



Executive Summary Microsoft Digital Defense Report 2024

The foundations and new
frontiers of cybersecurity



A Microsoft Threat Intelligence report

Complex, challenging, and increasingly dangerous

The new cyber threat landscape: an introduction by Tom Burt



“We all can, and must, do better, hardening our digital domains to protect our networks, data, and people at all levels.”

In the last year, the cyber threat landscape continued to become more dangerous and complex.

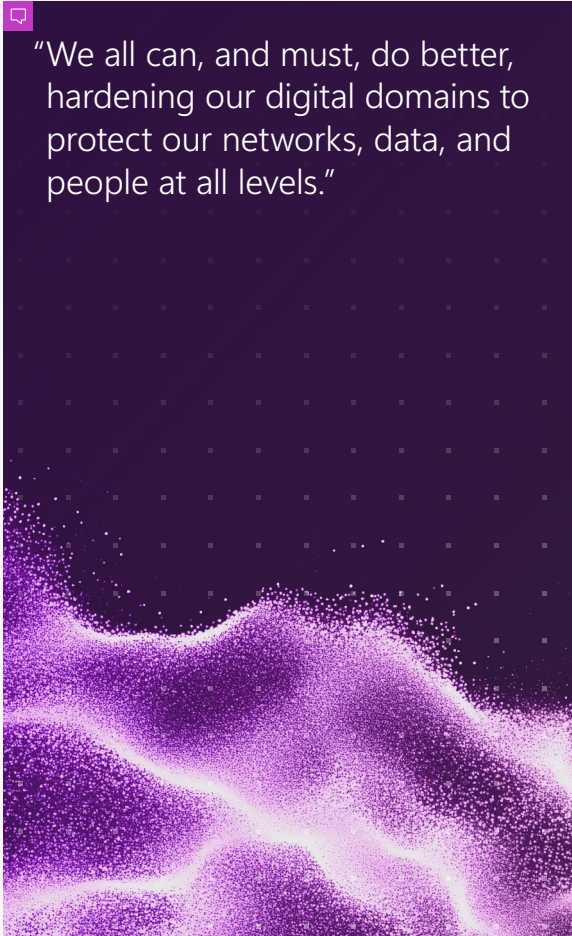
The malign actors of the world are becoming better resourced and better prepared, with increasingly sophisticated tactics, techniques, and tools that challenge even the world’s best cybersecurity defenders.

Because these actors conduct both targeted and opportunistic attacks, the threat they present is universal, meaning organizations, users, and devices are at risk anywhere, anytime. Even Microsoft has been the victim of well-orchestrated attacks by determined and well-resourced adversaries, and our customers face more than 600 million cybercriminal and nation-state attacks every day, ranging from ransomware to phishing to identity attacks.

These cyberattacks are continuing at a breathtaking scale, and as they increasingly put human health at risk, the stakes for stopping them couldn’t be higher. In the US alone this fiscal year, 389 healthcare institutions were successfully hit by ransomware, resulting in network closures, systems offline, critical medical operations delayed, and appointments rescheduled. Worse, the increased risk of cyberattacks is no longer limited to civilian cybercriminals. Nation-states are becoming more aggressive in the cyber domain, with ever-growing levels of technical sophistication that reflect increased investment in resources and training. These state-sponsored hackers are not just stealing data, but launching ransomware, prepositioning backdoors for future destruction, sabotaging operations, and conducting influence campaigns.

We have to find a way to stem the tide of this malicious cyber activity. We all can, and must, do better, hardening our digital domains to protect our networks, data, and people at all levels. This challenge will not be accomplished solely by executing a well-known checklist of cyber hygiene measures but through a focus on and commitment to the foundations of cyber defense from the individual user level to the executive level.

However, improved defense will not be enough. The sheer volume of attacks must be reduced through effective deterrence, and while the industry must do more to deny the efforts of attackers via better cybersecurity, this needs to be paired with government action to impose consequences that further discourage the most harmful cyberattacks.





While in recent years a great deal of attention has been given to the development of international norms of conduct in cyberspace, those norms so far lack meaningful consequence for their violation, and nation-state attacks have been undeterred, increasing in volume and aggression. Cybercriminals similarly continue to attack with impunity, knowing that law enforcement is hampered by the challenges of investigation and prosecution of cross-border crime, and often operating from within apparent safe havens where government authorities turn a blind eye to the malicious activity.

While the immediate outlook is pessimistic, there are changes on the near horizon that provide cause for optimism. In this year's Microsoft Digital Defense Report, we dive deeper into the subject of AI in cybersecurity. We explore the associated emerging threats and defense strategies, as well as examine the responses of governments around the world to this rapidly evolving technology. And although we must anticipate the use of AI by attackers, advances in AI-powered cybersecurity should give defenders an asymmetric advantage in the near future.

