CASE STUDY

For Sani Marc, Zero Networks “pays for itself”

ZERO Networks

Introduction

The Canadian chemical manufacturer saves 3x by choosing Zero Networks over a legacy microsegmentation vendor and an additional 30% by removing an existing Identity tool

Photos by Sani Marc © All rights reserved.

Microsegmentation is the “gold standard” of preventing lateral movement—the first step towards achieving Zero Trust. But microsegmentation has a reputation for having a hefty price tag and a long, labor-intensive deployment process that often ends up in broken applications.

What if full microsegmentation could be achieved quickly and with no hassle, without the high cost? What if a microsegmentation solution could be radically simple to deploy and manage, and actually save your organization money?

For Sani Marc, a leading chemical manufacturing company in Québec, Canada, simple segmentation has become reality. They chose Zero Networks Segment™ to protect their network against lateral movement. The result? They were able to achieve full, automated microsegmentation in 30 days, without burdening IT personnel, disrupting normal operational activities, or breaking the bank.

How Sani Marc Saved 3x on Microsegmentation

$180k Upfront savings by choosing Zero Networks Segment™ over VMware NSX’s high deployment and maintenance cost.

$150k Additional cost savings by being able to remove the zero-trust identity solution currently in place.

<30d To achieve full, automated microsegmentation (vs. estimated 3-6 months for hardware solution).

No additional IT members required for deployment and ongoing maintenance.

What Sani Marc was looking for

Sani Marc has 16 offices across Canada, and one in Europe, multiple datacenters as well as multiple warehouse sites that rely on IoT equipment.

The firm has firewalls to protect the perimeter, and EDR for endpoints. “However, most threats are not coming from the outside,” says George Henderson, Sani Marc’s IT Manager, “they come from a user that ‘invites’ someone inside the network with either an email or a URL they click on. So, we wanted to put something on the inside to protect us from lateral movement if anyone got in.”

Sani Marc has a small IT team of six people, so the solution needed to be easy to deploy and relatively low maintenance. Another challenge was the need for flexibility, and for the solution to be able to evolve with the firm as it grows and changes.

> *“We wanted to put something on the inside to protect us from lateral movement*

Shopping for a solution

Sani Marc considered three options and selected Zero Networks:

Hardware Solution

Why rejected:

- Required a six-month deployment
- Required changing all firewalls
- Lots of ongoing maintenance and reconfigurations
- Could not achieve full microsegmentation (client-to-client segmentation not supported)

VMware NSX

Why rejected:

- Protects VMware VMs but not clients or other servers outside of VMware
- Was $180k more expensive than Zero Networks over three years due to high cost of maintenance

Zero Networks Segment™

Why Selected:

- Protects servers, clients and OT without any agents
- Automated creation of rules/policies
- Option to apply MFA on every port, protocol and application
- Took only 30 days to fully microsegment the network, with nearly no human supervision

With Zero Networks, Sani Marc knew they could have all the benefits of a robust microsegmentation solution without the downsides like additional overhead and a long deployment process.

The results

By choosing Zero Networks over VMware NSX, Sani Marc had 3X upfront savings on deployment as well as ongoing maintenance. But once things were up and running, there was an additional cost saving benefit. The firm had been using an externally hosted zero-trust identity solution which it now plans to drop, saving them an additional $150k over three years. "Basically, Zero Networks would be paying for itself," says Henderson.

Sani Marc achieved full microsegmentation of all its clients and servers in just 30 days, in an automated process that was, according to Henderson, "95% hands off".

After 30 days of monitoring and learning all connections on the Sani Marc network, Zero Networks Segment™ auto-created highly accurate rules that microsegmented the entire network without breaking anything. Henderson says the automated microsegmentation has been "transparent" for the end users. For any privileged connections, Sani Marc's IT admins are required to use self-service just-in-time multi-factor authentication (MFA).

"I knew that the AI was good, but I thought we'd have to add a few manual rules," says Henderson, "but basically, we didn't have to touch anything. We have special applications, so we had to add a couple of rules, which took 2-3 days of fine-tuning. Besides that, it pretty much runs itself."

"What we value the most is when you change a rule for a server, it's not minutes or hours for the rule to be applied by the firewall. It's almost instant."

When asked what adjectives describe Zero Networks, Henderson said: "Reliable, easy to deploy, surprisingly efficient, transparent for end users."

> *"I knew that the AI was good, but I thought we'd have to add a few manual rules. But basically, we didn't have to touch anything."*

To see a demo and learn more about Zero Networks Segment™, go to: zeronetworks.com

ZERO. Networks