Microsoft Azure Security Engineer (AZ-500)

Full Learning Guide

This is a complete guide covering the **entire AZ-500 exam outline** in depth. It is written to function as a standalone study resource, but you are encouraged to cross-reference other materials to prepare.

Learning Objectives and Expectations

We'll cover:

- Every AZ-500 exam objective in full detail.
- Every critical Azure security concept you must know and connect together.
- How to think like a security engineer — not just memorize commands.

Each domain guide includes:

- Full concept breakdowns of services, configurations, and architectures.
- Real-world security scenarios drawn from Azure environments.
- Exam tips, tables, and memory tricks to lock in key ideas.

AZ-500 Domains (as of 2025)

Each domain carries a distinct weight on the exam:

- **Domain 1:** Secure Identity and Access (15–20%)
- **Domain 2:** Secure Networking (20–25%)
- **Domain 3:** Secure Compute, Storage, and Databases (20–25%)
- **Domain 4:** Secure Azure Using Microsoft Defender and Microsoft Sentinel (30–35%)

Quick Reminder: How the Exam Works

Attribute	Details
Questions	~40–60
Format	Multiple choice, drag & drop, hot area, case studies, JSON/CLI snippets
Time Limit	150 minutes
Passing Score	700 / 1000 (≈ 70 %)
Test Provider	Pearson VUE or Certiport (onsite or online proctored)
Languages	English (plus select localized versions)
Prerequisites	Strong understanding of Azure administration, Entra ID, networking, and security operations

Top 10 AZ-500 Exam Tips

- **Master the Azure Security Stack:** Understand how Entra ID, Defender for Cloud, and Sentinel integrate (identity → posture → detection).
- **Prioritize Least Privilege:** Always think scope > role > principal; assign roles at the lowest appropriate scope.
- **Know Identity Protection:** Grasp Conditional Access, MFA, PIM, and Permissions Management concepts.
- **Think Like a Defender:** Expect scenario-based questions on securing VMs, storage, AKS, hybrid connectivity.
- **Understand Networking Layers:** NSGs = L4 filtering; App Gateway = L7 + WAF; Azure Firewall = stateful L3–L7 control; Front Door = global edge security.
- **Memorize Data Protection Options:** SSE, ADE (disk encryption), BYOK, double encryption, immutable storage, TDE, Always Encrypted.
- **Be Fluent in Defender Plans:** Know Defender for Servers, Containers, Databases, Storage, Key Vault, etc., and what each monitors.
- **Understand Sentinel's Flow:** Data → Analytics Rules → Incidents → Playbooks. Know basic KQL and automation logic.
- **Get Hands-On:** Practice configuring policies, private endpoints, JIT VM access, Key Vault, and Sentinel connectors.
- **Manage Time & Nerves:** Use the 150 minutes wisely. Focus on scenario reasoning, flag and skip tough questions to revisit, and remember that 700 points (70%) is a pass.

Domain 1 – Secure Identity and Access (15–20%)

Identity is the foundation of Azure security. In Azure, users, apps, and services don't get access by default — everything must be explicitly granted. This domain focuses on **who can access what**, **how they prove who they are**, and **how to control and monitor those permissions.**

1. Role-Based Access Control (RBAC)

RBAC (Role-Based Access Control) defines *what actions someone can perform* on Azure resources.

When you give someone access, you assign:

- A **role** (set of permissions)
- A **principal** (user, group, service principal, or managed identity)
- A **scope** (what level of Azure hierarchy it applies to)

Scope Hierarchy

Permissions flow downward:
Management Group → Subscription → Resource Group → Resource

If someone gets "Contributor" at the subscription level, that access inherits down to all resource groups and resources in that subscription — unless blocked by a *deny assignment*.

Permission Evaluation Order

Deny → DenyAssignments → Allow
Azure always checks denies first.

Deny Assignments

- Created automatically by Azure (e.g., Blueprints)
- Override all allows
- You can't create them manually

The Core 3 Roles

Role	Description
Owner	Full control over all resources. Can modify anything and manage RBAC permissions (add/remove roles).
Contributor	Can create, modify, and delete resources — but **cannot** grant or remove permissions.
Reader	View-only access to resources and configurations. Useful for auditors or monitoring users.

Specialized Built-in Roles

These roles focus on particular functions — they don't grant full access to everything but allow control over specific services or settings.

Role	Description
User Access Administrator	Can manage RBAC role assignments without owning the underlying resource. Used to delegate access management.
Security Administrator	Manages Microsoft Defender for Cloud, security policies, and recommendations.
Security Reader	Can view all Defender alerts and recommendations, but can't make changes.
Policy Contributor	Can create, edit, and assign Azure Policy and Initiative definitions, but cannot assign RBAC access.
Blueprint Contributor	Can create and publish Blueprints (compliance templates), but not assign them.
Billing Reader	View-only access to billing data and cost reports (no ability to change payment methods).
Managed Identity Operator	Can assign or reset managed identities for Azure resources. Typically used by automation tools.

How RBAC Works in Practice

- **Example 1:**
  A team member managing only databases should have **Contributor** on the resource group containing databases — not on the full subscription.

- **Example 2:**
  An auditor should be given the **Reader** role at subscription or management group scope.

Best Practice: Always follow **Least Privilege** — give the narrowest possible role and scope that allows the task.

Azure AD (Entra ID) Roles

RBAC manages **resource-level** access.
Azure AD (now Microsoft Entra ID) manages **directory-level** access — meaning users, groups, MFA, Conditional Access, and applications.

Role	Description
Global Administrator	Full control of Azure AD tenant. Can manage users, groups, MFA, Conditional Access, domains, licenses, and enable Privileged Identity Management (PIM).
Security Administrator	Manages Conditional Access, Identity Protection, MFA, and security reports.
Privileged Role Administrator	Manages PIM setup and Azure AD role assignments. Can activate/deactivate privileged roles.
Application Administrator	Manages app registrations, enterprise applications, and consent settings for APIs.
Cloud Application Administrator	Similar to Application Administrator but cannot manage Conditional Access or tenant-wide consent.
Authentication Administrator	Can reset passwords and re-register MFA for non-admin users. Common helpdesk-level role.
Password Administrator	Resets passwords for users and limited admins (not Global or Privileged Admins).
Billing Administrator	Manages billing profiles, invoices, and payment methods.
User Administrator	Creates and manages users and groups, and can reset passwords for most accounts.
Compliance Administrator	Manages audit logs, retention, and labeling for compliance features like Microsoft Purview.
Reports Reader	Can view audit logs and sign-in reports (used for monitoring or integration with Sentinel).

