HORIZONSHIELD

Securing Your Digital Future, Today.

ARCHITECTURE SERIES · BOOK 06 OF 16

Zero Trust Architecture Guide

Never Trust, Always Verify — Implementation 2026

A practical guide to designing and implementing Zero Trust across hybrid environments. Identity-centric security, device trust, micro-segmentation, ZTNA, continuous verification, and CISA maturity model — with implementation roadmap.

PILLARS	MATURITY LEVELS	STANDARD	LEVEL
5 ZT Pillars	4	NIST 800-207	Advanced

Contents

ZERO TRUST ARCHITECTURE 2026

CHAPTER 01

Zero Trust Philosophy

Zero Trust is not a product — it is an architectural philosophy that requires rethinking every access decision from first principles.

NIST 800-207 | NEVER TRUST | ALWAYS VERIFY | ARCHITECTURE

Zero Trust — NIST 800-207 Framework

NIST SP 800-207 defines Zero Trust as 'an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources.' The core tenet: **never trust, always verify** — regardless of network location.

The Seven Tenets of Zero Trust (NIST 800-207)

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location — no trust based on network segment
3. Access to individual resources is granted on a per-session basis — not persistent access
4. Access is determined by dynamic policy including observable identity, application, and device state
5. The enterprise monitors and measures integrity and security posture of all owned assets
6. All authentication and authorisation is dynamic and strictly enforced before access is allowed
7. Maximum information is collected about current state of assets, infrastructure, and communications

Aspect	Traditional Perimeter	Zero Trust Architecture
Trust model	Implicit trust inside network perimeter	No implicit trust anywhere — every request verified

Aspect	Traditional Perimeter	Zero Trust Architecture
Access control	IP/subnet-based — inside = trusted	Identity + device + context + behaviour
Lateral movement	Easy once inside perimeter	Blocked by micro-segmentation — limited blast radius
Remote access	VPN with broad network access	ZTNA — per-application access, no network access
Session monitoring	Perimeter-focused, limited visibility	Every session logged, analysed, continuously evaluated
Compromise impact	Attacker has broad network access	Attacker limited to explicitly granted application access

ZERO TRUST IS A JOURNEY, NOT A PROJECT

Organisations do not "implement" Zero Trust in a single project. The CISA Zero Trust Maturity Model defines four maturity levels (Traditional, Initial, Advanced, Optimal) across five pillars: Identity, Devices, Networks, Applications, Data. Start with Identity. Achieve Advanced in one pillar before moving to the next.

CHAPTER 03

Device Trust & Endpoint Compliance

Every device accessing your resources is a trust decision. Unmanaged devices are your most common attack vector.

MDM | COMPLIANCE POLICY | CONDITIONAL ACCESS | ENDPOINT

Device Trust in Zero Trust Architecture

In a Zero Trust model, device compliance is a prerequisite for access. An identity with valid MFA on an unmanaged, unpatched device with malware is not a trusted access request — it is an attack in progress.

Device Compliance Policy Requirements

Compliance Check	Microsoft Intune	Jamf Pro (macOS)	Why Critical
Encryption enforced	BitLocker required — Intune compliance policy	FileVault required — Jamf policy	Unencrypted device = data exposed if stolen
OS version minimum	Windows 11 23H2 minimum — mark older as non-compliant	macOS 14 Sonoma minimum	Old OS = exploitable vulnerabilities
EDR agent installed & running	Defender for Endpoint — integration with Intune compliance	CrowdStrike/Defender — Jamf compliance check	No EDR = no malware detection/response
Patch state	Critical patches within 24h — Intune	Patch state check via Jamf policy	Unpatched = exploitable

