Microsoft

Secure Future Initiative

Security above all else

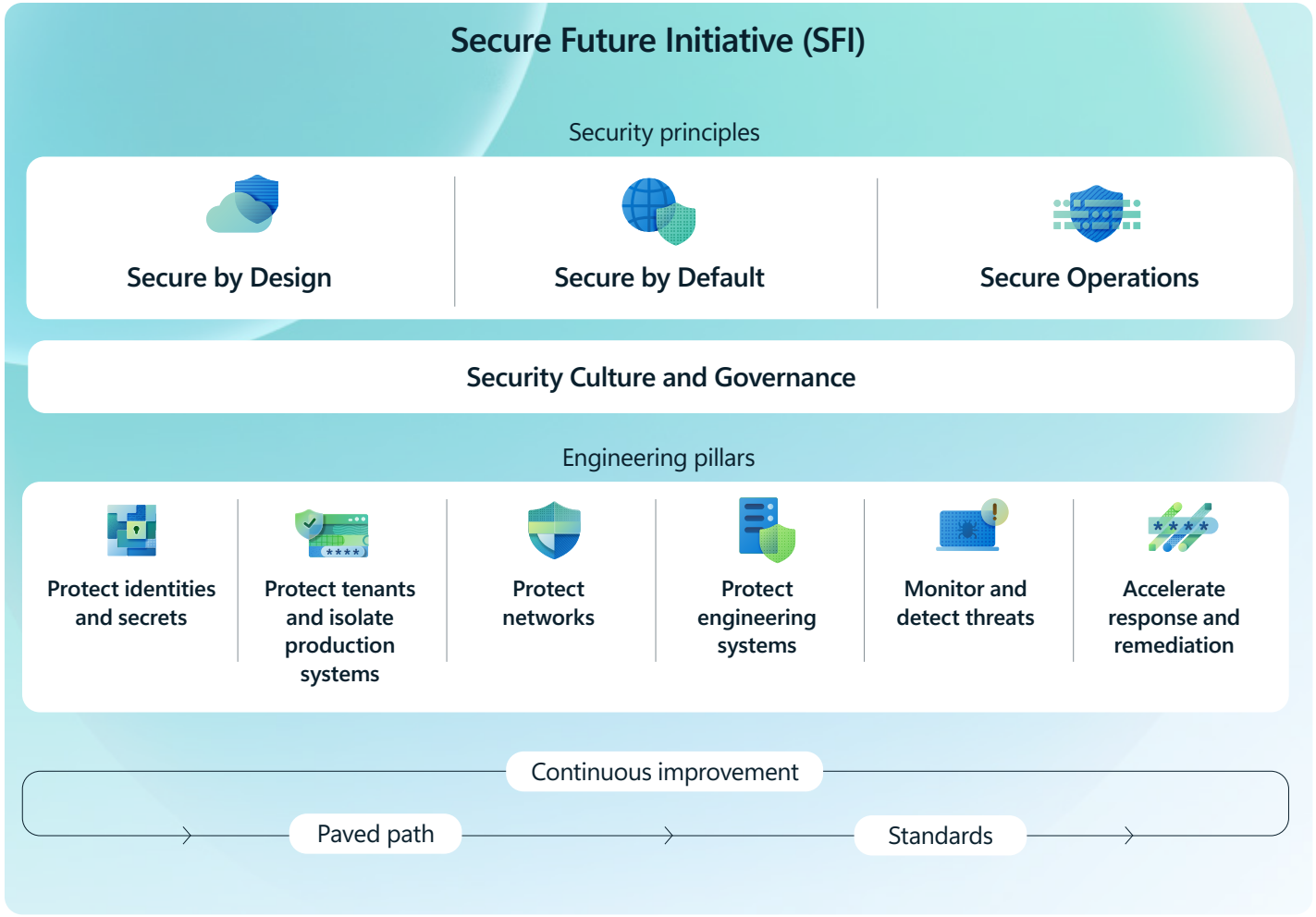
November 2025 Executive Summary

The Microsoft Secure Future Initiative (SFI) is a continuous commitment to revolutionize the way we design, build, test, and operate our products and services, to achieve the highest security standards.