Remember:

- Azure AD (Entra ID) roles apply to **directory and identity settings**
- Azure RBAC roles apply to **Azure resources**

Example:
A Global Admin can manage users and MFA policies but cannot modify virtual machines unless given an Azure RBAC role like Contributor or Owner.

Key Differences Summary

Category	Azure RBAC	Azure AD Roles
Scope	Management Group → Resource	Tenant / Directory
Used For	Resource permissions	Identity and access governance
Examples	Owner, Contributor, Reader	Global Admin, Security Admin
Assignment Target	Users, groups, service principals, managed identities	Users, groups, service principals
Interface	Azure Portal (resource access control)	Entra ID (Roles & Admins)
Purpose	What someone can do *with resources*	What someone can do *with identities*

Practical Example

Let's say your company runs multiple applications in Azure:

- **Developers** deploy and manage web apps → assign them **Contributor** on the Resource Group.
- **Security Team** reviews Defender alerts and configures policies → assign **Security Admin**.
- **Finance Team** checks usage costs → assign **Billing Reader**.
- **Helpdesk Staff** resets MFA for users → assign **Authentication Administrator** in Entra ID.

2. Conditional Access (CA)

Conditional Access (CA) is Azure AD's (Entra ID's) main system for **adaptive, context-based authentication**. It decides **whether to grant access** to an application based on conditions such as who the user is, what device they're using, where they're connecting from, and how risky the sign-in appears.

Think of it as a *smart gatekeeper* that constantly checks:
"Is this sign-in safe enough right now?"

How Conditional Access Works

When a user attempts to sign in, Azure evaluates multiple **signals**:

Condition	Example Trigger
User or Group	Apply the policy to specific users, departments, or security groups.
Cloud App or Action	Target specific services, e.g., Exchange Online, SharePoint, or Azure Portal.
Location	Allow sign-ins from trusted networks only, or block risky regions.
Device State	Require the device to be compliant (registered in Intune or Hybrid AD).
Client App Type	Block older, insecure protocols like POP or IMAP.
Sign-in Risk	Use Azure AD Identity Protection signals (medium/high risk).

Based on these signals, Azure applies **controls**:

Control Type	Example
Grant	Allow access only if MFA is completed or the device is compliant.
Block	Deny access outright.
Session	Limit user session behavior (e.g., sign out after X minutes).

Common Conditional Access Scenarios

Scenario	Typical Policy
Protect all admin accounts	Require MFA every time for privileged roles.
Reduce risk for normal users	Require MFA for risky sign-ins only.
Secure company resources	Block access from outside specific countries or IP ranges.
Support BYOD (personal devices)	Allow access only via compliant or enrolled devices.
Stop legacy protocols	Block basic authentication for all apps.

Conditional Access vs. Security Defaults

- **Security Defaults** (available in all tenants):
  Predefined Microsoft baseline enforcing MFA for admins and blocking legacy auth.
  Simplified, can't be customized.
- **Conditional Access** (requires Entra ID Premium P1 or P2):
  Fully configurable, policy-based system allowing multiple conditions and exceptions.

Best Practices

- Combine CA with Identity Protection (to use risk-based signals).
- Assign policies in "Report-only" mode first to monitor behavior before enforcement.
- Include *break-glass accounts* (emergency global admins) that bypass CA for recovery.
- Target "All users" and then exclude trusted system accounts only if absolutely necessary.

3. Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an **extra layer of security** on top of usernames and passwords.
A user must verify their identity using **two or more factors**:

Factor Type	Example
Something you know	Password or PIN
Something you have	Authenticator app, SMS code, FIDO2 key, or hardware token
Something you are	Fingerprint, face recognition

Azure MFA can be required through:

1. **Per-user MFA** (basic setup, legacy)
2. **Conditional Access policies** (modern method)
3. **Identity Protection** (risk-based MFA on suspicious sign-ins)

MFA Methods

Method	Description
Microsoft Authenticator App	Approve a push notification or enter a verification code.
Text Message (SMS)	One-time passcode sent to registered number.
Voice Call	User confirms by pressing a key.
FIDO2 Security Keys	Hardware-based, passwordless authentication.

Key MFA Details

- PIM role activation **always** requires MFA, even if user already signed in.
- Security defaults automatically enforce MFA for all admin roles.
- Trusted IPs or compliant devices can be excluded from MFA prompts.
- MFA reports and sign-in logs can be reviewed under:
  Azure AD → Security → MFA Reports.

Example:
A user logs in from an unfamiliar location. Azure flags the sign-in as *medium risk*.

Conditional Access policy enforces MFA, and only after successful verification is access granted.

Passwordless Authentication

Azure also supports modern, passwordless options that still satisfy MFA:

- **Windows Hello for Business**
- **FIDO2 security keys**
- **Authenticator app phone sign-in**

These reduce phishing risks and password fatigue while keeping strong security.

4. Azure AD Identity Protection

Identity Protection (part of Entra ID P2) is an automated system that detects **risky sign-ins and users** using Microsoft's global threat intelligence and machine learning.
It helps answer three critical questions:

1. Who is at risk?
2. What sign-ins look suspicious?
3. What policies should mitigate this risk?

Types of Risk

Type	What It Detects	Common Cause
User Risk	Compromised credentials or ongoing user-level threats	Leaked credentials, malware, or repeated suspicious logins
Sign-in Risk	Session-level anomalies	Unfamiliar IPs, impossible travel, TOR logins, atypical activity

Risk Detection Examples

Risk Event	Risk Level	Recommended Action

Leaked credentials found in breach	High	Force password reset
Sign-in from unusual IP or device	Medium	Require MFA
Impossible travel (login from 2 far locations in minutes)	Medium	Require MFA or block
Known malicious IP	Medium	Require MFA
Malware-linked sign-in	High	Block and force password reset
Atypical user activity (behavioral anomaly)	Low–Medium	Alert or enforce MFA

Automated Risk-Based Policies

Identity Protection can automatically apply Conditional Access actions:

- **User Risk Policy:**
  Forces a password reset if a user's risk ≥ Medium.
- **Sign-in Risk Policy:**
  Requires MFA if sign-in risk ≥ Medium.

