionals capture more essential facts, leading to more accurate and actionable reports that improve decision-making across the board.

49%

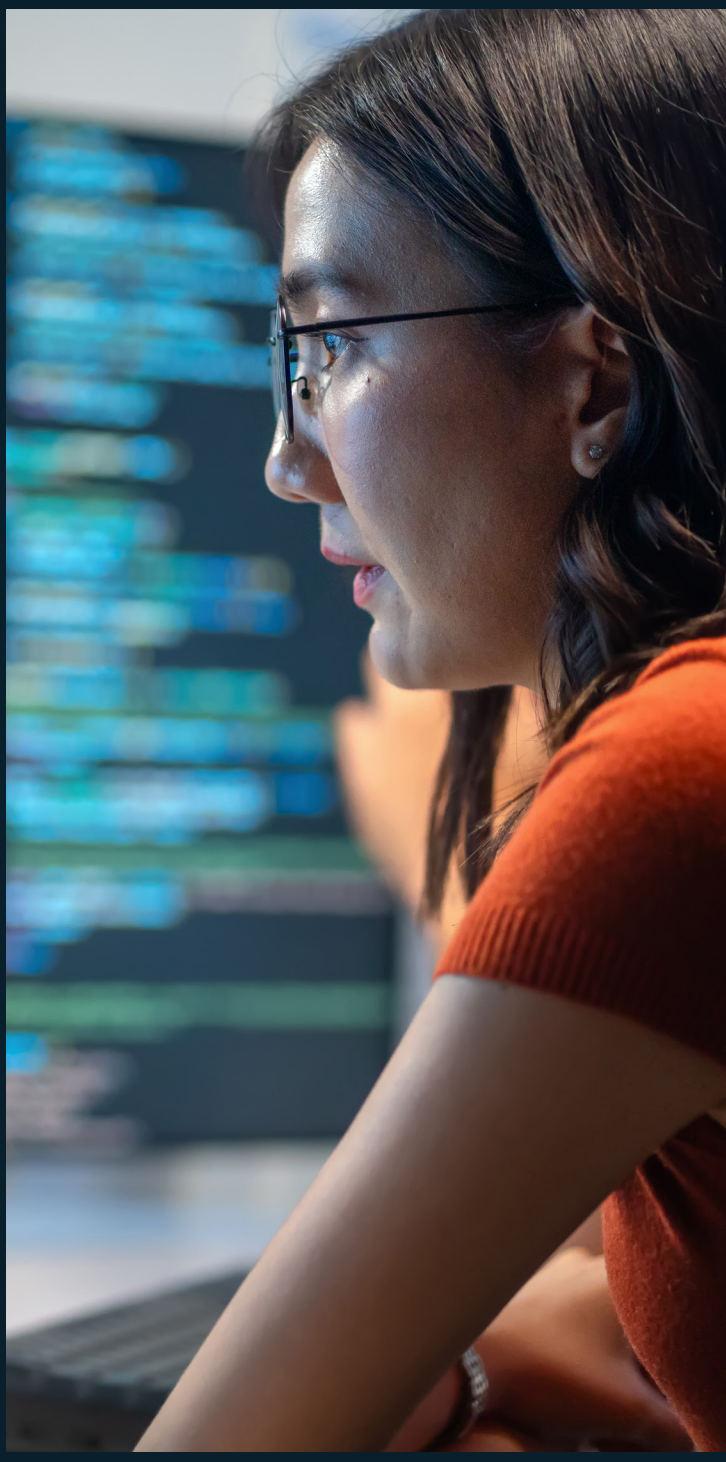
higher content score on incident summaries[6]

*These projected potential benefits of Microsoft Security Copilot (and related Microsoft Defender capabilities) are based on a fictional, composite organization (a retail organization with 10,000 FTEs and annual revenue of $5 billion) using a financial model that represents the aggregated self-reported experiences of interviewed decision-makers at organizations using Microsoft Defender, as detailed in Forrester's "The Total Economic Impact™ Of Microsoft Defender," a research study commissioned by Microsoft, June 2025. Actual results may vary from the fictional composite organization's projected benefits.

