

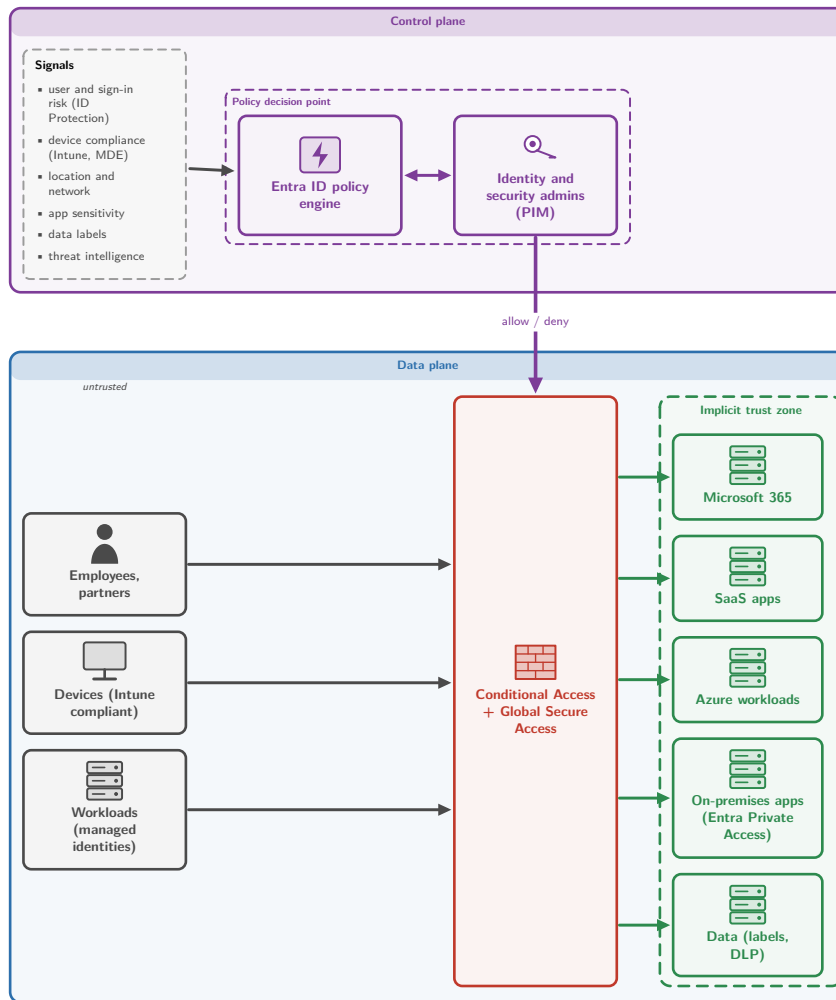


Zero Trust Strategy and Microsoft Security Frameworks

SC-100 domain 1, Design solutions that align with security best practices and priorities (part 1) | Zero Trust principles and RaMP, MCRA, Microsoft cloud security benchmark, CAF Secure methodology, Well-Architected security pillar, translating business goals into a security strategy

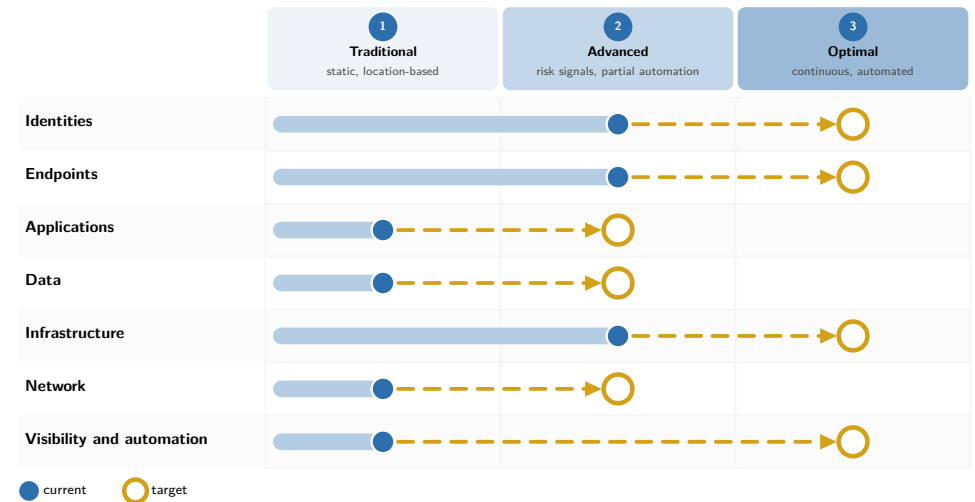
SC-100 Domain 1 Zero Trust MCSB MCRA

Zero Trust as the strategy



Every access decision runs through policy: Entra Conditional Access as PDP, enforcement at apps, network and data