These policies run silently in the background, protecting all sign-ins across the organization.

Identity Protection Dashboard

Provides detailed visibility into:

- Users flagged as compromised
- High-risk sign-ins and devices
- Risk trends over time
- Integration with Microsoft Sentinel and Defender for Cloud Apps

5. Privileged Identity Management (PIM)

PIM is Microsoft's solution for **Just-In-Time (JIT)** privilege elevation.
Instead of keeping permanent admin rights, users can *activate* privileges only when needed — with MFA, justification, and approval.

This enforces the **Principle of Least Privilege** and minimizes attack exposure.

How PIM Works

- **Eligible Role:**
  User is eligible to activate the role but doesn't have it active by default.
- **Active Role:**
  User has activated the privilege temporarily.
- **Activation Requirements:**
  MFA, justification text, approval (optional), and time limit.

PIM Features

Feature	Description
Time-Bound Roles	Privileges expire automatically after set duration.
Approval Workflow	Certain roles (e.g., Global Admin) can require manager approval before activation.
MFA Enforcement	MFA required on every activation.
Notifications	Alerts when privileged roles are activated or expire.
Access Reviews Integration	Periodic checks ensure users still need those roles.

PIM Example Scenarios

Use Case	Solution
A user occasionally needs Global Admin access	Assign as *Eligible* in PIM, 4-hour window per activation
You want approval before anyone activates Security Admin	Add approval workflow to the role

Need record of who elevated and when	Use PIM audit logs for all activations

Access Reviews

Access Reviews allow you to **periodically validate** who should keep access to groups, apps, or roles.

- Reviews can be **self-attested** (users confirm they still need access), or assigned to **managers/auditors**.
- Integrates directly with PIM to revoke privileges if no response is received.
- Enforces **ongoing least privilege** and ensures compliance alignment.

6. Application Access and Service Identities

Azure applications and services often need to access other resources (like Key Vault, Storage, or SQL) without any human sign-in.
Instead of embedding passwords or secrets, Azure provides **service identities** that authenticate securely and automatically.

These come in three main types:

1. **App Registration**
2. **Service Principal**
3. **Managed Identity**

App Registration

An **App Registration** is a *blueprint* of an application inside Microsoft Entra ID (Azure AD).
It defines:

- The app's name and redirect URLs
- Which permissions the app can request
- Its client ID and secret/certificate for authentication

You'll find it under:
Entra ID → App registrations → New registration

Example:

- Registering an internal web app that needs users to sign in with Azure AD.
- Registering an API so other services can access it using OAuth 2.0 or OpenID Connect.

Service Principal

A **Service Principal (SP)** is the *instance* of an App Registration in a specific tenant.
Think of it as the app's "identity card" within that tenant.

When you register an app:

- Azure automatically creates a Service Principal in your tenant.
- This SP is what actually signs in and gets tokens to access resources.

Use Cases

- CI/CD pipelines running in Azure DevOps use a Service Principal to deploy infrastructure.
- A Function App uses a Service Principal to read data from Key Vault.

Permissions

- Assign RBAC roles directly to the Service Principal just like a user.
  Example: Give *Key Vault Secrets User* role to allow it to retrieve secrets.

Managed Identities

A **Managed Identity** is an automatically managed Service Principal tied to an Azure resource.
Azure handles the credentials, rotation, and deletion — you never see any password or secret.

Two types:

Type	Description	Example
System-assigned	Created automatically for a single resource (VM, Function App, Logic App). Deleted when that resource is deleted.	VM authenticating to Key Vault.
User-assigned	Stand-alone identity that can be attached to multiple resources. Must be created manually.	Shared automation identity used by several Functions.

Key benefits

- No secret management (credentials rotate every 90 days).
- Works with RBAC and Azure AD-based authentication (no connection strings).
- Supports most Azure services (VMs, App Service, Functions, Automation, Logic Apps, etc.).

Comparison Summary

Feature	App Registration	Service Principal	Managed Identity
Created in	Entra ID	Automatically when app registered	Azure resource itself
Credential type	Client secret or certificate (manual)	Same as app	None (auto-rotated)
Lifecycle	Independent	Linked to App Registration	Linked to resource
Management overhead	Manual secret rotation	Manual	None
Common use	Multi-tenant apps or APIs	Automation tools, DevOps	Secure resource-to-resource access

How Managed Identity Authenticates

1. Azure issues a temporary access token to the resource's Managed Identity.

2. The resource presents that token to another Azure service (like Key Vault).
3. The target service verifies the token with Entra ID and grants access if the role allows it.

Example Flow:

- A VM with a **system-assigned MI** requests a secret from Key Vault.
- Azure injects an access token valid for a few minutes.
- Key Vault verifies the token and returns the secret.
- No passwords, no stored keys — completely managed by Azure.

7. Securing Applications with Key Vault

Azure Key Vault is the main service for securely storing and managing:

- Secrets (API keys, DB passwords)
- Certificates
- Encryption keys (for storage, VM disks, SQL TDE)

Access Control Models

1. **Azure RBAC (Model 1)**
    - Controls who can *manage* the vault itself (create, delete, configure).
    - Example roles: Key Vault Administrator, Key Vault Reader.
2. **Access Policies (Model 2 – legacy)**
    - Define which identities can *use* keys/secrets (get, list, set).
    - Some legacy services still depend on this model.

Best practice:
Use RBAC for administrative control and Access Policies only for legacy integration that doesn't yet support RBAC.

Soft Delete & Purge Protection

Feature	Purpose
Soft Delete	Retains deleted secrets, keys, or certificates for 90 days.
Purge Protection	Prevents permanent deletion during the retention period.

Both are required to meet compliance frameworks (HIPAA, ISO, CIS).
Always enable them before production deployment.

Customer-Managed Keys (CMK)

Some services encrypt your data automatically with Microsoft-managed keys.
If your organization requires control, you can use **Customer-Managed Keys** stored in Key Vault or Managed HSM.

