

# Six ways to protect against cloud security threats

Proactive strategies to keep your organization safe in an evolving threat landscape

The cloud stores vast amounts of critical data, making it a prime target for malicious actors seeking to disrupt business.

→ The average multicloud estate has 351 exploitable attack paths leading to high-value assets<sup>1</sup>

In this brief, explore the most significant security risks facing cloud environments today and discover six steps your organization can take to protect its digital assets from threats.

Cyberattacks are becoming more frequent and costly.

58%  
Phishing attacks grew by 58% in 2023, marking it as one of the fastest-growing cyberthreats<sup>3</sup>

≤4,500  
A rise in network DDoS attacks began in mid-March 2024, reaching 4,500 attacks per day in June<sup>2</sup>

600M  
Microsoft Entra data shows more than 600 million identity cyberattacks per day in 2024<sup>2</sup>

80%  
80% of organizations were found to have attack paths exposing critical assets in June 2024<sup>2</sup>

\$90B+  
Annual losses from global e-commerce payment fraud to surpass \$90 billion by 2028<sup>2</sup>

## Evolving threats to cloud security

Attackers range from individual hackers and organized cybercriminal groups to nation-state actors. By exploiting vulnerabilities in an organization's security posture, they can steal sensitive data, disrupt business operations, or gain a strategic advantage.

### Nation-state threats

Nation-state cyberthreats are highly sophisticated and well-resourced, using advanced tactics such as zero-day exploits, spear phishing, and malware to infiltrate systems. They often exploit software, cloud services, and supply chain vulnerabilities, targeting weak points that can give them access to valuable data or disrupt key systems. The most targeted sectors include IT, Education and Research, and Governments.<sup>2</sup>

### Cloud misconfiguration attacks

Hackers can gain access to cloud-based data and services through cloud misconfigurations, including failure to change default settings, unrestricted ports, and unsecured backups.

### Cloud Account Takeover (ATO)

ATO attacks are rising sharply, targeting accounts from banking to social media and gaming. Cybercriminals use phishing and automated bots to amplify their efforts.

### Distributed Denial of Service (DDoS)

DDoS attacks are becoming more sophisticated and harder to detect, often masked as legitimate traffic.

## Building a more resilient security posture: Six best practices

Here are some best practices for protecting your cloud workloads, along with tools to help you put them into action.

### 1. Prioritize security from day one

Setting up frameworks and securing parameters early in the process prevents vulnerabilities that might arise when retrofitting security measures later. By embedding security into the foundation of your networking and applications with [best practices](#), you create a proactive defense strategy that minimizes risks and strengthens your resilience against emerging threats. This approach aligns with initiatives like the [Secure Future Initiative](#), which prioritizes security above all else, establishing robust governance and engineering frameworks that help manage cybersecurity risk at scale.

**Dive deeper:** Learn more about building secure workloads using the [Azure Well-Architected Framework](#).

### 2. Unify your security management tools

A fragmented approach to security tools creates gaps, leaving critical workloads vulnerable. Using a [cloud-native application protection platform \(CNAPP\)](#) helps unify security management tools into a single platform, providing end-to-end visibility and control over multicloud and hybrid environments. This approach helps to eliminate gaps, ensure all assets are protected, and enable a faster, more coordinated response to threats. Consolidation isn't just efficient—it's essential for maintaining a robust and adaptive security posture.

**Dive deeper:** Find out how [Microsoft Sentinel](#) helps you modernize your security strategy and stay ahead of evolving threats.

### 3. Strengthen identity and access controls

Poor identity and access management can open the door for bad actors to infiltrate your cloud accounts. Enforcing [phishing-resistant multifactor authentication](#) and regularly reviewing access permissions are crucial to preventing unauthorized access. A robust identity management strategy protects your sensitive data while ensuring legitimate users can access what they need securely.

**Dive deeper:** Learn more about managing access and protecting against identity threats with [Microsoft Entra ID](#).

### 4. Encrypt data at every stage

Data is one of a business's most valuable assets—and a prime target for cybercriminals. Encrypting data at rest, in transit, and during use can help ensure its confidentiality and integrity. At the heart of encryption lies cryptographic keys, which enable secure data encryption and decryption. Tools like [Azure Key Vault](#) plays a pivotal role in managing these cryptographic keys, ensuring robust protection for sensitive data and preventing unauthorized access and data loss. For teams building data-hungry AI solutions, it's critical to keep data confidential among participants in production environments.

**Dive deeper:** Learn more about protecting data in use with [Azure confidential computing](#).

### 5. Fortify your network defenses

The network serves as the backbone of your cloud infrastructure. A breach at the network level—whether within your environment or a provider's—can give threat actors access to compute resources, storage, and more. Proactively defending your network with [advanced firewalls](#), [always-on monitoring DDoS protection](#), and secure configurations ensures workloads remain protected.

**Dive deeper:** Reference the [Microsoft cloud security benchmark](#) to see if your network remains aligned with the latest security standards and best practices.

### 6. Design secure applications from the ground up

Creating secure applications from the start is far easier and more effective than patching vulnerabilities later. To build secure apps from the ground up, developers and security teams must be able to collaborate closely and test solutions in controlled environments.

Identify and address potential risks before deployment using tools like [Azure Dev/Test Labs](#) to create consistent, controlled environments for development and testing. Meanwhile, [GitHub Advanced Security](#) helps developers and security teams work to keep vulnerabilities out of code.

**Dive deeper:** Learn more about strengthening your threat protection from code to cloud with [Microsoft Defender for Cloud](#).

## Partner up for protection

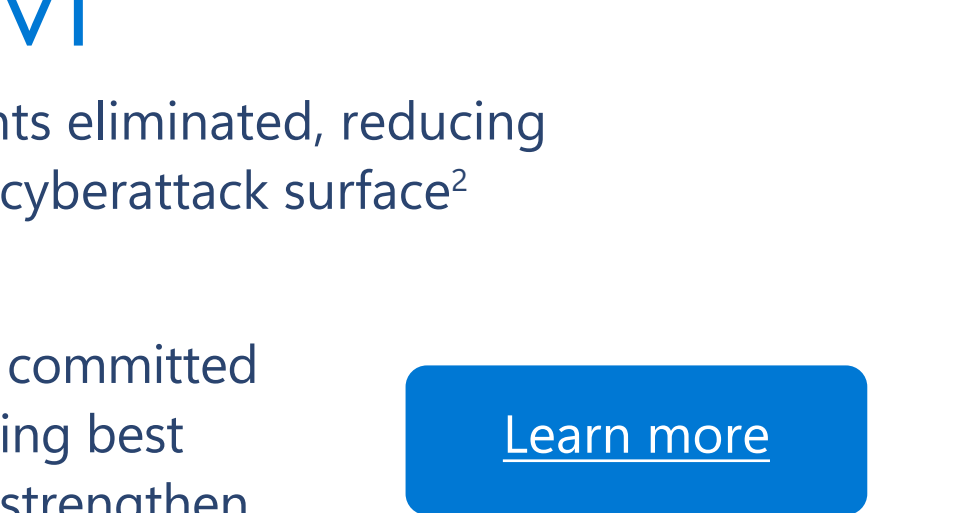
While perfect security is impossible to guarantee, adopting a **shared responsibility model** with a trusted cloud provider can greatly enhance your protection. This approach divides responsibilities into three key areas: what the **organization** handles independently, what the **cloud provider** manages, and the tasks they address **together**.

### Shared responsibility model

The **cloud provider** is responsible for:



The **organization** is responsible for:



### Shared responsibilities

The cloud provider offers the capabilities and the organization is responsible for enabling and using them.



## Questions to ask your cloud provider to ensure AI-ready security

Make sure your cloud platform partner checks all the boxes. **Start by asking these key questions:**

- How focused on security are you when developing the platform?
- How do you secure your data centers?
- How is your supply chain – both physical and software – secured?
- What security features are built into the platform?
- Are there any security features required to get through a 3rd party?
- What level of security investment and headcount does your company have?
- What guidance is available to help me take the right steps for security?
- How transparent are you when security incidents occur?

## Secure your future with Azure's AI-first, end-to-end security platform

Azure ensures security through multiple layers: a **state-of-the-art infrastructure** built to withstand modern threats, a **secure physical and software supply chain**, and a **protected Azure network** that prevents unauthorized access. Its **platform security capabilities** help detect and mitigate risks, while resources are available to guide you in strengthening your cloud security posture.

From chip-level protection to advanced resource management and identity verification, Azure delivers security-first solutions such as automated threat detection, always-on data encryption, and a zero-trust architecture. Collaboration with security organizations and government bodies worldwide ensures Azure stays ahead of cyberthreats and evolving regulations.

78T+ signals analyzed every 24 hours<sup>2</sup> | 3,500 Azure DDoS Protection mitigated a peak of 3,500 attacks daily in late 2023<sup>4</sup>

### Transparency, guidance, and expertise

**Microsoft Secure Future Initiative (SFI)** is a multiyear initiative to evolve the way we design, build, test, and operate our products and services to achieve the highest possible standards for security. SFI has mobilized the equivalent of 34,000 full-time engineers, making it the largest cybersecurity engineering initiative in the history of digital technology.<sup>2</sup>

730k

SFI non-compliant apps eliminated<sup>2</sup>

5.75M

inactive tenants eliminated, reducing the potential cyberattack surface<sup>2</sup>

As part of the initiative, Microsoft has voluntarily committed to the [CISA Secure by Design Pledge](#), implementing best practices and repeatable SFI standards that help strengthen developer productivity and accelerate progress.

[Learn more](#)

## Get started: Strengthen your security posture with Azure

Read executive insights on cloud security, foundational AI, data transformation, and more.  
[Explore Azure Innovation Insights](#)

Browse more best practices, get expert guidance, and ensure your cloud and AI success with enhanced security  
[Discover Azure Essentials](#)

Learn why Azure is a leader in cloud security and how Azure keeps your data, apps, compute, and networking resources secure.  
[Learn more](#)

<sup>1</sup> Microsoft 2024 State of Multicloud Security Report

<sup>2</sup> Microsoft Digital Defense Report

<sup>3</sup> Top 15 Phishing Stats to Know in 2024 | Trend Micro News

<sup>4</sup> Unwrapping the 2023 holiday season: A deep dive into Azure's DDoS attack landscape