Microsoft

Secure Future Initiative

September 2024 progress report

Security above all else

- Protect identities and secrets
- Protect tenants and isolate production systems
- Protect networks
- Protect engineering systems
- Monitor and detect threats
- Accelerate response and remediation

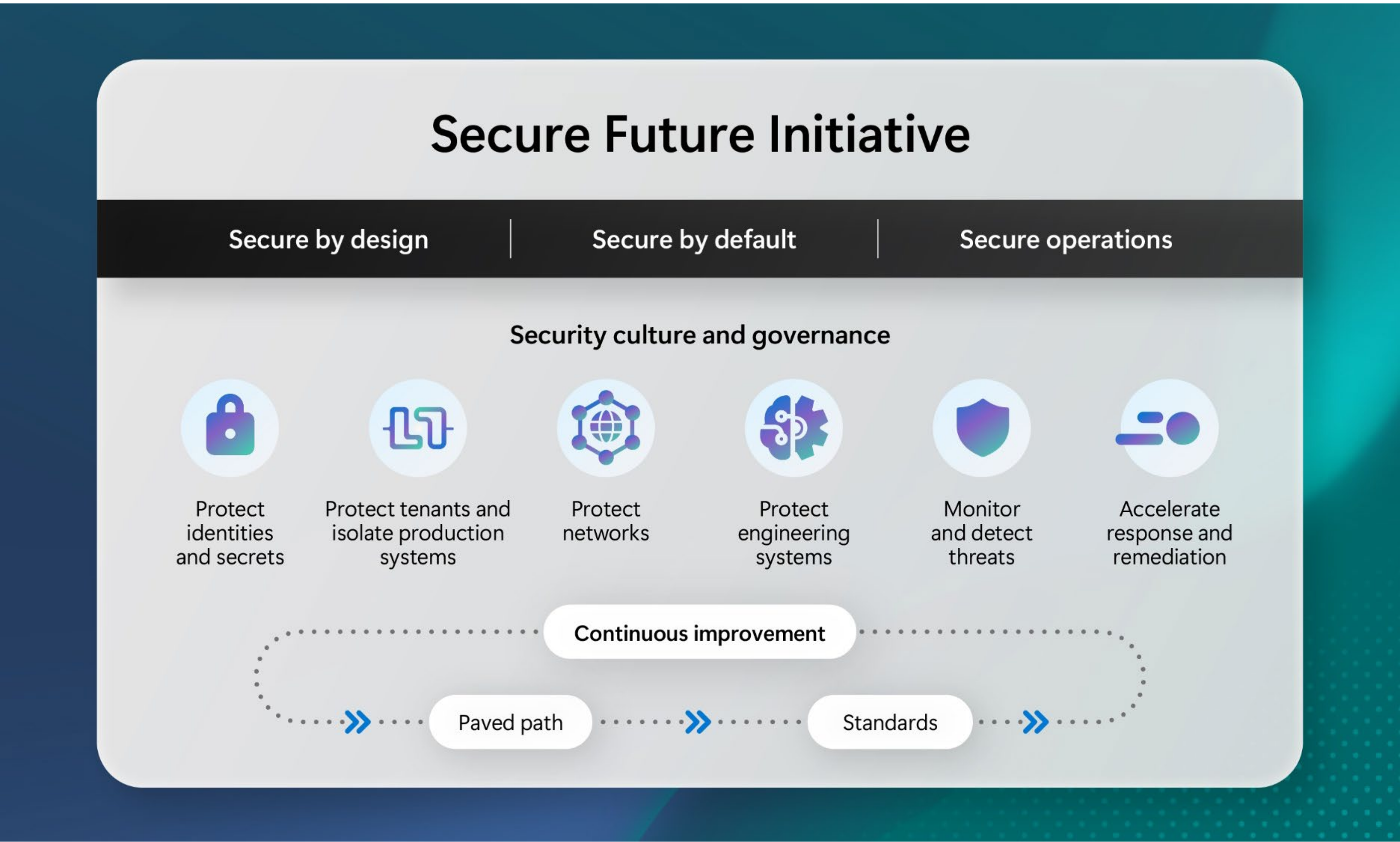
Executive summary

In November 2023, Microsoft announced the Secure Future Initiative (SFI) to address the increasing scale, speed, and sophistication of cyberattacks. Launched as a multi-year endeavor, SFI evolves how Microsoft designs, builds, tests, and operates products and services to achieve the highest possible standards for security.

In May 2024, CEO Satya Nadella made security the company's top priority, underscoring the importance of SFI as a comprehensive, cross-company effort that involves every employee in driving progress towards greater security and resiliency.

Our engineering teams quickly dedicated the equivalent of 34,000 full-time engineers to address the highest priority security tasks—the largest cybersecurity engineering project in history. We have also made significant improvements in governance and culture, such as integrating security into performance reviews and introducing the Security Skilling Academy.

This report includes highlights of the progress made over the past several months followed by individual sections with additional details.



Secure Future Initiative

Secure by design | Secure by default | Secure operations

Security culture and governance

Protect identities and secrets

Protect tenants and isolate production systems

Protect networks

Protect engineering systems

Monitor and detect threats

Accelerate response and remediation

Continuous improvement

Paved path

Standards

Highlights

Culture

- **Significant investment:** Dedicating the equivalent of 34,000 full-time engineers, SFI is the largest cybersecurity engineering project in history.
- **Security as #1 priority:** Security added as a core priority for all employees, measured against all performance reviews. The Microsoft senior leadership team's compensation is now tied to security performance.
- **Security Skilling Academy:** Launched in July, this academy offers curated training for all employees, reinforcing the importance of security in daily operations.

Governance

- The Microsoft senior leadership team reviews SFI progress weekly and updates are provided to the Microsoft Board of Directors quarterly.
- Introduction of Cybersecurity Governance Council and Deputy Chief Information Security Officers (Deputy CISOs) who are aligned with foundational security functions and all engineering divisions to help ensure comprehensive and cohesive security governance.

Engineering pillars

To ensure security is the #1 priority, we have integrated a common framework for security work prioritization across all engineering teams. We scale this work using platform engineering patterns, enabling rapid progress and productivity.

1. **Protect identities and secrets:** We completed updates to Microsoft Entra ID and Microsoft Account (MSA) for our public and US government clouds to generate, store, and automatically rotate access token signing keys using the Azure Managed Hardware Security Module (HSM) service. We have continued to drive broad adoption of our standard identity SDKs which provide consistent validation of security tokens. This standardized validation now covers more than 73% of tokens issued by Microsoft Entra ID for Microsoft owned applications. We have extended standardized security token logging in our standard identity SDKs to support threat hunting and detections and enabled those in several critical services ahead of broad adoption. We completed enforcement of the use of phishing-resistant credentials in our production environments and implemented video-based user verification for 95% of Microsoft internal users in our productivity environments to eliminate password sharing during setup/recovery.
2. **Protect tenants and isolate production systems:** We completed a full iteration of app lifecycle management for all of our production and productivity tenants, eliminating

730,000 unused apps. We eliminated 5.75 million inactive tenants, drastically reducing the potential attack surface. We implemented a new system to streamline the creation of testing and experimentation tenants with secure defaults and strict lifetime management enforced. We have deployed more than 15,000 new production-ready locked-down devices in the last three months.

3. **Protect networks:** More than 99% of physical assets on the production network are recorded in a central inventory system, which enriches asset inventory with ownership and firmware compliance tracking. Virtual networks with backend connectivity are isolated from the Microsoft corporate network and subject to complete security reviews to reduce lateral movement. To help customers secure their own deployments, we have expanded platform capabilities such as Admin Rules to ease the network isolation of platform as a service (PaaS) resources such as Storage, SQL, Cosmos DB, and Key Vault.
4. **Protect engineering systems:** 85% of our production build pipelines for the commercial cloud are now using centrally governed pipeline templates, making deployments more consistent, efficient, and trustworthy. We have slimmed down the lifespan of Personal Access Tokens to seven days, disabled SSH access for all Microsoft internal engineering repos, and significantly reduced the number for elevated roles with access to engineering systems. We also implemented proof of presence checks for critical chokepoints in our software development code flow.
5. **Monitor and detect threats:** We have made significant progress enforcing that all Microsoft production infrastructure and services adopt standard libraries for security audit logs, to ensure relevant telemetry is emitted, and retain logs for a minimum of two years. For instance, we have established central management and a two-year retention period for identity infrastructure security audit logs, encompassing all security audit events throughout the lifecycle of current signing keys. Similarly, over 99% of network devices are now enabled with centralized security log collection and retention.
6. **Accelerate response and remediation:** We updated processes across Microsoft to improve time to mitigate for critical cloud vulnerabilities. We began publishing critical cloud vulnerabilities as common vulnerability and exposures (CVEs), even if no customer action is required, to improve transparency. We established the Customer Security Management Office (CSMO) to improve public messaging and customer engagement for security incidents.

