Cyolo

CROSSING BARRIERS

CONQUERING THE 5 BIGGEST HURDLES OF THIRD-PARTY ACCESS

INTRODUCTION

What do the high-profile breaches at Uber, Kaseya, and SolarWinds have in common?

They all demonstrated the risks posed by third-party access and revealed just how much we don't know about our vendors' security posture. At the same time, these and other attacks have exposed the tremendous extent to which modern businesses depend on other businesses.

In particular, companies across industries and verticals have grown increasingly reliant on third parties to leverage specialized skills and perform various crucial tasks. These **third parties can be contract workers, vendors, suppliers, or other service providers who do not work directly for the company.** Organizations can take advantage of the efficiencies, intellectual capital, and economies of scale that third parties provide without incurring the costs and burdens associated with building and maintaining certain capabilities in-house.

When it comes to operational technology (OT) environments, third parties are especially important, as their expertise may be needed to troubleshoot a key piece of equipment or perform other essential tasks. Examples include outsourced contractors who manage, operate, and repair particular systems as well as highly specialized technicians who maintain Industrial Control Systems (ICS) environments.

To achieve the benefits associated with third parties, however, the organization typically must provide them with access to critical resources. For this reason, **third-party users are inherently high-risk users**, or users whose actions could (purposefully or inadvertently) cause enormous damage to the business. A cyberattack conducted against a third-party vendor or supplier could, as we have seen time and again, lead to serious consequences for all of its partnering organizations.

This paper will outline the risks and challenges associated with third-party access and how they can be overcome. We will also examine what it takes to deploy a zero-trust access solution that reduces risk while preserving the overall productivity and efficiency of the organization and its third-party users.

THE REALITY OF THIRD-PARTY BREACHES

THIRD-PARTY BREACHES HAPPEN EVERY DAY

Third parties pose an inherent risk to the companies for whom they are contracted to do work because organizations have little (or no) ability to enforce security controls on third-party users or their devices.

- 59% of organizations suffered a breach caused by a third party, while 54% suffered a breach **due to the breach of a third party**. (Ponemon)
- 98% of organizations have at least one vendor who has **suffered a breach in the past two years**. (Cyentia Institute)
- For every compromised vendor, an average of **4.73 companies were affected** in 2022. (Black Kite)

FOURTH-PARTY VULNERABILITIES ARE MORE COMMON BY AN ORDER OF MAGNITUDE

Businesses shouldn't forget that their vendors have vendors, too. Fourth-party vendors (and beyond) can further compromise an organization's security posture with their bad practices and vulnerabilities. This is called cascading risk, and it can quickly create a domino effect of disaster.

- The average firm has **60-90 times more fourth-party relationships** than they do third-party relationships. (Cyentia Institute)
- Half of organizations have relationships with over **200 fourth parties** who have suffered a breach in the past two years. (Cyentia Institute)
- First parties tend to have better security risk scores than third parties, and **third parties tend to have better security risk scores than fourth parties.** (DarkReading)

ACCESS IS A KEY PART OF THE EQUATION

Attackers commonly use social engineering schemes or phishing to obtain legitimate user credentials and exploit vulnerabilities in access control. When granted implicit trust and free lateral movement, they can use legitimate third-party credentials to access data, upgrade their own permissions if needed, and deploy malware across the network. While it's relatively simple to extend security and access management policies to in-house personnel, third-party contractors with corporate credentials – and especially those with privileged access credentials – pose a greater threat.

- **Unauthorized network access was the most common cause of third-party attacks, accounting for 40% of third-party breaches.** (Black Kite)
- 70% of breaches in 2022 resulted from **over-permissioned third-party users.** (Ponemon)
- 82% of companies **unknowingly give third parties access** to all of their cloud data, while 76% of companies have third-party roles that **allow for full account takeover**. (Wiz)

Despite these substantial risks, third parties aren't going anywhere. They simply provide too much value, often allowing businesses to perform in ways that might otherwise be impossible. But to achieve the maximum value from third-party partners, the high level of risk they pose must be mitigated. This requires that organizations grant appropriate, exact access for third parties to efficiently perform their duties — no more, no less.

Significant barriers may complicate this objective, but it can certainly be done. By examining the toughest challenges of securing third-party access, organizations can identify steps to shore up these gaps and gain protection without sacrificing productivity or the other benefits that third parties bring.

TOP 5 THIRD-PARTY ACCESS CHALLENGES

INHERITED RISK

Too many organizations procure first and ask questions… never.

