Search the blog

🔍

Enhancing protection: Updates on Microsoft's Secure Future Initiative

By Bret Arsenault, Corporate Vice President and Chief Cybersecurity Advisor

March 6, 2024

Security management

Security operations

At Microsoft, we're continually evolving our cybersecurity strategy to stay ahead of threats targeting our products and customers. As part of our efforts to prioritize transparency and accountability, we're launching a regular series on milestones and progress of the Secure Future Initiative (SFI)—a multi-year commitment advancing the way we design, build, test, and operate our technology to help ensure that we deliver secure, reliable, and trustworthy products and services, enabling our customers to achieve their digital transformation goals and protect their data and assets from malicious actors.

Secure Future Initiative

A new world of security.

Learn more ›

Microsoft's mission to empower every person and every organization on the planet to achieve more depends on security. We recognize that when Microsoft plays a role in pioneering cutting-edge technology, we also have the responsibility to lead the way in protecting our customers and our own infrastructure from cyberthreats. Against the exponentially increasing pace, scale, and complexity of the security landscape, it's critical that we evolve to be more dynamic, proactive, and integrated in our security model to continue meeting the changing needs and expectations of our customers and the market. Our rich history in innovation is a testament to our commitment to delivering impactful and trustworthy products and services that that shape industries and transform lives. This legacy continues as we consistently work to set new benchmarks for safeguarding our digital future.

Expanding upon our foundation of built-in security, in November 2023 we launched the Secure Future Initiative (SFI) to directly address the escalating speed, scale, and sophistication of cyberattacks we're witnessing today. This initiative is an anticipatory strategy reflecting the actions we are taking to "build better and respond better" in security, using automation and AI to scale this work, and strengthen identity protection against highly sophisticated cyberattacks. It's not about tailoring our defenses to a single cyberattack: SFI underscores the importance of a continually and proactively evolving security model that adapts to the ever-changing digital landscape.

Four months have passed since we introduced SFI, and the achievements in our engineering developments demonstrate the concrete actions we've implemented to make sure that Microsoft's security infrastructure stays strong in a constantly changing digital environment. Read more below for updates on the initiative.

Transforming software development with automation and AI

As noted in our November 2, 2023 SFI announcement, we're **evolving our [security development lifecycle (SDL)](#) to continuous SDL**—which we define as applying systematic processes to continuously integrate cybersecurity protection against emerging threat patterns as our engineers code, test, deploy, and operate our systems and service. [Read more about continuous SDL here](#).

As part of our evolution to continuous SDL, we're **deploying [CodeQL](#) for code analysis to 100% of our commercial products**. CodeQL is a powerful static analysis tool in the software security space. It offers advanced capabilities across numerous programming languages that detect complex security mistakes within source code. While our code repos go through rigorous SDL assessment leveraging traditional tooling, as part of our SFI work we now use CodeQL to cover 86% of our Azure DevOps code repositories from our commercial businesses in our Cloud and AI, enterprise and devices, security and strategic missions, and technology groups. We are expanding this further and anticipate that completing the consolidation process of the last 14% will be a complex, multi-year journey due to specific code repositories and engineering tools requiring additional work. In 2023, we onboarded more than one billion lines of source code to CodeQL, which highlights our commitment toward progress.

As part of efforts to **broaden adoption of memory safe languages**, we donated **USD1 million in December 2023 to the [Rust Foundation](#)**, an integral partner in stewarding the Rust programming language. Additionally, we're **providing an additional USD3.2 million to the Alpha-Omega project**. In partnership with the [Open Source Security Foundation (OpenSSF)](#) and co-led with Google and Amazon, Alpha-Omega's mission is to catalyze security improvements to the most widely deployed open source software projects and ecosystems critical to global infrastructure. Our contribution this year will help expand coverage, more than doubling the number of widely deployed open source projects we analyze, including 100 of the most commonly used open source AI libraries. The [Alpha-Omega 2023 Annual Report](#) highlights security and process improvements from last year and strides toward fostering a sustainable culture of security within open source communities.

Together, our SFI-driven advances in expanding continuous SDL, fostering secure open source updates, and adopting memory safe languages strengthen the foundation of software throughout Microsoft's own products and platforms, as well as the wider industry.

Strengthening identity protection against highly sophisticated attacks

As part of our SFI engineering advances, **we're enforcing the use of standard identity libraries such as the [Microsoft Authentication Library (MSAL)](#) enterprise-wide** across Microsoft. This initiative is pivotal in achieving a cohesive and reliable identity verification framework. It facilitates seamless, policy-compliant management of user, device, and service identities across all Microsoft platforms and products, ensuring a fortified and consistent security posture.

Our efforts have already seen noteworthy achievements in several key areas. We've reached a major milestone with full integration of MSAL into Microsoft 365 across all four major platforms: Windows, macOS, iOS, and Android marking a significant advancement toward universal standardization. This integration ensures that Microsoft 365 applications are underpinned by a unified authentication mechanism. In the Azure ecosystem, encompassing critical tools such as Microsoft Visual Studio, Azure SDK, and Microsoft Azure CLI, MSAL has been fully adopted, underscoring our commitment to secure and streamlined authentication processes within our development tools. Furthermore, over 99% of internal service-to-service authentication requests, using [Microsoft Entra](#) for authorization, now utilize MSAL, highlighting our dedication to boosting security and efficiency in inter-service communications. Ultimately, these milestones further harden identity and authorization across our vast estate, making it increasingly difficult for threats and intruders to move between users and systems.

Looking ahead, we're setting ambitious objectives to [further bolster our security infrastructure](#). By the end of this year, we aim to fully automate the management of Microsoft Entra ID and Microsoft Account (MSA) keys. This process will include rapid rotation and secure storage of keys within Hardware Security Modules (HSMs), significantly enhancing our security measures. Additionally, we're on track to ensure that Microsoft's most widely used applications transition to standard identity libraries by the end of the year. Through these collective efforts we aim to not only enhance security but also improve the user experience and streamline authentication processes across our product suite.

Stay up to date on the latest Secure Future Initiative updates

As we forge ahead with the SFI, Microsoft remains unwavering in its commitment to continuously evolve our security posture and provide transparency in our communications. We're dedicated to innovating, protecting, and leading in an era where digital threats

are constantly changing. The progress we've shared today is only a fraction of our comprehensive strategy to safeguard the digital infrastructure and our customers who rely on it.

In the coming months, we will continue to share our progress on enhancing our capabilities, deploying innovative technologies, and strengthening our collaborations to address the complexities of cybersecurity. We're committed to building a safer, more resilient digital world, with a focus on transparency and safety in every step.

To learn more about the Microsoft SFI and read more details on our three engineering advances, visit our built-in security site.

Learn more about Microsoft Security solutions and bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

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)