Zero Trust Security Architecture Case Study

Author's Statement

This report was created by Ruchi Giradkar as an independent security architecture design exercise based on a defined enterprise problem statement. The intent is to demonstrate enterprise-scale Zero Trust architecture design, including assumptions, constraints, tradeoffs, and sequencing. This document is original work and does not represent a deployed customer environment.

Design Objective

This case study presents a Zero Trust security architecture for a large hybrid enterprise undergoing long-term cloud modernization. The environment includes cloud workloads, on-premises systems, SaaS applications, remote users, and operational technology assets.

The architecture is designed with the explicit assumption that perimeter-based security is insufficient, credentials will be compromised, and some endpoints will eventually become untrusted. The goal is not absolute breach prevention, but measurable reduction of risk through continuous verification, limited blast radius, and effective detection and response, while maintaining business continuity and regulatory compliance.

Zero Trust Strategy Context

At a strategic level, Zero Trust is used to increase security assurance for business assets, including data and applications, regardless of where access originates. This applies equally to public networks, remote users, and internal systems.

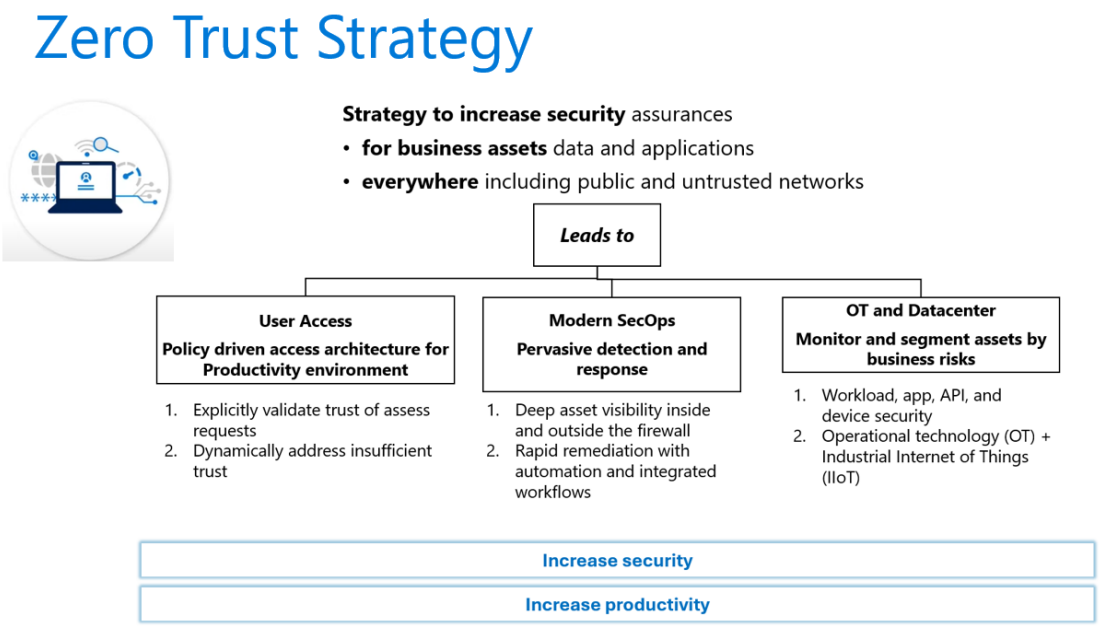

Figure 1: Zero Trust Strategy Overview

This figure establishes the strategic foundation of the architecture. It shows how policy-driven user access, modern security operations, and OT and datacenter protection work together to

increase both security and productivity. This framing is intentional and business-aligned, not tool-driven.

Design Assumptions and Constraints

The enterprise operates in a hybrid model and will continue to do so throughout the modernization period. Users and devices routinely access resources from untrusted networks. Identity-based attacks such as phishing, credential theft, and token replay are expected and must be assumed to succeed in some cases.

Operational technology environments impose strict availability and safety constraints. Aggressive endpoint or network enforcement is not acceptable in these environments. Protection must instead rely on visibility, segmentation, and tightly controlled access paths.

Security controls must be phased, reversible, and observable to avoid widespread disruption across a workforce of approximately one hundred thousand users.

Target Architecture Overview

The target state is a policy-driven Zero Trust architecture structured around core security domains that operate together rather than in isolation.

