Microsoft Azure Security Engineer (AZ-500)

Quick Exam Refresher

This is your condensed, **high-impact review guide** for the AZ-500: Microsoft Azure Security Technologies certification. It's built for fast recall and confidence-building right before test time — not deep instruction.

AZ-500 Domains

Each domain carries different weight. Expect most of your questions from identity, platform protection, and security operations:

- **Domain 1:** Manage Identity and Access (25-30%)
- **Domain 2:** Secure Networking (20-25%)
- **Domain 3:** Secure Compute, Storage, and Databases (20-25%)
- **Domain 4:** Manage Security Operations (25-30%)

Quick Reminder: How the Exam Works

- **Number of Questions:** 40–60
- **Format:** Multiple choice, multiple response, hot area, code snippets, drag-and-drop, and case studies
- **Time Limit:** 150 minutes
- **Passing Score:** 700 / 1000
- **Test Provider:** Pearson VUE (onsite or online via Examity or VUE)

IDENTITY & ACCESS MANAGEMENT (IAM)

Resource Roles

The core RBAC roles define broad access levels to manage or view any Azure resource, while the specialized roles focus on specific functional areas like security, policy, billing, or identity without granting full resource control.

The Core 3

Role	Description
Owner	Full control of all resources and can manage access permissions.
Contributor	Full control of resources but cannot manage RBAC access.
Reader	View-only access to resources and configurations.

The Specialized Built-in Roles

Role	Description
User Access Administrator	Assign and manage RBAC role permissions without owning all resources.
Security Admin	Manage security settings, Defender for Cloud configurations, and recommendations.
Security Reader	View security alerts, recommendations, and compliance results (no modify rights).
Policy Contributor	Create, edit, and assign Azure Policy and Initiative definitions (cannot manage access).
Blueprint Contributor	Create and publish Blueprints but cannot assign them.
Billing Reader	View billing and cost data (no configuration changes).
Managed Identity Operator	Assign or reset managed identities for Azure resources.

Scope hierarchy: Management Group → Subscription → Resource Group → Resource (inheritance downward)

Evaluation order: Deny > DenyAssignments > Allow (permissions inherited unless explicitly denied)

Deny assignments: Created by Azure or Blueprints; override all allows; users cannot author them directly.

Azure AD Roles

Azure AD built-in roles control *directory-level permissions* in **Entra ID** (e.g., manage users, groups, MFA, Conditional Access) — RBAC governs resources in Azure, AD roles govern identities and access policies.

Role	Description
Global Administrator	Full control of Azure AD; can manage users, groups, directory settings, app consent, and enable PIM.
Security Administrator	Manages Conditional Access, Identity Protection, MFA, and security reports.
Privileged Role Administrator	Manages PIM and Azure AD role assignments; can activate/deactivate privileged roles.
Application Administrator	Manages app registrations, consent, and API permissions for applications.
Cloud Application Administrator	Similar to Application Admin but cannot manage CA or organization-wide consent.
Authentication Administrator	Can reset passwords and re-register MFA for non-admin users. Common helpdesk role.
Password Administrator	Resets passwords for users and some limited admins (not Global/Privileged).
Billing Administrator	Manages subscriptions, invoices, and payment methods.
User Administrator	Creates and manages users/groups; resets most passwords.
Compliance Administrator	Manages compliance, audit, retention, and labeling settings.
Reports Reader	Reads sign-in/audit logs and access reports (for monitoring/Sentinel).

Exam cue:
→ *Azure AD (Entra ID) roles control directory-level permissions; RBAC controls resource-level access.*

App Registration vs Service Principal

• **App Registration** → Global definition of an app in Azure AD.
• **Service Principal (SP)** → App's identity instance in a specific tenant; used for authentication & access control.
• **Managed Identity** → Auto-managed SP tied to a resource.

- **System-assigned:** Lifecycle tied to resource.
- **User-assigned:** Reusable across resources.

