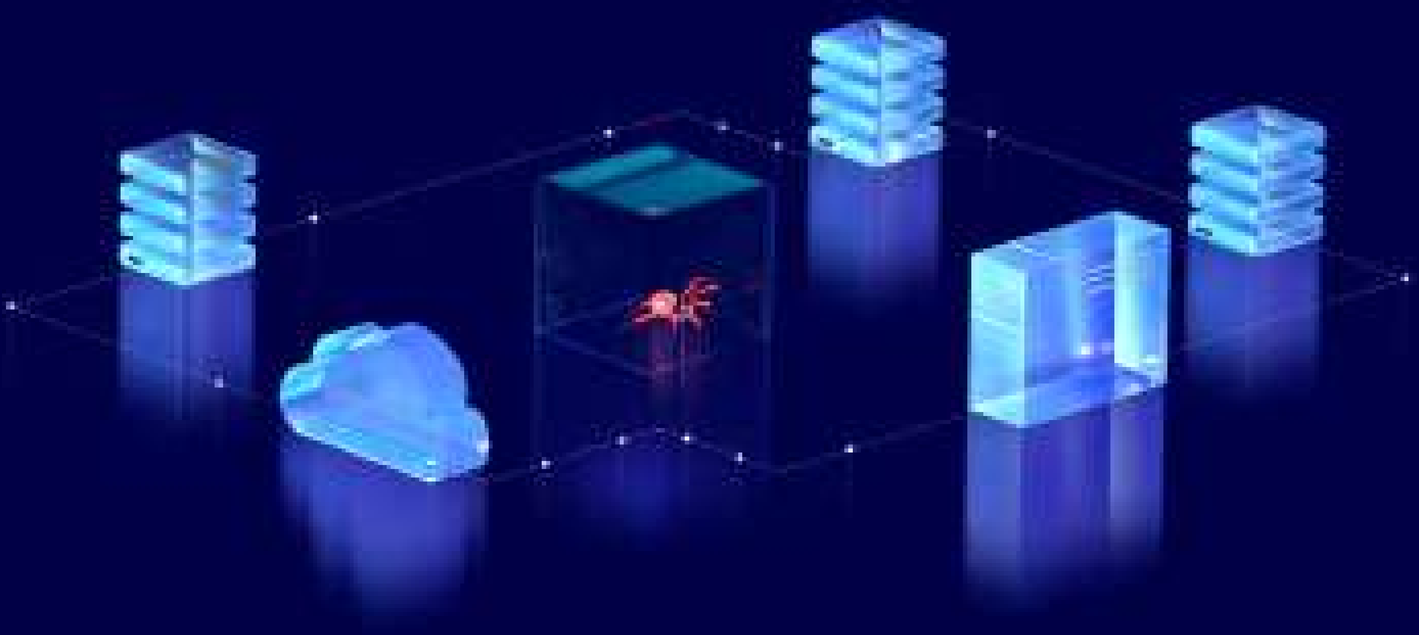
ZERO. Networks

Enable MFA anywhere you thought you couldn't to block ransomware and advanced attacks. **Forever.**

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Zero Networks Segment™

Technical Product Overview



ZERO Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

MFA-based Microsegementation: Immobilizing Lateral Movement with Zero Networks Segment™

Immobilizing Lateral Movement

When the history of cyber security is written—lateral movement will have THE leading role as the villain. In most cyberattacks—both in and not in the news—all have a basic and consistent plot. It starts with machine compromise, then onto recon, exploitation of a vulnerability and finally to lateral movement. All of these commonly used sequence of tactics rely on a basic attacker assumption: the compromised machine will have direct network line of sight to other machines that contain profitable data or IP to steal.

Immobilizing lateral movement is very hard. In theory, shutting down connections to the absolutely bare minimum needed into a fine grained allow list of IPs and ports would be extremely difficult. Any effort to maintain this would fail due to a constant and high volume state of flux. But from a cybersecurity standpoint, limiting internal network connections to just what is needed would doom virtually all cyberattack and limit any breach to just a few machines. Suddenly, concerns about board supervision, cyber insurance premiums and front page headlines would mostly evaporate.

Sadly, ransomware attacks continue to increase. Vendors respond with more and more point solutions that just increase complexity and stress operations. Detection, as we have learned, only proves useful if there's time to do something with the alert. An optimal solution would immobilize lateral movement without stressing security operations or infrastructure integrity.

