Microsoft

Microsoft Digital Defense Report 2025 CISO Executive Summary

Lighting the path to a secure future

A Microsoft Threat Intelligence report

Introductory statement by Amy Hogan-Burney and Igor Tsyganskiy from the full report

Mobilizing for impact:

Cybersecurity leadership in a defining era

Amy Hogan-Burney
Corporate Vice President,
Customer Security & Trust

Igor Tsyganskiy
Corporate Vice President and
Chief Information Security Officer

We are living through a defining moment in cybersecurity. As digital transformation accelerates, supercharged by AI, cyber threats increasingly challenge economic stability and individual safety. Cyber threats are rapidly evolving from technical problems affecting business to events impacting all aspects of our society.

The pace of change in the threat landscape has pushed us to rethink traditional defenses. The growth and adoption of AI by both defenders and threat actors benefits both sides. AI in cybersecurity is already creating new challenges for security organizations as they rush to adapt systems, understand new threats, and equip their people with new knowledge to keep pace.

Cyber threats are also playing an increasingly significant role in geopolitical conflicts and criminal activities, creating both a wide and deep scope of responsibility for defenders. AI will play a critical role in helping security professionals productively address the growing threat landscape, but as an industry we must step into this new paradigm cautiously. With the increased speed of an AI-centric world, the impact of action–whether by security organizations, criminal actors, or nation states–will have faster and potentially greater second, third, or fourth-order effects. It is imperative that defenders consider these ripple effects as they implement new security controls, share security research, fix new security vulnerabilities, and collaborate with each other.

Adversaries, whether nation-states, criminal syndicates, or commercial cyber mercenaries, are leveraging emerging technologies to attack with both greater volume and more precision than ever before, often by exploiting the trust that underpins our digital lives. International collaboration among defenders will be critical to define new coordinated defenses and set new international norms that enforce consequences for cyberattacks targeting the global critical infrastructure or essential services.

For security leaders, the imperative is clear: cybersecurity must be a priority, embedded into the fabric of organizational strategy and addressed regularly as part of risk management. Global partnerships across industry peers and even competitors must be established to coordinate and collaborate on defenses against common adversaries. Traditional perimeter defenses are no longer sufficient. Resilience must be designed into systems, supply chains, processes, and governance. New types of threats will emerge with increasing frequency; being informed and prepared is critical.

What's new in this year's report

AI as both a defensive necessity and a target

We're witnessing adversaries deploy generative AI for a variety of activities, including scaling social engineering, automating lateral movement, engaging in vulnerability discovery, and even real-time evasion of security controls. Autonomous malware and AI-powered agents are now capable of adapting their tactics on the fly, challenging defenders to move beyond static detection and embrace behavior-based, anticipatory defense.

At the same time, AI systems themselves have become high-value targets, with adversaries amping up use of methods like prompt injection and data poisoning to attack both models and systems, which could lead to unauthorized actions, data leaks, theft, or reputational damage.

Diverse vectors for initial access

In today's world, campaigns rely on multi-stage attack chains that mix tactics and techniques such as social engineering and technical exploits. This year, we saw the widespread adoption of "ClickFix," a social engineering technique that tricks users into executing malicious code themselves, bypassing traditional phishing protections. We also saw the incorporation of new access methods like device code phishing by both cybercriminal and nation-state actors.

The pervasive threat of infostealers

Increasingly, adversaries aren't breaking in, they're logging in. In today's specialized cybercrime economy, access is essential, and infostealers are a way for operators to collect credentials and tokens for sale on the dark web. Follow-on activities by the buyers of compromised credentials can include ransomware, data exfiltration, and/or extortion. Overall, this means that organizations that experience an infostealer infection are at high risk of future breaches.

Nation-state actors expanding operations

Geopolitical objectives continue to drive a surge in state-sponsored cyber activity, with a notable expansion in targeting the communications, research, and academia sectors. These expansions are mostly within expected scope and volume, and primarily focused on using cyber espionage against typical targets to complement traditional intelligence operations. Building on a trend we first noted last year, nation states continue to accelerate AI use to evolve their cyber and influence operations, making them more scalable, advanced, and targeted.

We urge you to read this report with a bias toward action. It is not just a reflection of the challenges both past and future; it is a call to mobilize, prepare, and confront. Innovation, resilience, and partnership are the pillars of a secure digital future. By embracing these principles, we can navigate uncertainty and build a world where technology empowers and protects us against the rising tide of threats.

Amy Hogan-Burney
Corporate Vice President,
Customer Security & Trust

Igor Tsyganskiy
Corporate Vice President and
Chief Information Security Officer

↗ Visit **microsoft.com/mddr**
for the full report

Our unique vantage point

Our global presence—spanning billions of users, millions of organizations, and a vast network of partners—provides us with an unparalleled perspective on the cybersecurity threat landscape.

Every day, we process more than 100 trillion security signals from across the world, from the broad spectrum of our customers, partners, and platforms. These signals originate from endpoints, cloud services, identity systems, and the intelligent cloud and edge, offering deep visibility into emerging threats, attack techniques, and adversary behaviors.

AI now plays a transformative role in our defense strategy, enabling us to synthesize vast data sets, detect novel threats, and respond in moments, not hours—empowering defenders to anticipate and disrupt attackers, to protect individuals, organizations, or critical infrastructure.

Yet, we recognize that no single organization can see or solve every challenge alone. By sharing our insights, lessons learned, and best practices in the full report, we aim to strengthen collective cyber resilience and empower defenders everywhere.

Microsoft remains dedicated to transparency, collaboration, and innovation—helping build a safer digital future for all.

Our breadth and depth of signals

100 trillion
security signals processed daily

4.5 million
net new malware file blocks every day

38 million
identity risk detections analyzed in an average day

15,000+
Partners in our security ecosystem, making it one of the largest in the world

34,000
full-time equivalent security engineers employed worldwide

5 billion
emails screened daily on average to protect users from malware and phishing

10+ AI projects and counting
250M+ threat intelligence
16 months
2,471 Command &
Control serve
156 signatures
38 months
1,213 endorsements
1.5M+ stolen credentials discovered by DCU investigations and
3.5M worker shortage

How threat actors are shaping the cyber risk environment

2025 marks a turning point in the cyber threat world. Attacks are increasingly defined by speed, scale, and sophistication.

Looking back over the past year, we've continued to see actors accelerate their development of new and novel techniques to challenge the defenses organizations are implementing to detect and prevent them. However, the daily threats organizations face largely remain the same: attacks by opportunistic threat actors targeting known security gaps. While users globally are at risk, we've observed most attacks in the last six months focused on the United States, the United Kingdom, Israel, and Germany.

For an interactive map with additional details visit **microsoft.com/mddr**

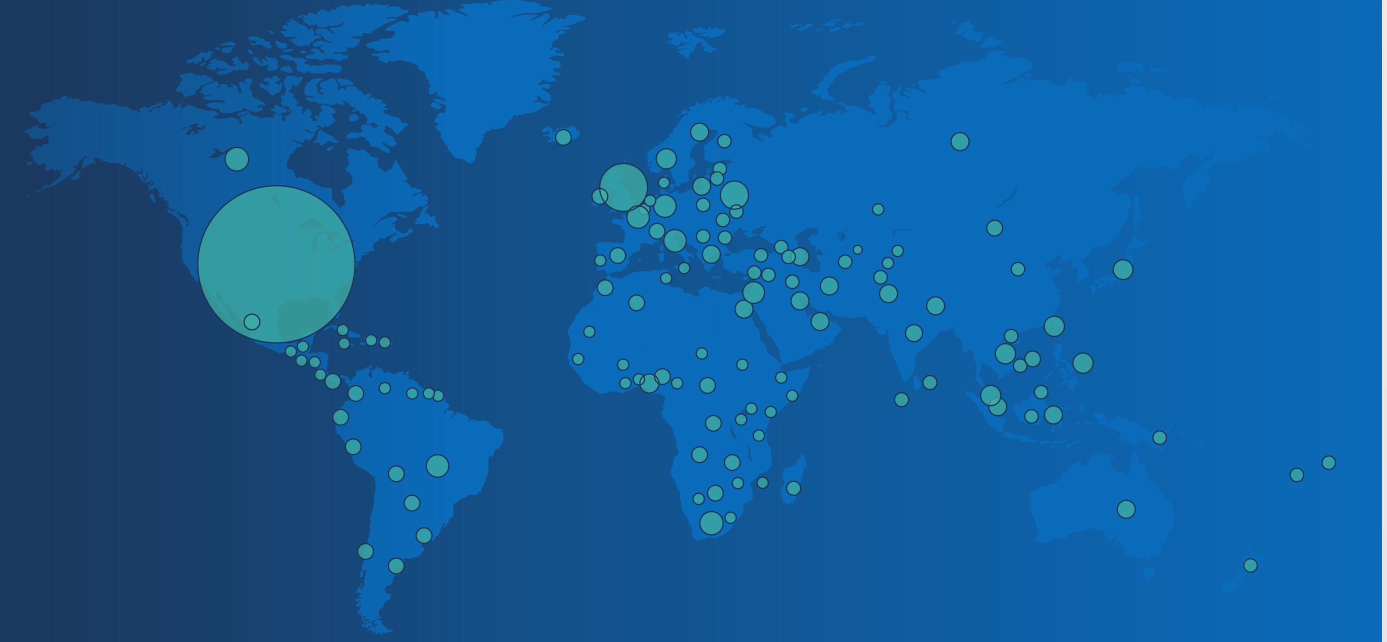
Countries where customers are most frequently impacted by cyber threats (January-June 2025)