Compliance Check	Microsoft Intune	Jamf Pro (macOS)	Why Critical
	patch compliance report		
Jailbreak/root detection	Intune mobile device compliance: Jailbroken = non-compliant	Jamf device integrity check	Rooted device bypasses OS security controls
Screen lock enforced	PIN minimum 6 digits or biometric — Intune	Passcode required — Jamf	Unattended unlocked device = physical access attack

```
# Azure Conditional Access — Require compliant device for all app access
# Create policy: 'All Apps — Require MFA + Compliant Device'

# Policy configuration (Entra ID → Security → Conditional Access):
# Assignments:
#   Users: All users (exclude break-glass account)
#   Cloud Apps: All cloud apps (or specific critical apps)
#   Conditions: Any platform, any location
# Grant Controls (AND):
#   Require: Multi-factor authentication
#   Require: Device to be marked as compliant (Intune)
# Session Controls:
#   Sign-in frequency: 4 hours
#   Persistent browser session: Disabled

# Result: Identity theft + session theft cannot access apps
# without a compliant Intune-managed device presenting valid MFA
```

1

Inventory All Devices

WEEK 1

Identify every device accessing company resources — managed, unmanaged, BYOD, IoT. You cannot apply device trust policies to devices you do not know exist. Use network scanning + identity provider sign-in logs.

2

Enroll Managed Devices

WEEKS 2-4

Enroll all company-owned devices in MDM (Intune, Jamf, or equivalent). Define and assign compliance policies. Set grace period for existing devices to achieve compliance.

3

Conditional Access Enforcement

MONTH 2

Enable Conditional Access requiring device compliance for sensitive applications. Start with admin access and critical business apps. Expand to all apps over 60 days.

4

BYOD Strategy

MONTH 3

Define BYOD policy: allow with MAM (Mobile Application Management) protecting corporate data without full MDM, or block unmanaged devices from corporate resources. MAM protects corporate data without enrolling personal device.

CHAPTER 04

Network Micro-Segmentation

Micro-segmentation limits lateral movement blast radius. When an attacker compromises one system, segmentation prevents access to everything else.

MICRO-SEGMENTATION | VLAN | FIREWALL | EAST-WEST TRAFFIC

Network Micro-Segmentation Design

Segment	Contains	Trust Level	Access Policy	East-West Control
Identity/Auth Zone	AD DCs, PKI, MFA servers	Maximum — Tier 0	Only management traffic from PAWs	Deny all except explicit DC replication
Server Zone	Business-critical servers, databases	High — Tier 1	Specific application ports only from known sources	Application-layer firewall between servers
Workstation Zone	User endpoints, laptops	Medium — Tier 2	No direct server access — all via application layer	No workstation-to-workstation lateral traffic
DMZ / Public Services	Web servers, email gateway, reverse proxy	Low	Inbound from internet only, outbound to internal blocked	WAF in front, no direct internal connectivity
OT/IoT Zone	HVAC, cameras, industrial devices	Untrusted	Outbound only — no inbound from any zone	Air-gapped from IT network, unidirectional gateway
Guest / BYOD WiFi	Visitor devices, personal devices	Untrusted	Internet only — no internal resource access	Captive portal, no lateral traffic at all

```
# AWS: Implement micro-segmentation with Security Groups
# Principle: Security Groups default-deny — explicitly allow only required traffic

# Web tier SG — only 443 from internet:
aws ec2 create-security-group --group-name web-tier-sg \
  --description 'Web Tier — HTTPS only from internet'
aws ec2 authorize-security-group-ingress --group-id sg-web \
  --protocol tcp --port 443 --cidr 0.0.0.0/0

# App tier SG — only from web tier SG (not CIDR — SG reference):
aws ec2 authorize-security-group-ingress --group-id sg-app \
  --protocol tcp --port 8080 --source-group sg-web
# NO 0.0.0.0/0 access — only from web tier

# Database tier SG — only from app tier SG:
aws ec2 authorize-security-group-ingress --group-id sg-db \
  --protocol tcp --port 5432 --source-group sg-app
# Result: Database is never directly accessible from internet
# Even if web tier is compromised, attacker cannot reach DB directly
```

FLAT NETWORKS ARE STILL EXTREMELY COMMON

The majority of SMBs and many mid-market organisations still run flat networks where any device can communicate with any other. A single compromised endpoint = access to all servers, all file shares, all databases. The cost of basic VLAN segmentation is minimal. The cost of lateral movement without segmentation is catastrophic.

HS

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

Zero Trust Architecture Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.