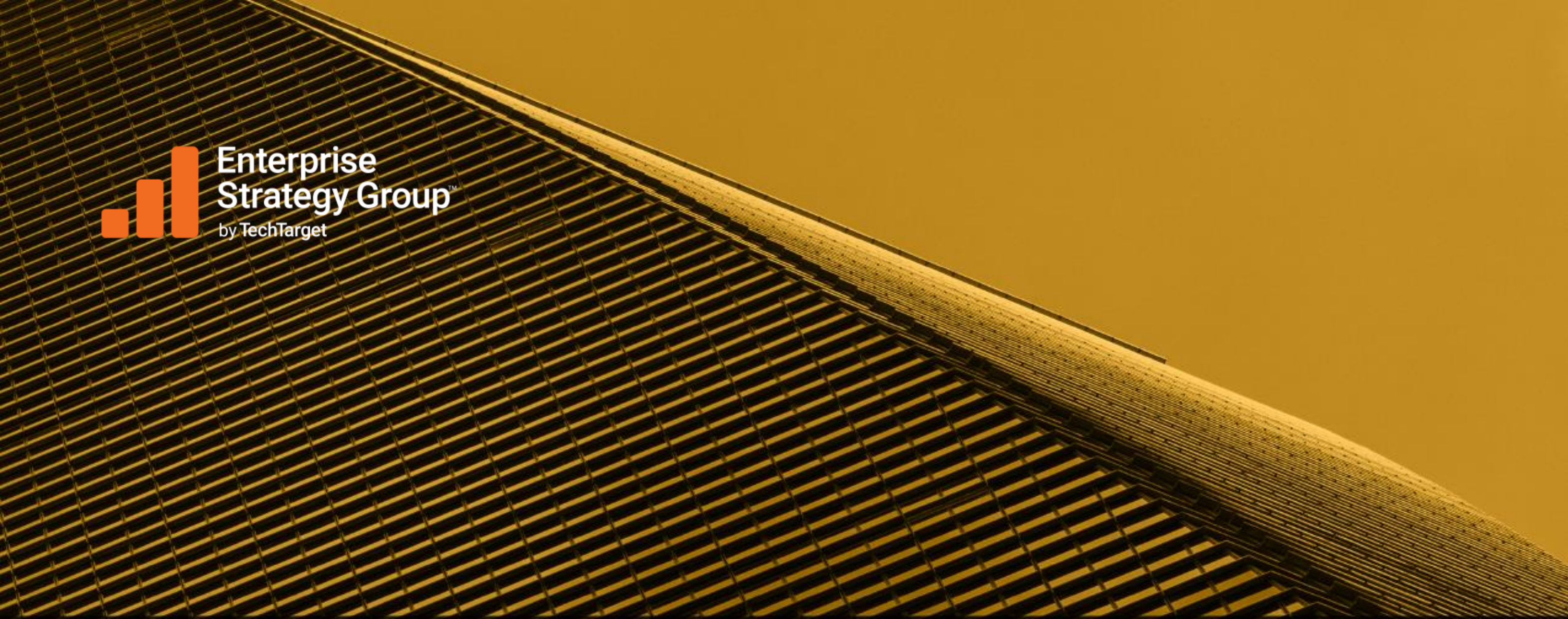


Enterprise Strategy Group™
by TechTarget

TECHNICAL VALIDATION

The Zero Networks Platform

Automated, Agentless Segmentation of Networks and Identities with Secure Remote Access

By Justin Boyer, Validation Analyst; and Tony Palmer, Practice Director
Enterprise Strategy Group

July 2024

Contents

Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group outlines the evaluation of the Zero Networks identity and network security platform. We validated how Zero Networks simplifies effective network segmentation, identity segmentation, and secure remote access.

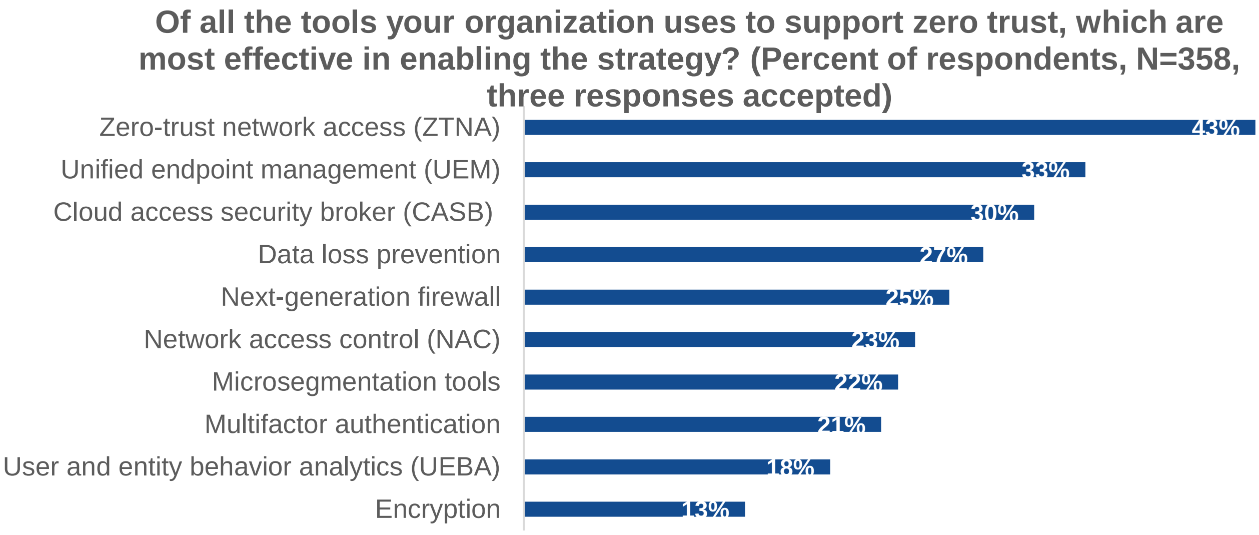
Background

As remote and hybrid workplaces become the norm, the modern workforce can be spread across the globe, connecting to an organization's network and applications from anywhere in the world. Workers need access to SaaS and on-premises applications, along with cloud services, no matter where they are or what device they're using. This digital transformation has blurred the boundary between "inside" and "outside" of a network, causing the traditional network perimeter model to become obsolete. It's no longer enough to only verify identities on the way into the network. Organizations must have the same levels of protection and verification for internal traffic. Otherwise, attackers who gain access will easily employ lateral movement tactics, moving freely through a network to access sensitive data and other high-value assets. These threats require modern IT environments to employ the same levels of protection and verification for every request, even for internal traffic.