Contents

For the full report, visit:

› aka.ms/SFIReportPage



Introduction

> “Security is just part of everything we do. It’s a way of life for inventing technology and using technology.”

Charlie Bell
EVP, Microsoft Security

In our third progress report, we share updates for every area and engineering pillar, introduce mapping to the NIST Cybersecurity Framework[1] to help customers understand progress made using a recognized industry framework, and highlight new security capabilities delivered to customers. We also share best practices and implementation guidance, aligned to Zero Trust principles, to help customers reduce their risk.

Culture and governance

We continue to foster a culture that puts security first by embedding security into our hiring, onboarding, and performance systems. This has reinforced accountability and accelerated cybersecurity talent development at every level, and increased engineering sentiment on security.

We have invested in additional governance structures to address cybersecurity risk and compliance, and expanded Deputy Chief Information Security Officer functions to cover additional domains. To address cybersecurity risk on a global scale we implemented the Microsoft European Security Program and participated in multistakeholder diplomacy efforts like the Advancing Regional Cybersecurity Initiative in the Global South.

1. https://www.nist.gov/cyberframework

Security principles

To help better protect customers, teams across the company delivered 17 innovations aligned with our security principles of Secure by Design, Secure by Default, and Secure Operations, for example:

- **Microsoft Azure** expanded mandatory MFA to all Azure service users and now offers secure-by-default VM connectivity through Azure Bastion Developer, significantly reducing the attack surface by ensuring secure credentials and protected connectivity.
- **Microsoft 365** introduced dedicated AI and security governance roles to enforce least-privilege for new capabilities, including the AI administrator role and Copilot agent lifecycle controls.
- **Windows 11** expanded passwordless sign-in support and introduced Quick Machine Recovery capabilities. Microsoft Surface enhanced device security by using firmware and drivers written in memory-safe languages.
- **Microsoft Purview** introduced the ability to centrally manage and proactively monitor AI data security across Copilots, agents, and apps, including those using third-party LLMs. Microsoft Sentinel can now ingest data and correlate signals across domains with new data lake, graph, and Model Context Protocol (MCP) server capabilities.

Secure by Design

Security comes first when designing any product or service.

Secure by Default

Security protections are enabled and enforced by default, require no extra effort, and are not optional.

Secure Operations

Security controls and monitoring will continuously be improved to meet current and future threats.

Introduction continued

> “There’s never a day that our mission is accomplished. The threat landscape will continue to evolve.”

Joy Chik
President, Identity & Network Access and Executive Sponsor, SFI

Engineering pillars

We continue to make steady progress in every engineering pillar: out of 28 objectives, 5 are nearing completion and 12 have made significant progress.

Key achievements include:

- **99.6%** adoption of phishing-resistant MFA for users and devices.
- **44,500** higher-risk users moved to locked-down Azure Virtual Desktops to reduce device compromise risk.
- Complete network device inventory and lifecycle management.
- **99.5%** detection and remediation of live secrets in code.
- More than **USD $17 million** awarded to promote responsible disclosure of vulnerabilities.
- **50+** new detections deployed to the Microsoft infrastructure to target high priority tactics, techniques, and procedures – applicable detections will be integrated into Microsoft Defender.

This progress drives continuous innovation across our products, services, and security portfolio - Microsoft Entra, Purview, Defender, Sentinel, and Intune.

Actionable guidance

It also informs the guidance we provide. In this report we highlight 10 patterns and practices customers can follow to reduce their risk in prioritized areas and share additional best practices and guidance for each area and pillar.

Key themes include:

- **Strengthen** identity and access controls
- **Enforce** least-privilege, stringently and at scale
- **Secure** multi-tenant environments
- **Harden** software development lifecycle and supply chain
- **Improve** visibility and monitoring
- **Accelerate** detection and response

99.6%
adoption of phishing-resistant MFA for users and devices.

Continuous improvement

With the equivalent of 35,000 engineers working full time to improve security, SFI remains the largest cybersecurity effort in digital history. Looking forward, we will continue to prioritize the highest risks, accelerate the delivery of security innovations to better protect customers, rigorously enforce our Security Durability Model, and use AI to increase engineering efficiency and accelerate threat response.

