Zero Trust doesn't start with identity - It starts with the platform

Why architecture is the real foundation of security

Why the foundation matters

While most security efforts start with identity, access, and policy, cloud security depends on foundational elements like network architecture, resource hierarchy, logging, control planes, and baseline configurations. Without a solid platform, Zero Trust remains theoretical, which is why many projects fail.

Architecture may not appear glamorous, but it fundamentally determines the security and resilience of your platform. A robust Hub-and-Spoke design within Azure offers several key advantages:

- Centralized network management for streamlined connectivity
- Consistent firewalling and logging practices
- Standardized routing and policy enforcement
- Effective workload isolation with enhanced visibility

Governance, Risk, and Compliance (GRC) are thus integrated into the architectural framework from the outset, rather than being added as an afterthought.

Small workloads, big risks

Many incidents originate not within mission-critical systems, but in neglected workloads that lack adequate monitoring. When governance fails to scale appropriately, it results in a hidden cloud environment characterised by:

- Absence of Privileged Identity Management (PIM)
- Insufficient logging
- Lack of network controls
- Missing policy enforcement

Neglected small workloads can evolve into significant risks. Therefore, effective architecture and governance are essential to manage these challenges, rather than relying solely on individual discipline.

CTO Sunday Thoughts #10

MyPlatform

Shared Responsibility in real life

The Shared Responsibility model is often misunderstood. Common misconceptions include:

- “Microsoft handles it” (only applies outside your tenant)
- “We have governance” (unenforced policies aren’t governance)
- “Logging is in Sentinel” (logging belongs to your platform)
- “It’s a one-time delivery” (governance needs continuous attention)

Shared Responsibility requires ongoing, proactive ownership—not blame-shifting when issues arise.

Security baselines are never done

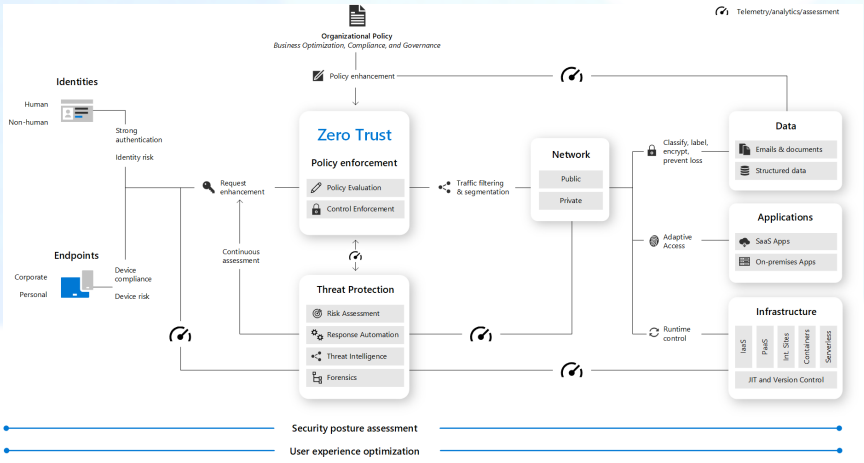
A common misconception is that a baseline represents a completed objective; however, this is not the case.

- Threat landscapes are continuously evolving.
- Azure frequently introduces new features and updates.
- Regulatory requirements also change over time.

Contemporary baselines should be designed to accommodate ongoing change, incorporating:

- Deployment rings for controlled rollouts
- Policy as Code for systematic version management
- Evergreen updates that minimize operational downtime
- Architectural approaches that support continuous adaptation

The baseline should be viewed not as the conclusion, but as the foundation from which progress begins.



Microsoft Partner

CTO Sunday Thoughts #10

MyPlatform

The MyPlatform model

Most organizations treat governance as an **afterthought**. Architecture gets built first, then someone comes in later to "add" security, compliance, and policies on top. That's exactly what creates complexity, drift, and risk.

At **MyPlatform**, we flipped that model from day one.

We built governance and architecture as a single, integrated foundation — not two separate workstreams.

That shift changes everything:

Hub-and-Spoke networking with central control
We standardize the network backbone from the start. All traffic flows through a controlled hub, enabling unified routing, firewall enforcement, VPN/ExpressRoute connectivity, and Bastion access. No ad hoc peering or shadow networks.

Policy inheritance through management groups
Governance isn't applied workload by workload. Instead, security policies, role assignments, and resource controls flow top-down — enforced at the platform layer through Azure Management Groups. This eliminates drift and ensures every new subscription or resource inherits guardrails automatically.

Unified firewalling and logging
Security events, network flows, and platform telemetry are collected centrally. Firewalling is standardized at the hub level. This gives immediate visibility and traceability across the entire environment — no blind spots between workloads.

Evergreen baselines aligned with Azure
Security and compliance baselines are not static documents. They are continuously updated in line with Microsoft's own platform evolution. As Azure evolves, so does the governance model — automatically, without new projects or procurement rounds.

Scalable governance from the very first workload
Because the platform foundation is standardized, the second, tenth, or hundredth workload doesn't require a redesign. Every new environment is automatically compliant, logged, and secured — from day one.

This **"platform-first security"** approach turns what used to be 250+ hours of consulting work into a **repeatable, automated, and evergreen baseline**.

Instead of securing workloads one by one, the **platform itself enforces governance** — continuously, consistently, and at scale.

It's not an overlay. It's the foundation.

CTO Sunday Thoughts #10

MyPlatform

CTO Takeaway

Zero Trust doesn’t start with identity. It starts with the platform.

Without architecture, there’s no governance.
Without governance, there’s no security.
Without security, there’s no cloud.

👉 Build the platform right from the start — the rest follows.