ELEVATE
SOLUTIONS

GUIDE · CYBERSECURITY

Zero Trust Architecture — A Practical Guide

Implementation in phases

How to implement zero-trust networking without big-bang disruption. A phased rollout with dependencies, risks, and quick wins at each stage — written for firms where downtime and lockouts have regulatory consequences.

01 — PRINCIPLES & MENTAL MODEL

Stop defending a perimeter that no longer exists

The traditional model assumed a hard outer wall and a trusted interior: get past the firewall and you are "inside." That castle-and-moat picture stopped matching reality years ago. Your data lives in SaaS applications, your people work from home networks and hotel Wi-Fi, and your vendors connect directly into your systems. There is no moat. There is only a set of users, devices, and services requesting access to resources — and every one of those requests can be verified or waved through.

Zero trust is the decision to verify. Three principles, formalized in NIST SP 800-207, define it:

1. Never trust, always verify. No request is trusted because of where it comes from. Being on the office VLAN, on the VPN, or behind the firewall earns nothing. Every access decision is made per session, based on who the user is, what device they are on, and what they are asking for.

2. Assume breach. Design as if an attacker already holds one set of valid credentials and one compromised laptop — because in a typical incident, they do. The question shifts from "how do we keep them out" to "how far can they get, and how fast do we see them." Containment speed is where the money is: breaches contained in under 200 days averaged $3.61M versus $5.49M for those that ran longer. IBM Cost of a Data Breach Report 2025

3. Least privilege. Every user, service account, and application gets the minimum access needed to do its job, granted for the minimum time needed. Standing broad access is the raw material of lateral movement; least privilege starves it.

60%	30%	$10.22M
Breaches involving the human element Verizon DBIR 2025	Breaches with third-party involvement — doubled YoY Verizon DBIR 2025	US average breach cost — a record high IBM Cost of a Data Breach Report 2025

> **WHAT ZERO TRUST IS NOT**
>
> Zero trust is not a product. No appliance, license tier, or "zero trust platform" SKU makes you zero trust on its own. It is an architecture: a sequence of decisions about identity, devices, and network paths, implemented with tools you mostly already own. Any vendor pitch that starts with a box and ends with "done" is selling the moat back to you with a new label.

Why phases, not a big bang. The fastest way to kill a zero-trust program is to break the managing partner's login on a Monday. Every control in this guide follows the same safe pattern: **inventory → monitor/report-only → enforce for a pilot group → enforce broadly → handle exceptions as time-boxed, documented exclusions.** The three phases are ordered by dependency. Identity comes first because device and network controls key off it. Device trust comes second because segmentation policies need a compliance signal to act on. Network segmentation comes last because it is the most disruptive and benefits most from the telemetry the first two phases generate.

02 — IDENTITY-FIRST IMPLEMENTATION

Phase 1: make identity the control plane

Identity is the new perimeter because it is the one thing present in every access request. Phase 1 has four workstreams. Expect 30–60 days for a firm of 20–200 staff; the long pole is exception handling, not technology.

Workstream 1: MFA everywhere — phishing-resistant where possible. Per CISA, "Over 90% of successful cyber-attacks start with a phishing email" CISA — and stolen credentials are what most of those emails are after. MFA on email and VPN only is not "everywhere": cover admin portals, remote access, line-of-business apps, and backup consoles. Prefer phishing-resistant methods — FIDO2 security keys, passkeys, Windows Hello for Business — over push notifications, and retire SMS and voice codes entirely; they are interceptable and prompt-bombable. In Microsoft 365, enforce via Conditional Access (**entra.microsoft.com → Protection → Conditional Access**) with an authentication-strengths policy requiring phishing-resistant MFA for admins first, then all users.

Workstream 2: Conditional access policies. Conditional access is the policy engine that makes "always verify" real: it evaluates user, device, location, and risk on every sign-in. Build a small, legible baseline — five well-understood policies beat thirty nobody can explain to an auditor:

- ☐ **Require MFA for all users, all cloud apps** — 1
  One break-glass account excluded, stored offline, sign-ins alerted on.
- ☐ **Require phishing-resistant MFA for admin roles** — 2
  Scoped to Global Administrator, Exchange Administrator, and similar privileged roles.
- ☐ **Block sign-ins from countries you never operate in** — 3
  Named locations + block policy. Crude, cheap, and it removes a large slice of noise.
- ☐ **Require MFA re-authentication for risky sign-ins** — 4
  Where licensing includes risk detection (e.g., Entra ID P2); otherwise alert on impossible-travel events.
- ☐ **Deploy every new policy in report-only mode first** — 5
  Run 1–2 weeks, review the sign-in log impact, then enforce. This is the no-lockout rule.