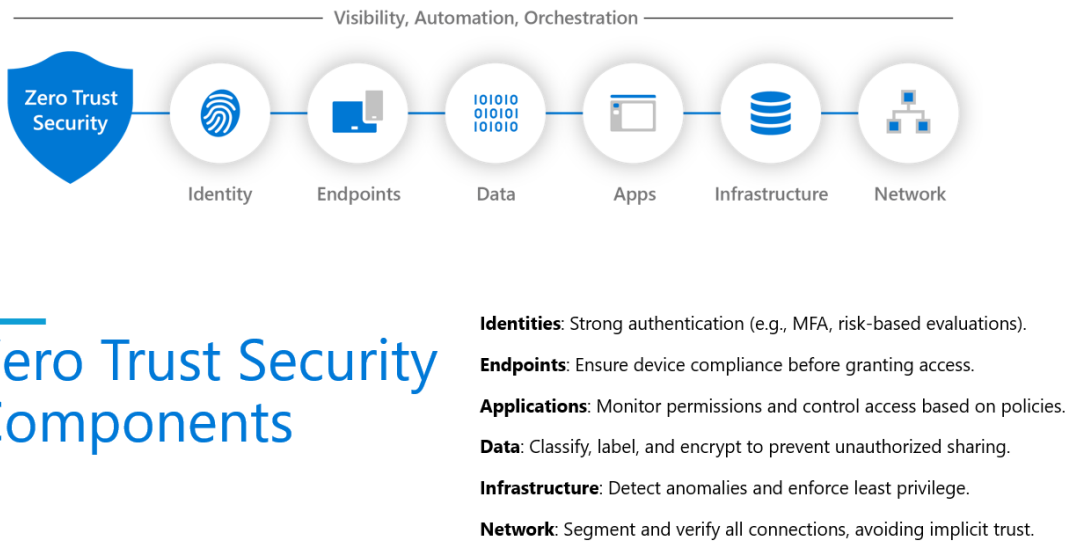

Figure 2: Zero Trust Security Components

This figure introduces the core components of the architecture: identity, endpoints, data, applications, infrastructure, and network. It aligns directly with how the architecture is structured in this case study and provides a clear mental model before diving into implementation details.

Policy-Driven Security Architecture

At the core of the architecture is centralized policy evaluation combined with distributed enforcement. Access decisions are made dynamically using multiple trust signals rather than static network location.

