E-book

5 Cybersecurity AI Myths Debunked

A guide to generative AI misconceptions, opportunities, and Microsoft Copilot for Security

Microsoft Security

Contents

Introduction

A new era of AI has arrived—along with new misconceptions

Cyberthreats are on the rise, both in numbers and severity, and security teams are struggling to keep pace with traditional cybersecurity tools. This is why many security leaders are turning to AI-powered solutions.

These transformative tools provide an opportunity to address your greatest security challenges and can be a game changer for your security team. Equipped with generative AI solutions, your security professionals can protect more, move faster, and gain an edge on cybercriminals. Plus, they'll spend less time performing tedious tasks and more time making strategic and proactive decisions.

Because generative AI-powered cybersecurity solutions are new, you may be hesitant to embrace these tools. As a security leader, it's natural to have questions about any new technology. In fact, it's a sign that you're good at your job. But when you work with a trusted technology partner, you'll find that the rewards of generative AI far outweigh the risks.

This e-book will explore and debunk the five most common myths about generative AI cybersecurity tools, including:

1. Unauthorized data access
2. Data privacy and ownership
3. Data leakage and exposure
4. Compliance issues
5. Hallucinations

Keep reading to delve deeper into these concerns and find out how Microsoft Copilot for Security addresses each one with built-in security, compliance, and privacy controls.

1

The case for AI in cybersecurity

Cyberattacks are growing increasingly prevalent, coordinated, and sophisticated. In the last year, the number of password attacks detected by Microsoft skyrocketed from 579 to more than 4,000 per second.[1] Because most organizations use dozens of cybersecurity tools to manage their environment, today's security teams face a deluge of data, alert fatigue, and limited visibility across multiple solutions—all while dealing with a global talent shortage and regulatory complexity.

The odds are stacked against today's security analysts:

- 4,000: Password attacks per second
- 72 minutes: Median time for an attacker to access your private data if you open a phishing email
- 3.5 million: Global shortage of skilled cybersecurity professionals

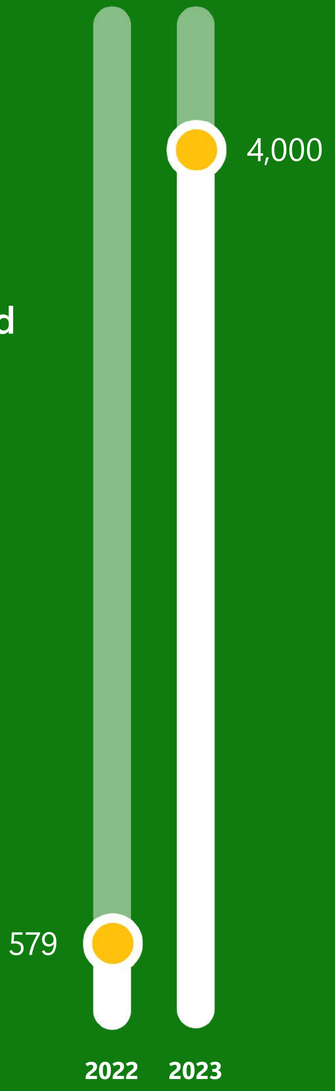
This is why it's more important than ever to equip your security teams with innovative solutions that help them quickly detect, investigate, and respond to escalating cyberthreats. To navigate today's complex challenges, security leaders are looking for:

- More automation and tools that work together to help their security teams outpace and outsmart cyberattackers.
- Ways to strengthen their team's expertise and alleviate tedious tasks so they can focus on protecting their organization.
- Solutions that help their analysts see more and move faster, so they can detect and respond to incidents before they cause harm.

AI is the key to making all this possible.

Many security teams are already gaining an edge with AI-powered solutions. And the impact is real.

Password attacks per second



[1] Microsoft Digital Defense Report 2023.

Microsoft Copilot for Security represents a groundbreaking advancement for Security Operations teams worldwide. Through our global Microsoft MXDR [managed extended detection and response] service, we're seeing up to 40% reduction in incident resolution time when modeling against current processes.

