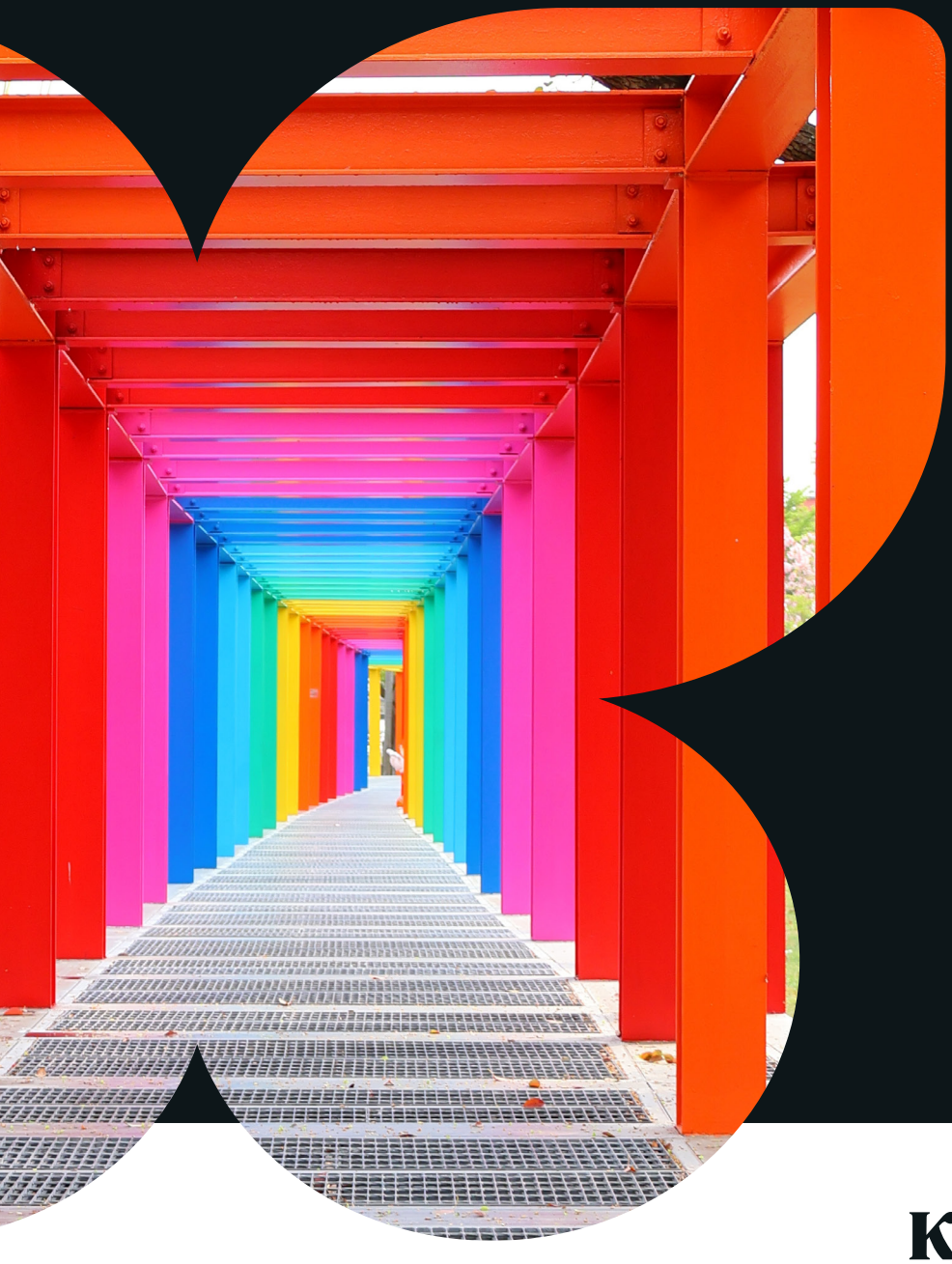
BECOME GREATER
KOCHO.CO.UK

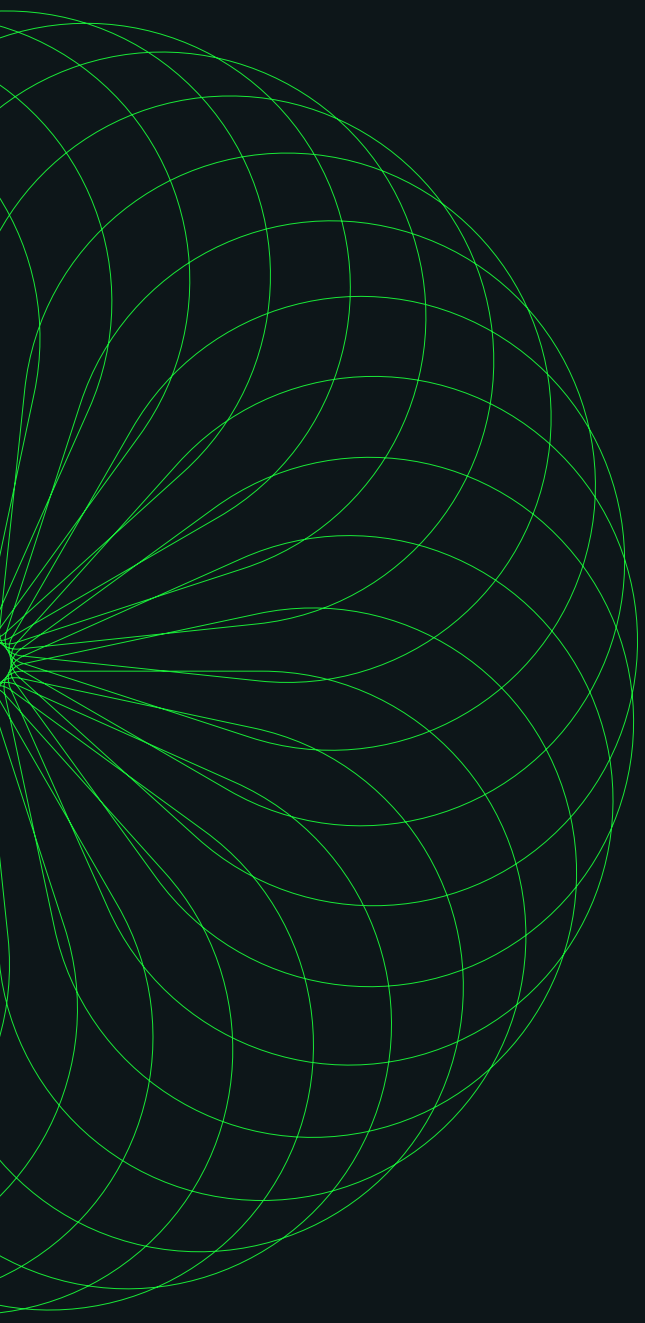
How Copilot works with the Microsoft Security stack

*Published with permission from Microsoft.



Kocho

Microsoft



Contents

An introduction to Microsoft Copilot for Security

Microsoft Copilot for Security (Copilot) is a generative AI-powered security platform that assists security and IT professionals in responding to cyber threats, processing signals, and assessing risk exposure at the speed and scale of AI, all while adhering to responsible AI principles.

It offers a natural language, assistive experience that supports security and IT professionals in end-to-end scenarios such as incident response, threat hunting, intelligence gathering, device management, and posture management. It is specifically designed to work with Microsoft Security products and other third-party tools, as well as integrate with natural language to generate tailored guidance and insights.

Some of the top Copilot features include:

Swiftly summarising information about an incident by enhancing incident details with context from data sources (e.g. data integrated from other security products or proprietary process documents uploaded to Copilot), assessing its impact, and providing guidance to analysts.

Providing information on events that might expose organisations to a known threat and prescriptive guidance on how to protect against those potential vulnerabilities.

Generating ready-to-share executive summaries, technical summaries, or reports on security investigations, publicly disclosed vulnerabilities, or threat actors and their campaigns.

Leveraging the full power of OpenAI GPTs and Azure AI architecture to generate a response to a user prompt using security-specific plugins, including organisation-specific information, authoritative sources, and global threat intelligence.

Seamlessly integrating with products in the Microsoft Security portfolio such as Microsoft Defender XDR, Microsoft Sentinel, Microsoft Purview, Microsoft Entra, and Microsoft Intune, as well as other third-party services such as ServiceNow, Netskope, and Cyware.

Copilot can help security and IT teams in various ways

Such as:

Improving the speed and efficiency of security and IT operations tasks, such as writing complex queries, summarising incidents, and providing remediation steps.

Enhancing the skills and confidence of security and IT professionals, especially novices, by providing guidance and insights in natural language.

Leveraging the power of OpenAI models and Azure AI hyperscale infrastructure with Microsoft's global threat intelligence to generate tailored and accurate responses to security-related questions.

Helping security and IT teams catch attacks that might otherwise be missed, swiftly respond to threats, protect against vulnerabilities, and strengthen their security posture.

Simplifying the complex and driving efficiency with AI-assisted insights and recommended actions.

Fetching and analysing key information and configuration data about your digital estate to minimise attack surface and worker-impacting vulnerabilities.

Providing tooltips, guidance, and insights about recommended policies and error codes to reduce time spent on what-if analysis, research, and troubleshooting.

But Copilot isn't just for organisations with stocked security skillsets.

Copilot can help organisations that don't have dedicated security teams and advanced security skillsets by providing them with a generative AI-powered assistant that can guide them through various security tasks and scenarios.

It provides security context to non-security roles, making security more accessible and redefining what security is and how security gets done.

How Copilot works with the Microsoft security stack

In the rapidly evolving landscape of cybersecurity, staying ahead of threats is paramount.

Copilot emerges as a cutting-edge ally, harnessing the power of artificial intelligence to bolster your security and IT operations. This innovative tool is designed to enhance efficiency, uncover hidden patterns, fortify defences, and accelerate incident response times.

Key benefits:

Increased efficiency

Speed up or automate routine tasks, freeing up valuable time for your security team to focus on strategic initiatives.

Reduced human error

Copilot provides insights that humans might miss or otherwise overlook.

Hardened defences

Strengthen your security posture using authoritative methods to help reduce the attack surface and vulnerability to threats.

Expert guidance

Get recommendations for things like the top DLP alerts to focus on today, steps to remediate an incident, or measure how vulnerable your organisation is against a specific bad actor.

Faster incident response

Respond to security incidents with unprecedented speed, minimising potential damage and recovery time.

Main use cases

For the initial launch of Copilot for Security, our focus was on making four primary use cases exceptionally easy to use:

1. **Incident summarisation:**

   Gain context for incidents and improve communication across your organisation by leveraging generative AI to swiftly distil complex security alerts into concise, actionable summaries, enabling quicker response times and streamlined decision-making.

2. **Impact analysis:**

   Utilise AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritise response efforts effectively.

3. **Reverse engineering of scripts:**

   Eliminate the need to manually reverse engineer malware, enabling every analyst to understand the actions executed by attackers. Analyse complex command line scripts and translate them into natural language with clear explanations of actions. Efficiently extract and link indicators found in the script to their respective entities in your environment.

4. **Guided response:**

   Receive actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation. Relevant deep links to recommended actions allow for quicker response.

Main use cases

Other product use cases that we have prioritised and will continue to grow with ongoing improvements are:

Device management: Generate policies and simulate their outcomes, gather device information for forensics, and configure devices with best practices from similar deployments.

Identity management: Discover overprivileged access, generate access reviews for incidents, generate and describe access policies, and evaluate licensing across solutions.

Data security and compliance: Identify data impacted by security incidents, generate comprehensive summaries of data security and compliance risks, and surface risks that may violate regulatory compliance obligations.

Cloud security: Discover attack paths impacting workloads and summarise cloud CVEs to proactively prevent threats and manage cloud security posture more efficiently.

Incident response: Quickly analyse and respond to security incidents with AI-driven insights and recommendations.

Threat hunting: Use natural language search to isolate advanced threats across the environment.

Security posture management: Assess and improve your organisation's security posture with actionable insights based on your unique organisation.

Security reporting: Generate comprehensive reports that provide clear visibility into your security landscape, aiding in decision-making, threat assessment, compliance, and management/Board-level briefs.

Threat intelligence research: Take advantage of Microsoft's extensive threat intelligence by accessing threat articles and threat actor security data on new and emerging threats, helping your organisation to prevent and protect itself from harm.

Copilot is an integral part of the Microsoft security ecosystem, designed to enhance and streamline security and IT operations. Its integration across the Microsoft Security suite of products allows for a unified approach to threat detection, analysis, and response.