Exam triggers:
• "App needs access to Key Vault without user sign-in" → Application permission or Managed Identity
• "App acts on behalf of a user" → Delegated permission with admin consent

Conditional Access

• Enforces sign-in controls based on **user, device, app, location, and risk**.
• Evaluates **User Risk** and **Sign-in Risk** (from Identity Protection).
• Common actions: require MFA, block access, or require compliant device.

Examples:

• Block legacy auth → *Client App condition*
• Require MFA if risky sign-in → *Sign-in risk policy*
• Force password reset if compromised → *User risk policy*

Licensing note: Risk-based Conditional Access and Identity Protection require **Entra ID P2**.

Azure AD Identity Protection — Risk Levels

Risk Type	Triggered Event	Level	Action
Leaked credentials	Found in public breach	High	Force password reset
Unfamiliar location/device	Unknown IP or device	Medium	Require MFA
Impossible travel	Geographically impossible sequence	Medium	Require MFA/block
Suspicious IP or TOR node	Known malicious address	Medium	Require MFA
Malware-linked or bot sign-ins	Automated pattern	High	Block + reset
Atypical user activity	ML-detected deviation	Low–Medium	Notify or enforce MFA

- **User risk** = identity-level (e.g., leaked password)
- **Sign-in risk** = session-level (e.g., suspicious location)

Policies can enforce:
- Require password reset for **user risk ≥ Medium**
- Require MFA for **sign-in risk ≥ Medium**

Multi-Factor Authentication (MFA)

- Second verification factor (password + something you have/are)
- **Methods:** Authenticator app, SMS, voice, FIDO2 key
- **Enabled via:** Conditional Access, per-user MFA, or Identity Protection

Key facts:

- PIM activation requires MFA (even if user is already signed in).
- **Security Defaults** enforce MFA for admins automatically.
- Trusted IPs/compliant devices can be excluded.
- Conditional Access can target specific apps or groups.
- "Require MFA on risky sign-in" → configure *Sign-in risk policy*.
- Reports: Azure AD → Security → MFA insights.

MFA Flow Example:

1. User login attempt → risk calculated.
2. Conditional Access evaluates.
3. Medium/high risk → require MFA or block.
4. If PIM activation → MFA triggered again.

Privileged Identity Management (PIM)

• **Eligible:** User can activate privilege on demand.
• **Active:** Role currently active.
• Requires MFA on activation, optional approval, justification, and time limit.
• Reduces standing admin rights; logs all activations.
• Integrates with **Access Reviews** for continuous validation.
• Sends notifications on activation/expiration.
Tip: PIM = time-bound least-privilege control (not replication; use Blueprints for that).

Access Reviews

• Validates ongoing access to roles, groups, or apps.
• Reviewers:

- Members (self)
- Group Owners
- Selected users (auditors/compliance)
  • Connects with PIM and Conditional Access; non-response can revoke access.

KEY VAULT & ENCRYPTION

Access Controls

• **RBAC** → Vault-level management and configuration permissions.
• **Access Policy** → Object-level permissions (get, list, add, delete).
• **Best practice:** Use RBAC for administrative control and Access Policies for object access when legacy integration requires.
• **Deny assignments:** Service-created (Blueprints, etc.), override all role allows.

Soft Delete & Purge Protection

• **Soft Delete:** Retains deleted items for **90 days** by default.
• **Purge Protection:** Prevents permanent deletion during retention.
• Both must be **enabled** to meet compliance (HIPAA, ISO, CIS benchmarks).

Key Management

• **Customer-Managed Keys (CMK):** Stored in Azure Key Vault or Managed HSM.
• **Microsoft-Managed Keys (MMK):** Default encryption for most services.
• CMKs are used by:

- Azure Disk Encryption (BitLocker / DM-Crypt)
- SQL Transparent Data Encryption (TDE)
- Azure Storage (Blob, Files, and optionally Table/Queue if enabled at creation)

Exam traps:

• CMK now supported for Table/Queue storage if enabled at creation (was not earlier).
• Basic-tier VMs → No Azure Disk Encryption support.
• Key Vault must have **Soft Delete + Purge Protection** enabled before setting up encryption.

