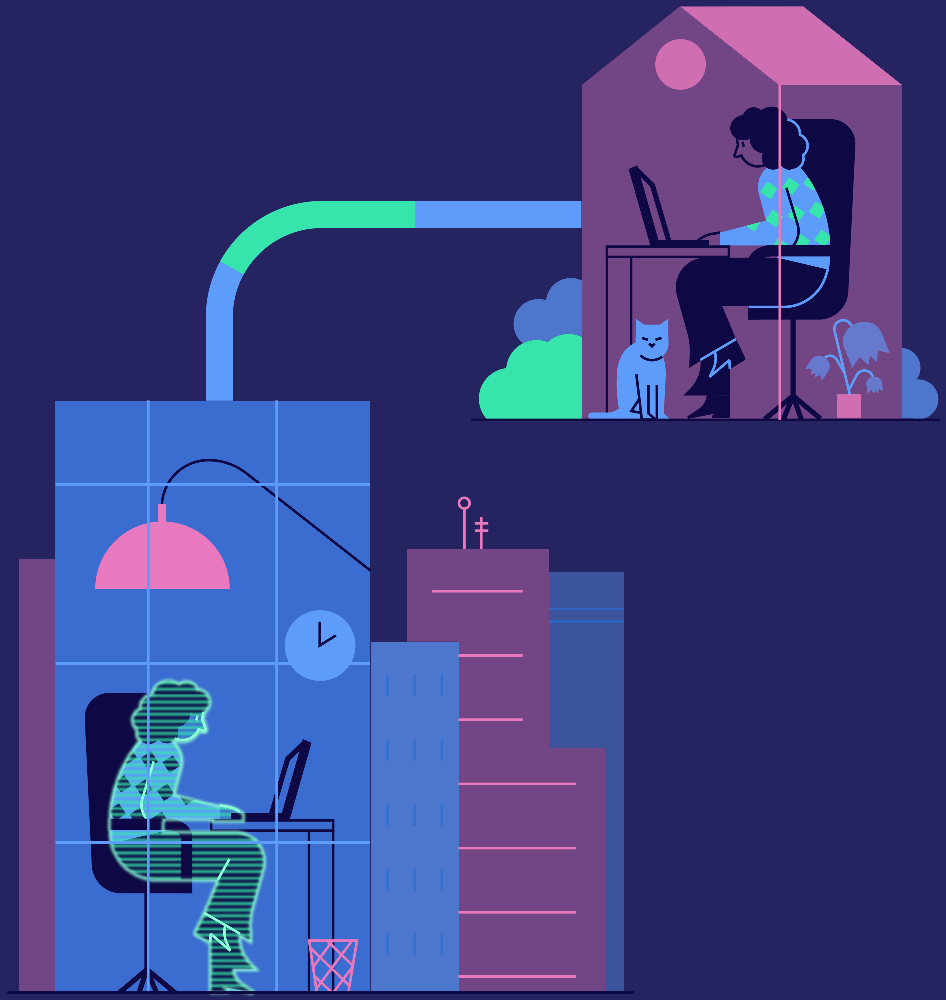
ZTNA

A Buyer's Guide



SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

ZERO. Networks

Introduction

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

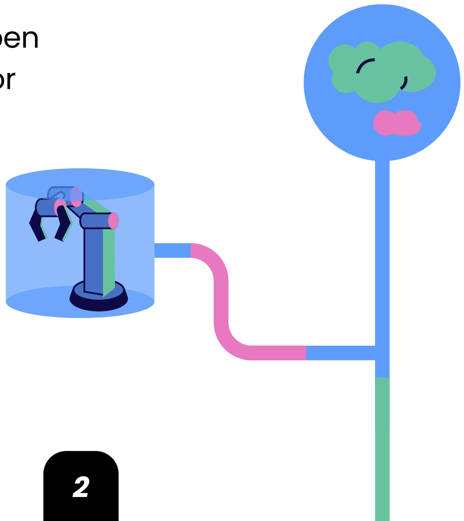
Zero Trust Network Access (ZTNA) has emerged as a critical component in securing remote access and mitigating the risks associated with traditional VPNs. Yet, the abundance of ZTNA vendors in the market can make selecting a ZTNA solution quite overwhelming. This is because many vendors throw around the latest buzzwords and make claims that are hard to evaluate. In practice, not all solutions are created equal, and finding the one that fits an organization's specific needs can be time consuming.

