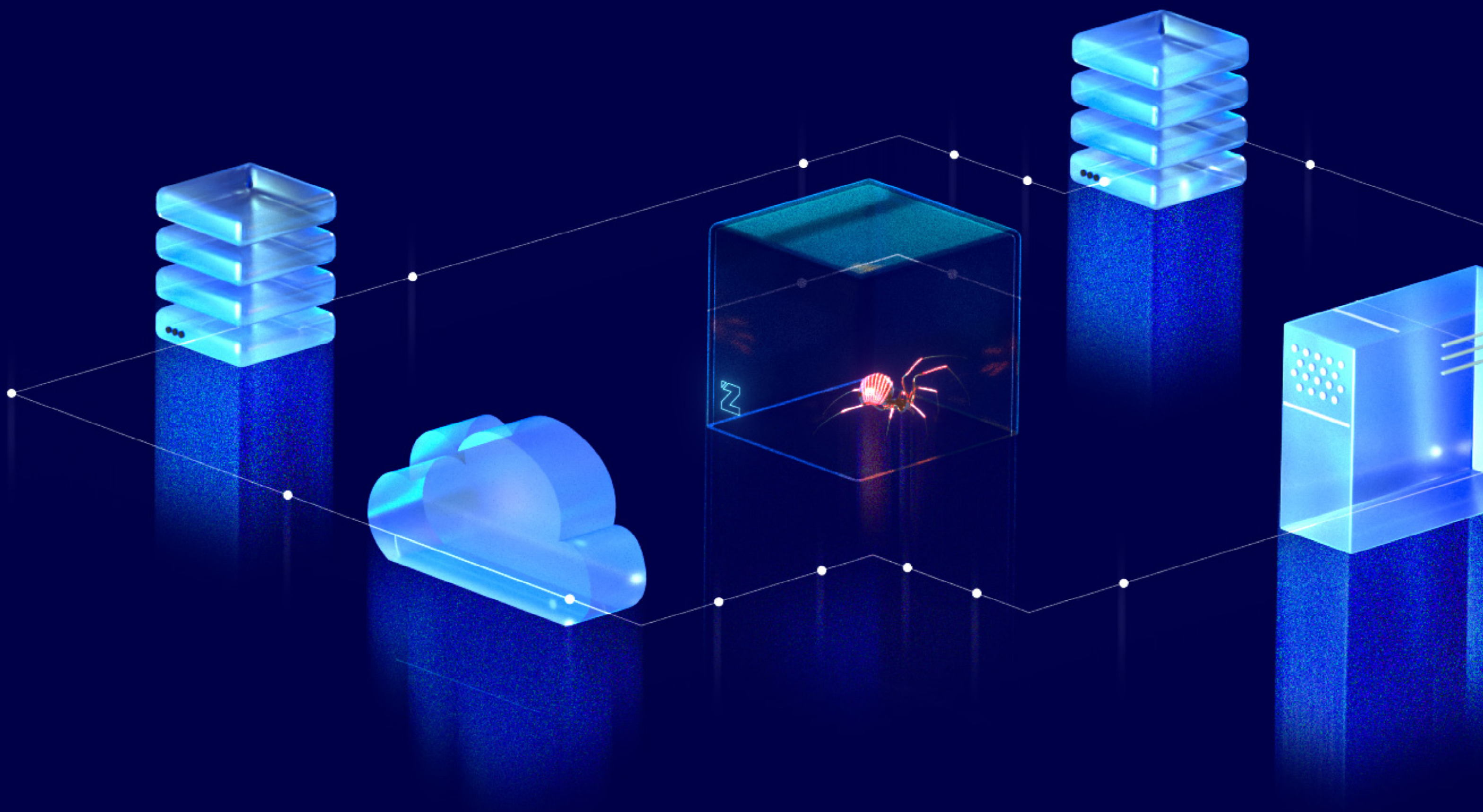
ZERO
Networks



Microsegmentation

A Buyer's Guide

Introduction

If you're a cybersecurity leader looking for better network segmentation to defend your organization against ransomware and lateral movement, then this guide is for you.