DEFENDER FOR CLOUD

Plans

- **Foundational CSPM (Free):**

Continuous posture management, recommendations, secure score, and regulatory compliance dashboard.

- **Defender CSPM (Paid):**

Adds attack path analysis, advanced exposure mapping, and cloud security graph.

- **Defender for Servers (Plan 1 / Plan 2):**

P1 → Basic endpoint protection, alerting, integration with Microsoft Defender for Endpoint (MDE).

P2 → Includes JIT VM Access, vulnerability management, adaptive controls, and threat analytics.

- **Auto-provisioning:** Deploys Defender agent or AMA automatically when enabled.
- **Compliance view:** Maps to CIS, NIST, and ISO 27001 benchmarks.

Just-in-Time (JIT) VM Access

• Temporarily opens RDP/SSH for authorized users.
• Requires **Defender for Servers Plan 2** and **NSG or Azure Firewall** (not Load Balancer).
• Automatically updates NSG rules during session.
• Supports approval workflows and custom time windows.

Adaptive Application Controls

- Uses machine learning to whitelist known apps and block unknown executables.
- Recommends rules based on observed behavior.

Adaptive Network Hardening

- Suggests NSG rules based on traffic flow analysis.
- Can auto-apply recommendations via Defender policy.

Vulnerability Assessment

- Uses **Microsoft Defender Vulnerability Management (MDVM)** instead of Qualys.
- Supports agent-based or agentless scanning.
- Available via Defender for Servers P2 and integrated into MDE dashboards.

LOGGING & MONITORING

Activity Log

• Captures **control-plane** events (resource creation, deletion, RBAC changes).
• Retention: **90 days by default**.
• Export to **Log Analytics, Event Hub, or Storage** for long-term retention.

Diagnostic Settings

• Capture **data-plane** operations (read/write, API calls).
• Required for continuous export.
• Destinations:

- **Log Analytics** → Query & correlate
- **Event Hub** → Stream to external SIEM
- **Storage** → Archive logs long-term

Log Analytics Workspace

• Centralized log collection for Azure Monitor, Defender, and Sentinel.
• Agents (AMA) require **Workspace ID + Key** for onboarding.
• Default retention: 30 days (extendable to 730).
• Supports role-based access at workspace level.

KQL Snippets

```
SigninLogs | where ResultType != 0 | summarize Fails = count() by UserPrincipalName
AzureActivity | where OperationName == "Delete" | project Caller, Resource
```

Alert Types

Type	Description	Trigger Speed
Metric Alert	Threshold-based (CPU, latency)	< 1 minute
Log Alert	Based on KQL queries	Few minutes
Activity Alert	Control-plane action trigger	Immediate

Azure Sentinel (Microsoft Sentinel)

- Cloud-native **SIEM + SOAR** built on Log Analytics.
- **Connectors:** Ingest data (Defender, Entra ID, M365, AWS, Syslog).
- **Analytic Rules:** Define detection logic (KQL-based).
- **Playbooks (Logic Apps):** Automate incident responses (disable user, isolate VM).
- Requires **Logic App Contributor** for playbook automation.
- Supports **Hunting Queries, Workbooks, and Notebooks** for threat hunting.

NETWORK SECURITY

Network Security Group (NSG)

- Filters inbound/outbound Layer 4 traffic (IP, Port, Protocol).
- Can be applied at **subnet** or **NIC** level.
- **Priority:** 100–4096 (lower = higher priority).
- **Default inbound:** Deny all.
- **Default outbound:** Allow all.
- Rules processed top to bottom; first match wins.
- Supports service tags (e.g., Internet, AzureLoadBalancer).

Application Security Group (ASG)

- Logical grouping of NICs within **same VNet and region**.
- Combine NSG + ASG for scalable rule management.
- Cannot span VNets or regions.
- Useful for dynamic segmentation (e.g., “WebTier” to “DBTier”).

