perimeter 81

The Ultimate MSP Guide to Zero Trust



perimeter 81

How MSPs Secure Networks with Zero Trust

Managed Service Providers (MSPs) face a pivotal mission in safeguarding networks against constant risks. With hybrid and remote work models becoming the norm, MSPs are turning to cloud-based solutions to provide their customers with efficient and secure network access for all users, anywhere.

This remote work era has brought about new risks for endpoint and resource exposure and compromise, which requires solutions that better address security and the need for 24/7 visibility and network management.

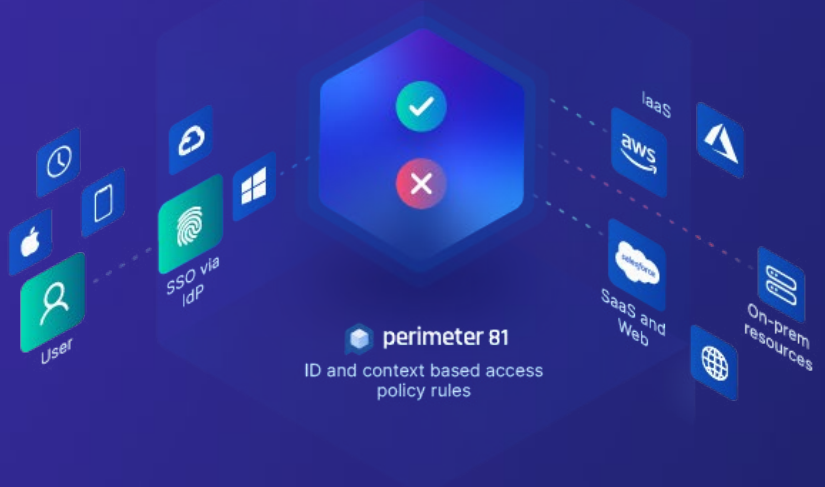
Today, MSPs need to create secure client networks for cloud and on-premises resources that are accessible from anywhere at any time. This approach provides full control and visibility into which cloud and on-premises resources are being used and by whom.

With the Zero Trust model, MSPs can secure on-premises and remote resources based on the “never trust, always verify” approach, protecting client networks ranging from small to mid-sized companies.

What is Zero Trust Security?

At its core, Zero Trust (ZT) is a security model that says organizations should not automatically trust anyone just because they are inside the network perimeter. Instead, companies should verify anything and everything before granting access to resources.

With a cloud-based Zero Trust Network Access solution that includes multi-tenant management capabilities, MSPs can handle networking and network security services for their clients with complete ease.



All rights reserved. Perimeter 81 | 2023

Follow Us

perimeter 81



Zero Trust Network Access (ZTNA)

ZTNA helps MSPs manage secure network access for remote and in-office employees while reducing the maintenance and hardware costs of on-prem solutions. ZTNA enables a stronger user-centric security posture based on identity and context, enabling secure access to cloud and on-premises resources.

ZTNA solutions must also integrate with Identity Provider-based authentication, enable Single Sign-On, and include policy-based network segmentation, encrypted tunneling, and real-time activity monitoring.

A key piece of ZTNA is also Device Posture Check, which ensures that only authorized devices can connect to your customer's network. DPC inspects devices for the presence of certificates, specific files or processes, antivirus software, disk encryption, and more. This helps prevent potentially dangerous or unauthorized devices from connecting. DPC reports provide an inventory of connected devices and device health, allowing you to zero in on suspicious activity.



Access for Unmanaged Devices

Agentless Zero Trust Network Access (ZTNA) allows employees and third-party contractors to securely access specific applications using the HTTP/S, RDP, VNC, and SSH protocols via a browser portal. With Agentless ZTNA, users are only given access to specific apps, not the wider network. Users' application access is tracked and limited according to criteria such as location, time, browser, OS, device, and more.