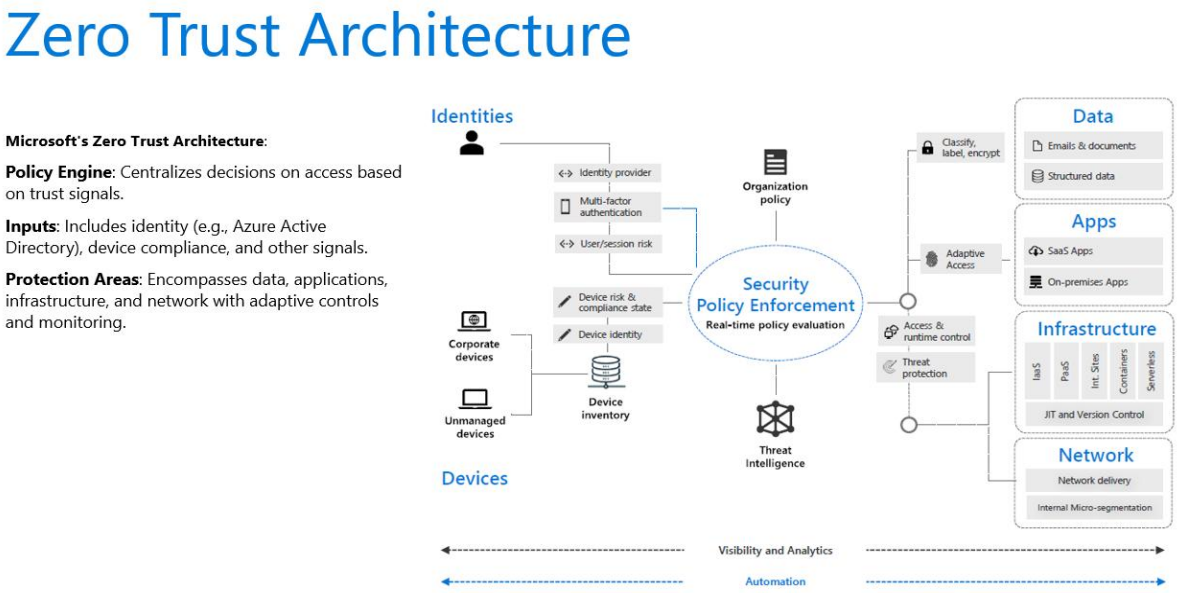

Figure 3: Zero Trust Architecture with Policy Enforcement

This figure represents the most important architectural concept in the case study. It shows how identity signals, device compliance, user risk, and contextual information feed into a policy engine that evaluates access in real time. Enforcement then occurs across applications, data, infrastructure, and network layers. This separation of decision-making and enforcement is fundamental to Zero Trust.

Identity Security and Risk-Based Access

Identity is treated as the primary enforcement layer because it provides the highest security leverage with the lowest operational friction at enterprise scale.

Strong authentication is enforced, legacy authentication paths are removed, and access is evaluated continuously using user risk, sign-in behavior, device posture, and resource sensitivity. Standing administrative privileges are eliminated. Privileged access is granted through just-in-time workflows that are time-bound, approved, and strongly authenticated. This intentionally prioritizes blast-radius reduction over administrative convenience.

Break-glass access paths are isolated and monitored to preserve recoverability during identity service outages.

Endpoint Security and Device Trust

Device trust is enforced based on risk rather than uniformly.

Managed and compliant devices are required for privileged access and sensitive workloads. Unmanaged devices are limited to low-risk, web-based access with restricted data operations. This tradeoff is explicit and intentional to preserve productivity while protecting critical assets.

Device compliance and exposure are continuously monitored, and high-risk devices are automatically restricted until remediation.

Data Discovery and Protection

Sensitive data is discoverable, classifiable, and protected regardless of where it resides.

Classification and labeling enforce encryption and usage restrictions, while data loss prevention controls reduce the risk of accidental or malicious exfiltration. These controls remain effective even after access is granted, acknowledging that access controls will eventually fail.

Cloud Workload and Web Application Security

Cloud workloads and web applications are protected through continuous posture assessment and runtime threat detection. Configuration weaknesses that enable initial access or privilege escalation are prioritized for remediation. Web-facing applications are monitored for exploitation attempts and abnormal behavior.

