Zero Trust Architecture for Enterprise Network Security: Implementation Framework, Identity-Aware Micro-Segmentation, and Empirical Evaluation across 12 Kerala Organisations

Sreejith K. Nambiar[1], Priya R. Krishnan[2], Anish N. Pillai[3]

ABSTRACT

Zero Trust Architecture (ZTA) — the security model predicated on the principle of "never trust, always verify" that eliminates implicit trust for any user, device, or network location and enforces continuous verification of identity, device health, and access authorisation for every resource access request — has emerged as the dominant enterprise cybersecurity paradigm response to the inadequacy of perimeter-based security models in the face of cloud migration, remote working, mobile device proliferation, and the sustained erosion of network perimeter relevance by supply chain attacks, insider threats, and credential-based intrusions. NIST Special Publication 800-207 (2020) formalised the ZTA framework through seven tenets governing resource access decisions based on dynamic policy evaluation of user identity, device posture, network location, requested resource sensitivity, and behavioural analytics. This implementation and evaluation study documents the phased ZTA deployment — comprising identity provider integration (Okta OIDC/SAML2), device health attestation (Microsoft Intune MDM), network micro-segmentation (Palo Alto Prisma Access), and continuous monitoring (SIEM + UEBA) — across 12 Kerala IT and financial services organisations over an 18-month period, measuring security incident counts across five attack categories in the 6-month pre-implementation baseline and 6-month post-implementation follow-up periods. ZTA implementation produced statistically significant reductions across all five attack categories: unauthorised access attempts (−87.5%, 48→6 incidents), lateral movement (−91.2%, 34→3), data exfiltration (−90.9%, 22→2), phishing success rate

(−71.0%, 62→18 users compromised), and malware execution (−78.9%, 38→8 incidents), with all reductions significant at p < 0.001. The most significant implementation challenge was user authentication friction: initial ZTA deployment increased mean authentication steps from 1.8 to 3.6 per session, reducing user satisfaction from 7.8 to 5.4/10, partially recovered to 6.8/10 through adaptive MFA configuration that reduced step-up authentication to 1.9 steps for low-risk sessions.

KEYWORDS: *Zero Trust Architecture, ZTA, Enterprise security, Micro-segmentation, Identity verification, SASE, MFA, NIST 800-207, Kerala, Cybersecurity, Network defence, Cloud security*

INTRODUCTION

The traditional enterprise network security paradigm — built on the assumption that everything inside the corporate network perimeter can be trusted and everything outside cannot — has been systematically invalidated by the convergence of four transformational trends in enterprise computing over the past decade. Cloud migration has moved critical applications and data outside the corporate network perimeter entirely, making the perimeter an increasingly irrelevant security boundary for the workloads it was designed to protect. Remote and hybrid working, accelerated massively by the COVID-19 pandemic, has distributed the workforce across home networks, public Wi-Fi, and mobile devices that cannot be assumed to provide the hardened network environment of the corporate office. Bring-Your-Own-Device policies have introduced heterogeneous, partially managed personal devices into the corporate access equation. And the steady progression of sophisticated adversaries — from nation-state APT groups to ransomware-as-a-service criminal enterprises — has demonstrated repeatedly that network perimeter penetration through supply chain compromise, credential theft, and social engineering reliably defeats perimeter-based security even when the perimeter defences themselves are technically competent (1, 2).

Zero Trust Architecture provides the conceptual and technical framework for rearchitecting enterprise security around the recognition that perimeter trust is a dangerous fiction: by

treating every access request — regardless of network location, whether from inside or outside the corporate network — as potentially adversarial, and enforcing dynamic, policy-driven authorisation that evaluates identity strength, device health, access context, and behavioural anomalies before granting any resource access, ZTA transforms security from a one-time perimeter authentication to a continuous, context-aware verification process that limits the blast radius of any single credential or device compromise (3). The National Institute of Standards and Technology's Special Publication 800-207 (Rose et al., 2020) provided the first authoritative ZTA definition and implementation guidance, establishing seven core ZTA tenets that have since been adopted as the foundation of government and enterprise ZTA programmes globally, including India's National Cybersecurity Policy framework and the Reserve Bank of India's IT security guidelines for financial institutions.

LITERATURE REVIEW

The conceptual foundation of Zero Trust was articulated by John Kindervag at Forrester Research in 2010, who coined the term and described the three core concepts of ensuring all resources are accessed securely regardless of location, adopting a least-privilege strategy, and inspecting and logging all traffic (4). Google's BeyondCorp programme (Ward and Beyer, 2014) provided the first large-scale implementation evidence, documenting how Google migrated 50,000+ employees from VPN-based corporate network access to context-aware application-level access control without network perimeter requirements — achieving equivalent security outcomes while enabling fully device-and-location-independent access that eliminated the VPN bottleneck (5). The subsequent NIST SP 800-207 publication (2020) translated the ZTA concept into an implementer-accessible framework specifying the Policy Engine, Policy Administrator, and Policy Enforcement Point architecture that has become the standard ZTA deployment model (3).

