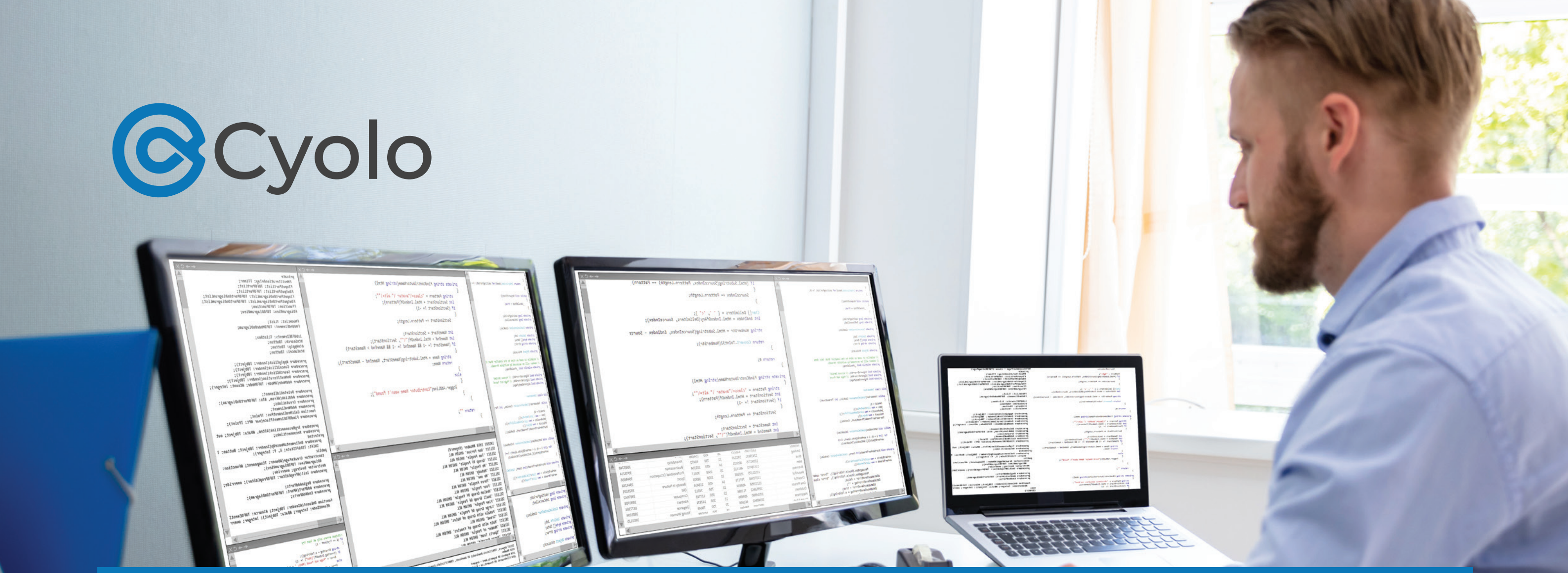
Cyolo



How to Replace Your VPN with a Zero Trust Solution

VPN usage has grown globally due to Covid-19, and many companies are realizing its shortcomings. As employees migrate to working remotely and companies go through digital transformation, companies are experiencing first hand how limiting a VPN is on their business. Instead of agility and effectiveness, businesses and employees have to deal with slow connections, high latency, and a growing number of cyber attacks.

This whitepaper will explain how you can migrate from a slow and insecure corporate VPN to a dynamic and secure Zero Trust solution. We will take you through four easy and actionable steps that can bring you to Zero Trust in a matter of hours, not years. But first, let's dive deeper into the challenges VPNs pose for organizations.

7 Reasons to Replace Your VPN Connection

1. Scalability Difficulties

VPNs were originally built for large companies as a private method for communication and file sharing between offices. This was a very specific need. VPNs were not built to support the entire workforce working and communicating remotely all the time.

Scaling your VPN requires adding bandwidth, adding security measures like encryptions, firewalls and authentication methods, running constant stress tests to ensure stability, and adding users to your license. Some companies find scaling so difficult, they build their own VPN solution to accommodate their needs.

