The Complete 3-Step Guide to Implementing Zero Trust ~~Network~~ Access

Cyolo

What is Zero Trust Anyway?

Once derided as merely a buzzword, zero trust has emerged in recent years as a very real cybersecurity framework and a more secure alternative to the traditional castle-and-moat security approach. But despite widespread acceptance of zero trust as a concept, there remains confusion about what exactly it entails and, to an even greater extent, how zero-trust security can be implemented.

The zero-trust framework is founded on the premise, "Never trust, always verify." This eliminates the transitive trust that characterizes perimeter security and, in its place, requires that all users and devices be authorized and then continuously authenticated before any access is granted.

The purpose of zero trust is to reduce the surface area for potential cyberattacks by:

1) Fully validating and continuously authenticating users, rather than blindly trusting attributes like originating network or domain membership.

2) Providing those users access only to the resources they need and not to the full network.

3) Keeping a robust audit trail of activity while the user is connected.

Starting a Successful Zero-Trust Initiative

The prospect of migrating to an entirely new security framework may be daunting, but this is true of most big and highly worthwhile projects.

The good news is that the journey to zero-trust access can be streamlined by breaking it down into three smaller and more manageable transitions based on user groups.

- Step 1: Secure access for high-risk users
- Step 2: Secure access for remote users
- Step 3: Secure access for hybrid and on-premises users

Dividing your zero-trust initiative into these 3 distinct stages not only makes it less intimidating, but it will also yield meaningful results at a faster rate.

STEP 1

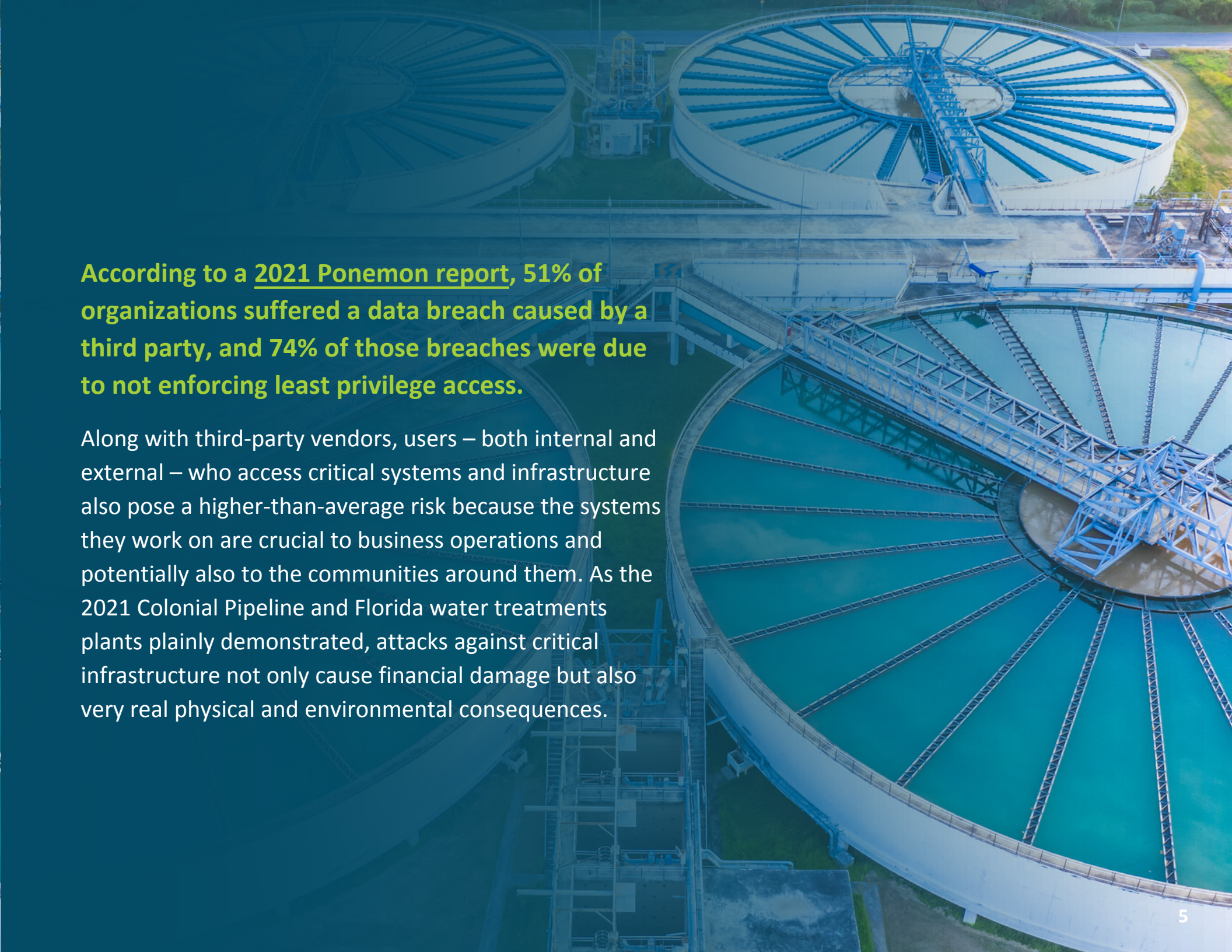
Secure High-Risk Access

Why Secure High-Risk Users First?

