Microsoft Security

Navigating Cybersecurity in the AI Era: Key Insights and Strategies

AI is rapidly reshaping the cybersecurity landscape. This guide, drawing insights from the 2024 Microsoft Digital Defense Report, explores four key themes to strengthen your security strategy:

- **AI security fundamentals**
  Learn how to implement AI responsibly and defend against emerging threats.
- **Identity protection**
  Discover emerging approaches to authentication and access management in an AI-enabled world.
- **AI-powered threat response**
  See how organizations are using AI to spot and respond to threats faster.
- **Securing the multicloud world**
  Understand new challenges in protecting data across cloud environments.

The content that follows presents detailed data and trends related to these themes, offering actionable insights to bolster your cybersecurity strategy.

AI security fundamentals

How can organizations harness the power of AI for security while mitigating its inherent risks? Recent data reveals key focus areas for building robust AI security practices:

Governance

The rapidly evolving AI regulatory landscape necessitates international standards to ensure responsible AI use and mitigate safety risks.

2
international standards for AI security[1]

Risk management

Microsoft's 1.6 billion risk evaluations highlight the ongoing battle against sophisticated e-commerce fraud, leveraging AI to detect and prevent unauthorized transactions effectively.

1.6 billion
payment fraud risk evaluations conducted in the last year[2]

Data protection

Threat actors target overprivileged cloud applications to access high-value resources. Secure development practices—including minimal permissions and protected test environments—can help mitigate these risks.

97.4%
of workload identity permissions were unused in the past year[3]

Threat detection

Despite a sharp rise in ransomware attempts, improved automatic disruption capabilities helped reduce successful encryptions significantly. Most breaches occurred through unmanaged devices lacking proper security.

2.75x
increase in ransomware-linked encounters[4]

3x
decrease in ransom-stage attacks[5]

Integrated cybersecurity resources

E-book: Four Imperatives to Secure and Govern AI, A Playbook
Get step-by-step guidance on securing and governing AI while protecting sensitive data.

Data security resources
Improve your data security with expert guidance.

Microsoft Digital Defense Report 2024 (p. 25, 43, 45, 47)
Drive deeper into the data behind this section's featured insights.

Learn more about our AI-driven cybersecurity solutions

Identity protection

In the age of AI, robust identity protection is more critical than ever. Learn how AI-enhanced authentication and Zero Trust principles help organizations defend against increasingly sophisticated attacks:

Identity attacks

Cybercriminals launch 600 million identity-based attacks daily, primarily targeting cloud services through phishing and malware. AI-driven monitoring helps detect and block these threats in real time.

99%
of identity attacks are password based[6]

AI-enhanced authentication

While MFA helps prevent breaches, attackers increasingly target authentication systems. Organizations are turning to AI-powered detection to protect their identity infrastructure from sophisticated bypass attempts.

41%
MFA adoption rate among Microsoft customers[7]

Security defaults

Simple changes yield significant results: Enabling MFA and disabling legacy authentication reduce breach compromises by 80%. These security defaults offer a clear starting point for strengthening identity protection.

80%
fewer compromises in tenants using security defaults[8]

Integrated cybersecurity resources

E-book: The Fundamental Guide to Zero Trust: A Leadership Approach to AI-enhanced Security
Learn how to build a Zero Trust security framework that protects AI-enabled systems.

Microsoft Digital Defense Report 2024 (p. 41, 49, 63)
Drive deeper into the data behind this section's featured insights.

Explore our identity and access management solutions

AI-powered threat response

Staying ahead of threats requires real-time intelligence. Here's how AI and automation are transforming threat detection and response:

Global threat monitoring

This unprecedented scale of security monitoring enables swift detection of emerging threats. Organizations benefit from automated analysis that would be impossible through manual methods alone.