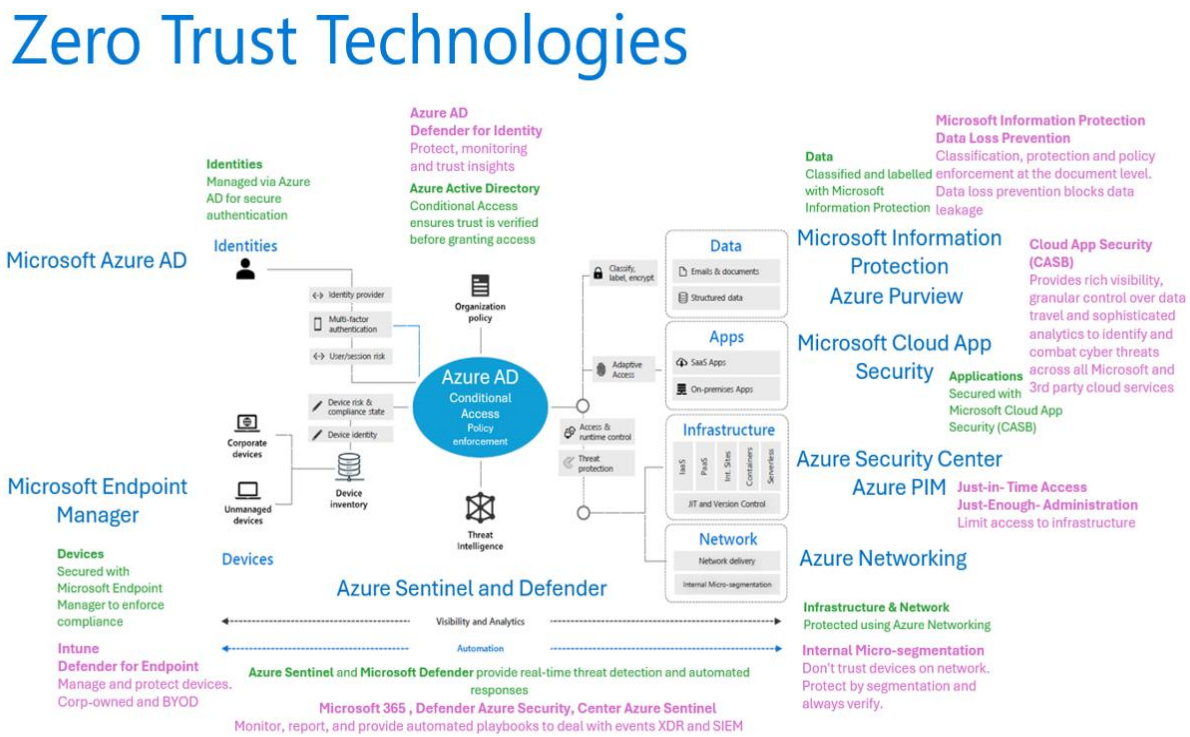

Figure 4: Zero Trust Technologies Mapping

This figure maps the Zero Trust architecture to concrete implementation layers, showing how identity, endpoints, data, applications, infrastructure, and network controls integrate with centralized detection and response. Only one version of this diagram should be used to avoid redundancy.

Operational Technology Security

Operational technology environments are protected through visibility, segmentation, and constrained access rather than aggressive enforcement.

Asset discovery and anomaly detection provide insight without disrupting fragile systems. Access between IT and OT environments is tightly controlled and logged. OT telemetry is integrated into centralized monitoring to detect cross-domain attack patterns without deploying intrusive endpoint controls.

Roadmap and Sequencing

The Zero Trust implementation follows a phased five-year roadmap to balance security improvement with operational stability.

Year	Focus Areas	Key Activities and Tools
Year 1	Foundation	• Assess risks with **Secure Score**, • Track compliance with **Purview Compliance Manager**, • Secure identities with **Entra MFA**, • Classify data with **Purview**.
Year 2	Deployment	• Deploy **Conditional Access**, • Automate data labeling with **Purview**, • Enable threat detection with **Sentinel** and **Defender for IoT**.
Year 3	Optimization	• Automate responses with **Sentinel playbooks**, • Refine detection with **Defender XDR**, • Manage insider threats with **Purview Insider Risk Management**.
Year 4	Expansion	• Scale Zero Trust to hybrid/multi-cloud with **Purview**, • Secure workloads with **Azure Site Recovery**, • Expand **Sentinel** integrations.
Year 5	Continuous Improvement	• Monitor compliance with **Sentinel** and **Purview**, • Conduct **Secure Score** reviews, and • Deploy **Security Copilot** for AI-driven threat response.

Year 1: Foundation and visibility

- Establish baseline security posture across identities, endpoints, applications, workloads, and data
- Enforce strong authentication and single sign-on
- Remove legacy authentication paths
- Enroll managed devices and define compliance baselines
- Implement initial data classification
- Centralize security telemetry and incident handling

Year 2: Controlled enforcement

- Expand conditional access using risk and device posture
- Extend automated data protection
- Implement continuous cloud posture management
- Begin OT asset visibility and segmentation
- Refine detection logic

Year 3: Operational optimization
• Introduce automated investigation and response
• Mature threat hunting
• Refine data loss prevention
• Introduce insider risk controls where required

Year 4: Scale and resilience
• Extend controls to remaining legacy workloads
• Strengthen recovery and continuity
• Expand OT integration
• Reduce manual workflows

Year 5: Continuous improvement
• Continuously tune policies
• Establish continuous compliance reporting
• Optimize control effectiveness
• Maintain a feedback loop between incidents and architecture decisions

What I Did in This Case Study

I designed a Zero Trust security architecture aligned with enterprise-scale constraints and long-term modernization goals. I translated business and technical requirements into security outcomes, defined explicit assumptions, and identified where enforcement was appropriate and where it was not.

I structured the architecture around identity, endpoint trust, data protection, workload security, detection and response, and OT visibility, and aligned it with a phased multi-year roadmap.

What I Learned from This Case Study

This case study reinforced that Zero Trust is an operating model, not a checklist or product deployment. Effective Zero Trust requires explicit assumptions, careful sequencing, and continuous adjustment.

I learned that identity provides the highest leverage for risk reduction, but only when combined with device posture and contextual signals. I also learned that visibility must come before enforcement in large environments to avoid widespread disruption.

Designing for OT environments highlighted the importance of adapting security controls to system constraints. Most importantly, this work emphasized that strong security architecture is defined by tradeoffs, not absolutes.