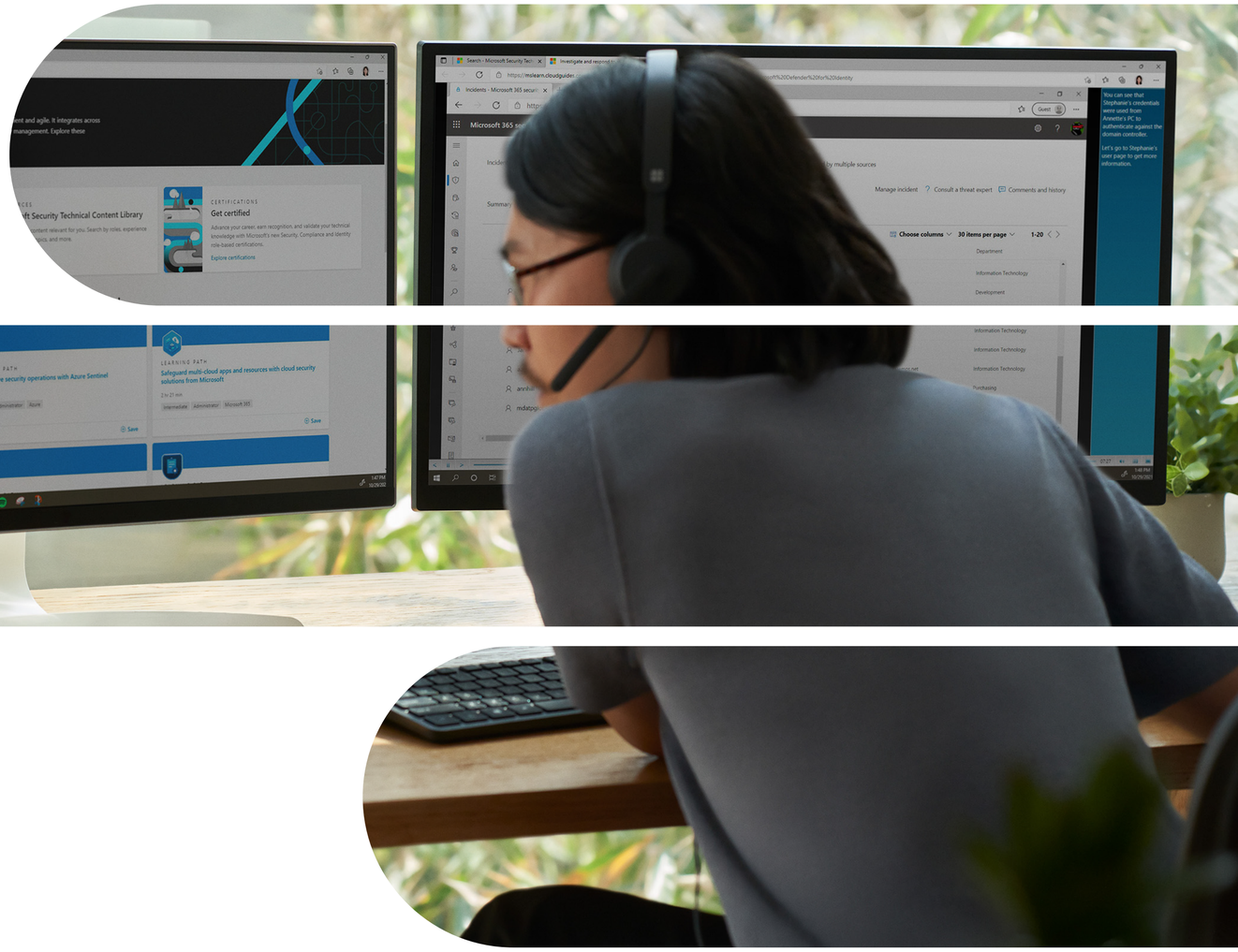
Microsoft Security

Generative AI

The defenders' advantage

This guide is for **Chief Information Security Officers (CISOs)** and cybersecurity professionals looking to partner with leaders across their organization and ensure the business is availing of generative AI. The article quickly summarizes the current threat landscape for Western European enterprises and contextualizes the game-changing nature of generative AI cybersecurity tools in a way that's accessible to leaders without a technology background.

Estimated reading time: 3-minutes.



Microsoft Security

The evolving threat landscape

The **World Economic Forum** estimates that 70% of new value created in the next 10 years will come from business models underpinned by digital platforms. Using technology like the cloud and AI, businesses are developing a new echelon of products, services and experiences for their customers. Public sector bodies are optimizing frontline services while simultaneously achieving greater efficiencies.