Culture and governance

Through SFI, Microsoft is evolving our practices, policies, and governance structures to ensure that every employee prioritizes security above all else and applies a growth mindset, resulting in continuous improvement. This section provides an update on progress made in culture and promoting a security-first mindset throughout Microsoft. This section also provides an update on the progress made in governance, to help manage risks and ensure compliance with the highest security standards.

Key learning

Continuous training and discussions geared toward all employees are essential to promoting a security-first mindset across all levels of the organization. Increased governance improvements are critical to maintaining and enhancing our security posture.

Culture and governance in practice

Culture

In May 2024, Satya Nadella emphasized that security is the number one priority for Microsoft, a commitment reinforced by integrating cybersecurity performance into the senior leadership team's compensation plans. Starting fiscal year 2025, security became a "Core Priority" in performance reviews for all employees, ensuring it remains central to our planning, execution, and governance. To support this, continuous training and resources help employees apply a growth mindset to security in their daily work. On July 15, 2024, Microsoft launched the Microsoft Security Academy, a personalized learning experience of security-specific, curated trainings for all worldwide employees. By prioritizing security in all operations and offering targeted training, we are fortifying our security posture.

Governance

To ensure accountability and transparency at the highest levels, the Microsoft senior leadership team reviews SFI progress weekly and updates are provided to the Microsoft Board of Directors quarterly.

To enhance governance, we have established a new Cybersecurity Governance Council and have appointed Deputy Chief Information Security Officers (Deputy CISOs) aligned to foundational security functions and all engineering divisions. Deputy CISOs, together with our CISO Igor Tsyganskiy, form the newly established Cybersecurity Governance Council. As a group, they take responsibility for the company’s overall cyber risk, defense, and compliance.

Each Deputy CISO represents and is accountable for a security domain—an engineering division into which they report or a foundational security function reporting to the CISO.

The Cybersecurity Governance Council collaborates with SFI engineering leadership to define and prioritize SFI work as well as set future direction. The council is accountable for the implementation of regulatory requirements, ongoing compliance, and determining the security architecture necessary to achieve our goals. The council reports on cyber risk and compliance to the CISO, who in turn reports this information to the Microsoft senior leadership team and to the Microsoft Board of Directors. Tom Burt, Corporate Vice President for Customer Security & Trust, serves as Secretary of the Council for its work specific to regulatory compliance. Microsoft currently has Deputy CISOs aligned to:

- Artificial Intelligence
- Azure
- Consumer
- Core Systems and Mergers and Acquisitions
- Customer Security Management Office
- Experiences and Devices
- Gaming
- Government
- Identity
- Microsoft 365
- Microsoft Security
- Regulated Industries
- Threat Landscape

Principles

The Secure Future Initiative (SFI) builds on three core principles which ensure that our products are secure from inception through deployment and ongoing use.

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.

Principles in practice

All product teams apply these principles by adopting the Microsoft Security Development Lifecycle (SDL), a practical security approach that is risk-driven and agnostic to development methodology or technology. It describes essential practices and specific requirements for all stages of a device, software, or service lifecycle to reduce the frequency and severity of vulnerabilities.

Examples of required processes

- Perform secure design review and threat modeling.
- Conduct usability testing to encourage secure configurations.
- Perform security testing to assess system security requirements.
- Incorporate threat intelligence feeds into security operations.
- Follow a well-developed and regularly tested incident response plan.

Examples of resulting product goals

- Encourage integrated authentication methods and use of Hardware Security Modules (HSM).
- Automate the application of best practices by enforcing automatic updates and conditional access.
- Provide mechanisms that help customers build their security awareness, adopt good security habits, and guard against social engineering and other deceptive attacks.
- Incorporate security logs and the ability to monitor activity into every product.
- Clearly and simply explain security settings and communicate risks of deviating from secure defaults.

The SDL has been a company-wide policy at Microsoft since 2004. Microsoft engineering teams are required to adopt the SDL, which is regularly updated based on current and future threats.

Using SDL requirements, SFI acts as a large-scale, Microsoft-wide campaign to apply the three core principles, address vulnerabilities, and implement defense-in-depth strategies. New learnings from incidents are continuously incorporated into the SDL, and significant learnings are considered for high-priority remediation to be driven through SFI standards.