Enterprise Strategy Group research shows that zero trust has emerged as the preferred model of security in these challenging modern environments. Sixty-nine percent of surveyed organizations have already implemented or begun to implement zero trust. Forty-one percent of those surveyed cited securing remote access for employees and third parties as a top driver for this adoption.[1]

Figure 1 shows what survey respondents believe are the most effective ways to support zero trust. The clear favorite is Zero Trust Network Access (ZTNA). Other effective tools include microsegmentation and secure access through Cloud Access Security Brokers (CASBs).

Figure 1. Top 10 Most Effective Zero-trust Tools



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Report, *Trends in Zero Trust: Strategies and Practices Remain Fragmented, but Many Are Seeing Success*, March 2024. All research references and charts in this Technical Validation are from this source unless otherwise noted.

Recently, the NSA released updated guidance that all companies—not just federal agencies—should aim to adopt the network and environment pillar of their zero-trust guidelines.[2] Organizations aiming to follow this guidance will be looking for more effective implementations of the tools in Figure 1, especially those lower on the list, such as microsegmentation, network access control, and multifactor authentication (MFA).

However, traditional microsegmentation tools often require agents on each asset and manual effort to define and maintain rules. These requirements can slow down deployment, break networks, and cause costs to soar. Many projects fail. Many organizations also struggle with network access control via identity management and ensuring their employees can securely connect from anywhere without increasing organizational risk.

To overcome these challenges, organizations need solutions that focus on simplicity and scalability, making them easier to deploy and operate, no matter the organization's size.

Zero Networks

The Zero Networks platform offers a simple, automated segmentation solution that restricts network and user access to what's strictly essential, preventing unauthorized lateral movement. It features three main components designed to address common challenges organizations face when implementing zero trust:

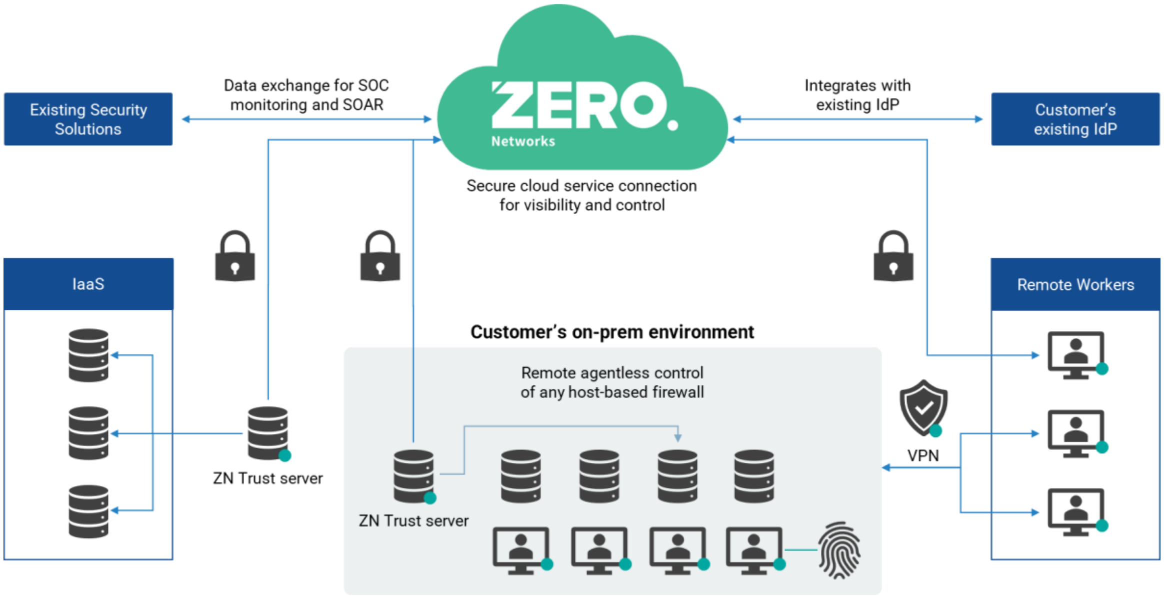
Zero Networks Segment creates micro-perimeters for every device on an organization's network, including IoT and operational technology (OT) devices, on premises and in the cloud. Fully automated and agentless, Segment watches network traffic and learns the common routes used within the infrastructure. It typically learns for 30 days for servers and two weeks for clients. Zero Networks uses deterministic and predictable automation to keep the necessary network permissions open, falling back on just-in-time MFA for privileged operations or when network permissions are missing.

Zero Networks Identity Segmentation restricts admin and service account access to operational needs only, stopping privileged account abuse. After revoking login rights for all admin and service accounts, Zero Networks then provisions them based on least privilege, enhanced by MFA. This blocks lateral movement even if credentials are stolen and prevents pass-the-ticket, golden ticket, Kerberoasting, and other attacks.

Zero Networks Connect provides secure remote access with the speed of a VPN and the security of ZTNA, while overcoming common flaws inherent in each. Remote users connect using a Zero Networks VPN Client (based on WireGuard). Zero Networks then forces MFA on the user (leveraging the preferred identity provider). After successful authentication and authorization, the Connect server opens an inbound rule to enable access from the user's IP address and establishes a secure tunnel for a defined period, after which the user can access the corporate network. There are no exposed ports on the internet, and user IP addresses are visible to the organization.

[2] Source: National Security Agency, *Advancing Zero Trust Maturity Throughout the Network and Environment Pillar*, March 2024.

Figure 2. Zero Networks Architecture


Existing Security Solutions
Data exchange for SOC monitoring and SOAR
ZERO. Networks
Integrates with existing IdP
Customer's existing IdP
Secure cloud service connection for visibility and control
IaaS
ZN Trust server
Customer's on-prem environment
Remote agentless control of any host-based firewall
ZN Trust server
VPN
Remote Workers

Source: Zero Networks, Inc and Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated the Zero Networks platform's ability to simplify and automate network segmentation and to protect admin and service accounts through identity segmentation. We also validated how Zero Networks securely connects remote employees and third parties into the network with the speed of VPN and the security of ZTNA. As part of our validation, we investigated how the various Zero Network**s** platform components also leverage just-in-time MFA. Finally, we reviewed the potential return on investment of using the Zero Networks platform for organizations of various sizes.