The threat landscape will continue to evolve. Technology will continue to advance. Microsoft will continue to prioritize security above all else.

We are grateful for the partnership and look forward to innovating together for a safer future.

35,000
equivalent of full-time Microsoft engineers dedicated to security.

Report background and methodology

> From the very beginning Satya has been clear. Our priority is security. And if you have to make a choice between security and something else, you choose security."

Amy Hogan-Burney
CVP, Customer Security & Trust

Culture, governance, and security principles

For each area we provide examples of progress and customer guidance. For principles we include innovation highlights and implementation insights.

Engineering pillars

In May 2024 we announced the expansion of SFI to include 6 prioritized engineering pillars and 28 aligned objectives. Engineering owners were assigned to each engineering pillar. They established an initial body of work and scope to advance the objective, according to Microsoft priorities. The work was then translated into standards and key results.

Since that time, pillar owners have expanded on the initial body of work, adding new scope, standards or key results based on changes in the threat landscape, risk prioritization from the Cybersecurity Governance Council, and learnings from ongoing implementation. In April 2025 we disclosed progress made towards completing each objective. In this report we continue to disclose cumulative progress made towards objectives, introduce mapping to NIST CSF, and provide customer guidance.

We calculated progress by recording the completed percentage of standards and key results, those defined initially and any additions.

Some objectives focus on a limited scope of products. We do not disclose the full body of work we are undertaking to advance an objective (such as standards and key results) but do share examples of progress made against specific standards and key results. In a few cases progress is not reflected as a percentage completed, instead we show the number of innovations, detections, or no-action cloud CVEs we have created since the previous progress report.

Each objective represents a significant body of work to improve security in a specific area and reduce risk for Microsoft and our customers. Some objectives will take several years to complete. Those nearing completion may require ongoing management to continue to maintain risk reduction.

Progress made will not be linear. Standards and key results may change over time due to emerging risks or technology. Progress may regress due to an increase in the body of work prioritized to complete the objective or advance rapidly due to innovation.

Measuring investments in cybersecurity risk reduction and communicating progress in a durable manner across the magnitude of engineering activities SFI covers is an imperfect science. While this report cannot address every nuance of Microsoft efforts, it is intended to communicate SFI progress in a way that demonstrates our Microsoft security investments and underscores important advancements relevant for the awareness and activities of our customers and the industry.

Progress legend

Each objective represents a significant body of work, most will take years to complete.

Out of 28 objectives, 5 are nearing completion, 12 have made significant progress, and we continue to make progress against the rest. We prioritized the highest risks, most critical assets, and used platform engineering practices to scale the work, drive clear prioritization, and reduce toil.

Icon	Description	Total objectives
	0-32% Initial progress	3
	33-65% Progress	4
	66-94% Significant progress	12
	95-99% Nearing completion	5
	No percentage	4

Progress highlights

This section provides a summary of key progress, with detailed explanations to follow.

Culture

We continue to foster a culture that puts security first across the organization.

- 95% of employees have already completed the latest security training assigned in July 2025 on Guarding Against AI-Powered Attacks, which remains one of our highest-rated courses.
- Engineering sentiment around security has increased by 9 points since February 2024.
- To reinforce a security-first mindset at work and at home, we developed resources for employees and made them available to customers for the first time to improve security awareness.

+9pts

Engineering sentiment has increased by 9 points since the initial survey.

Governance

We continue to scale our governance model to address the evolving threat landscape and increased regulatory complexity.

- Expanded the scope of the Council to include 3 additional Deputy CISO functions:
  - Supply Chain and Third-Party
  - Business Functions, Marketing, and Finance
  - Compliance with EU cybersecurity legislation
- Created the Microsoft European Security Program to deepen partnerships and better inform European governments about the threat landscape. Continued active engagement in the European Union Cyber Resilience Act Expert Group.
- Actively collaborated with industry partners to better align existing and future cybersecurity regulations and build cybersecurity capacity through the Advancing Regional Cybersecurity Initiative in the Global South.

+3

Expanded scope to include 3 additional Deputy CISO functions.

Progress highlights continued

Security principles

Guided by three security principles – Secure by Design, Secure by Default, and Secure Operations – teams across Microsoft continue to deliver innovations to help protect customers and Microsoft.

