WHITE PAPER

ZERO TRUST BEYOND PERIMETERS: A PRACTICAL GUIDE FOR ENTERPRISE SECURITY LEADERS

Abstract

Organizations are operating beyond traditional perimeters—across cloud platforms, mobile endpoints, and remote workforces—where implicit trust creates exploitable gaps. Zero Trust Architecture (ZTA) inverts the legacy assumption of 'trusted inside, untrusted outside' by continuously validating identity, device posture, and context before granting the least privilege access to specific resources. This white paper provides a concise, vendor-neutral blueprint for leaders to plan and execute a Zero Trust program. It synthesizes recognized models (NIST SP 800-207; Forrester ZTX), defines core building blocks (identity, device, network, application, and data controls), and offers a pragmatic roadmap with governance and metrics. Drawing on field experience, it highlights common pitfalls—from legacy integrations to change management—and provides actionable best practices to mature posture iteratively. The paper includes a high-level reference architecture and an implementation example to help security and IT teams align strategy with operations while maintaining user experience and compliance.

Infosys®
Navigate your next

Overview and Industry Problem

Perimeter-centric security was designed for castle-and-moat networks with managed devices and centralized applications. Modern enterprises distribute users, apps, and data across SaaS, IaaS/PaaS, and partner ecosystems. Attackers routinely exploit credentials, unmanaged endpoints, and flat networks to move laterally after an initial foothold. Compliance mandates increasingly expect risk-based access controls and demonstrable monitoring.

These realities make implicit trust dangerous: VPNs grant broad network access; shared secrets persist; and visibility gaps obscure insider and supply-chain risks. Zero Trust addresses this by making identity, device health, and context the new control plane for granular, session-based access—verifying every request and limiting blast radius through segmentation and continuous analytics.

Recommended Solution

Zero Trust is a strategic program—not a single product—that aligns people, process, and technology to enforce '**never trust, always verify**'. A practical solution stacks the following capabilities and integrates them through a policy engine (PDP) and enforcement points (PEP):

Identity & Access Management

SSO, MFA, phishing-resistant auth; role- and attribute-based access; step-up and conditional access.

Device Trust

Posture assessment (OS, patch, EDR, encryption); block or restrict access for non-compliant endpoints.

Network & Segmentation

Software-defined perimeters; micro-segmentation around applications and data; east–west inspection.

Application & Workload Security

Strong app identity (mTLS), API gateways, workload isolation, secret management.

Data Protection

Classification, DLP, encryption, key management; contextual policies near the data.

Visibility & Analytics

Centralized telemetry (SIEM/UEBA), behavior analytics, threat intel, automated response (SOAR).

Policy Engine & Governance

Risk scoring, continuous evaluation, standard controls codified as policy-as-code with change management.

Architecture Diagram

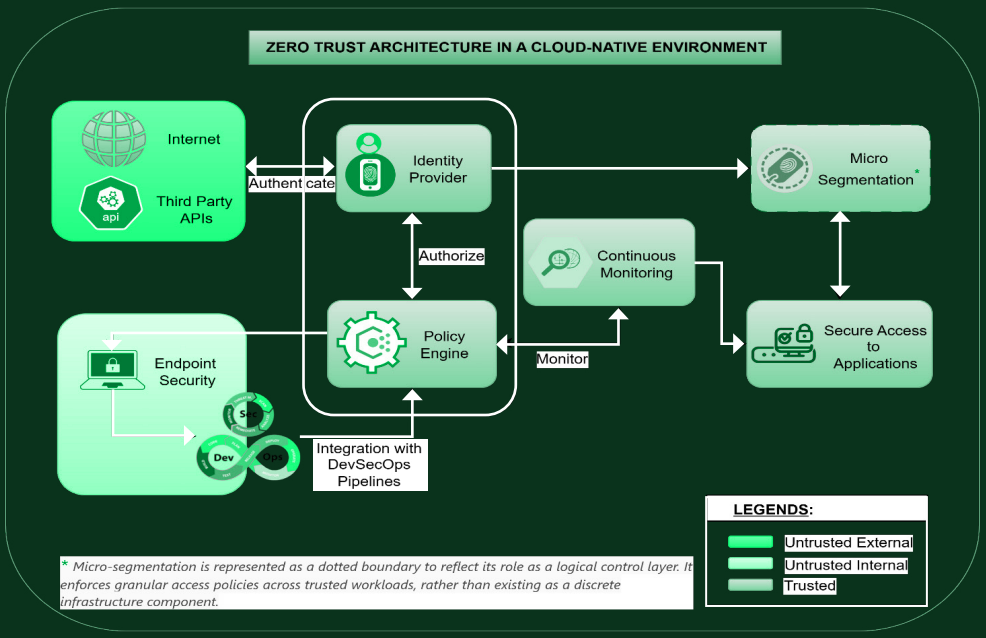

Figure 1: High-level Zero Trust Reference Architecture

Recommended Best Practices

Start with identity as the control plane

Consolidate identities, enforce MFA, and prefer phishing-resistant methods.

Adopt least privilege by design

Role/attribute-based access; just-in-time (JIT) and just-enough-access (JEA).

Continuously evaluate device health

Gate access on posture; block high-risk or unknown endpoints.

Replace broad VPN with ZTNA

Broker app-level access; no direct network connectivity.

Segment everything meaningful

Micro-segment critical apps and data; monitor east–west traffic.

Protect data where it lives

Classify, encrypt, and enforce DLP with contextual policies.

Instrument for visibility

Centralize logs (IdP, EDR, ZTNA, cloud) into SIEM; build detections and KPIs.

Automate response

Integrate SOAR/playbooks for containment (isolate endpoint, revoke tokens, step-up auth).

Design for user experience

Minimize prompts; use risk-based, adaptive controls and SSO.

Secure third parties

Use identity federation, scoped access, and device attestation for vendors/contractors.

Governance & change management

Define standards, exceptions, and communication; measure adoption and risk reduction.

Iterate

Run pilots, collect feedback, expand coverage, and continuously tune policies.

Conclusion

Zero Trust is not a one-time purchase, it's an ongoing journey toward sustained risk reduction and operational maturity. By prioritizing identity, device posture, and least-privilege access; enabling comprehensive telemetry; and scaling through iterative pilots, organizations can significantly reduce their attack surface while enhancing user experience and meeting compliance requirements.

References

1. NIST Special Publication 800-207: Zero Trust Architecture (defines the Zero Trust paradigm, components (PDP/PEP), and deployment patterns.)

   https://csrc.nist.gov/publications/detail/sp/800-207/final

2. CISA Zero Trust Maturity Model — https://www.cisa.gov/zero-trust-maturity-model
3. Forrester Zero Trust eXtended (ZTX) (focuses on protecting data by controlling users, devices, networks, workloads, and automation across the ecosystem.)

   https://www.forrester.com/report/Apply+Zero+Trust+To+Your+Security+Strategy/-/E-RES136133

4. Microsoft Zero Trust guidance — https://learn.microsoft.com/security/zero-trust/
5. Microsoft Entra ID (Azure AD) documentation — https://learn.microsoft.com/entra/identity/

About the Author

Sivaramakrishna SV
Lead Consultant

Sivaramakrishna is a Technology Consultant at Infosys CyberSecurity with over 12 years of experience in the cybersecurity domain. He has extensive expertise in production support and implementation for global clients. Currently, he serves as a Cybersecurity Technology Architect for a leading banking client, driving secure and resilient technology solutions.

For more information, contact askus@infosys.com

Infosys®
Navigate your next