Standards and paved paths

Operationalizing an infrastructure project at Microsoft's scale—more than 100,000 engineers, PMs, and designers with over 500,000 work items modified per day and 5 million builds per month—is an enormous task that requires significant alignment and coordination. Driving continuous improvement in operational efficiency requires measurement and feedback systems. To scale SFI, drive rapid progress, and to accelerate individual and team productivity, we are leveraging Microsoft Platform Engineering practices and tools. Platform engineering is a practice, built up from DevOps principles, that seeks to improve security, compliance, costs, and time-to-business value with streamlined developer experiences and self-service infrastructure within a secure, governed framework. Platform engineering is both a product-based mindset shift and the adoption of a set of tools, systems, and processes. Applying well-established platform engineering patterns to SFI enabled us to make significant progress and maintain individual and team productivity.

Key learning

When organizational objectives like security, resilience, and compliance are at odds with individual productivity, developers and operators will tend to "work-around" the requirement. As such, it's important that every standard helps not only to improve our security posture but also improves developer velocity, efficiency, satisfaction, and reduces ongoing toil.

Paved paths and standards in practice

In the adoption of platform engineering within Microsoft, we've formalized the concepts of "paved paths" and "standards." Paved paths are infrastructure and recommended best practices which measurably impact team productivity and the quality of our products. When paved paths move beyond just a recommendation to a requirement, we formalize it as a standard.

Standards are value-focused statements all products and infrastructure must achieve. By raising our baseline standards and by providing structured, secure methods for development and operations of those standards, we minimize vulnerabilities and enhance the overall security for our products and infrastructure. Standards can include the use of specific infrastructure to achieve a compliance goal or the adoption of a process.

Each standard must be clearly specified, actionable to specific code or infrastructure, and it should implement a plan for ensuring that compliance with the standard will endure. To drive the standards across our entire estate, we build and maintain comprehensive inventory systems with clear component ownership within the organization and ways to facilitate assignment of work items at scale. Our strategy for delivering enduring compliance with the standard is to identify how we will Start Right, Stay Right, and Get Right for each standard, which are then driven programmatically through dashboard driven reviews.

- **Start Right** equips developers and operators with self-service tools, enabling them to kickstart their projects quickly while adhering to standards defined through templates and policies.
- **Stay Right** defines automation, policy enforcement, and monitoring to ensure that projects remain compliant with standards.
- **Get Right** allows us to inventory our estate to understand the current state of compliance and identify areas that require focus to drive to compliance.

All six engineering pillars in the Secure Future Initiative include defined standards and the goal for each of those standards to be complete which means achieving 100% adoption of, or compliance with, that standard. The issuance of a standard does not mean we are immediately compliant. It means that we are driving towards 100%. In many cases we will never achieve 100% given the body of work to complete will change as we make progress towards that goal. We prioritize the sequencing of standards based on risk assessment.

Engineering pillars

1. Protect identities and secrets

Microsoft is fortifying protections across every layer of our stack, from the identity infrastructure to integration layers for apps and services. By investing heavily in modern identity standards, we strive to heighten protection of apps and services through ongoing platform investments that continually raise the bar.

Key learning

Attackers are exploiting user authentication using password spray or phishing as well as token theft and replay techniques, applying these techniques across both user and service accounts to obtain initial footholds in networks. After their initial secret or credential acquisition, attackers will often exploit vulnerabilities or errors in implementation of non-standard and/or complex authentication protocols to move laterally and avoid detection. Finally, attackers often take advantage of their initial footholds or subsequent lateral movement to exfiltrate data or additional keys/credentials from target systems.

Key standards and progress

Protect token signing keys using hardware protection to prevent exfiltration

We have completed the hardware security module (HSM) based storage implementations for Microsoft Entra ID and Microsoft Account (MSA) access token signing keys in our public and US government clouds, as well as Active Directory Federation Services (ADFS) token signing keys across all our environments.

Automatically rotate token signing keys, with no human interaction to prevent mishandling

We have completed the work to deliver automated rotation for Microsoft Entra ID and Microsoft Account (MSA) application access token signing keys without any human interaction in our public and US government clouds. All current Microsoft Entra ID and Microsoft Account (MSA) access token signing keys in public and US government clouds were established within the newly implemented hardware security module (HSM) based storage system.