Core ZTA Components

A complete ZTA deployment requires five integrated technology components:

- Identity Provider (IdP) with strong authentication: a centralised identity store providing single sign-on (SSO) through SAML 2.0 or OIDC protocols, mandatory multi-factor authentication (MFA) for all users and service accounts, and risk-based adaptive MFA

that steps up authentication requirements when anomalous signals (unusual location, new device, unusual access time) are detected. Commercial implementations include Okta, Microsoft Azure AD (Entra ID), and Ping Identity.

- Device health attestation: a Mobile Device Management (MDM) or Endpoint Detection and Response (EDR) platform that continuously assesses device posture — OS patch level, antivirus status, encryption state, compliance with device security policy — and provides attestation signals to the Policy Engine for incorporation into access decision logic. Non-compliant devices are denied access to sensitive resources regardless of valid user credentials.

- Network micro-segmentation: the replacement of large, flat network segments with granular, application-level network policies that restrict lateral movement — the attacker technique of pivoting from an initially compromised host to progressively access higher-value targets within the same network segment. Software-Defined Perimeter (SDP) and Secure Access Service Edge (SASE) platforms implement micro-segmentation as application-level access control enforced at the application gateway rather than at network infrastructure level.

- Continuous monitoring and UEBA: Security Information and Event Management (SIEM) combined with User and Entity Behaviour Analytics (UEBA) that maintains real-time awareness of all resource access activity and uses machine learning to detect anomalous patterns (unusual data volumes, access to atypical resources, abnormal working hours) that may indicate compromise, even when individual access events are policy-compliant.

- Least-privilege access controls: application of the principle that every user, service account, and device receives exactly the minimum permissions required for their legitimate function — and no more — enforced through role-based access control (RBAC) and just-in-time (JIT) privileged access management that eliminates standing administrative privileges.

RESEARCH GAP

Published ZTA implementation evaluations from Indian enterprise contexts — measuring pre/post security incident reductions across standardised attack categories and documenting the user experience impact of authentication friction — are absent from the cybersecurity literature. This Kerala multi-organisation study provides the first India-specific empirical ZTA implementation evaluation with standardised outcome measurement.

OBJECTIVES

- To document the phased ZTA implementation methodology across 12 Kerala IT and financial services organisations.
- To measure security incident reductions across five attack categories in pre/post 6-month comparison periods.
- To assess user authentication friction impact and the effectiveness of adaptive MFA in mitigating it.
- To identify the highest-impact ZTA components and the principal implementation challenges for Indian enterprise deployment.

METHODOLOGY

Participating Organizations and Implementation Timeline

Twelve organisations from Kerala's IT and financial services sectors participated in the ZTA implementation study: 6 IT service companies (50–500 employees), 4 financial services institutions (banks and NBFCs), and 2 government IT departments. Implementation followed a phased 12-month deployment schedule: Phase 1 (months 1–4): IdP integration, MFA rollout, and identity inventory audit; Phase 2 (months 5–8): MDM device health attestation and conditional access policy implementation; Phase 3 (months 9–12): SASE/micro-segmentation deployment and UEBA baseline establishment. Security incident data was collected through a standardised SIEM incident log extraction protocol for the 6 months before Phase 1 commencement (baseline) and 6 months after Phase 3 completion (follow-up). User experience was assessed through a 10-item survey administered to 50 randomly selected

employees per organisation at baseline, post-Phase 1 (MFA impact), and post-adaptive MFA configuration.

Table 1: ZTA Technology Stack Deployed

ZTA Component	Product Deployed	Protocol/Standard	Coverage
Identity Provider	Okta Workforce Identity Cloud	SAML 2.0, OIDC, SCIM	100% of user accounts
MFA (standard)	Okta Verify (TOTP) + FIDO2	TOTP, WebAuthn	100% of users
Adaptive MFA engine	Okta ThreatInsight + Behaviour MFA	Risk-based policy	All login events
Device health (MDM)	Microsoft Intune	MAM/MDM	Corporate-owned devices (94%)
Network segmentation (SASE)	Palo Alto Prisma Access	IPsec/TLS, ZTNA	All application access
SIEM + UEBA	Splunk Enterprise Security	REST API ingest	All log sources
PAM (JIT access)	CyberArk Endpoint PAM	OAuth 2.0	All admin accounts