Firewall as a Service (FWaaS)

Firewall as a Service enables granular access control to specific network resources, protecting the network from potential exploits or breaches. FWaaS allows admins to control who accesses which resources in their network, based on global user-centric security policies.



Secure Internet Access With SWG

Web Filtering and Malware Protection delivered as a Secure Web Gateway (SWG) is an essential part of any network security solution. Web Filtering allows MSPs to manage user Internet access according to role-specific permissions. You can block web categories and specific sites on a per-user or per-group basis. Malware Protection, meanwhile, stops ransomware and malvertising at their source. IT admins can keep track of all users' web activity and investigate any suspicious access with Web Activity Monitoring.

All rights reserved. Perimeter 81 | 2023

perimeter 81

Zero Trust and the Perimeter 81 Solution

Perimeter 81 provides all the essentials MSPs need from a Zero Trust-based networking and network security solution.

Securely manage each customer's networks, users, and assets with our easy-to-use cloud-based, multi-tenant console. This allows efficient management, seamless configuration and in-depth monitoring for each client.

In addition, Perimeter 81's Hybrid SWG provides a unique new approach for web protection with functionality both on user devices and in the cloud for the ultimate flexibility in deployment options. See our Hybrid SWG Feature Overview for more detailed information.

Additional Perimeter 81 key features include:

- Lightning fast deployment
- Single-pane-of-glass management console
- SSO, SAML, AD integration
- High performance global backbone
- Global coverage with more than 40 PoPs
- Web and mobile support
- Full auditing and monitoring

Partner up for the perfect match

Perimeter 81's Channel Partner Program enables channel partners to level up their networking and security offering with a comprehensive, yet easy to learn and manage, fully cloud-based solution.

Perimeter 81 enables partners to reduce operational complexity and costs by replacing multiple network security products with a single, converged, and easy-to-use cloud-based service. With no upfront investment and frictionless onboarding. Our comprehensive technical training, best-in-class sales and marketing collateral, and 24/7 dedicated technical support makes sure we always have your back.

With our single-pane-of-glass web portal, you can easily manage and secure your customers' access to cloud and on-premise resources, and track your own performance on the Partners Portal.

All rights reserved. Perimeter 81 | 2023

perimeter 81

> “For our partners, Perimeter 81 represents a one-stop shop where they can deploy both security and networking across any number of tenants. Our single management console and freedom from all hardware requirements helps partners ramp up recurring revenues in no time.”



Amit Bareket, CEO of Perimeter 81

Benefits of Partnering with Perimeter 81

- **Never pay before you are paid**
  You pay us only when your customers pay you
- **No Upfront Costs**
  No hardware, licenses or training costs in order to onboard
- **Prepackaged, ready to go campaigns**
  With Perimeter 81’s campaign-in-a-box kits, your marketing efforts are ready to hit the ground running
- **Free training**
  Perimeter 81 is committed to empowering our partners by openly sharing all learning collateral and providing training free of charge
- **Seamlessly scale customer footprint**
  As a fully cloud delivered SaaS platform we enable our partners and their customers to grow as much as they need
- **Expand your solution portfolio**
  Add additional security and network services to beef up your solution stack and offer more value to customers
- **Quick time to value**
  With Perimeter 81 you can get up and running within days, and onboard new customers within hours
- **Free professional services**
  Our professional services team can help solve any issues that arise in order to provide your customers with the best support possible

All rights reserved. Perimeter 81 | 2023

perimeter 81

About Perimeter 81

Perimeter 81 is a robust, yet easy-to-use, converged networking and network security platform that connects all users, in the office or remote, to all resources, located on-prem or in the cloud. It is a cloud-native service that includes advanced capabilities such as Zero Trust Remote Access, Internet access control, malware protection and firewall as a service. It enables any business to build a secure corporate network over a private global backbone, without hardware and within minutes. The entire service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

Learn More About Partnership Opportunities

Perimeter 81 Ltd.

sales@perimeter81.com

perimeter81.com

Partner With Us

All rights reserved. Perimeter 81 | 2023