Validation for Microsegmentation

Zero Trust Requires Zero Assumptions

Microsegmentation is essential to any Zero Trust architecture—but most deployments stop at enforcement and skip validation. That's a dangerous gap. Many organizations assume their policies are working, but lateral movement still happens. Attackers exploit drift, overlooked exceptions, and misconfigured firewalls to bypass boundaries silently.

Traditional segmentation approaches rely on manual configuration, the deployment of agents, or, a complete infrastructure overhaul—leaving security teams guessing whether controls are working as intended.

Securing modern infrastructure requires both automated segmentation and continuous verification—from design to daily operations.

Automated Enforcement Meets Continuous Validation

Horizon3.ai and Zero Networks bring together autonomous testing and automated enforcement to deliver segmentation that's both actionable and accountable.

Zero Networks automatically enforces segmentation through agentless, host-based firewall orchestration that scales across all environments.

Horizon3.ai's NodeZero® Offensive Security Platform continuously validates segmentation by probing communication paths attackers would use.

This closed-loop approach eliminates lateral movement risk and confirms—on demand or continuously—that your segmentation strategy is providing the expected outcomes.

Zero Networks Microsegmentation

Zero Networks makes enforcement as seamless as validation.

- Orchestrates segmentation via native host firewalls
- Automatically classifies assets and generates per-asset policies
- Supports dynamic tagging for scalable, adaptive policy enforcement

Organizations deploy Zero Networks across any environment without agents or re-architecture.

Achieve segmentation in days, not quarters.

NodeZero Segmentation Test

NodeZero emulates attacker behavior to validate segmentation policies in a production-safe, scalable way.

- Runs safe, read-only probes across defined source and target scopes
- Detects unintended access or policy violations in real-time
- Provides clear, actionable findings to security, compliance, and network teams

No exploits. No disruption. Just proof.

Key Benefits

Proof-Driven Defense
Continuously test segmentation effectiveness using attacker logic, not assumptions

Rapid Time to Enforcement
Deploy Zero Networks across hybrid networks and cloud workloads

Fewer Moving Parts
Simplify segmentation by avoiding architectural disruption or new enforcement layers

Audit-Ready Reporting
Validate and document segmentation controls with confidence

Policy That Evolves with You
Dynamic enforcement and validation adjust automatically as your environment changes

Use Case: Enforcing and Validating Segmentation at Scale

A leading financial institution needed to implement segmentation and validate that lateral access was effectively blocked in alignment with corporate security policies. Compliance, audit visibility, and attacker resistance were key evaluation priorities for any proposed solution. Through their partnership with an MSSP, a joint solution was implemented:

- Zero Networks enabled rapid, agentless segmentation across the institution's infrastructure.
- NodeZero continuously tested and validated enforcement across source and destination scopes.

The financial institution gained an automated enforcement and validation system that scales with change—while maintaining Zero Trust confidence.

Segmentation You Can Prove

Security should never rely on trust or guesswork, Zero Networks & NodeZero provides ongoing segmentation and validation, refining and testing policies for accuracy, all with nearly zero effort.

> **Segmenting your network is just step one. Proving segmentation works is how you stop breaches.**
>
> **Albert Estevez Polo**
> *Field CTO, Zero Networks*

ZERO Networks

Learn more

About Zero Networks

Zero Networks is a pioneer in automated microsegmentation and network security. Our agentless microsegmentation solutions provide effortless deployment, automatically learning and classifying endpoints to generate precise security policies that orchestrate native firewalls. By preventing unauthorized lateral movement, enforcing just-in-time multi-factor authentication for privileged access, and enhancing protection for critical assets, we empower organizations across every sector to strengthen their security posture with minimal effort.

HORIZON3.ai

Learn more

About Horizon3.ai

The NodeZero® Offensive Security Platform by Horizon3.ai drives continuous exposure management across production infrastructure. With NodeZero, customers overcome barriers of limited security talent and infrequent, expensive penetration testing. They stay ahead of a rapidly-evolving threat landscape with autonomous pentesting, emerging threat intelligence, threat detection, and unified data and reporting. Founded in 2019 by former industry leaders and U.S. National Security veterans, Horizon3.ai solves diverse use cases across all industries.