This year we will also share how Microsoft is responding to the significant attacks on our corporate infrastructure. This includes details of our Secure Future Initiative and how we are orchestrating a company-wide initiative to make security our top corporate priority. We hope that these learnings will help others think through their own security posture and approach to cyber defense.

Microsoft is proud to deliver the Microsoft Digital Defense Report, now in its fifth edition, as part of our commitment to helping the world understand and mitigate cyber threats. We believe transparency and information-sharing are essential to the protection of the global cyber ecosystem. Communicating the insights that we derive from our unique vantage point is one of the many ways we work to make the cyber world a safer place.

As our CEO, Satya Nadella, has said: "This is a consequential time." We stand on the frontier of an AI-empowered world. It is up to us, however, to leverage AI most effectively. In the tug-of-war between attackers and defenders in which the attackers currently have an advantage, it will take conscientiousness and commitment by both the public and private sectors to ensure the defenders win.

Tom Burt
Corporate Vice President,
Customer Security and Trust

Our presence in the digital ecosystem positions us to observe key trends in cybersecurity. Microsoft’s perspectives on cybersecurity are framed through 50 years of experience and insight.

Society | Microsoft Stakeholders | Microsoft Customers

Microsoft’s unique vantage point

Microsoft serves billions of customers globally, allowing us to aggregate security data from a broad and diverse spectrum of companies, organizations, and consumers.

An extra 13 trillion security signals per day

2023: 65 trillion, 2024: 78 trillion

from the cloud, endpoints, software tools, and partner ecosystem, to understand and protect against digital threats and criminal cyberactivity.

1,500 unique threat groups tracked

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.

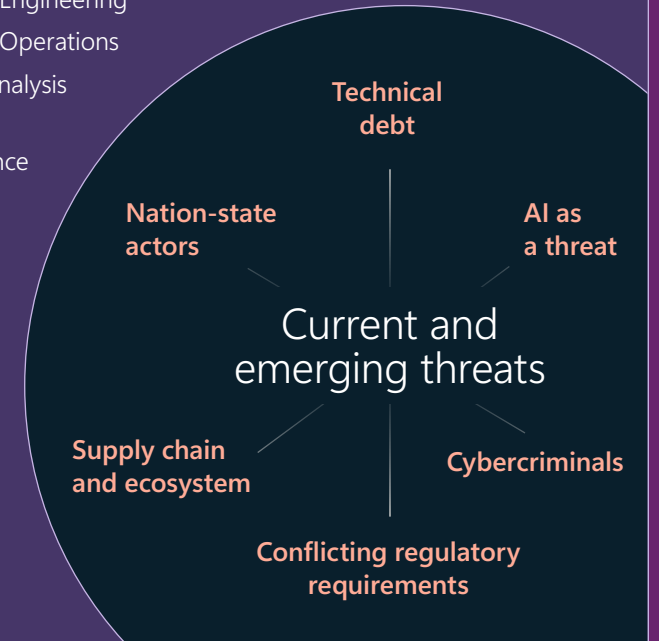
Microsoft’s cybersecurity approach

Microsoft security investments

- AI Red Teams
- Defending Democracy
- Detection and Response
- Digital Crimes
- Digital Safety
- Incident Response
- National Security
- Physical Security
- Public Awareness and Education
- Responsible AI
- Security Engineering
- Security Operations
- Threat Analysis
- Threat Intelligence

34,000 dedicated security engineers

focused full-time on the largest cybersecurity engineering project in the history of digital technology.



Chapter 1 Key developments The evolving cyber threat landscape

As with any landscape, things change over time. In the world of cybersecurity, however, the pace of change has been astounding.

Observations over the past year have reaffirmed the convergence of nation-state and cybercriminal threat activity. Nation-state threat actors used cybercrime as a force multiplier, while financially motivated cybercriminals pursued levels of defense evasion and technical complexity once elusive outside of nation-state operations.

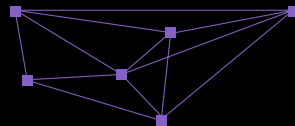
We have also seen rapid shifts in the tactics of hybrid war, wide-ranging attempts to interfere in democratic elections, and a surge in ransomware attacks and cyber-enabled financial fraud across the globe.

These trends underscore the ongoing necessity to enhance and implement robust deterrence and mitigation strategies to counter these threats effectively.

Read more about these developments
<https://microsoft.com/MDDR>

Blurred lines between nation-state threat actor activity and cybercrime

Nation-state threat actors are conducting operations for financial gain and enlisting the aid of cybercriminals and commodity malware to collect intelligence.



The many faces of hybrid war

Threat actors serving Russia and Iran are leaning into cyber and influence operations as tools to advance political and military objectives in wartime.



The need to impose deterrent consequences for cyber aggression

The pace of nation-state sponsored cyberattacks has escalated to the point that there is now effectively constant combat in cyberspace without any meaningful consequences to the attacker.

600 million identity attacks per day

As multifactor authentication blocks most password-based attacks, threat actors are shifting their focus.

Nation-state influence operations converge on elections

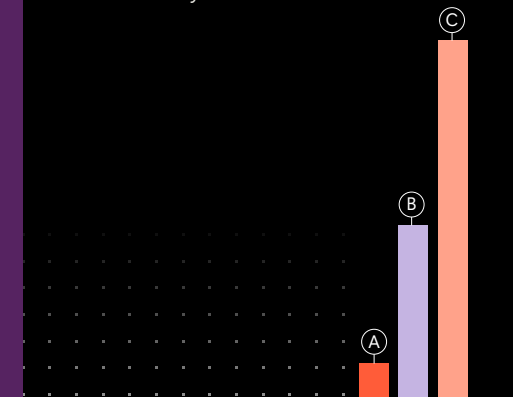
By the end of 2024, 2 billion people will have had the opportunity to vote in nationwide elections. Russia, Iran, and China all engaged in election influence efforts globally in 2024.

2.75x increase in human-operated ransomware-linked encounters

By disabling or tampering with defenses, attackers buy themselves time to install malicious tools, exfiltrate data for espionage or extortion, and potentially launch attacks like ransomware.

Ingenuity and scalability of fraud tactics surging globally

Cyber fraud not only presents a theft risk, but it undermines the security, trust, and reputation of individuals, businesses, and organizations of all sizes and types, in every region and industry.

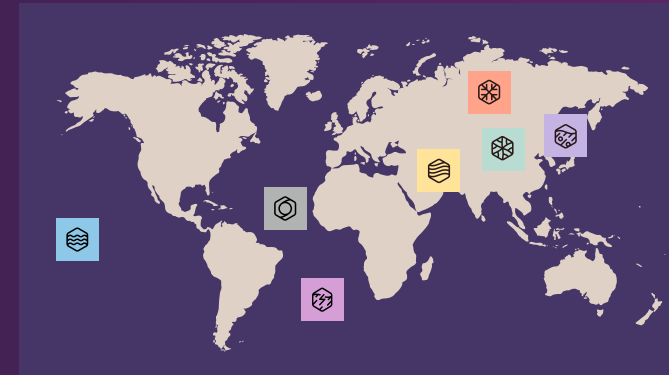


Threat actors and motivations

In the 2024 Microsoft Digital Defense Report, we discuss 30 different threat actors to provide examples of activity for a better understanding of attack targets, techniques, and motivations. Microsoft categorizes these actors using a weather-related naming system. For example, “Flood” refers to actors who engage in influence operations. The actors included in this year’s report demonstrated significant activity and effectiveness from July 2023 through June 2024. In the chart below, we map some of the motivations tracked over the past five years, to show how these actors often have multiple motivations driving their operations. It’s important to note that the threat landscape is vast, and the threat actors and motivations detailed here represent only a small portion of those tracked by Microsoft.

KEY TO MOTIVATIONS MAPPING

- Cryptocurrency theft C
- Cybercrime services CS
- Data destruction Dd
- Data theft for profit Dt
- Disruption D
- Election influence Ei
- Espionage E
- Influence operations I
- Ransomware/Extortion R



Nation-state actors

Cyber operators acting on behalf of or directed by a nation-state-aligned program, irrespective of whether for espionage, financial gain, or retribution.

Russia



- Aqua Blizzard E
- Midnight Blizzard E
- Seashell Dd D Ei
- Blizzard E I R
- Secret Blizzard E

China



- Flax Typhoon Dt E
- Granite Typhoon Dt E
- Nylon Typhoon E
- Raspberry Typhoon Dt E

North Korea



- Citrine Sleet C Dt
- Jade Sleet C Dt
- Moonstone Sleet E R
- Sapphire Sleet C Dt

Iran



- Cotton Dd Dt D
- Sandstorm Ei E I R
- Mint Sandstorm Ei E R

Influence Operations



Information campaigns or groups employing communications online or offline in a manipulative fashion to shift perceptions, behaviors, or decisions by target audiences to further a group or a nation’s interests and objectives.

- Ruza Flood Ei I
- Sefid Flood Ei E I
- Taizi Flood Ei I
- Volga Flood Ei I

Financially motivated



Cyber campaigns or groups directed by a criminal organization or person with motivations of financial gain and are not associated with high confidence to a known non-nation-state or commercial entity.

- Octo Tempest C Dt R

Groups in development



A temporary designation given to unknown, emerging, or developing threat activity. This designation allows Microsoft to track a group as a discrete set of information until we reach high confidence about the origin or identity of the actor behind the operation.

- Storm-0501 Dt R
- Storm-0539 Dt
- Storm-0593 E
- Storm-0784 D R
- Storm-0842 Dd D Ei I R
- Storm-0867 CS
- Storm-1101 CS
- Storm-1516 Ei I
- Storm-1575 D
- Storm-1679 I
- Storm-2049 E

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.



<1% of attacks



Less than 1% combined

<p>MFA attacks</p> <ul style="list-style-type: none"> SIM swapping MFA fatigue AitM 	<p>End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.</p>
<p>Post-authentication attacks</p> <ul style="list-style-type: none"> Token theft Consent phishing 	<p>Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.</p>
<p>Infrastructure compromise</p>	<p>Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.</p>

Chapter 2 Key developments Centering our organizations on security

In this chapter we emphasize the responsibility of everyone for keeping their own house in order, emphasizing robust accountability alongside a fundamental mastery of cybersecurity essentials. More than just compliance checklists, we advocate for a threat-informed strategy that enhances resilience across the cyber landscape.

We also extend our focus beyond organizational security to incorporate the broader ecosystem, particularly in critical environments and electoral processes. The chapter concludes with a call for collective action, urging stronger collaborations between industry and government to bolster our collective security.

Read more about these
<https://microsoft.com/MDDR>

↘

The Secure Future Initiative (SFI)

Taking proactive steps to keep security deficits from re-accumulating, we share what we are doing, how customers can benefit, and how they can better protect themselves.

↘

Security stories from critical infrastructure frontlines

Helping to support the ecosystem through transparency of datacenter application security findings.

↘

Taking a threat-informed approach to defense

80% of organizations have attack paths that expose critical assets.



↘

Best practices for robust cybersecurity governance and accountability

Everyone in the organization, including Board members, must have basic literacy of cybersecurity threats, a sense of personal responsibility for security, and clarity on their role.



↘

Hierarchical pyramid of cybersecurity needs

It starts with the basic need to protect identities, against ransomware, supply chain attacks, and other threats that bypass traditional security measures.



↘

Generative AI is fueling the need for data security policy implementation

The use of generative AI applications can pose serious risk to organizations that haven't implemented sufficient data governance controls. On the other hand, generative AI can be used to kick-start a strategy and approach to understanding their data perimeter.

↘

Collective action through deeper partnerships between industry and governments

Hybrid warfare, cyberattacks, and foreign influence operations pose grave risks to society.

↘

Supporting democratic elections

During this unprecedented period of critical elections worldwide, we are working to safeguard institutions from malicious schemes that aim to disrupt or influence electoral processes.

Putting security above all else

The Microsoft Secure Future Initiative (SFI) is a multiyear initiative to evolve the way we design, build, test, and operate our products and services, to achieve the highest possible standards for security.

It's our long-term commitment to protect both the company and our customers in the ever-evolving threat landscape.

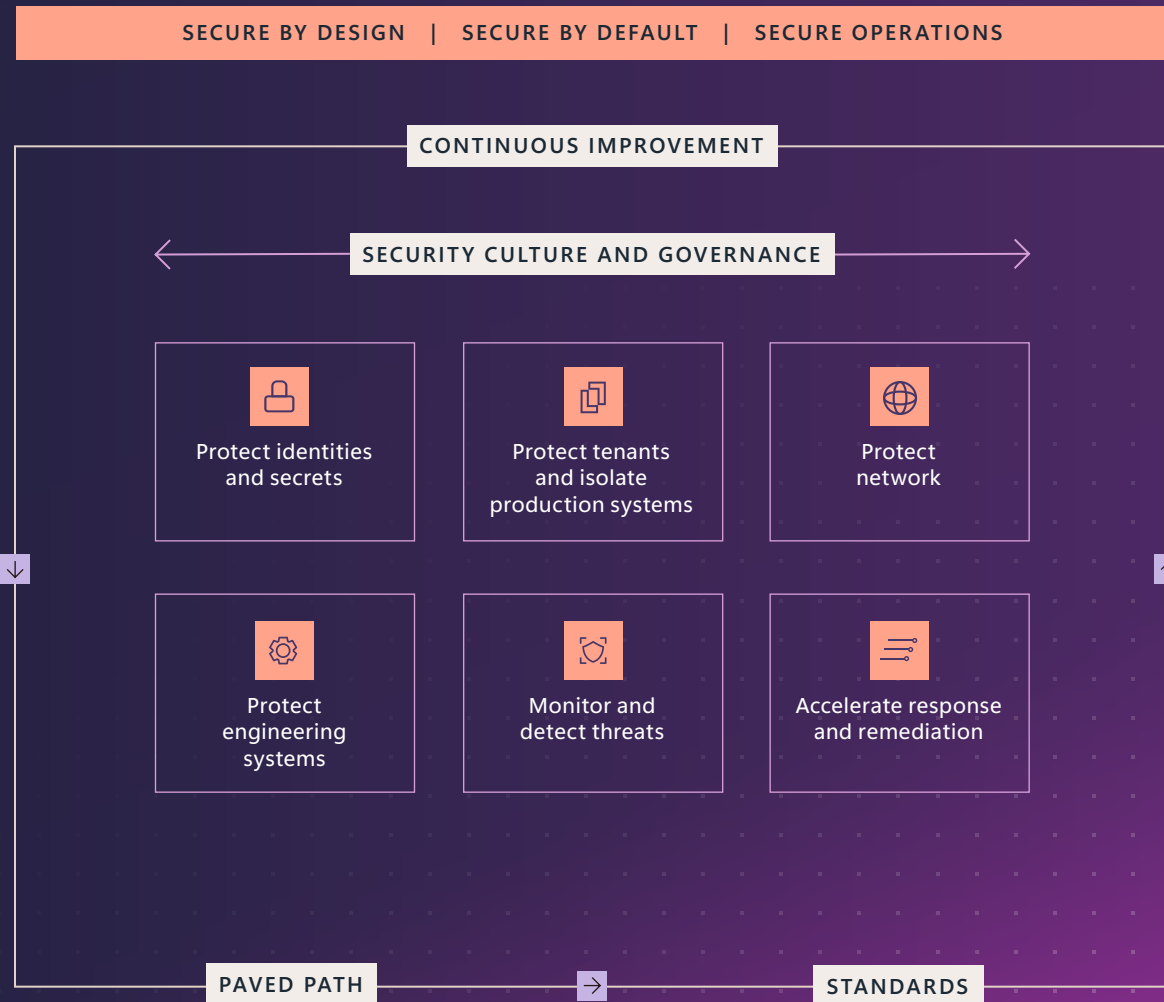
730k

SFI non-compliant apps eliminated

5.75 million

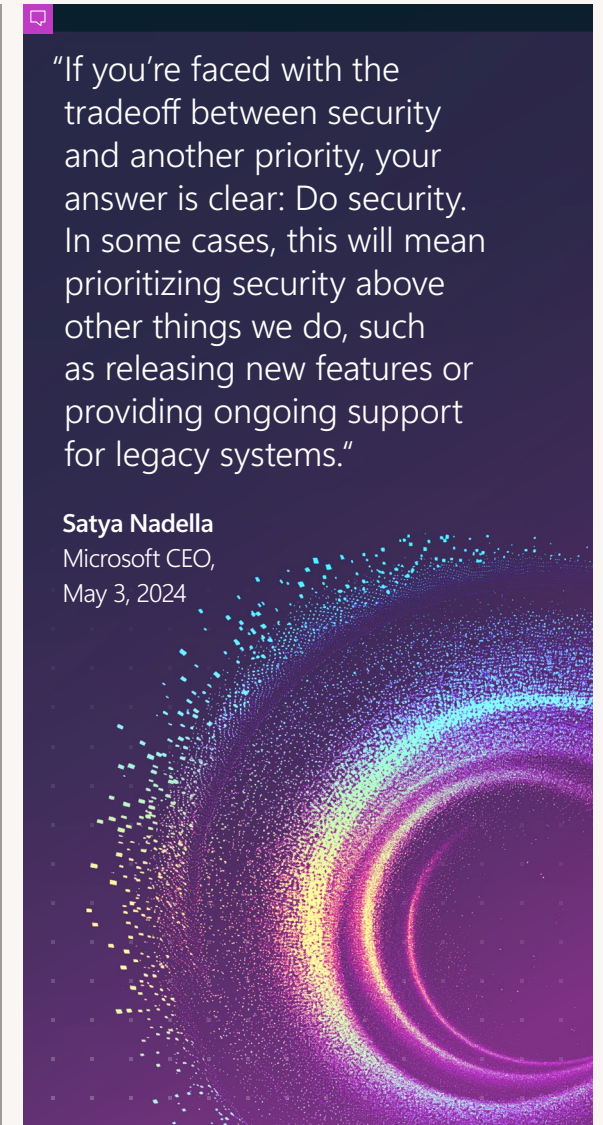
inactive tenants eliminated, drastically reducing the potential cyberattack surface.

Links
[Secure Future Initiative](#) | [Microsoft](#)



"If you're faced with the tradeoff between security and another priority, your answer is clear: Do security. In some cases, this will mean prioritizing security above other things we do, such as releasing new features or providing ongoing support for legacy systems."

