Microsoft Azure

Five Best Practices for Cloud Security

Cloud security is a fundamentally new landscape for many companies. While many of the security principles remain the same as on-premises, the implementation is often very different. This overview provides a snapshot of five best practices for cloud security: identity and access control, security posture management, apps and data security, threat protection, and network security.

01 Strengthen access control

Traditional security practices are not enough to defend against modern security attacks. Therefore, the modern security practice is to "assume breach": protect as though the attacker has breached the network perimeter. Today, users work from many locations with multiple devices and apps. The only constant is user identity, which is why it is the new security control plane.

Institute multifactor authentication

Provide another layer of security by requiring two or more of the following authentication methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

Take advantage of conditional access

Master the balance between security and productivity by factoring *how* a resource is accessed into an access control decision. Implement automated access control decisions for accessing your cloud apps that are based on conditions.

Operate in a zero-trust model

Verify the identity of everything and anything trying to authenticate or connect before granting access.

02 Improve security posture

With more and more recommendations and security vulnerabilities identified, it is harder to triage and prioritize response. Make sure you have the tools you need to assess your current environments and assets and identify potential security issues.

Improve your current posture

Use a tool like Secure Score in Azure Security Center to understand and improve your security posture by implementing best practices.

Educate stakeholders

Share progress on your secure score with stakeholders to demonstrate the value that you are providing to the organization as you improve organizational security.

Collaborate with your DevOps team on policies

To get out of reactive mode, you must work with your DevOps teams up front to apply key security policies at the beginning of the engineering cycle as secure DevOps.

03 Secure apps and data

Protect data, apps, and infrastructure through a layered, defense-in-depth strategy across identity, data, hosts, and networks.

Encryption

Encrypt data at rest and in transit. Consider encrypting data at use with confidential computing technologies.

Follow security best practices

Ensure your open source dependencies do not have vulnerabilities. Additionally, train your developers in security best practices such as Security Development Lifecycle (SDL).

Share the responsibility

When a company operates primarily on premises, it owns the whole stack and is responsible for its own security. Depending on how you use the cloud, your responsibilities change, with some responsibilities moving to your cloud provider.

- IaaS: for applications running in virtual machines, more of the burden is on the customer to ensure that both the application and OS are secure.
- PaaS: as you move to cloud-native PaaS, cloud providers like Microsoft will take more of the security responsibility at the OS level itself.
- SaaS: at the SaaS level, more responsibility shifts away from the customer. See the shared responsibility model.

04 Mitigate threats

Operational security posture—protect, detect, and respond—should be informed by unparalleled security intelligence to identify rapidly evolving threats early so you can respond quickly.

Enable detection for all resource types

Ensure threat detection is enabled for virtual machines, databases, storage, and IoT. Azure Security Center has built-in threat detection that supports all Azure resource types.

Integrate threat intelligence

Use a cloud provider that integrates threat intelligence, providing the necessary context, relevance, and prioritization for you to make faster, better, and more proactive decisions.

Modernize your security information and event management (SIEM)

Consider a cloud-native SIEM that scales with your needs, uses AI to reduce noise and requires no infrastructure.

05 Protect the network

We're in a time of transformation for network security. As the landscape changes, your security solutions must meet the challenges of the evolving threat landscape and make it more difficult for attackers to exploit networks.

Keep strong firewall protection

Setting up your firewall is still important, even with identity and access management. Controls need to be in place to protect the perimeter, detect hostile activity, and build your response. A web application firewall (WAF) protects web apps from common exploits like SQL injection and cross-site scripting.

Enable Distributed Denial of Service (DDoS) Protection

Protect web assets and networks from malicious traffic targeting application and network layers, to maintain availability and performance, while containing operating costs.

Create a micro-segmented network

A flat network makes it easier for attackers to move laterally. Familiarize yourself with concepts like virtual networking, subnet provisioning, and IP addressing. Use micro-segmentation, and embrace a whole new concept of micro perimeters to support zero trust networking.

What's next?

Are you looking to strengthen the security of your cloud workloads?

Learn more about security on Azure

Contact us