SECURITY · TEMPLATE

Zero-Trust for Regulated SMBs *Without* the Enterprise Price Tag

KAANSYSTEMS.COM/LIBRARY/ZERO-TRUST-FOR-SMBS · JULY 9, 2026

ABOUT THIS TEMPLATE

Zero-trust gets sold as a $200K platform purchase. An SMB can reach 80% of the benefit with tools it mostly already owns. The four-phase version, in the order that actually works.

THE TEMPLATE

The maturity model. Score each phase honestly — Not started / Partial / Done. Work top to bottom; a later phase built on an incomplete earlier one is wasted money.

Phase 1 — Identity

- ☐ SSO fronts every SaaS tool that supports it
- ☐ MFA enforced on 100% of human accounts, no exceptions
- ☐ Phishing-resistant MFA (FIDO2 / passkeys) on every admin account
- ☐ Shared / role logins eliminated; named accounts only
- ☐ Offboarding a person is a single revocation action

Phase 2 — Device

- ☐ Full-disk encryption enforced on every work device
- ☐ OS + critical updates enforced (not left to the user)
- ☐ Devices touching regulated data are enrolled in MDM
- ☐ Sensitive systems reachable only from managed devices

Phase 3 — Network

- ☐ Regulated environment segmented off the general/office network

- ☐ Cloud segmentation (VPC / security groups) enforces the boundary
- ☐ VPN-as-moat replaced with per-application access checks
- ☐ No single device can reach everything on a flat network

Phase 4 — Continuous verification

- ☐ Conditional access considers device posture + context, not just password
- ☐ Anomalous access (new device, new geo) is challenged or blocked
- ☐ Access events flow to centralized logging
- ☐ Access logs reviewed on a defined cadence

Most SMBs score Phase 1 at Partial and everything below at Not Started. That's a normal starting point. The path from there is one phase at a time, in order, using tools you mostly already own.

HOW TO USE IT

Sequence is the whole discipline. The reason zero-trust projects fail isn't the tooling — it's buying phase three before finishing phase one, then wondering why the expensive segmentation product didn't stop the phished credential that still had flat access to everything. Identity first, always.

Resist the platform pitch until you've earned it. The four phases above get an SMB to a genuine zero-trust posture using an identity provider you already have, a modest MDM, cloud-native segmentation, and an access proxy that's often cheaper than the VPN it replaces. There's a point of scale where a dedicated ZTNA platform earns its cost. Most regulated SMBs are years away from that point and would get more security per dollar finishing phases one and two.

The bar isn't "enterprise zero-trust." The bar is "a phished credential on an unmanaged device can't reach the PHI store." That bar is reachable this quarter, and it's the one that actually keeps you out of a breach notification.