This guide provides an understanding of legacy VPN and ZTNA solutions, their pros and cons, and a checklist for selecting a ZTNA solution that works best for most organizations. It also explores Zero Networks' new approach to ZTNA, which takes the best of ZTNA and VPN and eliminates their inherent shortcomings. Finally, we examine the benefits of combining ZTNA with microsegmentation to provide an end-to-end zero trust network security solution.

What is Zero Trust Network Access (ZTNA)?

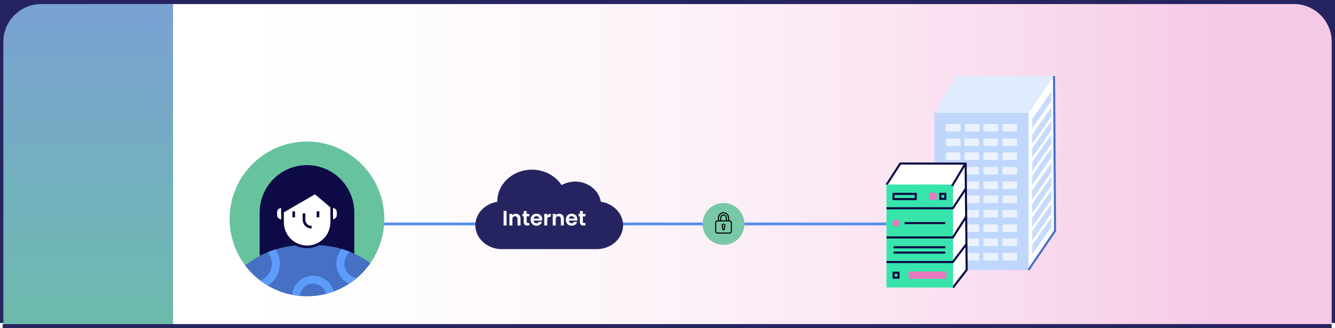
Zero Trust Network Access (ZTNA) is an advanced security approach representing an evolution beyond traditional VPNs. ZTNA emphasizes a highly secure remote access solution that doesn't require opening ports of the remote access server to the internet, a common VPN vulnerability exploited by hackers. It aligns with the Zero Trust security model, where network trust is not automatically granted. Instead, ZTNA verifies both the user's identity and the health of their device before granting access to the remote access service and later to internal resources. This approach removes a common infiltration tactic through an open port on the internet while also allowing for granular access control, considering factors such as device health, user identity, location, and specific application usage. It centralizes policy control and reduces the attack surface, making it a more secure alternative to traditional VPNs.

ZTNA serves various use cases, including VPN replacement and secure remote access for vendors or third parties, and is crucial for organizations looking to enhance their security posture in an increasingly threatening cyber landscape.



VPN: Speedy Path with Security Gaps

VPNs provide a fast and direct tunnel between remote users and the organization. However, they come with inherent security vulnerabilities and a lack of visibility and control over user activities.



Sample VPN Architecture

VPNs create a direct, fast, and encrypted tunnel connecting a remote user's device to a server within the organization's network. This connection grants the user access to network resources as if they were physically present within it. However, the VPN port remains exposed and visible on the internet, introducing security vulnerabilities.

Introduced in the late 1990s, Virtual Private Networks (VPNs) gained significant popularity in the mid-2000s as a solution for providing secure remote access to corporate networks, at a time when remote work and telecommuting started to become more common.

VPNs have remained popular in IT environments for many years due to their ability to provide a direct, fast, and encrypted tunnel between the user and the organization. However, their popularity has been declining with the changing technology landscape and security needs. While VPNs are still widely used and offer good network performance, there are some factors that have led to the exploration of alternative solutions. To better understand this evolving landscape, let's delve into a comparative analysis of the pros and cons of VPNs:

Pros and Cons of VPNs

Pros

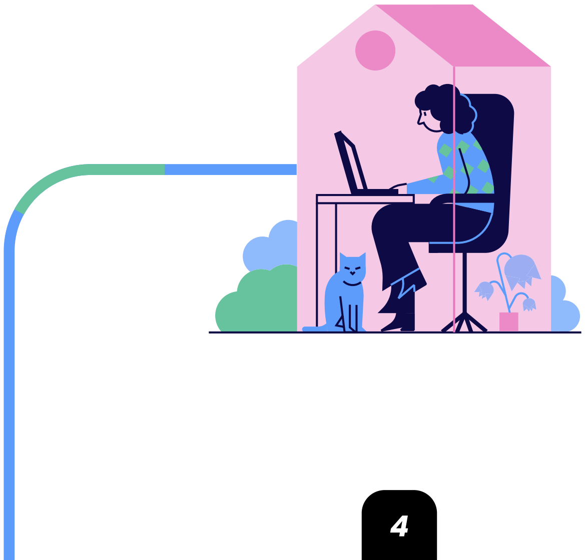
- ✓ **Optimal Performance:** VPNs offer a direct, fast, and encrypted tunnel between the user and the organization with minimal latency.
- ✓ **Cost Considerations:** VPNs are typically the most cost-effective solution, especially if an organization already has the infrastructure in place.
- ✓ **Simplicity and familiarity:** VPNs are well and widely used, making them familiar to many users and IT professionals.

Cons

- ✗ **Security Vulnerabilities:** VPNs must maintain an open port to the internet. Attackers actively search the internet for open ports and might engage in brute-force or DDoS attacks, or exploit zero-day vulnerabilities within the VPN software, which arise every several months.
- ✗ **Limited Control and Granularity:** VPNs provide users with access to the entire internal network rather than fine-grained control over access to applications and resources, making it harder to enforce the principle of least privilege.

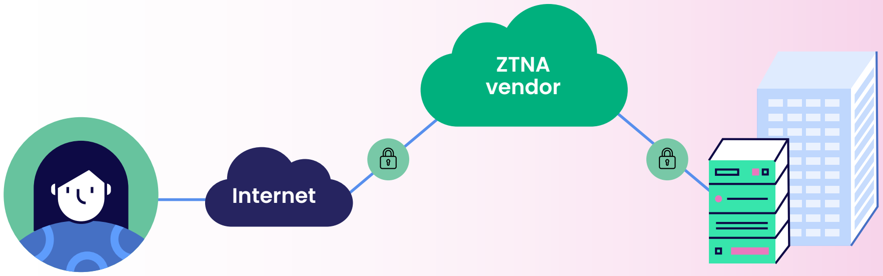
While VPNs offer fast and encrypted connectivity, they introduce security vulnerabilities and lack granular access control. They're cost-effective yet struggle with scalability and might not meet certain security standards.

In response to these challenges and evolving security needs, organizations are shifting to Zero Trust Network Access (ZTNA) technologies that offer a more tailored and secure approach to connecting remote users and devices.



Legacy ZTNA: Security at the cost of Latency

Legacy ZTNA strengthens security over VPNs by applying a zero trust approach that closes all open ports on the internet. However, ZTNA routes all traffic through cloud proxies, leading to higher latency, lower bandwidth, increased costs, and technical challenges like NATed gateway, which breaks various detection solutions.



Sample ZTNA Architecture

An access broker (ZTNA vendor) acts as an intermediary between users and their organization's network resources. It enforces access policies and controls by dynamically assigning access rights to specific users for specific resources. ZTNA solves the VPN security gaps by hiding behind a cloud proxy but introduces latency, higher costs, and other complexities because all network connections are routed through the cloud.

Zero Trust Network Access (ZTNA) marks a progressive step forward from the traditional VPN approach, addressing some of its shortcomings while introducing new capabilities. While VPNs have long provided a direct and encrypted tunnel for remote access, they often fall short in providing the necessary security, granularity, and flexibility required for today's complex networks, often granting users broader access than necessary.

ZTNA emerges as an answer to this challenge, adopting a "least privilege" philosophy that ensures users and devices only access specific resources pertinent to their roles. ZTNA offers controlled and context-aware access to resources, adopting a default deny approach and zero trust principles like resource isolation and just-in-time access. It grants access based on user identity, device, attributes, and context, minimizing risk by reducing the attack surface and adapting trust levels.