Iranian hackers are selling access to compromised companies on an underground forum. The Iranian hacker group who's been attacking corporate VPNs for months is now trying to monetize some of the hacked systems by selling access to some networks to other hackers. Source: ZDNet]

2. Poor Performance and High Latency

VPNs require routing all traffic through the data center. As a result, requests and responses go through a longer travel time, which increases latency. High server loads and encryptions also poorly affect latency, due to overloading and the encryption process. The subsequent poor performance frustrates employees, stresses IT managers and leads to an overall business slowdown.

3. Security Vulnerabilities

In 2020, hackers realised that the growing number of VPNs could provide them with access to entire networks. The danger was so grave, that NSA issued a special warning and recommended a series of tasks for network administrators to perform on a regular basis. Real attacks soon followed, like the Iranian adversary "Pioneer Kitten" that sold information on the dark web.

VPNs are not secure due to technological vulnerabilities, making them susceptible to network scanning, brute force attacks and zero-day exploitations. In addition and more importantly - VPNs operate according to the old-fashioned castle-and-moat approach. This means that once a perpetrator is in, they have access to the systems, assets and the crown jewels in the entire network or network segment.

4. Resource-intensive

As mentioned before, VPNs were built for a pinpointed use case: occasionally connecting remote offices securely. The expansion of a VPN to constantly support hundreds, thousands or tens of thousands of employees, each at a different location, requires many more resources. More bandwidth, load balancers, encryptions, authentication methods, DMZ configurations, and personnel are just the start. Especially if the company uses "heavy" network components, like databases and design systems.

5. Bulkiness

When you think "business agility" the first thought that comes to mind probably isn't staring at the screen of the VPN client waiting to connect. Setting up new devices for employees, integrating them into the access control system, changing network requirements, adding new applications to VPNs, responding to security emergencies and users connecting to networks - all these processes (and more) are slow, bulky and not agile. This negatively affects the business.

6. Limited Use Cases

Even if you've managed to set up a stable VPN for your entire remote workforce with proper IT support and the security team's sign-off, VPNs are still a challenge. Your daily use cases like connecting partners, 3rd parties and M&As cannot be solved through a VPN. Unless you're prepared to invest a heavy amount of resources and limit the parties you interact with, a different network access solution should be found.

7. Dated Technology

VPNs were invented decades ago, as a technological answer to a very different business world than the one we are working in today. The latency, security, agility, resource and additional issues detailed before are a clear testament to that. Today, businesses require an agile, granular framework that supports intense cloud connections and SaaS for digital businesses.

The Secure Network Access Solution: Zero Trust Connectivity

Zero Trust is a modern approach to answer the security needs of businesses going through digital transformation. Instead of securing the perimeter, Zero Trust secures the entire network, including systems, applications and the crown jewels.

Zero Trust is an identity-based approach. Users are not granted access just because they made it into the network, like a VPN does. Instead an efficient and agile user/device validation occurs before they are given access to systems, assets or applications.

In addition to better security, the ability to scale up and down at the click of a button and ease of use - Zero Trust users report higher levels of satisfaction when compared to using VPNs.

Compared to a VPN, Zero Trust is better equipped for today's business use cases: remote work, multiple partners and vendors, constant global communication, multiple M&As, and more.

VPN vs. Zero Trust Comparison

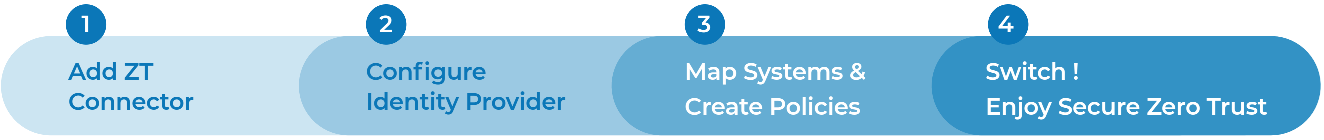
	Zero Trust	VPN
Agility	High	Low
Use Cases	Multiple	Limited
Security	High: identity-based	Low: perimeter-based
New User Set Up	Easy	Difficult
Implementation	Quick and easy	Long and bulky

4 Simple Steps to Replace Your VPN with Zero Trust Architecture

Despite the disadvantages of VPNs on businesses, many organizations are still afraid of the transition from VPNs. CISOs, IT managers and CIOs believe the transition is difficult and resource-intensive. They're anxious the schedules will be long, deadlines will not be met and their organization's network and security will be stuck in limbo.

In fact, replacing a VPN is a very clear and simple process. Today's Zero Trust technology is so advanced, that it can be done in an hour! If you're not feeling secure about switching so quickly, ZT vendors today enable VPNs and Zero Trust to operate side by side, for as long as required.

But before we dive into that, let's see what the replacement process looks like:



1 Add ZT Connector

2 Configure Identity Provider

3 Map Systems & Create Policies

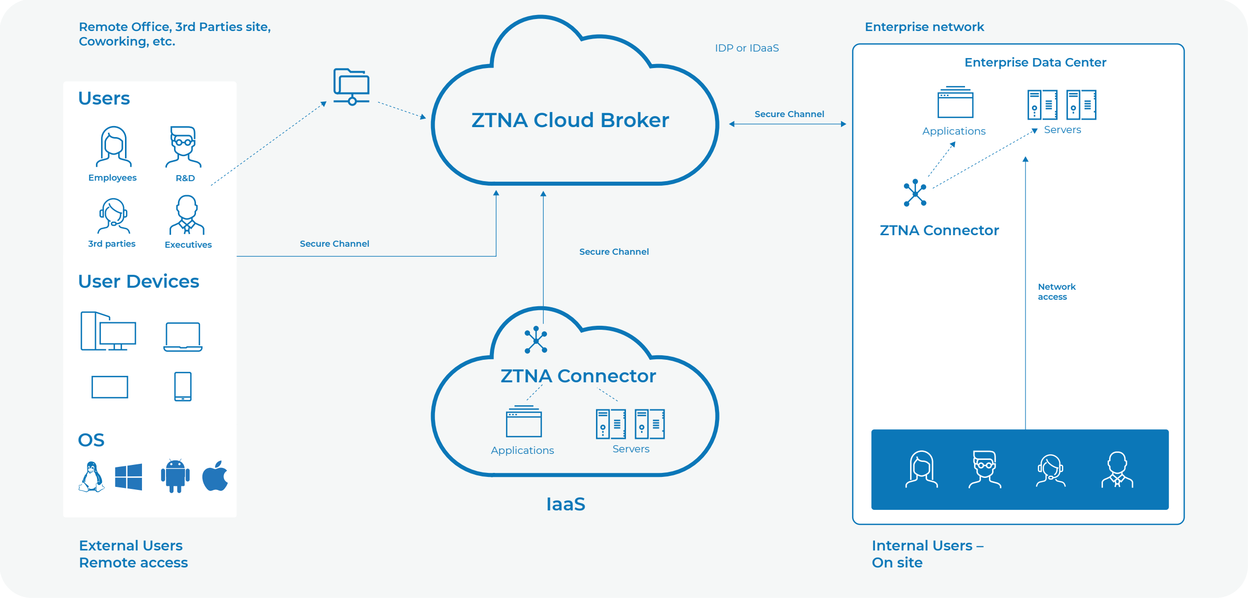
4 Switch ! Enjoy Secure Zero Trust

Now let’s dive into each milestone.