In it, we'll take a look at why lateral movement is one of the most basic and common tactics that attackers use to spread ransomware and access sensitive data. Then, we'll delve into microsegmentation: what it is and why old-school vendors could not provide it at scale. Finally, we'll lay out everything you should look for in potential microsegmentation solutions—from ease of deployment to integration with existing IT systems.

Our goal is to educate and support anyone looking to fully protect their network from ransomware and other advanced attacks by implementing microsegmentation in their organization.

The Dangers of Lateral Movement

When the history of cyber security is written, lateral movement will have the leading role as the villain. Most cyberattacks—even when they don't make the news—follow the same basic plot. It almost always starts with machine compromise, followed by recon, exploitation of a vulnerability and then a host of other tactics to move laterally and cause damage.

Luckily, this order of operations relies on a single basic assumption: the compromised machine will have direct network line of sight to other machines that the attacker can damage and steal information from. In other words, to stop attacks we need to stop lateral movement. This is where microsegmentation comes in.

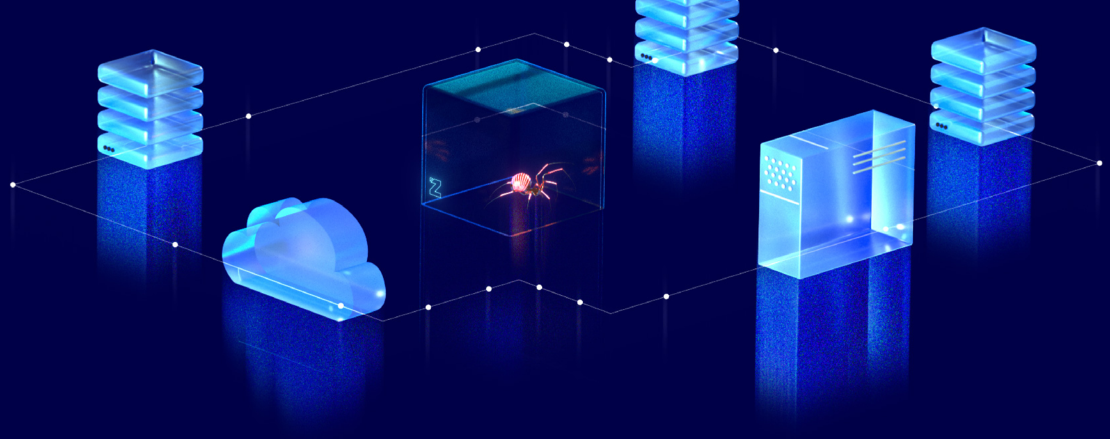
What is microsegmentation?

Microsegmentation is the practice of dividing a network into very small regions called microsegments, usually up to a segment per machine. The goal of microsegmentation is to reduce the attack surface of a network by isolating every element—all clients, workloads, applications, virtual machines, and operating systems—into its own protective barrier that cannot be penetrated by attackers. Segmenting the network in this way makes it virtually impossible for attackers to move laterally within the network and cause damage.

However, a network can consist of thousands, or even tens of thousands of elements on prem, in the cloud, at home, or in the office. Therefore, it can be extremely difficult to implement this type of segmentation manually. Luckily, you don't have to perform all this tedious work yourself, as many cybersecurity vendors offer microsegmentation as part of their solution. Still, this doesn't mean your job is done—not all vendors are created equal, so you need to be mindful when choosing one.

In the next section, we provide a "microsegmentation checklist" that will help you ask the right questions when shopping for a microsegmentation vendor that will fit your organization's needs.

You can also read more here



Microsegmentation Checklist

It can be difficult to evaluate the difference between one microsegmentation solution and the next. This is because many vendors will throw around the latest buzzwords and make claims that are hard to assess. In reality, not all microsegmentation solutions live up to this hype.

What things should security leaders look for when evaluating potential vendors? To answer that question, we've created the following guide.

For a microsegmentation project to truly succeed, it should meet the following criteria:

01

Is it easy to use?

