A new world of security: Microsoft's Secure Future Initiative

Nov 2, 2023 | Brad Smith - Vice Chair & President

The past year has brought to the world an almost unparalleled and diverse array of technological change. Advances in artificial intelligence are accelerating innovation and reshaping the way societies interact and operate. At the same time, cybercriminals and nation-state attackers have unleashed opposing initiatives and innovations that threaten security and stability in communities and countries around the world.

In recent months, we've concluded within Microsoft that the increasing speed, scale, and sophistication of cyberattacks call for a new response. Therefore, we're launching today across the company a new initiative to pursue our next generation of cybersecurity protection – what we're calling our Secure Future Initiative (SFI).

This new initiative will bring together every part of Microsoft to advance cybersecurity protection. It will have three pillars, focused on AI-based cyber defenses, advances in fundamental

Related Stories

Oct 19, 2023 | Amy Hogan-Burney

Microsoft, Amazon, and international law enforcement join forces to fight tech support fraud

Oct 5, 2023 | Tom Burt

Espionage fuels global cyberattacks

Oct 27, 2023 | Natasha Crampton

Progress with our AI commitments: an update ahead of the UK AI Safety Summit

Related Blogs

Oct 16, 2023 | Kevin Miller

software engineering, and advocacy for stronger application of international norms to protect civilians from cyber threats. Charlie Bell, our Executive Vice President for Microsoft Security, has already shared the Secure Future Initiative details with our engineering teams and what this action plan means for our software development practices.

I share below our perspective on the changes that have led us to take these new steps, as well as more information on each part of our Secure Future Initiative.

The changing threat landscape

In late May, we published information showing new nation-state cyber activity targeting critical infrastructure organizations across the United States. The activity was disconcerting not only because of its threat to civilians across the country, but because of the sophistication of the techniques involved. As we highlighted in May, the attacks involved sophisticated, patient, stealthy, well-resourced, and government-backed techniques to infect and undermine the integrity of computer networks on a long-term basis. We witnessed similar activities this summer targeting cloud services infrastructure, including at Microsoft.

These attacks highlight a fundamental attribute of the current threat landscape. Even as recent years have brought enormous improvements, we will need new and different steps to close the remaining cybersecurity gap. As we shared last month in our annual Microsoft Digital Defense Report, the implementation of well-developed cyber hygiene practices now protect effectively against a large majority of cyberattacks. But the best-resourced attackers have responded by pursuing their own innovations, and they are acting more aggressively and with even more sophistication than in the past.

Brazen nation-state actors have become more prolific in their cyber operations, conducting espionage, sabotage, destructive attacks, and influence operations against other countries and entities with more patience and persistence. Microsoft estimates that 40% of all nation-state attacks in the past two years have focused on critical infrastructure, with state-funded and sophisticated operators hacking into vital systems such as power grids, water systems, and health care facilities. In each of these sectors, the consequences of potential cyber disruption are obviously dire.

Leveraging AI capabilities to build community trust with law enforcement agencies >

Oct 5, 2023 | Brad Smith

Advancing AI governance in Japan >

Oct 2, 2023 | Jenny Lay-Flurrie

Creating a more disability-inclusive workplace >

More Cybersecurity Stories

Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries >

April 11, 2023

Digital Crimes Unit: Leading the fight against cybercrime >

May 3, 2022

At the same time, improving protection has raised the barriers to entry for cybercriminals, but has enabled some market consolidation for a smaller but more pernicious group of sophisticated actors. Microsoft's Digital Crimes Unit is tracking 123 sophisticated ransomware-as-a-service affiliates, which lock or steal data and then demand a payment for its return. Since September 2022, we estimate that ransomware attempts have increased by more than 200%. While firms with effective security can manage these threats, these attacks are becoming more frequent and complex, targeting smaller and more vulnerable organizations, including hospitals, schools, and local governments. More than 80% of successful ransomware attacks originate from unmanaged devices, highlighting the importance of expanding protective measures to every single digital device.

Today's cyber threats emanate from well-funded operations and skilled hackers who employ the most advanced tools and techniques. Whether they work for geopolitical or financial motives, these nation states and criminal groups are constantly evolving their practices and expanding their targets, leaving no country, organization, individual, network, or device out of their sights. They don't just compromise machines and networks; they pose serious risks to people and societies. They require a new response based on our ability to utilize our own resources and our most sophisticated technologies and practices.

AI-based cyber defense

The war in Ukraine has demonstrated the tech sector's ability to develop cybersecurity defenses that are stronger than advanced offensive threats. Ukraine's successful cyber defense has required a shared responsibility between the tech sector and the government, with support from the country's allies. It is a testament to the coupling of public-sector leadership with corporate investments and to combining computing power with human ingenuity. As much as anything, it provides inspiration for what we can achieve at an even greater scale by harnessing the power of AI to better defend against new cyber threats.

As a company, we are committed to building an AI-based cyber shield that will protect customers and countries around the world. Our global network of AI-based datacenters and use of advanced foundation AI models puts us in a strong position to put AI to work to advance cybersecurity protection.

Keeping your vote safe and secure: A story from inside the 2020 election >

June 22, 2021

As part of our Secure Future Initiative, we will continue to accelerate this work on multiple fronts.

First, we are taking new steps to use AI to advance Microsoft's threat intelligence. and the Microsoft Threat Analysis Center (MTAC) are using advanced AI tools and techniques to detect and analyze cyber threats. We are extending these capabilities directly to customers, including through our Microsoft security technologies, which collects and analyzes customer data from multiple sources.

One reason these AI advances are so important is because of their ability to address one of the world's most pressing cybersecurity challenges. Ubiquitous devices and constant internet connections have created a vast sea of digital data, making it more difficult to detect cyberattacks. In a single day, Microsoft receives more than 65 trillion signals from devices and services around the world. Even if all 8 billion people on the planet could look together for evidence of cyberattacks, we could never keep up.

But AI is a game changer. While threat actors seek to hide their threats like a needle in a vast haystack of data, AI increasingly makes it possible to find the right needle even in a sea of needles. And coupled with a global network of datacenters, we are determined to use AI to detect threats at a speed that is as fast as the Internet itself.

Second, we are using AI as a gamechanger for all organizations to help defeat cyberattacks at machine speed. One of the world's biggest cybersecurity challenges today is the shortage of trained cybersecurity professionals. With a global shortage of more than three million people, organizations need all the productivity they can muster from their cybersecurity workforce. Additionally, the speed, scale, and sophistication of attacks creates an asymmetry where it's hard for organizations to prevent and disrupt attacks at scale. Microsoft's Security Copilot combines a large language model with a security-specific model that has various skills and insights from Microsoft's threat intelligence. It generates natural language insights and recommendations from complex data, making analysts more effective and responsive, catching threats that may have been missed and helping organizations prevent and disrupt attacks at machine speed.

Another vital ingredient for success is the combination of these AI-driven advances with the use of extended detection and response capabilities in endpoint devices. As noted above, today more than 80% of ransomware compromises originate from unmanaged or "bring-your-own devices" that employees use to access work-related systems and information. But once managed with a service like Microsoft Defender for Endpoint, AI detection techniques provide real-time protection that intercepts and defeats cyberattacks on computing endpoints like laptops, phones, and servers. Wartime advances in Ukraine have provided extensive opportunities to test and extend this protection, including the successful use of AI to identify and defeat Russian cyberattacks even before any human detection.

Third, we are securing AI in our services based on our Responsible AI principles. We recognize that these new AI technologies must move forward with their own safety and security safeguards. That's why we're developing and deploying AI in our services based on our Responsible AI principles and practices. We are focused on evolving these practices to keep pace with the changes in the technology itself.

While most of our cybersecurity services protect consumers and organizations, we are also committed to building stronger AI-based protection for governments and countries. Just last week, we announced that we will spend $3.2 billion to extend our hyperscale cloud computing and AI infrastructure in Australia, including the development of the Microsoft-Australian Signals Directorate Cyber Shield (MACS). In collaboration with this critical agency in the Australian Government, this will enhance our joint capability to identify, prevent, and respond to cyber threats. It's a good indicator of where we need to take AI in the future, building more secure protection for countries around the world.

New engineering advances

In addition to new AI capabilities, a more secure future will require new advances in fundamental software engineering. That's why Charlie Bell is sending to our employees this morning an email co-authored with his engineering colleagues Scott Guthrie and Rajesh Jha. This launches as part of our Secure Future Initiative a new standard for security by advancing the way we design, build, test, and operate our technology.

You can read Charlie's entire email *here*. In summary, it contains three key steps:

First, we will transform the way we develop software with automation and AI. The challenges of today's cybersecurity threats and the opportunities created by generative AI have created an inflection point for secure software engineering. The steps Charlie is sharing with our engineers today represent the next evolutionary stage of the Security Development Lifecycle (SDL), which Microsoft invented in 2004. We will now evolve this to what we're calling "dynamic SDL," or dSDL. This will apply systematic processes to continuously integrate cybersecurity protection against emerging threat patterns as our engineers code, test, deploy, and operate our systems and services. As Charlie explains, we will couple this with other additional engineering measures, including AI-powered secure code analysis and the use of GitHub Copilot to audit and test source code against advanced threat scenarios.

As part of this process, over the next year we will enable customers with more secure default settings for multifactor authentication (MFA) out-of-the-box. This will expand our current default policies to a wider band of customer services, with a focus on where customers need this protection the most. We are keenly sensitive to the impact of such changes on legacy computing infrastructure, and hence we will focus on both new engineering work and expansive communications to explain where we are focused on these default settings and the security benefits this will create.