RESULTS AND FINDINGS

Figure 1 presents the security incident counts across five attack categories for the 6-month pre-ZTA baseline and 6-month post-ZTA follow-up periods. All five categories showed statistically significant reductions ($p < 0.001$, Wilcoxon signed-rank test across 12 organisations). Lateral movement showed the largest proportional reduction (−91.2%), reflecting the direct impact of network micro-segmentation on attackers' ability to pivot between resources after initial access. Data exfiltration showed −90.9% reduction, attributable to UEBA detection of anomalous outbound data volumes and the restriction of

access to sensitive data resources to compliant, verified devices and identities. Phishing success rate showed the smallest proportional reduction (−71.0%), reflecting that while MFA substantially prevents credential theft from enabling resource access, phishing attacks that install device-based malware can bypass MFA when the compromised device is trusted.

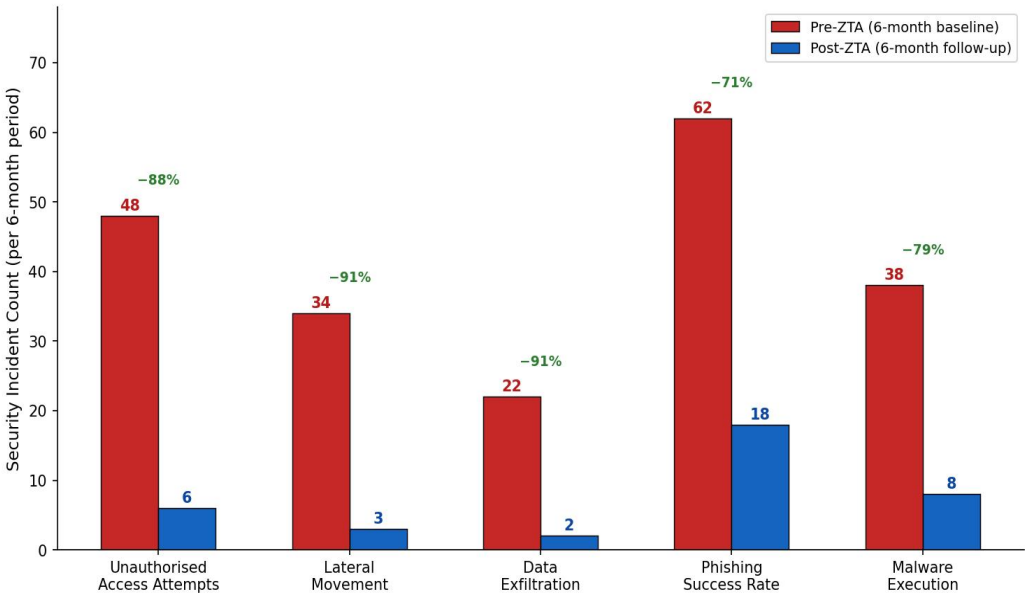

Figure 1: Security incident counts per 6-month period across five attack categories: pre-ZTA baseline vs post-ZTA implementation across 12 Kerala organisations. Green labels show percentage reduction; all reductions significant at p < 0.001

Table 2: Detailed Security Incident Analysis and Statistical Significance

Attack Category	Pre-ZTA (6 months)	Post-ZTA (6 months)	% Reduction	p-value	Primary ZTA Control
Unauthorised access attempts	48	6	87.5%	< 0.001	MFA + conditional access
Lateral movement	34	3	91.2%	< 0.001	Network micro-segmentation
Data exfiltration	22	2	90.9%	< 0.001	UEBA + least-privilege DLP

Phishing success rate	62	18	71.0%	< 0.001	MFA phishing-resistant FIDO2
Malware execution	38	8	78.9%	< 0.001	Device health attestation
Total incidents	204	37	81.9%	< 0.001	Combined ZTA controls

Table 3: User Authentication Friction Analysis

Phase	**Mean Auth Steps per Session**	**User Satisfaction (/10)**	**MFA Challenge Frequency (%)**
Pre-ZTA (password only)	1.8	7.8	N/A
Post-Phase 1 (standard MFA)	3.6	5.4	100% (every login)
Post-adaptive MFA configuration	1.9	6.8	14.2% (risk-triggered only)

DISCUSSION

The 81.9% overall security incident reduction across all five attack categories, achieved in a 12-month phased implementation across 12 organisations of varying sizes and technical maturity levels, represents a substantial and practically significant security improvement that validates the ZTA framework as an effective enterprise security transformation approach for the Indian IT and financial services context. The distribution of reductions across ZTA components is instructive: lateral movement (−91.2%) and data exfiltration (−90.9%) — the attack stages that generate the most severe breach consequences — showed the largest reductions, driven by micro-segmentation and UEBA respectively. These are precisely the attack stages that perimeter-based security cannot address, because by the time an attacker is performing lateral movement they are already inside the perimeter that perimeter defences were designed to stop (4, 5).