According to a 2021 Ponemon study, security is not a primary factor in assessing potential vendors, and more than half (51%) of organizations don’t perform any security assessments of third parties before granting them access to sensitive systems and data. Instead, they take organizations on their reputation or expect that a Non-Disclosure Agreement (NDA) will cover them. Most frequently, organizations merely stipulate in their contracts that vendors must abide by security and privacy practices.

Contractual agreements are necessary, but they too often focus more on recouping damages than preventing them. And in many instances, responsibility for a breach caused by a vendor still falls to the first party.

Though organizations should absolutely do more to vet vendors at the outset of the relationship, the truth is that there’s no possible way to extend security controls throughout the full web of vendors and vendors’ vendors, ad-infinitum.

Traditional castle-and-moat security strategies protect the perimeter but allow wide lateral access once a user makes it into the network. Instead of hardening an outer wall that is now far too porous to be adequately defended, organizations must harden the inner wall – namely, their people. This is what zero-trust access is all about.

LACK OF VISIBILITY AND SYSTEMS CONTROL

Security controls and policies are hard enough to enforce across internal users. When it comes to third parties, the task is virtually impossible. Remember, vendors service a wide customer base, so adhering to unique policies from each of their customers simply isn’t practical for them.

Traditional options for securing third parties have been quite limited. Shipping an agented machine is costly and time-consuming, workarounds like Virtual Private Networks (VPNs) are insufficient and overly complicated, and adding the vendor to the organization’s identity provider (IdP) is time-consuming and difficult.

Controlling third-party activity is especially challenging for operational technology (OT) environments in settings like manufacturing, energy, and infrastructure, as these systems were not designed to support modern authentication or to enable visibility and logging capabilities.

At the end of the day, third parties are guests, not family. To ensure their own security, organizations need the ability to detect every connection and, ideally, to monitor third-party activity in real time.

COMPLIANCE CONTROLS AND MANDATES

Regulatory agencies, legislative bodies, and insurance providers in many parts of the world are ramping up control requirements around both privacy and cybersecurity. Even though the cause of a data breach may originate from a third party, in the eyes of the law (and customers), the organization is the one who could be held liable.

From sweeping regional standards like GDPR to industry-specific regulations like PCI-DSS and HIPAA to commonly accepted frameworks like ISO 270001, NIST, and COBIT, almost all of these standards include requirements around vetting third parties and holding them accountable.

Additionally, many cybersecurity insurance providers now require the organization-wide application of multi-factor authentication (MFA) and other modern controls. Those who can't meet these basic requirements face gigantic premiums or outright denial of coverage.

Compliance mandates and cyber insurance pre-requisites will only grow more demanding as time goes on. In order to keep evolving at the pace of emerging legislation and standards, organizations need the ability to modernize without disruption.

ACCESS CONTROL MANAGEMENT

Once an organization takes on a vendor, that vendor's access still needs to be managed and controlled. Presumably for the sake of simplicity, many organizations assign third-party users an admin-level account in their Active Directory. This may save a few minutes, but it creates a severely overpowered permission set. And only adding to the risk, third parties often never have their access revoked once their work is done.

To provide a more appropriate level of access, organizations must be able to finely tailor controls for vendor roles to enforce role-based access control. In addition, they need the ability to enable controls without requiring the vendor to install an agent.

POST-BREACH RECOVERY

According to Forbes, almost 83% of businesses that suffer a breach will go on to experience additional cybersecurity events. An initial security incident can pave the way for subsequent breaches by exposing weaknesses in a company's security system that can be exploited later, or by creating a backdoor for the attackers to return to later. Visibility into the timeline of a breach can also be clouded by the long dwell times of attackers, who use sophisticated techniques to cover their tracks.

These factors are exacerbated and traceability is further obscured when it is an organization's third-party vendor or supplier who suffers a breach. The organization itself may have no visibility at all into the attack forensics and thus no ability to patch vulnerabilities and remediate them with confidence. The company is reliant on the third party to respond appropriately, with little to no input into their strategy.

ASSESS THE STAKES OF A THIRD-PARTY BREACH

When organizations think about breaches, they often think about a specific financial cost, especially at the leadership level of the company. Amazon's $877 million GDPR fine and Equifax's $575 million settlement for failing to fix a vulnerability and inform the public — these costs cause significant impact to even the largest and most-funded companies.

But fines are hardly the only consequence an organization suffers after an attack.

- They may never re-establish the trust of customers and employees.
- They may be forced to pivot abruptly and disrupt operations.
- In the worst cases, they may not be able to continue service.