Third-party vendors and workers who access critical systems likely form a small subset of an organization's overall user base; however, they generally pose the greatest security risk. In our definition, the greatest risk is when user access could cause enormous damage to the business.

Each organization is unique and will need to conduct its own assessment of which types of users pose the highest risk. But, broadly speaking, a third-party maintenance technician who works remotely on business-critical applications is riskier to grant access to than a marketing manager who logs in on a company-managed laptop.

Nearly every company these days hires third-party vendors and contractors to perform tasks that are too costly or complicated to handle in-house. While bringing in third-party users and services can accelerate an organization's progress, these outsiders can also significantly increase the risk of a cyberattack or breach. This is because, when proper security measures are not in place, the hiring organization absorbs the attack surface of the third-party vendor.



According to a 2021 Ponemon report, 51% of organizations suffered a data breach caused by a third party, and 74% of those breaches were due to not enforcing least privilege access.

Along with third-party vendors, users – both internal and external – who access critical systems and infrastructure also pose a higher-than-average risk because the systems they work on are crucial to business operations and potentially also to the communities around them. As the 2021 Colonial Pipeline and Florida water treatments plants plainly demonstrated, attacks against critical infrastructure not only cause financial damage but also very real physical and environmental consequences.

The Problem with Current High-Risk Access Practices

Even if an organization's security controls are top-notch, bad hygiene on the vendor's side can compromise its security posture and ultimately lead to a security incident, as in the case of the Okta breach made public in March 2022. This creates a conundrum: hiring third-party vendors is unavoidable for most organizations, but controlling their security practices is nearly impossible.

The logistics of forcing a third party to comply with specific security controls and processes are simply unmanageable. In most cases, organizations cannot require vendors or contractors to install specific security agents onto their devices instead of using the security measures they already have in place.

Some companies seek to solve this scenario by sending managed corporate devices out to third-party users, but this is a costly and complicated solution. Many others depend on virtual private networks (VPNs), but VPNs were built for individual use and can hardly meet the needs of an enterprise-sized organization. VPNs are also vulnerable to security threats because they generally provide authenticated users with full network access.

Keep in mind it's hard enough to get employees to follow their organization's security protocols, so how can that same organization secure third-party users without forcing them to download apps, adopt specific behaviors, or use certified devices?

How Zero-Trust Access Secures High-Risk Users

The solution to these problems is to implement a zero-trust access solution that can easily be implemented for third parties and other high-risk users, such as those who regularly access critical infrastructure or have joined the organization via an M&A.

Zero-trust access is the best way to enable secure connections for high-risk users, because, by definition, it requires full user validation and enforces least privilege access regardless of where users come from, or what device they connect with. Third-party users on their own private devices are required to verify their identity in just the same way as internal employees connecting via company-owned devices.

Still, it is important to recognize that many zero-trust access providers require their applications to be downloaded on every device, which is problematic for third-party users. Finding an agentless zero-trust access platform is, therefore, ideal when dealing with third parties.

Ensuring the ability of high-risk users to access applications securely gives an organization the biggest security boost with the smallest number of users secured. In addition, migrating high-risk users from VPNs and other traditional remote access solutions will dramatically reduce an organization’s attack surface and, as a bonus, its system's complexity. This is precisely why a zero-trust initiative should begin by focusing on high-risk users.

STEP 2

Secure Remote Access

Once the highest-risk users are connecting to all work resources via zero-trust access, step two is to secure employees who work remotely. With remote and hybrid arrangements now a permanent part of the work landscape, ensuring remote users can securely access corporate systems and applications is a critical stage in the journey to zero trust.

Remote employees present a greater security risk than others in the same role at the office because they are working in an environment that is outside of the control of the business and its IT team. And these days, “work from home” doesn’t even necessarily mean work from home. Users are now just as likely to log in from coffee shops, hotels, and other locations that may not even have password-protected Wi-Fi. Beyond the potential vulnerability of public (or improperly secured home) Wi-Fi networks, it is significantly more difficult to verify user identities, tailor access permissions, enforce best practices, and avoid the complications of shadow IT when employees are outside the office.

The Problem with Current Remote Access Practices

VPNs have been used for decades to tunnel remote workers into corporate networks. When the vast majority of workers came to the office daily, access was granted on the basis of whether a request originated from the company network – and VPNs behave in the same way. If a user has the right credentials or certificates, a VPN will trust that they belong on the corporate network and grant wide lateral access. VPNs don't assess the means through which the user arrived at the network, and whether those means are suspicious or risky. They also do not perform continuous authorization and cannot support advanced features like supervised access or session recording.

VPNs were an important access tool for workers on business trips or otherwise away from the office, but they were not built to support entire organizations. When used in this manner, it creates a slew of problems:

- VPNs are centered on sites and networks rather than applications or users.
- VPNs give broad access to applications, users, and other networks connected to the VPN. If a bad actor gains access to the VPN, they can essentially access everything.
- VPN performance issues can be detrimental to productivity and cause significant user frustration, not to mention the cost of bandwidth and licensing needed to terminate all the connections.

Many current VPN installations are a workaround born out of necessity in the early days of remote work. For the complications that come with VPN usage like firewalls, VPN agents, licenses, and credentials, the risk coverage they provide isn't sufficient for modern businesses. To put it most simply, VPNs present a highly insecure single point of failure.

How Zero-Trust Access Secures Remote Users

Instead of delivering users to a network, zero-trust access platforms deliver them directly to the individual application(s) they use in their work. This limits users' ability to wander around the network and potentially cause harm, or to inadvertently allow a bad actor to follow them in. Zero-trust access is the ideal way to enable remote users to connect to the resources they need seamlessly and securely. The best solutions offer a single-click experience that bakes security into the workflow, allowing users to continue their existing routines and discouraging the adoption of shadow IT.

Despite the clear advantages of zero-trust access, the core of many companies' existing remote access strategy still includes VPNs. The thought of replacing this long-used technology may be a non-starter. Whether it's due to the perceived complexity of the process, budgetary concerns, or simple avoidance of change, security and IT leaders may bristle at the idea of taking on an admittedly large project like VPN replacement.

In light of these reasonable hesitations, zero-trust network access (ZTNA) vendors should help organizations make the transition from their VPN without forcing them to immediately rip-and-replace large swaths of infrastructure.

The alternative is to augment existing VPN deployments by seamlessly integrating zero-trust access into remote workflows. This addition will add important security capabilities like continuous authentication, direct asset access, and session monitoring and recording.

A gradual transition from VPN to zero-trust access, potentially even including a period when the two run side by side, will reduce pressure and allow stakeholders to see the benefits of zero-trust access before turning the VPN off once and for all.

STEP 3

Secure Hybrid & On-Premises Access

Once an organization reaches this third and final stage of its zero-trust journey, the biggest challenges and hurdles have already been overcome. With high-risk and remote users connecting securely to corporate resources, the time has arrived to extend zero-trust access to all remaining users.

Even when returning to office, large numbers of workers prefer a hybrid work arrangement, where they split their time between remote and on-premises worksites.

Where people work is ultimately decided by the employer, but the employee preferences are clear:

- **32% prefer exclusively remote work**
- **59% prefer a hybrid work arrangement**
- **9% prefer exclusively on-site work**

The Problem with Current On-Premises Access Practices

Many organizations maintain the belief that on-premises users are inherently secure. After all, they are literally sitting at their desks inside the office; what is the harm in giving them full network access? Unfortunately, in the world of advanced cyber threats, even traditional office workers are a tempting target for nefarious actors.

On-premises users are generally only verified once, based on their connection to the corporate network with their approved device. This validation practice presents the same problem as a remote worker connecting through a VPN: once the user is inside the network, they have broad access that is difficult to control or monitor for unusual activity.

Authentication based purely on network connection provides a wide avenue for bad actors to wreak havoc inside an organization's network. It only takes one click on a malicious email to provide valid user credentials to an attacker. If an employee device with unfettered network access is compromised, the potential for damage is nearly unlimited. We also can't ignore the risk of insider threats, which is much greater when full network access is on the table. An over-permissioned on-premises user may have rights to grant themselves even more access and power.

How Zero-Trust Access Secures Hybrid & On-Premises Work

Zero-trust access solutions let employers set boundaries around employee access, including time of day, location, or method of access. This empowers the platform to assess whether or not the user is displaying anomalous behavior (and potentially cut off their access privileges if they are), and it enables the organization to adhere to the principle of least privilege access no matter if the employee is working from the office or remotely.

Still, it must be acknowledged that not all solutions make access seamless and agile in all scenarios. For on-site users, return-to-office users, and on-premise services or applications, most zero-trust access solutions require the access path to route through the cloud and then back to the site (also called tromboning), which adds latency to the workflow.

An ideal zero-trust access solution removes this latency by sitting on-premise to handle the routing of onsite requests to give those users the same speed and access as someone who is remotely connected.

