News AI and machine learning
6 min read

Announcing Microsoft Secure Future Initiative to advance security engineering

By Charlie Bell, Executive Vice President, Microsoft Security

November 2, 2023

Security management

> *Today Microsoft's Vice Chair and President Brad Smith shared insight on the global cybersecurity landscape and introduced our Secure Future Initiative. These engineering advances anticipate future cyberthreats, such as increasing digital attacks on identity systems. They also address how we will continue to build secure foundations necessary for the AI era and beyond.*
>
> *In the spirit of transparency and to emphasize the importance of this moment, we are sharing the internal email sent earlier about our Secure Future Initiative's strategy and objectives.*

Hi all,

As I'm sure you've all seen, cyberattacks have grown rapidly and dangerously in recent years. We now see daily headlines of major industrial disruption, attacks on medical services, and other critical aspects of our daily lives. The sheer speed, scale, and sophistication of the attacks we're seeing is a reminder for our industry and the world on how advanced digital threats have become. As computing has evolved from packaged software to cloud services, from waterfall to agile development, and with the new advances in AI, we must also evolve how we do security.

At Microsoft, we have a unique responsibility and leading role to play in securing the future for our customers and our community. We have a long and proud history of delivering innovative and impactful products and services that have shaped the industry and transformed the lives of billions of people around the world. We have also been at the forefront of developing and adopting security best practices, standards and tools that have helped us protect our customers and ourselves from cyberthreats and risks. Our move to Zero Trust, multifactor authentication, modern device management, and enhanced telemetry and detections have driven an embedded security culture across our company.

Satya Nadella, Microsoft Chief Executive Officer; Rajesh Jha, Microsoft Executive Vice President, Experiences and Devices; Scott Guthrie, Microsoft Executive Vice President, Cloud and AI; and I have put significant thought into how we should anticipate and adapt to the increasingly more sophisticated cyberthreats. We have carefully considered what we see across Microsoft and what we have heard from customers, governments, and partners to identify our greatest opportunities to impact the future of security. As a result, we have committed to three specific areas of engineering advancement we will add to our journey of continually improving the built-in security of our products and platforms. We will focus on 1. transforming software development, 2. implementing new identity protections, and 3. driving faster vulnerability response.

These advances comprise what we're calling the Secure Future Initiative. Collectively, they improve security for customers both in the near term and in the future, against cyberthreats we anticipate will increase over the horizon. We recognize that not all of you will be deeply involved in all of the advances we must make. After all, the first priority is security by default. But all of you will be engaged and, more importantly, your constant attention to security in everything you build and operate will be the source of continuous innovation for our collective secure future. Please read on, absorb the "what" and the "why," and contribute your ideas on innovation. We are all security engineers.

First, we will transform the way we develop software with automation and AI so that we do our best work in delivering software that is secure by design, by default, in deployment, and in operation. Microsoft invented the Security Development Lifecycle (SDL) and made it a bedrock principle of software trust and engineering. We will evolve it to "dynamic SDL" (dSDL). This means we're going to apply the concept of continuous integration and continuous delivery (CI/CD) to continuously integrate protections against emerging patterns as we code, test, deploy, and operate. Think of it as continuous integration and continuous security.

We will accelerate and automate threat modeling, deploy CodeQL for code analysis to 100 percent of commercial products, and continue to expand Microsoft's use of memory safe languages (such as C#, Python, Java, and Rust), building security in at the language level and eliminating whole classes of traditional software vulnerability.

We must continue to enable customers with more secure defaults to ensure they have the best available protections that are active out-of-the-box. We all realize no enterprise has the luxury of jettisoning legacy infrastructure. At the same time, the security controls we embed in our products, such as multifactor authentication, must scale where our customers need them most to provide protection. We will implement our Azure tenant baseline controls (99 controls across nine security domains) by default across our internal tenants automatically. This will reduce engineering time spent on configuration management, ensure the highest security bar, and provide an adaptive model where we add capability based on new operational learning and emerging adversary threats. In addition to these defaults, we will ensure adherence and auto-remediation of settings in deployment. Our goal is to move to 100 percent auto-remediation without impacting service availability.

One example from the past of secure defaults is widescale multifactor authentication adoption. Over the past year, we have learned a great deal as we made multifactor authentication on by default for new customers. Those learnings and our communications with customers helped pave the way for our introduction of wider multifactor authentication default policies for wider bands of customer tenants. By focusing on communications as well as engineering—explaining where we are focused on defaults and how customers benefit—we achieve more durable security for our customers. Multifactor authentication is just one area of defaults for us, but over the next year you will see us accelerate security defaults across the board, energized by our learnings and customer feedback. You will all be "customer zero" as we introduce these.

Second, we will extend what we have already created in identity to provide a unified and consistent way of managing and verifying the identities and access rights of our users, devices, and services, across all our products and platforms. Our goal is to make it even harder for identity-focused espionage and criminal operators to impersonate users. Microsoft has been a leader in developing cutting-edge standards and protocol work to defend against rising cyberattacks like token theft, adversary-in-the-middle attacks, and on-premises infrastructure compromise. We will enforce the use of standard identity libraries (such as Microsoft Authentication Library) across all of Microsoft, which implement advanced identity defenses like token binding, continuous access evaluation, advanced application attack detections, and additional identity logging support. Because these capabilities are critical for all applications our customers use, we are also making these advanced capabilities freely available to non-Microsoft application developers through these same libraries.

To stay ahead of bad actors, we are moving identity signing keys to an integrated, hardened Azure HSM and confidential computing infrastructure. In this architecture, signing keys are not only encrypted at rest and in transit, but also during computational processes as well. Key rotation will also be automated allowing high-frequency key replacement with no potential for human access, whatsoever.

Lastly, we are continuing to push the envelope in vulnerability response and security updates for our cloud platforms. As a result of these efforts, we plan to cut the time it takes to mitigate cloud vulnerabilities by 50 percent. We are in a position to achieve this because of our long investment and learnings in automation, monitoring, safe deployment, and AI-driven tools and processes. We will also take a more public stance against third-party researchers being put under non-disclosure agreements by technology providers. Without full transparency on vulnerabilities, the security community cannot learn collectively—defending at scale requires a growth mindset. Microsoft is committed to transparency and will encourage every major cloud provider to adopt the same approach.

These advances are not independent or isolated, but interdependent. They will work together to create a more holistic and comprehensive security infrastructure that can address both current and future cyberthreats. They are also aligned and consistent with our company's mission, vision, and values, and they support and enable our business goals and objectives. Over the coming months and year, you will see us announce milestones along the execution paths of the above.

As we enter the age of AI, it has never been more important for us to innovate, not only with respect to today's cyberthreats but also in anticipation of those to come. We are confident making these changes will improve the security, availability and resilience of our systems as well as increase our speed of innovation. In the coming weeks, Rajesh, Scott, and I will be meeting with our teams to share more details about these changes and how they will affect our organization, our processes, and our deliverables. We will also solicit your feedback and input on how we can implement them effectively and efficiently. We want this to be a collaborative and transparent effort that involves all of you as key stakeholders and contributors.

Security is not just a technical problem, but a human one. It affects millions of people around the world who rely on our products and services to communicate, work, learn, and play. We have the talent, the passion, and the vision to make a positive impact on the world through our work.

We appreciate your attention and your dedication.

-Charlie, Rajesh, Scott

Learn more

Learn more about Microsoft's Secure Future Initiative.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (formerly known as "Twitter") (@MSFTSecurity) for the latest news and updates on cybersecurity.

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

Azure for students

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

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads