Microsoft

Microsoft Digital Defense Report

Executive Summary

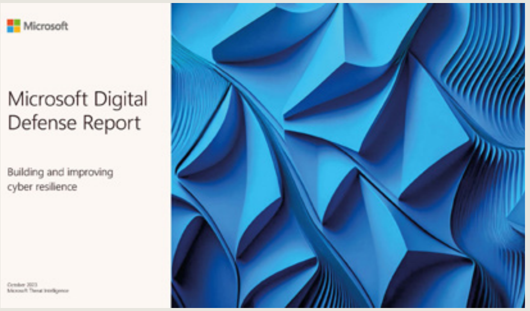
Building and improving cyber resilience

October 2023
Microsoft Threat Intelligence

Contents of the full report

The data, insights, and events in this report are from July 2022 through June 2023 (Microsoft fiscal year 2023), unless otherwise noted.

For easier viewing and navigating through the report on certain browsers, we suggest using Adobe Reader, which is available for free on the Adobe website.



Microsoft

Microsoft Digital Defense Report

Building and improving cyber resilience

October 2023
Microsoft Threat Intelligence

Find the full report here:
Microsoft Digital Defense Report 2023

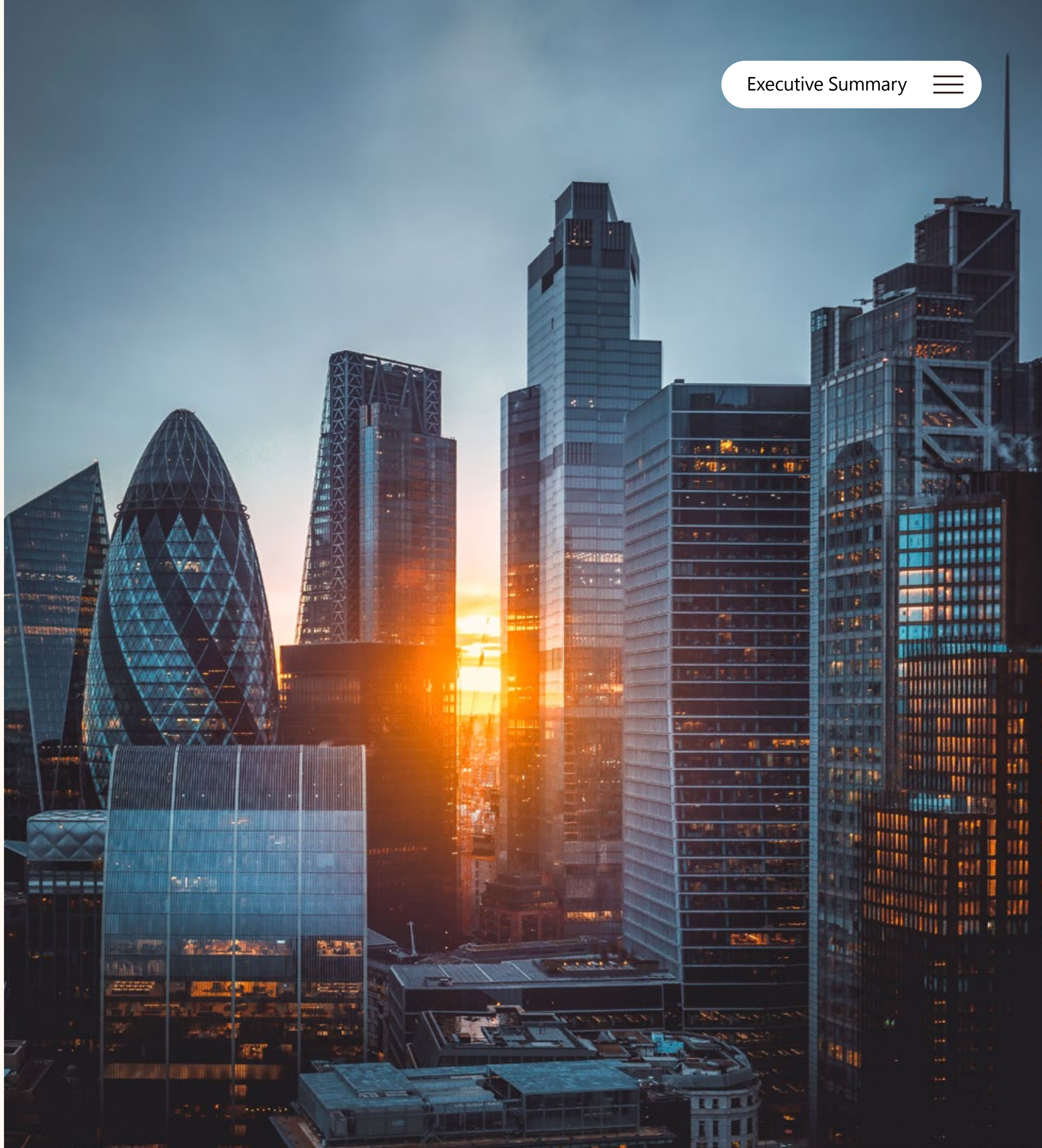
Securing our future together

Introduction from Tom Burt

Over the last year, threats to digital peace have reduced trust in technology and highlighted the urgent need for improved cyber defenses at all levels. Encouragingly, defenders the world over are responding to the call to improve security with the public and private sectors investing and collaborating to confront the challenges and build long-term resilience.

In this fourth annual edition of the Microsoft Digital Defense Report, we draw on our unique vantage point to share insights on how the threat landscape has evolved and discuss the shared opportunities and challenges we all face in securing a resilient online ecosystem which the world can depend on.

> "Close collaboration between the public and private sectors to formulate, enforce, and harmonize these requirements is crucial to improve global cybersecurity and foster innovation."



"As the digital domain faces new and more threatening challenges, defenders are being driven to innovate and collaborate more closely than ever."

As the digital domain faces new and more threatening challenges, defenders are being driven to innovate and collaborate more closely than ever. For example, Russia's use of cyberweapons as part of its hybrid war against Ukraine sparked sustained collaboration between Microsoft and Ukrainian officials to successfully defend against most of these cyberweapons.

Russia is not alone in its use of destructive malware; we have also seen increased use of cyberweapons by Iran to pressure the Albanian government and in its ongoing conflict with Israel. At the same time, nation states are becoming increasingly sophisticated and aggressive in their cyber espionage efforts, led by highly capable Chinese actors focused on the Asia Pacific region in particular.

