ZERO. Networks

Network Segmentation

Radically Simple Segmentation in a Click

Zero Networks automates policy creation to effortlessly microsegment each network asset, and applies MFA to block lateral movement

Networks were designed for connectivity, not security. This inherent flaw means that users and machines have excessive network permissions: Once an attacker breaches into one machine, it's easy for them to move laterally and compromise the entire network.

The Solution: Microsegmentation

Microsegmentation applies a firewall "bubble" around each asset in the network. If one asset is compromised, the attacker is blocked and cannot move laterally. However, legacy solutions require installing agents and manually configuring firewall rules for each asset – a process that takes months to deploy and years to scale, and often breaks the network.

Microsegmentation with Zero Networks

The Zero Networks platform features a fully automated, agentless, MFA-enhanced microsegmentation solution that is the very first to succeed at scale. It allows organizations to segment any asset in the network – IT and OT, on-prem and in the cloud – in a click, with no humans involved.

Automated

Agentless

MFA-Enhanced

1. Learning

Zero Networks learns all network connections and automates policy and rule creation for each asset

2. Segmenting

The policies are centrally applied on all host-based firewalls, permitting only necessary traffic

3. Applying MFA

Admin ports commonly used in attacks (e.g., RDP, SSH) are blocked and open temporarily after MFA

> "Essentially putting every computer and server on the network into their own individual DMZ"
>
> Gartner

Stop Attacks from Spreading

Ransomware kill switch
Completely block lateral movement to stop any attack

Segment any asset in a click
IT and OT, on-prem and in the cloud

Pass any pen test
Receive "green" reports on the first attempt

Reduce security OpEx
Leverage automation to reassign IT staff to other tasks

Comply with regulations and cyber insurance
Adhere to strict segmentation, MFA, and visibility requirements

Easy to deploy and manage
A set-and-forget technology transparent to end users

Apply MFA to Anything Patented

Multi-factor authentication (MFA) stops nearly all identity thefts but is typically limited to SaaS applications.
Zero Networks is the only solution that applies MFA at the port level, enabling just-in-time MFA to any asset, including those that could not have been protected by MFA before.

- Any Client
- Any Server
- Any Protocol
- Legacy Applications
- OT/IoT Devices
- Databases
- PaaS Solutions
- IaaS VMs
- On-prem VMs
- Global Clients

> My first impression was, it is too good to be true. The ease of deployment was shocking to me. It's a simple and elegant solution to a very difficult problem.

Henry Mayorga, CISO, Baron Capital

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

ZERO. Networks

Secure Remote Access

ZTNA Security at the Speed of VPN

Connect remote employees and third parties to the network with zero trust principles and maximum performance

In today's hybrid work landscape, IT teams are challenged with securely connecting remote employees and third parties to their networks.

While traditional VPNs offer direct, fast, and encrypted network access, they must expose open ports on the internet, making them vulnerable to brute-force, DDoS, and other attacks.

Zero Trust Network Access (ZTNA) mitigates this by hiding behind a cloud proxy, but this results in higher latency, lower bandwidth, higher costs, and IP address obfuscation, which blinds various detection solutions.

Secure Remote Access with Zero Networks

The Zero Networks platform melds the strengths of both VPN and ZTNA while eliminating their respective weaknesses.
Zero Networks provides a VPN-like tunnel between the user and the organization, ensuring maximum network performance without the latency associated with ZTNA.
It achieves zero trust security by not exposing open ports on the internet, and by maintaining visibility of user IP addresses within the organization, addressing a common concern in typical ZTNA solutions.

	VPN	ZTNA	ZERO.
Optimum network performance	✓	✗	✓
Zero Trust Principles	✗	✓	✓

> When I first saw Zero Networks, I walked away saying, this is too good to be true. When we put it in production, it was like a dream came true.

Justin Manifold, Senior IT Security Engineer, Vermeer Corporation

An Evolutionary Leap in Zero Trust Network Access

Maximum Performance
Direct, peer-to-peer connectivity with WireGuard®

Optimized User Experience
No additional bandwidth overhead for a fast, seamless experience

Minimum Friction
Designed to be installed, deployed, and managed seamlessly

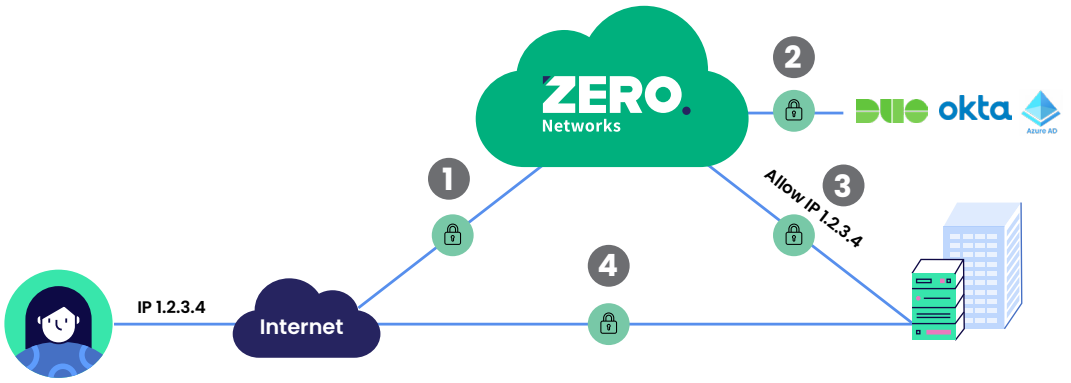
Maximum Visibility
Unlike traditional ZTNA, no obfuscation of user IP addresses

Comply with regulations and cyber insurance
Adhere to strict MFA and granular user access requirements

Connect Any User
Custom policies allow both employee and vendor access

How It Works

A ZTNA and VPN hybrid: All the benefits, none of the downsides



1 **Port is closed and invisible**
There are no open ports on the internet. When a user tries to connect, they are directed to the Zero Networks cloud.