Chapter 2

Respond faster

Security Copilot accelerates the entire incident response process, delivering AI-powered guidance* and automation directly within existing workflows to help security teams outpace adversaries.



*AI can deliver inaccurate information.
It is important to check for accuracy.

Accelerate incident response

Embedded across Defender, Intune, Purview, and Entra, Security Copilot eliminates the friction of tool-switching and accelerates response across your environment. The impact grows as teams integrate AI into their daily workflows, leading to a measurable leap in operational velocity. Evidence from live operations shows that three months post-adoption, SOC teams using Copilot in Microsoft Defender resolve incidents significantly faster, demonstrating a 30% reduction in security incident mean time to resolution (MTTR) and a sustained improvement that minimizes adversary dwell time.

30% reduction in security incident mean time to resolution (MTTR)[7]

Accelerate DLP alert triage

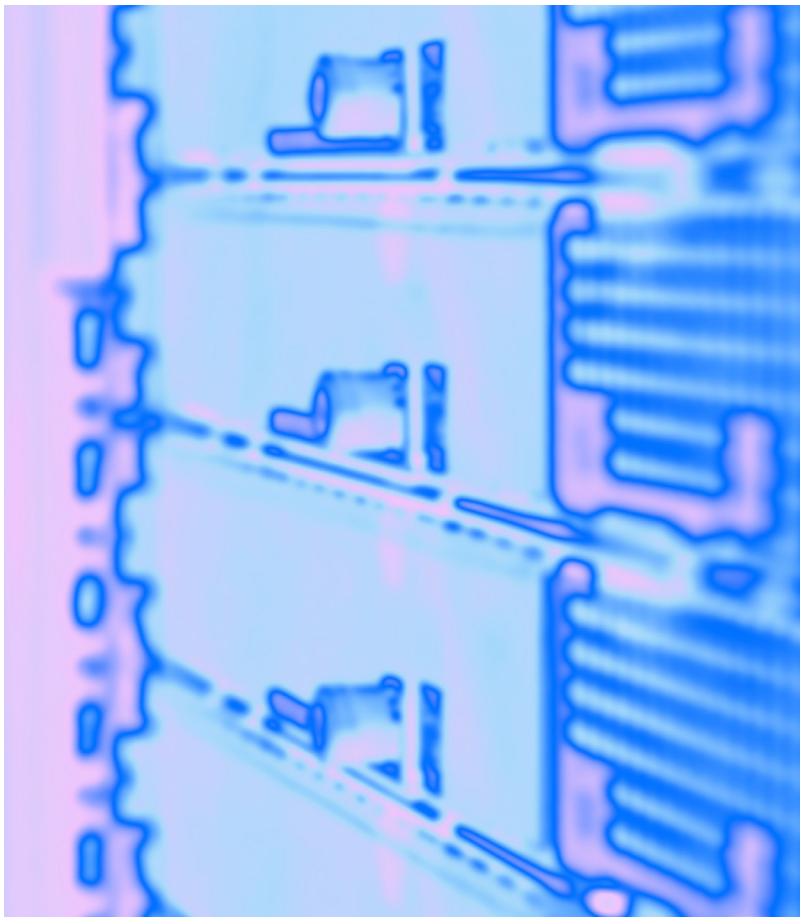
For data security teams, Security Copilot accelerates data protection by speeding up the triage of data loss prevention (DLP) alerts. This leads to an 18% reduction in time to classify a DLP alert in Purview, allowing teams to focus on the most critical data risks and ensure sensitive information is protected without slowing the business down.

18% reduction in time to classify a DLP alert in Purview[9]

Resolve policy conflicts faster

The embedded Security Copilot experience in Intune provides intelligent guidance that helps IT admins quickly identify and resolve conflicting policies. Building on this, agents like the Vulnerability Remediation Agent automate critical IT operations, further reducing misconfigurations and freeing up admin time.