Microsoft Azure

Introduced mandatory secure defaults, expanded hardware-based trust, and updated security benchmarks to help improve cloud security.

- MFA is now mandatory for all Azure users, reducing the risk of password-related attacks. Additionally, Azure Bastion Developer now offers secure-by-default connectivity to virtual machines in 35 regions.
- Version 2 of the Microsoft Cloud Security Benchmark (MCSB) provides customers with updated security baseline guidance, which can be implemented using Microsoft Defender for Cloud.
- Azure Local increased the number of security default settings by 25% (400 settings). This further simplifies customers' ability to comply with industry standards and better protects Azure Local nodes from additional threats such as fileless malware.

Microsoft 365

Introduced a dedicated AI role, enhanced agent lifecycle governance, and improved data security transparency to give organizations more control and visibility.

- The dedicated AI Administrator role enables more secure, least-privilege management of Copilot and other emerging AI capabilities, eliminating the need for broad administrative access.
- Centralized controls enhance agent lifecycle governance by enabling administrators to approve, restrict, and audit agents in Microsoft 365 while monitoring access and usage to ensure more secure, compliant operations.
- Copilot web search transparency with Microsoft Purview Data Security Posture Management (DSPM) enables prompt-level auditing and investigation of external data sourcing risks.

Windows 11

Introduced automatic recovery capabilities, expanded passkey and Windows Hello support, and improved memory safety in firmware and drivers. These updates help enforce Zero Trust principles, resulting in improved security and resilience.

- Quick Machine Recovery automatically detects and remediates boot failures via a secure, cloud-connected recovery environment, delivering built-in resilience.
- Windows Hello now supports additional passwordless sign-in options, such as Enhanced Sign-in Security fingerprint peripherals, and an API enables passkey managers to leverage Hello for seamless authentication with FIDO2-compliant credentials.
- Surface is improving device security by developing UEFI firmware in memory-safe languages, building drivers in Rust, and working with the ecosystem to open-source these innovations and elevate protection standards across Windows.

Microsoft Security

Introduced data security posture management for AI, evolved Sentinel into an AI-first platform with data lake, graph, and MCP capabilities, and delivered new agents to automate high-volume tasks.

- Microsoft Purview DSPM for AI helps secure AI app data and proactively monitor AI use, including Copilots, agents, and other AI apps that use third-party large language modules (LLMs).
- Microsoft Sentinel has evolved to be both a SIEM and AI-ready platform, giving defenders a single platform to ingest signals, correlate across domains, and empower AI agents built in Security Copilot, VS Code using GitHub Copilot, or other developer platforms.
- Security Copilot agents introduce autonomous, AI-powered support for high-volume security and IT tasks, integrated across Microsoft Security and partner solutions, available via Microsoft Security Store.

Progress highlights continued

Engineering

Out of 28 objectives, 5 are nearing completion, 12 have made significant progress, and we continue to make progress against the rest. As a result of SFI we have improved security in our platform and services, as well as our ability to detect and respond to threats.

1. Protect identities and secrets

We have improved identity security for Microsoft services and customers.

- Migrated 95% of Microsoft Entra ID signing VMs to Azure Confidential Compute.
- Moved 94.3% of Microsoft Entra ID security token validation to our standard identity Software Development Kit (SDK).
- Enforced phishing-resistant MFA for 99.6% of Microsoft employees and devices.

2. Protect tenants and isolate production systems

We continue to increase isolation and reduce the risk of lateral movement.

- Discontinued the use of Active Directory Federation Services (ADFS) in our productivity environment.
- Migrated 98% of cloud assets managed by Azure Service Manager (ASM) to Azure Resource Manager (ARM).
- Decommissioned 560,000 additional unused and aged tenants and 83,000 unused Microsoft Entra ID apps across Microsoft production and productivity environments.

3. Protect networks

Progress made has improved network security and delivered new capabilities for customers.

- Achieved complete network device inventory and mature asset lifecycle management.
- Strengthened security through enhanced isolation and protective controls.
- Accelerated adoption of Network Security Perimeter (NSP) with more than 1.1 million resources in learning mode and approximately 500,000 in enforced mode.

4. Protect engineering systems

We have improved the security of systems we use to build, test, and deploy code.

