Microsoft Security

Evolving Threats Require Evolved Security

Securing tomorrow requires proactive AI solutions today

The Secure Future Initiative

Security is a state of constant evolution. Learn, adapt, and embrace a Zero Trust approach, or be left vulnerable—it's that simple. That's why we developed the Secure Future Initiative (SFI), a multiyear commitment by Microsoft to ensure that we continuously meet the highest possible standards for security. With SFI as our map, compass, and GPS, Microsoft is wholly committed to the idea that the protection of our company, products, and customers always must be our primary focus.

SFI, however, is more than an internal shift in how we view our work. It's Microsoft leading the way toward a safer, more secure future for our customers, partners, and the broader community. With each step in our progress, we provide customer-centric guidance and actionable learnings so everyone can develop smarter security strategies suited to their own organizations.

The state of security

78 trillion — **threat signals**, across various platforms, are tracked and analyzed by Microsoft security experts every day.[1]

of cybersecurity breaches are caused by human error, making employee training essential in cyberattack prevention.[2]

1,500 — **unique threat groups**, including over 600 nation-state actor groups, are currently being tracked by Microsoft.[1]

Why SFI? Because traditional thinking on security isn't enough

> Security is a team sport and is best realized when organizational boundaries are overcome."
>
> – Charlie Bell, Executive Vice President, Microsoft Security

There's no one-size-fits-all approach to security, but it must be a proactive endeavor, not a reactive one. That's why SFI is about securing our present with an eye on our future—a future that's certain to be defined by a changing threat landscape. A security-first mindset and a desire to share Microsoft's learnings and best practices drove our creation of the **six SFI pillars:**

1 Protect identities and secrets

Enforce best-in-class standards across all identity and secrets infrastructure, securing user and application authentication and authorization.

2 Protect tenants and isolate systems

Use consistent, best-in-class security and strict isolation with all tenants and production environments to minimize breadth of impact.

3 Protect networks

Safeguard Microsoft production networks and implement network isolation of Microsoft and customer resources.

4 Protect engineering systems

Shield software assets and continuously improve code security through governance of the engineering systems infrastructure and software supply chain.

5 Monitor and detect cyberthreats

Provide comprehensive coverage and automatic detection of cyberthreats for Microsoft production infrastructure and services.

6 Accelerate response and remediation

Prevent exploitation of vulnerabilities discovered by internal and external entities through comprehensive and timely remediation.

While the SFI pillars are unique to Microsoft, we have uncovered best practices and formulated guidance aligned to the pillars as we've worked to implement SFI across our products and services. We are committed to sharing those learnings and practices with our customers to help them identify their own security needs and goals, now and in the future.

SFI principles

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.

Shift to a security-first mindset

Everything is changing quickly in terms of how we work. That's why a secure future is crucial for Microsoft, across our entire enterprise—and it should be for your organization too.

Explore the Secure Future Initiative (SFI) in greater depth

Discover new security strategies for the age of AI

Additional reading:

- A superior strategy for end-to-end security
- Security is a journey, not a destination

[1] "Microsoft Digital Defense Report 2024", Microsoft, October, 2024

[2] "Psychology of Human Error", Tessian, 2022