2 **User verified by MFA**
User authenticates using the MFA of their organization's existing identity provider (IdP).

3 **Port opens only to the authenticated user**
Zero Networks opens a port only to the authenticated user's IP address but remains invisible to everyone else.

4 **A direct tunnel is established**
A direct, fast, and encrypted tunnel is established; policies allow user access to all or pre-approved apps and services.

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

Gartner COOL VENDOR 2020 · Forbes · Top InfoSec Innovator Winner 2023 · Gartner ZTNA Market Guide · Winner CISO Choice Awards Network Security Zero Networks · 2021 Fortress Cyber Security Award · CSO · Winner CISO Choice Awards Zero Networks · Global InfoSec Awards Winner Cyber Defense Magazine 2022 · RSAC Launch Pad 2020 Startup · Top 100 Cybersecurity Startups Winner 2020 · Gartner Microsegmentation Market Guide · Big 50 2021 Startup 50 · MES Midmarket 100 2023

ZERO. Networks

Identity Segmentation

Gain Control of Admin and Service Accounts

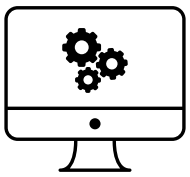
Zero Networks easily provisions all logon rights based on least privilege to prevent lateral movement

Admin and privileged service accounts are prime targets for attackers, as compromising them provides access to the organization's most sensitive servers. While the principle of least privilege aims to limit these risks, it is difficult to implement due to the manual, lengthy, and complex process of governing access rights. This results in broad logon permissions, leading to threats like data breaches, malware, and ransomware.

Identity Segmentation with Zero Networks

The Zero Networks platform features a simple, fully automated, and agentless identity segmentation solution. It revokes logon rights for all admin and service accounts and then provisions them based on least privilege, enhanced by multi-factor authentication (MFA).

Admin Accounts are restricted to pre-approved assets after MFA



Service Accounts are automatically restricted to necessary assets and logon types

Automated

Agentless

MFA-Enhanced

An Evolutionary Leap in Identity Security

Service account discovery and visibility
Get insights on account usage, eliminate inactive accounts

Auto-restrict service account logons
Prevent unauthorized access and lateral movement

MFA privileged logons
Enable admin logon where intended, blocking all other logon rights

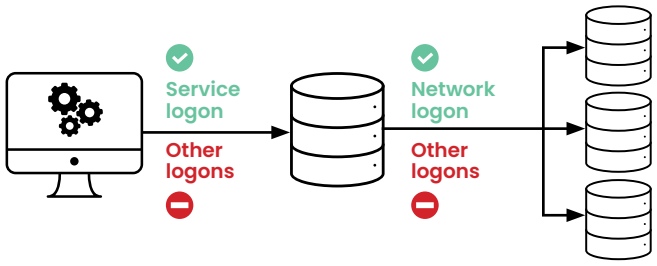
Eliminate risk from credential theft
Prevent Pass the Ticket, Golden Ticket, Kerberoasting, and other attacks

PAM augmentation & Tiered Model alternative
Extend granular security without the associated cost and complexity

Comply with regulations and cyber insurance
Adhere to visibility, MFA, and strict control of privileged and service accounts

How It Works

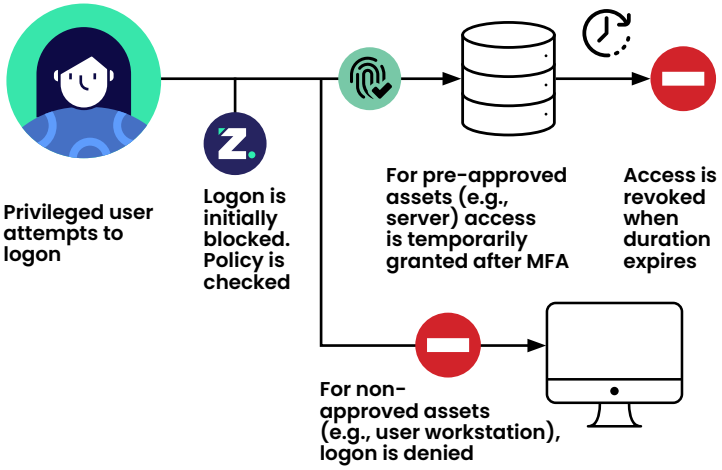
Service Accounts: Zero Networks' patent-pending technology learns all logons for a recommended 30-day period, understands which service accounts and logon types are intended to be used on each asset, and automatically restricts logon rights and types to these assets.



Service Account
Can only logon to backup server using service logon

Backup Server
Can only logon to servers it is backing up using network logon

Admin accounts: Zero Networks enables IT teams to restrict admin accounts, permitting temporary logon to pre-approved assets only after MFA, and blocking all other logon rights.



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