Satya Nadella
 Microsoft CEO,
 May 3, 2024



Threat-informed defense

Thinking differently to address threats

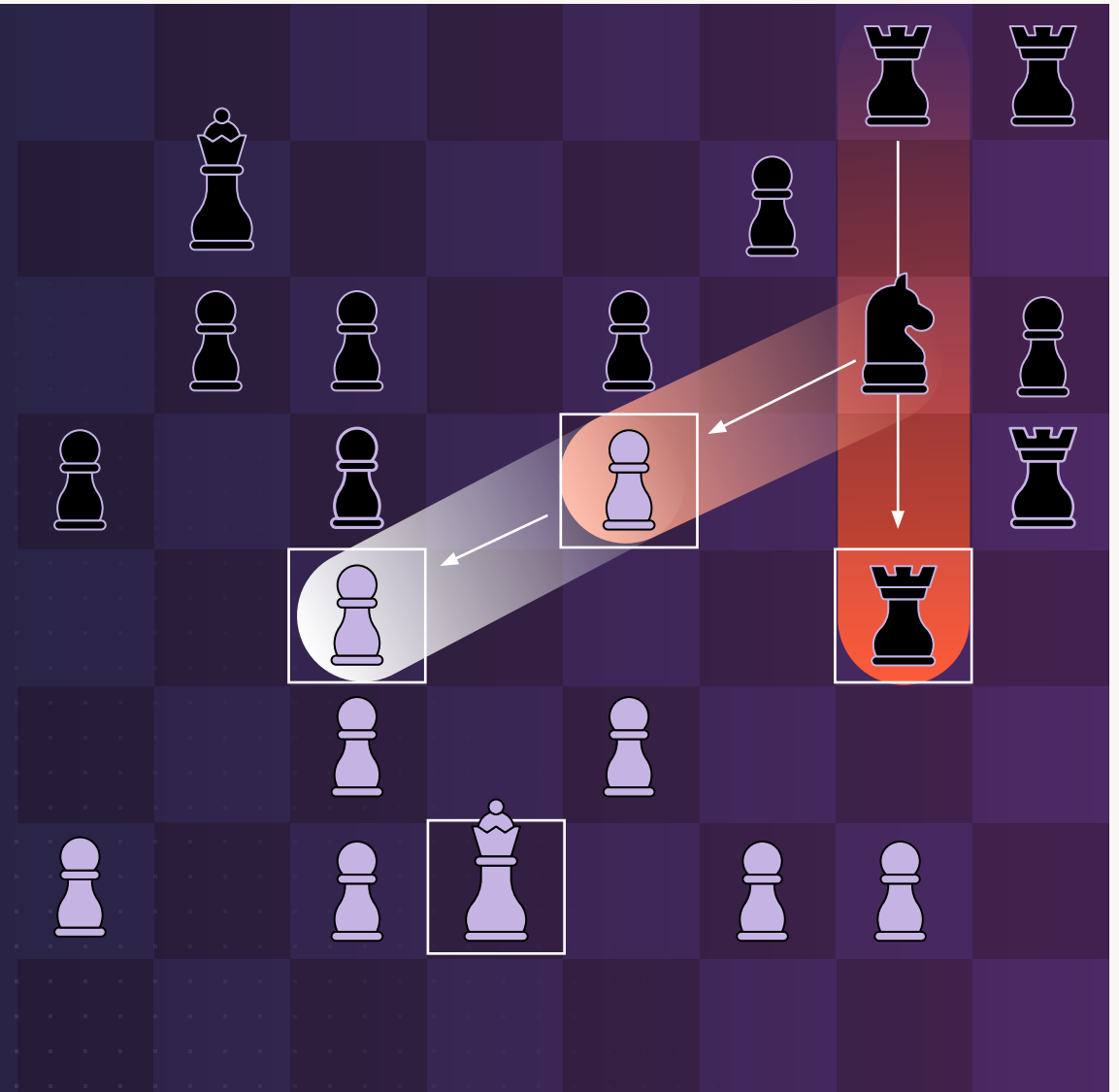
Most organizations rate bugs according to severity and how difficult they are to mitigate before assigning a team to fix them within a set compliance window. However, what happens is clashing prioritizations and silos with no knowledge of an adversary's attack path. Hence the saying: "Defenders think in lists and attackers think in graphs".

Organizations have complex operating environments that require defenders to see across various vendors in order to discover attack paths. Instead, they should look to understand their critical assets and crucially how they are, or could be, connected. The resulting view of an organization's posture is key to understanding the risk exposure to cyber threats. By adopting an attacker's perspective, the prioritization of mitigation efforts is enhanced.

The Silo Effect

Defenders must adapt to attacker's mindset.

