

SPEND LESS, CONTAIN MORE

Optimizing Security Spend with Zero Networks

Enterprises need fewer attack pathways, not more tools. Recapture budget dedicated to point solutions and manual configuration with Zero.

The average business juggles 83 different security tools – that complexity can cost organizations more than 5% of their annual revenue.¹ As cyber leaders face pressure to reduce the cost of security, they need a reliable way to contain threats and spending.

Instead of adding another layer of tooling, Zero Networks addresses the underlying exposure that made so many of those tools necessary in the first place. That means security outcomes improve, complexity shrinks, and spending gets sharper.

Where You Can Spend Less When You Have Zero Networks

Budget Category	What Drives Spending	How Zero Networks Reduces It
Internal/East-West Firewalls	Hardware, licensing, support, ongoing rule maintenance	Zero provides granular internal control and host-based enforcement – meaning there's no need to buy, license, or support firewalls for segmentation. Policies automatically generated from observed traffic eliminate the ongoing manual burden.
Network Access Control (NAC)	License, hardware, support	With identity-driven microsegmentation, network admission is no longer a separate control to buy, so there's no additional license or appliance needed.
PAM	Licensing (often per privileged account), deployment services, vaulting/rotation infrastructure, user experience friction	Internal pathways are closed by default, policies follow identities across the network, and privileged access is secured with just-in-time MFA; that means less reliance on PAM's vault servers, connectors, and session-proxy infrastructure – plus, no more costly deployment services and no operational friction.

¹ IBM, [Capturing the Cybersecurity Dividend Study](#)

Endpoint Firewall Add-Ons	Add-on licensing bundled or purchased separately for host-based firewall control	Host-based firewall enforcement is already covered – no need to pay for an add-on functionality.
Manual Configs, GPOs, Segmentation Changes	Security engineer hours spent on manual policy/rule work, higher risk of downtime caused by brittle policies	Policy is learned, created, enforced, and maintained automatically via a deterministic engine, returning hours of FTE bandwidth every week while adaptively protecting uptime.
Compliance Reporting & Audits	Internal audit-prep hours, external audit/consulting cost	Continuous evidence is generated automatically and available on demand, cutting the internal hours spent pulling audit exports and reducing reliance on consultants to run compliance projects.

Hard Cost Elimination, Reduction, and Tool Consolidation

Some of the highest-cost items in the security stack are compensating for gaps that Zero Networks closes directly – when the underlying exposure shrinks, so can the spend.



Reduce Internal Firewall Footprint by 74%²

When firewalls are built to guard the edges of security zones – not what’s inside of them – most server-to-server traffic never passes a firewall at all, and a routing change, a new VLAN, or a misconfigured port group can quietly undo a boundary that took months to build and leave the business vulnerable to outages.

With Zero Networks:

- Lateral movement pathways close, east-west traffic is granularly controlled by default
- No additional appliances to buy, license, or support for internal network segmentation
- Policies are generated and updated automatically based on observed traffic – no rulebase to write or maintain manually



Reduce Network Access Control (NAC) Footprint by 40–50%³

NAC defines whether a device should be allowed onto the network at all, and enforces that decision through dedicated hardware, licensing, and support.

With Zero Networks:

- Identity governs reachability at the network layer – admission is no longer a separate control to buy
- No NAC licensing or support contract to maintain
- Access controls adapt automatically, no admission layer configuration necessary as devices join or leave the network



Reduce Privileged Access Management (PAM) Footprint by 30–40%⁴

Rotating a password doesn't necessarily revoke access when a valid Kerberos ticket can outlive the credential behind it, even though PAM is intended to stop compromised credentials from delivering expansive network access.

With Zero Networks:

- A compromised credential or stolen ticket leads to a dead end – the path doesn't exist to exploit
- Admin protocols (RDP, SMB, WinRM, RPC) are closed by default and only open just-in-time after network-layer MFA verification
- Reduced reliance on PAM's vault servers, connectors, and session-proxy infrastructure as the primary line of defense; no more hidden deployment costs



Reduce Endpoint Firewall Add-Ons by 100%⁵

When endpoint platforms bundle host-based firewall control as a separate, paid add-on layered on top of the core agent, organizations absorb an extra line item to manage what a device can reach on the network. Instead, embrace defense in depth by letting EDR focus on its core objective.

With Zero Networks:

- Host-based firewall enforcement governs reachability – the add-on function is redundant
- No per-endpoint firewall policy to maintain as devices and access needs change

Soft Costs: Operational Savings and Efficiency

The labor hours spent on configuration, manual rule tuning, and policy creation and maintenance represent one of the largest hidden security costs. Zero Networks replaces manual burden with deterministic, highly accurate automation.



Manual Configurations, GPOs, and Segmentation Changes

Every new server, every access request, and every audit finding that calls for a rule change means another manual task – and added cost.

With Zero Networks:

- Policies are generated from observed traffic via deterministic, human-on-the-loop automation; they can be tested in a sandbox environment before go-live
- Teams can recapture 10–15 hours per engineer, per week – time that was previously spent on policy maintenance – and can manage 2–3x more assets without adding headcount
- Enterprises save 87% compared with traditional segmentation strategies⁶

^{4, 5} Zero Networks Customer Data

⁶ ESG Report, [Technical Validation of the Zero Networks Platform](#)

Compliance Automation

Audit readiness usually depends on point-in-time evidence pulled together under a deadline. With a real-time network map and granular policy enforcement, Zero Networks takes teams from resource-intensive checkbox exercises to automated, enforced compliance.



Reporting and Audits

Audit prep typically means pulling rulebase exports, documenting exceptions, and hiring additional consultants to build the segmentation evidence that auditors expect.

With Zero Networks:

- Every segmentation policy, access event, and enforcement action is logged automatically and continuously
- The combination of network segmentation, identity-based access control, network-layer MFA, and Zero Trust network access covers the core of major frameworks like PCI DSS 4.0, NIST 800-53, and more
- No fire drills for security teams and no need to dedicate budget to consultants for compliance initiatives

Uptime Protection and Risk Reduction

Downtime costs Global 2000 companies an average of \$300 million per year, with a price tag of \$15,000 per minute; nearly a third of unplanned outages are directly cybersecurity related.⁷ Zero Networks doesn't just reduce the cost of security investments – it **avoids** the cost of a disruptive attack, making containment the default posture so uptime is protected even when something goes wrong.



Proactive Breach Containment

A single compromised endpoint can reach 85% of the environment directly.⁸ That reachability turns a minor cyber incident into a major business crisis before analysts investigate the first alert. Between incident response fire drills and operational disruptions, the cost of an uncontained breach can quickly stretch into the millions.

With Zero Networks:

- Every asset, identity, and AI agent is segmented automatically – including the service account the agent runs on and the egress path it needs – so breaches are contained to the initial point of compromise
- Network-layer MFA enforces just-in-time verification for all privileged internal pathways
- Uptime is protected; the business keeps running through attacks

⁷ [The Hidden Costs of Downtime Report 2026](#)

⁸ Zero Networks, [Threat Analysis: One Compromised System and BOOM, Meet Your Blast Radius](#)

See how Zero Networks optimizes security budgets with a built-in containment layer that cuts the cost of overlapping controls, consulting-heavy projects, and manual policy maintenance.

Request a Demo→