

MICROSEGMENTATION SOLVED

Living off the Land Defense

The building blocks for containment already exist in your environment – Zero Networks orchestrates them at scale.

In living off the land attacks, threat actors use an operating system's own admin tools to blend in with normal activity and evade detection. Zero Networks turns that logic into an architectural principle – and a defensive advantage. We put what's already running in your environment to work, adding a central intelligence and orchestration layer on top of the native host-based firewalls built into every OS.

For years, living off the land has been an adversarial tactic. With Zero, defenders can reclaim it to build a self-defending network architecture – comprehensive microsegmentation with no agents (unless necessary), no latency, no manual policy creation, and no added complexity.

The Problem

Enterprises need security solutions that protect critical operations without introducing new outage risks. Traditional microsegmentation tools ask you to deploy an agent across every asset, then keep feeding those agents updates indefinitely – implementation takes years, manual work never ends, and every update carries a chance of failure.

The result is a forced tradeoff: accept security gaps or layer on more environmental complexity.

>90%

of cyber incidents are materially enabled by environmental complexity and tool sprawl

Unit 42, 2026 Global Incident Response Report

↑\$208K

the average added cost for a data breach when security system complexity is a factor

IBM, 2026 Cost of a Data Breach Report

How Zero Networks Solves It

The tools for proactive containment have existed on enterprise networks for 20 years, but manually coordinating policy across thousands of systems, identities, and workloads was impossible without adding agents and introducing new points of failure – until now.

Zero Networks delivers microsegmentation by centrally managing native OS firewalls directly and enforcing policy through them.

✓ Agentless Architecture

Zero seamlessly integrates with existing infrastructure and any host-based firewall, connecting through the operating system's own management interface to govern existing controls.

✓ Intelligent Orchestration

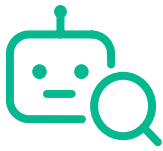
Each platform's native firewall has its own gaps. Zero's engineering closes them across every OS, delivering a consistent enforcement layer that effectively addresses individual weaknesses without introducing new complexity.

✓ Network-Layer MFA

Privileged access is gated by just-in-time MFA enforced at the network layer – not a separate, proprietary tool bolted on top. Using the same central enforcement layer, Zero's network-layer MFA only opens privileged access to pre-approved identities after JIT verification – and only temporarily.

✓ Deterministic Control

Zero takes a deterministic, human-on-the-loop approach to microsegmentation, automatically translating observed behavior into enforceable least-privilege policy at scale. The result is unprecedented speed to protection without relying on probabilistic guesswork for enforcement.



AI needs a deterministic babysitter

Just a 1% error rate in security policy can break the business – microsegmentation vendors that rely on AI-driven policy creation and enforcement are risking uptime on a statistically likely inference. As AI adoption accelerates in enterprise environments, you can't reliably secure AI infrastructure with another probabilistic model guessing what's safe. Zero delivers the deterministic enforcement layer modern networks need, building policies based on real, observed behavior and automatically enforcing boundaries as the network evolves.

From Discovery to Enforcement with Zero

1



Discover

Zero automatically pinpoints every asset, identity, and AI agent on the network

2



Learn

Observes real communication patterns to build rules based on what's actually needed

3



Generate Policy

Deterministic, explainable policies are built from observed baselines

4



Simulate in a Sandbox

Run generated rules against real traffic to test before enforcement

94% of Zero's automated rules are used exactly as produced

5



Enforce in Rings

Roll segmentation enforcement out in controlled waves

6



Continuously Maintain

Zero dynamically adapts policies as the environment changes

What a Living off the Land Defense Means for You

- **Fast, non-disruptive rollout:** Live in days, not years – no hardware upgrades or complex configurations to stall segmentation progress.
- **Fewer points of failure:** One unified enforcement layer, not a fragile stack of agents deployed on endpoints across enterprise environments.
- **Lower ongoing overhead:** No agent-update lifecycle to manage or troubleshoot means no hidden costs or added headcount requirements.
- **Reduced outage risk:** Zero’s agentless solution avoids kernel-level exposure, eliminating the added environmental complexity that puts uptime at risk.

What This Replaces

Traditional Microsegmentation	Zero Networks
Deploy new infrastructure and install agents broadly	Use the infrastructure you already have
Manually author policy	Automatically generate policies from real traffic
Invest in professional services	0.25 FTE for ongoing administration
Constant maintenance and tuning	Protection dynamically adapts to changes

+90%

Network microsegmentation coverage within 90 days

87%

Enterprise cost savings vs. traditional segmentation

ESG Technical Validation Report



Zero Networks is the only microsegmentation vendor with a 5/5 Gartner Peer Insights rating and 100% willingness to recommend



“Zero Networks is an elegant and simple solution for a very difficult problem ... It’s using technology that we’ve already had on the network for 20 years. For as long as we’ve had firewalls, we could have done this. We just couldn’t manage the firewall at scale. You couldn’t manage the firewall intelligently. We had every piece of the solution there – what we did not have was the brains that Zero Networks brought into the process.”

— Henry Mayorga, CISO, Baron Funds



**See how Zero Networks unlocks
preemptive cyber resilience with
a living off the land approach to
microsegmentation.**

Request a Demo