Copilot can be accessed through a standalone portal or directly within other Microsoft Security products. By connecting with existing security infrastructure, it creates a cohesive ecosystem that enhances overall security effectiveness.

Seamless integration with Copilot

Copilot integrates seamlessly with key components of the Microsoft security stack, including:

Microsoft Defender XDR:

Enhances threat protection and provides advanced attack analytics.

Microsoft Sentinel:

Offers cloud-native SIEM and SOAR capabilities for a comprehensive view of the entire digital estate.

Microsoft Intune:

Unifies apps and device management to simplify IT and security operations, protect a hybrid workforce, and power better user experiences.

Microsoft Purview:

Provides data governance and protection, helping to prevent data leaks and ensure compliance.

Microsoft Entra:

Manages identities and access, safeguarding against identity-based threats.

Microsoft Defender Threat Intelligence:

Improves understanding of the threat landscape by providing real-time, context-aware responses to prompts and empowering reactive threat enrichment and proactive hunting scenarios.

How Copilot works with third-party security tools and managed services

Copilot for Security was built to integrate with other security and IT software vendors via plugins. Microsoft collaborated with a broad set of design partners to build the initial plugins and will rapidly expand the plugin library.

Copilot for Security was designed to integrate with data sources, including third-party ones, by leveraging Plugins to gain more context and extend Copilot for Security's capabilities. Microsoft collaborated with a broad set of ecosystem partners to build the initial plugins and will rapidly expand the plugin library. This allows our rich, diverse partner ecosystem to bring their cultivated data sources and extend the visibility of Copilot for Security.

MSSPs (Managed Security Service Providers) are incorporating their unique knowledge and expertise to build custom promptbooks for specific scenario-based multi-stage process streamlining. Another way MSSPs are enriching the Copilot for Security experience is through knowledge bases that enrich analysts with important information around a specific scenario along with next steps and/or recommendations that can be loaded into Copilot for Security to be used as source material for user prompts.

Partners can use Copilot's extensibility framework to develop plugins that will provide customers with an end-to-end view of their security portfolio using a Gen-AI platform. Customers can bring their organisation's non-Microsoft signals, incidents, and alerts to correlate with Microsoft's Security solutions to reduce remediation time and increase productivity.

How Copilot might change security workflows

In the realm of cybersecurity, security workflows are the backbone of an organisation's defence strategy.

They are comprehensive, step-by-step processes that guide security teams through the identification, investigation, and resolution of security processes. By defining clear protocols and procedures, security workflows ensure that processes are handled systematically and effectively.

Copilot democratises security data and makes it more approachable. It affords anyone looking for security context the ability to ask simple questions and get profound advice.

Copilot enhances traditional security workflows by infusing them with artificial intelligence, leading to significant enhancements in several key areas:

Efficiency: By automating repetitive tasks and streamlining processes, Copilot allows security and IT teams to operate with greater speed and less manual intervention.

Consistency: It ensures that every step of the security workflow can be executed uniformly, reducing the likelihood of human error and variance in incident handling.

Accuracy: With the broad set of data sources that Copilot can pull from, it is able to evaluate more information, providing more complete and precise responses, which improves the decision-making process during incident response.

Scalability: As the volume and complexity of security threats grow, Copilot scales to meet the demands, ensuring that your security workflows remain robust and responsive.

Copilot is not just a tool; it was designed to work with your existing workflows, but it also provides the opportunity to be a transformative force, redefining how security and IT gets done.

For example, if you are conducting a vulnerability impact assessment, you likely will work with people from different departments. A security person will assess the severity of the vulnerability, an IT person will assess the impacted systems and configuration that would relate to the vulnerability, and an identity admin would investigate associated users and assess user risk. Without Copilot, these people would have to work separately and manually hand off to the next person in the remediation process. But with Copilot, these tasks could be swiftly completed by one person in a single Copilot session (with the right permission), freeing up other team members to tackle other work.

Best practices for using Copilot

Best practice 1: Educate your teams

Copilot is straightforward – you can just use it. However, to maximise the benefits of Copilot and to get your team excited, it's important to provide training for your security team. Resources such as Microsoft Learn modules, documentation, videos, and webinars can be invaluable. Adherence to responsible AI principles—transparency, accountability, reliability, and ethical use—is essential.