In the past, microsegmentation was legendary for its difficulty and complexity. This is because manually segmenting a network that contains thousands, or even tens of thousands, of elements is virtually impossible. A modern solution must be much, much simpler to implement; ideally based on a set-it-and-forget-it approach that automates the entire process.

02

Does it incur any additional friction?

Today's security teams are stretched thin. A good microsegmentation solution does not incur the need for additional headcount. It also does not add incremental work on top of a laundry list of existing activities.

03

Will it start working quickly?

Historically, deploying a microsegmentation solution meant agents and painstakingly complicated configurations. But CISOs and security teams need to show quick wins, and fast deployment cycles are no longer optional. This means a good solution promises fast deployment, no agents, and no lengthy configurations.

04

Does it offer heterogeneous segmentation?

Today’s segmentation solutions often force you to decide between sequestering users, clients or servers. A modern approach should do it all–taking a heterogeneous approach to asset segmentation. In addition, it should offer a single point of control, both in cloud and on-premises environments.

05

Is it IT/OT agnostic?

OT infrastructure is common in modern enterprises. Typically, OT environments require a separate approach to segmentation. For a microsegmentation solution to truly succeed in today’s world, it should cover both OT and traditional IT environments.

06

Are there any single points of failure?

The old adage “you’re only as strong as your weakest link” no longer applies. An effective solution will have no single point of failure, to make sure availability is close to 100%.

07

Are there hidden costs associated with it?

A good microsegmentation solution should have no hidden costs. This is because a properly segmented network should lead to simplified network security operations, as well as reduced spending on NACs, internal firewalls, IPS and manual router, ACL-based segmentation.

08

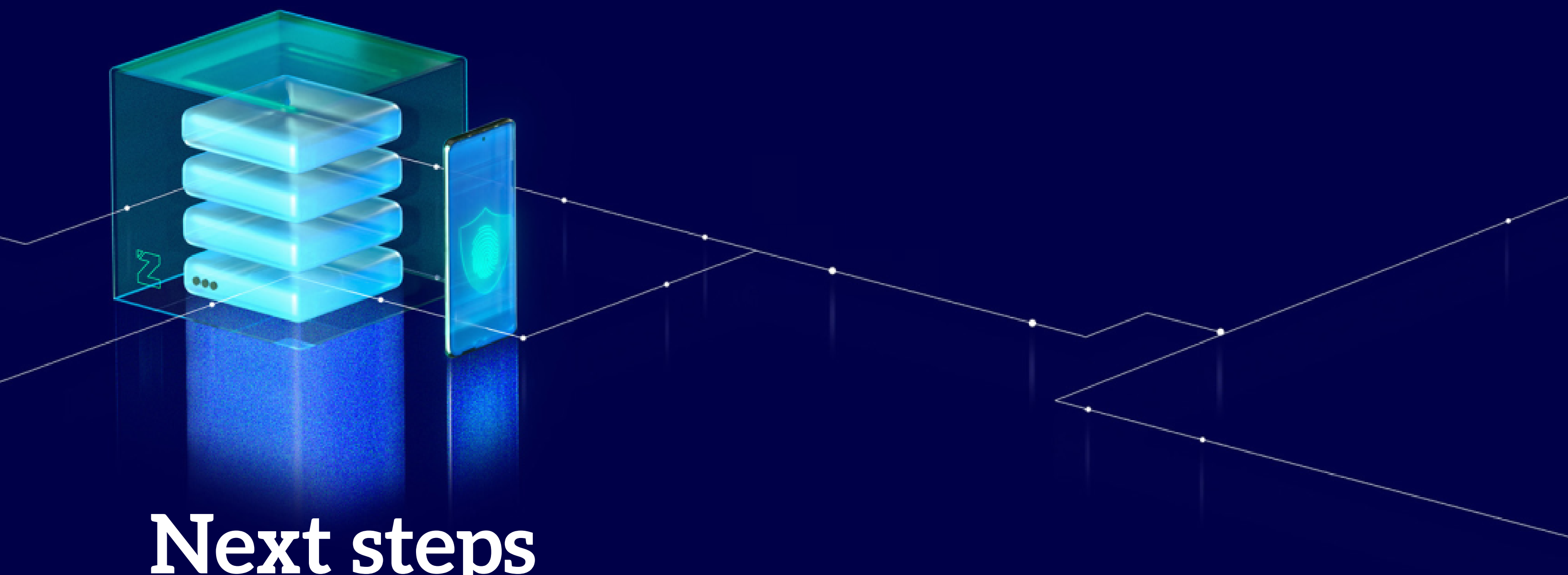
Does it offer ‘continuous segmentation’?

