

Microsoft SC-100 Quick Summary

Fast 3-5 minute refresh for the core ideas, comparisons, and architecture traps that matter most on the current exam.

Best for Ultra-fast memory refresh	Focus Definitions, shortcuts, and common exam traps	Use with Use with the cheat sheet for deeper review
--	---	---

1. Fast refresh

SC-100 focus	Strategy, operations/identity/compliance, infrastructure, apps/data.
Think architecture	This is not a narrow product exam.
Identity is central	Many good answers start with identity and privileged access design.
Integrated security wins	Strong solutions combine posture, visibility, protection, and governance.

2. High-yield comparisons

Sentinel vs Defender XDR	SIEM/SOAR and broad incident coordination versus integrated detection/response workloads.
PIM vs RBAC	Privilege lifecycle control differs from base authorization assignment.
Purview vs Defender	Governance/information protection differs from threat protection and posture management.
Architecture vs implementation	SC-100 usually wants design direction, not one exact click path.

3. Security shortcuts

Zero Trust	Strong default design lens.
PIM	Reduce standing privilege.
Sentinel playbooks	Automate where response benefits from consistency.
Defender for Cloud	Posture and recommendation-driven improvement.

4. Exam traps

One product is rarely enough	The exam prefers integrated architecture.
Compliance is not only documentation	It needs technical enforcement and evidence.
Monitoring without action is weak	Visibility should connect to response and improvement.

**Least privilege still applies
to architecture**

Convenience-heavy designs are often wrong.