Second, we will strengthen identity protection against highly sophisticated attacks. Identity-based threats like password attacks have increased ten-fold during the past year, with nation-states and cybercriminals developing more sophisticated techniques to steal and use login credentials. As Charlie explains, we will protect against these changing threats by applying our most advanced identity protection through a unified and consistent process that will manage and verify the identities and access rights of our users, devices, and services across all our products and platforms. We will also make these advanced capabilities freely available to non-Microsoft application developers.

As part of this initiative, we also will migrate to a new and fully automated consumer and enterprise key management system with an architecture designed to ensure that keys remain inaccessible even when underlying processes may be compromised. This will build upon our confidential computing architecture and the use of hardware security modules (HSMs) that store and protect keys in hardware and that encrypts data at rest, in transit, and during computation.

Third, we are pushing the envelope in vulnerability response and security updates for our cloud platforms. We plan to cut the time it takes to mitigate cloud vulnerabilities by 50%. We also will encourage more transparent reporting in a more consistent manner across the tech sector.

We no doubt will add other engineering and software development practices in the months and years ahead, based on learning and feedback from these efforts. Like Trustworthy Computing more than two decades ago, our SFI initiatives will bring together people and groups across Microsoft to evaluate and innovate across the cybersecurity landscape.

Stronger application of international norms

Finally, we believe that stronger AI defenses and engineering advances need to be combined with a third critical component – the stronger application of international norms in cyberspace.

In 2017, we called for a Digital Geneva Convention, a set of principles and norms that would govern the behavior of states and non-state actors in cyberspace. We argued that we needed to enforce and augment the norms needed to protect civilians in cyberspace from a broadening array of cyberthreats. In the six years since that call, the tech sector and governments have taken numerous steps forward in this space, and the precise nature of what we need has evolved. But in spirit and at its heart, I believe the case for a Digital Geneva Convention is stronger than ever.

The essence of the Geneva Convention has always been the protection of innocent civilians. What we need today for cyberspace is not a single convention or treaty but rather a stronger, broader public commitment by the community of nations to stand more resolutely against cyberattacks on civilians and the infrastructure on which we all depend. Fundamentally, we need renewed efforts that unite governments, the private sector, and civil society to advance international norms on two fronts. We will commit Microsoft's teams around the world to help advocate for and support these efforts.

First, we need to stand together more broadly and publicly to endorse and reinforce the key norms that provide the red lines no government should cross.

We should all abhor determined nation-state efforts that seek to install malware or create or exploit other cybersecurity weaknesses in the networks of critical infrastructure providers. These bear no connection to the espionage efforts that governments have pursued for centuries and instead appear designed to threaten the lives of innocent civilians in a future crisis or conflict. If the principles of the Geneva Convention are to have continued vitality in the 21st century, the international community must reinforce a clear and bright red line that places this type of conduct squarely off limits.

Therefore, *all states should commit publicly that they will not plant software vulnerabilities in the networks of critical infrastructure providers such as energy, water, food, medical care, or other providers. They should also commit that they will not permit any persons within their territory or jurisdiction to engage in cybercriminal operations that target critical infrastructure.*

Similarly, the past year has brought increasing nation-state efforts to target cloud services, either directly or indirectly, to gain access to sensitive data, disrupt critical systems, or spread misinformation and propaganda. Cloud services themselves have become a critical piece of support for every aspect of our societies, including reliable water, food, energy, medical care, information, and other essentials.

For these reasons, *states should recognize cloud services as critical infrastructure, with protection against attack under international law.*

This should lead to three related commitments:

- *States should not engage in or allow any persons within their territory or jurisdiction to engage in cyber operations that would compromise the security, integrity, or confidentiality of cloud services.*
- *States should not indiscriminately compromise the security of cloud services for the purposes of espionage.*
- *States should construct cyber operations to avoid imposing costs on those who are not the target of operations.*

Second, we need governments to do more together to foster greater accountability for nation states that cross these red lines. The year has not been lacking in hard proof of nation-state actions that violate these norms. What we need now is the type of strong, public, multilateral, and unified attributions from governments that will hold these states accountable and discourage them from repeating the misconduct.

Tech companies and the private sector play a major role in cybersecurity protection, and we are committed to new steps and stronger action. But especially when it comes to nation-state activity, cybersecurity is a shared responsibility. And just as tech companies need to do more, governments will need to do more as well. If we can all come together, we can take the types of steps that will give the world what it deserves – a more secure future.

Tags: AI, cyberattacks, cybercrime, cybersecurity, Responsible AI, Secure Future Initiative, Security Copilot, SFI

Follow us:

What's new

- Surface Laptop Studio 2
- Surface Laptop Go 3
- Surface Pro 9
- Surface Laptop 5
- Microsoft Copilot
- Copilot in Windows
- Explore Microsoft products
- Windows 11 apps

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Certified Refurbished
- Microsoft Store Promise
- Flexible Payments

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- How to buy for your school
- Educator training and development
- Deals for students and parents

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Copilot for Microsoft 365
- Small Business

Developer & IT

- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability