

# Five Best Practices for Cloud Security

Cloud security is a fundamentally new landscape for many companies. While many 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 management, security posture management, apps and data security, threat protection and network security.



Strengthen access control



Improve security posture



Secure apps and data



Mitigate threats



Protect the network

## 1 Strengthen access control

Traditional security measures are not enough to defend against modern security attacks. Today's best practice is to 'assume breach' and protect as though the attacker has breached the network perimeter. A Zero Trust approach that verifies and secures every identity, validates device health, enforces least-privilege access and captures and analyses telemetry is therefore a new security mandate.



### Institute multi-factor 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)



### Enforce Conditional Access policies

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

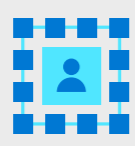


### Ensure least privilege access

Simplify access management in multi-cloud environments with unified cross-cloud visibility into all permissions and identities and automate least privilege policy enforcement consistently to protect your most sensitive cloud resources.

## 2 Improve your security posture

With the dynamic nature of the cloud and ever-growing landscape of workloads and other resources, it can be difficult to understand your company's security state in the cloud. Make sure you have the tools you need to assess your current environments, identify risks and mitigate them.



### Assess and strengthen your current posture

[Secure score](#) in Microsoft Defender for Cloud offers hundreds of out-of-the-box recommendations mapped to industry best practices and regulatory standards.



### Educate stakeholders

[Track your secure score progress](#) over time and create rich, interactive reports that you can share with key stakeholders to demonstrate how your security team is continually improving the organisation's cloud security posture.



### Collaborate with your DevOps team on policies

Involve your DevOps teams in your security strategy. Help them understand and implement key policies and deploy application security at the beginning of the development lifecycle.

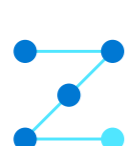
## 3 Secure apps and data

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



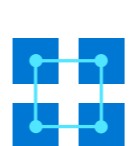
### Encryption

Encrypt data at rest and in transit, and consider also 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.

- Infrastructure-as-a-Service (IaaS): For applications running in virtual machines, more of the burden is on the IT organisation to ensure that both the application and OS are secure.
- Platform-as-a-Service (PaaS): As you move to cloud-native PaaS, cloud providers like Microsoft will take more of the security responsibility at the OS level.
- Software-as-a-Service (SaaS): At the SaaS level, more responsibility shifts away from the IT organisation. See the [shared responsibility model](#).

## 4 Defend against threats

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



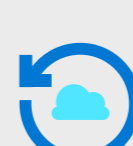
### Enable detection for all resource types

Ensure threat detection is enabled for virtual machines, containers, databases, storage, IoT and your other resources. Microsoft Defender for Cloud has built-in threat detection that supports all major Azure and AWS resource types.



### Integrate threat intelligence

Use a cloud provider that integrates threat intelligence and provides the necessary context, relevance and prioritisation 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.

## 5 Protect the network

The network security landscape is rapidly transforming. To keep pace with the 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. You need controls 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. Familiarise yourself with concepts like virtual networking, subnet provisioning and IP addressing. Use micro-segmentation and perimeter the concept of micro-perimeters to support zero-trust networking.

## What's next?

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

Get expert guidance through the [Azure Migration and Modernisation Programme](#)