Best practice 2: Leverage plugins and data sources

Copilot utilises data sources, like Microsoft products, third-party plugins, and uploaded files (knowledge base functionality) to provide tailored responses. Copilot leverages plugins to connect to systems across your organisation to formulate responses. Plugins encapsulate solutions from Microsoft (Defender XDR, Intune, Defender Threat Intelligence, Entra, Purview, etc.), and third parties such as ServiceNow and Tanium. Plugins work according to individual user permissions and can be enabled or disabled based on the need of a workflow or configured in a way as to better direct response from Copilot. Knowledge base files are a data source that extends Copilot so that users can include contextual information specific to your organisation. You can upload documents containing organisation policies, best practices, etc. to leverage inside a Copilot session. This allows Copilot to provide more accurate responses because it can consider your unique context in its decision making.

Best practice 3: Integrate with existing security workflows

Copilot augments or drives efficiency in existing workflows stemming from security, IT, or data systems such as Microsoft Defender XDR, Microsoft Sentinel, etc., through its interconnected AI platform. The extensible plugin model attached to the platform facilitates further extension and integration into specific datasets, custom applications, or different disciplines. Build custom prompt books and upload your organisation's knowledge base documents to enable Copilot to work your way.

Best practices for using Copilot

Best practice 4: Review and verify generated content

It's important to review and verify the content generated by Copilot due to the inherent limitations of generative AI. This includes checking sources and using expert judgement to ensure accuracy and reliability. Just as you would in conversing with a human, trust but verify any information presented.

Best practice 5: Provide feedback and suggestions

Feedback and suggestions are vital for the continuous improvement of Copilot. Users can contribute through the feedback button in the portal, the Microsoft Tech Community, or by contacting the support team.

Best practice 6: Develop good prompts for Copilot

The process of writing, refining, and optimising inputs—or "prompts"—to encourage generative AI systems to create specific, high-quality outputs is called prompt engineering. It helps generative AI models organise better responses to a wide range of queries—from the simple to the highly technical. The basic rule is that good prompts equal good results. Prompt engineering is important because it allows AI models to produce more accurate and relevant outputs. By creating precise and comprehensive prompts, an AI model is better able to synthesise the task it is performing and generate responses that are more useful to humans.

Trial findings: Improving productivity, accuracy, and upskilling

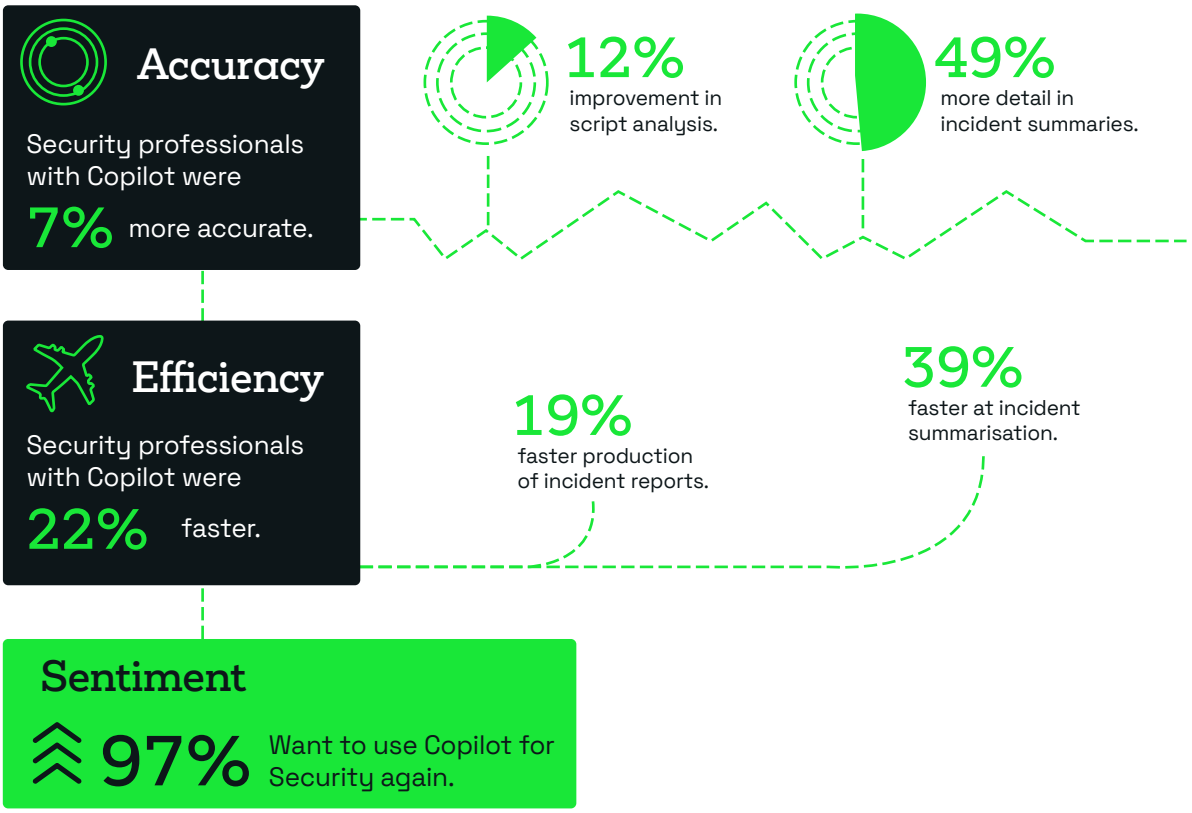
Validating Copilot for Security's real-world advantages.

