perimeter 81

Radically Simplifying Cybersecurity with Zero Trust Networking

perimeter 81

Network Security in a Post-Pandemic World

The pandemic of 2020-2021 brought seismic shifts to the global economy and transformed the way we work. While some of us are returning to offices, we've learned how efficient we can be operating in a hybrid or fully remote environment. Work has become decentralized, cloud-based, and edgeless, with staff working from literally anywhere they can.

In Perimeter 81's Second Annual State of Cybersecurity Report, which surveyed over 500 IT professionals in US firms with 50 or more employees, an overwhelming 87% of respondents reported that they will continue to work in decentralized, hybrid frameworks into 2022. More than half plan on remote work continuing 3 to 4 days a week regardless of pandemic conditions.

This is not a trend. It is a new reality.

With the remote distribution of employees and corporate networking resources come far-reaching IT, networking, and data security concerns. Perhaps the most clear-and-present danger is that the attack surface is now significantly larger than when employees were onsite and using on-prem networks. Perimeter 81's report revealed that 64% of respondents experienced a significant cybersecurity incident in 2020-2021, including ransomware (33%) and phishing (43%). Other reported threats included data theft (19%), supply chain attacks (13%), employee leaks (12%), vishing (10%), and more.

In other words, if your company has migrated any network resources to the cloud, securing these attack surfaces should be your number one priority.

Too Much of a Good Thing?

As the number and diversity of attacks grows, so has the number of IT solutions we have available to throw at them. Like Authentication, Cloud Access Security Broker (CASB), Cloud Sandboxing, DNS Security, Endpoint Security, Firewalls, Firewall as a Service, Mobile Device Management, Secure Web Gateways (SWG), SD-WAN, VPN, ZTNA, and more.

Thirty percent of all responding companies in our survey use more than 20 cyber and network security tools. As the size of a company grows, so does the number of tools. Exactly half of all companies with more than 1,000 employees use at least 20 cyber and network tools and 19% use more than 30!

But the complexity of using so many tools—which we call the Cyber Complexity Trap—has a price. Forty-five percent of respondents, and 71% of the VPs and CIOs among them, feel that the number of cybersecurity tools negatively impacts the ability of their IT departments or service providers to detect and prevent threats. Some 29% of VPs and CIOs feel that this always or almost always occurs, while 36% feel that this occurs often.

So how can your company avoid the Cyber Complexity Trap?

perimeter 81

Zero Trust for Near-Zero Attacks

A good place to start is with a unified, cloud-based Zero Trust Network Access (ZTNA) solution. An elegant, unified cloud-based ZTNA solution helps make network security significantly less complex.

Zero Trust, or Zero Trust Network Access (ZTNA), is a cybersecurity concept centered on the best practice that no network user should be automatically trusted to access any computing resource on the network or on the cloud. Zero Trust access means to first verify the identity of the user, classify them, and then allow access based on who they are and what they need to do—not where they are located. Users are granted access only to applications they have a legitimate need for, with rights and permissions granted to reflect that need.

It starts by directing all traffic through a unified ZTNA solution. There it is either blocked or permitted to pass through. When combined with virtual network segmentation using Firewall as a Service (FWaaS), a hacker with stolen credentials will have their access limited to only specific areas and will not be able to fully traverse the network. This approach will reduce the level of exposure by an order of magnitude.

Many companies are also choosing to deploy a ZTNA solution because it allows them to offload traffic when the capacity or bandwidth limitations of traditional VPNs are an obstacle for expanding their remote workforce. Furthermore, phasing out legacy VPNs can reduce the never-ending need to support widely deployed VPN agents and outdated hardware. And with the concept of agentless identity, organizations can realize the benefits of ZTNA even for non-managed devices.

Zero Trust as a Secure Access Service Edge (SASE) Service

One of the biggest challenges of deploying a ZTNA solution lies in the inherent architecture of networks and cybersecurity solutions. As more and more companies scale and grow (or just survive like in a pandemic!) by using cloud-based IT products and services, more data, users, devices, applications, and services are being deployed outside the perimeters of traditional enterprise premises.

