ZERO. Networks

Incident Response

Solution Brief

Contain a Breach in As Little as 24 Hours

▶ Zero Networks offers an automated, agentless, and MFA-powered approach to microsegmentation that can stop the spread of an attacker in as little as 24 hours.
▶ It creates highly accurate security policies, which are centrally applied to all host-based firewalls, effectively blocking lateral movement while keeping the network operational.

Cyber breaches are increasing in number and impact, posing serious repercussions for organizations worldwide, such as ransomware, data exfiltration, operational disruption, legal and regulatory concerns, and damage to trust and brand reputation. A skilled and persistent attacker can remain undetected within a network for months, making it one of the most significant challenges for incident response teams globally.

Zero Networks offers an automated, agentless, and MFA-enabled approach to microsegmentation that can stop the spread of an attacker in as little as 24 hours. It creates highly accurate security policies, which are centrally applied to all host-based firewalls, effectively blocking lateral movement while keeping the network fully operational.

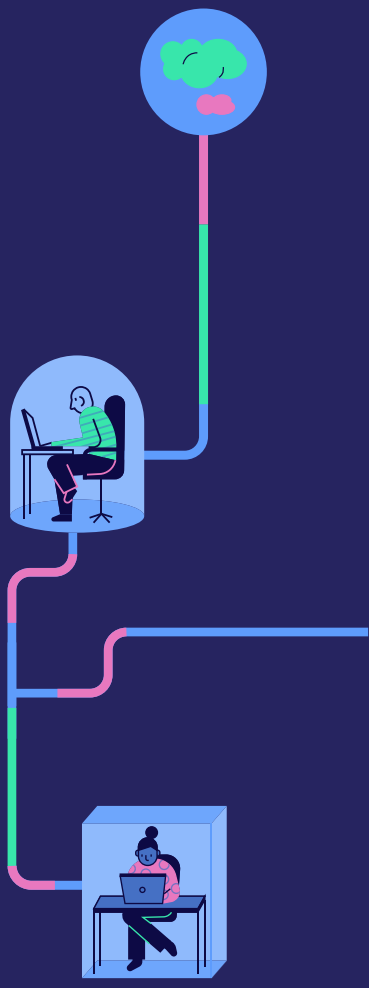
Blocking Lateral Movement with Microsegmentation

Microsegmentation is the most effective solution against lateral movement, establishing a firewall bubble around each network asset to permit legitimate traffic only and block everything else. Although microsegmentation cannot prevent security breaches, it can prevent the lateral movement of attackers, significantly limiting further damage.

However, legacy microsegmentation solutions are notoriously complex, requiring agent installation and manual firewall rule maintenance on each machine. This labor-intensive process takes months to deploy and sometimes years to scale. In the event of an ongoing attack, manually microsegmenting a compromised network is simply too slow.

Key Benefits

- **Defend against and contain the spread of an attacker in as little as 24 hours in urgent IR scenarios.**
- **Prevent lateral movement through microsegmentation of your entire network – IT and OT, on-prem, and in the cloud.**
- **Fully automated – no humans are involved.**
- **No agents – install just one VM.**
- **Apply just-in-time MFA on any network asset.**



Microsegmentation with Zero Networks: Automated, Agentless, MFA-powered

Zero Networks provides a radically simple and scalable approach to microsegmentation:

- **Automated:** The system learns network connections and generates highly accurate security policies, centrally applied to all host-based firewalls.
- **Agentless:** No installation is required on clients or servers, enabling rapid and straightforward deployment at scale.
- **MFA-powered:** All privileged ports remain closed and only open temporarily after admin users have authenticated using MFA.

Incident Response with Zero Networks

In urgent incident response situations that demand immediate action, Zero Networks can assist in thwarting an attack in less than 24 hours while preserving most network operations. Swift and effective responses to security breaches are essential to mitigate further damage, safeguard sensitive data, minimize financial losses, and maintain customer trust. Such rapid response also aids organizations in identifying the root cause of the breach, understanding the extent of the damage, and taking appropriate actions to contain the incident.

