avanade

Do what matters

AI-powered cyber resilience

Driving secure growth in the digital era

Robust cybersecurity is vital for fostering growth and innovation.

This guide explores the relationship between cybersecurity and AI, offering insights on how you can turn security challenges into opportunities. We discuss the escalating risks and the obstacles to effectively leveraging AI, while emphasizing the need for a comprehensive security strategy across all business functions.

We outline five strategies you can adopt to enhance cyber resilience, ensuring that security becomes a catalyst for growth. From securing your digital assets and optimizing your security tools to empowering your teams with AI capabilities, we share our experiences with Microsoft Security Copilot in combating evolving threats.

Cybersecurity as a catalyst for growth and AI adoption

Cyber resilience drives success

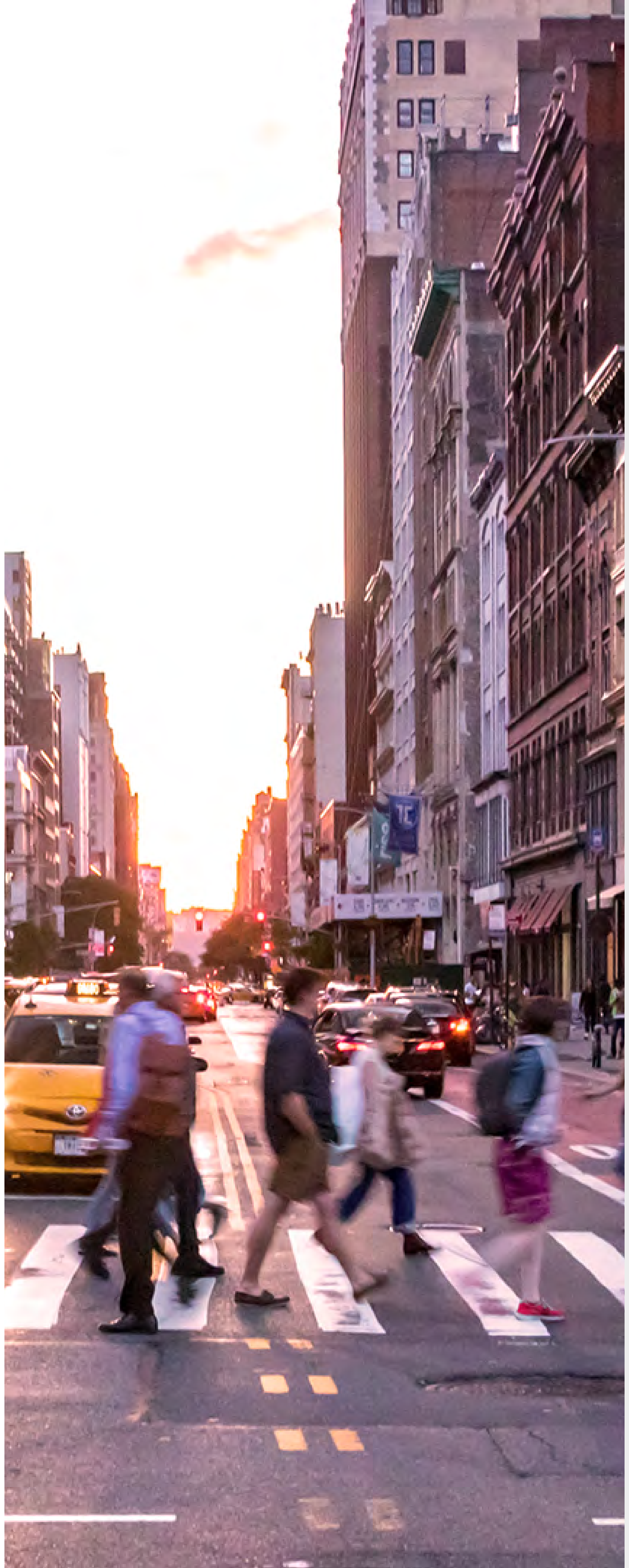
Avanade research shows that **57%** of IT leaders are prioritizing cybersecurity in the next year, aligning it with their organization's growth and AI goals.[2]

Security concerns are a significant barrier to AI implementation

A striking **93%** of organizations report that various security challenges, such as cloud security (42%), data protection (40%) and threat protection (38%), negatively impact their ability to adopt AI technologies.[2]

AI is transforming the threat landscape, creating both challenges and opportunities

While **99.9%** of respondents see its potential to enhance security, AI's complexity also increases the sophistication of threats, prompting organizations to proceed with caution.[2]



Cyber resilience is business resilience.

Building cyber resilience is a complex challenge in a constantly changing landscape. As the digital ecosystem expands, effective cybersecurity requires adapting to emerging threats and implementing effective strategies.

Strong security and recovery capabilities are essential for organizational resilience.

Research shows that companies viewing cybersecurity as a strategic enabler and aligning it with their goals are 18% more likely to see positive outcomes, including revenue growth, increased market share and enhanced customer trust.[1]

Unlock the potential of generative AI with strong cybersecurity.

As you embark on your growth and AI journey, cyber resilience is crucial. Security concerns can often impede or slow down AI projects, making it important to safeguard these initiatives to ensure they are trustworthy and reliable.

When AI is secure, you can fully use its capabilities without compromising safety. Addressing these security challenges is necessary to effectively implement AI and foster innovation.

AI - your security superpower.

Imagine using AI to strengthen your defenses against hackers, allowing for quicker detection, prevention and response to attacks.

Generative AI can lighten the load for stretched security teams by enhancing their skills and capabilities. By combining AI's processing power with human insight, you can gain a significant edge over cybercriminals.

To harness AI effectively, it's important to find the right balance, maximizing its benefits while managing associated risks.

Navigating the evolving security landscape

Security leaders are dealing with a growing set of challenges. The rapid expansion of the threat landscape, driven by digital adoption and remote work, has made managing risks increasingly difficult. Compounding these issues are complex regulations, limited budgets and the pace of emerging technologies. The rise in cyberattacks and a global shortage of skilled security professionals are also putting a strain on existing resources, limiting the ability to respond quickly to threats.

Many security teams are using more than 75 different cybersecurity tools, creating integration problems and security gaps.[3] As threat tactics become more advanced, organizations need to improve their resilience by adopting AI-driven solutions to automate threat detection and response, helping to strengthen overall protection.

78%

of organizations **fear a major cyber-attack could shut them down.**[2]

92%

of enterprises say that data security is **one of the greatest concerns** related to their adoption of AI.[2]

76%

of enterprises admit **they lack the in-house skills** to handle security effectively.[2]

$4.88m

the average **cost of cyber crime**, driven by data breaches, ransomware attacks and financial fraud.[4]

Strengthening cybersecurity

Five key steps

Step 1

See the big picture: Aligning cyber strategy, compliance and risk

To effectively manage cybersecurity, start by developing a cyber strategy that addresses your overall risks. Begin with understanding your organization's priorities to ensure alignment across your commercial, IT and cyber strategies. This alignment creates a cohesive approach.

Additionally, incorporate a compliance strategy to meet regulatory requirements and industry standards. A proactive compliance strategy not only ensures adherence to legal mandates but also enhances your security framework by integrating best practices, minimizing risks and fostering a culture of accountability.

Also consider undertaking a thorough risk assessment. This should give you a clearer view of your risk posture and key vulnerabilities. This proactive step will help you develop strategies to defend against evolving cyber threats, including ransomware, insider threats and system vulnerabilities, ensuring your defenses are always a step ahead.

Step 2

From siloed to seamless: Integrating security throughout your organization

Security is essential across all aspects of an organization, influencing everything from daily operations to long-term strategies. However, security teams are often siloed, operating in isolation rather than being integrated throughout the organization. This disconnect can create gaps in protection, leaving vulnerabilities that affect multiple functions. For security to be truly effective, it must be embedded across all areas, following a "secure by design" approach.

This means incorporating security considerations from the outset, ensuring they are embedded in every process, technology and all functions, to create a resilient and unified defense strategy.

Step 3 - Accelerate growth: Securing your digital core

Securing your digital core - the critical technology capability that brings together key components like cloud, data and AI - is vital for fostering growth and innovation. By prioritizing cybersecurity, organizations can establish a solid foundation that allows them to effectively leverage advanced technologies.

Cloud security

Cloud security is crucial for enhancing resilience during cloud transformations. By focusing on getting the fundamentals right, you can enable a smooth and secure transition to the cloud. A modular approach can help establish robust guidelines and optimize your overall cloud security posture, integrating security measures at every stage of the journey. Zero trust principles also ensure security is integrated across platforms, cloud services and infrastructure.

Data security

To protect sensitive data, we recommend developing a comprehensive data protection strategy. This can help you:

- Assess your current measures
- Implement strong security protocols
- Ensure compliance with regulations
- Establish data loss prevention measures

Regularly reviewing and optimizing security tools is also essential for minimizing risks. This approach helps create a secure data foundation, enhances visibility and strengthens overall resilience against potential breaches.