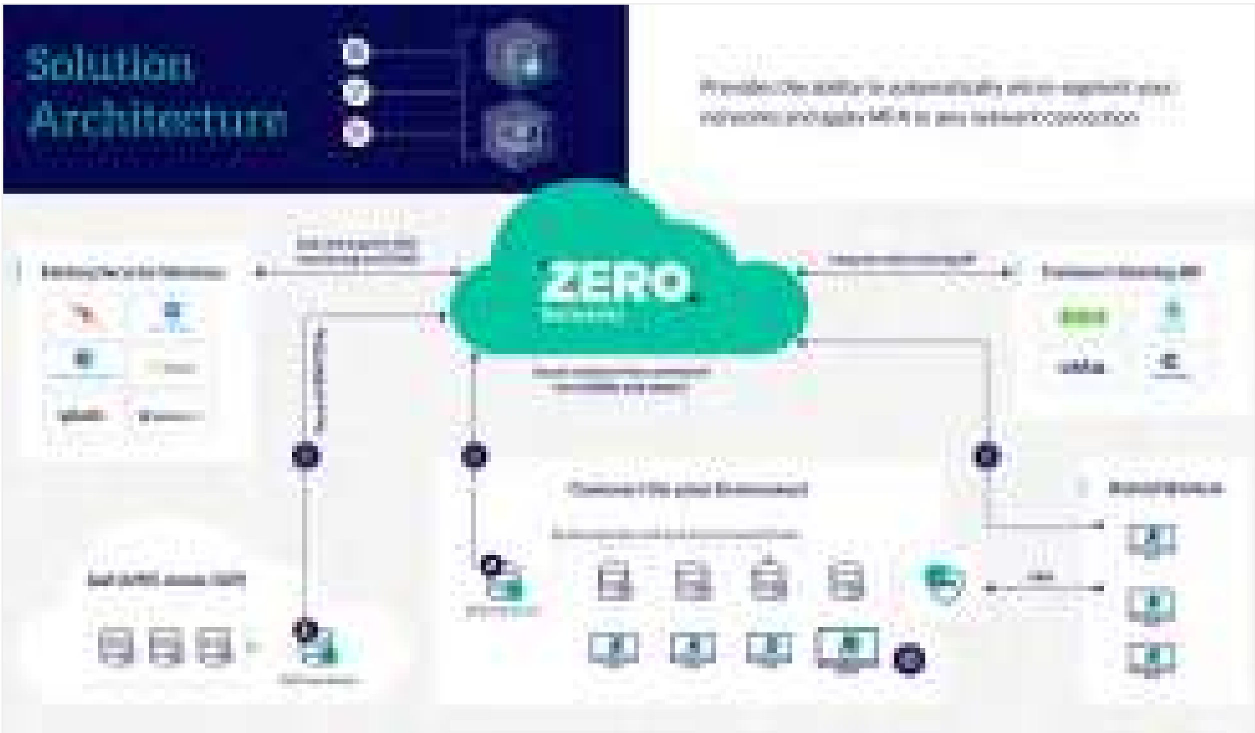
What would that look like?

Deploying An automated microsegmentation solution with built-in MFA Everywhere

Zero Networks Segment helps you to close the network down from within to permanently inhibit free lateral movement. With **Zero Networks Segment**, any breach will be limited to a few machines, freezing the attackers and giving time for the organization to respond on the few machines compromised. Our SaaS solution provides the ability to automatically micro-segment your networks with no agents and apply MFA to any network connection using your existing identity provider while not impacting anything in production.

PART I

How does it work



Cloud service: The brains of the operations

Our cloud service learns and automatically creates allowed traffic rules and determines where toapply MFA protections. **Zero Networks Segment** starts by learning server-to-server and client-to-server traffic. Then, it adds allow-lists for traffic from non-risky trivial applications used by users--such as HTTPS--and not used by attackers to spread internally. Lastly, **Zero Networks Segment** leaves the risky/privileged ports that are almost exclusively used by IT, security and DevOps teams--and therefore attackers—applying MFA for any of these remote operations.

The key capabilities of the cloud service include

Management	Data storage	Highly availability and flexibility	Highest standards of security and compliance
The admin portal.	All of the data is stored in an elastic storage pool with ethical walls that ensure the data is segregated and encrypted.	Worldwide data centers US, EU and APAC both for redundancy and scale.	We currently comply with SOC2 Type 2 and GDPR.

Trust Server: The orchestrator

The trust server orchestrates all host-based firewalls without agents via remote API control of machines; over WinRM for Windows & SSH for Linux. The key components of the Trust Server include:

Stateless virtual appliance

The appliance doesn't need any backup or maintenance and is not inline to any of the traffic. The virtual appliance is automatically updated from the cloud service for any code changes.

Auto scale out

Establishing access controls effective enough to stop lateral movement requires sophisticated policies and experts that not readily available for most organizations.

High availability

Deploy an additional trust server to get built-in high availability with no configuration required.