Remove credentials handling in user account bootstrap and recovery processes to prevent credential leaks

To enhance our internal employee authentication procedures, we have implemented video-based user verification for 95% of Microsoft internal productivity environment users based on the NIST standards for mid-assurance identity proofing (NIST SP 800-63-4). This solution helps to verify a user's identity, including remote employees, before granting them access to corporate resources, ensuring credentials are securely transmitted.

Enforce use of phishing-resistant user credentials to prevent account compromise

We have completed adoption and enforcement in our production environment for phishing-resistant credentials and are in broad adoption across all users in our productivity environment.

Use system-managed credentials for service-to-service authentication to prevent mishandling and leaks

We are in broad adoption of Azure Managed Identity for service to service (S2S) authentication for Microsoft Entra ID applications and Azure resources across all environments, which eliminates a broad class of application credentials that require manual management and associated risks.

As part of our ongoing data security governance actions in our productivity environment, we have enabled Microsoft Purview features to block sharing or restrict access or exfiltration of sensitive information such as passwords, secrets, and keys that would enable an attacker to extract and reuse that information in future attacks.

Implement authentication protocols in common implementations and libraries to avoid implementation errors

We have completed the implementation of Microsoft Authentication Library (MSAL) across core Office apps across all platforms (iOS, Linux, Windows, MacOS). We are in broad adoption of our common Identity SDKs across all services at Microsoft. Today, over 73% of tokens issued by Microsoft Entra ID for Microsoft apps are validated using one standardized implementation.

Protect identity tokens with validation to detect forged tokens

We have completed the work to extend the standardized authentication token logging within our standard identity libraries and utilized this additional telemetry from the services that have adopted those updates to add token forgery detections using proprietary data in security tokens. This is currently in limited adoption and will be scaled for all services as part of our standard protocols and libraries investments.

2. Protect tenants and isolate production systems

To better protect all Microsoft tenants and production environments, it is crucial to implement consistent, best-in-class security practices and maintain strict isolation. This approach minimizes the impact of potential threats by reducing the attack surface and limiting the window of opportunity for lateral movement.

Key learning

In recent years, cyberattacks have escalated. Attackers are increasingly using gaps in the security posture, and in peripheral areas of systems, to establish a foothold and then move laterally to achieve objectives. It is essential in a modern enterprise and cloud environment to have comprehensive, consistent, strictly enforced security baselines to deny a foothold to threat actors and robust isolation boundaries to protect against lateral movement in case of a breach.

Key standards and progress

Apply governance processes on creation and lifecycle of Microsoft Entra ID tenants

Threat actors often look for a foothold in legacy systems knowing that such systems are less likely to be kept up to date with modern security standards. To control the new tenants used by employees for test and experimentation, we implemented a new system to streamline the creation of tenants with secure defaults and enforce strict lifetime management. We have also eliminated 5.75 million tenants, drastically reducing the potential attack surface.

Remove resources managed by Azure Service Management (ASM) API

We have removed over 440,000 resources which were being managed by the legacy Azure Service Management (ASM) API system.

Manage Microsoft Entra ID applications to a high, consistent security baseline to protect resources

We completed a full iteration of lifecycle management for all of our production and productivity tenants which eliminated over 730,000 unused apps. We have defined a standard for patterns of access for multi-tenant Microsoft Entra ID applications which have been repeatedly targeted by threat actors for lateral movement. We are in broad adoption of this standard across all production and productivity tenants.

Maintain inventory and ownership of all Microsoft Entra ID tenants and applications for effective security investigation and response

We have completed revising our internal system for emergency response to scale to the thousands of applications we have. We are backfilling data into it across all production and productivity tenants. So far, we have backfilled 23,000 apps.

Isolate credentials and secrets within security boundaries to prevent lateral movement

We have added controls that isolate application credentials within desired security/tenant boundaries to prevent movement across those boundaries and have applied those controls to over 110,000 certificate registrations. To avoid secrets moving across security boundaries, we have completed a program to restrict access to production environment crash dumps.

Use Just-in-Time (JIT) and Just-Enough-Access (JEA) for privileged administration roles to limit blast radius of compromised accounts

We created a system to do automated detection of persistent (as opposed to transient) access to production resources and when possible, automate cleanup or initiate manual investigation.

Enforce device compliance strictly to protect against and limit impact of device compromise on user identity

We eliminated several classes of tools and business process blockers allowing stricter enforcement of device security compliance standards affecting user access for over 75,000 users. Over 15,000 new production-ready, locked-down devices were distributed in the last three months alone.