Automated Microsegmentation

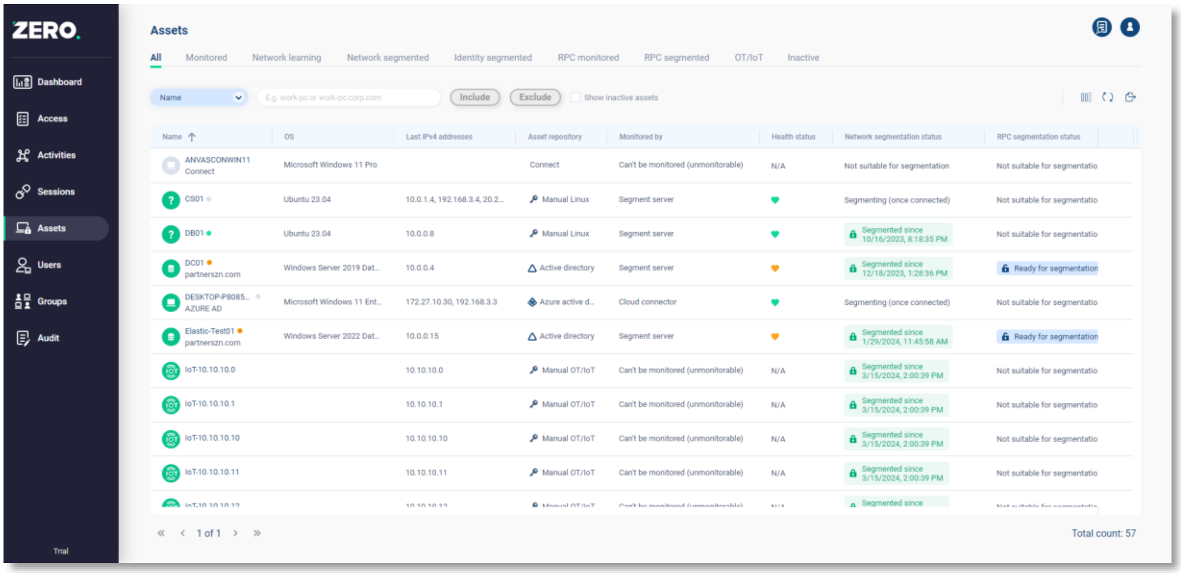
First, we looked at how Zero Networks automates microsegmentation, providing secure perimeters around organizational assets connected to the network.

Enterprise Strategy Group Analysis

Microsegmentation is often challenging to accomplish. Many organizations struggle for years to implement any form of segmentation due to its high expense, complexity, and error rate. Zero Networks focuses on segmenting each device on the network with automation, making microsegmentation achievable and much less expensive. Enterprise Strategy Group walked through a microsegmentation process using Zero Networks.

In the Assets view, Zero Networks provides an overview of the network-connected assets and related information (see Figure 3). Both segmented and non-segmented assets are viewable here. The user can filter the assets by using the tabs at the top of the screen to see categories or through a more specific search above the asset list.

Figure 3. Segmenting an Asset



Assets

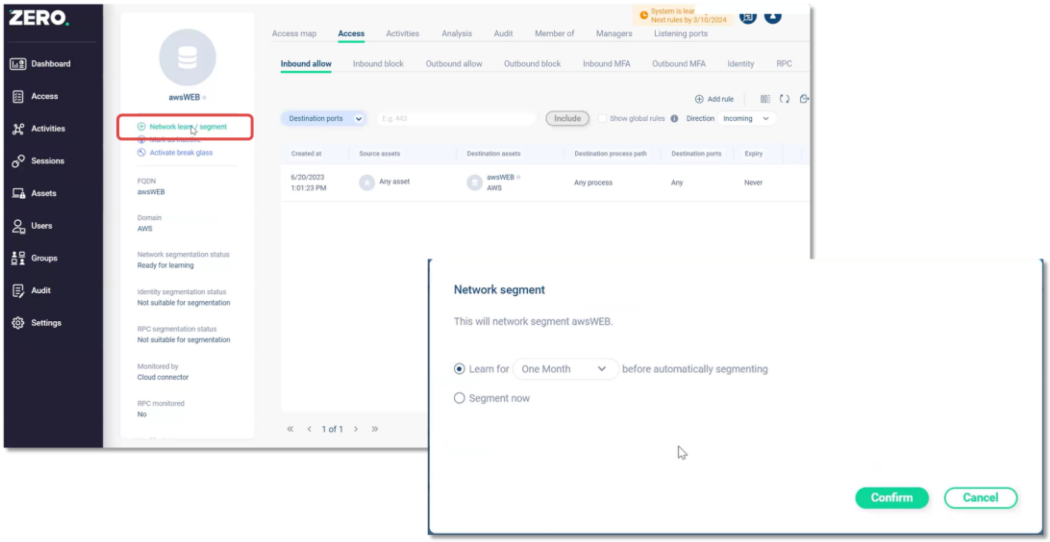
Name	OS	Last IPv4 addresses	Asset repository	Monitored by	Health status	Network segmentation status	RPC segmentation status
ANVASCONWIN11 Connect	Microsoft Windows 11 Pro		Connect	Can't be monitored (unmonitorable)	N/A	Not suitable for segmentation	Not suitable for segmentatio
CS01	Ubuntu 23.04	10.0.1.4, 192.168.3.4, 20.2...	Manual Linux	Segment server	♥	Segmenting (once connected)	Not suitable for segmentatio
DB01	Ubuntu 23.04	10.0.0.8	Manual Linux	Segment server	♥	Segmented since 10/16/2023, 8:18:35 PM	Not suitable for segmentatio
DC01 partnerszn.com	Windows Server 2019 Dat...	10.0.0.4	Active directory	Segment server	♥	Segmented since 12/18/2023, 1:28:36 PM	Ready for segmentation
DESKTOP-P8085... AZURE AD	Microsoft Windows 11 Ent...	172.27.10.30, 192.168.3.3	Azure active d...	Cloud connector	♥	Segmenting (once connected)	Not suitable for segmentatio
Elastic-Test01 partnerszn.com	Windows Server 2022 Dat...	10.0.0.15	Active directory	Segment server	♥	Segmented since 1/29/2024, 11:45:58 AM	Ready for segmentation
IoT-10.10.10.0		10.10.10.0	Manual OT/IoT	Can't be monitored (unmonitorable)	N/A	Segmented since 3/15/2024, 2:00:39 PM	Not suitable for segmentatio
IoT-10.10.10.1		10.10.10.1	Manual OT/IoT	Can't be monitored (unmonitorable)	N/A	Segmented since 3/15/2024, 2:00:39 PM	Not suitable for segmentatio
IoT-10.10.10.10		10.10.10.10	Manual OT/IoT	Can't be monitored (unmonitorable)	N/A	Segmented since 3/15/2024, 2:00:39 PM	Not suitable for segmentatio
IoT-10.10.10.11		10.10.10.11	Manual OT/IoT	Can't be monitored (unmonitorable)	N/A	Segmented since 3/15/2024, 2:00:39 PM	Not suitable for segmentatio
IoT-10.10.10.12		10.10.10.12	Manual OT/IoT	Can't be monitored (unmonitorable)	N/A	Segmented since	Not suitable for segmentatio

Total count: 57

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Next, Enterprise Strategy Group walked through the process of segmenting an asset. After selecting an asset from the Assets view, we clicked **Network learn / segment** (see Figure 4). We then chose one month for the learning time.

Figure 4. Segmented Assets



awsWEB

FQDN
awsWEB

Domain
AWS

Network segmentation status
Ready for learning

Identity segmentation status
Not suitable for segmentation

RPC segmentation status
Not suitable for segmentation

Monitored by
Cloud connector

RPC monitored
No

Created at	Source assets	Destination assets	Destination process path	Destination ports	Expiry
6/20/2023 1:01:23 PM	Any asset	awsWEB AWS	Any process	Any	Never

Network segment

This will network segment awsWEB.

● Learn for One Month before automatically segmenting

○ Segment now

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

After watching network traffic for 30 days, Zero Networks uses deterministic rule creation to create inbound and outbound rules for the host-based firewall of every client and server on the network (Windows Firewall, Mac Firewall, Linux iptables), along with MFA rules and identities found connecting to the asset. Zero Networks performs this work without installing agents or interfering with network traffic in any way, reducing expenses and eliminating negative performance impact.

Preventing Lateral Movement with MFA

When Zero Networks detects privileged login traffic for protocols typically used by IT and security teams to administer servers, such as remote desktop protocol, SSH, or Windows Remote Management, it will create an MFA rule to govern those connections for a time-limited period. Attackers use these ports to move laterally within an environment, so these need to be locked down.

Zero Networks' patented approach applies MFA on Layer 3 (Network layer), which enables it to protect assets that are challenging to protect with MFA, such as network ports or protocols, databases, OT devices, and legacy applications.

Why This Matters

Although many consider zero trust to be an essential security model for modern organizations, implementing zero trust can be challenging. According to Enterprise Strategy Group research, 46% of organizations paused or abandoned their zero trust projects due to rising expenses, and 42% paused or abandoned them because of technical issues encountered while implementing the project.

Zero Networks designed its microsegmentation solution to address common issues in implementing zero trust segmentation. Enterprise Strategy Group validated that Zero Networks automatically segments traffic by monitoring network communications between assets without using agents or devices in the traffic path, permitting necessary connections, rejecting abnormal ones, and prompting MFA for privileged access—adding an extra layer of protection against lateral movement. This approach eliminates the need for costly and labor-intensive agent installation and manual rule creation, ensuring easy scalability and savings in space, speed, and cost.

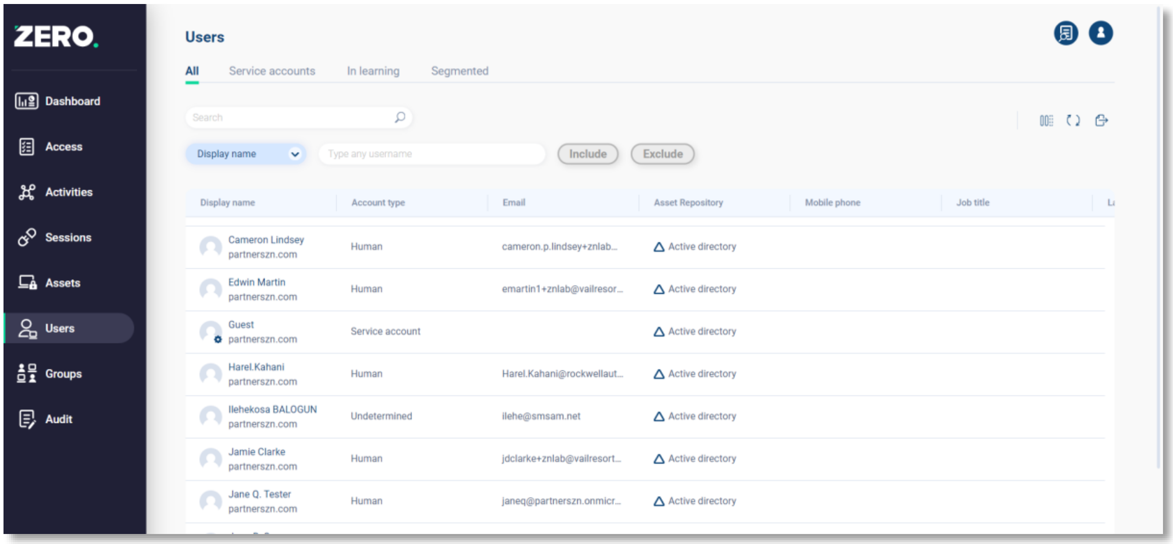
Admin and Service Account Protections Through Identity Segmentation

Second, we considered how Zero Networks automates identity segmentation, restricting access to admin and service accounts to operational needs only.

Enterprise Strategy Group Analysis

For zero trust to be successful, network segmentation is only the start. Identity segmentation is vital to ensure attackers can't assume an identity and move undetected throughout an environment. While learning, Zero Networks segments identities along with individual assets. Each of these users can be seen in the Users view within the Zero Networks console. Here, we viewed all human users and service accounts (see Figure 5).

Figure 5. Users View

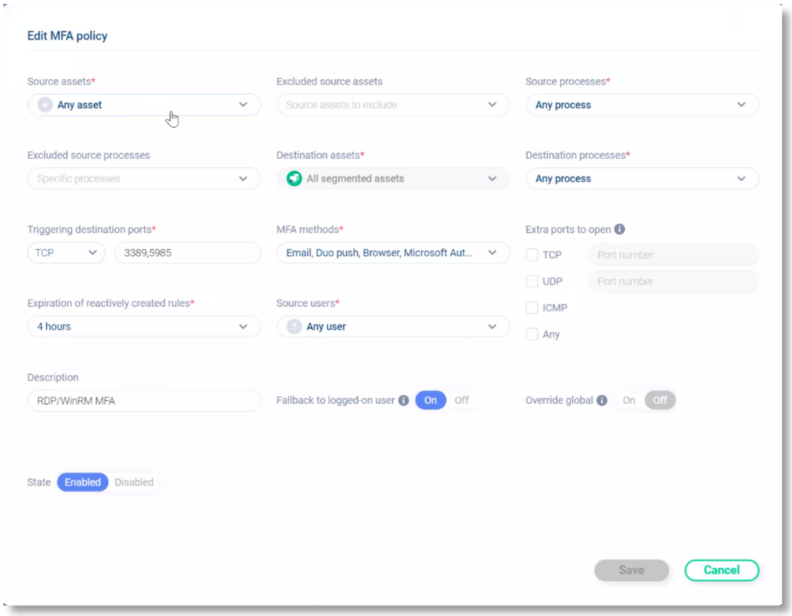


Display name	Account type	Email	Asset Repository	Mobile phone	Job title	L
Cameron Lindsey partnerszn.com	Human	cameron.p.lindsey+znlab...	Active directory			
Edwin Martin partnerszn.com	Human	emartin1+znlab@vailresor...	Active directory			
Guest partnerszn.com	Service account		Active directory			
Harel.Kahani partnerszn.com	Human	Harel.Kahani@rockwellaut...	Active directory			
Ilehekosa BALOGUN partnerszn.com	Undetermined	ilehe@smsam.net	Active directory			
Jamie Clarke partnerszn.com	Human	jdclarke+znlab@vailresort...	Active directory			
Jane Q. Tester partnerszn.com	Human	janeq@partnerszn.onmicr...	Active directory			

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

MFA policies define what happens when IT administrators use privileged protocols to access servers. Upon connecting, the admin receives a prompt via MFA, using many potential methods, that they must complete in order to connect for a limited time period. This prevents attackers from successfully moving throughout an environment even if user credentials, Kerberos tickets, or NTLM hashes are stolen. Figure 6 shows the MFA policy dialog administrators use to define or change MFA rules for specific segmented assets.

Figure 6. Editing an MFA Policy



Edit MFA policy

Source assets*: Any asset

Excluded source assets: Source assets to exclude

Source processes*: Any process

Excluded source processes: Specific processes

Destination assets*: All segmented assets

Destination processes*: Any process

Triggering destination ports*: TCP 3389,5985

MFA methods*: Email, Duo push, Browser, Microsoft Aut...

Extra ports to open: □ TCP Port number; □ UDP Port number; □ ICMP; □ Any

Expiration of reactively created rules*: 4 hours

Source users*: Any user

Description: RDP/WinRM MFA

Fallback to logged-on user: [✓ On] Off

Override global: On [✓ Off]

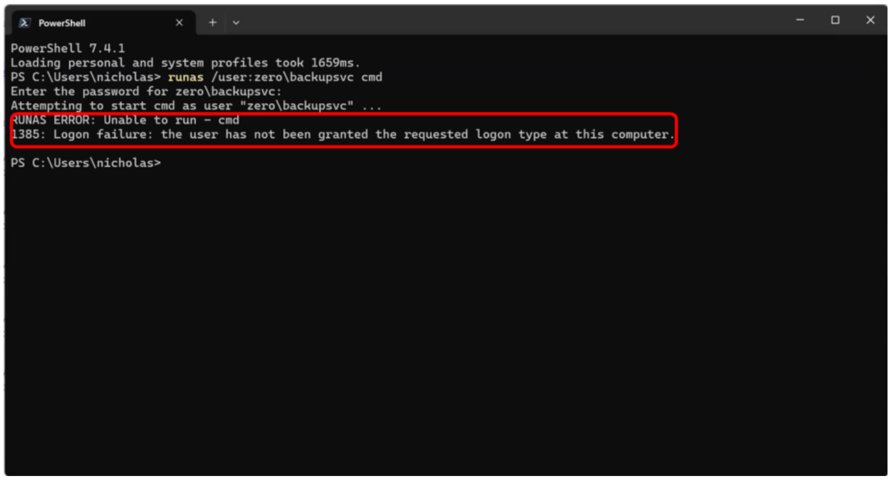
State: [✓ Enabled] Disabled

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Zero Networks also detects and identifies service accounts during the learning process and automatically creates rules to control how these service accounts can be used. We walked through an attempt to log into a service account used for backups from an end user's machine, simulating what an attacker might do to move throughout an environment.

Zero Networks successfully blocked the attempt because it had created a rule stating that local logins are not allowed. Only approved batch processes from the correct group of segmented servers can use this login to gain access to perform backups (Figure 7).

Figure 7. Blocked Service Account Login Attempt



```
PowerShell 7.4.1
Loading personal and system profiles took 1659ms.
PS C:\Users\nicholas> runas /user:zero\backupsvc cmd
Enter the password for zero\backupsvc:
Attempting to start cmd as user "zero\backupsvc" ...
RUNAS ERROR: Unable to run - cmd
1385: Logon failure: the user has not been granted the requested logon type at this computer.

PS C:\Users\nicholas>
```

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Securing service and admin accounts is notoriously challenging for many organizations. Lack of visibility into service accounts often means that they remain unmonitored, and given their elevated privileges and static, long-lived credentials, these accounts are highly vulnerable to compromise.

By a similar token, admin accounts are a prime target for attackers given their broad and powerful access rights, but enforcing strict least-privilege policies tends to be highly complex and difficult to maintain consistently across an organization.

Zero Networks segments identities, along with network assets, and grants permission for users to connect to specific endpoints when necessary. In addition to MFA policies that administer least-privilege policies for admin accounts, a robust system of inbound and outbound rules provides service account protection against lateral movement by attackers. Enterprise Strategy Group saw how a compromised service account used for backups was not allowed to connect to the backup server from a local workstation, illustrating that an attacker with access to the account would not be able to connect to it to steal data and move throughout the environment.

Attackers will try to masquerade as known identities to keep safe from detection. Zero Networks provides identity segmentation that prevents lateral movement and only allows service accounts to perform the specific function required, from a specific origin. Stealing credentials will no longer enable unfettered access across the network. Those who need access to do their work will have it; otherwise, it is not allowed, greatly reducing the risk of a data breach and stopping attackers from remaining undetected for large amounts of time.

Fast and Zero-trust Secure Remote Access

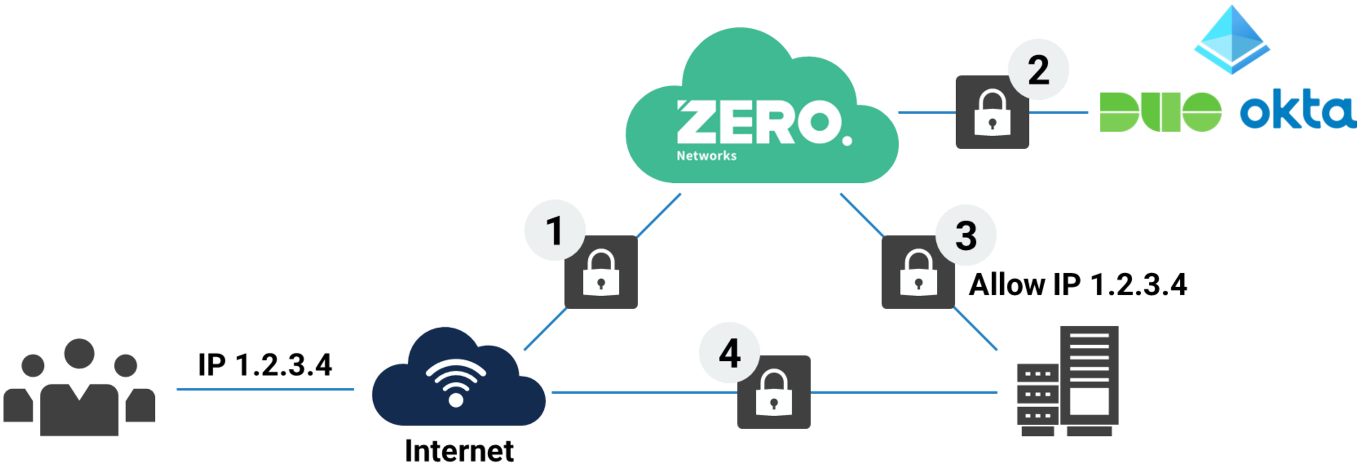
Finally, we considered how Zero Networks' secure remote access solution connects remote users securely and without sacrificing performance.

