

Shrink Your Internal Firewall Footprint Up to 79% with Zero Networks

How three organizations of different sizes achieved the same result: fewer firewalls, tighter segmentation, and real savings.

Most internal firewall estates have the same problem: the appliances enforce policy at the edges of security zones and almost nothing inside of them.

Here's how a regional healthcare provider, a multi-site manufacturer, and a global financial services firm solved that challenge with Zero Networks, taking out 67%–79% of internal firewalls – and saved hundreds of thousands of dollars.

Before Zero Networks: Paying for Segmentation That Didn't Exist

Three organizations ranging from SMB to enterprise shared a common set of challenges before implementing identity-based microsegmentation:



Firewalls guarded zone edges, not what was inside of them:

Each zone held dozens or hundreds of servers, reachable on any port. Most server-to-server traffic never passed a firewall at all.



Clients were never behind an east-west firewall:

Endpoints sat on flat campus VLANs where any workstation could reach any other on RDP, SMB, or WinRM.



Rulebases outgrew the teams that wrote them:

Rules were often unused, shadowed, or lacked a single owner.



Enforcement sat on the network path, where anything could route around it:

A routing change, a new VLAN, or a VM provisioned into the wrong port group was enough to undo a boundary.

SMB

Regional healthcare provider
~750 staff · 15 sites
900 clients · 140 servers

MIDMARKET

Multi-site manufacturer
~4,000 staff · 45 sites
5,000 clients · 1,020 servers

ENTERPRISE

Global financial services
~28,000 staff · 180 sites
35,000 clients · 8,700 servers

Six internal firewalls across DC server zoning, a PCI and billing zone, and the medical-device VLANs. 1,400 rules, 35% unused or shadowed.

24 internal firewalls and 6,200 Panorama rules, 40% unused or shadowed. East-west hairpinning had outgrown the licensed capacity.

120 internal firewalls carrying 48,000 rules across five management planes with no single owner. The largest zones held 200-plus servers.

With Zero: Replacing Internal Firewalls with Identity-Based Microsegmentation

	SMB Regional healthcare provider	MIDMARKET Multi-site manufacturer	ENTERPRISE Global financial services
What changed with Zero	4/6 internal firewalls eliminated. The four unpatchable Server 2012R2 boxes went from sitting behind a zone boundary to individually ringfenced. A \$180K medical-device segmentation project was cancelled outright.	18/24 internal firewalls eliminated. Client-to-client reachability is now zero, closing the path a phished laptop had used to reach 200+ workstations. Containment fell from four hours to under a minute.	95/120 internal firewalls eliminated. A repeat audit finding on legacy rule justification, three years running, was closed. Two management clusters and their log collectors were decommissioned.
What stayed	One mid-range pair fronting a vendor-managed imaging enclave, where the contract mandates IPS inspection.	OT cell pairs at the two largest plants for Modbus and DNP3 inspection at the Purdue 3/3.5 boundary, plus one DC pair held in monitor-only.	The regulated trading enclave, DMZ-internal pairs at two datacenters, M&A isolation until integration completes, and a few third-party-owned segments.
Audit impact	HIPAA evidence moved from a rulebase export the auditor took on faith to per-asset policy with continuous proof. Segmentation and MFA moved to “yes” on the cyber-insurance renewal.	PCI DSS 4.0 cardholder scope shrank. The Req 11.4.5 segmentation test went from eleven zone boundaries to a targeted one, and the QSA accepted host-based enforcement as the control.	DORA, NIS2, ISO 27001 and NIST CSF 2.0 evidenced at asset level; the SOX ITGC deficiency closed. The network-controls portion of the annual exam cycle fell from nine weeks to three.

What Came Off the Budget: Different Scale, Consistent Outcome

Between recurring spend eliminated, hardware refreshes avoided, and tool consolidation or cancelled upgrades, Zero Networks saves organizations hundreds of thousands of dollars when they swap internal firewalls for granular microsegmentation.

	SMB	MIDMARKET	ENTERPRISE
Internal firewalls eliminated	4 of 6 (67%)	18 of 24 (75%)	~95 of 120 (79%)
Recurring spend eliminated	~\$59K/yr	~\$312K/yr	~\$2.0M/yr
Hardware refresh avoided	~\$150K	~\$540K	~\$5.6M
Other confirmed savings	~\$180K project cancelled	~\$300K upgrade, ~\$90K/yr MSP	~\$800K/yr platform, SIEM & change desk
Capacity returned	0.45 FTE	1.9 FTE	5.5 FTE

Modelled customer profiles built on unit-cost assumptions: Low-end / branch: \$6K subscription + \$3K support + \$1K facilities = \$10K recurring, on roughly \$15K of hardware; Mid-range: \$12K + \$6K + \$1K = \$19K recurring, on roughly \$60K of hardware; High-end datacenter: \$30K + \$14K + \$2K = \$46K recurring, on roughly \$175K of hardware. Recurring cost covers subscriptions, support and maintenance; hardware is counted once as an avoided refresh rather than amortized into recurring spend.

**Learn how you can cut costs and
achieve more comprehensive
protection with Zero Networks.**

Request a Demo

ZERO.
Networks