Scale of impact

Most impacted

Least impacted

		% of total
1	United States	24.8%
2	United Kingdom	5.6%
3	Israel	3.5%
4	Germany	3.3%
5	Ukraine	2.8%
6	Canada	2.6%
7	Japan	2.6%
8	India	2.3%
9	United Arab Emirates	2.0%
10	Australia / Taiwan	1.8%



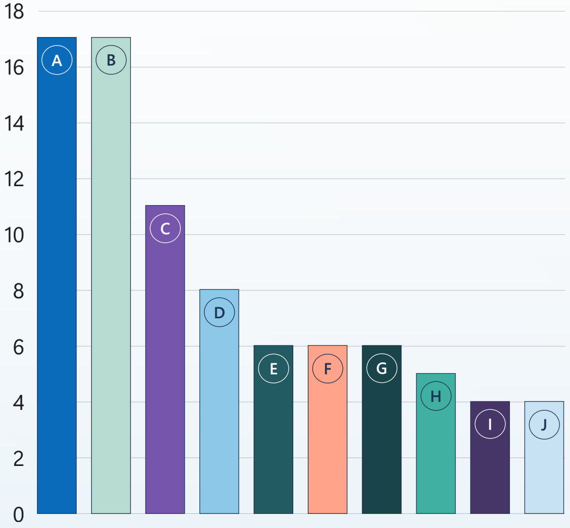
Source: Microsoft Threat Intelligence

Adversaries are targeting entities for data

Government organizations, IT companies, and research and academia were the sectors most impacted by cyber threats this year, as they were last year. These organizations manage critical public services and store vast amounts of sensitive data, including personally identifiable information (PII) and authentication tokens, which can enable future attacks.

Additionally, many government, non-governmental organizations (NGO), and research and academia institutions operate on legacy systems that are difficult to patch and secure, and have small IT teams with limited incident response capabilities. This makes them high-value targets for both nation-state actors and financially motivated cybercriminals. Given adversaries' desire for data, it is no surprise that in the past year, Microsoft Incident Response, the Detection and Response Team (DART) observed attackers performed data collection in 79.5% of reactive engagements.

Ten global sectors most impacted by threat actors (January-June 2025)



	%
A. Government agencies & services	17
B. Information technology	17
C. Research and academia	11
D. Non-governmental organizations	8
E. Critical manufacturing	6
F. Transportation systems	6
G. Consumer retail	6
H. Communications infrastructure	5
I. Financial services	4
J. Healthcare & public health	4

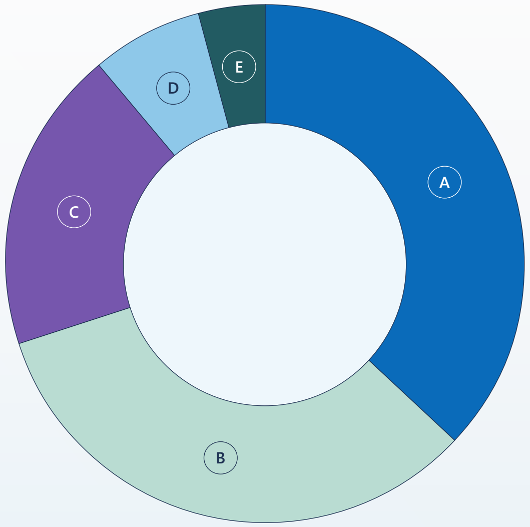
Source: Microsoft Threat Intelligence

Most attacks are for money

The vast majority of attacks are conducted by cybercriminals, not nation-state threat actors. 33% of the incidents DART investigated this year involved extortion, compared to only 4% motivated by espionage.

Ransomware or destructive activity was noted in 19% of incidents. Notably, 7% of organizations were impacted by infrastructure building. This means threat actors might be taking advantage of organizations' unmanaged digital assets to stage attacks against other third-party targets downstream.

Identified motivations in incident response engagements



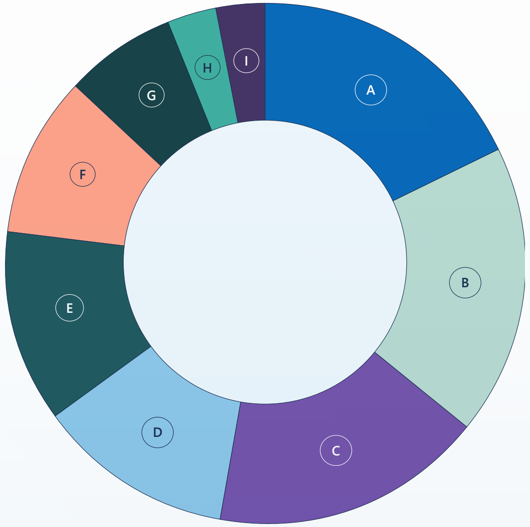
	%
A. Data theft	37
B. Extortion	33
C. Destruction/human-operated ransomware	19
D. Infrastructure building	7
E. Espionage	4

Source: Microsoft Incident Response, Detection and Response Team

Adversaries are using diverse—but well-known—initial access routes

While attack techniques, tactics, and procedures (TTPs) continue to evolve at a rapid pace, over the past year, attackers nevertheless continued to target well-known pain points, regardless of target industry or attacker motivation. DART found that 28% of breaches were initiated through phishing or social engineering, 18% were via unpatched web assets, and 12% leveraged exposed remote services.

Observed initial access vectors in DART engagements



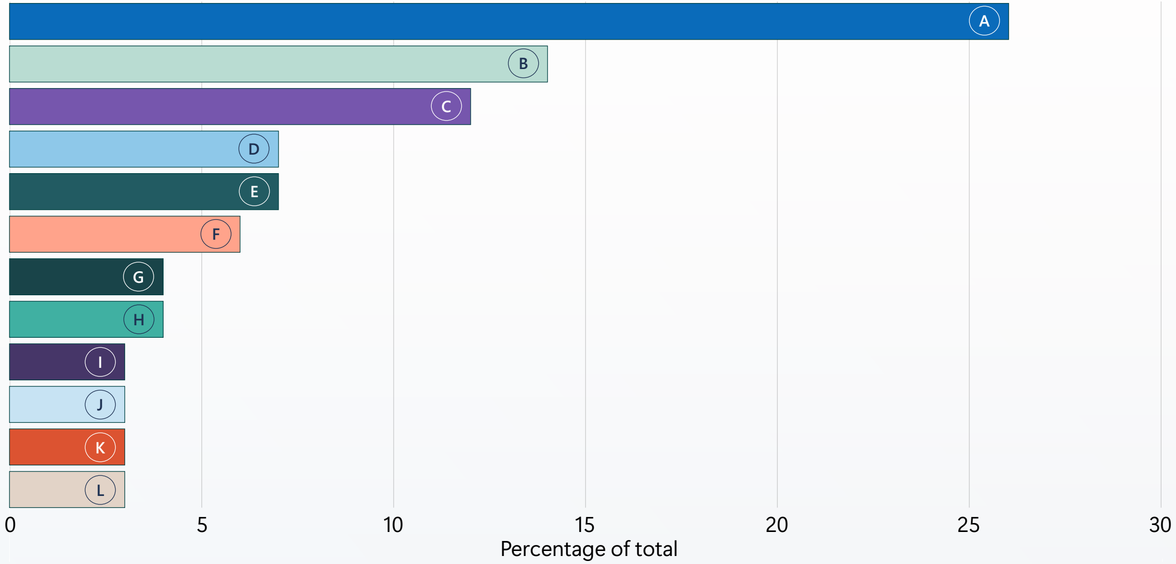
	%
A. Exploit public facing application	18
B. Social engineering	18
C. Valid accounts	17
D. Other	12
E. External remote services	12
F. Phishing	10
G. Drive-by compromise	7
H. Content injection	3
I. Supply chain compromise	3

Source: Microsoft Incident Response, Detection and Response Team

Nation-state actors are expanding their operations, but are still espionage focused

Nation-states have expanded their targeting both by volume and geographic reach, with most activity focused on using cyber espionage to complement traditional intelligence operations.

Most-targeted sectors by nation-state actors



	% of total
A. IT	26
B. Research and academia	14
C. Government	12
D. Think tanks/NGOs	7
E. Consumer retail	7
F. Manufacturing	6

	% of total
G. Transportation	4
H. Communications	4
I. Finance	3
J. Health	3
K. Defense	3
L. Energy	3

Source: Microsoft Threat Intelligence nation-state notification data

Emerging threats: What's next from attackers

While attackers' motives don't change over time, the methods they use do, as they continually pursue new approaches to access, evasion, and persistence. Given the rapid advancement of AI, the decentralization of malicious actor infrastructure, and the rise of commercialized cyber capabilities, Microsoft believes the following emerging threats will play an increasing role in the next year.

1 AI-enhanced social engineering and attacks

The integration of generative AI into adversarial operations has significantly elevated the persuasiveness and scale of social engineering campaigns. As organizations improve their hardening against traditional cybersecurity threats, threat actors will increasingly turn to AI-enabled social engineering to achieve initial access. For example, these threat actors will leverage AI to improve the speed and effectiveness of their attacks by deploying autonomous malware capable of lateral movement, vulnerability discovery, and privilege escalation without human intervention.

Or they could use AI-powered agents capable of adapting in real time to defensive environments, rerouting command and control channels or rewriting payloads dynamically to evade EDR systems. This level of autonomy could enable them to conduct scalable, multi-vector intrusions across sectors with little operational overhead.

2 More supply chain compromise

For years, threat actors have increasingly exploited the interconnectedness of modern software ecosystems and operational structures to conduct malicious activity. Microsoft continues to observe threat actors targeting the trusted relationships with upstream managed service providers (MSPs), remote access services like virtual private network (VPN) or virtual private server (VPS) systems, remote monitoring and management (RMM) solutions, cloud backups, continuous integration/continuous delivery (CI/CD) pipelines, and third-party deployment vendors to gain access through trusted or commonly deployed IT systems. These intrusions generally compromise privileged vendor accounts, exploit unpatched software, or insert malicious code into legitimate components.

The persistent danger posed by supply chain threats highlights the need for organizations to audit access privileges, validate software bills of materials (SBOM), maintain dependency hygiene, and perform runtime integrity checks.

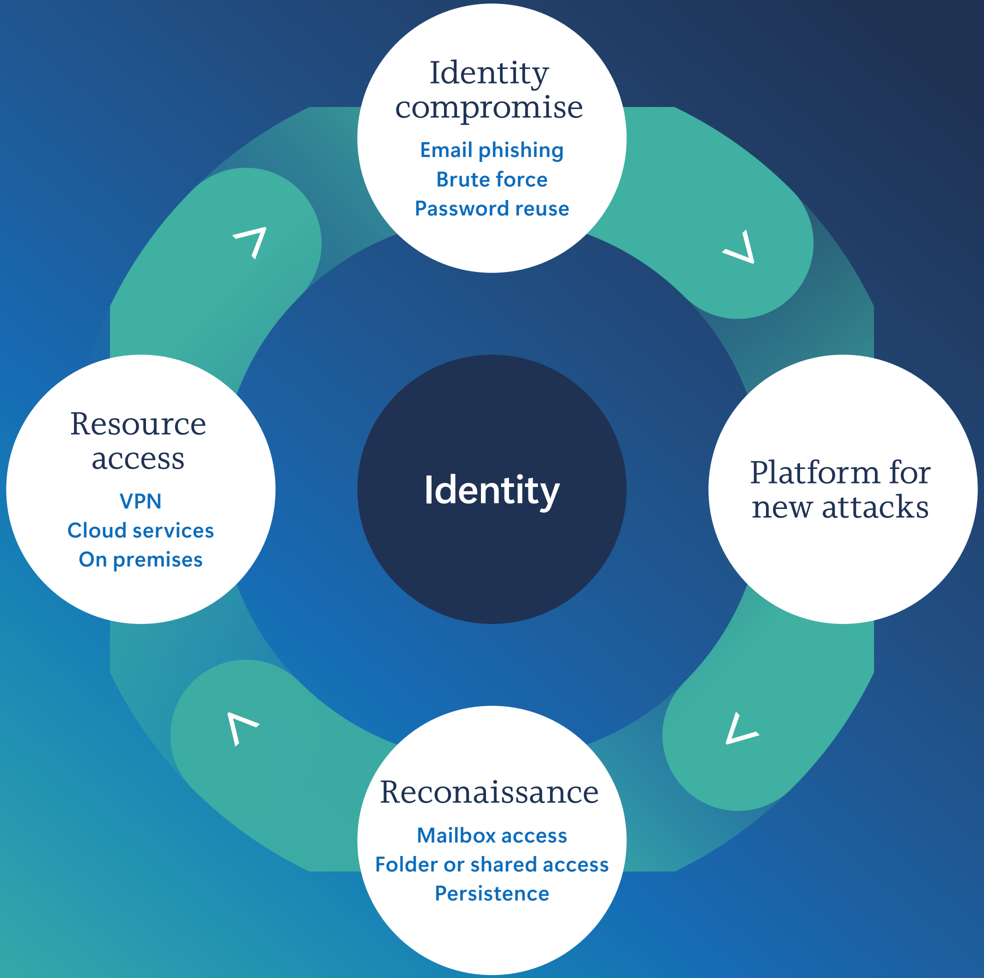
3 Expansion of covert, decentralized networks