Azure Firewall

- Stateful Layer 4–7 firewall with centralized outbound control.
- Features:
    - DNAT/SNAT
    - Threat intelligence-based filtering
    - FQDN & URL filtering
    - TLS inspection + IDPS (**Premium SKU**)
        - Logs to Log Analytics or Event Hub.
        - Can enforce outbound traffic restrictions and egress control.
        - Deployed in **hub-and-spoke** or **secured virtual hub** models.

Application Gateway (WAF)

• Layer 7 reverse proxy for web traffic.
• Performs **TLS termination**, cookie-based affinity, and SSL offloading.
• **Web Application Firewall (WAF)** defends against OWASP Top 10 threats.
• Supports both **OWASP CRS 3.x** and custom rules.
• Can integrate with **AKS** using the **Application Gateway Ingress Controller (AGIC)** — optional; AKS can also use NGINX or App Routing Ingress.

Azure Front Door

• Global Layer 7 load balancer with **WAF** and **CDN caching**.
• Routes traffic across multiple regions using health probes.
• Supports DDoS protection and global failover.
• Ideal for high-availability web applications or APIs.

Private Link / Private Endpoint

• Assigns a **private IP** from your VNet to a PaaS service (e.g., Storage, SQL, Key Vault).
• Traffic stays entirely on the **Azure backbone**, never on public internet.
• Prevents data exfiltration and enables compliance isolation.

Service Endpoint

• Extends a VNet to PaaS services using **public endpoints**, but restricts access by VNet/subnet.
• Traffic still uses Azure public IP but remains within Azure datacenter backbone.
• Easier setup, less isolation than Private Link.

VNet Peering

• Provides private, low-latency connectivity between VNets.
• Peered VNets act as one network for routing, but **DNS zones remain separate**.
• Does not support transitive routing.

STORAGE & DATA PROTECTION

Azure Storage Security

- Restrict access with **Storage Firewall + VNet rules**.
- Enable **Soft Delete** for blob recovery (default 7–365 days).
- Enable **Immutability Policy (WORM)** for regulatory compliance (e.g., SEC 17a-4).
- Use **Stored Access Policies** to revoke SAS tokens instantly.
- Only regenerate account keys if SAS not linked to a stored access policy.
- Encryption at rest is enabled by default using Microsoft-managed keys or CMK.

Defender for Storage

- Detects **malware, unusual access patterns, and data exfiltration**.
- Uses machine learning on blob-level telemetry.
- Integrated with Defender for Cloud dashboard.

Azure Backup & Immutable Vault

- Backs up VMs, SQL, and file shares to a **Recovery Services Vault**.
- Retention up to **99 years**.
- **Immutable Vaults** prevent deletion/modification until retention expires.
- To delete a vault, immutability must first be explicitly disabled.
- Supports cross-region restore for disaster recovery.

AZURE SQL SECURITY

Transparent Data Encryption (TDE)

• Encrypts database, logs, and backups at rest.
• Uses service-managed key or CMK stored in Key Vault.
• Required for most compliance frameworks (HIPAA, PCI DSS).

Always Encrypted

• Encrypts sensitive columns on the **client side**.
• Keys:

- **Column Encryption Key (CEK)** → encrypts column data
- **Column Master Key (CMK)** → encrypts CEK metadata
  • Server never sees decrypted values.
  • Used when app must handle encryption independently.

Advanced Threat Protection (Defender for SQL)

• Detects suspicious activity such as:

- SQL injection
- Brute-force login attempts
- Data exfiltration or anomalous queries
  • Sends alerts to Defender for Cloud and Azure Security Center.
  • Includes **Vulnerability Assessment reports** (weekly).

POLICY, BLUEPRINTS & GOVERNANCE

Policy Effects

• **Deny** → Blocks creation of non-compliant resources.
• **Audit** → Logs non-compliance (no enforcement).
• **AuditIfNotExists** → Flags missing related resource (e.g., diagnostic setting).
• **DeployIfNotExists** → Automatically deploys missing resources (requires Managed Identity).

Initiatives

• Collections of related policies mapped to frameworks (CIS, NIST, ISO 27001).
• Provide aggregate compliance scoring and inheritance.

Blueprints

• Bundle of **RBAC assignments**, **Policies**, and **ARM templates** for consistent deployment baselines.
• Assigned at **management group** or **subscription** level.
• Common use: replicate compliance baseline across multiple subscriptions.
• Replaced by **Template Specs + Policy Initiatives** for new deployments (Blueprints remain supported for existing use).

Resource Locks

• **Delete lock** → Prevents deletion only.
• **ReadOnly lock** → Prevents modification *and* operational actions such as start, stop, restart, or scaling VMs.
• Locks inherit down the resource hierarchy.
• To remove, you must first delete the lock itself.

SECURITY AUTOMATION

Azure Update Manager (2025 successor to Update Management)

- Replaces the classic Automation Account-based model.
- No longer requires a **Log Analytics workspace** (integration optional).
- Supports dynamic scoping and scheduling for **Azure, Arc, and on-prem VMs**.
- Integrates with **Defender for Cloud** for patch compliance.

Playbooks (Logic Apps)

- Triggered automatically from **Microsoft Sentinel incidents**.
- Automate remediation such as disabling a user, isolating a VM, or posting alerts to Teams.
- Requires the **Logic App Contributor** role in the Sentinel resource group.

Policy Remediation

- Use **DeployIfNotExists** to automatically deploy missing agents or configurations (e.g., Defender, AMA, Key Vault diagnostics).
- Supports **bulk remediation tasks** from the Azure Policy dashboard.

HYBRID SECURITY

Azure Arc

• Extends Azure management to **on-premises, AWS, and GCP** servers.
• Enables use of **Defender**, **Policies**, **Update Manager**, and **Log Analytics** on non-Azure machines.
• Azure Arc SQL Server adds advanced data-security assessments and TDE enforcement visibility.

Agents

• **MMA (Log Analytics Agent)** → Legacy, deprecated.
• **AMA (Azure Monitor Agent)** → Current default for all new VMs and Arc machines.
• AMA supports multiple data streams (Metrics, Logs, Custom tables) with simplified configuration.

REAL-WORLD SCENARIOS

These are the *most frequently recurring scenario patterns* in the AZ-500 exam and in Microsoft Learn case studies.

They test whether you can choose the correct Azure feature for a specific security, governance, or monitoring situation — not syntax or configuration.

Identity & Access Scenarios

Question Cue	Correct Answer / Explanation
A user must have elevated privileges only when needed	**Azure AD Privileged Identity Management (PIM)** → Assign eligible roles with MFA, justification, and approval to reduce standing admin rights.
Prevent permanent admin accounts from persisting	**PIM time-bound activation** → Ensures admins revert to non-privileged after expiration; triggers alerts and audit entries.
View who activated Global Admin temporarily	**PIM Audit Log** → Shows activation, approval, and duration of privileged sessions.
Require MFA for risky sign-ins only	**Identity Protection + Conditional Access** → Configure sign-in risk policy (medium/high = require MFA).
Detect sign-ins from anonymous or TOR IPs	**Entra ID Identity Protection report** → Flags sign-ins from high-risk IP categories.
Rotate application secrets automatically	**Azure Key Vault** → Store and auto-rotate app secrets with Event Grid + Function trigger.
Analyze failed sign-in attempts by user	**SigninLogs (KQL)** → ` SigninLogs

Governance & Compliance Scenarios

Question Cue	Correct Answer / Explanation
Ensure identical RBAC and Policy setup across subscriptions	**Azure Blueprints / Initiatives** → Apply consistent RBAC, Policy, and ARM template baselines. *(Modern replacement: Template Specs + Initiatives.)*
Enforce that every resource has a tag named “CostCenter”	**Azure Policy (Deny effect)** → Rejects creation of untagged resources.
Audit if a diagnostic setting is missing	**Azure Policy (AuditIfNotExists)** → Detects resources without logging enabled.
Automatically deploy missing agent extensions	**Azure Policy (DeployIfNotExists)** → Remediates non-compliant VMs with AMA/Defender agents.

