

Microsoft AZ-500 Cheat Sheet

One-page cram sheet for Azure identity, networking, compute/storage security, Defender for Cloud, and Sentinel.

Best for	Focus	Use with
Last review before drills or exam day	High-yield Azure security controls and exam decision patterns	Use with the quick summary for rapid refresh

1. Secure identity and access

RBAC and custom roles	Know built-in roles, custom roles, PIM, and least-privilege assignment strategy.
Conditional Access	Use context-aware controls like MFA, device state, and user risk to protect Azure access.
Managed identities	Prefer managed identities over embedded secrets for workload-to-service auth.
App registrations	Understand service principals, permission consent, and delegated vs application permissions.

2. Secure networking

Network boundaries	VNet design, NSGs, Azure Firewall, DDoS Protection, and private endpoints shape security posture.
App protection	WAF, Application Gateway, Front Door, and segmentation controls often appear together.
Private access	Use service/private endpoints and private link patterns when public exposure is unnecessary.
Network visibility	NSG flow logs and monitoring support detection and troubleshooting.

3. Secure compute, storage, and databases

Compute hardening	Use Defender recommendations, patching, JIT VM access, and secure admin practices.
Storage security	RBAC, SAS, keys, private access, immutability, and encryption all matter.
Database protection	Think SQL, Cosmos DB, and data-layer controls like threat protection and audit trails.
Secrets and keys	Key Vault is central for certificates, secrets, and key management.

4. Defender for Cloud and Sentinel

Defender for Cloud	This is now the heaviest exam block, so know posture, recommendations, and plan coverage well.
---------------------------	--

Sentinel basics	Workbooks, analytics rules, incidents, playbooks, connectors, and investigation flow are high-yield.
Threat protection	The exam likes scenarios where visibility, response, and security posture connect together.
Vulnerability remediation	Findings should turn into prioritized fixes, not just dashboards.

5. Practical exam mindset

Choose built-in security first	Managed Azure security controls often beat custom complexity.
Least privilege + logging	These two ideas improve many scenarios at once.
Identity + network + monitoring	Strong answers often combine all three rather than focusing on one control.
Compliance-aware choices	The best answer is secure and operationally realistic.