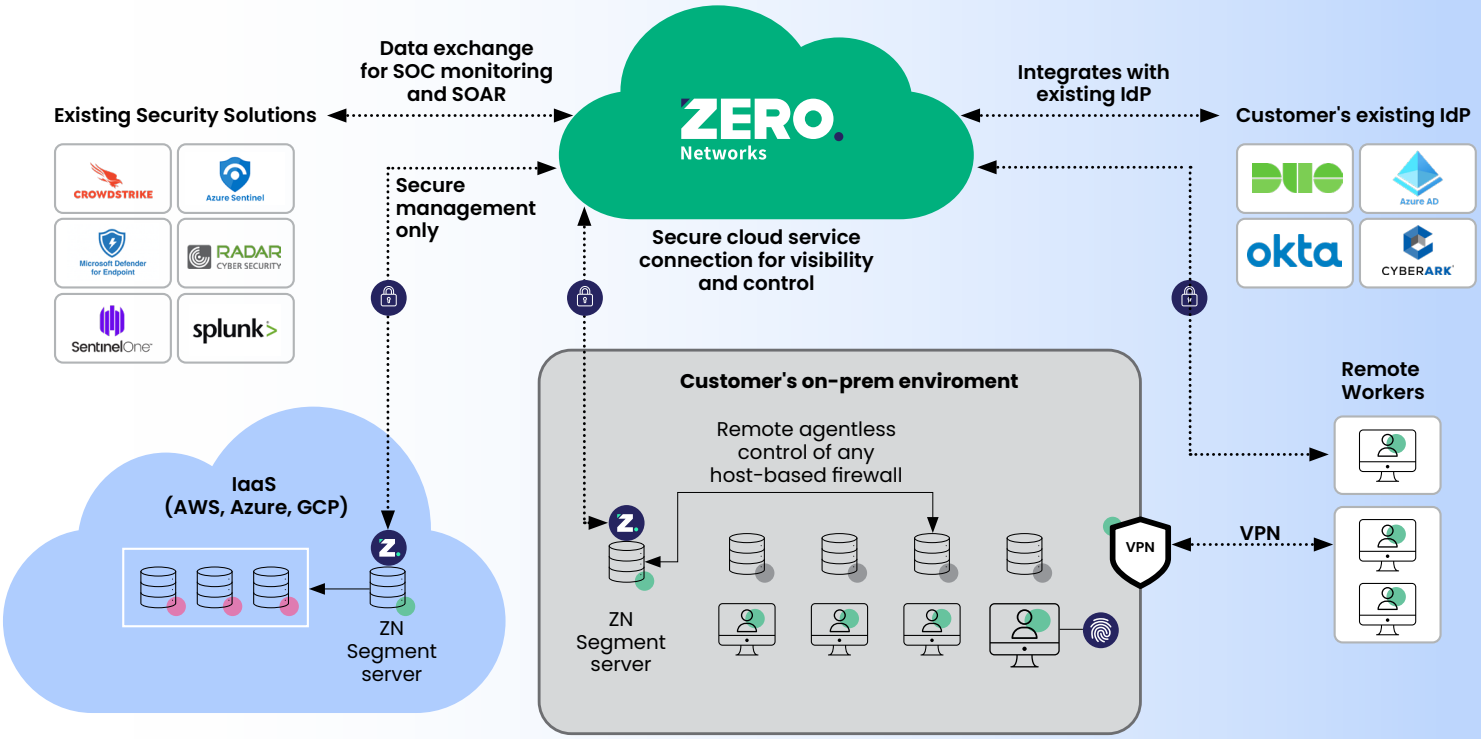
Zero Networks quickly learns about 90% of network activities within 24 hours and creates corresponding security policies, which are applied to the host-based firewalls of all network assets. It also applies MFA to remote admin protocols like RDP, SSH, SMB, and others, which attackers typically use for lateral movement. This approach allows organizations to resume near-normal operations while additional firewall rules are created for any network activity not captured within the initial 24-hour learning period.

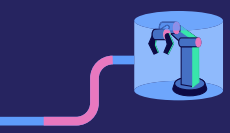
For incidents that allow a longer response time, a recommended learning period of 14 to 30 days ensures Zero Networks accurately captures all network connections and creates highly precise rules and policies for microsegmentation without causing any network disruptions.

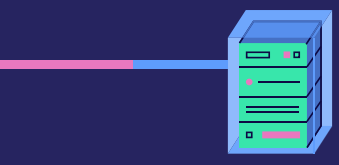
Reporting & Auditing

The Zero Networks platform offers comprehensive network visibility, enabling the monitoring of all machine connections, ports, internet communication, and even unsanctioned and unauthorized devices. It features an Access Map for visualizing connections and integrates Threat Intelligence to evaluate and automatically block high-risk internet connections if required. In addition, all platform activities are audited and logged for 1 year.

How does it work?







1. **Monitoring**
   A Segment Server, a simple virtual machine that takes minutes to install, monitors all network connections on the organization's on-prem and cloud environments, and sends their metadata to the Zero Networks cloud.
2. **Learning**
   The Zero Networks Cloud learns the network and creates highly accurate security policies that restrict network traffic only to what is strictly necessary, blocking everything else.
3. **Segmenting**
   The policy is then centrally applied by the Segment Server to the host-based firewalls of all endpoints in the network to achieve accurate, full zero trust microsegmentation. OT/IoT (or other devices which do not have a firewall) are segmented by blocking all outbound connection requests from IT to OT. Access is granted temporarily after users have authenticated with MFA from their organization's preferred identity provider.
4. **Applying MFA**
   MFA can be applied to any network asset. For instance, all privileged ports (e.g., RDP, SSH, SMB) are closed by default and only open temporarily after an admin user has authenticated with MFA from their organization's preferred identity provider.

Incident Response Timelines

Urgent Remediation

It takes only 24 hours to segment 90% of the network and stop lateral movement

When immediate response is necessary, a 24-hour period is enough to stop the spread by learning about 90% of network traffic. Then, MFA is instantly applied on all remote admin protocols (e.g. RDP, SSH, SMB) to prevent further lateral movement.

- **Attacker is blocked.**
- **90% of the network is automatically segmented and secured (further learning or manual configuration is needed for the rest).**
- **Most legitimate network traffic is intact.**

30-Day Remediation

It takes only 3 human hours to supervise automated segmentation of 100% of the network

Day 1

One hour call to deploy

Learning period begins: Network connections are monitored.

Day 14

One hour call to monitor

Learning period is halfway through. All clients and most servers are fully segmented and secure.

Day 30

One hour call at completion

Learning period ends. The remaining servers are fully segmented. MFA is applied on all remote admin protocols to prevent lateral movement.

- **Attacker is blocked.**
- **100% of the network is segmented and secured.**
- **Network is fully operational.**
- **No apps are broken.**

ZERO. Networks

Segment Everything
Connect Everyone

Zero Networks is a unified zero trust platform for network segmentation, identity segmentation, and remote access. To see us in action visit zeronetworks.com or contact us at contact@zeronetworks.com