Apply CIS or NIST framework baseline	**Azure Policy Initiative** → Built-in definitions mapped to compliance standards.
Prevent accidental deletion of critical resources	**Resource Lock (Delete)** → Must remove lock before deletion.
Prevent configuration or operational changes	**Resource Lock (ReadOnly)** → Blocks edits and operations (start, stop, restart).
Verify least-privilege adherence over time	**Access Reviews (PIM)** → Periodic re-validation of role or group membership.

Data & Storage Scenarios

Question Cue	Correct Answer / Explanation
Restrict storage access to internal networks only	**Private Endpoint** → Assigns private IP; traffic stays on Azure backbone.
Detect malware or unusual access in blob uploads	**Defender for Storage** → Monitors and alerts on suspicious or anomalous operations.
Protect backups from deletion or tampering	**Immutable Vault (Azure Backup)** → Enforces retention lock until expiry.
Rotate or revoke shared access links immediately	**Stored Access Policy** → Revokes SAS instantly by modifying or deleting the policy; regenerate account keys only if no policy used.
Store logs for 2 years and enable queries	**Log Analytics Workspace** → Extend retention up to 730 days; query with KQL.
Encrypt data at rest using own keys	**Customer-Managed Keys in Key Vault** → Used by Storage, SQL TDE, and Disk Encryption.
Prevent permanent deletion of secrets	**Enable Purge Protection** in Key Vault → Required for compliance frameworks (CIS, ISO, HIPAA).

Network & Perimeter Protection Scenarios

Question Cue	Correct Answer / Explanation
Control outbound internet traffic from VMs	**Azure Firewall** → Centralized egress filtering with FQDN & DNAT/SNAT rules.
Inspect HTTPS traffic for threats	**Azure Firewall Premium** → TLS inspection + IDPS for deep packet scanning.
Protect a web application from SQL injection	**Application Gateway (WAF mode)** → OWASP CRS ruleset filters malicious input.
Protect global web apps across regions	**Azure Front Door + WAF** → Global Layer-7 load balancing with DDoS and WAF integration.
Allow only secure private access to PaaS databases	**Private Link / Private Endpoint** → Assigns private IP to SQL or Storage service.

Suggest optimal NSG rules based on traffic	**Adaptive Network Hardening (Defender for Cloud)** → ML-based NSG recommendations.
Create temporary RDP/SSH access for admins	**Just-In-Time VM Access (Defender for Servers P2)** → Opens NSG ports on demand with auto-close.

Compute, Endpoint & Application Scenarios

Question Cue	Correct Answer / Explanation
Scan all VMs for vulnerabilities	**Defender for Servers Plan 2** → Uses Microsoft Defender Vulnerability Management (MDVM) agentless or with MDE integration.
Automatically patch VMs across hybrid environments	**Azure Update Manager** → Replaces classic Automation Update Management.
Whitelist only approved executables	**Adaptive Application Controls** → Learns baseline and blocks unknown apps.
Detect fileless malware or suspicious process behavior	**Microsoft Defender for Endpoint (MDE) integration** → Unified alerts surfaced in Defender for Cloud.
Apply policies to on-prem or multi-cloud servers	**Azure Arc** → Enables Defender, Update Manager, and Policy on non-Azure systems.

Monitoring & Incident Response Scenarios

Question Cue	Correct Answer / Explanation
Find who deleted a VM or resource	**Activity Log** → Control-plane audit (who, what, when).
Detect repeated failed logins	**KQL Query on SigninLogs** → Used in Sentinel or Log Analytics.
Investigate sign-ins from suspicious IPs	**Sentinel + KQL** → Correlate with threat-intel feeds and geolocation.
Centralize logs from Arc servers and Azure VMs	**Log Analytics Workspace** → Unified ingestion for Sentinel/Monitor.
Automate incident response on alert trigger	**Playbooks (Logic Apps)** → Example: disable user, isolate VM, send Teams alert.
Correlate Defender alerts and raise incidents	**Microsoft Sentinel Analytic Rules** → Detect and escalate anomalies into incidents.
Forward logs to external SIEM or data lake	**Diagnostic Settings → Event Hub / Storage** → Enables streaming and retention.