Used by:

- Azure Disk Encryption (BitLocker/DM-Crypt)
- Azure Storage Service Encryption
- Azure SQL TDE (Transparent Data Encryption)

CMK Advantages:

- Full key ownership and lifecycle control
- Supports key rotation and audit logging
- Enables compliance with data residency and regulations

Integration Example

Scenario: A Function App needs to read secrets from Key Vault.

1. Enable a **system-assigned Managed Identity** for the Function App.
2. In Key Vault, grant that identity **Secrets User** role.
3. In code, use the **DefaultAzureCredential()** method (SDK).
4. The Function authenticates silently using its Managed Identity token.

Result: No stored passwords, no expired keys, and full audit visibility.

Key Vault Best Practices

- Always enable Soft Delete + Purge Protection.
- Assign access using Azure RBAC roles instead of Access Policies when possible.
- Rotate keys and secrets regularly (using Event Grid + Azure Functions for automation).
- Enable diagnostic logging to Log Analytics for all vault activities.
- Restrict network access using Private Endpoints or Firewalls.
- Monitor Defender for Key Vault alerts (suspicious access or exfiltration).

Domain 2 – Secure Networking (20–25%)

Azure networking security protects **how data moves** between resources, users, and the internet.
The main goal: **control traffic flow**, **minimize exposure**, and **enforce segmentation**.

Azure uses multiple layers of defense — from basic network rules (NSGs) to advanced, centralized protection (Azure Firewall, WAF, and DDoS).

1. Network Security Groups (NSG)

Purpose:
Network Security Groups act like virtual firewalls at the subnet or network interface level.
They filter inbound and outbound traffic based on rules (Layer 4 – TCP/UDP).

How NSGs Work

Each rule has:

- **Priority** (lower = processed first)
- **Direction** (inbound or outbound)
- **Source/Destination** (IP, subnet, service tag, or application group)
- **Protocol** (TCP, UDP, Any)
- **Action** (Allow or Deny)

Defaults

- **Inbound:** All denied by default
- **Outbound:** All allowed by default
- First matching rule is applied (top-down processing)

Common Service Tags

Tag	Description
Internet	Any external IP address
VirtualNetwork	Any resource in the same VNet
AzureLoadBalancer	Azure's internal load balancer traffic
Storage	Azure Storage public endpoints

NSG Rule Example

Priority	Direction	Source	Destination	Action
100	Inbound	VirtualNetwork	WebVM	Allow
200	Inbound	Internet	WebVM	Deny

Example:
A web server needs inbound HTTP (80) from the internet but no RDP access.
Allow inbound TCP 80 → Deny inbound TCP 3389.

2. Application Security Groups (ASG)

Purpose:
Application Security Groups make NSG management easier by grouping VMs logically. They act as "labels" for dynamic segmentation — you assign rules to ASGs instead of individual IPs.

How It Works

- You can place NICs of multiple VMs into an ASG (e.g., "WebTier" or "DBTier").
- NSG rules then reference the ASG name rather than IP addresses.

Example:

Allow WebTier → DBTier on port 1433 (SQL)

Limitations

- Must be in the same VNet and region.
- Cannot span VNets.
- Combine NSG + ASG for flexible, scalable segmentation.

Best Use Case:

Segmenting multi-tier applications (Web, App, DB) within the same network.

3. Azure Firewall

Purpose:
Azure Firewall is a **stateful**, fully managed firewall that operates from Layer 3 to Layer 7. It protects outbound, inbound, and east-west (internal) traffic using centralized rules.

Key Features

Feature	Description
Stateful Inspection	Tracks active connections and allows return traffic automatically.
Threat Intelligence Filtering	Blocks traffic from/to known malicious IPs and domains.
FQDN & URL Filtering	Control outbound traffic by domain name (e.g., allow only *.microsoft.com).
TLS Inspection (Premium SKU)	Decrypts and inspects HTTPS traffic for threats.
Intrusion Detection & Prevention (IDPS)	Detects exploits and attacks.
DNAT/SNAT Support	Translate private ↔ public IPs for inbound/outbound traffic.
Logs & Alerts	Send to Log Analytics, Event Hub, or Storage.

Deployment Models

- **Hub-and-Spoke:** Firewall in a hub VNet controlling traffic from multiple spokes.
- **Secured Virtual Hub:** Firewall integrated into Azure Virtual WAN for large enterprises.

When to Use Azure Firewall

- You need **centralized egress control** (e.g., allow only specific URLs).
- You need **deep inspection** (TLS/IDPS).
- You must log all network activity for compliance.

4. Web Application Firewall (WAF)

Purpose:
Protects web applications (Layer 7) from common attacks like SQL injection, XSS, or header manipulation.
Implemented through:

- **Application Gateway (regional)**
- **Azure Front Door (global)**

Application Gateway (WAF)

Acts as a **reverse proxy** that terminates client connections and forwards traffic to backend web servers.
It handles:

- SSL/TLS termination
- Cookie-based session affinity
- Load balancing
- Health probes
- WAF inspection (optional mode)

WAF Modes

Mode	Description
Detection	Logs suspicious activity but doesn't block.
Prevention	Blocks and logs malicious traffic automatically.

Rule Sets

- Uses **OWASP Core Rule Set (CRS) 3.x** for common vulnerabilities.
- You can also add **custom rules** for specific patterns or IP blocking.

Example Use Case:
Host an e-commerce site behind an Application Gateway WAF to filter malicious requests before reaching your VMs or App Services.

Azure Front Door (Global WAF)

Azure Front Door combines a global load balancer, CDN, and WAF at Microsoft's edge network.

Feature	Description
Global Layer 7 Load Balancing	Routes traffic to closest or healthiest region.
DDoS Protection	Automatically mitigates volumetric attacks.
Caching / CDN	Reduces latency by serving content from edge locations.
WAF Rules	Same OWASP CRS and custom rule support as App Gateway.

When to Use:

- Multi-region or global web applications.
- Public-facing apps requiring low latency and DDoS protection.

5. DDoS Protection

Purpose:
Defend against Distributed Denial of Service (DDoS) attacks that flood your network or application with traffic.

Two Tiers

Tier	Description
Basic	Automatically included for all Azure services; protects Azure infrastructure.
Standard	Adds adaptive, per-VNet protection for customer workloads.