Workstream 3: Privileged account separation. Admins get two accounts: a daily-driver with no admin roles, and an admin account with no mailbox, no productivity license, and phishing-resistant MFA. A phished mailbox should never equal a domain takeover. Where licensing allows, make admin roles just-in-time — activated for a set window with justification (Privileged Identity Management in Entra ID P2, or the equivalent in your identity platform) — rather than standing.

Workstream 4: Service account inventory. Service accounts are the accounts nobody owns and everybody fears touching. Inventory every one: what it runs, what it can reach, when the password last changed, what breaks if it is disabled. Then shrink the list — replace credentials with managed identities or workload identities where the platform supports it, scope the rest to least privilege, and block them from interactive

sign-in. An unowned service account with a five-year-old password and domain admin rights defeats every other control in this guide.

WORKSTREAM	QUICK WIN (FIRST 2 WEEKS)	PRIMARY RISK & MITIGATION
MFA everywhere	Enforce MFA on all admin and remote-access accounts	User friction and helpdesk surge — communicate dates ahead, stage by department, brief the helpdesk on reset procedure first.
Conditional access	Geo-block policy in report-only, enforced after one clean week	Locking out a legitimate edge case — report-only mode plus a tested break-glass account before any enforcement.
Privileged separation	Strip admin roles from every mailbox-bearing account	Admins bypassing the second account out of convenience — make the daily account genuinely sufficient for daily work.
Service accounts	Inventory with owner, purpose, and last password change per account	Breaking an undocumented integration — disable in a maintenance window with a rollback plan, never delete first.

03 — DEVICE TRUST & CONDITIONAL ACCESS

Phase 2: only healthy devices get in

Phase 1 verified the user. Phase 2 verifies the machine. A valid login from a malware-ridden, unencrypted laptop is still a breach in progress — so device state becomes a condition of access, enforced through the same conditional access engine you stood up in Phase 1.

Device compliance policies. Define what a "healthy" device means and have your management platform attest to it continuously. In Intune (**intune.microsoft.com → Devices → Compliance**), a workable baseline: disk encryption on (BitLocker / FileVault), a supported OS version with a maximum patch age, endpoint protection running and reporting, screen lock with PIN or biometric, and no jailbroken or rooted devices. Keep the first baseline achievable — the goal is a trustworthy compliance signal, not a perfect device. You can tighten settings later; you cannot easily rebuild trust after marking half the fleet noncompliant on day one.

Health attestation, not self-reporting. Where hardware supports it, use measured attestation — Secure Boot and TPM-backed health claims on Windows, equivalent platform attestation on macOS — so the compliance signal reflects what the device *is*, not what an agent says about itself. Malware that owns the OS can lie to an agent; it has a much harder time forging a TPM measurement.

Block legacy authentication. Legacy protocols — IMAP, POP3, SMTP AUTH, ActiveSync basic auth — cannot carry MFA, which makes them a standing bypass of everything in Phase 1. Attackers know this and aim password sprays squarely at them. Before blocking: filter the sign-in logs (**entra.microsoft.com → Monitoring → Sign-in logs**, filter by Client app) for legacy protocol usage over 30 days. The usual culprits are scan-to-email copiers, ancient billing software, and one partner's beloved mail client. Remediate each — modern auth, app passwords retired, device replaced — then enforce a "Block legacy authentication" conditional access policy. This single policy ends more account compromises than almost any other change in this guide.

The BYOD decision: MAM vs MDM. Personal phones reading firm email is the question every regulated firm eventually has to answer in writing. There are two honest options:

	MAM — APP PROTECTION ONLY	MDM — FULL ENROLLMENT
What's managed	Corporate apps and their data only (e.g., Intune App Protection: PIN on Outlook, copy/paste restrictions, selective wipe of firm data)	The whole device: compliance policy, encryption enforcement, full or selective wipe, OS update control
User reaction	Low friction — the firm never touches personal data	Resistance on personal devices; routine on firm-owned ones
Best fit	Personal phones — email, Teams, document access	Firm-owned laptops and phones, and any device touching PHI, client funds, or privileged matter files

Limit	No device health signal — a compromised phone with a protected app is still compromised	Cost, enrollment effort, and a privacy conversation you must have before, not after

A defensible default for regulated firms: **MDM on every firm-owned device, MAM on personal phones, and no access from devices in neither bucket** — enforced with a conditional access policy requiring a compliant device or an approved protected app. Write the policy down, have staff acknowledge it, and decide the wipe question (who authorizes, what gets wiped) before the first lost phone, not during it.