One recent example of the troubling increase in aggression and capability involves a Chinese actor, which Microsoft calls Volt Typhoon. It used inventive tradecraft to infiltrate and pre-position malware in the networks of a range of communications companies and other critical infrastructure organizations in Guam and the United States, deploying "living off the land" techniques to evade detection.

Nation-state actors were not alone in stepping up their abuse of the digital ecosystem. Well-resourced cybercriminal syndicates also continue to grow and evolve, leveraging the cybercrime-as-a-service ecosystem we highlighted last year. Ransomware-as-a-service and phishing-as-a-service are key threats to businesses and cybercriminals have conducted business email compromise and other cybercrimes, largely undeterred by the increasing commitment of global law enforcement resources.

Many vendors are taking steps to improve the cybersecurity of their products and services, developing new tools to help customers better defend against attackers. Governments across the globe are providing the public with more information about cyber threats and how to counter them, like the effective alerts from the US Cybersecurity and Infrastructure Security Agency's (CISA) Shields Up campaign. Governments are also imposing new legal and regulatory requirements for cybersecurity. While many of these are beneficial, they can impose counterproductive conditions—such as requiring overly rapid reporting of cybersecurity incidents or establishing inconsistent or conflicting requirements across agencies or geographies. Close collaboration between the public and private sectors to formulate, enforce, and harmonize these requirements is crucial to improve global cybersecurity and foster innovation.

As we are seeing, Artificial Intelligence (AI) technologies are set to become a major focus of regulators and industry. We will undoubtedly see attackers using AI as a tool to refine phishing messages, develop malware and enable other abuses of technology. But AI will also be a critical component of successful defense. For example, in Ukraine we saw the first successful use of AI technology to help defend against Russian cyberattacks. In the coming years, innovation in AI-powered cyber defense will help reverse the tide of cyberattacks.