Modern networks are dynamic, which means there’s no time to discover everything in your environment—by the time you do, it has changed. Therefore, your microsegmentation solution of choice should automatically and continuously observe network access to identify the network permissions necessary for day-to-day activity.

09

Does it integrate with existing infrastructure?

A good microsegmentation solution should be engineered to ensure easy integration with existing IT infrastructure. This will guarantee that typical network usage patterns remain unaffected.



Next steps

First, a few words about us.

Zero Networks protects organizations of all sizes with **Zero Networks Segment**™—an automated microsegmentation solution that works at scale, and with the click of a button, without agents or painstaking manual rule creation. By leveraging MFA-everywhere, **Zero Networks Segment**™ blocks ransomware and completely stops lateral movement, all without interrupting normal network traffic. **Zero Networks Segment**™ is an award-winning solution that has deployed across many different verticals, including finance, healthcare, law, and manufacturing.

We wrote this guide to help cybersecurity leaders make sense of the often-confusing landscape of network segmentation solutions. Not all microsegmentation solutions are created equal, and choosing one that falls short is likely to end up being a futile effort, particularly at scale. However, when it's done right, microsegmentation can help your organization stay safe AND run smoothly.

We are proud to offer the first truly automated microsegmentation solution designed to work effortlessly at scale, with no additional operational effort.

Here's how we do it:

01 Is it easy to use?

An easy, agentless, scalable implementation

With **Zero Networks Segment**™, segmentation is automated; there's no need to manually segment thousands of elements. **Zero Networks Segment**™ remotely manages the host-based firewall of every operating system to both see and segment all assets—without any agents and without being in-line.

02 Does it incur any additional friction?

No extra overhead required

Because it's so easy to implement, **Zero Networks Segment**™ does not incur the need for additional work or extra headcount to manage and maintain, freeing up IT resources to work on other projects.

03 Will it start working quickly?

Speedy deployment

Not only is **Zero Networks Segment**™ easy to deploy, but it also works fast. With **Zero Networks Segment**™, you can segment your whole network, down to each individual machine, in a matter of minutes. It's basically microsegmentation at the click of a button.

04 Does it offer heterogeneous segmentation?

Designed for the modern network

Zero Networks Segment™ doesn't make you choose between segmenting users, clients or servers. You can segment anything and everything with one platform. Plus, you'll have one point of control for everything, whether it's on-prem or in the cloud.

05 Is it IT/OT agnostic?

Works in both OT and IT environments

Zero Networks Segment™ is OT/IT agnostic: our solution is configured to work in both types of environments.

06 Are there any single points of failure?

Eliminates points of weakness

Zero Networks Segment™ prevents 99% of attacks from spreading and causing damage by taking every single machine and putting it in its own segment. This leaves no room for an attack to succeed—if there's a breach, there's no way for it to spread.

07 Are there hidden costs associated with it?

Cost-effective

Zero Networks Segment™ is a software-defined microsegmentation solution that reduces the need for spending on other security solutions such as internal firewalls and NACs.

08 Does it offer ‘continuous segmentation’?

Requires no manual monitoring

Zero Networks Segment™ keeps itself up-to-date by automatically monitoring network access and identifying which permissions are necessary.

09 Does it integrate with existing infrastructure?

Plays nice with existing infrastructure

Zero Networks Segment™ integrates easily with existing infrastructure and any host based firewall. With **Zero Networks Segment**™ deployed, typical network usage patterns remain unaffected.