3. Protect networks

The protect networks pillar focuses on safeguarding the Microsoft network infrastructure and the networks of first-party services, while also enabling third parties to do the same. This is achieved by applying network security principles such as isolation, traffic flow identification, monitoring, and implementing least privilege.

To improve security hygiene and hardening, we onboard all physical assets on the production network to a central inventory system which enriches asset inventory with ownership and firmware compliance tracking. By applying network isolation and micro-segmentation, we enforce service tags on all first party services and opt out of default outbound to explicitly identify the owner of any traffic in the Microsoft network. Each service applies the principle of least privilege and creates a security perimeter using mechanisms like Private Link, Virtual Network Service endpoints, and Network Security Perimeter. For services exposing endpoints or ports to third parties, multiple layers of defense and best practices in perimeter protection are applied.

Key learning

By protecting Microsoft production networks and isolating Microsoft and customer resources, we increase segmentation between operating environments, which prevents lateral movement within a system and provides secondary intrusion defense.

Key standards and progress

Track and maintain complete inventory of network devices to ensure vulnerabilities are managed and devices are configured to baseline

Over 99% of physical assets, infrastructure, and access controls on the production network are recorded in a central inventory system, which enriches asset inventory with ownership and firmware compliance tracking. All physical devices are monitored for hygiene of credentials, firmware updates, and access control lists. Reviews of network topology and routing graphs allow for greater understanding and defense of network terrain.

Apply uniform perimeter controls and micro-segmentation within the perimeter to limit blast radius and lateral movement

We are enforcing service tags on all Microsoft services and opt out of default outbound so we can identify the owner of any traffic flowing in the Microsoft network. Additionally, every service will apply the least privilege and create a security perimeter for their resources. All infrastructure services have firewall policy enforcement to simplify reduction of the attack surface. Additionally, virtual networks with backend connectivity are restricted to the least privilege access and subject to complete security reviews to reduce lateral movement from consumer and commercial workloads into infrastructure layers. Service perimeters are protected using multiple Azure Virtual Networking mechanisms, including Network Security Groups, Network Manager Admin Rules, Private Link, Service Endpoints, and Network Security Perimeter. This contains all resource access within a service and constrains access between different services. If a service is customer-facing, we use multiple layers of defense applying best practices in perimeter protection for the internet-exposed endpoint.

Centrally configure network policies to ensure new deployments start right with network perimeter by default

We focus on enabling customers to successfully deploy their services in a secure fashion and to make their networks secure by default. Thus far, platform capabilities have been expanded in the areas of Admin Rules which allow organization administrators to centrally manage perimeter isolation policy and Network Security Perimeter, which eases the network isolation for PaaS resources such as Storage, SQL, Cosmos DB, and Key Vault.

4. Protect engineering systems

The goal of the protect engineering systems pillar is to protect software assets. Given the adversarial threat landscape, continuously improving code security through governance of the software supply chain and engineering systems infrastructure is essential. This approach helps us stay ahead of potential vulnerabilities tied to emerging technologies, making our software more resilient to new threats.

We are now tracking and taking inventory for the majority of software assets used in our production environments, facilitating rapid response and remediation while maintaining compliance with secure standards. We also apply Zero Trust and least privilege policies to secure access to our source code and engineering systems infrastructure and help ensure only authorized personnel have access to critical resources. Microsoft incorporates state-of-the-art security checks that aim to continuously eliminate attack surface areas and enhance resilience against emerging threats in its production environments. Work under SFI seeks to ensure that engineering and test environments are isolated, build and release environments are centrally managed, and our supply chain and open-source usage are well governed.

Key learning

Our engineering systems are the foundation upon which all our products are built, making them a prime target for threat actors attempting to infiltrate our systems and our customers' environments. In recent attacks, we’ve seen threat actors exploit the software supply-chain through both code exploits and social engineering. We then see them attempt to exfiltrate source code to find secrets and vulnerabilities in source to be used immediately or stored to use at a later date. Threat actors then attempt to use developer and engineering system credentials to move laterally to other systems.

Key standards and progress

Track and maintain an inventory of all software assets to ensure consistent application of policies

We are now tracking and maintaining inventory and ownership for a majority of software assets in our production environments.

Apply policies to block check in of secrets in code repositories to prevent leaks and replay of credentials

We have rolled out policy enforcement to detect and eliminate secrets in our codebase and prevent new secrets from being checked in via push protection.

