ZERO Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

USE CASES

Reduce Security OpEx and See Immediate ROI

TL;DR

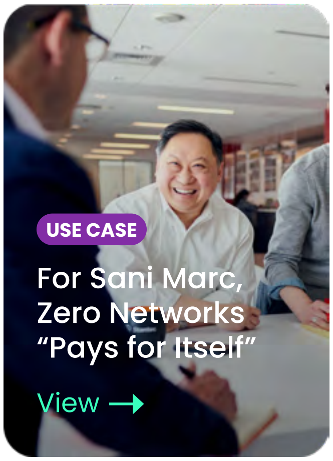
Traditional network segmentation is expensive. Hardware firewalls are costly, deployment is lengthy, and ongoing maintenance heavily relies on professional services for continuous, manual rule updates. Legacy microsegmentation, using software firewalls, is no different.

Zero Network's agentless and automated microsegmentation architectures is fast to deploy and requires nearly no maintenance – saving a staggering 83% of the cost of traditional segmentation and 71% of the cost of legacy microsegmentation.

Segmenting Your Network? Get Ready to Pay Out The Nose.

Traditional network segmentation is heavily relying on high capital expenditures to buy or replace expensive firewalls, and high operating expenditures on professional services for configuration (manually creating rules that do not break the environment) and ongoing maintenance.

Legacy microsegmentation that uses software firewalls also requires high OpEx on lengthy deployment, manual rule creation and ongoing maintenance.



USE CASE

For Sani Marc, Zero Networks "Pays for Itself"

View →

What makes segmentation so costly?

Traditional Segmentation with hardware firewalls

- Expensive firewalls to buy or replace.
- Lengthy deployment: Rules/policies are created manually.
- Lengthy maintenance: Rules/policies must be continuously updated manually.
- Reconfiguration needed every time hardware changes.
- Hundreds of hours to set up.

Legacy Microsegmentation with software firewalls

- Lengthy deployment: Installing agents on each machine, manually reviewing and creating rules/policies.
- Lengthy maintenance: Human review of rules and activities, manually changing rules as applicable.
- Hundreds of hours to set up.
- Hairpinning

Both traditional segmentation and legacy microsegmentation require a lengthy configuration – a process that involves spending hundreds, and sometimes thousands of hours manually setting each firewall rule (of which there can be thousands, or even tens of thousands). To get everything set up, someone must sit there, look at and think about each rule--one by one.

The amount of time it takes to get segmentation up and running can be staggering, but that's just the beginning. Even if you've already made the investment and your network is finally segmented, these solutions are far from "set and forget". Anytime there's a change that requires old rules to be updated or new rules to be created (e.g., adding a new business unit), you need someone to come in and look at each rule and manually update it. On top of that, you need to constantly reevaluate existing rules to make sure you are not leaving any vulnerabilities open, as well as delete rules that are no longer needed—a complex, time-consuming process that incurs more expenses.

Glossary

What is Network Segmentation?

View ⟶

What is Microsegmentation?

View ⟶

What is multi-factor authentication (MFA)?

View ⟶

The Zero Networks Difference

Both traditional segmentation and legacy microsegmentation require a lengthy configuration – a process that involves spending hundreds, and sometimes thousands of hours manually setting each firewall rule (of which there can be thousands, or even tens of thousands). To get everything set up, someone must sit there, look at and think about each rule--one by one.

The amount of time it takes to get segmentation up and running can be staggering, but that's just the beginning. Even if you've already made the investment and your network is finally segmented, these solutions are far from "set and forget". Anytime there's a change that requires old rules to be updated or new rules to be created (e.g., adding a new business unit), you need someone to come in and look at each rule and manually update it. On top of that, you need to constantly reevaluate existing rules to make sure you are not leaving any vulnerabilities open, as well as delete rules that are no longer needed—a complex, time-consuming process that incurs more expenses.

The Numbers

For the average mid-market organization with about 2,000 users and 300 servers, Zero Networks saves a staggering 83% of the cost associated with traditional segmentation using hardware firewalls, and 71% of the cost associated with legacy microsegmentation using software firewalls. These savings are calculated over a period of 3 years.

In each of these scenarios, Zero Networks cuts the costs associated with long deployment times, hiring 2-3 full time employees for ongoing maintenance and rule management, as well as IT or helpdesk costs to respond to any network access requests users might have.

Check out the Zero Networks Segment ROI Calculator to receive a breakdown of the cost savings of Zero Networks for your organization, compared with the estimated costs of traditional segmentation and legacy microsegmentation vendors.

MFA Included: Increase ROI by 30%

One of the core features of Zero Networks Segment is the ability to apply MFA on every port, protocol, and application. This allows organizations to drop existing MFA enablement solutions and increase ROI by an additional 30%.

While other vendors apply MFA only to Active Directory authenticationbased applications, therefore susceptible to attackers exploiting vulnerabilities and servers that are not domain joined Zero Networks ties MFA to the network layer to protect any application/protocol, denying attackers access to to anything and everything in the organization including even zero days vulnerabilities.

The Bottom Line:

	Traditional Segmentation	Legacy Microsegmentation	Zero Networks
Deployment	Hardware firewalls	Agents	Agentless
Setup Time	Hundreds of hours	Hundreds of hours	10 hours
Maintenance per month	Tens of hours	Tens of hours	1-2 hours
Segmentation granularity	Segment per site / network segment	Segment per server	Segment per anything (Clients, Servers, OT/IoT, on-prem and in the cloud)
Segmentation capabilities	Area to area	Server to server	Everything to Everything (Clients, Servers, OT/IoT, on-prem and in the cloud)

ABOUT SRC CYBER SOLUTIONS LLP

SRC Cyber Solutions LLP is a renowned name in India for Cybersecurity. We are known for our exclusive distribution of cutting-edge solutions in India, GCC, Africa and APAC. We take pride in offering a comprehensive suite of Cybersecurity solutions which includes Platforms and Technologies for AI-powered Comprehensive Email Security, Automated Patch and Endpoint Management, Asset Visibility and Risk Management, securing the Cloud environments with Hybrid Cloud Workload Protection, enhancing Network Security with Agentless Micro- Segmentation, ensuring Third-Party Data Flow Management and API Management, and Agentless Compliance Management, thereby strengthening our commitment to protecting organizations against evolving known and unknown Cyber Threats. With a focus on embracing innovation, we continuously evolve to meet the dynamic threat landscape, offering a comprehensive range of Nex-Gen technologies with a high degree of automation, reducing the dependency on IT Resources and ensuring a strong value proposition.

ZERO. Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS