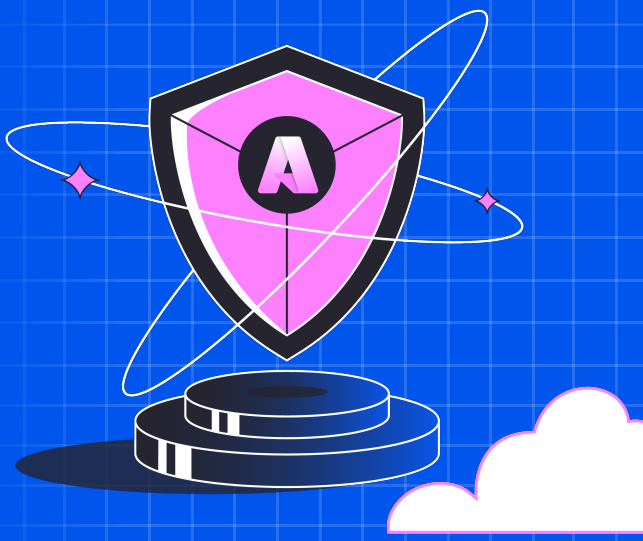
WIZ

Cheat Sheet

Azure Security Best Practices

Security is a key priority for any CISO of any organization with an extensive footprint in Azure. In the first part of our blog series, we covered the basics of Azure security, including no-brainer solutions that you can implement quickly.

Part 2 discusses actionable recommendations that can help you strengthen your Azure cloud security posture. We'll explore detailed aspects of Azure best practices, from role-based access control (RBAC) to cloud security posture management, that you can adapt to secure your Azure subscriptions.



Azure RBAC

Azure RBAC is a granular security solution designed to meet the dynamic security needs of Azure workloads. Going beyond traditional security mechanisms, it offers a flexible and granular solution for organizations to regulate who can take what type of actions on Azure Resources.

1 Centralized identity and access management

Azure RBAC works in conjunction with Microsoft Entra ID, a cloud-based service, for centralized identity and access management in Azure. It enables administrators to assign roles to users, groups, and service principals based on their responsibilities, ensuring that access is granted in a granular manner. You can either use built-in roles or create custom roles, assigning permissions only as necessary per the principle of least privilege.

2 Risk-based access policies

Azure RBAC also works in conjunction with multi-factor authentication (MFA) to identify and prevent risky behavior. Enabled by the identity protection feature of Microsoft Entra ID, you can configure your access control policies based on either sign-in risk or user risk.

If a threat is detected during a sign-in, the relevant policy will be applied. For example, organizations could insist on MFA above a specific risk level, say, medium or high. This feature also enables auto-remediation, so if the steps enforced by the policy are executed, the user session will be allowed without admin intervention.

3 Privileged access control

Privileged identity management in Microsoft Entra ID allows for time-bound and approval-based roles for Azure resources. You can use this feature to configure additional approvals for admin roles with excess privileges or to restrict access to defined time periods.

This lets you enforce user policies to provide justification for activating roles, generate alerts when privileged roles are activated, and ensure that access is reviewed periodically.

All of the above features fortify Azure security and ensure that only authorized users can access your resources at any given time.

Policy management

One of the biggest challenges that organizations face in large-scale Azure deployments is ensuring the governance of resources and that necessary security measures are applied consistently across resources.

1 Management hierarchy

Azure provides **four levels of management hierarchy** to achieve this:

- **Management groups**
- **Subscriptions**
- **Resource groups**
- **Resources**

The first three all offer different levels of logical groupings of Azure resources.
Resources with the same lifecycle and access control requirements can be grouped together into **resource groups**.

There can, in turn, be many such resource groups in a **subscription**, which is again another logical segregation of resources with a defined set of quotas, limits, RBAC, and cost and billing configurations.

These subscriptions are then grouped into **management groups**, allowing you to configure security policies and RBAC controls that are applicable to multiple subscriptions.

2 Built-in policies

Once you have organized your resources into management groups, subscriptions, and resource groups, you can configure Azure policies to enforce your organizational standards and evaluate your compliance status.

It is recommended to use Azure Policy for implementing consistent resource configuration, cost management, and security. This service includes a policy definition, i.e., a set of enforcement conditions and effects if those conditions are met. Policy definitions can be applied to any of the four levels of management hierarchy.

Policy definitions also let you implement different types of constraints. For example, you can allow only specific SKU types, permit resources to be deployed in compliant locations, add tags to resources, deny specific resource types from being deployed, etc.

