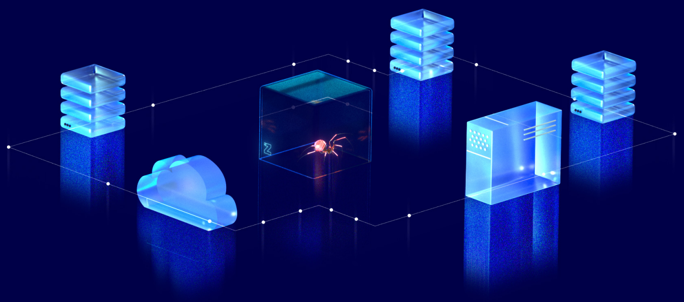
ZERO.
Networks

Zero Networks Segment™ makes segmentation the easiest and most effective way to protect your organization



Why do ransomware and advanced attacks continue to succeed?

Excessive network permissions allow attackers to move freely in the network. Networks are built for connectivity, not security. This inherent flaw means users and machines have way more network access than they will ever need. Once an attacker compromises one machine inside the network, it's easy for them to spread and do whatever they want.

The Zero Networks Solution

Zero Networks Segment™ is an MFA-based segmentation solution that **automatically restricts network access** to only what users and machines actually need. When a compromise occurs, attackers are boxed in and unable to move around the network and spread to additional hosts. In light of the continuous increase in attacks' sophistication and frequency, **Zero Networks Segment™ creates a military-grade network security posture** to help prevent ransomware and attackers from successfully spreading and causing damage.

How does it work?

Zero Networks Segment™ allows enterprises to segment every and any asset in their network at scale with a click of a button to protect against lateral movement. Our patented methodology combines **simple**, **deterministic**, and **predictable automation** to keep the necessary network permissions open, while falling back on self-service MFA when network permissions are missing.

Our **self-service MFA** approach focuses on administrative protocols used in most attacks, and used mainly by admins. By contrast, day-to-day employees don't experience any change in workflow or experience.

Offered as a subscription, Zero Networks' cloud-based service **integrates with any organization's infrastructure** to dynamically manage user and machine network access. All subscriptions include maintenance and support.

> "Finally a network segmentation and control solution that can scale without adding additional costs"
>
> **Malcolm Harkins** Former CISO of Intel

Gartner
COOL
VENDOR
2020™

“Essentially putting every computer and server on the network into their own individual DMZ”

Key Capabilities

Common use cases where our customers use Zero Networks Segment™:

01

Ransomware kill switch: With an airtight, properly segmented network, organizations dramatically reduce the likelihood of ransomware spreading through their network.

02

Segment everything with a click to radically improve security while reducing CapEx and OpEx.

03

Pass pen tests by universally applying MFA and segmentation.

04

Lower operational costs by replacing old network security solutions with a modern one that utilizes automation and self-service.

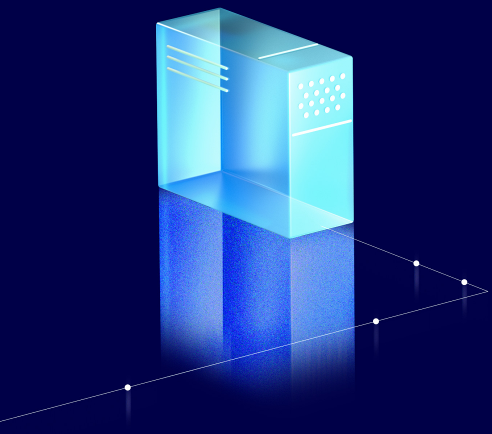
05

Extend MFA to every machine in the organization.

06

Comply with new cyber insurance standards.

Key Benefits



Resilience

Bring perpetual, organic network resilience to thwart attackers and pen testers to secure your enterprise and keep the Board happy.

Visibility

With just-in-time privileged access, each access is audited and visible while security leaders enjoy a single pane of glass to visualize and control everything in the network.

Reduce Security costs

With segmented networks, enjoy simplified security operations as well as reduced product spending for NACs, internal firewalls, IPS and manual ACL based micro segmentation products.

To learn more and see ZeroNetworks in action, visit zeronetworks.com

Contact us contact@zeroneworks.com