Copilot for Security in healthcare

Gain future-proofed protection
with advanced AI and Avanade expertise

avanade

Healthcare pays the highest price of any sector for cyberattacks

The surge in cyberattacks and a global shortage of security talent is making healthcare organizations increasingly vulnerable. As threat actor tactics become more advanced, now is the time to take a new look at the heightened protections generative AI powered security solutions offer.

Hospital mortality rises in the aftermath of an attack. Doctors are unable to look up past medical care, or check patient allergies, for example. Scheduled surgeries can be canceled, and ambulances rerouted because a cyberattack has disrupted electronic communications or medical records and other systems.

$10.93M

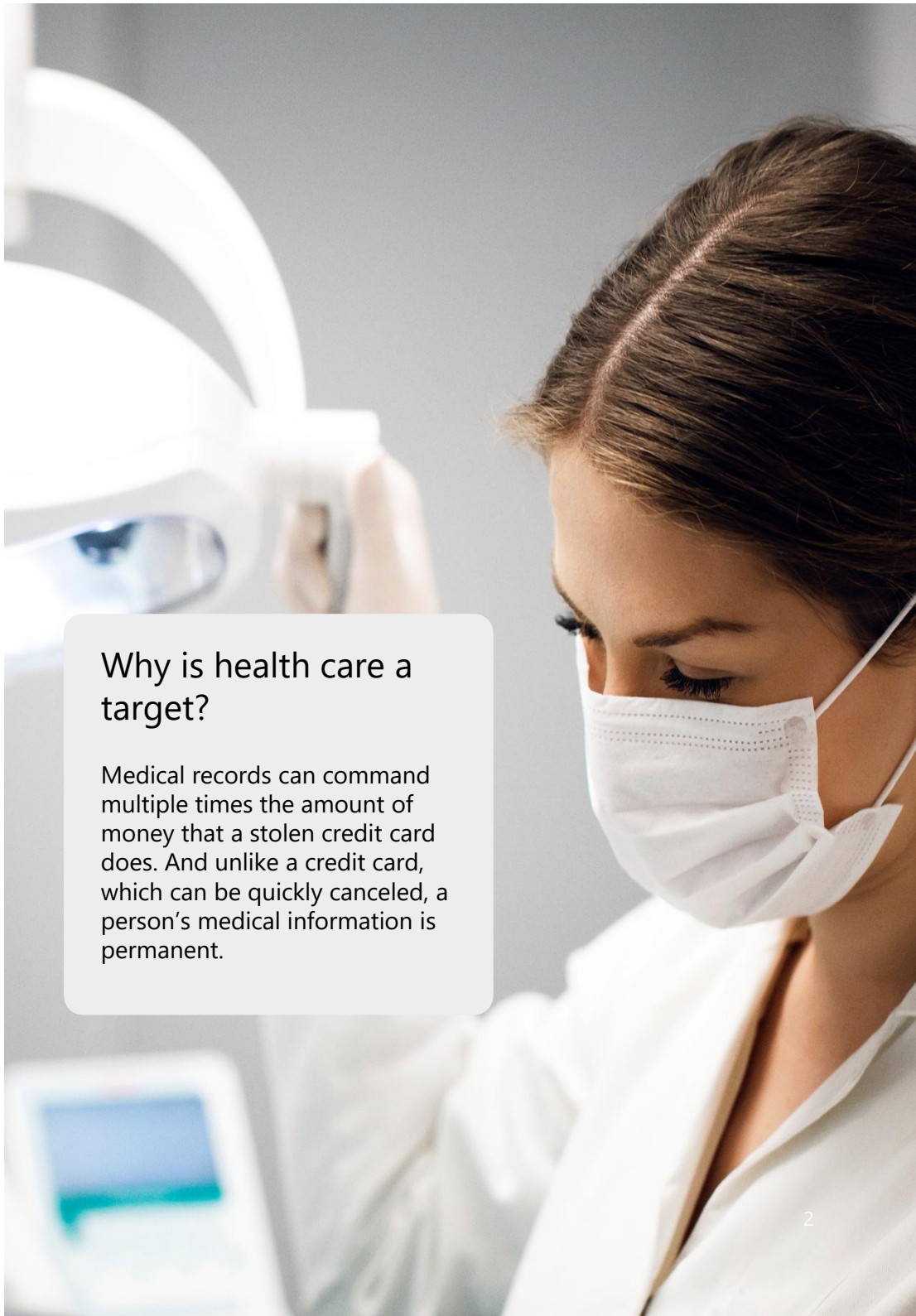
is the global healthcare industry reported cost of a data breach -- almost double that of the financial industry

World Economic Forum

79.7%

of healthcare data breaches in the U.S. were due to hacking incidents in 2023

HIPAA Journal



Why is health care a target?

Medical records can command multiple times the amount of money that a stolen credit card does. And unlike a credit card, which can be quickly canceled, a person's medical information is permanent.

Copilot for Security:

Changing the game in cybersecurity

With the power of generative AI, Copilot for Security holds tremendous promise to aid Healthcare Defenders in thwarting the sophisticated threats posed by malicious actors.

While the era of AI gives us tools that can be used to bolster defenses, it also creates a new way for malicious actors to launch new and advanced attacks.

Generative AI arms data security professionals with lightning-fast processing, rapid pattern recognition, and continuous learning and improvement to rapidly investigate and mitigate new and growing risks.

Copilot for Security assists novice and professional security experts greater speed and accuracy

Microsoft Copilot for Security not only natively integrates with the Microsoft Security platform but is also highly extensible and backed by a rich ecosystem of partner integrations.

It aids security, data and identity departments close the talent gap and overcome the challenge of disconnected tools to respond more effectively and faster to threats and admin tasks.

Your all-in-one security assistant

Copilot for Security gives users a single incident experience and an end-to-end view of threats across their digital estate. With just one set of automation rules and playbooks enriched with generative AI, coordinating responses to attacks is easier and quicker.

Based on a Microsoft study, security operations center (SOC) tasks finished faster with overall greater speed and accuracy for novice and professional security experts. More than 93% of users wanted to use it again.

Microsoft proprietary Security Large Language Model, built using Microsoft's World Leading Open AI platform, backed by Enterprise Grade Security.

Early Copilot for Security Access Program: Microsoft invited Avanade to be part of an Early Access Program. Operational results from early access to Copilot for Security[1] have been overwhelmingly positive, with:

86% rise in productivity for 'new-in-career' analysts

40% time saving on core security operations tasks

44% increase in accuracy

26% speed boost for generated results

83% of respondents saying Copilot reduced the effort needed to complete a task

90% planning to use Copilot the next time they perform the same task

avanade

References

[1] Microsoft Copilot for Security randomized controlled trial conducted by Microsoft Office of the Chief Economist, November 2023

Microsoft Copilot for Security integrates advanced AI capabilities

Access to end-to-end security, identity and compliance across a portfolio of capabilities.

Copilot for Security brings together many of the applications your team may already be using. Only now with a coordinated experience, you can make a more rapid informed response and cover more threat vectors.

Device management

- Prompts to investigate suspicious device activity
- Natural language queries to pull information about device enrollments, compliance, sign-ins and hardware
- Execution of custom skills logic apps using to update configuration policies

Natural language KQL

- Ability to write Sentinel analytics rules using natural language
- Conversion of TTPs (tactics, techniques and procedures) identified in hunts or from threat intelligence into KQL (query language)
- Migration support from other products

Attack surface management

- Integration with external attack surface management (EASM) to get a summary attack surface that aids in incident investigation
- Logic apps integration to act on unmanaged devices

Vulnerability management

- Threat actor insights and list of technologies susceptible to the vulnerability
- Prompts to get mitigations and remediation recommendations
- Automated validation of vulnerabilities after remediation