Enforce proof-of-presence checks to ensure only authorized code is merged into production branches

We have implemented proof-of-presence checks for critical chokepoints in our software development code flow.

Limit lifetime of derived credentials and minimize membership in privileged groups to limit blast radius of compromised accounts

We've slimmed down Personal Access Token lifespan to seven days, disabled SSH access for all Microsoft internal engineering repos, and have significantly reduced the number of elevated roles with access to our engineering systems. We removed persistent admin access for Project Collection Admins (PCAs) and Project Admins (PAs) and are reducing memberships for all other Azure DevOps roles like repo contributors, readers, feed owners, etc. to align with the principle of least privilege access. We have also initiated user access reviews every 180 days to ensure that all access is still valid.

Use centrally governed pipeline templates to consistently protect all code deploying to production

85% of our production build pipelines for the commercial cloud are now using centrally governed pipeline templates, making builds more consistent, efficient, and trustworthy.

Isolate build, development, and test environments to prevent lateral movement between environments

We are making progress towards build, development and test isolation through network and tenant isolation allowing us to have consistent and secure CI/CD processes.

5. Monitor and detect threats

The monitor and detect threats pillar focuses on ensuring that all assets within Microsoft production infrastructure and services are emitting security logs in a standardized format that are accessible from a centralized data system for both effective threat hunting/investigation and monitoring purposes. This pillar also emphasizes the development of robust detection capabilities and processes to rapidly identify and respond to any anomalous access, behavior, and configuration.

Key learning

Recent attacks and internal studies have reinforced the importance of a comprehensive—and up to date—asset inventory for effective investigation and monitoring. Each asset must emit standardized logs through centrally managed agents to ensure proper telemetry collection and retention. Easy authorized access to security logs for both internal teams and customers is crucial for efficient forensics. Logs must be available in a centralized data system for threat hunters and investigation teams. Providing timely security logs to customers enables their own investigations and detections. To stay ahead of threats, we must build detections using advanced analytics, machine learning, and threat intelligence to identify malicious activity.

Key standards and progress

Validate all infrastructure in inventory is emitting sufficient telemetry to support effective security investigation

The majority of Microsoft production resources and devices on the backend networks in our inventory are emitting security logs. Over 99% of network devices are now enabled with centralized security log collection and configured to retain for two years.

Implement service-level security audit logging in standard libraries to ensure all required data is available for security investigation

The majority of Microsoft services are now adopting standard libraries for security audit logs to ensure relevant telemetries are emitted.

Centrally enforce security log retention period to ensure logs are available to support security investigations over time

We are in progress of centrally enforcing a minimum of two-year retention period for all Microsoft production infrastructure and services. For instance, we have already established central management and a two-year retention period for identity infrastructure security audit logs, encompassing all security audit events throughout the lifecycle of current signing keys. This enables us to conduct more thorough security investigations.

Continue to add effective detections for known tactics, techniques, and procedures (TTPs) to detect threat actor and red team simulations and drills

We are developing detections based on top TTPs identified through recent security events and validating them through continuous attack campaigns and simulations. We have added paging alerts to notify of any interaction with signing key systems, new detections for anomalous app behavior including anomalous authentication patterns, and detections for anomalous authentication to critical resource types (e.g., storage, key vault, graph) across production tenants.

Provide expanded security logs to customers to support their security investigations and enhance visibility

We have made Microsoft 365 (M365) audit logs available to all customers, eliminating the previous E5 license requirement as part of the Microsoft Purview Audit (Standard). Additionally, we have enabled more M365 audit logs through Microsoft Purview. Furthermore, the default free-retention period for M365 audit logs has been extended from 90 days to 180 days.

6. Accelerate response and remediation

Our mission is to protect customers, Microsoft, and communities from current and emerging security and privacy threats. This is achieved by partnering with internal and external researchers to identify and fix security vulnerabilities in products and services that could pose a threat to customers.

To prevent the exploitation of vulnerabilities discovered by external and internal entities, Microsoft focuses on comprehensive and timely remediation. This approach reduces the time that customers are at risk from known vulnerabilities and ensures continuity in operations. The threats posed by nation-state actors are significant, impacting national security, economic stability, political influence, and data privacy.