Offline work (AKA DR)

In case of loss of all service or connectivity, a break glass procedure is available until return to 100% operation.

Host-based firewall: The enforcer

With no need to reinvent the wheel, **Zero Networks Segment** leverages your native firewall to enforce the paralysis of lateral movement. Specifically, **Zero Networks Segment** gets all metadata on every connection and helps to segment all individual machines from everything else—both clients and servers. Capabilities include:

Agentless

No need to deploy any agent, the host-based firewall is controlled remotely using APIs from the trust server in a centralized fashion with no performance impact or maintenance required.

Broad OS support

- Windows clients including
- Windows 2008 and above
- Mac OSX 10.3 and above
- Windows 7 and above
- All Linux versions released after 2007

Anti-tampering

The remote APIs are also used to make sure no tampering is possible.

Applying MFA via an existing identity provider

Zero Networks Segment leverages your identify provider to enable MFA everywhere. Today, we support any SAML based identity provider for MFA including AAD, Duo, Okta, NetIQ, CyberArk and many more.

SIEM/SOAR

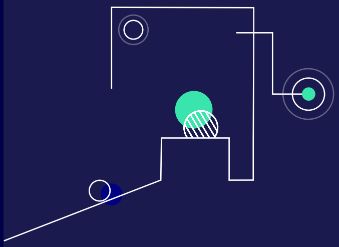
If you want to integrate **Zero Networks Segment** with your SIEM or SOAR solution, using an open API and can easily synchronize data to any desired SIEM that has API support including Splunk, Azure Sentinel, IBM Qradar. Likewise, for any SOAR solution, **Zero Networks Segment** provides automation scripts for various use cases such as isolation.

PART II

Democratizing security with self-service

Zero Network's unique approach to micro segmentation avoids putting work on security teams. **Zero Networks Segment** makes micro segmentation airtight and work at scale. By democratizing MFA, security teams avoid the impossible task of manually managing a network allow-list of which machines can connect over what ports/application to individual machines in your network.

On the backend, we eliminate operational friction with



01

No agents

02

No Hardware dependency

03

One solution to segment all clients and servers for on prem and cloud deployments. Our solution can even protect OT devices as well.

Our automated and self service approach closes everything except for the commonly used ports/applications in your environment. **Zero Networks Segment** gives special care to close down the privileged ports (RDP, SSH, WinRM or WMI), those are heavily used by most attackers. **With Zero Networks Segment, opening privileged access channels automatically invokes self-service MFA just in time.**

As a side benefit of having MFA at the network layer, with a click of a button organizations can create an MFA policy to any desired port or application across legacy, on prem or cloud deployment. **With Zero Networks Segment, you can apply MFA anywhere with no agents and no need to rewrite the application.**

Zero Networks Segment™ was designed to bring zero impact to operational efficiency

No impact on normal users

Non-risky application ports that normal users use will be kept open by the AI creating the allow-list.

MFA impact for privileged/technical users

Only IT, security and DevOps teams will need to MFA for any remote administrative task done over the network.

No impact for server-to-server communication

All server-to-server communication ports in use between servers will be kept open using Zero Network's AI. Our technology creates the allow-list as well as self-service adaptation of the allow-list by the server owners which will be orchestrated by Zero Networks.

PART III

How does a POC / deployment looks like?

Prepare a VM for the virtual appliance.

Installation (one hour)

Login to the **Zero Networks Segment** Admin Portal, download the setup.exe, click a few next buttons and you are done, start piloting by adding a few machines to learn mode from the admin portal.

Automated rule review and training (one hour duration performed two weeks after install)

Going over all of the important admin portal components and how to work with them as well as reviewing the AI created rules (seeing is believing)

Protection (one hour duration and four weeks after install)

Machines that marked for learning will automatically move to protection after verification that these assets work normally and that administration will be protected by MFA.

High availability deployment (1 hour, optional)

An extra trust server virtual appliance to be deployed to avoid any single point of failure.

Long term maintenance

As a SaaS solution, no maintenance or manual operation is required from IT and security teams.

PART IV

Life with Zero Networks

With Zero Networks Segment, organizations enjoy

- **The** eradication of lateral movement with MFA based segmentation covering on prem and cloud infrastructure that shuts down almost all open ports
- **Reporting** detailing who has permission to access what to support several compliance standards
- **The** democratization security with self-service MFA
- **Reduced** alert quantity SOC needs to investigate
- **Ability** to focus on high risk issues
- **A set** and forget product deployment
- **Dramatic** decrease in stale, pervasive network permissions

SRC CYBER SOLUTIONS LLP

CYBER RISK SOLUTIONS

ZERO.
Networks

www.zeronetworks.com