3 Custom policies

Azure features several built-in policies. However, if you have a niche security requirement that cannot be met by these, you can create a custom policy. For example, you may need to enable HTTPS access for storage accounts.

Network protection

Azure offers different services enabling multifaceted security for your network-connected resources in Azure. We will look at a few to protect your workloads from unauthorized access, threats, and vulnerabilities.

1 Network segmentation & groups

Azure Virtual Network provides logical segmentation of various resources in Azure. Unless explicitly connected through options such as VPN or peering, resources in different VNets cannot talk to each other. So, segregating resources in different VNets will help prevent lateral movements in the event of a security breach.

Network security groups (NSGs) control ingress and egress traffic to resources connected to a VNet.

2 Zero trust security

You can implement a zero trust security strategy by explicitly denying all traffic and allowing only required traffic using rules that have higher priority.

When there is a multi-tiered architecture deployed in the same VNet, you can bring in additional security by permitting only required traffic between tiers even if the traffic is internal. This helps prevent the proliferation of threats if one of the tiers is compromised.

3 NSG flow logs

For visibility into network traffic that flows in and out of your VNet, enable NSG flow logs that capture this information. These provide valuable insights into network traffic, flag any unauthorized access attempts, and help troubleshoot security issues.

Data encryption

Azure offers strong encryption solutions for data in transit and at rest, in addition to key management services to safeguard and manage encryption keys.

1 Key management

The native key management service in Azure is called Key Vault. You can use this for managing cryptographic keys, secrets, and certificates, as it centralizes the key management requirement for encryption data, SSL/TLS certificates, and application secrets.

If your data is highly sensitive, you can opt for Azure Dedicated Hardware Security Module (HSM), which supports the management of keys in a FIPS 140-2 Level 3 compliant environment.

2 Encryption of data at rest

For visibility into network traffic that flows in and out of your VNet, enable NSG flow logs that capture this information. These provide valuable insights into network traffic, flag any unauthorized access attempts, and help troubleshoot security issues.

For services where encryption keys are managed via Azure Key Vault, make sure that you implement a key rotation policy for all the keys. Microsoft recommends that keys be rotated at least every two years.

3 Encryption of data in transit

For encryption of data in transit, TLS is supported for services like Azure App Service, Azure SQL Database, and Azure Storage. You can also use Azure Application Gateway, which supports end-to-end SSL encryption and can be used to terminate SSL connections from the internet.

Operational security

Azure offers strong encryption solutions for data in transit and at rest, in addition to key management services to safeguard and manage encryption keys.

1 Multi-factor authentication

It is recommended to enable multi-factor authentication for all users including administrators. Microsoft Entra ID security defaults help you to quickly enable and enforce this. When used in conjunction with a conditional access policy, MFA is enforced when specific conditions are met, such as untrusted devices, risky applications, or different locations.

2 Password management

reset their passwords, you can use the self-service password reset feature from Microsoft Entra ID.

Make sure to review usage through the built-in reporting features of Microsoft Entra Password Protection. These reports give you a view of the number of people registering for password resets, the frequency of password resets, and any associated suspicious activities.

You can enable Just-in-Time (JIT) access for your VMs as well, especially for admin accounts. This will allow traffic to selected ports and from allowed source IP addresses for a specific timeframe only to further reduce the attack surface.

3 IaC adoption

To eliminate manual operational errors, you should always opt for automated builds, deployments, and configurations wherever possible. Infrastructure as code (IaC) can help you achieve this by ensuring consistency across environments and eliminating the problem of drifts, as the configuration is versioned and saved as code just like your application.

This makes the configuration repeatable and auditable, and eliminates human error. It also aligns with the concept of "idempotence," i.e., the same result every time the same operation is executed.

Look to implement:

- **Azure Resource Manager (ARM) templates:** These are written in a declarative format to deploy multiple resources and their dependencies.
- **Azure DevOps:** IaC in Azure DevOps lets you streamline the build and deploy process; it also helps to avoid misconfigurations and eliminate security gaps.
- **Terraform:** Hashicorp Terraform is a popular open-source IAC tool you can use across multiple hybrid and multi-cloud environments. Azure supports the configuration of Azure resources, Azure AD, and APIs, plus the integration with Azure DevOps through Terraform.

Application layer security

Application layer security is indispensable in the realm of cloud security. Whether to protect your internet-facing applications from unknown (and known) attack vectors or against a myriad of sophisticated and evolving threats, Azure offers a set of native services that can help fortify your application layer.