Detection and response

- Natural language prompts and promptbooks for Microsoft Sentinel and Microsoft Defender XDR incidents
- Execution of logic apps to take remediation and actions as part of an incident
- Executive summary reporting and incident graphs

Identity access management

- Natural language querying of Entra
- Custom skill query for independent software vendor (ISV) products (i.e., "What access does user X have?")
- Embedded experience to bring Copilot into third party product

Data protection

- Natural language prompts to investigate data loss prevention incidents
- Custom skills using LogicApps to allow / block users / devices for data transfer
- Custom skills to update data classification and risk profile

Threat intelligence and threat hunting

- Natural language KQL (query language) for threat hunting (Microsoft Defender XDR and Microsoft Sentinel)
- Custom skills to pull threat intelligence information from external databases
- Prompts to get summary of recent threat intelligence

Game-changing results for security teams

Security Administrators and Security Operations Analysts are facing increasing pressures. Supported by Microsoft's unique global threat intelligence, Copilot removes laborious manual tasks and gives them the skills and insight to drive successful security outcomes.

Rapid incident response

In minutes, identify an attack, assess its scale, and start remediation based on real-world incidents.

Report on incidents at speed

Quickly summarize incidents and threats and prepare customized security reports.

Enhanced quality of life

Natural language prompts increase analyst engagement, retention and effectiveness, through improved quality of life.

Hunt threats and vulnerabilities

Pinpoint vulnerabilities using simple natural language prompts that examine your IT environment for breaches.

Address talent shortages

Get analysts up to speed with engineered promptbooks, designed to bridge the skills gap.

Skill development unique to every organization

Teams can leverage in-house knowledge to train Copilot to meet specific needs and extend out-of-the-box capabilities.

Start your Copilot for Security journey

To embrace AI for your future security operations, there are steps you can take today in readiness for Copilot adoption. Our end-to-end services can help you with this process and build a case for investment.

1 Become generative-AI literate

Begin generative AI fundamentals training within your teams, including essential prompt engineering basics.

2 Understand the technical pre-requisites

Copilot for Security works with other Microsoft security products to generate guidance, including Microsoft Defender XDR, Microsoft Sentinel, Microsoft Intune, Microsoft Entra, Microsoft Purview and Microsoft Defender for Cloud. The minimum requirements for use are Microsoft Defender for Endpoint and Microsoft Entra ID.

3 Identify your pain points

Look at the challenges and skills gaps within your Security Operations Center (SOC), teams and surrounding security services, such as Entra, Intune and Purview. Then map out Copilot's capabilities against these pain points to establish tangible outcomes and benefits.

4 Assess key stakeholders

This could be anyone in your SOC team, as well as those who manage Entra ID, Intune, Purview, and Defender for Cloud. Capture use cases by examining your top three manual processes and identifying the ways that Copilot can bring value to your teams in these areas.