As threat intelligence and attribution capabilities improve, sophisticated threat actors are evolving their infrastructure strategies. Rather than relying on centralized command-and-control (C2) servers or conventional bulletproof hosting (which refers to hosting services that knowingly allow malicious activity to persist online), threat actors might shift toward peer-to-peer (P2P) covert networks built atop blockchain technologies or dark web overlays. These networks could be used to coordinate espionage, facilitate decentralized malware distribution, or obfuscate ownership and control of malicious assets. In particular, ransomware-as-a-service (RaaS) actors and nation-state actors are likely to create semi-autonomous affiliate networks that can survive takedowns and adapt quickly by redistributing workloads across participants, much like resilient botnets.

4 Increasing cloud identity abuse

Cloud identity systems are a primary target for attackers seeking persistent, covert access. Attackers are targeting these systems by deploying malicious OAuth apps, abusing legacy authentication, and evolving device code phishing and adversary-in-the-middle (AiTM) attacks. These methods bypass MFA and enable long-term access and data exfiltration without triggering alerts. To confront this threat, defenders must enforce app governance, conditional access policies, and continuous token monitoring.

Lifecycle stages for a cloud abuse attack



5 The growth of high-stakes commercial intrusion markets

Cyber mercenaries are private sector entities who offer their hacking skills and tools for hire and/or sale. As the commercial offensive cyber market continues to grow, so does the demand for high-precision, low-detection exploits. In the future, these markets could shift from surveillance to disruption. For example, a cyber mercenary might offer to sell a zero-click implant capable of disabling satellite uplinks or manipulating public financial data feeds to governments or corporate competitors. The commodification of such advanced capabilities introduces scenarios such as the outsourcing of sabotage or political interference campaigns, which would create layers of deniability and complicate attribution for defenders.

The future threat environment is poised to become more adaptive, covert, and focused on using humans to achieve initial access. This shift will challenge existing security paradigms and demand more anticipatory, behavior-based defense models across the public and private sectors.

AI: Both a solution and vulnerability

As adversaries begin to leverage the capabilities of AI, so too must defenders. While AI is still new, its impact is already significant: thanks to AI-based protections, providers report automatically neutralizing the vast majority of identity attacks. With the assistance of AI, security teams can remediate threats before they cause damage, with minimal false alarms or missed detections, making defenses both faster and smarter.

AI's defensive applications are broad: it can be used to conduct threat analytics, identify detection gaps and vulnerabilities, validate detections, identify homoglyph phishing, automate remediation and patching, and shield vulnerable users. AI agents, specifically, can help in threat mitigation and incident response by automatically responding to threats—for example by suspending suspicious accounts and initiating a password reset, containing a breach before an attacker can conduct further malicious activities. Agents can also enforce policies, monitor credentials and app permissions and behaviors, and control employee accesses.

AI use, however, comes with vulnerabilities and risks. These include both threats to AI systems and their users and threats enabled by AI.