Microsoft conducted a randomised controlled trial among 147 security professionals and 149 security novices.

The aim: To measure Copilot for Security's effect on productivity, accuracy, and user buy-in.

The results demonstrated were remarkable.

Security professionals



Security novices

Conclusion

The study demonstrated how leveraging the power of Microsoft Copilot for Security can dramatically improve accuracy, productivity, and efficiency in cyber security operations.

It's also clear validation of Copilot for Security's ability to bridge skills gaps and significantly speed up the training of newcomers to cyber security.

To dive deeper into the study and its findings, get your copy of the full 19-page report.

DOWNLOAD NOW

Resources

- Machine Learning and AI Innovation at Microsoft Research: The scale and coverage of security signals across the entire Microsoft digital estate enables us to track and prevent adversarial activities across the security kill chain. This is the foundation upon which we're building the teams, tools, analytics, models, and research to responsibly use this data to protect users around the world.
- Evaluation of generative AI applications with Azure AI Studio - Azure AI Studio | Microsoft Learn: The goal of the evaluation stage is to measure the frequency and severity of language models' harms by establishing clear metrics, creating measurement test sets, and completing iterative, systematic testing (both manual and automated). This evaluation stage helps app developers and ML professionals to perform targeted mitigation steps by implementing tools and strategies such as prompt engineering and using our content filters.
- MSRC - Microsoft Security Response Center: Part of the defender community, the Microsoft Security Response Center is the front line of security response evolution. For over twenty years, we have been engaged with security researchers working to protect customers and the broader ecosystem.
- Generative-AI-for-beginners/05-advanced-prompts at main · microsoft/generative-ai-for-beginners · GitHub: Access our just released prompt guides on GitHub. Better prompts help AI to generate more relevant and useful outputs, set the context, tone, and style of outputs, and serve as a starting point for an AI model's "thought process."

***This e-Guide was orginally published by Microsoft and has been re-published with their permission.**

Trial results are taken from: Randomized Controlled Trial for Copilot for Security, Microsoft, 2024.

Next Steps

Book a Vision Call and get a roadmap to improvement.

If you're looking to improve your security, the technology discussed in this e-Guide will certainly help achieve that.

But how to deploy it effectively in your business can often be a challenge.

That's where a short vision call can help. It's a chance for our experts to:

- → Learn about your business and challenges
- → Identify your security strengths and weaknesses
- → Develop a roadmap for improvement

Take control of your security strategy and book your no obligation Vision Call today.

Book a Vision Call →

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Data & AI (Azure)

Microsoft Solutions Partner
Infrastructure (Azure)

Microsoft Solutions Partner
Digital & App Innovation (Azure)

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Advanced Specialisation
Microsoft
Cloud Security
Threat Protection
Identity & Access Management
Information Protection & Governance

CISSP

CYBER ESSENTIALS CERTIFIED PLUS

ISO 9001 CERTIFIED

bsi. ISO/IEC 27001 Information Security Management