Cyolo

SECURING THIRD-PARTY ACCESS: A STRATEGIC BUYER'S GUIDE

After multiple years of headline-grabbing breaches caused by the actions of third-party vendors and contractors, the enterprise world has lifted the rock off implicit third-party trust and found underneath an entire ecosystem of vulnerabilities and unknowns.

Many of these breaches weren't enabled by what would be called privileged users.

- In 2013, **Target was famously hacked** through its third-party HVAC vendor.
- In 2022, **Okta was compromised** by a third-party customer support engineer using the systems of a company the vendor had recently acquired.
- Also in 2022, **Toyota revealed a years-long exposure** of customer information and real-time vehicle location data after a third-party developer accidentally uploaded source code to a public GitHub repository.

In light of these and many additional incidents, **it is time for organizations to accept that all third-party partners, vendors, suppliers, and contractors accessing corporate systems and resources should be treated as "high-risk," no matter how innocuous their work may be.** After all, even well-intentioned third-party users are not invested in an organization and its security the same way that employees are. Similarly, their own security hygiene–over which the hiring organization has little to no control–may not meet the corporate standard and can easily lead to serious consequences. And even if a breach is entirely the fault of a vendor, the organization still bears all the damages (financial, reputational, etc.) from the incident.

But securing third parties is easier said than done.

THIRD PARTIES OFTEN REQUEST OR REQUIRE MORE ACCESS THAN THEY NEED.

Organizations typically grant wide lateral access and administator-level privileges so that vendors can work efficiently and minimize their billable hours. However, vendors are not deeply invested in the organization's security posture and their actions within the network can have far-reaching consequences.

NO CONTROL OVER THIRD-PARTY DEVICES.

Vendors cannot be forced to download or adopt the company's own agented security tools on their personal devices. But at the same time, it is impractical, costly, and slow to ship all vendors a managed device.

DIFFICULT TO MANAGE.

Once third-party users are in the system, organizations often lack processes for managing their connections and activity. This holds true both during the course of the vendor relationship and when it comes to off-boarding once the relationship ends.

CASCADING RISK IS REAL.

Third parties work with their own third parties. When organization onboards a new third-party connection, it is also connecting to all of their vendors, their vendors' vendors, and so on.

MAKING THE SHIFT TO ZERO TRUST

The **zero-trust security framework** provides a ready-made methodology for mitigating third-party risk. Rather than attempting to extend controls outward to devices, users, and systems that are ultimately uncontrollable, zero trust hardens protection around the assets and users that matter most.

Still, it is vital to recognize that zero trust is not a tool in and of itself. It is a framework that can be implemented through people, processes, and technology. Understanding the underlying principles of zero trust is vital to proper tooling, strategy, and adoption.

The ground rules of zero trust

- Trust is based on user or device identity, and authentication is performed by verifying identity-based credentials rather than network-based credentials.
- Zero trust assumes the network perimeter has already been breached and treats all users accordingly by continuously validating them even after they have been granted initial access.
- Zero trust protects applications, assets, and resources rather than the network.

Given a growing recognition of the value the zero-trust model brings, the market for zero-trust access tools has become quite noisy. In fact, many software providers have merely slapped a “zero trust” label on their existing solutions in order to take advantage of increased demand.

This guide is designed to help cut through the noise and help organizations understand how to find a partner who can accelerate a true zero-trust implementation that encompasses the full spectrum of users, use cases, and assets.

TAKE STOCK OF THE ENVIRONMENT

Before turning to the market to search for zero-trust access tools, assess the current environment to identify any specific needs and gaps in the existing security stack.

INVENTORY AND SCORE EXISTING THIRD-PARTY RELATIONSHIPS

Compile a list of all third-party vendors with access to the network, and categorize them based on risk, e.g. low, medium, and high. How are these connections currently secured? From this assessment, draft a third-party access policy that defines risk levels and how each should be mitigated. This policy can mandate procedures for onboarding, reviewing, and revoking access for future vendors.

ASSETS, SYSTEMS, AND USERS

Compile an inventory of the assets, systems, users, devices, and applications currently connecting to corporate systems. Pay special attention to the most sensitive assets, as well as applications that are typically hard to secure or modernize — like legacy, custom-built, and offline apps.