Threats from AI cyberattack augmentation

Malicious use of AI has always been inevitable, but for the first time, we're witnessing adversaries deploy generative AI to enhance a broad spectrum of activities, including scaling social engineering, data analysis, and even real-time evasion of security controls. Autonomous malware and AI-powered agents are now capable of adapting their tactics in real life, challenging defenders to move beyond static detection and embrace behavior-based, anticipatory defense.

In the past six months, AI in influence operations has picked up aggressively. In addition, we've seen the emergence of AI-first actors—including nation-state entities—that prioritize AI-generated content and tools over traditional methods and manipulations.

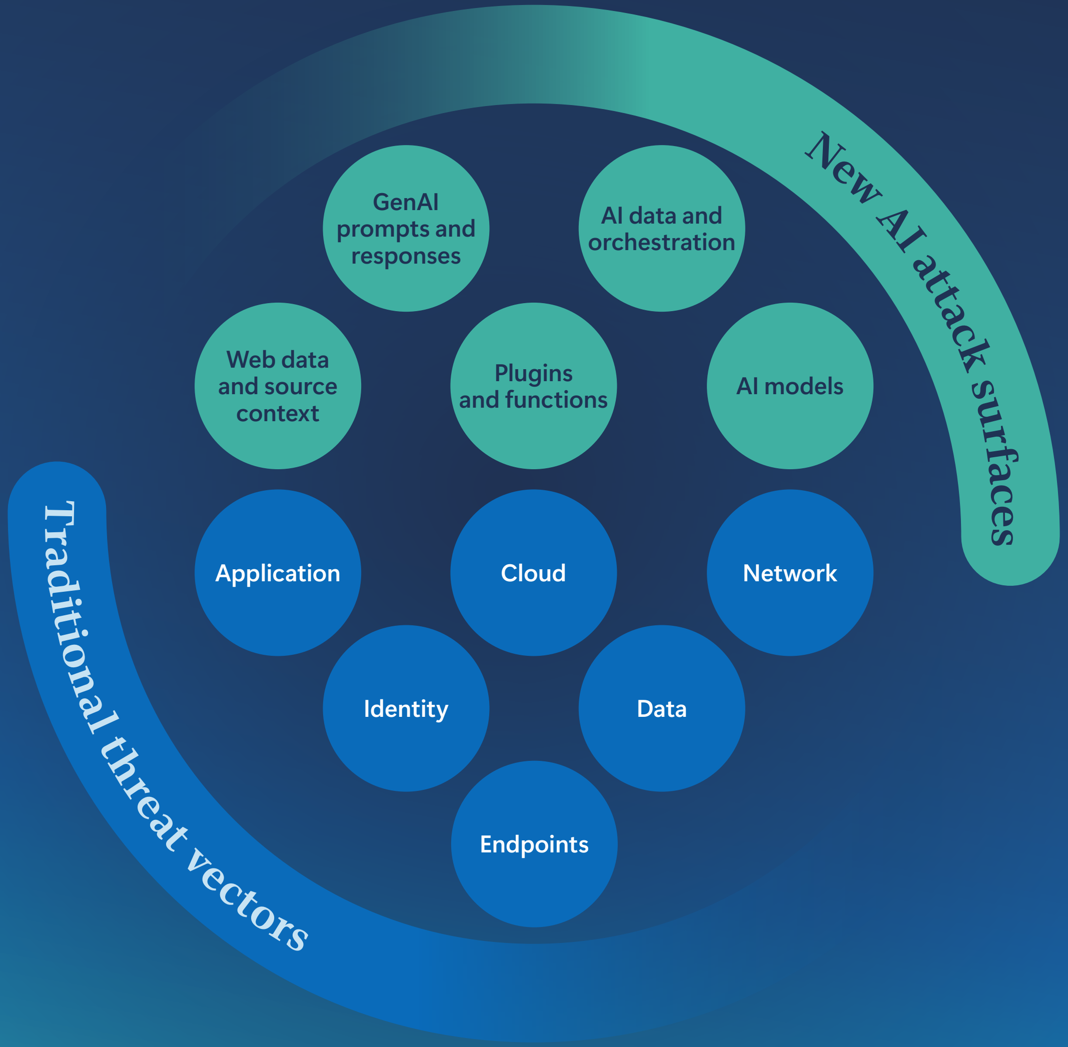
*

In this AI-first era, defending AI with AI is not just a security necessity —it's a strategic advantage.