1 Endpoint application security

Securing endpoints in Azure entails safeguarding the apps and services that run in your Azure environment from potential attacks and vulnerabilities. This should start in the application design phase with threat modeling.

You can leverage the SDL Threat Modeling tool to identify threats and receive possible mitigation steps. In addition to options such as encryption and identity protection that we have seen so far, the mitigation plan should also include services that protect the application layer.

2 WAF

The Web Application Firewall (WAF) feature in Azure Application Gateway can be leveraged to protect your applications against common threats such as cross-site scripting, SQL injection, HTTP protocol violation, remote file inclusion, etc. This is aligned with the Core Rule Set (CRS) defined in the Open Worldwide Application Security Project (OWASP). In addition to the pre-configured rule set, you can build custom rules to best suit your application requirements.

3 Azure Firewall

Application layer security can be augmented by the L7 protection capabilities offered by Azure Firewall, such as HTTPS traffic filtering in hybrid deployments.

You can also leverage Azure Firewall premium features to inspect HTTP headers and perform deeper packet analysis using TLS inspection. **Note:** It is a recommended design pattern to use Web Application Firewall along with Azure Firewall.

Cloud Security Posture Management

Cloud Security Posture Management (CSPM) is a comprehensive framework that provides organizations with the tools and capabilities required to ensure a secure, compliant, and well-governed Azure environment. Let's look at some of the native Azure capabilities that will help with managing the security posture of your workloads.

1 Microsoft Defender for Cloud

This serves as the cloud-native application protection platform (CNAPP) that helps protect your application from a wide range of vulnerabilities, threats, and misconfigurations. It includes the capabilities of DevSecOps, cloud security posture management (CSPM), and a cloud workload protection platform (CWPP).

Microsoft Defender lets you shift security left by integrating best practices early on in the development process through code pipeline insights, which detect loopholes such as exposed secrets and misconfigurations.

The CSPM capability of Microsoft Defender analyzes the security configuration of your resources and provides recommendations to fix any misconfigurations.

2 Secure Score

Microsoft Defender for Cloud helps quantify your security posture using Secure Score. This service continuously assesses your cloud resources against the Microsoft cloud security benchmark (MCSB) and assigns a "secure score" for your environments. A lower secure score means the environment is at risk and needs remedial measures to be implemented to improve the score. This can be accomplished by implementing the actionable recommendations offered by Microsoft Defender, thereby minimizing the attack surface.

Compliance

Ensuring compliance for your Azure deployments starts with defining the compliance requirements for your organization. This may depend on factors such as the industry vertical that you are in or data residency and sovereignty requirements. Once this is done, you can look at the tools and services available for ensuring adherence to the relevant regulations and standards.

1 Built-in benchmark assessment & dashboards

Microsoft Defender for Cloud has built-in Azure benchmark assessments and dashboards for all leading regulatory and compliance standards. You can also leverage this service to perform foundational compliance assessments for AWS and GCP.

The dashboards provide a bird's-eye view of your organization's compliance posture against leading regulations such as CIS, SOC 2, PCI DSS, FedRamp, and HIPAA. Assessments against compliance standards are automatically run every 12 hours.

The dashboards also provide details of the actions, manual and automated, that need to be implemented to mitigate any problems detected. These capabilities provide a good starting point for you to meet your compliance requirements.

Augmented security through Wiz

While there are many cloud-native security features available in Azure, with complex hybrid and multi-cloud deployments, it is recommended to implement specialized solutions to augment your security posture.

Wiz offers a cloud-native application protection platform that can help you achieve this. Wiz's suite of capabilities ensures comprehensive cloud security: CSPM, CWPP, vulnerability management, cloud infrastructure entitlement management (CIEM), CI/CD, CDR, and data security posture management (DSPM).

Wiz CNAPP is an agentless graph-based solution that provides 100% visibility across multiple clouds, enabling you to prioritize identified risks and take remedial action. It can be used to scan VMs, serverless resources, data volumes, databases, and other PaaS services to visualize the security status of your resources. Plus, Wiz uses an agentless approach with a unified solution to scan multiple cloud environments.

The real-time threat detection and end-to-end visibility offered by Wiz CNAPP help you track and mitigate attack vectors quickly. It also features a single risk queue that lets you prioritize threats and promotes cooperation between teams to improve your cloud security and compliance posture.