- ↓ Defenders think in lists
- ↗ Attackers think in graphs
- ⚠ As long as this is true, attackers win



Threat-informed defense continued

Pre-breach attack path analysis

Traditionally, organizations have leaned on all sorts of different security tools to manage threat exposure across their estate. This messy patchwork of approaches however, can lead to exposure visibility gaps and efficiency challenges.

This makes it imperative for security leaders to reach a unified and comprehensive view of their estate and to both continuously and smartly prioritize exposure reduction efforts. Prioritization should seek to understand threats and attacker perspective, identify “crown jewels” of interest to the attacker, and both identify and mitigate any paths that lead to them.

Three key components are required for threat-informed defense: single pane of glass, critical asset protection, and attack path management.

Single pane of glass

Organizations should consolidate threat exposure insights across their estate into a single view covering cloud assets, on-prem devices, data, identities, applications, network, and the Internet of Things (IOT). This should then be used to manage top threats such as ransomware and business email compromise, as well as exposure to threat campaigns and actors.

80%
of organizations have attack paths that expose critical assets

Critical asset management

It is imperative to thoroughly map an estate’s “crown jewels.” This can include critical servers, highly privileged identities, sensitive data, or other assets. Microsoft data indicates that an average <1% of organizational assets are of high interest to attackers.

Attack path management

Organizations should identify the most likely attack paths leading to critical assets and continuously mitigate them. An attack path calculation incorporates things such as asset inventories, vulnerability/weakness data, and external attack surfaces to construct a possible attack chain leading to a critical asset.



Links

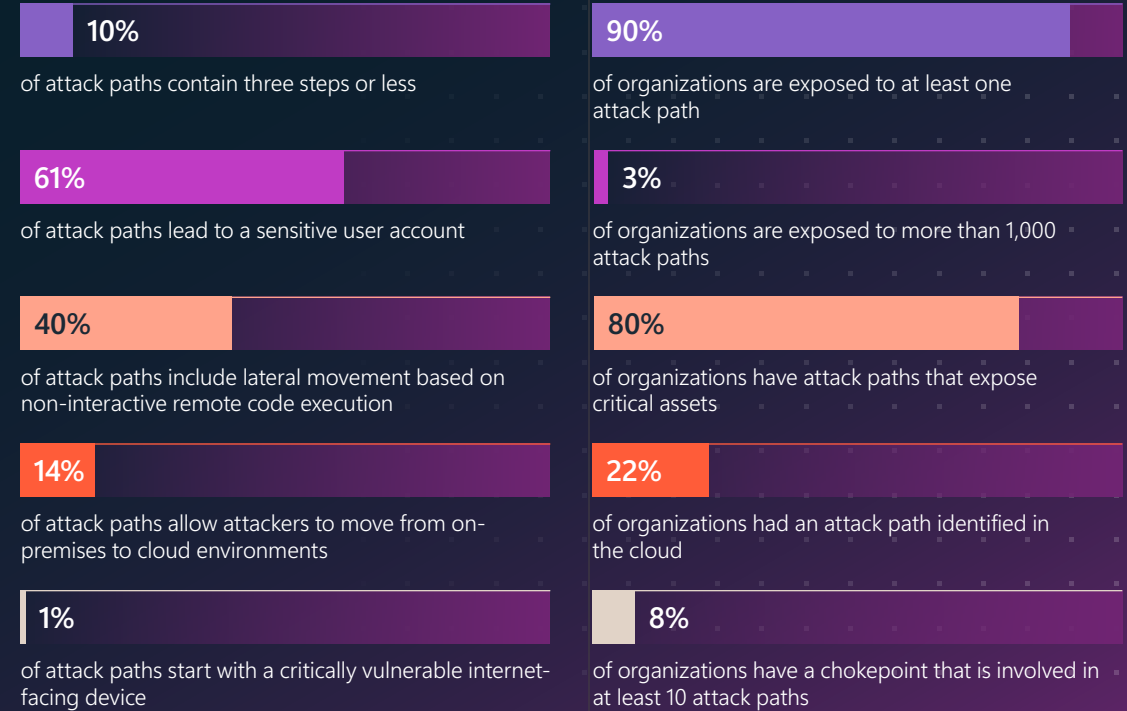
[Introducing Security Exposure Management - Microsoft Community Hub | Mar 2024](#)

[Identifying and Protecting the Crown Jewels of your Cloud | Aug 2024](#)

[Exposure insights and secure score in Microsoft Security Exposure Management | Aug 2024](#)

[One graph of everything - Microsoft Security Exposure Management Graph | May 2024](#)

Attack path insights for threat-informed defense (June 2024)



<1%
of organizational assets are of high interest to attackers

Source: Microsoft Security Exposure Management

Chapter 3 Key developments

Early insights: AI's impact on cybersecurity

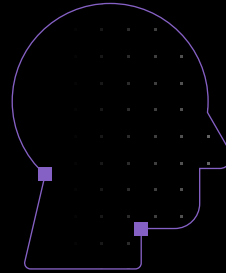
AI is reshaping the landscape of cybersecurity, arming defenders with powerful tools to preempt and counteract evolving threats with unprecedented precision. As we explore this transformative era, we are met with both promising advancements and daunting challenges—from sophisticated AI-powered targeting to complex influence operations orchestrated by nation-state threat actors.

As ever, information is power. The more knowledge and understanding an organization has of the emerging threats, the better it can prepare. In this chapter we explore how AI is changing everything from enhancing detection capabilities and operations efficiencies, to customized mitigations. At the same time, governments and industry are collaborating, and using a variety of approaches, to advance global cybersecurity initiatives in the AI era.

Read more about these <https://microsoft.com/MDDR>

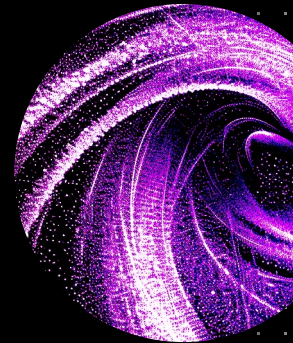
AI-enabled human targeting

These threats will be more difficult to detect and defend against—even with AI tools assisting defensive strategies.



Emerging threat actor techniques

AI-enabled spear phishing, résumé swarming, and deepfakes emerge.



Governments and industries working to advance global AI security

While there is a consensus on the importance of security in the development of AI, governments have pursued different approaches in implementing security requirements.

Nation-state threat actors are using AI for influence operations

AI-generated images and audio manipulations are being used to shape audience perception and engagement in conspiratorial narratives.

AI for defense

Defenders are using AI to become more efficient, especially in security operations.

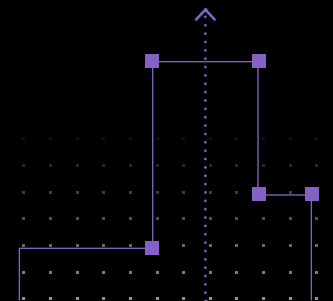


Limiting foreign influence operations in the modern era

Existing limitations of foreign influence operations under international law are no longer sufficient in the modern era.

Staying a step ahead of threat actors in the age of AI

Policy principles can mitigate risks associated with use of AI tools.




AI for defense

Microsoft’s significant investment in AI innovation is aimed at providing cybersecurity defenders with an asymmetric advantage over attackers in the realm of defense.

In our efforts, we prioritize cutting-edge research and the development of groundbreaking solutions like Copilot for Security. These solutions amplify defenders’ efforts by optimizing resources and scaling cybersecurity endeavors. This is particularly crucial considering the significant shortage of skilled cybersecurity workers, which poses one of the biggest challenges in the field of cybersecurity.

Currently, cybersecurity teams operate at their limits, facing staffing constraints, escalating regulatory compliance demands, and an ever-growing number of increasingly sophisticated adversaries. However, the introduction of AI will change this workload, offering various benefits to both attackers and defenders.

For defenders, the “automated ingenuity” of generative AI can now be applied across the entire defense chain, from initial detection of anomalies to prompt triage and response. Beyond merely enhancing existing security operations centers (SOC), AI holds the potential to introduce entirely new methods of defense. For instance, it enables persistent systems that constantly monitor for vulnerabilities and promptly address any breaches. Additionally, AI streamlines the sharing of information among defenders, transforming it from a labor-intensive manual process into a continuous, automated one.



“AI holds the potential to be as much of a transformative technological revolution for human beings as things like electricity or modern computing, if not possibly more so; a tool that opens up benefits across the board, transforming zero-sum problems into non-zero-sum opportunities and creating massive net long-term gains for humanity.

But, as we’ve seen repeatedly throughout the course of history, when in the wrong hands, any sufficiently new and powerful tool that people are given can be used by those people to cause harm. The good news is that these same AI tools, when paired with creativity, innovation and diligence, can put those of us on the side of defense and security ahead of disruptive threat actors, and allow everyone a chance to fully realize the tremendous benefits that AI can bring.”

Kevin Scott, Chief Technology Officer



Microsoft Digital Defense Report

The foundations and new frontiers of cybersecurity



Learn more: <https://microsoft.com/mddr>



Dive deeper: <https://blogs.microsoft.com/on-the-issues/>



Follow us for MDDR insights and more:
<https://www.linkedin.com/showcase/microsoft-security/>



For more news on cybersecurity policy follow us on:
<https://www.linkedin.com/showcase/microsoft-on-the-issues/>