78 trillion
security signals analyzed daily[9]

Extensive threat intelligence network

Microsoft Threat Intelligence now tracks more than 1,500 unique threat groups—including more than 600 nation-state threat actor groups, 300 cybercrime groups, 200 influence operations groups, and hundreds of others.

1,500
unique threat groups tracked[10]

Fraud prevention

Automated detection plays a key role in combating cyber fraud, which caused $1 billion in losses in 2023. Rapid identification and suspension of malicious accounts help disrupt criminal networks before they can cause harm.

64 million
abusive service accounts suspended annually[11]

Integrated cybersecurity resources

Cyber threat protection resources
Optimize your security operations with expert guidance.

E-book: Microsoft Security Copilot: Safeguards for the Age of AI
Discover how AI-powered Copilot transforms security operations and enhances team capabilities.

Microsoft Digital Defense Report 2024 (p. 5, 42)
Drive deeper into the data behind this section's featured insights.

Learn more about AI-powered threat response

Securing the multicloud world

Protecting data across multiple cloud platforms presents unique challenges. Explore recent data insights and best practices for securing your multicloud environment:

Unnecessary cloud risks

Microsoft's analysis reveals a concerning trend: Over half of cloud workload identities sit inactive while 1.5 million credentials remain exposed in repositories. This widespread overprovisioning creates necessary security risks. Organizations should prioritize regular reviews and deactivation of unused identities.

51%
of workload identities are inactive[12]

Secure development in the cloud

Microsoft research revealed that nearly one in five code repositories contained exposed secrets last year. To mitigate this widespread risk, organizations should implement secure development practices like minimizing permissions and preventing credentials in code.

18%
of code repositories exposed secrets[13]

Integrated cybersecurity resources

Executive Summary: The New Zero Trust Guide for CISOs: Perimeter-free Security for the Age of AI-accelerated Threats
Learn how to implement Zero Trust security principles in an AI-accelerated threat landscape.

Microsoft Digital Defense Report 2024 (p. 65, 71)
Drive deeper into the data behind this section's featured insights.

Learn more about data security solutions and tools

Strengthening your security posture in the age of AI

As AI transforms the cybersecurity landscape, organizations need a comprehensive approach that addresses both new opportunities and emerging threats. Success requires integrating AI capabilities thoughtfully across your security strategy while maintaining strong fundamentals in identity management, threat detection, and cloud security.

Start your journey today.

To strengthen your security posture and enhance threat detection, explore our AI cybersecurity solutions.

To secure your cloud infrastructure and enhance visibility, learn more about our cloud security posture management solutions.

For more details on the data points featured in these infographics, please see the Microsoft Digital Defense Report 2024.

© 2025 Microsoft Corporation. All rights reserved. This document is provided "as is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. This document is provided "as-is." You may copy and use this document for your internal, reference purposes.

[1] "Microsoft Digital Defense Report 2024," page 105. Microsoft, 2024.
[2] "Microsoft Digital Defense Report 2024," page 43. Microsoft, 2024.
[3] "Microsoft Digital Defense Report 2024," page 45. Microsoft, 2024.
[4] "Microsoft Digital Defense Report 2024," page 47. Microsoft, 2024.
[5] "Microsoft Digital Defense Report 2024," page 47. Microsoft, 2024.
[6] "Microsoft Digital Defense Report 2024," page 49. Microsoft, 2024.
[7] "Microsoft Digital Defense Report 2024," page 63. Microsoft, 2024.
[8] "Microsoft Digital Defense Report 2024," page 63. Microsoft, 2024.
[9] "Microsoft Digital Defense Report 2024," page 5. Microsoft, 2024.
[10] "Microsoft Digital Defense Report 2024," page 42. Microsoft, 2024.
[11] "Microsoft Digital Defense Report 2024," page 71. Microsoft, 2024.
[12] "Microsoft Digital Defense Report 2024," page 65. Microsoft, 2024.
[13] "Microsoft Digital Defense Report 2024," page 65. Microsoft, 2024.