ERICOM
Be Connected, Be Secure

Time to upgrade to Zero Trust Network Access

Contents

Executive summary

Businesses worldwide are facing substantially elevated security risks -- the unintended result of doubling down on VPNs to quickly connect suddenly remote workforces to the corporate apps and data they need. Cybercrime has surged as hackers exploit new opportunities to penetrate organizations with relative ease.

In response to this increase in advanced threats, more businesses are exploring adding Zero Trust Network Access capabilities to protect their networks. In this paper, we discuss two ways to add these important safeguards: Through Software Defined Perimeter (SDP) solutions and with a new solution called Ericom Application Isolator. We compare these solutions as alternatives for organizations committed to protecting their networks, highlighting their abilities to secure remote connections to apps and IT resources as well as protections they offer within the office environment.

Is it time to retire your VPN?

It's been a struggle to update VPNs to operate securely within the modern threat landscape

For decades, virtual private networks -- VPNs, for short -- have been the most popular tool for connecting remotely to corporate work environments. A VPN enables corporate users to send and receive data across public networks such as the internet through a secure encrypted tunnel. It provides something akin to a direct, private connection to the corporate network.

VPN technology, however, was introduced at a time when business IT environments resided on a business's premises, and did not include distributed elements that are now commonplace, such as cloud computing, mobile devices, and flexible remote work policies. While VPNs have adapted to remain relevant, despite changes in how people now work, it has been a struggle to update them to operate securely within the modern threat landscape.

Despite this, thanks to office closures associated with COVID-19, VPN traffic is at an all-time high. Organizations doubled down and invested heavily in VPN technology to quickly connect their newly distributed workforce to the applications and resources they need. While VPNs were perhaps not the perfect solution, they were on-hand, familiar, and easy to augment quickly.

The recent increased dependence on VPNs notwithstanding, change is unquestionably coming. Ironically, the impetus for that change is also a phenomenon that experienced rapid growth during the pandemic: Specifically, burgeoning – and often VPN enabled -- threats to network security.

The stranger dangers of VPN

Susceptibility to attacks is built into many legacy VPN architectures. Corporate network VPNs must be discoverable on the public internet to enable access. As a result, any malicious agent can "come knocking" on an organization's VPN gateway.

In the majority of cases, traditional VPN implementations establish a simple flat network between authorized users and the corporate computing environment. Once a user has gained access, that access is typically granted for the entire network: The IP addresses of all applications, databases, and other IT resources are discoverable. Authorized users do not encounter any interior perimeters, but can move laterally within the network and see every corporate application and IT resource.

This, of course, facilitates extremely broad access to sensitive resources for users – as well as for hackers who manage to get in. Using brute-force attacks, vulnerability scanners and/or harvested credentials, they can then hack into resources and applications and steal sensitive data from anywhere within the perimeter, without breaking a sweat.

VPNs enable broad access to sensitive resources for users – as well as for hackers who manage to get in

In addition, numerous vulnerabilities have been uncovered in VPNs and VPN services that could give hackers a foothold on client devices, potentially making it even easier for them to breach corporate networks.

Making this worse, VPNs provide no internal monitoring capabilities, meaning that there's no way to tell what users are doing on the network once they are in. Thus, a hacker – or a malicious insider – can operate inside the network with impunity, and without fear of detection.

Zero Trust Network Access (ZTNA)

The Zero Trust model dictates that nothing outside or inside the network perimeter should be granted complete trust

In an effort to reduce the enterprise attack surface as well as IT overhead, and with the encouragement of industry analysts such as Forrester Research and Gartner, many security-minded organizations have begun exploring technology replacements for VPNs that correspond with Zero Trust security principles.

In contrast to the conventional network security model, which focuses on securing the network perimeter against external threats, the Zero Trust model dictates that nothing outside or inside the network perimeter should be granted complete trust. Instead, a Zero Trust network is segmented into numerous small microsegments, each with a carefully guarded micro-perimeter. Every microsegment contains a carefully defined set of resources. Only the particular users and devices that need access to a given microsegment are granted authorization to individual secure zones.

The concept of Zero Trust Network Access (ZTNA) is software-defined perimeter (SDP) technology. SDPs use controllers to authenticate and connect authorized users to specific network resources or applications through a secure gateway, based on identity policies. Any network resources which a given user is not authorized to access are concealed, and thereby protected against unauthorized access. In essence, the SDP is able to create granular user-to-application network segments on the fly, and support continuous tracking of all user activity, even after log in.