Key learning

A key learning that helped us improve time to mitigate (TTM) was to adopt standard engineering mechanisms, like the Microsoft internal incident management system. We now use this tool to work on security cases with engineering teams across Microsoft. Additionally, we received feedback from engineering teams to have Microsoft Security Response Center (MSRC) work reflected in the same dashboards and tracking systems used by other high priority engineering work. Another learning was proactively providing signals about cases at risk of missing TTM deadlines, for which we published and communicated org-level scorecards. We also tracked the reasons for cases missing TTM deadlines and found that the number one reason is the delay in production deployments.

Key standards and progress

Reduce time to mitigate (TTM) for critical cloud vulnerabilities with accelerated response time

We saw improvements during this period as a result of working with multiple engineering teams to improve processes and response times.

Transparently communicate vulnerability mitigations to accelerate broad adoption

Common vulnerability and exposures (or CVEs) are industry-standard, unique identifiers that allow security professionals to assess information about security vulnerabilities across multiple sources using a common ID. Since 1999, Microsoft has been assigning CVEs to vulnerabilities where customers need to take action, and now we have begun publishing CVEs for critical cloud vulnerabilities whether user action is required or not. We have begun to enrich this data with root cause information and impacted products using industry standards. This helps the entire industry focus on eliminating whole classes of vulnerabilities.

Apply consistent standards for effective and accurate communication on security incidents

To improve the accuracy, effectiveness, transparency, and velocity of public messaging and customer engagement during and after a security incident, we have created a new Customer Security Management Office (CSMO). This new office will work in partnership with teams across the company, ensuring that our public messaging and customer engagement are aligned with our security goals. The establishment of the CSMO is a concrete step in supporting transparency, demonstrating our commitment to enhancing customer engagement and communication.

Appendix: CSRB report mapping

The table below maps progress in this report to the Cyber Safety Review Board (CSRB) recommendations made in March 2024 that apply to Microsoft and/or all cloud service providers (CSPs). Like SFI pillars and standards, our work to address these recommendations will be ongoing and status may remain in progress for some time, given the breadth or complexity of certain recommendations.

Recommendation category and CSRB number		Applicable sections and standards	Status
Microsoft corporate security culture	**1**	Page 2: Executive summary Pages 5–6: Culture and governance	Complete
	2	Pages 5–6: Culture and governance	Complete
	3	Pages 5–6: Culture and governance	In progress
CSP cybersecurity practices	**6**	Pages 12–13: Protect identities and secrets • Protect token signing keys using hardware protection to prevent exfiltration • Automatically rotate token signing keys, with no human interaction to prevent mishandling • Implement authentication protocols in common implementations and libraries to avoid implementation errors • Protect identity tokens with validation to detect forged tokens	In progress
	9	Updates provided as part of original CSRB response. As noted in pages 5–6: Culture and governance a Deputy CISO has also been appointed for Core Systems and Mergers and Acquisitions	In progress
Audit logging norms	**4**	Page 20–21: Monitor and detect threats • Centrally enforce security log retention period to ensure logs are available to support security investigations over time • Provide expanded security logs to customers to support their security investigations and enhance visibility • Implement service level security audit logging in standard libraries to ensure all required data is available for security investigation	In progress

Recommendation category and CSRB number		Applicable sections and standards	Status
Audit logging norms (cont.)	**5**	Pages 20–21: Monitor and detect threats • Centrally enforce security log retention period to ensure logs are available to support security investigations over time • Provide expanded security logs to customers to support their security investigations and enhance visibility • Validate all infrastructure in inventory is emitting sufficient telemetry to support effective security investigation • Continue to add effective detections for known tactics, techniques, and procedures (TTPs) to detect threat actor and Red Team simulations and drills	In progress
	10	Pages 20–21: Monitor and detect threats • Centrally enforce security log retention period to ensure logs are available to support security investigations over time • Provide expanded security logs to customers to support their security investigations and enhance visibility	In progress
Digital identity standards and guidance	**11**	Work is ongoing. No specific updates provided in this report.	In progress
	13	Work is ongoing. No specific updates provided in this report.	In progress
CSP transparency	**14-16**	Pages 22–23: Accelerate response and remediation • Apply consistent standards for effective and accurate communication on security incidents	In progress
	17	Pages 22–23: Accelerate response and remediation • Transparently communicate vulnerability mitigations to accelerate broad adoption	In progress
Victim notification process	**18**	Eager to collaborate	
	19	Pages 22–23: Accelerate response and remediation • Apply consistent standards for effective and accurate communication on security incidents	In progress
	20	Eager to collaborate	

Note: CSRB recommendations 7, 8, 12, and 21–25 are not applicable to Microsoft or CSPs.