As all organizations digitize and become data led, the promise of increased growth and prosperity are significant. However, the opportunities ahead call for increased vigilance.

The cyber threat landscape continues to shift and evolve as cybercrime proliferates. For example, according to **Microsoft's 2023 Digital Defense Report** the number of password-based attacks worldwide increased 10x year over year – with 4,000 attacks blocked *per second*.

The cyber threats facing Western Europe continue to change as criminals have become more entrepreneurial and collaborative. One illustration of this: organized cybercrime services are increasingly available for hire on the dark web. This means a bad actor no longer needs skills or resources to disrupt a business or compromise its data – just a willing partner in crime. Today, Europe trails only the US in terms of the volume of DDoS attacks.

These trends are compounded by the fact that many cybersecurity teams in Europe are stretched thin.

The **EU** estimates that there's currently a **shortage of up to 500,000 trained cybersecurity professionals.**

The advent of security tools powered by Generative AI could not be timelier. Technology like Microsoft Copilot for Security will address the asymmetry between criminals and defenders – and give the good guys a compelling advantage.

The technology helps security teams:

1

Pre-empt

Identifying and fixing security vulnerabilities before they can be exploited. Stopping incidents before they start is the best way ensure business continuity and build trust with company stakeholders.

2

Mitigate

Spotting issues at machine speed and acting as an assistant to security analysts as they respond. This makes team members more effective while easing the stain on them.

3

Automate

By automating time-intensive jobs like reporting, security professionals have more time and energy to focus on keeping threats at bay. This benefits daily operations, clearly. But by giving time back so analysts can focus identifying blind spots and pre-emption, their jobs become more rewarding and engaging.

4

Augment

Putting analysis and recommended next steps into natural language, GenAI tools help junior analysts augment and uplevel their skills. These professionals feel empowered and are learning on the job while they effectively do their jobs.

Microsoft Security

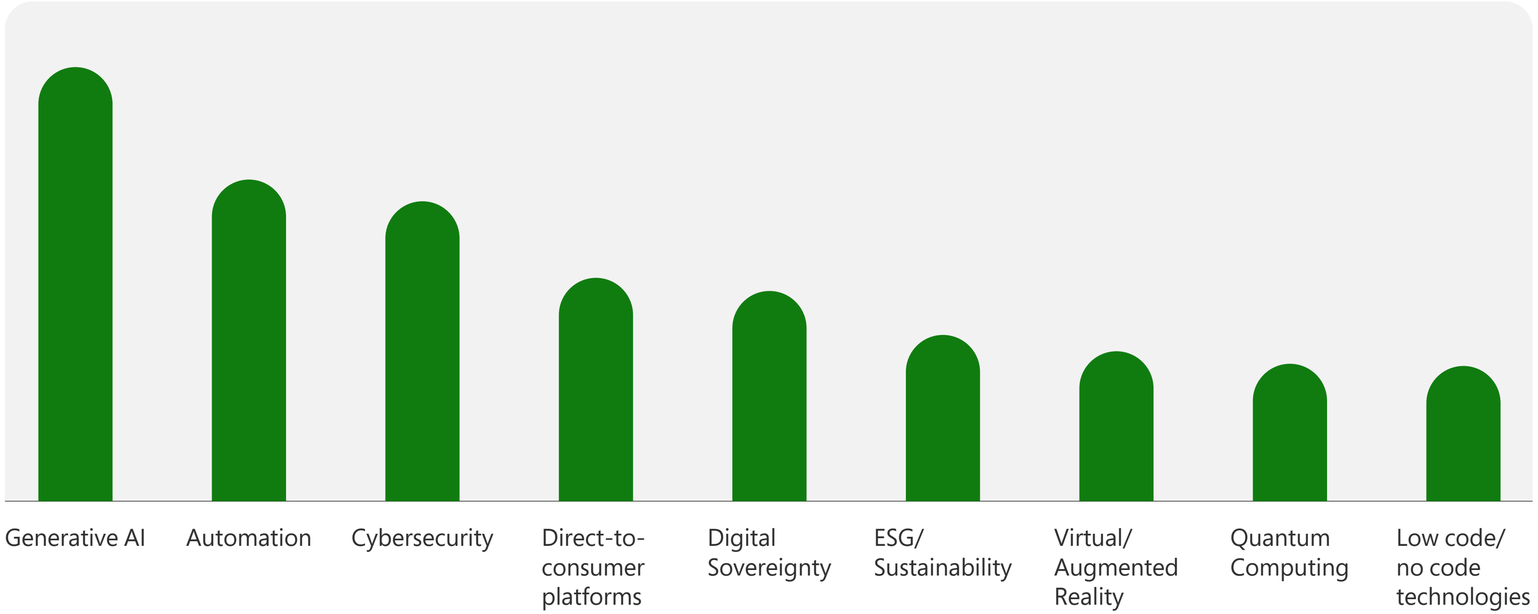
Mike Hughes,
Business Group Director,
Security at Microsoft Western Europe