Zero Trust is a Journey, Not a Destination

Ensuring secure zero-trust access for on-premises workers marks the culmination of the 3-step zero-trust journey. Once this phase is complete, organizations will have the controls they need to securely enable their business, especially the parts where user access could cause enormous damage to the business.

But it's important to keep in mind that sometimes cliches are true, and zero-trust is ultimately a journey rather than a destination. Policies and workflows can always be updated and optimized. In particular, organizations should build processes for adding and removing users and applications as they come and go over time. Developing and enforcing these processes will help maintain the zero-trust framework and keep high-risk, remote, and hybrid access secure for the long term.

The Cyolo Difference
for Zero-Trust Access

At the end of the day, many instances of high-risk access exist within most organizations. These are users who need to connect to internal systems to perform critical business functions, and yet giving them this access opens the company to heightened risk. The problem has been a lack of control, which can leave security teams feeling powerless to lower the risk of enormous damage to their organization. Cyolo exists to return control to its customers, empowering them to enforce the level of control needed to securely enable their business.

With the realities of modern work always in mind, Cyolo designed a zero-trust ~~network~~ access solution to solve today's toughest access-related challenges.

Trustless Architecture Enables Real Zero Trust

To deliver a true zero-trust access solution, the provider must also abide by zero-trust principles. This means customers should not be required to give implicit trust to their ZTNA vendor. At Cyolo, customer data remains with the customer at all times, and no traffic is ever decrypted outside of the customer's secure boundary. Cyolo never has visibility to private encryption keys or other sensitive data and therefore does not risk the exposure of private customer information in the case of a breach.

Application Access, Not Network Access

Cyolo enables organizations to deliver users directly to the resources they need, without ever providing visibility to the full network. This is true for all types of users, wherever they are located and whether they are internal employees or external contractors. The principle of least privilege is enforced by default, and administrators can easily tailor permissions to include only the necessary applications. This is why we call our solution Zero-Trust ~~Network~~ Access.

The Cyolo Identity Access Controller (IDAC) is an application connector that brings users straight to the applications they need. The Cyolo IDAC supports any application protocol and can be implemented on-premises or in a cloud provider, like AWS or Google. The Cyolo platform can be deployed anywhere, even without internet connection, enabling secure access in OT as well as IT environments.

Agentless

Unlike other ZTNA offerings, Cyolo takes an agentless-first approach. This means the Cyolo platform can be easily accessed in the user's web browser using on-premise, native, or cloud clients. There is no need to download an application in order to achieve security with Cyolo. This feature is particularly valuable when it comes to securing third-party users who may be unwilling or unable to download an agent.

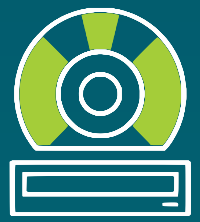
Supervised Access and Controls

The Cyolo platform includes oversight controls that can be applied to specific critical applications and high-risk users. These capabilities include real-time monitoring and live session recording, which is essential for auditing purposes and many compliance mandates.

Cyolo also supports supervised access, which requires users to explicitly request access from an administrator before connecting to sensitive systems or applications. Once approval is granted, the admin can monitor and interact with that user's session and terminate it immediately if unusual activity is suspected.

Supports Transition Away from a VPN

In recognition of the fact that some security and IT leaders may be overwhelmed by the prospect of VPN replacement, Cyolo allows organizations to augment the security features of their existing VPN deployment by layering zero-trust access on top. Once the benefits of zero-trust access become clear, the migration away from VPN access can be completed at the customer's own pace. Since Cyolo does not require change management, it is quick and easy to stand up this additional layer of security. During the VPN-augmentation period, the Cyolo platform will enable not just multi-factor authentication (MFA) of previously unsupported systems but also continuous authorization of all users.



Retrofits On-Premise and Legacy Applications to Support Modern Identity Infrastructure

Cyolo has the unique ability to modernize the identity infrastructure of on-premises, legacy, and homegrown applications without massive costs or disruption to business operations. Cyolo creates a single point of access and identity validation that extends to legacy tech stacks and architecture, modern cloud environments, and homegrown on-prem applications. This single point of access creates a seamless and agile experience for both internal (remote, hybrid, or on-premises) and external users.

Checklist for Implementing Zero-Trust Access

Step 1: Secure High-Risk Access

1a: Identify third-party users, including vendors and contractors

1b: Identify users of critical systems and infrastructure

1c: Move third-party and critical systems users to agentless zero-trust access

Step 2: Secure Remote Access

2a: Identify remote users on the organization's VPN

2b: Run agentless zero-trust access alongside legacy VPN (optional)

2c: Move remote users to agentless zero-trust access

Step 3: Secure Hybrid and On-Premises Access

3a: Identify remaining hybrid and on-premises users

3b: Move hybrid and on-premises users to agentless zero-trust access

3c: Retire legacy VPN

cyolo.io