Enigma Networks

Network-Centric Zero Trust

From ZTNA to ZTNX: Completing the Zero Trust Architecture

From ZTNA to ZTNX: Completing the Zero Trust Architecture

Executive Summary

Zero Trust is not a product—it's a strategy. Yet most Zero Trust implementations focus almost entirely on access control. Zero Trust Network Access (ZTNA) has emerged as the dominant model for securing remote users and applications, but it leaves a massive gap: what happens after access is granted. This white paper introduces ZTNX: Zero Trust for Internal Networks—a new architectural layer that extends Zero Trust deep inside the network to address lateral movement, internal visibility, and breach containment.

1. Zero Trust Today: Powerful But Incomplete

ZTNA has redefined how users securely access enterprise applications. By replacing VPNs with identity-aware access brokers, organizations have enforced least privilege and reduced external attack surfaces. However, once access is granted:

- There is little visibility into what users or workloads do next
- Internal traffic (east-west) remains implicitly trusted
- Segmentation is coarse or outdated
- Insider threats and compromised accounts move freely

ZTNA stops threats at the door. But today's attackers often start from within.

2. The Internal Network: Zero Trust's Final Blind Spot

Modern enterprises are sprawling, hybrid, and dynamic. As identities and endpoints multiply, the network interior has become:

- Unseen: Most organizations cannot baseline or monitor east-west communication
- Uncontrolled: Few controls exist between workloads once access is allowed
- Vulnerable: Lateral movement is the default attack path in most breaches

Without Zero Trust inside the network, attackers thrive in what should be trusted zones.

3. Introducing ZTNX: Zero Trust for Internal Networks

ZTNX is the missing layer of the Zero Trust architecture. Where ZTNA secures access, ZTNX secures what happens next. It brings Zero Trust principles to traffic, behavior, and segmentation inside the network by:

- Continuously verifying post-access activity
- Discovering all internal assets and flows
- Baseline normal behavior and detecting anomalies
- Recommending segmentation policies to reduce blast radius
- Integrating with SOARs and enforcement points for active response

ZTNX extends Zero Trust beyond authentication into the living, breathing activity of your environment.

4. ZTNA vs. ZTNX: A Complementary Architecture

Capability	ZTNA	ZTNX
Primary Focus	Access control (pre-session)	Internal behavior (post-session)
Traffic Type	North-south (user ↔ app)	East-west (system ↔ system)
Trust Boundary	Before connection	Throughout session
Control Model	Brokered access	Visibility + behavioral enforcement
Enforcement	Gateway, policy engine	Anomaly detection, segmentation, SOAR

ZTNA and ZTNX are not competitors—they are complementary layers that together deliver holistic Zero Trust.

5. ZTNX in the Zero Trust Stack

ZTNX completes the Zero Trust Architecture by providing internal visibility and continuous enforcement at the network behavior layer.

Zero Trust Layer	Focus	Example Vendors
Identity-Centric ZT	User verification	Okta, Microsoft Entra
Endpoint-Centric ZT	Device posture	CrowdStrike, SentinelOne
ZTNA / Access-Centric ZT	Session brokering	Zscaler, Palo Alto Prisma
Network-Centric (ZTNX)	Internal behavior & flows	**Enigma AI™**

ZTNX complements all these layers and fills the internal security gap they leave behind.

6. Enigma AI and ZTNX: Purpose-Built for the Internal Layer

Enigma AI is the first platform to implement ZTNX as a unified, agentless Zero Trust layer inside the network. Key capabilities include:

- Agentless internal visibility via SPAN ports or cloud packet mirroring
- Passive asset discovery and inventory of all internal systems
- Behavioral baselining and ML-powered anomaly detection
- Segmentation intelligence with recommended policy enforcement
- SOAR integration for orchestrated blocking and containment

Enigma AI complements your ZTNA stack, SIEM, and EDR by closing the most dangerous blind spot: what happens after access.

7. Use Cases and Business Impact

ZTNX enables outcomes that matter to security and business leaders:

- Stop lateral movement from compromised accounts or insider threats
- Reduce breach dwell time from weeks to minutes
- Visualize internal flows for segmentation hygiene and compliance
- Lower TCO with agentless deployment and fewer false positives

Conclusion:

ZTNX Completes Zero Trust

ZTNA solved one half of the Zero Trust puzzle. ZTNX solves the other.

With the rise of sophisticated threats, hybrid infrastructure, and identity sprawl, organizations must go beyond access control. ZTNX brings Zero Trust to the internal network experience—where risk lives, and where current tools fall short.

Enigma Networks® is proud to lead the ZTNX movement. To learn more or see the platform in action, visit **getenigma.ai** or request a demo today.

Enigma Networks