Advancing the promise of digital peace requires public-private collaboration to ensure we are bringing to bear the best technological and regulatory tools to combat cyber aggression. We need more and deeper alliances in the private sector and stronger partnerships between the private and public sectors. Enabling this collaboration can be challenging but, when successful, it drives meaningful impact. We must accelerate the move of critical computing workloads to the cloud, where vendors' security innovations will be most impactful, and ensure AI innovation provides defenders with the durable technological advantage over attackers that it promises.

Tom Burt
Corporate Vice President, Customer Security & Trust

Sharing Microsoft's unique vantage point

Cybersecurity is a defining challenge of our time. Organizations of every size across every industry around the globe feel the urgency and pressure of protecting and defending against increasingly sophisticated attacks.

While AI is transforming cybersecurity, using it to stay ahead of threats requires massive amounts of diverse data. Here at Microsoft, our more than 10,000 security experts analyze over 65 trillion signals each day with the help of AI, and Microsoft Threat Intelligence teams track hundreds of threat actor groups worldwide. The Microsoft security ecosystem includes more than 15,000 security partners with specialized solutions, while the global open community of security researchers and testers contribute to bug bounties and security challenges. This broad, deep, and diverse security ecosystem is driving some of the most influential insights in cybersecurity. Together, we can build cyber resilience through innovative action and collective defense.

As part of our longstanding commitment to create a safer world, Microsoft's investments in security research, innovation, and the global security community include:

65 trillion
signals synthesized daily

That is over 750 million signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

4,000
identity attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+
partners in our security ecosystem

15,000+ partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

135 million
managed devices

135 million managed devices providing security and threat landscape insights.

All data is based on Microsoft fiscal year 2023 unless otherwise indicated.

The power of partnership in building cyber resilience

We believe every individual and company around the world should be empowered to meet its security needs. Achieving this will require a collective global effort as we harness the power of partnership to strengthen our defenses together.

Strength in numbers. Stronger together. Together we stand. Societies around the world recognize the benefits of collective behavior. The power of multistakeholder partnerships in cybersecurity, too, cannot be ignored as we seek to answer the question, “What can we do to ensure a more safe and secure world for everyone on the planet?”

Individual organizations are often focused on safeguarding their own data and systems and protecting their customers, constituents, and communities.

But partnerships act as a force multiplier for everyone involved in cybersecurity. Collaborative efforts among stakeholders—including government agencies, private sector entities, academia, non-profits, and other organizations—are crucial in building resilient defenses against cyber threats.

The cyber poverty line

To understand the need for collaboration, it is useful to consider the concept of a “cyber poverty line.” In the same way that governments and economists establish a social poverty line to determine a bare minimum standard of living, the cyber poverty line is the minimum level of resources required for adequate protection from cyber threats. As we ponder the implication of the existence of a cyber poverty line, important questions begin to surface. How, exactly, do we quantify the cyber poverty line? Who is below it and how can we work together to support them to rise above it? These questions underscore the imperative of partnership in cybersecurity and serve as the genesis of meaningful conversations we must have.

Public-private partnerships, policy, and standards

The opportunities for partnership across the public and private sectors, policy organizations, and standards bodies are multi-dimensional. From ensuring the technology community is building safer, more secure technology and collaborating on threat intelligence and trends to developing common standards to take down and block the tools cybercriminals use, strong and bi-directional partnerships between organizations are crucial.

As much as any individual company’s shareholders would like it to be so, no one technology company can solve or overcome every cybersecurity challenge. Partnerships across the technology community are an absolute necessity to ensure organizations of all types and sizes, in every industry and region, can protect themselves. This means working together to push the boundaries of innovation, ensuring technical integration of products in the security space and addressing the end-to-end security needs of customers.

> The concept of a cyber poverty line allows us to identify the minimum level of resources required for adequate protection from cyber threats and who we must support to rise above it.