- Code signing is now almost entirely locked to production identities, and secrets detected in code are continuously remediated.
- Near complete software asset inventory enables rapid incident response and universal policy enforcement.
- Expanded secure-by-default pipelines and network isolation, with nearly all production builds and 94% of release pipelines using governed templates.

5. Monitor and detect threats

We are advancing threat hunting, rapid incident response, and unified security controls.

- 98% of production infrastructure is centrally tracked, with logs retained for 2 years.
- 50+ new detections deployed across Microsoft infrastructure, targeting high-priority tactics, techniques, and procedures (TTPs) – applicable detections will be integrated into Microsoft Defender.
- AI integration is accelerating detection lifecycle improvements – from identification to efficacy validation.

6. Accelerate response and remediation

We are increasing the speed of identification, triage, and resolution of vulnerabilities.

- AI-based vulnerability triage contributed to a 72% success rate addressing vulnerabilities within our reduced time to mitigate, despite continued increase in volume and scope.
- Expedited deployment processes have accelerated vulnerability mitigation.
- Microsoft published 1,096 CVEs, including 53 no-action cloud CVEs, and paid out USD $17 million in bounties, demonstrating increased transparency and external engagement.

Customer guidance

SFI patterns and practices offer repeatable, proven approaches to solving complex cybersecurity challenges. Each pattern is crafted to address a specific security risk and is grounded in Microsoft's own experience. Like design patterns in software architecture, these security patterns are modular, extensible, and built for reuse across diverse environments.

Each pattern follows a consistent structure – clearly defining the cybersecurity challenge, outlining the problem, describing Microsoft's solution, offering practical guidance, and clarifying the implications.

SFI patterns and practices (Taxonomy)

Pattern name:	Concise handle to describe a cybersecurity problem
Problem:	Explain the security challenge and its operational context
Solution:	Describes how Microsoft addressed the issue internally
Guidance:	Describes how customers can apply these learning in their own environments
Implications:	Outcomes and trade-offs of applying this pattern

SFI based actionable guidance

- **Phishing-resistant MFA** – Adopt cryptographic, phishing-resistant methods such as passkeys, FIDO2 security keys, and certificate-based authentication across all users and tenants to reduce exposure to credential based attacks.
- **Eliminate identity lateral movement** – Segment access, enforce Conditional Access policies, and restrict risky guest authentication to prevent attackers from pivoting across tenants or roles.
- **Secure all tenants and their resources** – Help eliminate "shadow" tenants. Apply baseline security policies, such as MFA and Conditional Access, to every cloud tenant and retire unused ones, so cyberattackers can't exploit forgotten, weakly-secured environments.
- **Remove legacy systems that risk security** – Decommission unmanaged tenants and outdated infrastructure to reduce configuration drift and shrink your attack surface.
- **Standardize secure development pipelines** – Implement governed continuous integration and continuous delivery (CI/CD) templates to embed security gates, encourage the generation of Software Bill of Materials (SBOMs), and drive consistent compliance.
- **Protect the software supply chain** – Lock down builds and dependencies. Govern your CI/CD pipelines and package management – use standardized build templates, internal package feeds, and automated scanning to block supply chain cyberattacks before they reach production.
- **Complete production infrastructure inventory** – Ensure real-time visibility into assets and telemetry by consolidating inventories, centralizing monitoring, and removing unused applications.
- **Centralize access to security logs** – Speed up investigations. Standardize and centralize your log collection (with longer retention) so that security teams have unified visibility and can detect and investigate incidents faster – even across complex, multi-cloud environments.
- **Rapid anomaly detection and response** – Leverage AI and user behavior analytics, alongside automated response workflows, to detect malicious activity quickly and reduce dwell time.
- **Accelerate vulnerability mitigation** – Automate detection, triage, and patching workflows. Integrate vulnerability management with orchestration tools to minimize time-to-mitigate and enhance resilience.

Customers are encouraged to review the full library of SFI patterns and practices at **aka.ms/SFIpnp**, as well as the best practices and guidance detailed throughout the report.

Microsoft

Secure Future Initiative (SFI)

November 2025 progress report

©2025 Microsoft Corporation. All rights reserved.