Additionally, it significantly enhances the work environment for Security Operations Center (SOC) analysts by serving as their AI security assistant for day-to-day operations.

Jason Revill
Global Security Center of Excellence Lead, Avanade

Artificial Intelligence will be a critical component of successful defense. In the coming years, innovation in AI-powered cyberdefense will help reverse the current rising tide of cyberattacks.

Tom Burt
Corporate Vice President, Customer Security and Trust, Microsoft

To address increasingly complex cybersecurity challenges, many security teams are embracing generative AI tools—such as Microsoft Copilot for Security—that enhance human expertise with intelligent insights and automated workflows.

Copilot for Security is an AI assistant for daily operations in security and IT. This generative AI-powered solution is designed to help security teams be faster, more productive, and more accurate. With Copilot, security teams get tailored insights based on global threat intelligence, industry best practices, and their organization's security data. These actionable insights give security professionals the knowledge they need to outsmart and outpace cyberattackers.

40%

of time is saved by analysts using Copilot for typical security operations tasks

60%

of time is saved by analysts using Copilot for tedious tasks, such as alert triage and reporting[2]

[2] Microsoft Copilot for Security early customer data, 2023.

2

5 myths about generative AI-powered security solutions debunked

While it's clear that generative AI can help amplify the impact of security teams, some leaders are wary of jumping in right away without careful consideration. It's reasonable to be hesitant about any new technology and curious about its potential impact on your team and organization. This is why it's important to do your research.

Here are the top five concerns security leaders have about generative AI—and how Copilot for Security is built to address them.

Myth 1:

Unauthorized data access

Some security leaders are concerned that if an unauthorized user asks an AI-powered tool a question, they could get an answer that includes information the user isn't authorized to see. But this isn't the case.

Data security is the primary concern for organizations adopting new generative AI tools. When any unauthorized user, whether internal or external, gains access to data, this can disrupt business and put an organization's reputation at risk. To generate useful answers to queries, generative AI applications may have access to sensitive data. However, the app will only show the user what they have access to see.

Frequently asked question:
Can unauthorized users gain access to sensitive data with Copilot?

Answer: No.

This won't happen with Copilot because it uses "admin on behalf of" rights for the user logged in. This means the rights are limited to that specific user and that user only. Copilot runs queries as the user, so it never has elevated privileges beyond what the user has.

Myth 2:

Data privacy and ownership

Ensuring data privacy is essential for an organization to create a culture of transparency, build customer trust, and meet compliance regulations. When considering generative AI solutions, security leaders are concerned that their customer data will be used to train other models, which could ultimately jeopardize the organization's reputation. This won't happen when you work with a trusted technology partner.

Frequently asked question:
Will my customer data be used to train language models in Copilot?

Answer: No.

At Microsoft, we're setting the standard for security, privacy, and compliance when it comes to AI. This is true not only for Copilot for Security, but for all our AI offerings.

By default, Microsoft doesn't train language models on customer data. There's a dedicated opt-in functionality within Copilot for customers who choose to contribute to collective security and innovation in AI.

When it comes to data, unlike ChatGPT, Copilot is grounded in the unique context of your organization. That means when you ask Copilot any question, the answer will be based on what's happening in your organization at that moment. Your data isn't used to train the foundation AI models. It's a closed learning loop that continuously improves based on your use.

Built with security, privacy, and compliance

Your data is your data.

Your data is not used to train the foundation AI models.

Your data is protected by the most comprehensive enterprise compliance and security controls.

Frequently asked question: Is transferred data protected from unauthorized access?

