Microsoft Azure

Five Best Practices for **Cloud Security**

Follow these best practices to strengthen your security posture while running Windows Server and SQL Server in the cloud.

Assume a Zero Trust stance

Instead of assuming safety behind the corporate firewall, operate under the assumption of a breach and rigorously verify every user and request. Zero Trust adapts to the complexities of remote workforces and helps safeguard systems, apps and assets regardless of their location.

Institute multi-factor authentication

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

Something you are
Like a fingerprint

Something you know
Like a password

Something you have
Like a phone

Consolidate your identity and access management (IAM) tools

Rather than relying on a patchwork of solutions, centralise your IAM solutions so your identity management professionals can work quickly to outpace potential attackers.

Automate least privileged access

Simplify access management in multi-cloud environments by automating least privilege policy enforcement to protect your most sensitive cloud resources without compromising productivity.

Enable code-to-cloud security

Using a cloud-native application protection platform – like Microsoft Defender for Cloud – helps safeguard cloud-based applications throughout the entire app lifecycle across multicloud and hybrid environments.

Assess your current security posture

Get your secure score to understand where your security gaps are. Use Defender to get actionable recommendations for reducing risk and enhancing your security posture.

Keep stakeholders in the loop

Track your secure score over time and create shareable, interactive reports to show stakeholders how your team continually improves your organisation's cloud security posture.

Embed security across the development lifecycle

Give your DevOps team a single pane of glass that provides full visibility of your security posture across continuous integration and delivery pipelines.

Activate cloud-native defences

Microsoft is the only public cloud provider with an integrated CNAPP in the cloud portal for defending hybrid and multicloud workloads.[3]

Secure apps and data to prepare for AI adoption

Use a layered defence strategy across identity, access, networks and hosts, and adapt your security strategy to include AI.

Encryption

Reduce the likelihood of attacks from the inside by encrypting sensitive data stored in your SQL Server database.

Build a secure IT foundation for AI advancement

Prepare to innovate with AI by securing your infrastructure against threats across hybrid and multicloud environments. Watch the on-demand webinar for practical tips and demos.

Share the responsibility

Security responsibilities change when you shift from on-premises to a cloud-first or hybrid environment. Find out which responsibilities can be moved from your organisation to your cloud provider.

Partner with a trusted cloud provider

34.7 B
identity threats blocked in one 12-month period

15,000+
partners in the Microsoft security ecosystem

100,000
cybercriminal domains removed to date[4]

Mitigate threats

Operational security posture – protect, detect and respond – should be informed by security intelligence that exposes malicious actions early and hastens your team's response to incidents..

Identify vulnerabilities

Use an integrated vulnerability assessment scanner to help remediate potential vulnerabilities in your SQL Servers on Virtual Machines, on-premises and hybrid environments.

Incorporate threat intelligence

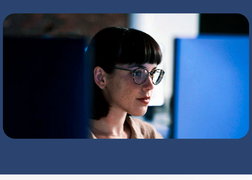
Use a threat modelling framework to generate a list of potential threats and identify means of reducing or eliminating those risks.

Consider a cloud-native security information and event management (SIEM)

Cloud-native SIEMs – like Microsoft Sentinel – offer a streamlined view of your data to help detect, investigate and respond to threats before they harm business operations.

Protect your network

Make it harder for attackers to exploit your networks by establishing multilayered network security across public, private and hybrid cloud networks.



Use a cloud-native network firewall

A cloud-native network firewall will let you inspect network traffic in real time and prevent the transmission of malware through hybrid connections.

Enable distributed denial-of-service (DDoS) protection

Enterprise-grade DDoS protection helps defend virtual networks and public IP endpoints from malicious traffic to ensure legitimate users don't lose access to their applications.

Disable lateral threat movement

Segmenting your network minimises the 'blast radius' when unauthorised users access to your data so they can't propagate across your network.

Secure legacy systems

Ensure your workloads are safe with the most up-to-date security upgrades.

Strengthen security for cloud and hybrid workloads

Get expert help and guidance on your cloud adoption journey through Azure Migrate and Modernize.

Learn more ›

[3] Microsoft Defender for Cloud provides CNAPP security | Microsoft Security Blog
[4] Microsoft Digital Defence Report 2022 Executive Summary