DDoS Standard Benefits

- Auto-tuned to your network traffic profile
- Mitigates L3/L4 volumetric attacks
- Provides telemetry and metrics via Azure Monitor
- Supports attack analytics reports for incident investigation
- Includes a $300,000 service credit for post-attack cost protection

Enable it per Virtual Network hosting internet-facing endpoints.

6. Private Link & Private Endpoints

Purpose:
Provide **private network access** to Azure PaaS services like Storage, SQL, or Key Vault — without ever exposing traffic to the public internet.

How It Works

- Azure assigns a **private IP** from your VNet to the service endpoint.
- Traffic flows entirely within Azure's backbone network.
- DNS resolves to the private IP instead of a public endpoint.

Benefits

- Eliminates public exposure and data exfiltration risk.
- Enables compliance isolation (HIPAA, ISO, PCI).
- Works with NSGs and Azure Firewall for fine-grained control.

Example

Your database (Azure SQL) can only be reached from your application subnet via a **Private Endpoint** — not from the internet, even if someone knows its FQDN.

7. Service Endpoints

Purpose:
Allow resources in a VNet to securely access specific Azure services (like Storage or SQL) *without a private IP assignment*.

Traffic still uses Azure's public backbone but is restricted by the subnet ID.

Comparison: Private Endpoint vs. Service Endpoint

Feature	Private Endpoint	Service Endpoint
Connectivity	Uses private IP from your VNet	Uses Azure backbone but public endpoint
Isolation Level	Highest	Moderate
Data Exfiltration Protection	Yes	No
Setup Complexity	Higher	Easier
Best For	Strict compliance / zero internet exposure	Quick secure connection to PaaS

8. Virtual Network (VNet) Peering

Purpose:
Connect multiple VNets so they can communicate privately over Azure's backbone, as if they were a single network.

Features

- Low-latency, high-bandwidth private link
- VNets must be in the same region or paired regions
- Non-transitive (VNet A ↔ VNet B, but not A ↔ C unless directly peered)

Use Case Example:
A shared "Hub" network hosts the Azure Firewall, and each "Spoke" VNet (App, DB, Analytics) is peered to it.

9. Adaptive Network Hardening

Available under **Microsoft Defender for Cloud**, this feature uses AI to suggest improved NSG rules.

- Analyzes real traffic patterns
- Identifies unnecessary exposure
- Recommends rule changes (e.g., restrict SSH to corporate IPs only)
- Can auto-apply changes with Defender policy

This ensures NSG configurations evolve securely over time.

10. Just-in-Time (JIT) VM Access

Purpose:
Limit RDP/SSH exposure on VMs to only authorized users, and only for a limited time.

How It Works

- When enabled in Defender for Servers Plan 2, JIT modifies NSG rules dynamically.
- User requests access → Defender approves → temporary NSG rule opens the port (e.g., 22 or 3389).
- After session ends, rule auto-closes.

Example:
Admins can RDP into production servers for maintenance for 2 hours, after which ports close automatically.

11. Monitoring & Logging

Network events can be monitored through:

Tool	Description
Network Watcher	Packet capture, connection monitor, topology view
NSG Flow Logs	Log all allowed/denied traffic per rule
Traffic Analytics	Visualize and analyze network flows
Defender for Cloud	Detect unusual traffic or open ports
Sentinel	Correlate network logs with security events for investigations

Best Practice:
Send all NSG, Firewall, and WAF logs to **Log Analytics** or **Sentinel** for centralized analysis.

Domain 3 – Secure Compute, Storage, and Databases (20–25%)

Azure compute and data services must be **hardened**, **monitored**, and **protected at rest and in transit**.
This domain covers securing VMs, containers, data encryption, and storage access through RBAC, network controls, and Defender for Cloud.

1. Virtual Machine (VM) Security

VMs are the most common compute resources in Azure. Their security relies on a mix of **host-level**, **network-level**, and **identity-based** controls.

Key VM Protection Layers

Layer	Security Control	Description
Compute	OS patching, baseline configuration	Keep OS updated and remove unnecessary services.
Network	NSGs, JIT Access, Firewall	Control inbound/outbound traffic.
Identity	Managed Identity	Allow VMs to authenticate without credentials.
Storage	Disk encryption	Use Azure Disk Encryption with platform-managed or customer-managed keys.
Visibility	Defender for Servers	Continuous monitoring and vulnerability detection.

Azure Disk Encryption (ADE)

Encrypts Windows and Linux VM disks using BitLocker (Windows) or DM-Crypt (Linux). Keys are stored securely in Azure Key Vault.

Key Options:

- **Platform-Managed Keys (PMK):** Managed by Azure automatically.
- **Customer-Managed Keys (CMK):** You create and control them in Key Vault (for compliance).
- **Double Encryption:** Encrypts both the storage layer and the volume itself (Defense in Depth).

Just-in-Time (JIT) VM Access

Part of Defender for Cloud, JIT restricts access to management ports (RDP/SSH) by requiring approval and automatic time-based rule expiration.

Step	Description
1	Admin requests access (e.g., port 3389).
2	Defender approves and opens the port temporarily.
3	After timeout, access is revoked.

Benefit: Eliminates always-open management ports and reduces attack surface.

Endpoint Protection

Install Microsoft Defender for Endpoint or another AV solution on all VMs.
Defender for Cloud checks for missing endpoint protection and raises recommendations if absent.

2. Azure App Service Security

App Services host web apps, APIs, and functions.
They are Platform-as-a-Service (PaaS), so Microsoft handles the OS and runtime — your job is to secure **configuration, identity, and access.**

App Service Security Controls

Control	Description
Authentication / Authorization (EasyAuth)	Integrate Azure AD, Google, or other IdPs without code.
Managed Identity	Allow your app to access other Azure resources without secrets.
Private Endpoints	Restrict access to internal networks only.
TLS/SSL Enforcement	Redirect all HTTP to HTTPS; use App Service Certificates.
Backup & Restore	Regular snapshots of configuration and content.
Defender for App Service	Detects malicious requests and configuration weaknesses.

Example:
An internal API app can use a Managed Identity to access Key Vault secrets without storing keys in code.

