MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

SECURITY ARCHITECTURE · 2026 EDITION

Zero Trust Architecture Implementation Blueprint

A resource-centric migration blueprint aligned to NIST SP 800-207 and the 2025 NIST implementation practice guide.

7	5	2025
Core tenets	Migration phases	Practice guidance

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Zero trust is an enterprise architecture and operating model—not a single product. Use this blueprint to reduce implicit trust through identity, device, application, data, policy, and telemetry controls.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **Zero Trust Principles**
Protect resources through explicit, per-session decisions informed by current context.

02 **Logical Architecture**
Separate policy decisions from enforcement and feed both with reliable information.

03 **Identity, Device, Network & Workload**
Build multiple independent signals instead of trusting a location.

04 **Migration Roadmap**
Move incrementally from discovery to measured enforcement.

05 **Policy & Measurement**
Make every access decision explainable and continuously reviewable.

06 **References & Implementation Gate**
Use official models and validate organizational readiness.

Zero Trust Principles

Protect resources through explicit, per-session decisions informed by current context.

- Treat all data sources and computing services as resources
- Secure all communication regardless of network location
- Grant access per session and with least privilege
- Use dynamic policy based on identity, device, resource, behavior, and environment
- Monitor and measure asset integrity and security posture
- Enforce authentication and authorization before resource access
- Collect telemetry and improve policies continuously

Logical Architecture

Separate policy decisions from enforcement and feed both with reliable information.

Policy Engine

Evaluates policy and context to grant, deny, or revoke access.

Policy Administrator

Establishes or terminates the communication path based on decisions.

Policy Enforcement Point

Controls the connection between subject and enterprise resource.

Data sources

Identity, device posture, threat intelligence, logs, asset status, and policy data.

Identity, Device, Network & Workload

Build multiple independent signals instead of trusting a location.

Pillar	Target state
Identity	Strong lifecycle, phishing-resistant MFA, risk-aware access, privileged isolation
Device	Inventory, health signals, encryption, EDR, patch posture, certificate identity
Network	Encrypted flows, application-aware policy, segmentation, monitored egress
Application/workload	Service identity, authenticated APIs, secret rotation, workload policy
Data	Classification, minimization, encryption, rights controls, exfiltration monitoring
Visibility	Unified telemetry, decision logs, response automation, policy metrics

Migration Roadmap

Move incrementally from discovery to measured enforcement.

Phase 1 · Discover

Identify critical resources, subjects, workflows, dependencies, and current controls.

Phase 2 · Design

Choose priority use cases, trust algorithm inputs, policy model, and enforcement points.

Phase 3 · Pilot

Start with a bounded workflow, observe decisions, validate recovery and user experience.

Phase 4 · Enforce

Progress from monitor to step-up to deny; integrate incident response.

Phase 5 · Optimize

Measure policy outcomes, false positives, attack paths, coverage, and business friction.

Policy & Measurement

Make every access decision explainable and continuously reviewable.

Policy inputs
Identity assurance, role, device health, resource sensitivity, behavior, threat state.

Decision outputs
Allow, deny, step-up authentication, restrict action, or revoke.

Resilience
Define behavior when identity, posture, or policy services are degraded.

Metrics
Coverage, legacy bypass, privileged sessions, denied risky access, response time.

Privacy
Minimize telemetry, define purpose and retention, control analyst access.

Testing
Exercise compromised identity, unmanaged device, token theft, and service failure.

References & Implementation Gate

Use official models and validate organizational readiness.

- NIST SP 800-207 — https://doi.org/10.6028/NIST.SP.800-207
- NIST SP 800-207A — https://doi.org/10.6028/NIST.SP.800-207A
- NIST SP 1800-35 (2025) — https://doi.org/10.6028/NIST.SP.1800-35

Owner
Executive sponsor and architecture owner assigned.

Use case
Critical resource and workflow selected.

Signals
Identity and device data quality validated.

Enforcement
PEP placement and bypass paths reviewed.

Operations
Help desk, incident response, and break-glass tested.

Outcome
Security and user-experience metrics baselined.



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.