Advanced identity

To establish a strong identity and access management (IAM) foundation, focus on strategies that promote trust and resilience within your organization. Integrate IAM practices that enhance security and efficiency across your operations, using a mix of internal expertise and reliable third-party tools. Regularly assess and update your IAM strategies to address new challenges and technologies. This proactive approach will help safeguard sensitive information and support growth securely. A robust IAM framework is essential for creating a resilient environment that aligns with your digital transformation efforts.

Emerging technologies

Emerging technologies are reshaping how organizations operate. To stay competitive, it's important to integrate information technology (IT) with operational technology (OT) and use connected devices to improve operations and meet customer demands. A strong cybersecurity strategy tailored to these technologies is essential. It protects your operational environment and secures the connected products and services that drive your organization, allowing you to fully benefit from digital transformation.

Step 4

Cyber defense: Using AI to stay ahead of fast-moving threats

With cyber attacks becoming more frequent and complex – 77% of organizations are reporting increased difficulty in detecting and managing cyber risks[5] – organizations must shift away from using traditional, fragmented threat hunting methods that rely on numerous costly security tools.

To strengthen your security posture, consolidate your tools for better visibility across the threat landscape. This allows for quicker threat remediation and reduces the burden on your teams. Incorporate AI and automation into your security strategy to stay ahead of evolving threats and improve your detection and response capabilities.

81%
of security executives agree that staying ahead of attackers is a constant battle, and the cost is unsustainable.[6]

Step 5

Support talent: Empowering security teams and fostering collaboration

Security is about enabling your organization and adapting to a changing environment, not just protecting assets. It requires investing in security education and fostering collaboration – especially between development and security teams – to maximize the use of tools. With a cybersecurity skills shortage, supporting talent development is vital. Prioritize training and resources to equip your workforce for emerging threats. By promoting continuous learning and engaging all employees, you can strengthen security practices and encourage a proactive approach to managing risks.

How we've helped our clients build resilience against cyberthreats

EDF makes a secure move to the cloud

EDF's new Hinkley Point C station - Europe's largest current construction project - will provide 20% of the UK's electricity. The company needed its data and applications securely in the cloud to support this massive project. Avanade planned the migration and helped build the secure cloud and application platform.

The result

We helped EDF enable more secure collaboration among employees and better compliance with industry regulations. Avanade's factory model expands the Azure platform on which sensitive nuclear information can securely sit - a world first.

Better security at LifeWorks empowers new ways of working

When LifeWorks wanted to improve its security and enhance its employee experience, it turned to Avanade. We worked with the company to explore existing security policies and tools, using Microsoft Secure Score to determine high-risk areas and map Microsoft 365 E5 security tools against business needs.

The result

LifeWorks has a stronger security posture, can easily detect and respond to security issues and provides an enhanced workplace experience and more secure remote working capabilities.

Global hotel chain optimizes security portfolio and licensing

This global hotel chain faced a 62% increase in software costs across its secure modern workplace space. Avanade responded by optimizing the company's licensing, aligning its technology strategy with Microsoft and establishing a strategic partnership with Microsoft.

The result

We developed a Microsoft roadmap and security strategy, which resulted in a five-year projected $11.7 million reduction in total cost of ownership.

Avanade case study

How AI empowers our security team

Security focus

At Avanade, protecting our global teams is a top priority. With a distributed workforce relying on the internet as our primary network, we adopt a zero trust approach to security. We use managed security services from our parent company, Accenture, while our internal team manages escalations and oversight. Through our early preview work with Microsoft, we've been utilizing the power of Microsoft Security Copilot within our own business.

The value of Microsoft Security Copilot

We've integrated Microsoft Security Copilot at every level of our team, enhancing productivity from senior analysts to interns. Senior analysts use it for complex tasks, like writing KQL queries, while junior analysts benefit from natural language prompts to build their skills quickly. Copilot also helps identify vulnerabilities from emerging threats, curating necessary information for informed decision-making. Its continuous learning capabilities ensure it adapts to our evolving security needs.

Discover how we're unleashing Microsoft Security Copilot

Greg Peterson, Avanade's Senior Director of Security, Technology and Operations, reveals how we've been using Copilot to upskill and empower our security teams.

Watch now

> *"Copilot for Security will be critical in helping us close the talent gap, helping junior analysts get up to speed more quickly and free up time by allowing more senior team members be more effective."*

— **Greg Petersen**
Senior Director of Security Technology and Operations, Avanade

Is your security strategy fit for the future?