The ZTNA market has undergone significant growth. According to Gartner, the market grew by 87% between 2021 and 2022, and by 51% between 2022 and 2023. The trend is shifting towards adopting an agent-based architecture for most deployments. However, ZTNA is not without its downsides. The routing of all network traffic through cloud proxies leads to higher costs and higher latency compared to VPNs, affecting user experience. Additionally, the implementation and management of ZTNA solutions are often complex, demanding careful planning and resources. Here is a balanced view of the strengths and weaknesses of legacy ZTNA:

Pros and Cons of Legacy ZTNA

Pros

✓ **Reduced Exposure:**
With ZTNA, the organization is hidden from discovery since it doesn't have an open port on the internet. This reduces vulnerabilities to scanning and various online attacks.

✓ **Granular Access Control:**
ZTNA provides finer control over user access by allowing organizations to define access based on user identity, device health, location, and other contextual factors. This ensures that users only access the applications and data relevant to their roles.

Cons

☒ **Decreased Performance:**
ZTNAs route all network traffic through a cloud proxy, resulting in higher latency compared to traditional VPNs, which can hurt user experience.

☒ **Higher Cost:**
ZTNA solutions are cloud based, and routing network traffic through the cloud incurs much higher costs than traditional VPNs.

☒ **Obfuscation:**
Due to their NAT (Network Access Translation) architecture, ZTNA makes all users connecting to the organization appear to be coming from a single IP. This may break some technologies and render many detection solutions ineffective.

Checklist:
How to Select a ZTNA Vendor

Selecting the right ZTNA vendor is a critical decision that will significantly impact your organization's security posture for years to come. However, the influx of ZTNA vendors in the market making hard-to-evaluate claims can make this task overwhelmingly complex.

To assist you in making an informed choice, we have compiled a 12-point checklist that covers the most common considerations when evaluating ZTNA solutions. This checklist will help you navigate through essential features, security aspects, deployment ease, scalability, and more.

1 Does the vendor offer a "least privileged" model capable of granular access control for applications and resources?
This allows administrators to define specific permissions based on user identity, device health, location, and other contextual factors.

□ Yes □ No

2 Does the vendor provide Single Sign-On (SSO) and Multifactor Authentication (MFA) that integrate with your existing Identity Provider (IdP)?
MFA is critical to prevent misuse of compromised user credentials, and integration with existing IdP simplifies and streamlines user authentication.

□ Yes □ No

3 Can the vendor guarantee no negative impact on user experience caused by network performance and latency?
Routing traffic through cloud proxies frequently leads to increased latency, resulting in a negative impact on user experience.

□ Yes □ No

4 Can the vendor keep the IP addresses of all users visible while connecting inside the organization?
NAT architecture often obfuscates users' IP addresses, making it appear as if all users are connected from a single IP, creating security blind spots and breaking various detection solutions.

□ Yes □ No

5 Can the vendor combine ZTNA with microsegmentation on the same platform to offer a holistic approach to zero trust both internally and externally?
Microsegmentation and ZTNA enforce the strictest access controls at both user and application levels, dramatically reducing the attack surface both internally and externally.

□ Yes □ No

Does the ZTNA solution offer visibility into user activities and network traffic?
Visibility enables monitoring of user actions and network traffic, aiding in threat detection and incident response.

□ Yes □ No

7 Can the vendor's solution accommodate the geographic distribution of your organization's workforce?

Geographic flexibility ensures that users in different locations can access the network securely without performance issues.

□ Yes □ No

8 Is there support for secure access to both on-prem and cloud-based resources?

Secure access to both on-prem and cloud resources is essential for organizations with hybrid or multi-cloud environments.

□ Yes □ No

9 Can the vendor's solution accommodate the scalability needs of your organization?

Scalability ensures the solution can handle an increasing number of users, devices, and resources without performance degradation.

□ Yes □ No

10 Is the ZTNA solution compliant with relevant security standards, such as SOC 2 Type 2, ISO, and GDPR?

Compliance with security standards demonstrates the vendor's commitment to maintaining a secure and trusted solution.

□ Yes □ No

11 Does the solution provide integration with SIEM or SOAR solutions through an open API that is well documented?

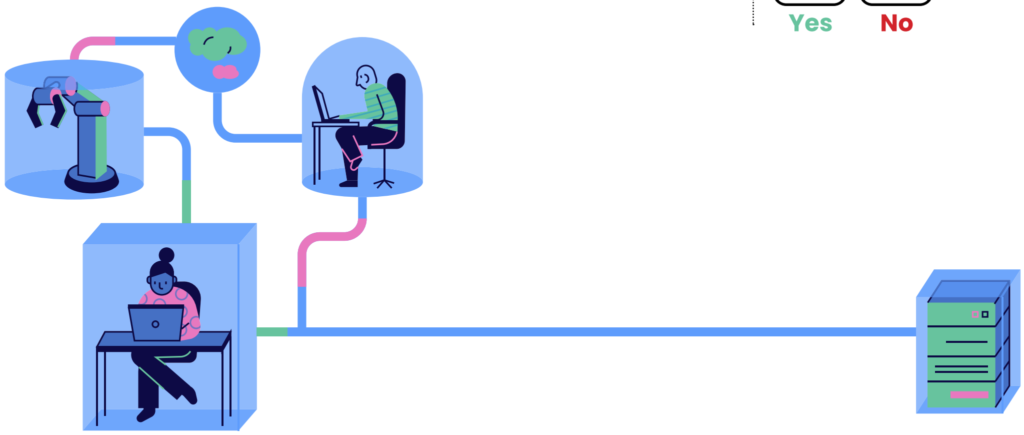
Integration with Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) tools enhances threat detection and response capabilities.

□ Yes □ No

12 Does the vendor offer pricing models that align with your organization's budget and usage? Is the solution cost-effective, and does the additional expenditure justify its advantages over VPN?

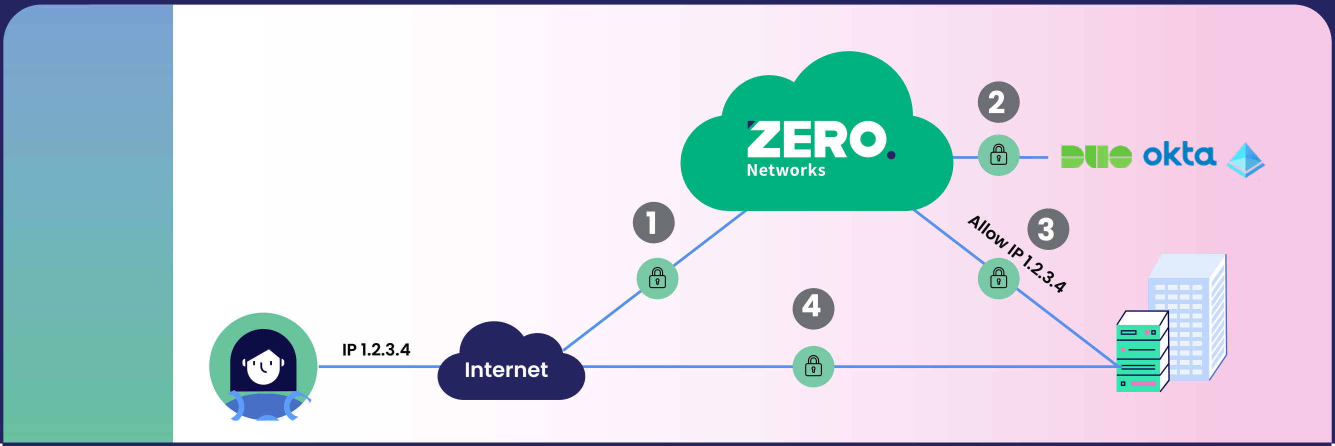
Routing traffic through cloud proxies can be very expensive: Pricing should match your organization's budgetary requirements and usage patterns.

□ Yes □ No



Zero Networks Secure Remote Access: Best of VPN & ZTNA

VPNs are fast but less secure. Legacy ZTNA is secure but introduces latency, obfuscation, and higher costs. Zero Networks combines the best of both worlds while eliminating their shortcomings.



Zero Networks Secure Remote Access Architecture

Zero Networks leverages patented MFA-based segmentation to deliver a unique VPN and ZTNA hybrid:

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.

As we've previously examined, the changing landscape of remote work has led to a focus on security solutions such as VPNs and ZTNA. However, each of these approaches has its own advantages and drawbacks, leaving IT teams in search of a comprehensive and balanced remote access solution. While VPNs offer direct, fast, and encrypted network access, they must expose open ports on the internet, making them vulnerable to hacking. 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.

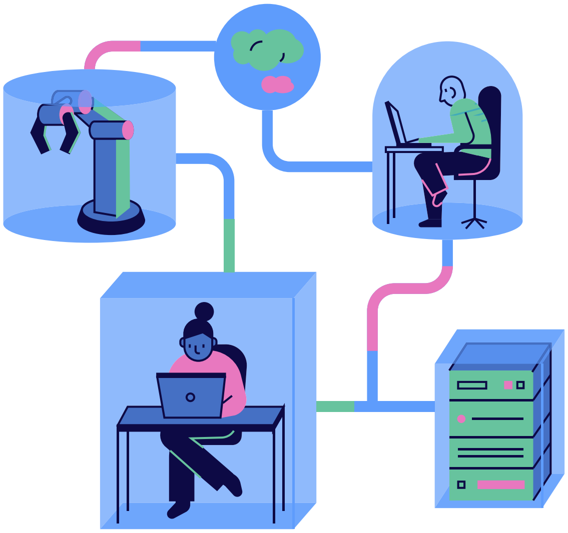
Zero Networks is an evolutionary leap in network security that melds the strengths of both VPN and ZTNA while eliminating their respective weaknesses.

Zero Networks provides optimal network performance without the latency associated with ZTNA. It ensures maximum security by not exposing servers to the internet and by avoiding the obfuscation of connections behind a single NATed IP address, a concern in typical ZTNA solutions.

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

This solution delivers benefits such as achieving a zero-trust architecture, thereby minimizing the attack surface. Both employees and third parties gain streamlined and secure remote access, enhancing usability without compromising security. With little management overhead and easy deployment, Zero Networks is designed to seamlessly integrate into existing workflows, enhancing enterprise security while minimizing disruption.

The technology behind Zero Networks is designed to optimize the end-user experience. It combines MFA-based segmentation with ZTNA capabilities. When a user connects, the solution redirects them to MFA from a pre-approved device, and it establishes a direct connection without relying on latency-inducing cloud services. Access policies are implemented based on user permission profiles, ensuring that network access is controlled and tailored according to specific needs.



Combining ZTNA with automated, agentless microsegmentation

ZTNA ensures that users and devices are authenticated and authorized before accessing resources. Microsegmentation takes this a step further by creating isolated segments within the network, up to a segment per machine, to block lateral movement. Together, they provide multiple layers of security, minimizing the attack surface.

Zero Networks is a unified platform for segmentation and secure remote access.

Combining our fully automated, agentless, MFA-powered segmentation with secure remote access enables the adoption of a holistic zero trust approach to network security.

Adaptability:
This approach accommodates changing network environments like cloud migration or remote work trends.

Granular Access Control:
Zero Networks manages user access and controls communications between applications, achieving precise control over both.

Least Privilege Principle:
Users and applications have limited access, aligning with the principle of least privilege, which reduces the impact of breaches.

Improved Compliance:
The combination enforces strict access controls and network isolation, aiding compliance with regulatory requirements.

Simplified Audits:
Clear visibility into user access and application communication eases compliance audits.

Reduced Attack Surface:
Zero Networks divides the network into isolated segments, and only authorized users can access specific segments. This minimizes potential attack paths.

Reduced Breach Impact:
Breaches are contained due to Zero Networks' limitation of lateral movement and prevention of unauthorized resource access.

Better Visibility and Monitoring:
Zero Networks offers insight into user activities and monitors application-level communication for anomalies.

Enhanced User Experience:
Authorized users access resources smoothly, and applications communicate efficiently within allowed segments.

Common Use Cases

Zero Networks Secure Remote Access

- ✓ Secure Remote Workforce Access
- ✓ Limit Third-Party Vendor Access
- ✓ Modernize VPN and legacy ZTNA
- ✓ Boost Connectivity Speed

Secure Remote Access Combined with Segmentation

- ✓ End-to-end zero trust network security
- ✓ Segmentation and lateral movement prevention
- ✓ M&A (mergers and acquisitions) Integration
- ✓ Virtual Desktop Infrastructure (VDI) Replacement
- ✓ Compliance with security standards

Checklist:
How to Select a ZTNA Vendor

1 Does the vendor offer a "least privileged" model capable of granular access control for applications and resources?
With Zero Networks, you can finely tailor access permissions, ensuring that users only have access to the specific applications and resources they require for their roles.