USER ROLES AND PRIVILEGES

Work to understand in-house and third-party users’ workflows so permissions can be tailored to enforce least privilege access without impeding productivity. Make note of current authentication methods, access control lists, role-based permission sets, and other existing access controls. Once implemented, the zero-trust access solution will help cover gaps in these controls.

THREAT DETECTION

Perform a threat assessment to gain a better picture of the internal and external threats facing the organization and how they could affect the IT (and, if relevant, OT) environment. Identify any current shortcomings in proactively detecting and mitigating these threats.

SECURITY CONTROLS

Examine the security measures already in place and gauge their effectiveness at preventing threats, including existing discovery capabilities.

NETWORK SEGMENTATION

Map the current network topology, assess the firewall rules securing traffic between those segments, and check the access control lists to gauge the security of each segment.

After examining their environment and outlining existing controls and processes, organizations should have a to-do list of problems the zero-trust access solution should be expected to help solve. This preparatory work primes the environment for an effective deployment and implementation of zero-trust access.

PRINCIPLES TO SEARCH BY

Every organization is different and will require a unique tool stack to successfully execute a zero-trust initiative. However, understanding a few guiding principles can help separate the tools that offer the most value from those that will only complicate existing systems without providing adequate coverage or benefit.

NEVER TRUST, ALWAYS VERIFY

"Never trust, always verify" stands as the core principle of the zero-trust model. Zero trust assumes that every user or device is a potential threat and secures them through a two-pronged approach:

- **Every user is authenticated before gaining access to applications or systems.**
- **Even after a user or device is granted initial access, a continuous authorization process verifies their legitimacy and monitors them for suspicious or anomalous activity.**

If a solution only performs an initial authentication and does not continuously validate users, it is not following the principles of zero trust.

Note: None of this is to say that network access controls are useless. Network access controls can certainly help with the passive inventory and management of internet of things (IoT) devices and other endpoints. When combined with role-based access controls, network access controls and segmentation can grant more flexibility in adjusting device access.

IDENTITY IS THE NEW PERIMETER

Tools commonly used to control third-party access — such as virtual private networks (VPNs) and firewalls — were designed to secure the network perimeter. But in today's world of remote connections and distributed clouds, that perimeter is effectively irrelevant.

Practically all perimeter-focused security solutions can be easily bypassed by an attacker with stolen credentials. According to Black Kite, unauthorized network access was the most common cause of third-party attacks, accounting for 40% of third-party breaches.

People – or more specifically, identities – are the new perimeter. Zero trust relies on modern, strong authentication methods to validate users based on something they know (e.g., a password), something they have (e.g., a device), and something they are (e.g., a fingerprint).

SIMPLICITY IS JUST AS IMPORTANT AS CAPABILITY

The zero-trust approach is not only used to secure access for third-party vendors and partners. When zero-trust acccess in deployed fully, no user is inherently trusted and every access attempt is subject to the same level of scrutiny, regardless of the user's relationship to the organization. This both hardens and simplifies an organization's security approach.

Likewise, the tools selected to enable zero-trust access must be simple and non-disruptive. Poor security habits like account sharing, weak passwords, and shadow IT arise when security controls become a hindrance to productivity. If the access solution adds steps or complexity to users' workflows, they will likely take even more shortcuts.

When it comes to third parties specifically, simpler tools enable vendors and partners to ramp up faster and start returning value to the business more quickly.

VISIBILITY AND AUDITABILITY

Even if you add a vendor to your own identity provider (IdP), it is difficult to continue monitoring their activity once they are inside the network. Without this visibility, it is impossible to detect unusual or suspicious behavior.

A zero-trust access tool should provide more control over third-party connections and activities. It should consider contextual awareness when granting access, enable greater granular control, and automatically log activity to improve analysis, simplify audits, and meet compliance regulations.

CORE CAPABILITIES

"So what does a zero-trust access solution *do*?"

This is a worthy question. While every organization has its own set of unique needs and use cases, a few core capabilities will be vital to ensuring success. Any zero-trust access solution without these features is practically a non-starter.

AGENTLESS OR AGENT-BASED

An agent is any piece of software that must be installed on the user's device. Common examples include anti-virus software and VPNs. Requiring a third-party vendor to install an agent is a complicated task, as they likely work with dozens (if not hundreds) of clients and can hardly be expected to juggle tools and policies across all of them.

Ideally, your zero-trust access solution should not need an agent for at least the majority of its functionality. But if it does, be sure to weigh the benefits of the solution with the complexities of ensuring the agent can be installed and managed.

SUPPORTING FEATURES

- Browser based connectivity
- Ability to validate device health prior to access approval
- Web-portal user interface

QUESTIONS TO ASK

- Which use cases require an agent?
- How lightweight is the agent? Does it consume a lot of resources on the machine?
- Can the end user install and upgrade the agent themselves?
- How much does the agent degrade the user experience?
- Is an agent required to broker access? If so, does it decrypt credentials?

FAST ONBOARDING

The whole point of working with third parties is to increase productivity. Ramping them up quickly is key to optimizing ROI on the relationship. But adding these users to your identity provider or Active Directory adds complexity without securing or validating user identities. Often, the default approach is to add a new vendor as a generic user account and give all users working for that vendor access via that single account. While it may save time, this approach clearly does not follow secuity best practices.

A zero-trust access solution should improve security without interfering with existing systems or workflows. Set-up and configuration should take no more than a few hours, and the tool should be deployable in a way that suits the customer's unique environment — on-premises, on-cloud, or in a hybrid model. Once the zero-trust access solution is implemented, it should be easy to provide secure and controlled access for every third party.

SUPPORTING FEATURES

- The access broker is placed onsite, which preserves users' existing workflows
- The solution can be implemented in under an hour, and access policies can be set up in seconds with no disruption
- The solution can be deployed on-premises, on-cloud, or in a hybrid arrangement

QUESTIONS TO ASK

- How long will it take to install the solution?
- Will the deployment/installation process disrupt operatons?
- Does the solution function in all environments/deployment scenarios?
- Can the solution integrate with my existing identity providers?
- Who is responsible for installing and upgrading the solution?

GLOBAL POINTS OF PRESENCE

In today’s global economy, people are connecting to corporate environments from everywhere. This is especially true for third parties, who provide their much needed business services from all over the globe. Any solution used to secure third-party access must account for the highly distributed way companies currently work.

Because speed is a critical factor, a zero-trust access solution should have enough Points of Presence (POPs) to make global connectivity a reality. Having a distributed connectivity network also enables faster loading of both cloud and on-premise resources for all users. Speed becomes even more important when third parties are billing by the hour.

SUPPORTING FEATURES

- Distributed global points of presence
- Low-latency connections
- Fully encrypted transport layer

QUESTIONS TO ASK

- What is the round trip time for connection requests?
- How is encryption handled end-to-end?
- Are any global regions not supported?

APPLICATION-SPECIFIC ACCESS

Granting lateral network access is always risky, whether it is given to third-party users or direct employees. If their credentials are stolen or otherwise compromised — especially the over-permissioned profiles typically given to third parties — an attacker can easily move into other parts of the network and ultimately cause serious damage.

To avoid such a scenario, a zero-trust access solution should deliver users directly to the assets they need to work while cloaking the network and assets they do not need. This way, even if a user's credentials are compromised, the attacker's access is contained.

SUPPORTING FEATURES

- Policy-based multi-factor authentication (MFA) and single sign-on (SSO)
- Integration with existing identity providers (IDPs)
- Native IdP to keep third party identities out of sensitive corporate resources

QUESTIONS TO ASK

- Does the solution provide application-level access or wider network access?
- How does the solution enforce third-party entitlements?
- What type of granular controls does the solution use?
- Can the solution enforce MFA for every application, including legacy and custom-built apps that do not natively support MFA?

LOGGING AND REPORTING

For businesses with regulatory oversight (and that is most businesses these days), logging and reporting are non-negotiable. However, documentation (and compliance) should not be viewed as an end in itself, though it is still often seen this way by business leaders. Rather, logging and reporting should be used as an opportunity to tangibly harden the organization's security posture.

Still, compliance regulations are coming for every industry. Around the world and across industries, new regulations are emerging around the logging and reporting of cybersecurity incidents. Some countries (like India) require companies to report security incidents within just a few hours, while others (like the U.S.) require a report within a few days. International companies face the challenge of juggling various and sometimes conflicting reporting standards.

While they may cause frustration on the ground, compliance regulations lay the groundwork for better collaboration and information-sharing between public, private, and government sectors, which will inform a more robust set of security standards and practices for all.

More simply put, logging and reporting are becoming table stakes in the cybersecurity conversation. The longtime practice of handing third-party vendors the keys and trusting them to work unsupervised is no longer tenable. In order to meet existing or emerging standards, any zero-trust access should automate the logging and reporting of access and behavior.

SUPPORTING FEATURES

- Record complete details of each access
- Provide full analytics onusers who login with generic accounts or passwords
- Log exporting and easy integration with other security tools

QUESTIONS TO ASK

- What kind of data is logged for users with generic username and passwords?
- Are there any access attempts or decisions that are not logged?
- How easy is it to export or share the logs with other tools?

SUPERVISORY APPROVAL

For the most sensitive use cases, such as access to regulated information or process control networks, supervisory approval provides an administrator with real-time control over third-party access. This additional step in the access workflow ensures that any third-party access to critical data and systems is expected, approved, and monitored. With this feature, a third-party user must request access each time they need to a particular resource or system. The administrator then grants access and monitors the user’s behavior in real-time and can revoke access at any point.

Additional security is extended by an option to record the entire session while the third party is connected. When session recording is enabled, a full audio/visual recording of the user's activity is captured and stored for analysis and inspection as needed.

SUPPORTING FEATURES

- Ease of use to request access
- Streamlined process to grant access approval
- Ability for administrator to terminate access at any time, for any reason
- Real-time session recording

QUESTIONS TO ASK

- What steps are required for users to request access?
- How involved does a supervisor need to be while the third party has access
- Can session recording be turned on, if needed?

AGILITY AND SCALABILITY

The ripple effects of the digital transformation era are not going away. Business processes will continue to be digitalized and optimized, new use cases will emerge, and fresh innovations will further complicate enterprise systems landscapes.

In the past, complexity equaled capability. But today, scalability is king. It does no good to enable some new capability if it slows down the user's workflow, impedes the system's performance, or obscures visibility. The problematic application of VPNs serves as a perfect example.

Truly scalable and agile zero-trust access solutions are lightweight, user-friendly, and can be tailored to protect what matters most to the business.

SUPPORTING FEATURES

- No change management needed to install
- Lightweight software can be installed in any form factor
- Solution can be up and running in less than a day

QUESTIONS TO ASK

- What are the technical requirements needed to install the software?
- Is a VPN still required to connect to the tool?
- How long will it take to install?
- What changes to the network or system are required?

RED FLAGS

The criteria for choosing the right zero-trust access solution will vary from organization to organization, depending on each one's unique spectrum of needs, goals, and use cases. However, the marketing haze around zero trust can make it more difficult to conduct meaningful product evaluations. It does not help that many vendors simply stick a zero-trust label on tools they have been selling for years or even decades.

As security leaders search for an ideal zero-trust access solution, they should keep an eye out for the following red flags.

THE SOLUTION IS FOCUSED ON SECURING THE NETWORK PERIMETER.

Traditional security and access tools, including VPNs, firewalls, and intrusion prevention systems, were built to defend the network perimeter. These products worked well enough in the early days of the internet, but the onset of remote work, cloud computing, vendor dependence, and other developments have rendered the traditional castle-and-moat security strategy inadequate.

Zero-trust access solutions are designed to guard assets and resources rather than the network perimeter. Remember, the zero-trust methodology assumes the network has already been compromised. For this reason, zero trust does not focus on security at the network level.

THE ZERO-TRUST VENDOR REQUIRES YOU TO TRUST THEM.

Many vendors claiming to provide zero-trust access actually require you to trust them. Often, these vendors decrypt traffic in their own cloud and have access to customer passwords, tokens, etc. This is not zero trust; it is "Don't trust anyone except us."

"Vendor trust" violates the principles of zero trust and positions the vendor as a single point of failure that, if breached, could spell disaster for all of its customers. A provider offering true zero-trust access will understand that "Trust no one" includes the vendor itself.