Some organizations looking to adopt a Zero Trust Network Access approach may assume it requires full-scale adoption of SDP solutions to, among other things, replace VPNs. But the recent increase in VPN deployments to support new distributed workforces demonstrates that full scale rip-and-replace is not going to occur for many organizations in the foreseeable future. Even without Black Swan events like the pandemic, many organizations tend to hang on to tried and tested legacy tools such as VPN, regardless of the issues associated with securing and maintaining them.

While SDP is one known way to achieve ZTNA, it is certainly not the only way. Ericom Application Isolation is an innovative solution that works with VPNs to enforce Zero Trust Network Access controls, without the wholesale network infrastructure replacement that many SDP solutions entail. Users log in and connect via their standard VPN client or local network as usual -- no extra sign-ins or hoops to jump through, and applications and IT resources get protected with powerful Zero Trust security capabilities.

Let's take a look at some of the key elements of ZTNA and compare how they're achieved via SDP and Ericom Application Isolation solutions.

SDP is one well-known way to achieve ZTNA, but it is certainly not the *only* way

ERICOM
Be Connected, Be Secure

When choosing a ZTNA solution, look for one that…

- Has agentless options to simplify deployment
- Controls access on a per-user, per-resource basis
- Leverages rule-based policies that take time and location into account
- Enables easy creation of granular rule-based policies for individual users

Weighing your ZTNA options

Streamlined connectivity for remote and on-premise users

A key tenet of ZTNA is that access must be easy and secure, regardless of where users are – at the office, at home, or on the road. SDP solutions provide the identical connectivity solution for both remote and on-premises users. They authenticate the individual who is requesting access and, based on policy, connect users to applications and resources only if they are permitted to do so. Some SDP solutions require a separate agent to be deployed on endpoints for users to be able to connect to the SDP software or service.

Ericom Application Isolation ***integrates with existing VPNs and NGFWs*** to secure remote access as well as log ins to local enterprise networks. No additional agents need to be deployed on users' endpoints and there is no required change in user behavior. Like SDP solutions, it provides geolocation, time-of-day and anomalous access blocking controls.

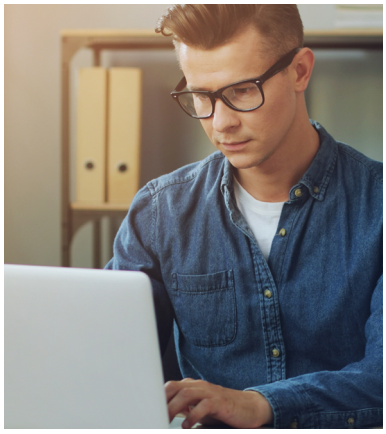
Microsegmentation

With traditional VPN and NAC solutions, the network segments that you set up are the network segments you're typically stuck with – they can't be changed on the fly. SDP, however, rapidly creates custom policy-based networks-of-one for every user, comprising only the resources they're authorized to use.

Ericom Application Isolator likewise leverages granular policies to limit access on a per-user, per-resource basis. How this is done differs between the solutions: SDP builds connections on the fly, while Ericom Application Isolation cloaks all resources that a user is not authorized to access so they cannot be seen or accessed by the user. It prevents attacks by limiting remote and internal application and resource access to only what is required. Cloaking applications from unauthorized users isolates them from attack, significantly improving security.

Flexible security policies

Both SDPs and Ericom Application Isolator leverage rule-based security policies to determine which device and user, at what time or location, should be able to access the network and/or specific resources. For instance, you can create a dynamic rule that will automatically limit access if someone is trying to reach specific applications outside of normal business hours, or from a location other than where a user is typically located.



User-centric policies

Granular, least-privilege access policies are the key to securing enterprise networks and resources from cyberattack. But creating those policies for individual users, and keeping them updated, is such a huge task that least-privilege access remains an elusive goal. For most organizations, more manageable group policies are applied, at the cost of over-privileging many users.

SDP solutions rely on IT personnel to specify policies. This, of course, is prohibitively time consuming (to say nothing of tedious) to do on an individual basis for large enterprises. As a result, most organizations apply group-based policies at best.

Ericom Application Isolator, in contrast, includes a patent-pending Automatic Policy Builder that generates granular, per-user policies based on user activity during an observation period. Policies may be simultaneously created for thousands of users, and IT admins can easily fine-tune policies as needed. As a result, Ericom Application Isolator enables organizations to enact a true Zero Trust default-deny security posture.

North and South, East and West

While much of the discussion regarding Zero Trust Network Access is focused on the security threats associated with remote access (aka "North-South" access), there are also risks associated with overly broad internal access. Security professionals know that one of the key challenges they need to address is the risk of a malicious insider, who can steal data, disrupt systems, and create havoc. Securing this internal network access use case, known as "East-West" access, is something that the majority of SDP solutions do not address.