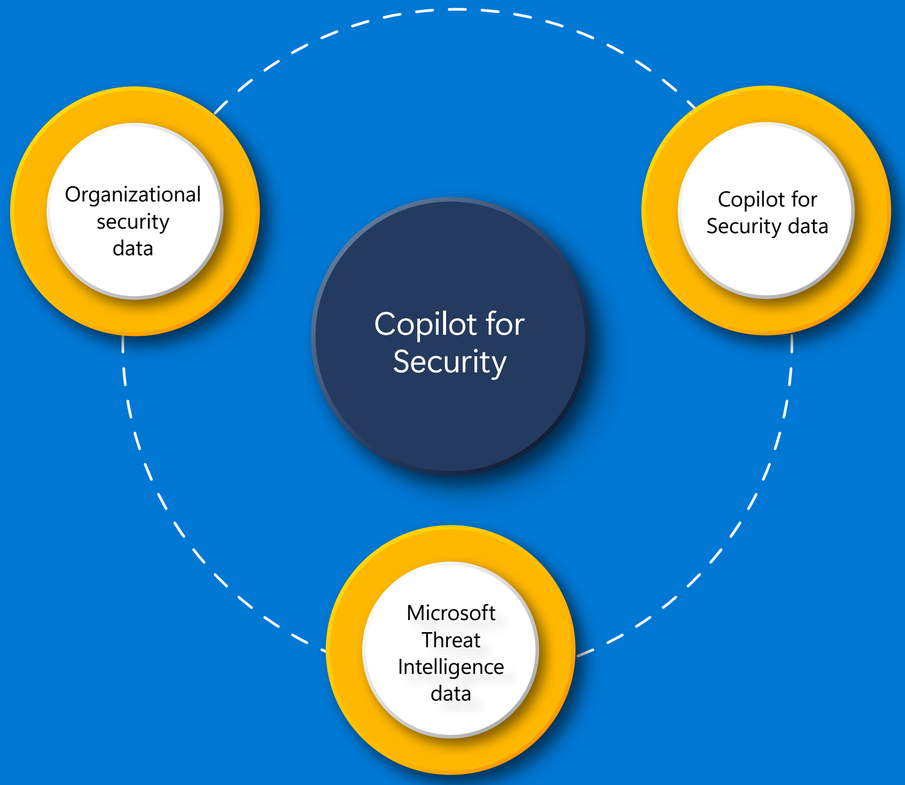
Answer: Yes.

No human users have access to the database, and access is restricted to the private network where the Copilot for Security application is deployed. If access is required for a human to respond to an incident, then the on-call engineer will need elevated access and network access approved by authorized Microsoft employees. Copilot complies with all Microsoft privacy, security, and compliance requirements.

When using Copilot for Security, your data:

- Is your data.
- Is stored where you choose and always encrypted at rest.
- Isn't used for sales or shared with third parties.
- Is housed in systems governed by Microsoft SOC and International Organization for Standardization-certified processes.
- Isn't used to train foundation AI models.
- Is never shared with OpenAI.
- Is protected by the most comprehensive enterprise compliance and security controls.

Powered by data that's unique to you and your organization



Myth 3:

Data leakage and exposure

In the past year, 74% of organizations experienced an incident that exposed business data, such as intellectual property.[3] Data breaches are extremely costly for organizations, and not just in the financial sense. These incidents also diminish the trust of customers who may become the victims of identity theft, credit card fraud, or other malicious activities because of the breach. With so much at stake, security leaders are understandably concerned that new technologies such as generative AI could lead to data leakage.

Frequently asked question: Could Copilot expose my data to others using the tool?

Answer: No.

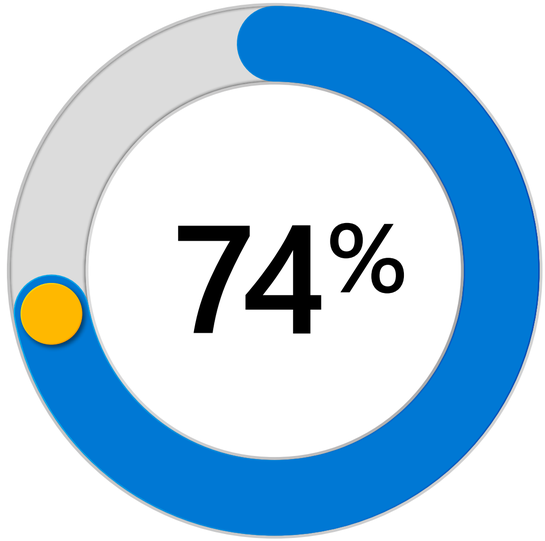
Copilot for Security was designed based on responsible AI. It includes the same security, privacy, and compliance controls as other trusted Microsoft products, as well as AI-specific safety mechanisms. Your data is analyzed within the Copilot system and doesn't leave the Microsoft Azure production tenant. Per Microsoft standards, your data is encrypted in transit and at rest.

Plus, session data is stored only in logs and for runtime purposes to operate the service. In the runtime database, when a session is deleted using the in-product user experience (UX), all data associated with that session is marked as deleted, and the time to live (TTL) is set to 30 days. After the TTL expires, the data can't be accessed by any queries. At that time, the data is physically deleted by a background process.

Additionally, there are periodic database backups, which will age out. These have short-lived retention periods.

Copilot:

- Runs queries as its user, so it never has elevated privileges.
- Is an Azure production service and is protected by Microsoft security controls.[4]
- Stores limited data (logs and investigation context) and encrypts all data it uses at rest.
- Is within the EU Data Boundary—a geographically defined boundary within which Microsoft has committed to store and process customer data and personal data for enterprise online services.



of organizations experienced an incident that exposed business data

[3] Data Security Index, Microsoft, Oct 2023
[4] Protection of customer data in Azure, Microsoft Learn

Myth 4:

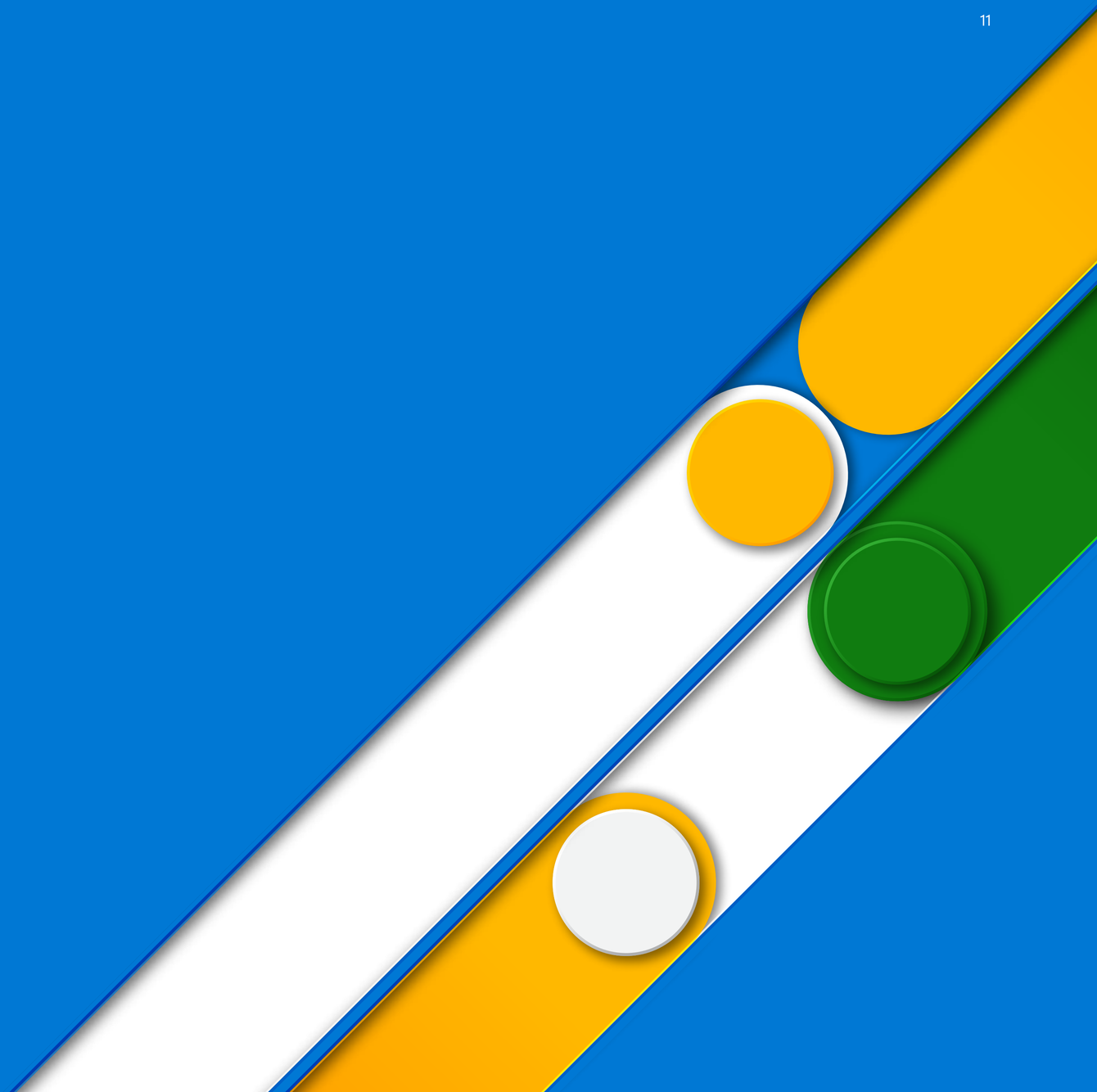
Compliance issues

Helping your organization meet compliance requirements may be one of the most demanding business challenges you face as a security leader. Many organizations must comply with a range of strict business and regulatory requirements that vary by region and industry. In some cases, noncompliance could result in financial penalties or cause your organization to lose access to an entire market segment. Considering the complexities of the current compliance landscape, some security leaders are concerned that new generative AI solutions won't meet requirements. With trusted solutions like Copilot, this isn't a problem.

Frequently asked question:
Does Copilot for Security meet industry or regional compliance requirements?

Answer: Yes.

Copilot meets General Data Protection Regulation (GDPR) requirements for EU markets by implementing the Azure Public Preview requirements. It stores all EU customer data within the EU Data Boundary and is available in multiple languages. Copilot also provides compliance controls to help you meet business and regulatory requirements.