"After the remarkable advancements we've seen over the past year, there's significant interest in both GenAI and cybersecurity technology within the C-Suite according to new research from IDC. In fact, these are the investment areas that are among the most top of mind as Europe's enterprise leaders look to the year ahead.

The defenders' advantage comes from AI's ability to reason over a massive number of signals and produce insights that augment security analysts' abilities in an unprecedented way."

Gen AI is top of mind for the C-Suite

Which of the following technology areas is top of mind for the C-Suite in terms of new investments for the next 12 months?



Source: IDC, *C-Suite Tech Agenda: Priorities and the Power of AI,* doc #US51335623, November 2023

Microsoft Security

Equipped with modern AI tools, cybersecurity teams can spend less time putting out fires and reacting. They will have **greater capacity to innovate and develop strategies** and programs that pre-empt incidences. So, their roles become even more rewarding and higher value.

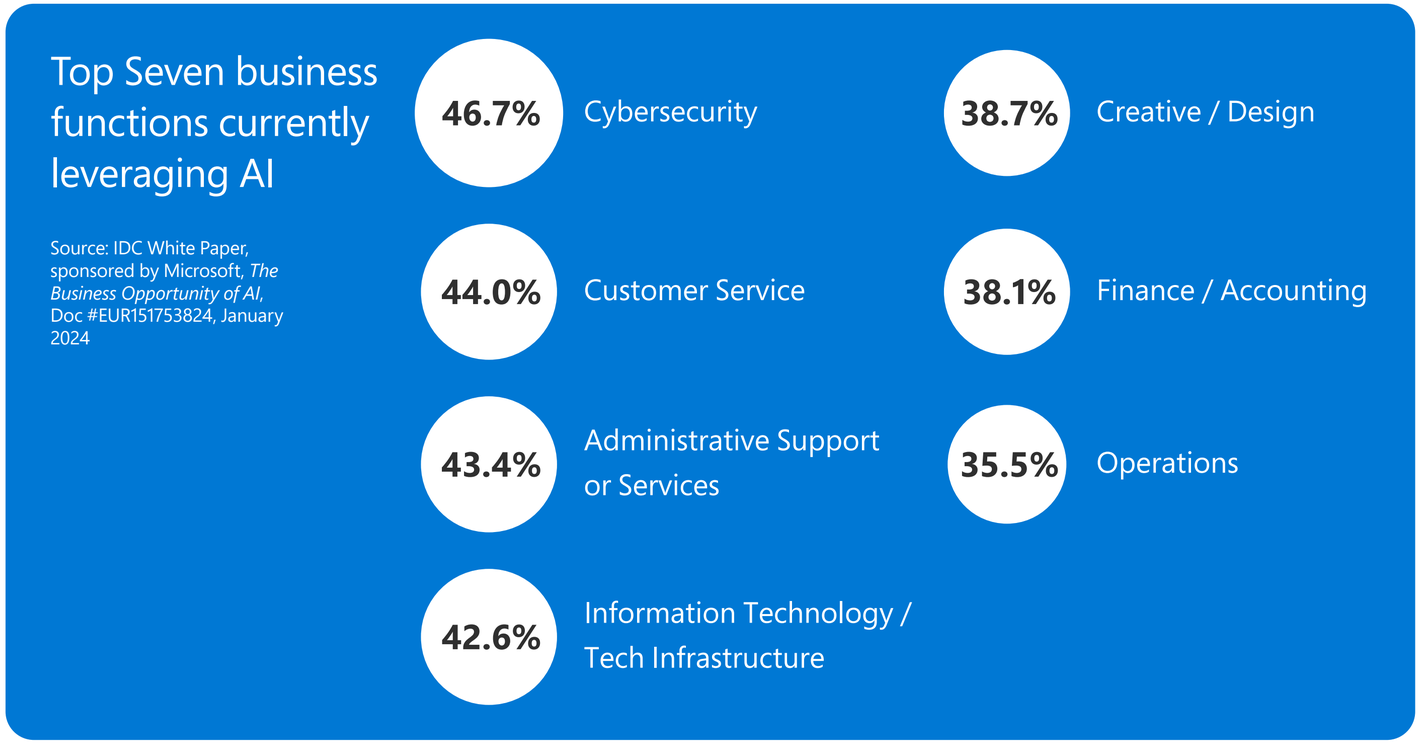
Ultimately, this creates a virtuous circle – resulting in organizations that are more secure today, and in a stronger position to attract and retain the best cybersecurity talent. This translates into **a more secure tomorrow.**