Ericom Application Isolator addresses both North-South and East-West use cases. Whether the challenge is keeping external hackers away from sensitive corporate applications and data, or it is ensuring that internal access is limited – thereby mitigating the impact of any insider malicious activity – the solution has an organization covered.

"Ericom Application Isolator is a streamlined, cost-effective way to add important zero-trust security controls to existing VPNs and firewalls, protecting organizations from lateral movement attacks that result in ransomware spread, data loss, and significant business disruption."

John Grady, Analyst, Enterprise Strategy Group (ESG)

Many tools or one?

If you wanted to try to replicate the functionality of ZTNA using legacy tools, you'd need multiple VPN licenses, extra networking hardware, NAC, and a lot of spare time for manual configuration. SDP, by contrast, is multifunctional, and it replicates (and improves on) the functionality of both NAC and VPN with a single solution for remote access use cases.

In contrast, Ericom Application Isolator builds on existing VPNs and firewalls to secure access to networks, resources and applications, without requiring wholesale replacement of functioning network infrastructure. It's a simple, low-cost yet highly effective solution that can be up and running in little over an hour, without disruption.

Budget

IT organizations have had a great deal of unplanned spending to enable their remote workers during the COVID-19 pandemic. While it's clearly necessary to improve security for these remote workers, the price of many SDP solutions is daunting. A more effective way to gain ZTNA controls, especially given recent investments in VPN and NGFW infrastructure, is to add capabilities that complement and leverage existing investments. Ericom Application Isolator has a significant cost advantage over most SDP solutions, from both licensing and cost of implementation perspectives.

	SDP	Ericom Application Isolator
Works with existing VPN & network		✓
Large scale infrastructure replacement	✓	
Application isolation for remote access	✓	✓
Application cloaking	✓	✓
Application access auditing	✓	✓
Automated access policy creation		✓
Application isolation for internal access		✓
Geolocation access blocking	✓	✓
Time-of-day access blocking	✓	✓

Adding ZTNA security need not involve wholesale replacement of existing networks or acquisition of costly new technologie

Choose the right security upgrade for your business

If you're relying on VPN alone to provide secure remote access to internal resources, it's definitely time to upgrade to a Zero Trust Network Access solution (ZTNA). The question is, what is the most effective and efficient way to do so?

While many SDP solutions have clear benefits, they also have some downsides, like cost, spinning up a project to replace VPNs, and limited ability to secure internal access use cases. Fortunately, thanks to Ericom's approach with Ericom Application Isolator, implementing ZTNA security does not have to involve a wholesale replacement of existing networks or a significant acquisition of new technologies.

The solution prevents attacks by limiting remote and internal application and resource access to only what is typically required. Cloaking applications from unauthorized users isolates them from attack, eliminating lateral movement within the network and stopping the spread of threats like ransomware. The software's patent-pending Automatic Policy Manager simplifies the process of establishing per-user remote (North-South) and internal (East-West) secure access policies. The software is transparent to users and integrates with the market's leading NGFWs and VPNs.

Ericom Application Isolation: A lightweight solution to implement today

In an era of proliferating endpoints, increased mobility, hyper-interconnectivity and globalization – to say nothing of what seems to be a long-term from-home workforce -- legacy perimeter-centric technologies are no longer effective against sophisticated cyber attacks.

Ericom Application Isolator enables IT to quickly and simply implement a Zero Trust security framework by providing each user or group of users with access only to those specific resources they need to do their jobs effectively. It prevents lateral movement attacks within the network, by hackers as well as by malicious insiders, while simultaneously providing users the instant, vital application access they require to do their jobs.

When designed properly, granular secure application access software can be added to your existing VPN as a simple, cost effective way to introduce ZTNA security to your organization. While Zero Trust Security is indeed a journey, the first step – Zero Trust Network Access – can be just a short drive around the block.

Prevent lateral movement attacks by hackers or malicious insiders, while providing the vital application access users require to do their jobs

Ericom Application Isolator software is the simplest, most cost-effective way to add Zero Trust Network Access security controls to VPNs and corporate networks. It prevents attacks by limiting remote and internal application and resource access to only what is typically required. Cloaking applications from unauthorized users isolates them from attack, significantly improving security.

Download Ericom Application Isolator Standard Edition for free at www.ericom.com/ericom-application-isolator or contact us for more information.

Contact us

www.ericom.com

US: (201)767-2210
Europe: +44 (0)1905 777970
ROW: +972-2-591-1700

ERICOM
Be Connected, Be Secure