It is no longer sustainable to hope a breach never happens. Organizations must up the rigor around their vendor vetting policies and seriously audit their provisioning processes, onboarding and offboarding, and vendor monitoring practices.

RECENT THIRD-PARTY BREACHES

PUMA

Their payroll and scheduling provider, Kronos, was victim to a ransomware attack, which allowed a breach of Puma's systems.

CVS

A third-party hosted database had no form of authentication and exposed more than 1.1 billion customer email addresses, user IDs, and customer search history on the CVS Pharmacy website. This puts CVS customers at risk of phishing campaigns due to exposed email addresses.

OKTA

In January 2022, Okta was compromised by Lapsus$ after they gained remote access to a machine from a third-party customer service vendor.

ZERO-TRUST ACCESS:
A MODERN MEANS TO MINIMIZE RISK

How an organization thinks about security will drive strategy and solution implementation. Traditionally, perimeter security was the dominant method, with known, trusted users kept inside the perimeter wall and potential bad actors kept out (at least in theory). The types of solutions used to fortify the perimeter included physical security, firewalls, and network tools to monitor access and behavior.

But the nature of work has changed, and even more significantly, user behavior has changed. Today, dependence on third-party contractors and remote work capabilities extends the potential attack surface far beyond any perimeter that once existed. Simply put, no user, device or machine can be inherently trusted – inside or outside of the company's environment.

The zero-trust framework can be a powerful tool to lower the risks of third-party access, especially when combined with security and oversight controls. This comprehensive approach to cybersecurity keeps corporate resources secure while allowing organizations to reap the benefits that third-party partners can offer.

Zero trust requires all users and devices to be authenticated on an ongoing basis. There is no more “tunneling into the perimeter” through a VPN to achieve access. Instead, the zero-trust access model demands limits on access, verification to use resources, and logging and monitoring of all activity. In addition, the principle of least privilege is strongly enforced, and access is granted to specific applications and never to the entire network.

Zero-trust access offers a pathway to minimize the risks associated with granting third parties (along with anyone else) access to sensitive resources. Under the zero-trust framework, trust is never inherently given and must be explicitly granted following verification of the user and device identity. The most basic description of how zero-trust access works is “Never trust, always verify.”

A well-thought-out implementation of zero-trust access will not happen overnight. Still, **the shift to zero-trust security** can pay dividends and reduce the risk to critical assets, such as manufacturing lines, intellectual property, and other critical infrastructure.

PROTECTING AGAINST THIRD-PARTY RISK WITH CYOLO

The Cyolo Zero-Trust ~~Network~~ Access solution empowers organizations to securely connect all types of users, including high-risk third parties, to the applications and systems they need to do their jobs.

The network and platform-agnostic approach can be easily deployed and integrated across all types of users and environments. The Cyolo solution gives security professionals the ability to tailor controls based on high-risk access scenarios, implement policy-based multi-factor authentication, and achieve secure access and action control for advanced and legacy applications alike.

Third-party risk is further minimized through features like session recording and supervised access. Session recording captures a third-party user's activities, enabling organizations to assess behaviors and ensure appropriate use. Meanwhile, supervised access provides an added layer of security and real-time monitoring for risky users.

With Cyolo, organizations gain the ability to:

- Control permissions and requests in real time.
- Grant administrative approval in real-time, including through SMS notification.
- Monitor and control sessions, with the ability to allow only specific actions and to revoke connectivity at any time.
- Maintain session recordings to audit all types of sessions, including SSH and RDP.

Collectively, these capabilities empower organizations to apply zero-trust principles to control and protect all high-risk access. Organizations can develop and easily configure highly specific access policies to establish rules for third-party access. For instance, access can be limited to certain times or days, and explicit access can be required for locked-down activities. Furthermore, recordings of all access create a trail to forensically support incident response activities.

TARGETED CAPABILITIES TO ENABLE SECURE THIRD-PARTY ACCESS

Agentless

Supervised Access

Session Recording

MFA & SSO for all applications

Native Client

Online or Offline

Platform Agnostic

Multiple Accounts → One Identity

Cyolo exists to prevent the access-related nightmares that haunt security and IT teams. In a global economy where third-party contractors, vendors, and suppliers play a crucial role, Cyolo allows organizations to confidently connect even the riskiest third-party users to critical systems without compromising security controls.

Cyolo

ABOUT CYOLO

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep modern business operations running.

Cyolo provides the only trustless zero-trust access solution, giving organizations visibility and access control over the users who leave organizations most exposed to risk, including third-party workers, remote OT operators, and post-M&A employees and applications.

cyolo.io