perimeter 81

The CISO's Guide to Avoiding the Next Breach

It ain't easy being you. The role of a CISO is very demanding. First and foremost, you have to make sure your security is strong enough to withstand attacks that lead to breaches, all the while meeting increasingly stringent budget constraints.

That's why we developed Perimeter 81's networking and network security platform. We want to make it easier for companies to provide robust security that's easy to scale up as needed, while reducing the total cost of ownership. All it takes from you is a willingness to let go of that antiquated VPN appliance guarding an increasingly non-existent perimeter.

The Challenge of Modern Network Security

Most companies are a long way from the days of using exclusively on-prem resources. The sales team has their CRM in the cloud, the DevOps team has a bunch of operational data in the public cloud, R&D is using GitHub or Bitbucket, and on and on it goes. Of course, the on-prem data centers are still a key part of the operation, but they're augmented by SaaS applications and the public cloud.

That presents a real challenge for network security since company resources are no longer centralized. But it's not just the resources that are distributed, your employees are also global. Modern companies can have employees in the U.S., the U.K., Singapore, as well as freelancers anywhere between India and Illinois.

If your company resources and employees are everywhere, shouldn't your network security be too?

Right now, for many companies it's not. Instead, they rely on a hardware VPN located at a data center that could be halfway around the world. Employees from all over the world connect to that for their on-prem needs, as well as for secure access to the Internet.

That just doesn't make practical sense. Why backhaul Internet traffic halfway across the world when people could just connect directly to the Internet through a gateway in their region? The on-prem approach creates laggy connections that unnecessarily lower employee productivity and raise general frustration levels. Employee needs are not served by a hardware solution with locations at a single, or at best, handful of locations.

All rights reserved. Perimeter 81 | 2022

Even when VPNs were the best solution for companies to provide remote access, they still had serious shortcomings. For starters, VPNs can only be gatekeepers at the perimeter. Once inside the network, users often have free access to the network since segmenting the network into access zones with firewall appliances isn't so simple.

The Answer for the Distributed Company

If VPN hardware paired with firewalls isn't the answer then what is? Modern companies need a solution that provides fast access to the Internet and company resources with a network of globally distributed PoPs. In addition, they need an easy way to segment resources that adds modern security enhancements such as continuous verification.

Add it all together and you get a security formula that reduces the risk of enduring a breach, and even if a determined attacker gets in, their ability to achieve lateral movement will be greatly reduced.

Zero Trust Network Access: A Collection of Technologies

The centerpiece of a modern remote access and network security strategy is Zero Trust Network Access (ZTNA). This isn't so much a turnkey solution as much as it is a strategy. It combines secure connections, application-focused firewall rules, identity verification via a single sign-on provider with MFA, and customized (and continuous) device posture checks.

Unlike hardware solutions, all of Perimeter 81's ZTNA components are cloud-based meaning you can set the rules from a single dashboard and see them instantly propagate across the network. In addition, we make it easy to set granular access rules by individual or group, and device posture checks can require hat company devices are running a specific antivirus suite, a minimum operating system version, and more. These device rules are then checked at regular intervals to make sure that the status of connected devices hasn't changed. If they do, they are immediately disconnected from the company resource.

As for unmanaged devices, Agentless ZTNA allows them to connect to specific applications through a web portal with support for applications using HTTP/S, RDP, and SSH.

ZTNA is one of the top defenses against breaches for a simple reason: very few people have access to the entire network. If an attacker took over an employee account they would only be

All rights reserved. Perimeter 81 | 2022

able to see what the employee could see making lateral movement much harder.

CISOs and IT Managers can also reduce the threat of administrator accounts falling into the wrong hands with a higher degree of multi-factor authentication requirements, and careful log monitoring for unusual behavior from those accounts.

Protect Users Online

While ZTNA goes a long way toward keeping company resources secure, web security should also be a major concern. If malware infects your network, the most likely delivery method will be via the web. This could be anything from an infected download from webmail to a malicious ad or website.

To combat these threats, Perimeter 81 offers Web Filtering and Malware Protection. The former restricts access to websites by employees on managed devices. We offer general prevention categories such as blocking gambling or social media sites, as well as known phishing sites and other undesirable web destinations.

Malware Protection, meanwhile, protects employee devices from harmful code delivered via the web whether they're connected to the company network, or not.

Avoiding the Next Breach

With a set of solid ZTNA access rules in place backed up by continuous verification and MFA from your SSO provider, getting into the network becomes much harder. Even with a set of employee credentials, breaching with user credentials is difficult since there are so many obstacles to overcome including MFA and device posture checks. But even if threat actors are able to overcome all of those challenges, they will not have access to the complete network thanks to ZTNA. They will only have access to what the employee can access. That, at the very least, will restrict the amount of data a threat actor can extract.

On the Agentless ZTNA side, you can help prevent the misuse of credentials by adding context rules such as time of day and regions from where access is permitted.

Finally, Perimeter 81's web protection helps protect against threats that could lead to a data breach such as keyloggers and other spyware, ransomware, and Trojans.

All rights reserved. Perimeter 81 | 2022

perimeter 81

Cloud Secured and Delivered

In addition to the basic tools, Perimeter 81's cloud-based solution lets you control everything from a centralized dashboard. This allows you to quickly and easily update access and device posture rules, monitor network activity, spin up or down new gateways, and view logs or integrate them with your SIEM solution for automated security monitoring.

Our lightning-fast deployment will get smaller companies up and running in minutes, while mid-size enterprises can be ready to go in a few days. Since there's no hardware to purchase you reduce maintenance and training costs, and scaling up to meet your growing needs is as easy as a few clicks.

Finally, all of this is available at a significantly lower cost than a hardware solution with no long term commitments required.

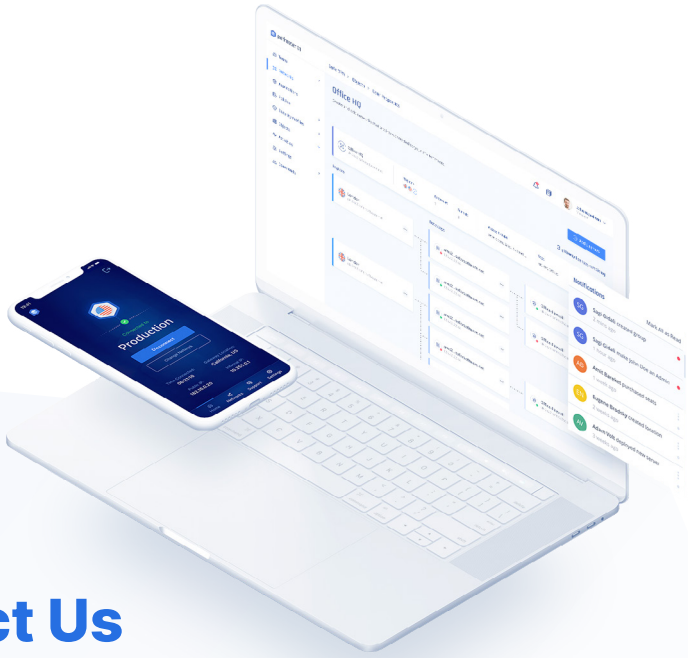
Ready to give it a try? Book a demo with a Perimeter 81 network expert today.

All rights reserved. Perimeter 81 | 2022

perimeter 81

About Perimeter 81

Perimeter 81 is a robust, yet easy-to-use, converged networking and network security platform which connects all users, in the office or remote, to all resources, located on-prem, or clouds. 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.



Contact Us

Perimeter 81 Ltd.

sales@perimeter81.com

perimeter81.com

Request a Demo

All rights reserved. Perimeter 81 | 2022