Enterprise Strategy Group Analysis

VPNs must be available to employees from anywhere they travel. High-ranking executives or sales team members may travel all over the world to conduct business. Because of this, traditional VPN solutions leave ports open across the internet so that these employees can connect when necessary.

The Zero Networks Connect platform connects remote users without obfuscation or performance impact and doesn't open ports to the internet. Figure 8 shows the process by which an employee connects to a company's network via Zero Networks Connect. Since there are no open ports to connect to, the user is directed to the Zero Networks cloud (1). The Zero Networks cloud then forwards the user to the organization's identity provider (IdP) to authenticate using MFA (2). Once the IdP verifies the user's identity, Zero Networks cloud assigns a VPN server to the user and gives the VPN server the user's IP address, and the server opens its firewall to accept requests only from that IP address (3). By doing this, Zero Networks provides VPN access without leaving any ports open to the internet. Finally, the VPN server uses the WireGuard protocol to create a direct tunnel to the user, completing the process (4).

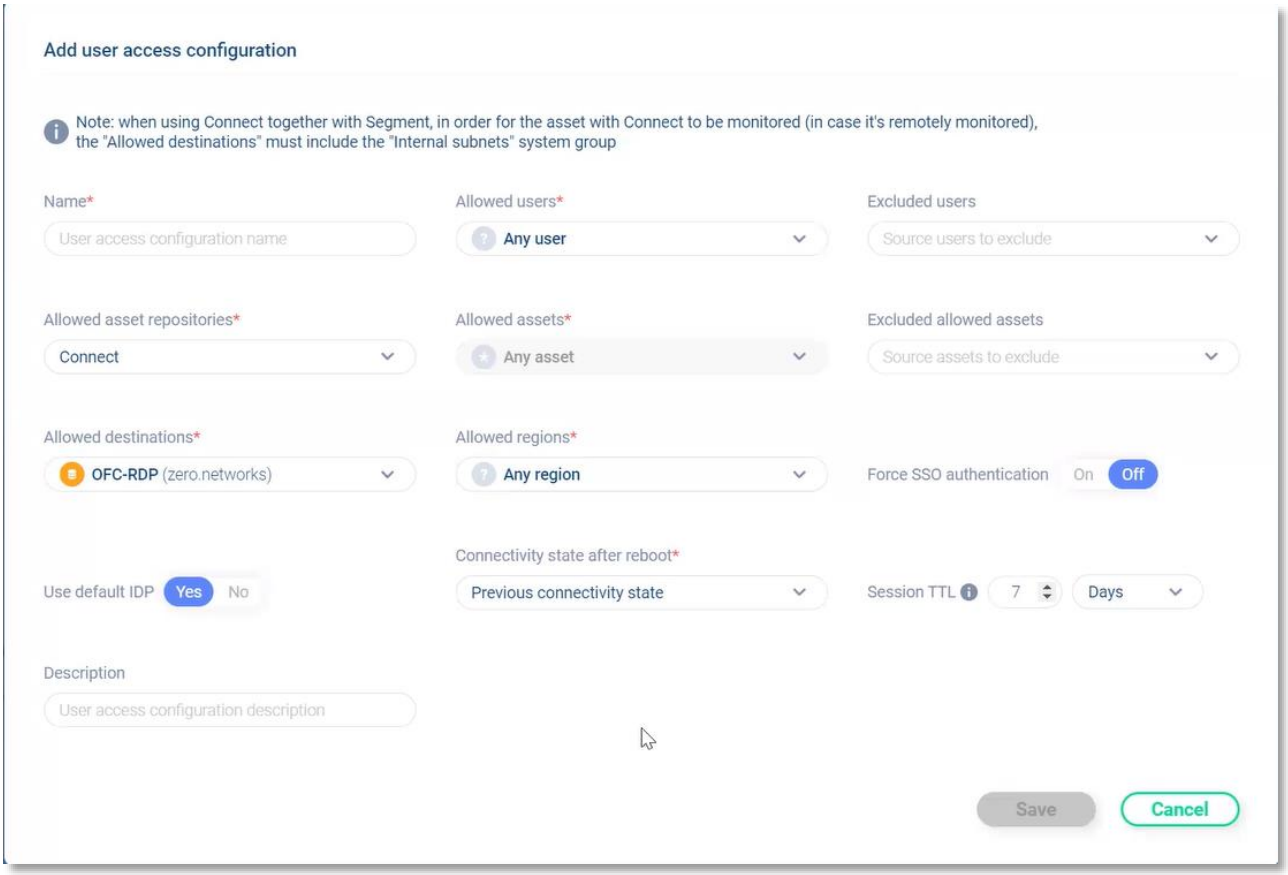
Figure 8. Zero Network Connect Architecture



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Zero Networks adds a ZTNA access control structure on top of the VPN, further enhancing an organization's zero-trust architecture. As shown in Figure 9, administrators can assign a user access configuration to users to control what they can access during a VPN session. For example, a contractor can be given access to the VPN but only to access specific machines, where an employee may be granted access to the entire internal subnet. Figure 9 shows a configuration where a user connected via Zero Networks Connect is only granted access to an RDP server.

Figure 9. Zero Networks Connect Architecture



Add user access configuration

Note: when using Connect together with Segment, in order for the asset with Connect to be monitored (in case it's remotely monitored), the "Allowed destinations" must include the "Internal subnets" system group

Name*: User access configuration name

Allowed users*: Any user

Excluded users: Source users to exclude

Allowed asset repositories*: Connect

Allowed assets*: Any asset

Excluded allowed assets: Source assets to exclude

Allowed destinations*: OFC-RDP (zero.networks)

Allowed regions*: Any region

Force SSO authentication: On [✓ Off]

Use default IDP: [✓ Yes] No

Connectivity state after reboot*: Previous connectivity state

Session TTL: 7 Days

Description: User access configuration description

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

According to Enterprise Strategy Group research, 41% of organizations listed securing remote access for employees and third parties as a key driver in their decision to move to zero trust. To support this, network and identity segmentation isn't enough to complete a zero-trust transformation. An effective tool that supports zero trust must be able to know who can access the corporate network and under what circumstances that may happen.

Enterprise Strategy Group validated that Zero Networks Connect is designed to provide secure remote access for employees and third parties without exposing ports on the internet or impacting performance. Connect uses MFA to verify a user's identity and then allows access to the VPN server only from the user's IP address. Additionally, access policies dictate what access is granted to each user.

Zero Networks Connect is a VPN-ZTNA hybrid providing connectivity without opening ports on the internet and offering granular control over user access, reducing an organization's overall attack surface. It also enables organizations to change access rules based on how users connect, offering increased flexibility to cover various use cases. All these features also make compliance with various regulations and guidelines easier.

Economic Benefit of Using Zero Networks

Enterprise Strategy Group compared the cost savings that could be expected when deploying the Zero Networks platform as compared with traditional network segmentation using firewalls and legacy microsegmentation software.

Enterprise Strategy Group Analysis

We calculated the costs associated with purchasing, deploying, and maintaining each solution in U.S. dollars using data supplied by Zero Networks for their platform and by market data for legacy solutions. For labor, we assumed a fully burdened labor cost of $165,700 per year for a skilled network engineer. We modeled the expected cost of ownership for a small-to-medium-sized business (SMB), small-to-medium-sized enterprise (SME), and large enterprise organization to support and secure their networks and users:

SMB: 500 employees, 550 endpoint devices, and 100 servers.

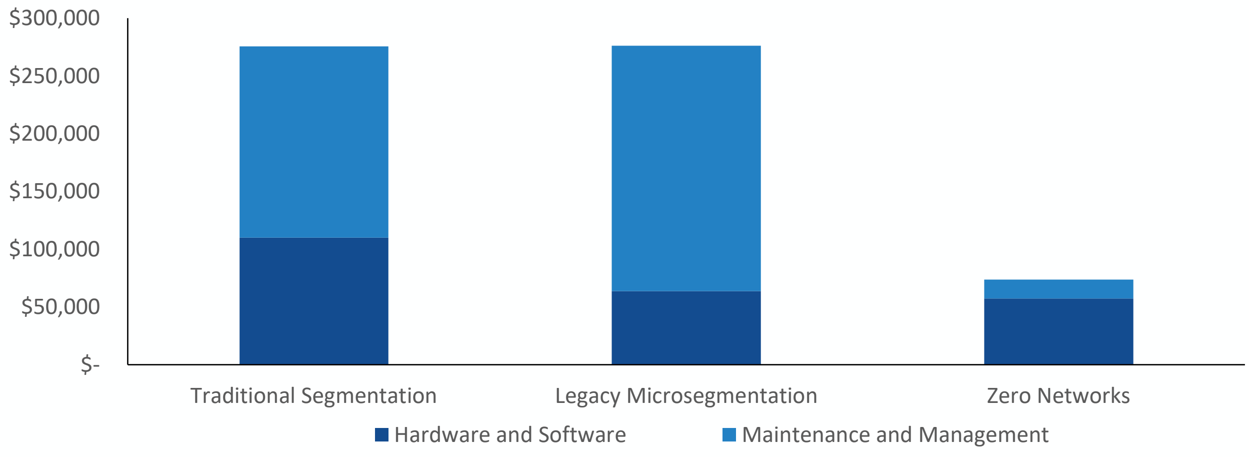
SME: 2,500 employees, 2,750 endpoint devices, and 225 servers.

Enterprise: 10,000 employees, 11,000 endpoint devices, and 1,000 servers.

Cost of ownership was calculated using a simplified model based on costs that would be incurred over a one-year period, taking into consideration typical customer costs for hardware, software, and maintenance.

For our SMB example with 500 employees and 100 servers, we calculated that Zero Networks would save 73% compared with both traditional firewall network segmentation and legacy microsegmentation. While Zero Networks acquisition costs are lower than both options, the largest savings come from the elimination of maintenance and rule management (see Figure 10).

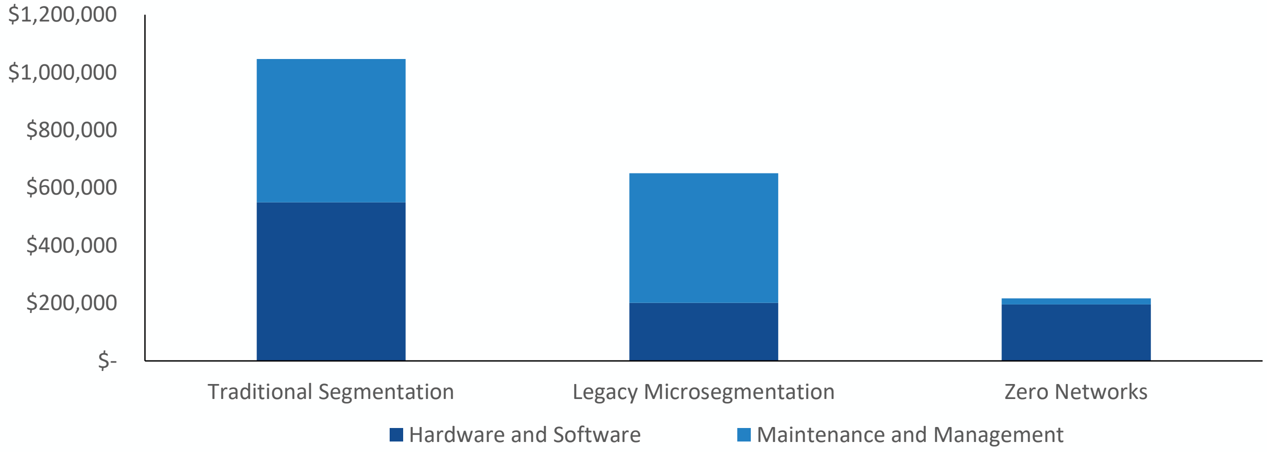
Figure 10. Network Protection Cost of Ownership Comparison: SMB



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As we scaled the number of employees and servers, we found that the savings scaled along with the size of the environment. For an SME with 2,500 employees and 225 servers, we calculated that Zero Networks would save 79% compared with traditional firewall network segmentation and 67% compared with legacy microsegmentation (see Figure 11).