Throughout Europe, cybersecurity has emerged as the number-one use case for AI technology.

In the next section you will find three scenarios where the latest GenAI cybersecurity tools are quickly augmenting teams to improve organizational speed and resilience.

Top Seven business functions currently leveraging AI

Source: IDC White Paper, sponsored by Microsoft, *The Business Opportunity of AI*, Doc #EUR151753824, January 2024



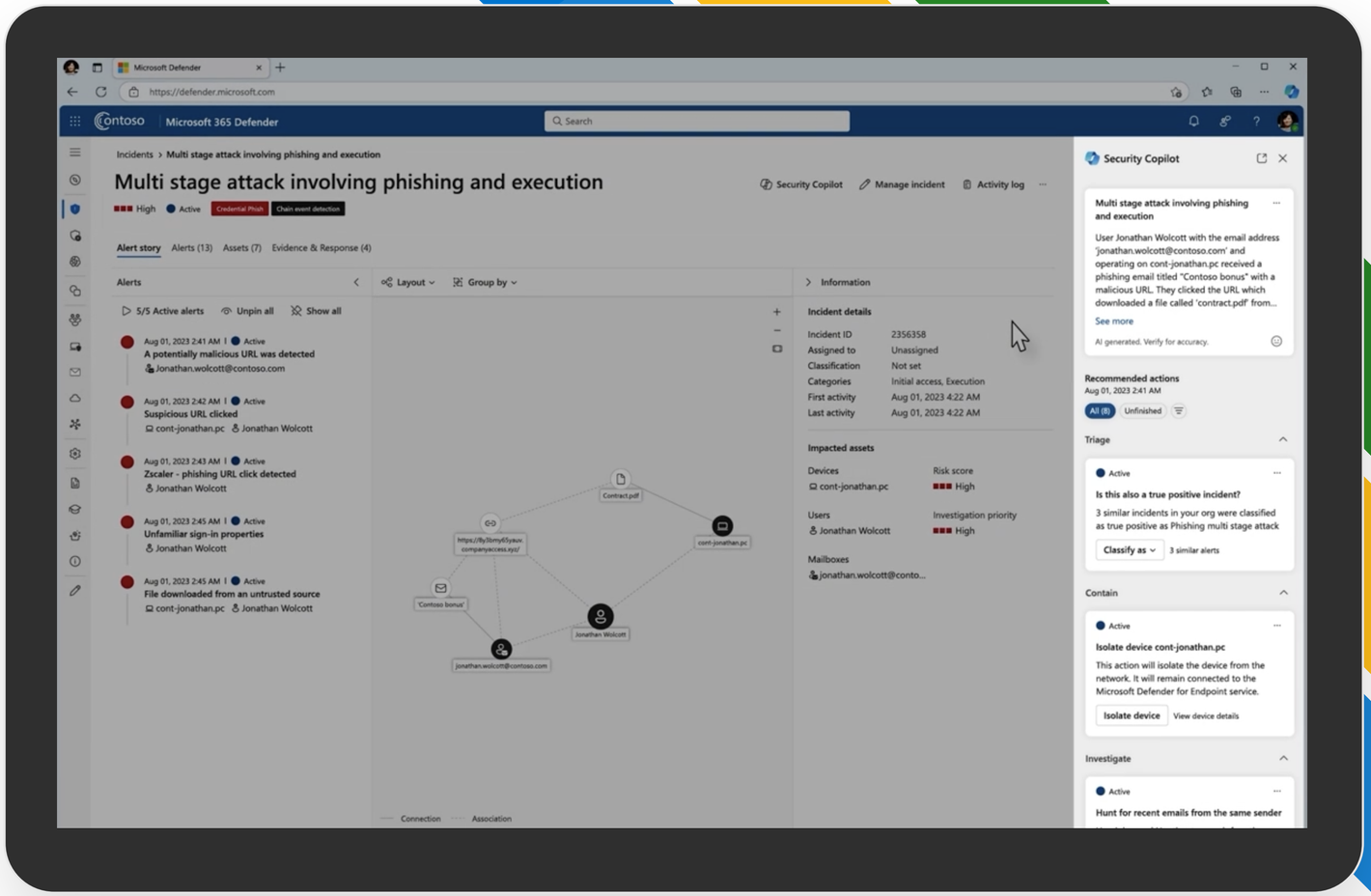
Microsoft Security

Seamless deployment. Fast ROI.

1. Helping teams work smarter to preempt and remediate.

Microsoft Copilot for Security provides analysts with access to **real-time insights, analytics, search and summarization** – all within the natural workflows they are already accustomed to. This GenAI technology can reason over data across endpoints, emails, identities, apps – giving analysts full visibility across the data estate.

With a multistage attack incident Microsoft Copilot for Security provides an incident summary and offers suggestions for immediate actions – like quarantining a comprised device. In phishing incidents the technology can instantly provide a view of people who have been targeted, recommended next steps and then create an incident report that can be shared with colleagues.



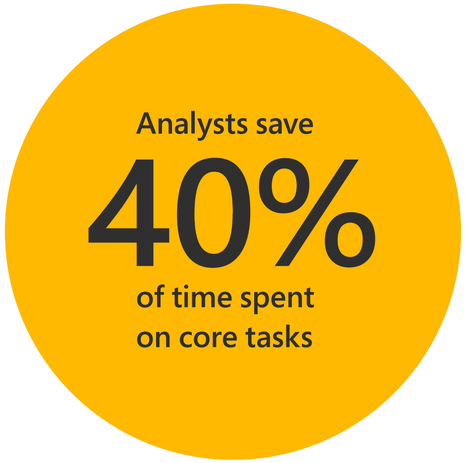
Microsoft Security

2. Access to more data means faster action, better remediation.

Using AI, **Microsoft analyzes 65 trillion cybersecurity signals** each and every day to quickly identify emerging criminal activity. Coupled with the insights from Microsoft's 10,000 worldclass cybersecurity experts, rich and actionable intel is shared with customers so they can more effectively pre-empt and address risks.

This Microsoft Defender Threat Intelligence is available to Microsoft Copilot for Security customers at no cost. Further, Microsoft Copilot for Security allows teams to use natural language queries to summarize investigations and explore built-in threat intelligence to help them stay a step ahead.

Results from preview customers speak for themselves.



This includes time on investigations and hunting. Teams are working smarter to keep organization safe – not just clocking longer days.

This means more time and headspace for their main focus: thwarting criminals. Further, with legislation like NIS2 coming into effective in the next year, making reporting more efficient will be more important than ever.

Microsoft Security

3. Immediate upskilling of cybersecurity team talent.

Microsoft Copilot for Security provides intel and guidance around multiple cybersecurity tasks, from incident summarization to script analysis to incident reporting.

So, in a phishing attack, Microsoft Copilot for Security takes a junior analyst through the attack and identifies a hidden powershell script used by the attacker. **Not having the technical skills to understand the script is no longer a barrier to getting to an effective response.** Microsoft Copilot for Security can break down the actions undertaken by the script in natural, intuitive language – at speed. In fact, Microsoft Copilot for Security can analyze and understand 500 lines of code in under one minute.

In the same attack, the junior analyst will want to investigate whether other devices have been affected. However, they may not yet have sophisticated Keyword Query Language (KQL) skills to investigate. Microsoft Copilot for Security is able to use contextual information and build a KQL query to find other affected users and see if they've too clicked on the malicious link.

A new-to-career analyst needing to update the CISO on the incident can instantly create a professional summary report of the investigation and the remediation actions.

For business leaders looking to learn more about achieving a clear defender advantage please click here.

Or speak with your local Microsoft account lead.

For those analysts new in career using Microsoft Copilot for Security:

86% reported an improved the **quality** of their work.

86% reported an increase in **productivity**.

Microsoft Security

Vasu Jakkal,
CVP, Microsoft Security

"Today the odds remain stacked against cybersecurity professionals. Too often, they fight an asymmetric battle against relentless and sophisticated attackers.

With Microsoft Copilot for Security, we are shifting the balance of power into our favor. Microsoft Copilot for Security is the first and only generative AI security product enabling defenders to move at the speed and scale of AI."