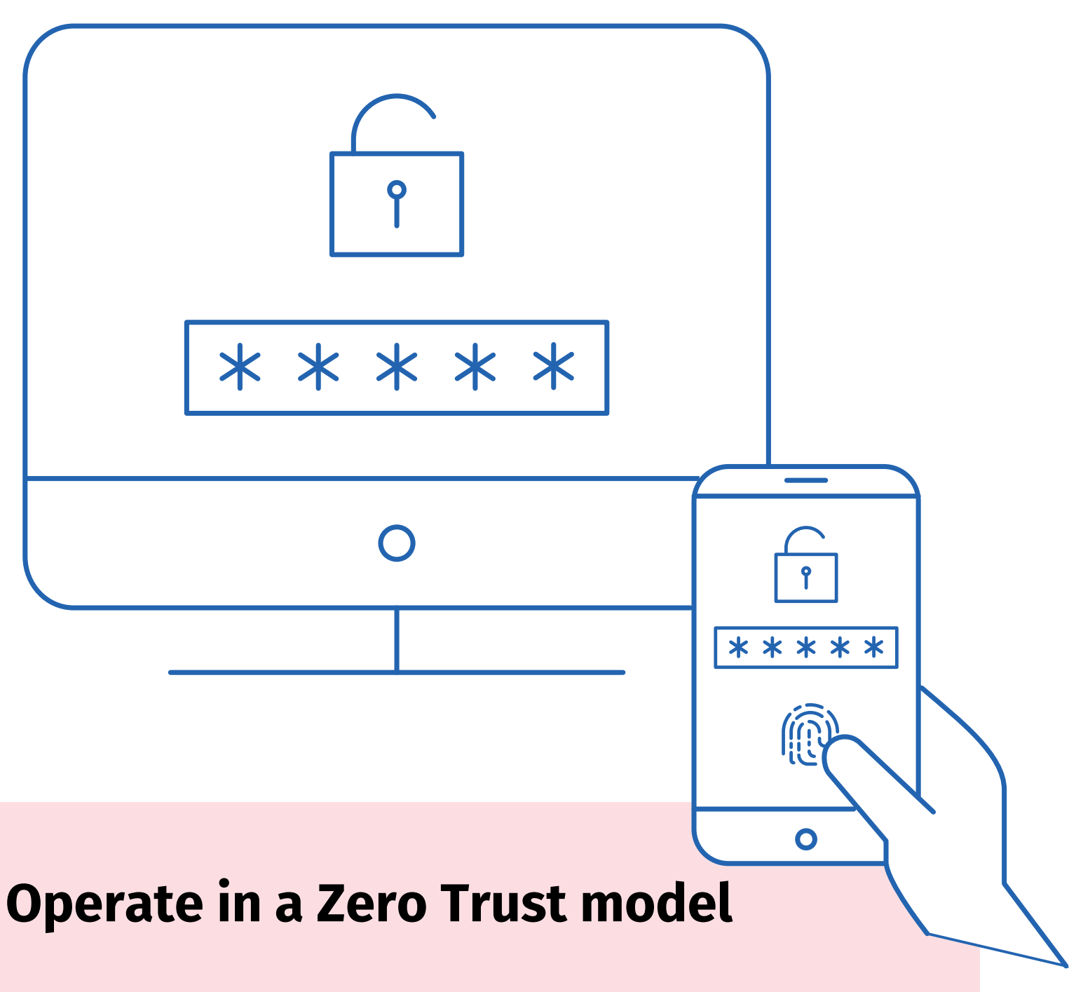
rackspace technology | Microsoft Azure

Five Best Practices for Cloud Security

- Strengthen access control
- Improve your security posture
- Secure applications and data
- Mitigate threats
- Protect the network

Cloud security is a fundamentally new landscape for many organisations. While many cloud security principles remain the same as on-premises, the implementation is often very different. And when it comes to cloud security, both the provider and the customer assume some important responsibilities. 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**.

1 Strengthen access control



Traditional security practices are often insufficient to defend against modern security attacks. Therefore, modern security practice is to “assume breach”: protect as if an attacker has already breached the network perimeter. Users today work from many locations and across a variety of devices and applications. 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 when making access-control decisions by considering how a resource is accessed. Automate access to cloud applications where you can using conditional access controls.

Operate in a Zero Trust model

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

2 Improve your security posture

As more recommendations and security vulnerabilities are identified, it becomes more difficult to triage and prioritise your responses. Make sure you have the necessary tools to assess your current environments and assets, as well as identify potential security issues.

Improve your current posture

Use a tool like Secure Score in Azure Security Centre 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 you bring to the organisation as you improve organisational security.

Collaborate with your DevOps team

Work with your DevOps teams early in the engineering cycle to develop and apply key security policies as secure DevOps.

3 Secure applications and data

Protect data, applications and infrastructure with a multi-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

Make sure your open-source dependencies are free of vulnerabilities. In addition, train your developers in security best practices such as Security Development Lifecycle (SDL).

Share the responsibility

When you operate primarily on-premises, your organisation owns the whole stack and is therefore responsible for its security. Your responsibilities change based on how you use the cloud, with some responsibilities moving to your cloud provider.

- **IaaS:** For applications running on virtual machines, it’s your responsibility to ensure that both the application and operating system are secure.
- **PaaS:** As you move to cloud-native PaaS, cloud providers like Microsoft will take more responsibility for the OS-level security themselves.
- **SaaS:** At the SaaS level, more responsibility shifts away from the you. See the shared responsibility model.

4 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

Be sure to enable threat detection for virtual machines, databases, storage and IoT. Microsoft Defender for Cloud has built-in threat detection that supports all Azure resource types.

Integrate threat intelligence

Use a cloud provider that integrates threat intelligence and provides the context, relevance and prioritisation you need to make faster, better and more proactive decisions.

Modernise 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

We’re in a transformative time for network security. As the landscape changes, your security solutions must meet the challenges of an evolving threat landscape.

Maintain your firewall protection

Even with today’s identity and access management tools, proper installation of your firewall remains essential. Set up controls to protect the perimeter, detect hostile activity and build your response. A web application firewall (WAF) protects web applications 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 such as virtual networking, subnet provisioning and IP addressing. Use micro-segmentation to take advantage of a whole new concept of micro-perimeters to support Zero Trust networking.

Ready to strengthen the security of your Azure workloads?

Our experts are ready to provide you with a customised threat and vulnerability analysis of your hybrid and multicloud environment. **Get started today**.

Learn more >

Cloud security is constantly evolving. Review your organisation's existing cloud security measures to see if there's more you can do now to increase your security posture and reduce risk. Consider these best practices a solid starting point to ensure a sound strategy that helps prevent your proprietary data from unnecessary and potentially costly exposure.

rackspace technology | Microsoft Azure