Technology area	Optimal state (what 'done' looks like)	Microsoft capability
Identities	phishing-resistant MFA, risk-based Conditional Access, no standing admin	Entra ID, ID Protection, PIM
Endpoints	every device managed, compliant and monitored before access	Intune, Defender for Endpoint
Applications	SSO through Entra, session controls, shadow IT discovered	Entra app proxy / Private Access, Defender for Cloud Apps
Data	classified, labelled, encrypted, DLP everywhere	Purview (SC-401)
Infrastructure	posture managed, JIT access, workloads protected across clouds	Defender for Cloud, Arc, Azure Policy
Network	micro-segmented, encrypted, no implicit trust in location	Azure Firewall, NSGs, Private Link, Global Secure Access
Visibility and automation	unified SIEM/XDR with automated response	Sentinel, Defender XDR, Security Copilot



Zero Trust maturity of a sample organisation: current (dot) vs 18-month target (ring)

- 1 Explicit trust validation for users and devices** MFA everywhere, Conditional Access, device compliance, passwordless
- 2 Ransomware and privileged access recovery readiness**, PIM, privileged access workstations (sheet 02)

- 3 Modern security operations XDR + SIEM, automation, threat hunting (sheet 03)
- 4 Data protection and governance classification, labels, DLP (Purview)
- 5 Cloud and data centre infrastructure posture, segmentation, workload protection (sheet 06)
- 6 OT and IoT asset discovery and monitoring with Defender for IoT

Zero Trust Rapid Modernization Plan (RaMP): what to do first

The framework toolbox

Framework	Use it to	Exam signal
MCRA (Cybersecurity Reference Architectures)	see how Microsoft capabilities fit together: identity, SecOps, multicloud, OT, attack chain coverage, SASE	'which capabilities and integrations'
MCSB (cloud security benchmark)	define controls and measure them; Defender for Cloud default initiative; per-service security baselines	'baseline', 'benchmark', 'regulatory compliance dashboard'
CAF Secure methodology	embed security in every adoption phase (strategy, plan, ready, adopt, govern, manage) and team roles	'cloud adoption', 'landing zone', 'organisation'
Well-Architected security pillar	design one workload securely; SE:01-SE:12 checklist; review with the assessment tool	'workload', 'design review', 'trade-offs'
Zero Trust guidance and RaMP	prioritise a modernisation programme across all areas	'strategy', 'prioritise', 'roadmap'
Enterprise access model	design privileged access across control, management and data planes	'privileged access', 'admin workstations'

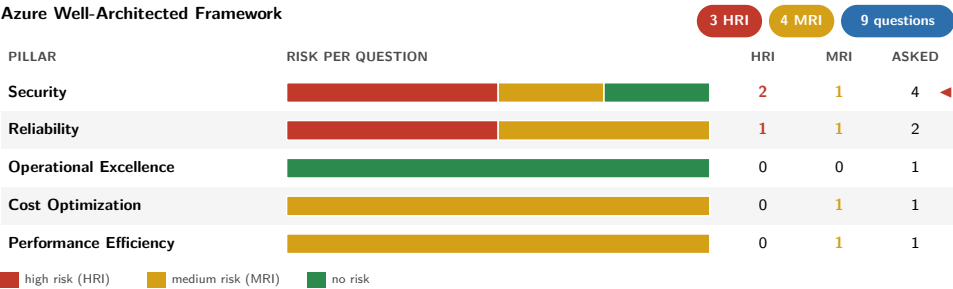
Requirement	NIST SP 800-53	CIS v8	PCI DSS 4.0	Zero Trust area
NS Network security	SC-7	12, 13	1	Network
IM Identity management	IA-2	5, 6	8	Identities
PA Privileged access	AC-6	5, 6	7	Identities
DP Data protection	SC-28	3	3, 4	Data
LT Logging and threat detection	AU-6	8, 13	10	Visibility
PV Posture and vulnerability mgmt	RA-5	7	6, 11	Infrastructure
BR Backup and recovery	CP-9	11		Infrastructure
DS DevOps security	SA-11	16	6	Applications

covered partly covered not covered

MCSB control domains and where other frameworks cover them

INFO

The 12 MCSB domains: Network security (NS), Identity management (IM), Privileged access (PA), Data protection (DP), Asset management (AM), Logging and threat detection (LT), Incident response (IR), Posture and vulnerability management (PV), Endpoint security (ES), Backup and recovery (BR), DevOps security (DS), Governance and strategy (GS). A newer MCSB version adds AI-related guidance (as of 2026, check whether v2 is generally available).



