Microsoft Azure Security Best Practices

Microsoft Azure is the cornerstone of cloud infrastructure for many enterprises across the globe. Mission-critical workloads, ranging from distributed Kubernetes clusters to .NET applications to Software-as-a-service (SaaS) products, run on Azure. As a result, knowing the ins and outs of Azure security best practices is a must for enterprises that depend on Microsoft's cloud platform.

Here, we'll provide an overview on Azure security (/cyber-hub/cloud-security/what-is-microsoft-azure-security/), take an in-depth look at best practices for the Azure cloud, and discuss how Check Point can help you improve your overall Azure security posture.

Microsoft Azure Security Best Practices for 2021

Because there is such a wide variety of Azure services, no one-size-fits-all security "recipe" will ensure you've optimized your security posture. However, as you break down the different aspects of Azure to more specific categories, you'll discover actionable best practices you can implement. Let's look at those categories and the resulting Azure security best practices.

But First, the Prerequisites: The Shared Responsibility Model and Principle of Least Privilege

Before you dive into specific Azure security best practices, be sure you understand the basic security paradigm on the platform: Azure's shared responsibility model (https://pages.checkpoint.com/shared-responsibility-model-introduction.html).

In short, the shared responsibility model means Microsoft is responsible for security **of** the cloud, while you're responsible for security **in** the cloud. The demarcation point between the two varies depending on the specific product type. For example, with a SaaS app, Microsoft is responsible for operating system security. However, with an infrastructure-as-a-service (IaaS) product, you're responsible for operating system security. Understanding where that dividing line lies for your Azure infrastructure is a must.

Additionally, in all cases, you should follow the principle of **least privilege**. While *how* you implement the principle of least privilege will vary depending on your workloads and apps, the idea stays the same: grant users, devices, apps, and services only the access they need

and nothing more. For example, with an Azure database, as opposed to granting everyone read access to the entire database, you can and should use row-level security to restrict access down to database rows.

Azure security best practices checklist

With the prerequisites out of the way, let's dive into the checklist. We'll take a look at individual aspects of Azure and provide specific actionable items your team can audit against.

Encryption and data security

Data breaches are one of the biggest threats to your security posture. Therefore, getting your encryption and data security right is a must. This checklist will help you make sure you're on the right path, and applies to any area of Azure that consumes, transmits, or stores sensitive data.

- **Identify all sensitive information**. From an operations and compliance perspective, you must identify all the sensitive data transmitted or stored on your infrastructure. Doing so allows you to properly decide how to achieve adequate security and compliance.
- **Encrypt data at rest**. This one is data security 101. Use modern encryption protocols and secure data storage methods for all data at rest.
- **Encrypt data in transit**. Just like encrypting data at rest is a must, so is encrypting data in transit. Even if the data isn't traversing the Internet, encrypt it.
- **Have a backup and disaster recovery (DR) plan.** In the event you fall victim to ransomware or other malware, backups and a DR plan can make a world of difference. A robust backup and DR plan is a must-have for Azure security.
- **Use a key management solution**. Solutions like Azure Key Vault enable you to securely manage your keys, secrets, and certificates.
- **Harden your management workstations**. Accessing sensitive data from an insecure workstation is a major risk. Make sure only hardened workstations can access and manage

systems that store sensitive data.

- **Use Azure Information Protection.** Azure Information Protection makes it easier to achieve full visibility over your sensitive data, implement controls, and securely collaborate. Using it can make your overall data security efforts easier and more effective.

Storage and database security

Securing your databases is a critical element of your overall security posture. Additionally, in many cases it is a must from a compliance perspective. Here is where you should start with database security in Azure.

- **Restrict database and storage access**. Use firewalls (/cyber-hub/network-security/what-is-firewall/) and access controls to limit what level of access users, devices, and services have to your databases and storage blobs.
- **Leverage auditing**. Turn on auditing for your Azure databases. Doing so enables you to gain visibility into all database changes.
- **Configure threat detection for Azure SQL**. If you use Azure SQL, activating threat detection helps you identify security issues faster and limit dwell time.
- **Set log alerts in Azure Monitor**. It isn't enough to simply log events. Make sure you are alerting against security-related events in Azure Monitor so you can remediate issues quickly (and automatically when possible).
- **Enable Azure Defender for your storage accounts.** Azure Defender provides you harden and secure your Azure storage accounts.
- **Use soft deletes**. Soft deletes help you ensure data is still retrievable (for 14 days) in the event a malicious actor (or user error) leads to data you wanted to keep – getting deleted.
- **Use shared access signatures (SAS)**. SAS enables you to implement granular access controls and time limits on client access to data.