Figure 11. Network Protection Cost of Ownership Comparison: SME

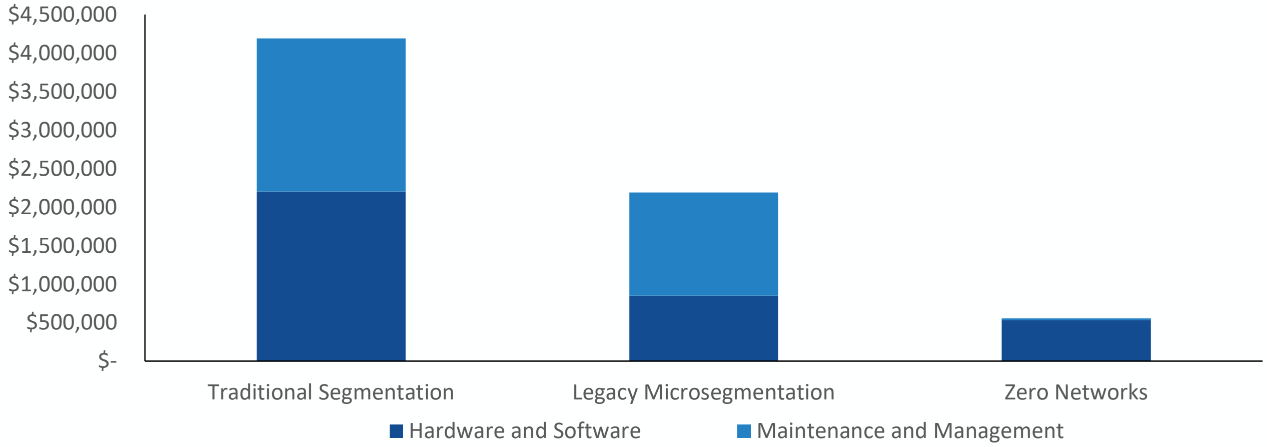


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Here we can see the challenges of scaling traditional segmentation and microsegmentation. While legacy microsegmentation acquisition costs don't increase as much as a traditional firewall approach, the labor required for maintenance and rule management is significant compared with Zero Networks.

For a large enterprise with 10,000 employees and 1,000 servers, we calculated that Zero Networks would save 87% compared with traditional firewall network segmentation and 75% compared with legacy microsegmentation (see Figure 12).

Figure 12. Network Protection Cost of Ownership Comparison: Large Enterprise



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Again, we see that the savings compared to traditional network segmentation comes from acquisition costs as well as maintenance and management of the physical firewall environment. While legacy microsegmentation scales infrastructure better, with lower software costs, Zero Networks' ability to automatically segment everything in an environment drastically reduces the overhead required by traditional and legacy solutions.

Why This Matters

According to Enterprise Strategy Group research, a broad majority (69%) of organizations have implemented or are in the process of implementing zero trust across their ecosystem, but a significant number of respondents (34%) say that they have had to pause or abandon a zero-trust project in the past for various reasons, with project cost overruns (46%) near the top of the list, just under organizational issues (47%).

Clearly, maintaining a balance between security and user experience to prevent friction when users access resources, while simultaneously controlling costs, is key.

Enterprise Strategy Group modeled and compared traditional segmentation with firewalls, legacy microsegmentation solutions, and Zero Networks' automated "segment everything" approach. We found that, in every case, Zero Networks provided significant capital and operational savings that scaled with the size of the organization. The more users and devices an organization needs to protect, the more savings Zero Networks can provide. In our calculations, we saw up to 87% savings compared to traditional firewall-based segmentation and up to 75% savings compared with legacy microsegmentation. In both cases, the lion's share of the savings was operational, thanks to the virtual elimination of maintenance and rules management.

Conclusion

As the use of SaaS, cloud-native applications, and cloud services grows, so, too, does the complexity of securing IT infrastructure. Zero trust has emerged as the preferred security model organizations use to combat this increased complexity, with 69% of surveyed organizations indicating that they've already implemented or have begun to implement zero trust within their organization. However, implementing zero trust using traditional methods of network segmentation often results in challenges, both in errors and expense, that lead to some abandoning it altogether.

Zero Networks is designed to tackle the many challenges of implementing zero trust within an IT environment. It is an automated, agentless, and MFA-powered platform for network and identity segmentation as well as zero-trust secure remote access. Zero Networks Segment watches network traffic and learns the common routes used within the infrastructure, using deterministic and predictable automation to keep the necessary network permissions open. Zero Networks IDSeg restricts admin and service account access to operational needs only, stopping privileged account abuse. Zero Networks Connect provides secure remote access with the speed of a VPN and the security of ZTNA, while overcoming common flaws inherent in each.

Enterprise Strategy Group validated that Zero Networks' automated, agentless platform segments every asset, including OT and IoT devices, on premises and in the cloud, with minimal deployment effort and maintenance. Zero Networks' fully automated network and identity segmentation reduces manual effort and prevents errors that can cause network outages. We also saw how Zero Networks prevented a compromised service account from connecting to a backup server from an endpoint device, preventing lateral movement and data theft tactics commonly employed by attackers. Zero Networks secure remote access provides connectivity without exposing ports on the public internet, making sure end users only see what they need to perform their duties. Organizations can use the Zero Networks platform to enable zero-trust transformations without expensive, complex, and manual steps that are often necessary during zero-trust implementation, delivering Opex savings of up to 87% for large enterprises.

If your organization is looking to implement zero trust throughout its environment, Enterprise Strategy Group recommends that you consider Zero Networks as an essential piece of your strategy.

Just-in-time Multifactor Authentication: Critical for Zero Trust

When asked in which identity-related security technologies organizations plan to invest the most over the next 12 months, MFA was the number one response, chosen by 41% of survey respondents.[3] MFA has become a preferred method of providing access, especially to sensitive functions or data.

Just-in-time MFA is a critical component of every solution offered on Zero Networks' unified identity and network security platform, and it serves an essential role in delivering zero-trust features to organizations. By applying MFA across the platform, including on difficult-to-protect network layer protocols, OT devices, and legacy applications, the Zero Networks platform greatly accelerates an organization's migration to a zero-trust architecture.

In each instance of MFA use in the platform, it's applied at the point of activation on the principle of least privilege and is, ultimately, what makes the tools zero trust, end to end. Further, Zero Networks' integrations with many popular identity providers enable organizations to use their existing infrastructure to secure their network. Zero Networks' use of MFA is flexible, comprehensive, and works to prevent lateral movement and unauthorized access by malicious actors.

[3] Source: Enterprise Strategy Group Research Report, *2024 Technology Spending Intentions Survey*, February 2024.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
www.esg-global.com