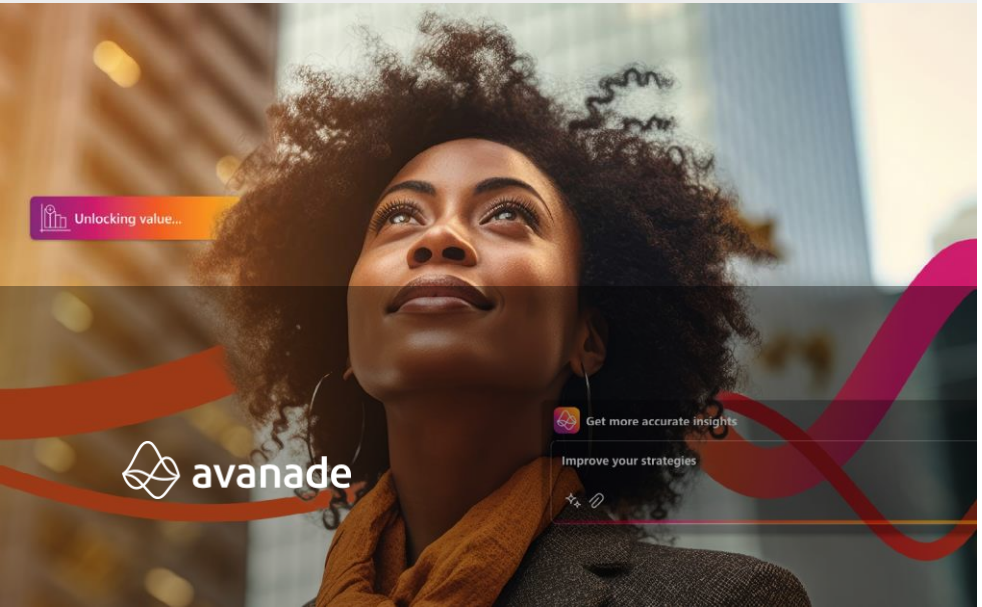
5 Develop a business case

Estimate the time you could save with Copilot, attribute a monetary value to it and then forecast this across all of your manual SOC processes to develop a return on investment. Then look to the future and consider what strategic projects your team could unlock if you achieved the projected time and monetary savings.

Avanade, leading the field in Copilot for Security adoption

As members of **Microsoft's Design Advisory Council for Copilot for Security**, we have a deep understanding of how the technology works and how to get the best from it. Together with Microsoft, we've helped shape its functionality, ensuring it has the capabilities and features to protect our clients from ever evolving cyberthreats – now and into the future.

Our holistic approach, combining advisory, consulting and managed security, is complemented by an in-depth knowledge of AI learned from our work across 6,000+ AI projects for over 350 clients. This means we can help you create genuine human impact with Copilot protecting your customers, employees and data.



Awards

2x	Microsoft Security Zero Trust champion
18x	Microsoft Global Systems Integrator Partner of the Year
90+	Partner of the Year awards
60,000+	Microsoft certifications – more than any other partner

Microsoft Advanced Specializations

- Cloud Security
- Information Protection and Governance
- Microsoft Threat Protection
- Identity and Access Management

End-to-end services

- Security Advisory
- Security Consulting
- Managed Security Services

Member of
Microsoft Intelligent Security Association

Microsoft Security

Start your Copilot for Security journey, today

Avanade can give you an in-depth understanding of the value Copilot for Security can bring to your healthcare organization. We start by working with your security team to discover your business need and identifying the Copilot and Microsoft capabilities that can help. Then we take a deep dive into your pain points, creating a proposal for deployment and ongoing support.

Learn and Discuss: 1 to 2 hours

In this free discussion, find out how to get started with Copilot for Security, including our exclusive demonstration and readiness assessment.

Copilot for Security workshop: 2 hours

In this workshop, we identify your top three SOC pain points and manual investigation processes and show you how they can be transformed with generative AI. You'll come away with a detailed roadmap outlining how to deploy and modernize your SOC with Copilot for Security.

Deploy and Modernize: 6 weeks to 6 months

With our expert support and guidance, we make your deployment plan a reality.

Imagine what you will do with AI

Take the first step on your Copilot for Security journey.
Contact us to find out more about Copilot or to get started.

Start now

avanade

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

About Avanade

Avanade is the leading provider of innovative digital, cloud and advisory services, industry solutions and design-led experiences across the Microsoft ecosystem. Every day, our 60,000 professionals in 26 countries make a genuine human impact for our clients, their employees and their customers.

We have been recognized, together with our parent Accenture, as Microsoft's Global SI Partner of the Year more than any other company. With the most Microsoft certifications (60,000+) and 18 (out of 18) Gold-level Microsoft competencies, we are uniquely positioned to help businesses grow and solve their toughest challenges.

We are a people first company, committed to providing an inclusive workplace where employees feel comfortable being their authentic selves. As a responsible business, we are building a sustainable world and helping young people from under-represented communities fulfill their potential.

Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation.

Learn more at www.avanade.com.

Do what matters