3. Azure Kubernetes Service (AKS) Security

AKS manages containerized workloads using Kubernetes.
Because it orchestrates multiple components, hardening AKS requires securing **cluster, nodes, and workloads.**

AKS Security Layers

Layer	Focus	Example Controls
Control Plane	Managed by Azure	RBAC, secure API server access
Nodes (VMs)	Customer-managed	OS patching, disk encryption
Network	Traffic control	NSGs, Network Policies, Private Cluster
Workloads	Container runtime	Pod Security Policies, image scanning
Identity	Authentication	Managed Identity, AAD integration

Best Practices

- **Use Azure AD-integrated authentication** for kubectl access.
- **Enable RBAC within AKS** for role-scoped permissions (cluster-admin, developer, viewer).
- **Limit API server access** — use private clusters or authorized IP ranges.
- **Scan container images** with Defender for Containers or ACR image scanning.
- **Enable Defender for Containers** for runtime threat detection.
- **Use Network Policies** to restrict pod-to-pod communication.

Azure Defender for Containers

Monitors:

- Untrusted or outdated container images.
- Privileged containers or escalated permissions.
- Suspicious runtime behaviors (e.g., crypto mining, reverse shells).

Integrated with Azure Monitor, Microsoft Sentinel, and Kubernetes audit logs.

4. Azure Storage Account Security

Azure Storage Accounts hold blobs, files, queues, and tables.
They support **multiple authentication methods**, **encryption models**, and **network restrictions**.

Authentication Options

Method	Description

Azure AD Authentication	Use RBAC roles like *Storage Blob Data Contributor* for users, SPs, or MIs.
Shared Access Signature (SAS)	Time-limited token granting specific permissions to blobs/files.
Storage Account Keys	Root-level access; should be rotated and rarely used.

Network Controls

Feature	Description
Private Endpoints	Connect privately within VNets.
Firewall Rules	Allow specific IPs or VNets.
Service Endpoints	Restrict access to specific subnets.
Secure Transfer Required	Enforce HTTPS (TLS 1.2+) only.

Tip: Always disable public access unless required.

Storage Encryption

All data in Azure Storage is encrypted at rest by default.
You can choose:

Type	Description
Microsoft-Managed Keys (MMK)	Default, automatically rotated.
Customer-Managed Keys (CMK)	Stored in Key Vault or Managed HSM.
Customer-Provided Keys (CPK)	Passed by the client per request.
Double Encryption	Extra protection for highly regulated environments.

Data Redundancy Options

Option	Scope	Description
LRS (Locally Redundant Storage)	Single region	3 copies in one datacenter.
ZRS (Zone Redundant Storage)	Multi-zone	3 copies across zones in one region.

GRS (Geo Redundant Storage)	Multi-region	Copies to paired region.
RA-GRS	GRS + read access	Allows read-only failover access.

Exam pattern: ZRS = regional high availability; GRS = disaster recovery.

5. Azure SQL Database Security

Azure SQL provides PaaS relational databases with integrated encryption, auditing, and access control.

Authentication and Access Control

Option	Description
Azure AD Authentication	Recommended; uses centralized identities and Conditional Access.
SQL Authentication	Uses local username/password (legacy).
Managed Identity Access	Application connects to SQL without credentials.

Network Security for SQL

Feature	Description
Private Endpoint	Access SQL over private IP, no public exposure.
Firewall Rules	Restrict allowed IPs.
Allow Azure Services	Toggle for trusted internal services only (use carefully).

Encryption Types

Type	Purpose
TDE (Transparent Data Encryption)	Encrypts data at rest automatically.
Always Encrypted	Encrypts data in transit and at rest; keys stay client-side.
TLS (Transport Layer Security)	Encrypts data in transit.

TDE with Customer-Managed Keys (CMK) enables full key control for compliance.

Auditing & Threat Detection

- **Auditing:** Logs every query and login event to Log Analytics, Event Hub, or Storage.
- **Advanced Threat Protection:** Detects anomalies like SQL injection or unusual data exfiltration.
- **Defender for SQL:** Combines these features with continuous vulnerability scanning and alerts.

6. Azure Defender for Cloud (Compute, Storage, Data)

Microsoft Defender for Cloud unifies protection across compute, data, and network layers.

Relevant Defender Plans

Plan	Protects	Key Features
Defender for Servers	VMs (Azure, on-prem, multi-cloud)	JIT access, vulnerability assessment, file integrity monitoring
Defender for Containers	AKS, ACR	Image scanning, runtime threat detection
Defender for Storage	Blob, File shares	Detects anomalous access, malware uploads
Defender for SQL	Azure SQL, SQL on VMs	Threat detection, audit integration

Security Posture Management

Defender continuously evaluates resource configurations and gives **recommendations** with severity ratings:

- Missing encryption
- Public IP exposure
- Weak NSG rules
- Missing Defender agent

These feed into the **Secure Score** — a measurable gauge of compliance with Microsoft's security best practices.

Domain 4 – Manage Security Operations (25–30%)

Security operations in Azure revolve around three goals:
Detect, **Respond**, and **Improve**.

You'll use tools like **Microsoft Defender for Cloud**, **Microsoft Sentinel**, **Azure Policy**, and **Log Analytics** to continuously evaluate, alert, and remediate risks.

1. Microsoft Defender for Cloud

Purpose:
A unified cloud-native protection platform (CNAPP) that provides **visibility, threat detection, compliance insights, and recommendations** for all Azure (and hybrid) resources.

Defender for Cloud Overview

Feature	Description
Secure Score	Quantifies your overall security posture. Higher = better compliance.
Recommendations	Step-by-step security improvement actions (e.g., "Enable MFA for all admins").
Security Policies	Define standards to enforce through Azure Policy.
Defender Plans	Add workload protection (VMs, Containers, SQL, Storage, etc.).
Compliance Dashboard	Maps your environment to frameworks like CIS, ISO 27001, NIST, PCI-DSS.
Regulatory Compliance Reports	Automated view of control compliance and gaps.

Defender for Cloud Plan Coverage

Plan	Protects	Capabilities
Defender for Servers	VMs & hybrid servers	JIT access, vulnerability assessment, file integrity, EDR integration
Defender for Containers	AKS, ACR	Image scanning, runtime protection
Defender for SQL	Azure SQL, SQL on VMs	Threat detection, audit analysis
Defender for Storage	Blob & Files	Detects malware, exfiltration
Defender for Key Vault	Secrets & Keys	Alerts on unusual access
Defender for App Service	Web apps, APIs	Detects injection & misconfigurations

Secure Score

Every recommendation in Defender contributes to your **Secure Score**:

- Score = Completed Controls / Total Controls
- Weighted by importance
- Helps prioritize which issues to fix first (e.g., enabling Defender or MFA boosts the score).