> **PHASE 2 QUICK WIN**
>
> Blocking legacy authentication needs no new licenses, no agents, and roughly a day of log review. If you do exactly one thing from this section this quarter, do that.

04 — NETWORK SEGMENTATION ROLLOUT

Phase 3: make lateral movement expensive

Phases 1 and 2 decide who and what gets in. Phase 3 limits what an attacker can reach after a foothold — the difference between losing one workstation and losing the file server, the practice management system, and the backups in the same afternoon.

Identity-aware segmentation. Classic segmentation grouped machines by IP range and VLAN; rules said "this subnet can reach that subnet," and meant nothing about who was asking. Zero-trust segmentation writes rules in terms of identity and role: *members of the Finance group, on compliant devices, can reach the accounting application — and nothing else on that server.* Group resources by sensitivity (client files, finance, infrastructure management) and write access rules per group. The Phase 1 directory work is the dependency: rules are only as good as the group memberships behind them, so access reviews become part of the control.

ZTNA over flat VPN. A traditional VPN drops a remote user onto the network — reach the file server, and also every workstation, printer, and forgotten test box on the same subnet. One phished VPN credential equals interior access; ransomware operators rely on exactly this. Zero-trust network access (ZTNA) brokers the connection per application instead: the user reaches the practice management app and the document store they are entitled to, and nothing else exists from their vantage point. Entra Private Access, Cloudflare Access, Zscaler Private Access, and Tailscale all implement the pattern. Migrate application by application — publish the two or three most-used internal apps through the broker first, run dual-stack alongside the VPN, then shrink VPN entitlements as each app moves. The VPN's last job is the legacy systems that cannot be brokered; scope it to only those, then retire it.

Server-to-server rules. Most east-west traffic between servers is wide open by default, and it is the highway lateral movement travels. You do not need a microsegmentation platform to start: host firewalls (Windows Defender Firewall with Advanced Security via GPO or Intune, nftables/ufw on Linux) can express "the web tier talks to the database on port 1433, and nothing else does." Start with the crown jewels — domain controllers, backup infrastructure, file servers, the database behind your line-of-business app. Backup servers deserve special hostility: management access from a dedicated admin subnet or PAW only, no inbound from general workstation ranges, ever. If ransomware on a workstation can reach your backup console, you do not have backups — you have a second ransom.

Monitoring mode first — the non-negotiable. Every segmentation rule starts in log-only/audit mode. Run two to four weeks, review what *would* have been blocked, chase down each flow (a surprising number turn out to be undocumented but load-bearing), then flip to enforce. Segmentation deployed straight to enforcement is how zero-trust programs get cancelled by their own outage. The logging phase also pays a second dividend: it is the first real map of east-west traffic most firms have ever had, and feeding it to your monitoring stack shortens detection. Organizations using security AI and automation extensively saw breach costs average $1.9M lower and lifecycles roughly 80 days shorter. IBM Cost of a Data Breach Report 2025

The roadmap at a glance.

PHASE	DEPENDS ON	BIGGEST RISK	QUICK WIN
1 — Identity	Clean user directory; leavers disabled, groups accurate	Lockouts during MFA enforcement	MFA on all admin and remote access within two weeks
2 — Device	Phase 1 conditional access engine; device inventory	Mass noncompliance from an overstrict baseline	Block legacy authentication after 30 days of log review
3 — Network	Phase 1 groups + Phase 2 compliance signal	Outage from enforcing rules before mapping flows	Lock down inbound access to backup infrastructure first

WHERE TO START MONDAY

Pull the list of accounts without MFA. Pull 30 days of legacy-authentication sign-ins. Pull the inbound firewall rules on your backup server. Those three reports cost nothing, take an afternoon, and tell you exactly where your zero-trust program begins.

ELEVATE SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io