THE VENDOR OR SOLUTION CANNOT EXTEND CONTROLS TO EVERY DEVICE, USER, AND APPLICATION.

Zero trust means zero exceptions. This includes third-party vendors, remote users, and legacy applications. Often, teams must adopt multiple tools to cover all gaps and use cases, which creates unnecessary redundancy and complexity that incurs extra costs and takes up more of the team's bandwidth to maintain.

Almost every company, including the most modern and "cloud-first," depends on at least one legacy application that is problematic to secure or modernize. However, securing 85% or even 95% of your systems is not enough to reliably guard against sophisticated cyber threats. Be skeptical of any vendor who asks you to modernize or replace a given system before they are able to secure it.

THE SOLUTION DOESN’T IMPROVE THE USER EXPERIENCE.

Despite all of our technological sophistication, humans remain the single biggest security vulnerability. This is not an insult, it is simply a fact. After all, the most hardened security postures can be compromised by poor password practices, account sharing, shadow IT, or plain old human error.

Security and IT teams must understand that bad user hygiene results from a conflict between security and productivity. A solution that adds extra steps or complexity to business users' routines will only encourage them to subvert the controls and undermine the tool’s effectiveness.

A zero-trust access solution should take security out of users' hands as much as possible by consolidating iIdPs and enabling modern access controls like MFA. The greatest security tool in the world will have no chance of success if it disrupts user workflows so much that they bypass it.

THE SOLUTION REQUIRES A HEAVY DEGREE OF SETUP AND CHANGE MANAGEMENT.

Third-party access is not some new phenomenon that businesses are just beginning to grapple with. Third parties are already on the inside and putting organizations at risk today. A solution that requires a months-long implementation will therefore be a non-starter in many cases. In addition to fulfilling the immediate need for protection, solutions should require minimal change to user workflows.

A zero-trust access tool should come with a fast, seamless setup that can go virtually if not fully unnoticed by end users. Not only does this improve the ROI and time-to-value of the purchase, but it increases the likelihood that the tool will be fully adopted and provide the maximum possible value.

ZERO TRUST: TRANSFORMATION HAS COME FOR CYBERSECURITY

According to Ponemon, 59% of organizations suffered a breach caused directly by a third party in 2022, and 54% of respondents suffered an incident from the breach of one of their third-party connections.

Extending controls into the vast thicket of the digital wilderness is impractical if not fully impossible. There are simply too many variables and unknowns to contend with, including the cascading risk of vendors' vendors, vendors' vendors' vendors, ad infinitum.

Rather than attempting the impossible task of securing a boundless perimeter, organizations can use zero-trust security to prioritize risk and defend both assets and users through an identity-based approach to secure access.

To ensure a zero-trust deployment that meets its full set of goals, enterprises need more than just a zero-trust access provider. They need a true strategic partner willing to meet them where they are and provide actionable solutions to complex problems.

Cyolo was designed for just this purpose. Built by the former head of the Israeli Navy's Cyber-security Unit and two leading ethical hackers, Cyolo brings true zero-trust access to all industries, including high-governance verticals like life sciences, finance, insurance, and pharma. Unlike other zero-trust accesss tools, the Cyolo solution has the unique ability to retrofit legacy infrastructure with modern authentication capabilities like MFA and SSO, eliminating the need for a drastic rip-and-replace project that could take months or years.

No matter where organizations are on their zero-trust journey, Cyolo can solve the challenges associated with high-risk access and help build a more secure, scalable future.

ABOUT CYOLO

As business extends beyond the office walls to form an entire ecosystem, organizations are experiencing more access-related nightmares. Cyolo gives both IT and OT enterprises the visibility and control they need to securely manage who can connect to what and what they can do while they're connected, as well as the ability to directly monitor the connections that could cause the most serious damage to their business.

The unique and proven architecture of the Cyolo platform enables organizations to deliver a frictionless experience that is 3x faster and significantly easier to deploy than other zero-trust access solutions. But what makes Cyolo truly unique is that it was built by a CISO. It's the solution you would have created to confidently secure access to everything everywhere – no exceptions.

To learn more, visit cyolo.io