SECURITY ARCHITECTURE · FIELD NOTES

Zero Trust Architecture: A Practical Starting Point

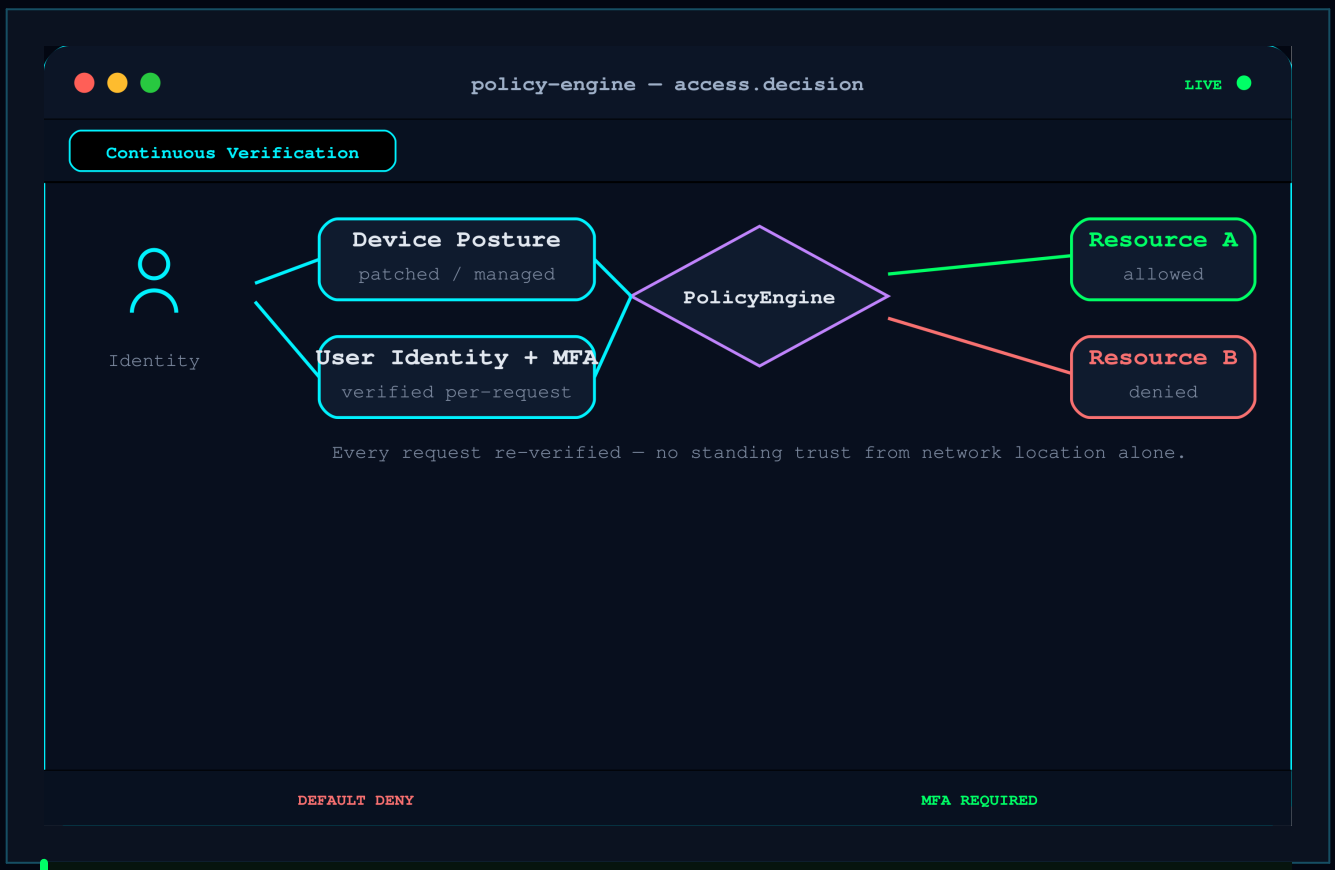
> *“Zero Trust doesn't mean nobody is trusted. It means trust is never assumed from network location alone, and is re-verified continuously instead of granted once at login.”*

Zero Trust is often presented as an enterprise-scale multi-year program. For a resource-constrained Kenyan business, that framing is actively unhelpful. This dossier is a realistic, staged starting point — not a rip-and-replace of your existing infrastructure.

Scope	Identity, device, and access architecture
Audience	Resource-constrained SMEs & startups
Approach	Staged adoption, not a full rebuild
Analyst	Nazline Mwita, Cybersecurity Assurance Lead, HarLyn Digital Partners

1. What Zero Trust Actually Means, Operationally

Traditional network security draws a perimeter (firewall, VPN) and trusts anything inside it. Zero Trust replaces that with continuous, identity-centric verification: every request is checked against device posture and user identity, regardless of whether it originates inside or outside the office network.



Security Principle

Never trust, always verify — per request, not per session.

2. The Three Practical Pillars

Identity-centric access: every access decision is tied to a verified user identity and MFA, not just network location.

Device posture: is the requesting device patched, managed, and free of known compromise indicators?

Micro-segmentation: systems are broken into smaller zones so a compromise in one doesn't grant automatic reach into others.

3. A Realistic Starting Point

Full Zero Trust adoption is a multi-year program for large enterprises with dedicated security teams. For a small Kenyan business, the honest starting sequence looks different:

Stage	What it looks like in practice
1. Identity first	Enforce MFA everywhere; kill shared/generic logins
2. Least privilege	Audit who has access to what; remove standing admin access
3. Device hygiene	Require OS/browser patching before granting access to sensitive systems
4. Segment critical systems	Separate production data access from general staff network access
5. Continuous verification	Move from "trusted once at login" to session-level re-checks for sensitive actions

4. What This Is Not

It is not a single product purchase. Vendors selling a “Zero Trust appliance” as a drop-in fix are selling a component, not the architecture. It is also not a reason to rip out existing VPN/firewall infrastructure overnight — those still have a role during a staged transition.

Related Service

This dossier supports the Cybersecurity Consultant service — ongoing security advisory sequencing exactly this kind of staged architecture change against real budget constraints.

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.