Non-profit, academia, and research

Non-profit, academia, and research organizations play a crucial role in advancing cybersecurity. By collaborating with industry partners, they bridge the gap between theoretical knowledge and practical application. Academic institutions contribute to cybersecurity research, develop innovative technologies, and educate the next generation of cybersecurity professionals. Collaborative research projects and initiatives between academia, non-profits, and industry promote innovation and help tackle emerging cyber threats effectively.

It is essential that stakeholders recognize their shared responsibility and actively engage in partnerships that enhance cybersecurity. History has already shown that by working together, we can build a safer digital future for individuals, organizations and nations—but there is so much more to be done.

How can we protect against 99% of attacks?

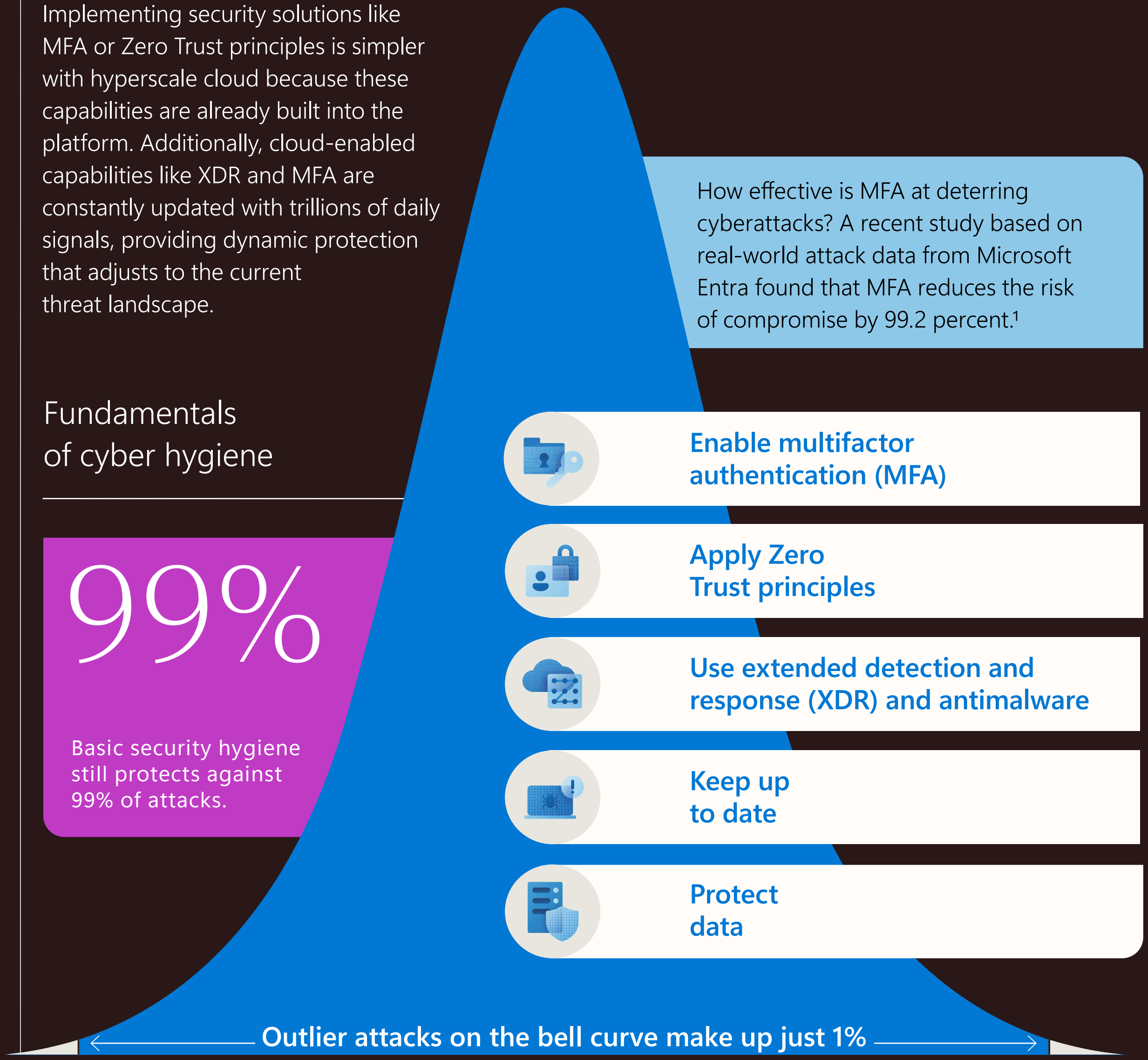
While we explore the many dimensions of the cyber threat landscape, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
   - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
   - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.
   - Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.



Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]

Key developments

The State of Cybercrime

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands on keyboard attacks, using living-off-the-land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

80-90%

of all successful ransomware compromises originate through unmanaged devices.

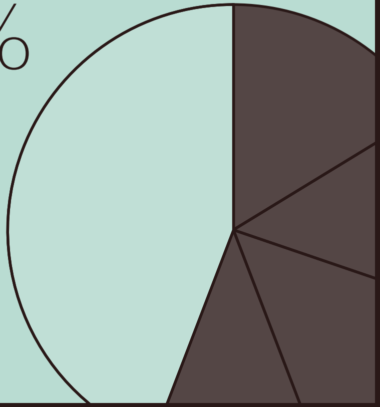
A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

70%

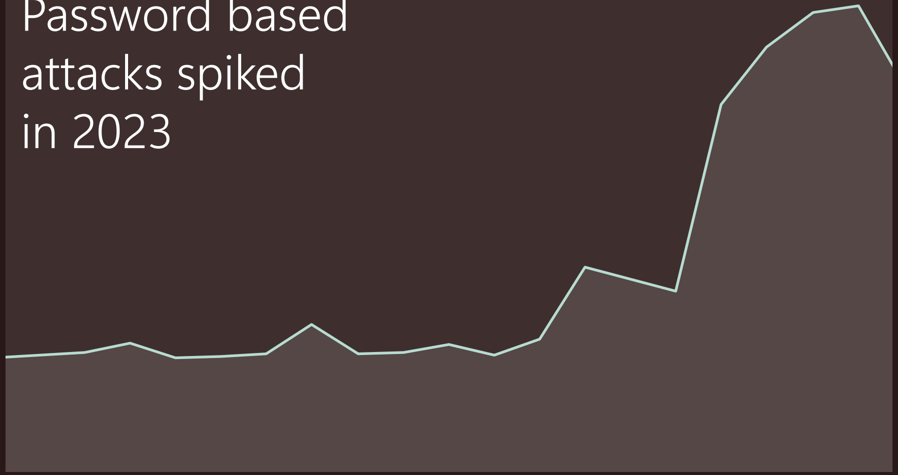
of organizations encountering human-operated ransomware had fewer than 500 employees.

Human-operated ransomware attacks are up more than

200%



Password based attacks spiked in 2023



Last year marked a significant shift in cybercriminal tactics

with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.

Key developments

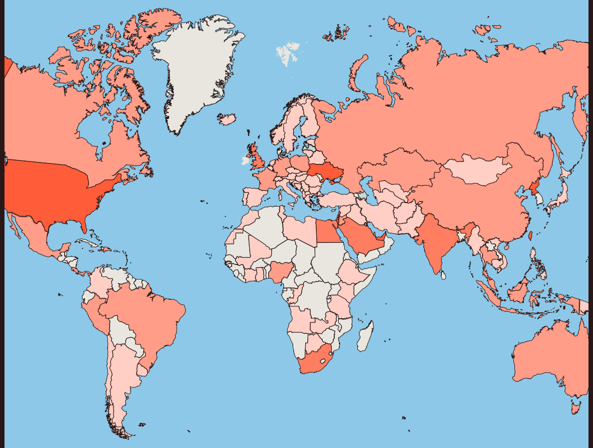
Nation State Threats

After last year's flurry of high-profile cyberattacks, nation-state cyber actors this year pivoted away from high-volume destructive attacks and instead directed the bulk of their activity toward cyber espionage.

As nation-state threat actors continue to grow in sophistication, they have been increasingly used by governments to understand the plans of other nations, transnational bodies, and non-governmental organizations. Critical infrastructure also remains a popular target, with threat actors employing stealthier techniques to establish persistence and evade detection, as is the education sector. At the same time, some governments have used cyber-enabled influence campaigns to manipulate public opinion at home and abroad. Cyber operations are expanding globally, with increased activity in Latin America, sub-Saharan Africa, and the Middle East due to heightened Iranian activity.

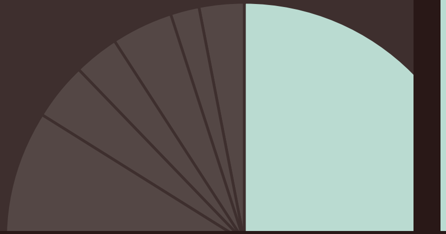
Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

Nation-state and state-affiliated threat actor activities pivoted away from high volume destructive attacks in favor of espionage campaigns.



The unchecked expansion of the cyber mercenary marketplace threatens to destabilize the broader online environment.

Russian state-sponsored threat actors used diverse means to access devices and networks in NATO member states.



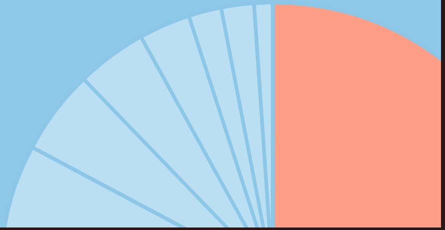
Iranian state actors are using increasingly sophisticated tradecraft

including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.

Chinese cyber threat groups carried out sophisticated worldwide intelligence collection campaigns.

At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.

North Korean actors conducted a supply chain attack using an existing supply chain compromise.



Key developments

Critical Cybersecurity Challenges

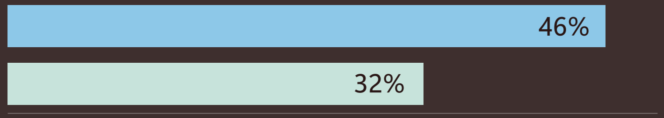
Growing attacks on the highly vulnerable intersection of information technology and operational technology (IT-OT) emphasize the importance of a comprehensive defense strategy that covers the entire business ecosystem.

While nation-state actors were previously the main perpetrators of critical infrastructure attacks, the ease of entry for malicious actors has led to a surge in threats to OT. This calls for a more comprehensive security approach. Unmanaged devices in critical infrastructure pose a significant vulnerability, making it crucial to address the problem of unsupported operating systems in OT devices.

Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

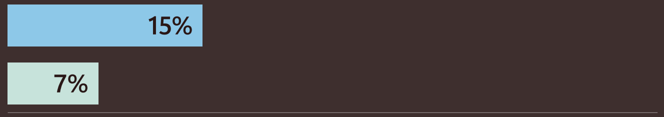
46%

Of the 78% of IoT devices with known vulnerabilities on customer networks, 46% cannot be patched.



25%

of OT devices on customer networks use unsupported systems.



15

We discovered 15 new zero-day vulnerabilities in the CODESYS runtime,

highlighting the significant risks associated with not addressing supply chain vulnerabilities to ensure the security of critical infrastructure and systems.

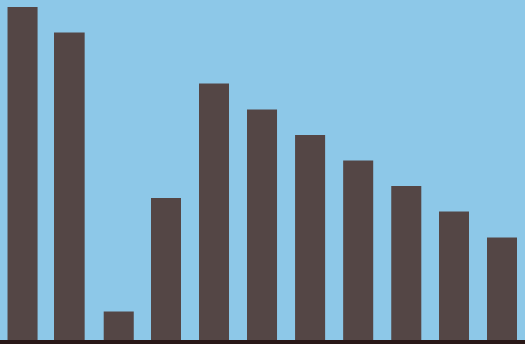
Attacks targeting open source software have grown on average

742%

since 2019.

57%

of devices on legacy firmware are exploitable to a high number of CVEs (>10).