Top six questions to tackle now

01
Are your organizational, IT and cybersecurity priorities aligned?

What specific challenges are you encountering in achieving compliance and meeting regulatory requirements?

02
Is your security landscape overly complex?

Are you relying on multiple tools and products, and would you like to explore options for reducing costs and simplifying your approach?

03
Has security been embedded into your cloud strategy?

What initiatives are you undertaking to ensure compliance in the cloud, and would you benefit from assistance in evaluating your cloud security posture?

04
What strategies are you considering to enhance your identity and access management (IAM) practicwes?

Do you believe your IAM can adapt to evolving threats, and are you interested in learning how to future-proof these practices?

05
What measures are you implementing to protect sensitive information and comply with data protection regulations?

Would you like to explore strategies for building a scalable, secure data foundation, achieving full data visibility and implementing effective data loss prevention measures?

06
Have you considered integrating AI into your security operations for quicker threat detection?

Which tools, like Security Copilot, are you currently exploring or utilizing to improve your security operations?

Enhance your cyber resilience with a trusted partner

At Avanade, we specialize in securing Microsoft and hybrid IT environments through a comprehensive approach that integrates advisory, consulting and managed security services. With deep AI expertise, gained from over 6,000 AI projects for 350+ clients, we provide customized solutions for evolving security challenges.

How we help:

Cyber strategy: Align organizational, IT and cybersecurity priorities for cohesive risk management and understand and adhere to compliance and regulatory requirements

Cyber protection:

- **Cloud security:** Implement enterprise-grade, compliant security throughout your cloud journey
- **Identity and access management:** Build resilient IAM strategies that adapt to threats
- **Data protection:** Develop strategies to safeguard sensitive information
- **Emerging technologies:** Leverage emerging technologies safely so that you can drive your business forward confidently

Cyber defense: Utilize AI for rapid threat detection, modernize operations with tools like Security Copilot and provide advanced protection through managed extended detection and response (MXDR)

Get started with:

Risk assessment. Our risk assessment service helps identify, prioritize and mitigate security risks. By outlining your vulnerabilities, we create a tailored remediation plan with proactive strategies to defend against evolving threats, such as ransomware and insider risks. Our comprehensive analysis provides an unbiased evaluation of your IT environment, highlighting areas for improvement and best practices for prioritizing security efforts.

Cyber portfolio evaluation. We offer a cyber portfolio evaluation to map your existing tools against Microsoft's security solutions. This can streamline your security roadmap and potentially reduce costs by up to 60%, enhancing both efficiency and risk management.

Microsoft Security Copilot. Avanade can give you an in-depth understanding of the value Security Copilot can bring to your organization. We start by working with your security team to discover your needs 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.

Visit **www.avanade.com/security** to see how Avanade can help you build cyber resilience.

Leader in the IDC MarketScape

Worldwide Cybersecurity Consulting Services 2024

2x

Microsoft Security Zero Trust champion

18x

Microsoft Global Systems Integrator Partner of the Year

End-to-end services

- Security Advisory
- Security Consulting
- Managed Security Services

Microsoft Security

Member

Microsoft Intelligent Security Association

Microsoft Design Advisory Council for Security Copilot Member

Together with Microsoft, we've helped shape Security Copilot's functionality, ensuring it has the capabilities and features to protect our clients from ever evolving cyberthreats - now and into the future.

Microsoft Advanced Specializations

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

avanade

Do what matters

AI-powered cyber resilience

About Avanade

Avanade is the world's leading expert on Microsoft. Trusted by over 5,000 clients worldwide, we deliver AI-driven solutions that unlock the full potential of people and technology, optimize operations, foster innovation and drive growth.

As Microsoft's Global SI Partner we combine global scale with local expertise in AI, cloud, data analytics, cybersecurity, and ERP to design solutions that prioritize people and drive meaningful impact.

We champion diversity, inclusion, and sustainability, ensuring our work benefits society and business.

Learn more at www.avanade.com

Sources:

1. Accenture, "State of Cybersecurity Resilience 2023."
2. Vanson Bourne, "The State of Cybersecurity 2024."
3. Panaseer, "2022 Security Leaders Peer Report."
4. IBM, "Cost of a Data Breach Report 2024."
5. Forrester, "The Total Economic Impact™ Of Microsoft SIEM And XDR, 2022."
6. Accenture, "State of Cybersecurity Resilience 2021."