Buy Protection, Not a Segmentation Project

Why Enterprises Are Choosing Zero Networks over Legacy Microsegmentation

Microsegmentation can't be another never-ending, multi-year project. The goal isn't visibility into network traffic. It's containing attacks, shrinking the blast radius, and keeping the business running. And against AI-driven attacks, time to protection is what matters most.

Legacy microsegmentation racks up operational costs long before it enforces anything: agent deployment, asset tagging,manual policy work, testing, exceptions, and maintenance. None of it appears in the software quote, yet it decides whether the project succeeds or stalls.

Zero Networks takes a different approach: automated, agentless-first microsegmentation that protects without adding operational burden.

A Control That Manages Itself, Not a Project You Manage

The difference isn't features. It's how much work it takes to deploy, enforce, and maintain protection

Criteria	Akamai · cisco · illumio Legacy Approach	ZERO Networks The Zero Networks Difference
Deployment	Extensive, manual agent installation on every machine; requires hefty infrastructure preparation	**Agentless-first; 90% agentless enforcement with a lightweight agent option available for enterprises who require them**
Asset tagging	Manual tagging, grouping, and ongoing maintenance	**Automated, optional tagging; no manual taxonomy required to start or manage**
Policy creation	Significant manual policy design and tuning	**Policies automatically generate from observed behavior and dynamically update when new assets and identities leave or join the network**
Time to protection	Extended deployment, learning, and validation; often only covers the crown jewels	**90%+ network protection in weeks, with staged enforcement**
Ongoing operations	Continuous policy updates and exception management	**Automated policy lifecycle and optimization**
Change risk	Extensive testing and change-window coordination	**Simulation and controlled enforcement**
Professional services	Costly professional services are often needed for implementation and ongoing software management	**No professional services costs with Zero; we're focused on enablement, not ongoing manual labor**

Every month spent building policies or deploying agents is another month systems stay exposed. Success is measured by how many systems are protected, and how fast – not how many are discovered, tagged, or monitored.

Zero Networks put that to the test against a real AI attacker. In a lab evaluation, Zero Networks ran Claude Code as a standard domain user on a workstation in a segmented, enterprise-style environment. The AI attacker only compromised the one deliberately unsegmented host. Every protected system stayed out of reach.

Zero Networks Eliminates the Hidden Tax of Microsegmentation

Licensing is only part of the total cost of ownership. Over three years, legacy approaches carry seven hidden costs:

- **Mechanic tax:** Dedicated personnel to design, deploy, tune, and maintain segmentation.
- **Policy tax:** Manual policy authoring, reviews, exceptions, and approval cycles.
- **Tagging tax:** Creating and continuously maintaining asset classifications.
- **Infrastructure tax:** Deploying agents, managing upgrades, and coordinating changes.
- **Maintenance tax:** Ongoing policy updates as applications and infrastructure evolve.
- **Delay tax:** Extended exposure while deployment and policy development progress.
- **Outage tax:** Application testing, change windows, and the operational consequences of incorrect enforcement.

Zero Networks automates most of that burden away. Across customer deployments:

- **90% agentless enforcement** with lightweight agents only where customers want them or where agentless won't work.
- **94.2%** of automatically generated rules never require manual edits.
- **Approximately 45 days** median time to a segmented asset, including customer change processes.
- **Less than 0.01% false-positive rate,** supported by simulation and validation before enforcement

Proven at Enterprise Scale

Gartner Peer Insights reviews from customers with more than $10 billion in annual revenue.

> "Invoking MFA for end users using RDP, for example, has been a game changer! Tremendously easy to set up and deploy. We don't need to hire an FTE to feed and water the platform. It genuinely just works as advertised. It has already paid for itself by preventing a pretty gnarly lateral movement attempt"
>
> **IT Associate**
>
> *Read the Gartner Peer Insights Review*

> "We were able to roll out segmentation in controlled weekly waves, review expected blocks with system owners, and use break-glass procedures when troubleshooting was required"
>
> **Director of IT Security and Risk Management**
>
> *Read the Gartner Peer Insights Review*

> "Great product, unbelievably easy to rollout and have it up and running! We deployed several thousand end points in 2 months! Almost too good to be true!"
>
> **Director of IT**
>
> *Read the Gartner Peer Insights Review*

See the Zero Networks difference.

Request a Demo