Workloads and Virtual Machine Protection

This section of our Azure security best practices checklist deals with virtual machines and other workloads. There are a few other best practices that will help you to protect your resources in Azure:

- **Enforce multi-factor authentication (MFA) and complex passwords.** MFA can help limit the threat of compromised credentials. Complex passwords help reduce the effectiveness of brute force password attacks.
- **Use just-in-time (JIT) virtual machine access.** JIT access works with NSGs and the Azure firewall and helps you layer in role-based access controls (RBAC) and time-bindings on access to virtual machines.
- **Have a patch process in place**. If you're not patching your workloads, all your other efforts may be for nothing. A single unpatched vulnerability can lead to a breach. A patch process to keep your operating systems and applications up to date helps you mitigate this risk.
- **Lock down administrative ports.** Unless absolutely necessary, restrict access to SSH, RDP, WinRM, and other administrative ports.
- **Use the Azure firewall and network security groups (NGSs) to limit access to workloads.** Consistent with the principle of least privilege, use NSGs and the Azure firewall to restrict workload access.

Cloud Network Security

Network security is an important aspect of keeping your Azure workloads secure. Here are the Azure security best practices to keep in mind for your cloud networks:

- **Encrypt data in transit.** As we mentioned in the encryption and data security section: encryption of data in transit (and at rest) is a must. Leverage modern encryption protocols

for all network traffic.

- **Implement zero trust**. By default, network policies should deny access unless there is an explicit allow rule.
- **Limit open ports and Internet-facing endpoints**. Unless there is a well-defined business reason for a port to be open or workload to be Internet-facing, don't let it happen.
- **Monitor device access**. Monitoring access to your workloads and devices (e.g. using a SIEM (/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/) or Azure Monitor) helps you proactively detect threats
- **Segment your networks.** Logical network segmentation can help improve visibility, make your networks easier to manage, and limit east-west movement in the event of a breach.

Compliance

Maintaining compliance is one of the most important aspects of security in the Azure cloud. Here are our recommendations to help you do just that.

- **Define your compliance objectives**. What data and workloads are in scope from a compliance perspective? What standards and regulations (e.g. PCI-DSS, ISO 27001, HIPAA) are relevant to your organization? Clearly answering those questions and defining your compliance objectives is a must.
- **Use the Azure Security Center's regulatory compliance dashboard and Azure Security Benchmark**. The compliance dashboard in the Azure Security Center can help you identify how close you are to achieving compliance based on a wide range of standards. Azure Security Benchmark provides recommendations you can follow to move closer to full compliance. Using these tools helps you simplify compliance in the cloud.

Improving Azure Security with The Check

Point Unified Cloud Security Approach

As you can see, a lot goes into achieving security in the Azure cloud. To help enterprises streamline the process and implement cloud security best practices at scale, we developed the Check Point Unified Cloud Security Approach (https://blog.checkpoint.com/2021/03/25/the-advantages-of-a-unified-approach-to-cloud-data-security/). Based on the principles in that unified approach, Check Point CloudGuard (https://pages.checkpoint.com/cloudguard-cspm-trial.html) is the ideal tool to help you implement these cloud security best practices.

To learn more about Azure security and how Check Point can help you, download the free Achieving Cloud with Confidence in the Age of Advanced Threats (https://pages.checkpoint.com/cloud-with-confidence.html) whitepaper where you'll learn:

- How to secure multi-cloud environments at scale
- How to improve cloud visibility
- How to maintain compliance across different deployments

Alternatively, if you want to evaluate your current cloud security posture, sign up for a free security checkup (https://pages.checkpoint.com/security-checkup.html). After the checkup, you'll receive a comprehensive report detailing items such as number of malware infections, threats to endpoints and smart devices, bot attacks and intrusion attempts, use of high-risk applications, and loss of sensitive data.

Get Started

Azure Security Solutions (/solutions/microsoft-azure-security/)

Cloud Security Solutions (/solutions/cloud-security/)

Cloud Network Security (/products/iaas-public-cloud-security/)

Cloud Security Posture Management (/products/cloud-security-orchestration/)

Cloud Workload Protection (/products/workload-protection/)

Cloud Intelligence in Azure (/products/cloud-intelligence-threat-hunting/)

Application Security (/products/cloudguard-appsec/)

Related Topics

What's the Shared Responsibility Model (/cyber-hub/cloud-security/what-is-aws-shared-responsibility-model-and-how-it-works/)

What is Cloud Security? (/cyber-hub/cloud-security/what-is-cloud-security/)

What is DevSecOps? (/cyber-hub/cloud-security/what-is-devsecops/)

AWS Security Groups (/cyber-hub/cloud-security/what-is-aws-security-groups/)

What is Serverless Security? (/cyber-hub/cloud-security/what-is-serverless-security/)

What is Shift Left? (/cyber-hub/cloud-security/what-is-shift-left-security/)

What is Application Security (AppSec)? (/cyber-hub/what-is-application-security-appsec/)