BROADCOM®

Executive Summary

A ZTA Primer—The Critical Technical Components of Zero Trust Architecture

Zero trust architecture (ZTA) is reshaping modern cybersecurity by enforcing strict, context-based access controls. This enforcement is the essential component of a mature ZTA and the technical enablers needed to support ZTA implementation.

Foundational Principles

Zero trust rejects implicit trust in users, devices, or network segments. It assumes compromise at all levels and requires:

- Continuous verification of access conditions
- Granular least privilege enforcement
- Microsegmentation to contain breaches
- Data-centric protection to safeguard assets at rest, in transit, and in use

A critical concept is the **zero trust agent (ZT agent)**—a dynamic construct that evaluates multiple trust attributes, including user identity, device posture, location, behavior, and context. Access decisions must adapt in real time as these conditions evolve.

ZT Application Across Five Pillars

ZTA must be implemented consistently across five domains:

- **Identity:** Users and services must be authenticated with multifactor and contextual verification.
- **Device:** Both managed and unmanaged devices must be assessed for compliance and vulnerabilities.
- **Network:** All traffic must be encrypted, monitored, and segmented.
- **Applications and workloads:** Application security must consider user, session, and environment context, while minimizing privileges.
- **Data:** Data must be identified, labeled, and controlled independently of its storage or transmission path.

Cross-Cutting Capabilities

Three capabilities are essential for ZTA maturity:

Visibility and Analytics

Organizations must log, monitor, and analyze access behavior across all five pillars.

Automation and Orchestration

AI and SOAR tools are needed to enforce policies and respond to threats at scale.

Governance

Clear policies and controls must align with business goals and be continuously enforced.

Implementation Guidance

ZT implementation is a journey, not a destination. Organizations should:

- Start small—such as applying zero trust network access (ZTNA) to one application.
- Integrate with existing governance structures to identify opportunities.
- Balance trade-offs between encryption, monitoring, and operational needs.
- Align ZTA with existing compliance frameworks for efficient progress.

Conclusion

Zero trust is more than a security strategy—it's a shift in mindset. By embedding presumption of compromise and enforcing continuous validation across identity, devices, networks, and data, ZTA transforms how organizations manage risk. With careful planning, incremental implementation, and the right technologies, organizations can modernize their security posture, enhance data protection, and reduce the impact of inevitable breaches.

Enabling Technologies

ZTA is not a single product, but an architecture enabled by key technologies:

Segmentation Gateways (e.g., NGFWs, SASE platforms)

Enforce policy between trust zones.

Local Host Security

EDR, host firewalls, and posture assessments are vital for validating and protecting endpoints.

Identity, Credential, and Access Management (ICAM)

Enables granular, identity-based access controls.

SIEM and SOAR

Centralize telemetry, drive analytics, and orchestrate automated responses.

SANS | Research Program