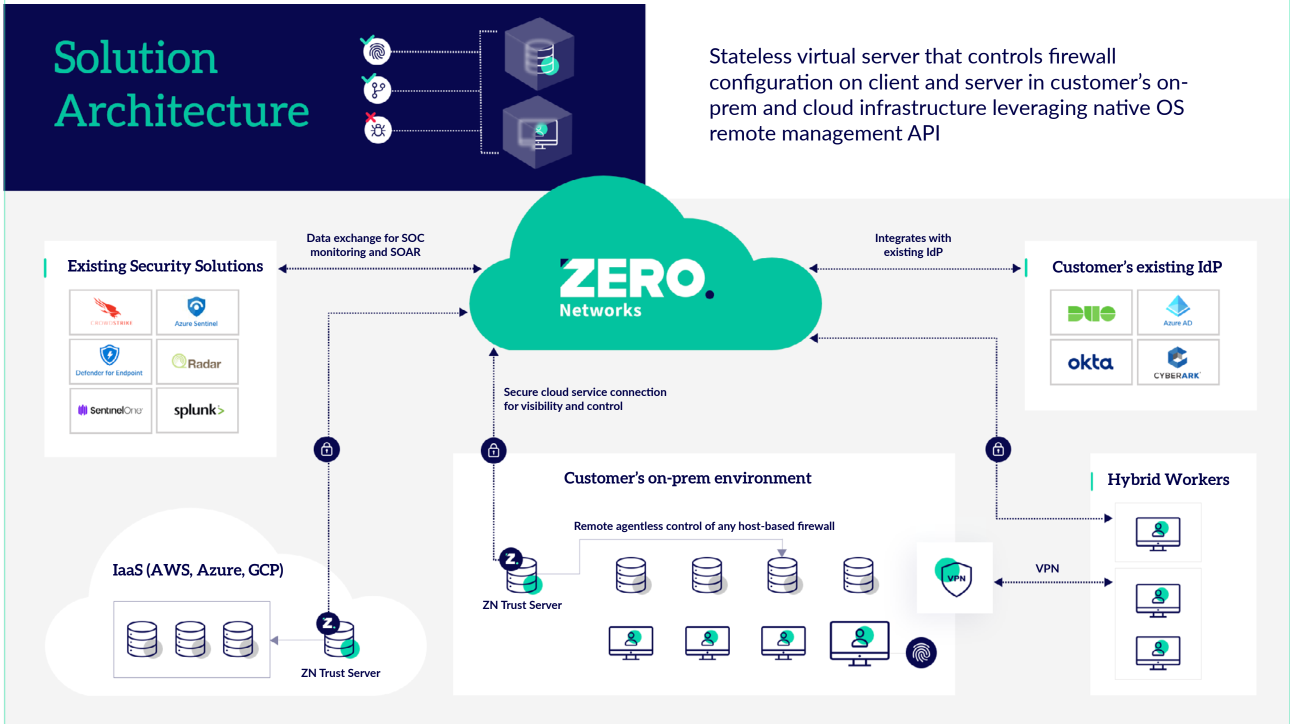
Bonus

Untethered to hardware

Finally, **Zero Networks Segment**™ removes hardware from the segmentation equation—you can move and change any router, firewall or network security appliance without having to migrate your segmentation policies to the new hardware.

Solution Architecture

Stateless virtual server that controls firewall configuration on client and server in customer's on-prem and cloud infrastructure leveraging native OS remote management API



Existing Security Solutions
CROWDSTRIKE
Azure Sentinel
Defender for Endpoint
Radar
SentinelOne
splunk>
Data exchange for SOC monitoring and SOAR
ZERO. Networks
Integrates with existing IdP
Customer's existing IdP
DUO
Azure AD
okta
CYBERARK
Secure cloud service connection for visibility and control
IaaS (AWS, Azure, GCP)
ZN Trust Server
Customer's on-prem environment
Remote agentless control of any host-based firewall
ZN Trust Server
VPN
VPN
Hybrid Workers

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

ZERO. Networks

ZERO.
Networks