Key developments

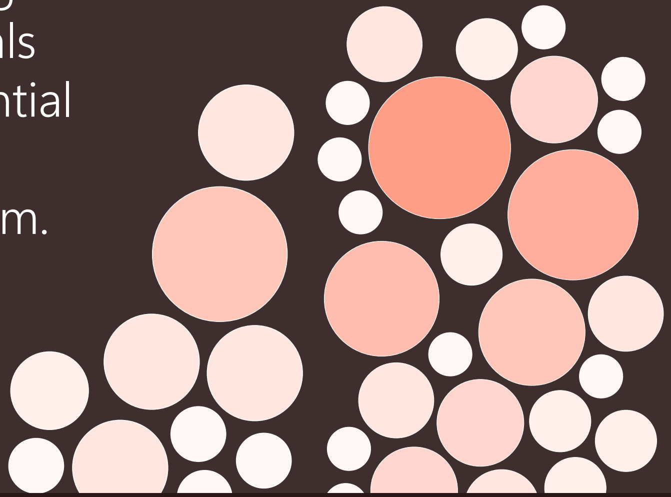
Innovating for Security and Resilience

Against an ever more complex cyber ecosystem, AI offers the potential to change the security landscape by augmenting the skill, speed, and knowledge of defenders.

Since Microsoft has the largest and most diverse set of products in the industry, we are continuously seeking out and eliminating vulnerabilities before threat actors can exploit them. One way that we are confronting cybercrime is by leveraging AI and large language models (LLMs). LLMs can automate and augment many aspects of cybersecurity, including: threat intelligence; incident response and recovery; monitoring and detection; testing and validation; education; and security governance, risk, and compliance.

Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

With modern AI advancements analyzing trillions of security signals daily, we have the potential to build a safer, more resilient online ecosystem.



Our approach for the next year will focus on bringing to bear AI in combating threats while also embracing the three SDL principles of Secure by Design, Secure by Default, and Secure in Deployment (SD3).

LLMs have the potential to transform cyber defense for next-gen cybersecurity.

Microsoft's researchers and applied scientists are exploring many scenarios for LLM application in cyber defense.

Many modern apps will become LLM-based in time.

This will increase the threat surface, making them vulnerable to both inadvertent and deliberate misalignments. As LLM-based apps bring new and unique threats, we adapt our security measures and protocols to address them.

Key developments

Collective Defense

By forging strong partnerships that transcend borders, industries, and the public-private divide, we are creating a united front against cybercrime.

As cyberthreats evolve, productive relationships across a spectrum of stakeholders will be essential to improve threat intelligence, drive resilience, and contribute to mitigation guidance.

Find out more about The State of Cybercrime in the Microsoft Digital Defense Report 2023

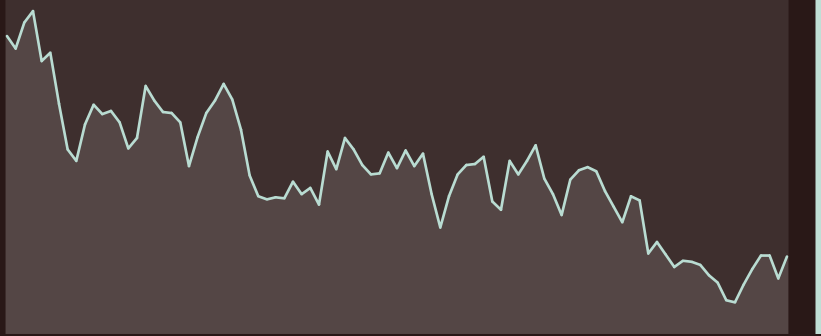
The fragmented cybersecurity landscape means we are not making the most of the vast amount of threat intelligence and data that is available.

The new Cybercrime Atlas will maximize global data collection while ensuring intelligence is thoroughly cleansed, enriched, and vetted by experts from diverse industries.

Fewer than 15% of NGOs have cybersecurity experts on their staff.

The CyberPeace Institute is providing critical support and assistance to humanitarian organizations.

A ground-breaking lawsuit aimed at ending the illicit use of Cobalt Strike shows the power of uniting efforts to identify and take down criminal infrastructure.



75% of eligible citizens in democratic nations have the opportunity to vote in the next year and a half. We must ensure that strong cyber defenses keep elections safe.

Microsoft

Microsoft Digital Defense Report

Building and improving cyber resilience

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

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

𝕏 **Stay connected:** @msftissues and @msftsecurity

October 2023
Microsoft Threat Intelligence