54% reduction in time to resolve a device policy using Security Copilot in Intune[8]



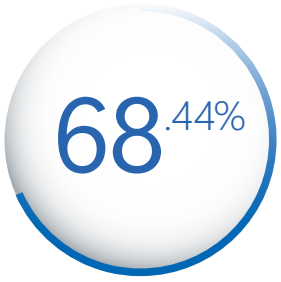
Chapter 3

Strengthen team expertise

Security Copilot directly addresses the cybersecurity skills gap by elevating the proficiency of your existing team and scaling their expertise.

Increase resolution accuracy

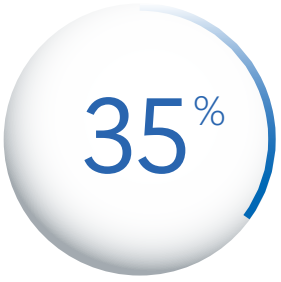
With AI-powered insights, teams aren't just faster; they're getting it right the first time. This precision translates directly into more reliable outcomes for the entire security operation, leading to a 68.44% decrease in the probability of an incident being reopened. A resolution this effective means fewer mistakes and less time spent re-investigating old incidents, allowing your team to focus on emerging threats with confidence.



decrease in the probability of an incident being reopened[10]

Bridge the cybersecurity skills gap

Empowering analysts to perform at a higher level is what makes this leap in resolution quality possible. In a randomized controlled trial, novice analysts using Security Copilot demonstrated a dramatic leap in performance and detail, showing 35% more accurate performance across all tasks. The data confirms that Security Copilot doesn't just make analysts feel more productive—it makes them objectively better at their jobs.



more accurate performance for novice analysts across all tasks[11]

Drive higher-quality, actionable outputs

Security Copilot helps junior analysts think and act like senior experts, leading to more thorough investigations and higher-quality outputs the whole organization can rely on. Novice analysts using Security Copilot included nearly twice as many critical facts in their incident summaries, ensuring reports are more accurate and actionable.

more detail in incident summaries[12]

Conclusion

The path to a predictive SOC

The cybersecurity landscape has shifted. Threat actors now leverage generative AI to automate attacks at unprecedented scale, making AI a necessity for modern defense. This new reality requires moving beyond a fragmented "single pane of glass" to an agent-first approach, where intelligent AI operates across a unified platform.

By including Security Copilot with Microsoft 365 E5, we place powerful agentic AI side by side with security and IT teams. This partnership transforms how defenders protect, detect, and respond, enabling your team to reduce incident resolution times, strengthen expertise, and scale their capacity to neutralize threats. This is how you shift from managing complexity to achieving true resilience.

The journey starts now.

Discover how to transform security with agents in your daily workflow

Learn why Microsoft is the trusted leader in secure AI innovation

Microsoft Security

[1] "Randomized Controlled Trials for Phishing Triage Agent," Microsoft, October 2025
[2] "Randomized Controlled Trial for Conditional Access Agent," Microsoft Corporation, October 2025
[3] "Transforming security with agents in your daily workflow," Microsoft Security Blog, November 2025
[4] The Total Economic Impact™ Of Microsoft Defender, Forrester, June 2025
[5] Security Copilot: Evidence of Productivity Gains in Live Operations, page 2, Microsoft, March 2025
[6] Randomized Controlled Trial for Copilot for Security, page 5, Microsoft January 2024
[7] Generative AI and Security Operations Center Productivity: Evidence from Live Operations, page 2, Microsoft, November 2024
[8] Security Copilot: Evidence of Productivity Gains in Live Operations, page 9, Microsoft, March 2025
[9] Security Copilot: Evidence of Productivity Gains in Live Operations, page 7, Microsoft, March 2025
[10] Security Copilot: Evidence of Productivity Gains in Live Operations, page 2, Microsoft, March 2025
[11] Randomized Controlled Trial for Copilot for Security, page 10, Microsoft January 2024
[12] Randomized Controlled Trial for Copilot for Security, page 10, Microsoft January 2024