Threats to AI and their users

AI risks span across usage, application, and platform levels and include issues such as sensitive data exposure, prompt injection, malicious tool invocation, and system compromise. AI use creates new attack surfaces for an organization. For example, as AI adoption accelerates, so does AI's access to sensitive data.

Whether through user-supplied inputs, credentialed access to existing content, or the creation of custom fine-tuned models built on proprietary data, the volume and sensitivity of data involved continues to grow—which means risks associated with compromise, leak, or unauthorized access to that data are also growing.


New AI attack surfaces
GenAI prompts and responses
AI data and orchestration
Web data and source context
Plugins and functions
AI models
Application
Cloud
Network
Identity
Data
Endpoints
Traditional threat vectors

Top 10 recommendations from this year's report

1. Manage cyber risk at the boardroom level

Treat cybersecurity as a business risk on par with financial or legal challenges. It is important that corporate boards and CEOs understand the security weaknesses of their organization. Track and report metrics like multifactor authentication (MFA) coverage, patch latency, incident counts, and incident response time to develop a comprehensive understanding of both your organization's potential vulnerabilities and its preparedness in the event of a cybersecurity incident.

2. Prioritize protecting identities

Since identity is the top attack vector, enforce phishing-resistant multifactor authentication across all accounts, including administrative accounts.

3. Invest in people, not just tools

Cybersecurity is a whole-of-organization effort. Find ways to upskill your workforce and consider making security part of performance reviews. Culture and readiness—not just technology—are primary factors in both an organization's defenses and its resilience.

4. Defend your perimeter

A third of attackers use crude tactics as the easy path into an organization's exposed footprint, often looking beyond what you deploy to the vendors and supply chain you trust, including perimeter web-facing assets (18%), external remote services (12%), and supply chains (3%). Knowing the full scope of your perimeter, auditing the accesses you grant to trusted partners, and patching any exposed attack surface forces attackers to work harder to be successful.

5. Know your weaknesses and pre-plan for breach

Combine knowledge of the organization's exposure footprint with organizational risk awareness to develop a proactive plan for responding to future breach. Tie security controls to business risks in terms the board can understand. Since a breach is a matter of when, not if, develop, test, and practice your incident response (IR) plan—including specific scenarios for ransomware attacks, which remain one of the most disruptive and costly threats to operations. How fast can you isolate a system or revoke credentials?

6. Map and monitor cloud assets

Since the cloud is now a primary target for adversaries, conduct an inventory on every cloud workload, application programming interface (API), and identity within the organization, and monitor for rogue virtual machines, misconfigurations, and unauthorized access. At the same time, work proactively to enforce app governance, conditional access policies, and continuous token monitoring.

7. Build and train for resiliency

If breaches are all but inevitable, resilience and recovery become key. Backups must be tested, isolated, and restorable, and organizations should have clean rebuild procedures for identity systems and cloud environments.

8. Participate in intelligence sharing

Cyber defense is a team, not individual, sport. By sharing and receiving real-time threat data with peers, industry groups, and government, we can make it harder for cyber adversaries to achieve their goals.

9. Prepare for regulatory changes

It's more important than ever for organizations to align with emerging laws like the European Union (EU) Cyber Resilience Act or United States (US) critical infrastructure mandates, which may require reporting cyber incidents within a certain timeframe or Secure by Design practices. These regulations reinforce the importance of timely incident reporting and stronger internal oversight of an organization's cybersecurity practices.

10. Start AI and quantum risk planning now

Stay ahead of emerging technologies. Understand both the benefits and risks of AI use within an organization and adjust your risk planning, attack surface exposure, and threat models appropriately. Prepare for a post-quantum cryptography (PQC) world by taking the time to inventory where encryption is used and create a plan to upgrade to modern standards as they evolve.

↗ Visit **microsoft.com/mddr** for the full report

Microsoft

Microsoft Digital Defense Report 2025

Lighting the path to a secure future

For more news on cybersecurity, visit:
microsoft.com/corporate-responsibility/cybersecurity

For more report insights, visit:
microsoft.com/mddr

For more news on cybersecurity policy, follow us on LinkedIn:
aka.ms/MOILinkedin

For insights and trends for security leaders, visit:
www.microsoft.com/security/security-insider

A Microsoft Threat Intelligence report
October 2025
v2