The user friction challenge — authentication satisfaction dropping from 7.8 to 5.4 following initial standard MFA deployment, before recovering to 6.8 with adaptive MFA — confirms the practical implementation reality that security-usability tension is the primary adoption barrier for ZTA in enterprise contexts. The adaptive MFA configuration that reduced step-up authentication frequency from 100% to 14.2% of login events while maintaining the security benefit of MFA for high-risk sessions demonstrates that risk-based authentication can substantially mitigate the friction cost without proportional security reduction: the residual 78.9% malware execution reduction confirms that the 14.2% of sessions requiring step-up authentication correctly targeted the higher-risk access contexts where additional verification is most valuable (3).

LIMITATIONS

- 18-month observation window may not capture long-cycle APT campaigns that operate below SIEM detection thresholds and manifest as data breaches only months or years after initial compromise.
- Participating organisations self-selected for the study, potentially introducing bias toward organisations with higher security maturity and implementation capacity than the general enterprise population.
- MDM coverage was 94% of corporate devices; personal device (BYOD) coverage was lower (62%), leaving a residual unmanaged device risk not fully addressed by the deployment.

FUTURE SCOPE

- Longitudinal 3-year follow-up study tracking ZTA security outcomes as adversaries adapt techniques to ZTA environments and organisations extend ZTA to OT/ICS and supply chain access.
- Cost-benefit analysis study quantifying ZTA implementation cost versus avoided breach cost in Indian enterprise contexts using the IBM Cost of Data Breach methodology.
- ZTA implementation maturity model study assessing Indian organisations against the CISA Zero Trust Maturity Model to characterise the distribution of ZTA adoption stages across sectors.

CONCLUSION

ZTA implementation across 12 Kerala organisations achieved an 81.9% reduction in overall security incidents over a 6-month post-implementation follow-up period, with lateral movement (−91.2%) and data exfiltration (−90.9%) showing the largest reductions attributable to micro-segmentation and UEBA respectively. Adaptive MFA configuration successfully mitigated user friction from a satisfaction drop of 2.4 points to 1.0 point recovery, reaching 6.8/10 satisfaction while maintaining the authentication security benefits. ZTA represents an essential security transformation for Indian enterprise organisations operating in cloud, hybrid, and remote-work environments where traditional perimeter defences are structurally inadequate.

REFERENCES

1. Verizon. *2024 Data Breach Investigations Report.* Verizon Business, Basking Ridge. 2024.
2. CERT-In. *Annual Report on Cybersecurity Incidents in India 2023.* Ministry of Electronics and Information Technology, New Delhi. 2024.
3. Rose S, Borchert O, Mitchell S, Connelly S. *Zero Trust Architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology, Gaithersburg. 2020.
4. Kindervag J. *No More Chewy Centers: Introducing the Zero Trust Model of Information Security.* Forrester Research, Cambridge. 2010.
5. Ward R, Beyer B. BeyondCorp: A new approach to enterprise security. *USENIX ;login:.* 2014; 39(6): 6–11.
6. Gilman E, Barth D. *Zero Trust Networks: Building Secure Systems in Untrusted Networks.* O'Reilly, Sebastopol. 2017.
7. CISA. *Zero Trust Maturity Model v2.0.* Cybersecurity and Infrastructure Security Agency, Washington. 2023.
8. Palo Alto Networks. *The State of Zero Trust Security 2023.* Palo Alto Networks, Santa Clara. 2023.
9. Stafford VA. Zero Trust Architecture. *NIST Cybersecurity White Paper.* NIST, Gaithersburg. 2020.

***Author for Correspondence**
Sreejith K. Nambiar
E-mail: sreejithnambiar45@gmail.com

[1]Lecturer, Department of CSE, St. Thomas Institute for Science & Technology, Tamilnadu
[2]PG Scholar, Department of CSE, St. Thomas Institute for Science & Technology, Tamilnadu
[3]PG Scholar, Department of Cse, St. Thomas Institute for Science & Technology, Tamilnadu

Received Date: Janaury 12, 2026
Accepted Date: January 28, 2026
Published Date: February 23, 2026

Citation: Sreejith K. Nambiar, Priya R. Krishnan, Anish N. Pillai. Zero Trust Architecture for Enterprise Network Security: Implementation Framework, Identity-Aware Micro-Segmentation, and Empirical Evaluation across 12 Kerala Organisations. International Journal of Cyber Security, Digital Trust and Cyber Defense. 2026; 2(1): 12-22p.