☑ Yes □ No

2 Does the vendor provide Single Sign-On (SSO) and Multifactor Authentication (MFA) that integrate with your existing Identity Provider (IdP)?
Zero Networks provides seamless integration with your existing IdP for SSO and MFA. We integrate with trusted IdPs like Azure AD, Duo, Okta, RSA, NetIQ, and more, ensuring a streamlined and robust authentication experience.

☑ Yes □ No

3 Can the vendor guarantee no negative impact on user experience caused by network performance and latency?
Zero Networks often improves network performance and reduces latency compared to existing corporate VPNs and legacy ZTNA by establishing a secure and direct tunnel between the user and the organization using WireGuard®.

☑ Yes □ No

4 Can the vendor keep the IP addresses of all users visible while connecting inside the organization?

Unlike legacy ZTNA solutions that obfuscate user IP addresses due to their NAT architecture, creating security blind spots, Zero Networks keeps the IP addresses of all users visible to the organization.

☑ Yes □ No

5 Can the vendor combine ZTNA with microsegmentation on the same platform to offer a holistic approach to zero trust both internally and externally?

Zero Networks is a unified platform for ZTNA and automated, agentless, MFA-enabled microsegmentation. With two powerful security controls combined, organizations can achieve end-to-end zero trust security with a simple-to-deploy, fully automated platform.

☑ Yes □ No

6 Does the ZTNA solution offer visibility into user activities and network traffic?

Zero Networks provides comprehensive insights into user interactions, application usage, and data flow. This empowers IT teams to make informed decisions, proactively detect anomalies, and ensure airtight security across your network landscape.

☑ Yes □ No

7 Can the vendor's solution accommodate the geographic distribution of your organization's workforce?

Zero Networks seamlessly accommodates the geographic distribution of your organization's workforce. Located in the US, EU, and APAC, our data centers ensure optimal connectivity, redundancy, and compliance.

☑ Yes □ No

8 Is there support for secure access to both on-prem and cloud-based resources?

Zero Networks offers secure access to a comprehensive range of resources, whether they're located on-prem or in the cloud.

☑ Yes □ No

9 Can the vendor's solution accommodate the scalability needs of your organization?

Zero Networks is engineered to effortlessly accommodate the scalability needs of any organization size without compromising on security or performance.

☑ Yes □ No

10 Is the ZTNA solution compliant with relevant security standards, such as SOC 2 Type 2, ISO, and GDPR?

Zero Networks is fully aligned with industry-leading security standards.

☑ Yes □ No

11 Does the solution provide integration with SIEM or SOAR solutions through an open API that is well documented?

Zero Networks offers seamless integration with SIEM (Security Information and Event Management) or SOAR (Security Orchestration, Automation, and Response) solutions through an open API. This capability empowers your security operations with real-time data synchronization, enabling swift and effective responses to security events.

☑ Yes □ No

12 Does the vendor offer pricing models that align with your organization's budget and usage? Is the solution cost-effective, and does the additional expenditure justify its advantages over VPN?

Zero Networks does not route traffic through expensive cloud proxies and is, therefore, among the most cost-effective ZTNA solutions on the market. Your security and peace of mind shouldn't come at the expense of your budget, and we're here to ensure they don't.

☑ Yes □ No

About Us

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, User-Friendly and scalable solution. Our robust solutions include Comprehensive Email Security, Automated Patching and Endpoint Management, Asset Risk Visibility and Management with Policy Enforcement (ARM), Third-Party Data Flow Security solutions, Agentless Micro Segmentation, Endpoint Management and Compliance Platform and an Online Gamified Simulation Platform for Cyber Security Trainingattacks.

Seeing is Believing: Book a Demo

Schedule a demo and explore how Zero Networks can fit into your organization’s cybersecurity strategy.
Visit us at srccybersolutions.com

ZERO. Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

For more information please visit us today

www.srccybersolutions.com | +91 120 232 0960 /1 | sales@srccybersolutions.com