Example:
“Enable Endpoint Protection on VMs” → +6 points to Secure Score when resolved.

2. Azure Policy

Purpose:
Automate compliance and configuration management.
Azure Policy ensures all resources comply with organizational standards.

How It Works

Azure Policy evaluates every resource against defined **rules** and takes action:

- **Effect:** What happens if the policy is violated (e.g., deny, audit, append, deployIfNotExists).
- **Assignment:** Which scope the policy applies to (management group, subscription, RG).
- **Initiative:** A collection of multiple policies grouped together for frameworks (e.g., "CIS Azure Benchmark").

Common Policy Examples

Policy	Effect
Disallow public IPs on NICs	Deny
Enforce resource tagging	Append or Audit
Require encryption on storage accounts	Deny
Automatically deploy Log Analytics agent	deployIfNotExists

Blueprints (Deprecated)

Azure Blueprints (legacy feature) combined Policies, Role Assignments, and ARM Templates for environment governance.
Now replaced by **Terraform with Policy as Code** or **Azure Landing Zones** for enterprise deployments.

Best Practices

- Apply policies at **management group** level for consistency.
- Use **initiative definitions** to align with frameworks (e.g., NIST SP 800-53).

- Combine with Defender for Cloud for real-time compliance evaluation.

3. Azure Monitor & Log Analytics

Azure Monitor is the platform for collecting metrics, logs, and alerts across Azure services.

Log Analytics Workspace stores the logs and supports **KQL (Kusto Query Language)** for analysis.

Common Log Sources

Source	Description
Activity Logs	Subscription-level operations (e.g., resource creation).
Azure AD Sign-in Logs	Authentication events and MFA results.
NSG Flow Logs	Traffic flow (allowed/denied packets).
Defender for Cloud Alerts	Detected threats or policy violations.
Resource Logs	Service-specific diagnostic data (Key Vault, SQL, etc.).

Key KQL Examples

Purpose	KQL Query
Failed sign-ins	`SigninLogs
VM restarts	`AzureActivity
Threat alerts	`SecurityAlert
Suspicious IP logins	`SigninLogs

Action Groups and Alerts

You can configure alerts that trigger:

- Email, SMS, Teams notifications
- Automation Runbooks
- Logic Apps (e.g., auto-remediate VM configuration)

Example:
If a new public IP is assigned, trigger a Logic App that automatically removes it or alerts the SOC.

4. Microsoft Sentinel (SIEM & SOAR)

Purpose:
Microsoft Sentinel is a **cloud-native SIEM** (Security Information and Event Management) and **SOAR** (Security Orchestration, Automation, and Response) solution.

It aggregates logs from across your environment and applies analytics, automation, and AI for threat detection and response.

Core Components

Component	Description
Data Connectors	Integrate data from Azure AD, Office 365, AWS, on-prem logs, firewalls, etc.
Analytics Rules	Define detection logic using KQL (e.g., brute-force login).
Workbooks	Visual dashboards for trends and insights.
Playbooks	Logic App-based automation workflows (SOAR).
Hunting Queries	Manual or automated searches for IOCs.
Incidents	Grouped alerts with investigation timelines and actions.

Common Sentinel Use Cases

Use Case	Description
Identity Compromise Detection	Correlate sign-in anomalies from Entra ID + Defender.
Insider Threats	Track excessive data downloads or policy bypasses.
Malware Spread	Detect lateral movement via network logs.
Phishing Investigation	Link Outlook logs, Defender alerts, and AAD events.

SOAR Automation Example

1. Sentinel detects repeated failed logins from a foreign country.
2. A **Playbook** automatically triggers to:
    - Disable the account.
    - Notify admin via Teams.
    - Open an incident in ServiceNow.
3. Analyst reviews and closes with justification.

Hunting Queries (Examples)

Threat Type	KQL Example
Brute-force attacks	`SigninLogs
VM Port Scanning	`AzureNetworkAnalytics_CL
Data exfiltration	`StorageBlobLogs
Suspicious privilege elevation	`AuditLogs

5. Security Alerts & Incident Response

Purpose:
Efficiently detect, prioritize, and handle incidents before they escalate.

Azure Alert Flow

1. **Defender for Cloud or Sentinel detects anomaly**
2. **Alert created** (security alert or policy violation)
3. **Incident generated** (grouped alerts)
4. **SOC triages** using dashboards and playbooks
5. **Automated or manual response** executed
6. **Post-incident review** documents findings

Alert Severity Levels

Level	Meaning
High	Active threat or confirmed compromise (e.g., malware found)

Medium	Suspicious or abnormal behavior
Low	Minor configuration issue or info event
Informational	No immediate threat, for tracking only

Incident Response (IR) Lifecycle

Phase	Description
Preparation	Policies, training, detection rules, playbooks
Detection	Alerts and SIEM monitoring
Containment	Isolate affected resources, block access
Eradication	Remove threat (malware, misconfigurations)
Recovery	Restore systems and re-enable access
Lessons Learned	Update detections and policies

6. Governance and Continuous Improvement

Security isn't one-time setup — Azure provides tools to measure, enforce, and evolve your posture.

Key Governance Tools

Tool	Purpose
Microsoft Defender for Cloud	Ongoing recommendations and threat protection
Azure Policy	Compliance enforcement and remediation
Microsoft Purview	Data governance and classification
Sentinel + Playbooks	Automated response and investigation
Secure Score / Compliance Score	Continuous benchmarking of security readiness

Best Practices

- Regularly review **Secure Score** and **Sentinel incidents**.
- Conduct **Access Reviews** for privileged users.
- Enable **Azure Monitor and Diagnostic Logs** on all critical resources.
- Apply **role separation** — SOC Analysts shouldn't hold Global Admin.
- Automate **remediation** where possible (Logic Apps, Policies).

- Document IR playbooks and update them quarterly.