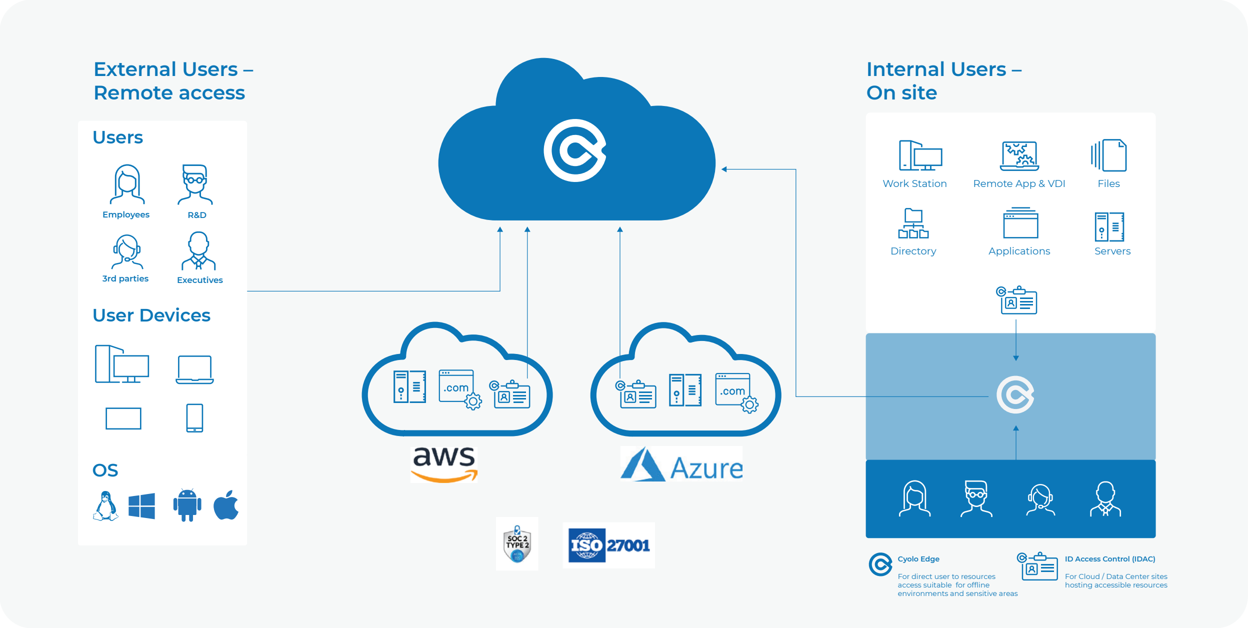
Milestone 1: Add a Zero Trust Connector

The Zero Trust connector will connect to the cloud broker, and is the key component in your zero trust strategy. From this, access and segmentation will be managed, ensuring only authorized IDs have access to your network assets.

When choosing your ZTNA provider, it’s important to choose a provider you can trust. Most providers will terminate TLS sessions and will have access to your sensitive data, such as keys, passwords, tokens, etc.



Cyolo’s Zero Trust solution does not have access to your sensitive data, providing a truly secure zero trust solution and higher performance. Cyolo’s connector also takes only 15 minutes to install.



Milestone 2: Configure Your Identity Provider

Once the connector is added, configure your identity provider and users, import your servers and applications and configure the entities and connections.

Milestone 3: Map Your Systems and Create Policies

Zero Trust is based on your network, not the perimeter. Therefore, it is important to map the connections between identities and applications. These include:

- Systems
- Applications
- Protocols
- Identities
- Privileged users
- Mission critical assets
- 3rd parties
- Unique networks like OT
- And more

Today, many IT managers and security teams do not have a single source of truth for managing and maintaining their networks internally. The purpose of this step is to gain visibility into the network's behavior and requirements, for defining the Zero Trust policies. In addition, the mapping step is also an opportunity to consolidate the organizational knowledge in one place to provide network visibility.

Once the connections inside the network are mapped out and clear, it's time to build the policies. Policies will determine which devices and users can access which systems and applications. This is the core of Zero Trust - providing identity-based secure access. If you already have the network mapping, you can skip straight to policy creation.

Cyolo's modules can automatically map and create automated policies based on the network and existing requirements. Then, users can easily request access to additional applications and systems through Cyolo, and network administrators can approve or reject, at the click of a button. You can also execute these steps manually.

The length of the mapping and policy creation changes from company to company. In very large organizations automatically learning the systems and creating policies should not take longer than 30 days and can even take a week. During this time, network admins can manually grant access and create their own policies.

Milestone 4: Switch (OR - Run Side by Side)

If you've come this far in the process, you de facto have Zero Trust running in your network. So all you have to do is turn off your VPN.

However, you can always run Zero Trust side by side with your VPN, until you have confidence in the solution or for supporting certain systems some ZT providers don't support, like OT. Cyolo does support these systems.

Pro tip

Gradually migrate your systems and applications from the corporate VPN to the Zero Trust architecture. Each system migrated will reduce the attack surface of your network. Therefore, even if you're not comfortable yet with a complete transition, a partial transition is still far more secure than VPN only.

About Cyolo

Cyolo is the leading zero trust security provider for organizations that require third party access. By securely connecting all users from anywhere without requiring a VPN, Cyolo enables employees to focus on their work and your business to grow. Cyolo provides advanced user management features, real-time recording abilities and an easy to use UI. Cyolo can also integrate with your VPNs, if needed.

Cyolo takes minutes to implement and is compatible with any network topology and identity infrastructure. In addition, Cyolo does not have access to the organizational data. Not only does this ensure true privacy and security, it also improves performance as a better user experience.

Request a demo to learn more: cyolo.io/demo-request.