AI augments human expertise, not the other way around.

Myth 5:
Hallucinations

Cautionary tales about an AI phenomenon called hallucinations have become all too common. A hallucination is content generated by a language model that appears plausible but is either factually incorrect or irrelevant. It comes across as qualified knowledge, and is delivered in a confident response, but it's false.

These hallucinations become an even bigger problem when humans:

- Accept the content as fact without verification.
- Assume the content is free from bias or misinformation.
- Rely on the content for critical decisions without human input or oversight.

While this is an understandable concern, hallucinations aren't an issue when you use transparent AI solutions that empower humans to make their own decisions.

Frequently asked question: Does Copilot for Security help detect hallucinations?

Answer: Yes.

Trust is paramount in security. If you can't trust security data and insights, you can't achieve the right outcomes. For humans to confidently work with AI-powered tools such as Copilot, it's critical to build trust in the technology.

At Microsoft, we're committed to responsible AI, which is why Copilot is designed to:

- Show reasoning, sources, debug, and runtime.
- Ensure data is compliant, secure, and private.
- Address harms and hallucinations.
- Be transparent and allow for an open dialogue.

With or without hallucinations, it's critical that people always feel confident they're in control when using AI-powered tools. AI augments human expertise, not the other way around.

With Copilot, the goal is to help security teams achieve positive security outcomes more efficiently without an overreliance on AI. Security analysts get suggestions from Copilot to help them act on insights, but it's up to them to decide whether and how to use these recommendations.

In other words, the human decides what to trust, what to share, what's important, what's relevant, and when and how to take action. Copilot users can not only control and grade the AI output, but also edit and correct the AI outputs and provide feedback.

Human creativity and knowledge will always be imperative for cybersecurity. Copilot is designed to complement your security team's skills and expertise so they can work faster, more accurately, and more proactively.

3

Give your security team an edge with industry-leading generative AI

As AI-powered capabilities become more prevalent in cybersecurity, and cyberthreats grow increasingly complex, generative AI is quickly becoming essential for SOCs. Microsoft Copilot for Security is a comprehensive, generative AI cybersecurity solution that can help you:

- Empower cybersecurity talent with the insights and expertise they need to understand what's going on in the environment and take action.
- Advance the work of less experienced team members through step-by-step guidance and alleviate tedious tasks for senior staff so they can focus on more strategic priorities.
- Put critical guidance and context at your security team's fingertips so they can respond to incidents in minutes instead of hours or days.
- Streamline reporting and prepare customizable reports for your executive leadership team and board of directors.
- Turn vast quantities of data signals into key insights to cut through the noise, detect and respond to cyberthreats in minutes, and reinforce your security posture.

Boost productivity to new levels with Copilot for Security

The Microsoft Office of the Chief Economist conducted a study[5] to test the productivity gains experienced security professionals achieved with Copilot for Security, and the results exceeded expectations.

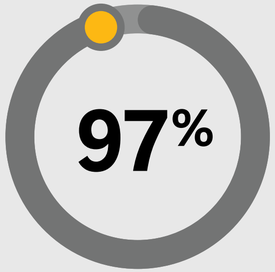
Using Copilot for Security, security professionals were:

- 22% faster across all tasks
- 7% more accurate across all tasks
- 14% faster at analyzing scripts
- 12% more accurate at script analysis
- 39% faster at summarizing an incident

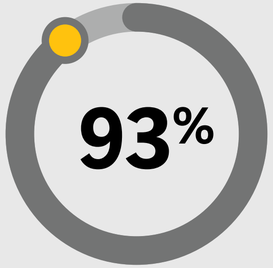
Plus, analysts using Copilot for Security created incident summaries with 49% more incident facts.

[5] Microsoft Copilot for Security randomized controlled trial (RTC) with experienced security analysts conducted by Microsoft Office of the Chief Economist, January 2024.

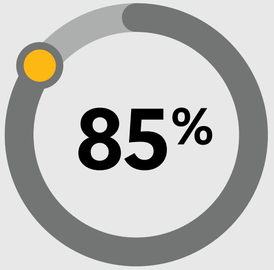
When asked about their experience:



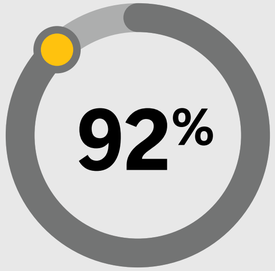
97% of security professionals said they want Copilot next time they do the same task.



93% reported Copilot helped them improve the quality of their work.



85% reported Copilot reduced effort on tasks.



92% reported that Copilot made them more productive.

With Copilot, you'll also get leading threat intelligence and threat signals from around the world. Threat intelligence is constantly evolving, so it's critical for organizations to stay up to date.

Microsoft Threat Intelligence:

- Synthesizes 65 trillion signals a day, across all types of devices, apps, platforms and endpoints, using industry-leading AI.
- Protects more than 1.4 billion endpoints across the planet comprising mobile devices, servers, IoT devices, and PCs.
- Graphs the entire internet every day to map out cyberattackers and their infrastructure.

Plus, 8,500 Microsoft security engineers and researchers are hard at work digging deeper into unknown signals to determine their true nature.

All Copilot for Security customers get premium workbench access to Microsoft Defender Threat Intelligence (MDTI) at no additional cost (API not included). MDTI helps you directly access, ingest, and act upon the massive Microsoft repository of finished and raw threat intelligence to expose and neutralize cyberattackers.

Welcome to a new era in cybersecurity

If you want to outpace cyberattackers in the era of AI, it's more important than ever to equip your team with next-generation security tools. Empower your analysts to gain an edge against cyberthreats with built-in security, compliance, and privacy controls from Microsoft Copilot for Security.

Learn more about Microsoft Copilot for Security

Learn how to solve today's challenges with AI