Despite this shift outside the perimeter, network architectures and security solutions often lag behind and force all traffic through an on-prem network perimeter only to go back out. That's why more companies are selecting ZTNA products aligned with Secure Access Service Edge (SASE) architecture to enable scalable networks and foolproof security delivered completely as a cloud service.

perimeter 81

Four Great Reasons to Replace VPNs with a Cloud-Based ZTNA Solution

1. Security

VPN technology was created in a world where cloud computing didn't yet exist, SaaS was in its infancy, and most employees went to an office every day. Using antiquated technology to secure and provide remote access in modern distributed networks is simply asking for trouble. Cybercriminals have been tremendously successful in exploiting the many vulnerabilities of legacy VPNs. A key problem is their inability to segment the network. This means that once a bad guy hacks a VPN, they get free access to the entire network.

2. Monitoring and Management

Compounding VPN's inherent security flaws is a lack of visibility and control at the network edge. Today's distributed networks and remote hybrid workers dramatically enlarged the corporate networks' attack surface, exponentially increasing risks of network breaches. User access must be monitored and managed to identify and remove potential threats quickly. A high-performance ZTNA solution provides for continuous user authentication and activity monitoring. Your IT staff or service provider is tasked with the job of monitoring and management. The right ZTNA solution makes this job easy and seamless.

3. Performance

According to Forrester, VPN performance issues were the main reason customers chose to adopt during the Covid-19 pandemic. The inability of VPNs to deliver high-speed access to cloud resources became painfully clear as companies shifted to almost 100% remote work during pandemic lockdowns.

It makes no technical sense for remote users to connect to on-premise data centers (where there are no workers) for authentication before going back out to the Internet to access cloud-based applications like Zoom or Office 365. ZTNA solutions are optimized for high performance and scalability, and the best offerings will provide dedicated, high-speed, and encrypted tunnels directly to cloud resources.

4. Scalability

Employees and contractors come and go, acquisitions are made, new devices, and applications are deployed. Changes like these mean burdensome and time-consuming tasks—like reconfiguring your VPN. And adding third-party contractors to VPNs is especially cumbersome as you need to protect your internal resources from a less-trusted user.

A single ZTNA management console allows IT staff to perform tasks in minutes tasks that would take hours and days with a VPN. Create networks and add bandwidth capacity with a few mouse clicks. Adding or deleting users is equally fast and easy, and third-party contractors can be granted access to only the applications they need to perform their job.

perimeter 81

The Perimeter 81 ZTNA Advantage

Perimeter 81 offers a powerful cloud-based ZTNA solution built into its Cybersecurity Experience (CSX) Platform. The CSX Platform is the first platform to streamline SASE. The platform's groundbreaking ease-of-use and radically simple design are based on four principles:

- **Instant Deployment:** In just a few clicks, Perimeter 81 allows you to purchase, provision, and enable secure zero-trust access on-prem, in the cloud, and anywhere in between. Quickly scalable microservice architecture and transparent pricing allow you to easily grow, backed by our 24/7 Customer Success engineers.
- **Unified Management:** Effortlessly manage and onboard network users, instantly deploy secure cloud gateways, create multi-regional networks, and install cross-platform applications across all endpoints within a single dashboard.
- **Full Visibility:** Effectively monitor network health, view employee resource access, integrate with leading SIEM providers, and identify any suspicious activity with a unified view of your network security.
- **Integrated Security:** Avoid the complexity of using dozens of cybersecurity solutions with a single well-designed platform that makes it easy to configure your network, implement security policies, detect active attacks, and defend against data breaches.

The Perimeter 81 CSX Platform allows enterprises to ditch legacy hardware and fully embrace the agility of the modern era. It's the right solution in a world where accelerating complexity is the single greatest threat to effective cybersecurity.

Secure Network Architecture

The Perimeter 81 ZTNA solution ensures that users access cloud resources via encrypted tunnels directly from the Perimeter 81 network, so you can lock down network resource and application access using Zero Trust policies, rules, and permissions. The Perimeter 81 network is global with over 40 PoPs located across the globe. Traditional VPNs generally allow access to all network resources after the initial connection, but Perimeter 81 ZTNA ensures that users only have access to the resources they need, even after they are connected. DNS filtering adds another layer of protection to ensure users cannot access risky websites. The Perimeter 81 solution secures access to any network resource: on-prem data centers, public cloud (AWS, Azure, GCP), or private cloud via an IPsec or Wireguard tunnel. And Perimeter 81 supports all ports, all protocols, including non-web applications like VoIP. Each Perimeter 81 gateway offers 1Gb/s of bandwidth.

perimeter 81

Secure Connectivity

Perimeter 81 constantly checks credentials to ensure that only authorized users are connected, while traditional VPNs assume user and device security only after a credential check upon initial login. The Perimeter 81 Agent Supports Mac, Windows, Linux, IOS, and Android. No VPN solution can offer Device Posture Check to ensure devices are compliant with security components like antivirus and more. And in terms of scalability, Perimeter 81 ZTNA offers a browser-based, agentless option that provides secure access to internal network applications without access to the network. This feature is particularly useful for contractors and other third parties

Radically Simple Management Platform

A major factor in the radically simple design of Perimeter 81 is its management platform. Perimeter 81 provides a single dashboard for multi-tenant security policies and tracking access across networks and resources. The management platform, which can get a secure network up and running in under 30 minutes, provides for easy and seamless integration with existing identity provider solutions, enabling secure and user-friendly Single Sign On (SSO) capability. This elegant and intuitive user interface makes it easy to independently set and change access rules and policies as well as to add and remove users. Traditional VPN solutions lack the edge network control and visibility that IT admins need in today's modern hybrid environments.

This, and more, is why Forrester named Perimeter 81 as a Zero Trust Network Access leader and gave Perimeter 81 the highest marks possible in the non-web and legacy apps, client support, product vision, and planned enhancements criteria.

POSTMAN

"We selected Perimeter 81 as our SASE partner because they exceeded all of our acceptance criteria. We needed a solution that did not require any additional hardware to implement, and that is one of the strengths of a SASE: We can define everything via software. We were able to configure secure tunnels directly to our Cloud VPCs for specific workloads, create applications to allow users to launch internal web resources from any device securely, and restrict access to internal resources to just our users."

- Ryan Nolette, Technical Security Lead

perimeter 81

Perimeter 81. Radically Simple Cybersecurity

Protecting customer data is important for every organization. The Perimeter 81 Cybersecurity Experience (CSX) Platform delivers smarter, more scalable security for businesses. Providing cost-effective, scalable security and outstanding performance, the Perimeter 81 CSX platform secures all your data with a seamless, unified network security tool.

Scale with Total Ease

Control access to specific network segments, create and manage traffic policies, whitelists and blacklists, and enforce rules based on role, location, or device.

Protect Against Breaches

Multilayer network security platform covers access management, encryption, traffic rules, IP whitelisting, DNS security, and 2FA.

Simplify Regulatory Compliance

Protect sensitive business information with a single solution compliant with all regulations, including HIPAA, HITRUST, GDPR, SOC 2 Type 2, and ISO 27001/2.

Enable Secure Work from Anywhere

On-site, at home, or on the road, secure network as a service delivers easy and secure connectivity for low latency remote resource access.

About Perimeter 81

Perimeter 81 radically simplifies cybersecurity with the world's first Cybersecurity Experience (CSX) Platform. As a holistic, cloud-based solution, Perimeter 81 allows organizations of all industries and sizes to support the immediate desires of the nomads with a purpose—while still granting IT teams the ability to manage it all safely. The company was founded in 2018 by two IDF elite intelligence unit alumni, CEO Amit Bareket and CPO Sagi Gidali, and is based in Tel Aviv, the heart of the startup nation. Our clients include SMBs to Fortune 500 businesses and industry leaders across a wide range of sectors. Our partners are among the world's leading integrators, managed service providers, and channel resellers.

perimeter 81

Contact Us

Perimeter 81 Ltd.
www.perimeter81.com
+1-929-575-9307

Book a Demo