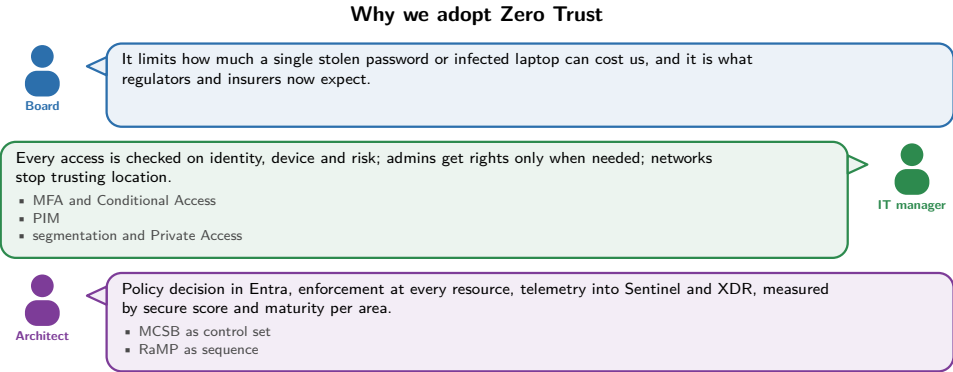
TOP 4 IMPROVEMENTS

1	HIGH	Move owners to PIM eligible assignments, enforce FIDO2 Security: SE:05 Admin access uses PIM and phishing-resistant MFA?
2	HIGH	Run a ransomware tabletop and restore test Security: SE:12 Incident response tested this year?
3	HIGH	Immutable vault + quarterly restore drill Reliability: Backups immutable and restore-tested?
4	MEDIUM	Replace connection strings with managed identities Security: SE:09 Secrets in Key Vault with managed identities?

HRI = high-risk issue, MRI = medium-risk issue: a question answered with that risk. Fix HRIs first; the marks the pillar with the most HRIs.

Well-Architected review of an e-commerce workload: high-risk items first

From business goals to a strategy



- Start from business goals (growth, M&A, cloud move), risks (ransomware, data theft, regulation), constraints (budget, skills, residency)
- Prioritise Microsoft guidance: protect against ransomware and privileged compromise first, then broader Zero Trust; quick wins with high risk reduction
- Measure Microsoft Secure Score and Defender for Cloud secure score, Exposure Management initiatives, maturity per Zero Trust area, MTTD and MTTR
- Govern security policy and standards, exceptions with expiry, architecture review board, roles from CAF (security architecture, operations, posture, compliance)

Worked example: prioritise three initiatives by risk reduced per cost

Score each initiative R / C , where R = expected annual loss avoided (EUR) and C = first-year cost (EUR). Phishing-resistant MFA for admins: $R = 400,000$, $C = 60,000 \rightarrow 6.7$. Immutable backups and restore drills: $R = 900,000$, $C = 150,000 \rightarrow 6.0$. Full micro-segmentation: $R = 300,000$, $C = 250,000 \rightarrow 1.2$. Order: MFA, backups, then segmentation, which matches the RaMP order (identity and ransomware first).

MYTH

❌ Zero Trust is a product you buy

❌ Zero Trust removes the network perimeter controls

❌ MCSB and MCRA are the same thing

❌ The Well-Architected review is only for reliability

FACT

✅ It is a strategy across six areas
Products implement parts; policies and operations make it work.

✅ Network becomes one signal and one control among many
Segmentation and firewalls stay; location stops granting trust.

✅ MCSB lists controls, MCRA draws capabilities
Benchmark vs reference architecture.

✅ It covers five pillars
Security, reliability, cost, operational excellence, performance.

Q1 Three Zero Trust maturity stages in Microsoft guidance?

A Traditional, advanced, optimal.

Q2 MCSB domain for logs and detections?

A LT, Logging and threat detection.

Q3 Which framework guides security in each adoption phase?

A Cloud Adoption Framework, Secure methodology.

Q4 WAF security checklist item for secrets?

A SE:09 Protect application secrets.

Q5 Model that replaced the AD tier model for privileged access?

A Enterprise access model (control, management, data/workload planes).

Q6 RaMP first initiative?

A Explicit trust validation for users and devices (MFA, Conditional Access, device compliance).

Q7 Where is MCSB measured in Azure?

A Defender for Cloud regulatory compliance and recommendations (default initiative).

Q8 Which Microsoft programme sets secure by design, by default, in operations?

A Secure Future Initiative (SFI).

Key takeaways

01

Zero Trust is the strategy

verify explicitly, least privilege, assume breach

02

RaMP sets the order

identity and ransomware first

03

MCSB = controls, MCRA = capabilities

CAF = adoption, WAF = workload

04

Prioritise by risk reduced per cost

and measure with secure score and maturity

05

Explain to each audience

board, IT, architects