Azure Services Summary

Domain 1 – Secure Identity and Access

Category	Service / Feature	Purpose / Function
Identity Platform	**Microsoft Entra ID**	Central identity management, authentication, and authorization (formerly Azure AD).
Access Control	**Role-Based Access Control (RBAC)**	Assign granular permissions to users, groups, and managed identities.
	Custom Roles	Define JSON-based permission sets for custom access needs.
Privileged Access	**Privileged Identity Management (PIM)**	Just-in-time elevation, approvals, MFA for sensitive roles.
	Permissions Management (CloudKnox)	Discover and remediate excessive permissions across multicloud.
Authentication Security	**Multi-Factor Authentication (MFA)**	Add extra verification (app, token, FIDO2).
	Conditional Access	Policy-based access control (e.g., location, device, risk).
Application Security	**Enterprise Applications**	SaaS integrations with SSO and access controls.
	App Registrations	Register custom apps, APIs, and manage service principals.
	Managed Identities	Securely authenticate Azure resources without secrets.
Monitoring & Logs	**Sign-in Logs / Audit Logs**	Track authentication and directory changes.

Domain 2 – Secure Networking

Category	Service / Feature	Purpose / Function
Network Segmentation	**Virtual Networks (VNets)**	Logical isolation for Azure resources.
	Subnets / Address Spaces	Segment workloads within VNets.
	Network Security Groups (NSGs)	Stateful inbound/outbound traffic control (Layer 3/4).
	Application Security Groups (ASGs)	Group VMs by role for easier rule management.
Routing Control	**User-Defined Routes (UDRs)**	Custom routing for traffic steering (e.g., through firewalls).
	Virtual Network Manager	Centralized policy management for multiple VNets.
Connectivity	**VNet Peering**	Private, low-latency connectivity between VNets.
	VPN Gateway	IPSec/IKE tunneling for hybrid or remote connectivity.
	ExpressRoute	Dedicated private fiber connection to Azure.
	Virtual WAN	Microsoft-managed global hub-and-spoke connectivity.
Private Access	**Service Endpoints**	Extend VNet identity to PaaS services via public endpoint.
	Private Endpoints / Private Link	Assign private IPs for fully internal service access.
Network Security	**Azure Firewall (Basic, Standard, Premium)**	Stateful, cloud-native firewall with threat intelligence.
	Application Gateway + WAF	Layer 7 load balancing and OWASP Top 10 protection.
	Azure Front Door	Global edge load balancing, CDN, and DDoS mitigation.
	Azure DDoS Protection (Basic/Standard)	Volumetric and protocol-level DDoS mitigation.
Monitoring	**Network Watcher**	Flow logs, packet capture, and connection troubleshooting.

	Azure Monitor (Network Metrics)	Collect metrics, logs, and create alerts.

Domain 3 – Secure Compute, Storage, and Databases

Category	Service / Feature	Purpose / Function
Compute Security	**Azure Virtual Machines**	Secure compute with Bastion, JIT, encryption, Defender.
	Azure Bastion	Browser-based RDP/SSH without public IPs.
	Just-in-Time (JIT) VM Access	Temporary, auditable port access via Defender for Cloud.
	Azure Disk Encryption (ADE)	OS/data disk encryption using BitLocker/DM-Crypt.
	Encryption at Host / Double Encryption	Adds extra layer for data in transit and at rest.
	Confidential VMs	Hardware-based TEE isolation using Intel SGX or AMD SEV-SNP.
Containers	**Azure Kubernetes Service (AKS)**	Managed Kubernetes clusters with Defender integration.
	Azure Container Registry (ACR)	Private registry with image scanning and signing.
	Azure Container Instances (ACI)	Run serverless containers on demand.
	Azure Container Apps (ACA)	Managed microservice platform with internal/external ingress.
Serverless / APIs	**Azure API Management (APIM)**	API gateway enforcing auth, rate limits, and network isolation.
Storage Security	**Azure Storage Accounts**	Blob, File, Queue, Table storage.
	Shared Access Signatures (SAS)	Temporary scoped access tokens for limited permissions.
	Azure AD / RBAC Integration	Identity-based access to Blob and File services.
	Customer-Managed Keys (CMK)	Key Vault-based encryption control.
	Soft Delete / Versioning / Immutable Storage	Data recovery and compliance features.
Databases	**Azure SQL Database / Managed Instance**	PaaS database with TDE, auditing, and Defender integration.

	Dynamic Data Masking (DDM)	Mask sensitive data in queries.
	Transparent Data Encryption (TDE)	Encrypt data files and backups.
	Always Encrypted	Client-side encryption for sensitive columns.
	Defender for SQL	Detect injection, brute-force, and anomalies.

Domain 4 – Secure Azure Using Microsoft Defender for Cloud and Microsoft Sentinel

Category	Service / Feature	Purpose / Function
Governance	**Azure Policy**	Define and enforce compliance rules across Azure.
	Initiatives / Effects (Deny, Audit, Modify)	Aggregate and apply policy sets.
	Azure Resource Graph	Inventory and query resources across tenants.
	Tags / Resource Manager	Metadata and organization for assets.
Key Management	**Azure Key Vault**	Secure secrets, keys, and certificates.
	Managed HSM	Hardware Security Module with CMK support.
Security Posture (CSPM)	**Defender for Cloud**	Assess compliance, secure score, and recommendations.
	Secure Score	Quantitative measurement of environment security.
	Defender CSPM	Agentless scanning for misconfigs and secret leaks.
Workload Protection (CWPP)	**Defender for Servers**	EDR, vulnerability management for VMs.
	Defender for Containers	Protects AKS and ACR.
	Defender for Storage	Malware and anomaly detection in Storage Accounts.

	Defender for Databases	SQL/CosmosDB threat protection.
	Defender for APIs / Key Vault / Resource Manager	Protection for specific services.
Threat Detection & Response	**Microsoft Sentinel**	SIEM + SOAR for centralized monitoring and automation.
	Data Connectors	Ingest logs from Azure, M365, AWS, and Syslog.
	KQL Analytics Rules	Custom or built-in detection queries.
	Logic Apps (Playbooks)	Automated response workflows.
Monitoring Infrastructure	**Azure Monitor**	Collect metrics, create alerts, and track health.
	Data Collection Rules (DCRs)	Control what telemetry is gathered and where it's sent.