Cyolo

Control Third-Party Risk with Cyolo Remote Privileged Access

Reliance on third-party vendors and partners is simply a reality in today's enterprise world — but several years of headline-grabbing cyberattacks have shown that even the most innocuous-seeming third-party contractor can open the door for bad actors and serious security incidents.

Typically, third parties receive over-permissioned access and are granted implicit trust once inside the network. Security teams have limited visibility into vendors' behavior or control over their security hygiene. Consequently, the response to a breach caused by a third party is reactionary at best.

In light of the potential damage they could cause the business (whether intentionally or accidentally), **all third-party users must be considered high-risk users**. Security teams need the ability to monitor their activity, finely tailor their permissions, and validate their identities without impeding their productivity. Perimeter-focused models are unable to accomplish this. Identity must become the new center of gravity for cybersecurity.

The Cyolo platform protects what's connected to your network by continuously authorizing access to applications by all employees, vendors, contractors, and partners.

- **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*)
- **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*)
- For every compromised vendor, **an average of 4.73 companies** were affected in 2022. **(***Black Kite*)
- Unauthorized network access was the most common cause of third-party attacks, accounting for **40% of third-party breaches**. (*Black Kite*)

MOST COMMON ATTACK VECTORS

UNAUTHORIZED NETWORK ACCESS

Attackers commonly use social engineering tactics like phishing to obtain legitimate user credentials and exploit vulnerabilities in access control. When granted implicit trust and free lateral movement, they can steal data, upgrade their own permissions, and deploy malware. While policies can extend to in-house personnel, third-party contractors with access credentials pose a threat.

UNSECURED SERVERS AND DATABASES

When unguarded by login processes or SSL certificates, these resources may as well be open to the public. Attackers possess tools that can easily detect these vulnerabilities and take advantage of a wide open door. This is particularly dangerous for organizations hosting personally identifiable information (PII) or other sensitive data. When companies perform a security audit, unsecured assets can easily be missed if they are hosted by a third party.

MISCONFIGURATIONS

As digital systems become more vast and complex, misconfigurations slip through the cracks and allow attackers an easy entry point—especially in the cloud. SaaS tools often come with over-permissioned default settings that attackers use to disable other controls and upgrade their own access permissions. Misconfigurations on the vendor's side can provide an easy access point into corporate systems and networks.

THIRD-PARTY ACCESS NIGHTMARES

OKTA, 2023

Okta was compromised through a third-party IT supplier who had recently acquired another company. The acquired company's legacy network provided the attacker's initial entry point.

KASEYA, 2021

Kaseya offers IT solutions to Managed Service Providers (MSP) who act as IT partners for their commercial customers. Threat actors exploited a vulnerability in Keyasa's Virtual System Administrator product to bypass authentication and deploy ransomware to tens of thousands of MSPs, affecting hundreds of thousands of small businesses.

SOLARWINDS, 2021

A sophisticated attack compromised SolarWinds's Orion platform by creating a backdoor that allowed the threat actors to disguise their activity by impersonating users. They then injected malicious code into the platform, which was later distributed to customers as a typical update. The attack affected 425 of the Fortune 500, as well as the US Department of Homeland Security.

THIRD-PARTY ACCESS CHALLENGES

OVER-PERMISSIONED ACCESS IS THE DEFAULT

Companies often grant third-party vendors highly privileged roles with access and abilities that they do not need. If such an over-permissioned account is compromised, the bad actor can escalate their own permissions, disrupt systems, and access sensitive resources and data.

LACK OF SYSTEM CONTROL

Organizations have little ability to enforce security controls on third-party users or their devices. Shipping an agented machine is costly and time-consuming, workarounds like virtual private machines (VPNs) are insufficient and overly-complicated, and adding the vendor to the corporate IdP is not effective for tracking their activity.

NO CENTRALIZED RESPONSIBILITY

Responsibility for third-party risk is typically shared among compliance, security, procurement, and others — but no one fully owns it. This drastically obscures visibility and very few organizations have a comprehensive inventory of third-party vendors. Therefore, they cannot assess how many third parties have access to critical information.

VENDOR COMPLEXITY

A network of vendors can be just as complex as any systems landscape, for many of the same reasons. Organizations often lack the resources and tools to keep track of third parties, especially if there is frequent turnover in third-party partners. Consequently, they end up having to take the vendor at their word, self-assessment, or reputation.

CASCADING RISK

Vendors have vendors too. Fourth party vendors (and beyond) can compromise an organization's security posture with their own bad hygiene and vulnerabilities. It is important to know who third-party partners are sharing sensitive information with before an incident occurs.

SECURING THIRD-PARTY ACCESS WITH CYOLO

The traditional castle-and-moat security approach grants intrinsic trust to anyone who can access the network. **The Cyolo remote privileged access platform, by contrast, protects everything connected to the network by validating and continuously authenticating all third-party identities and then providing access only to explicitly authorized resources.** Beyond enabling more secure access, Cyolo gives security teams the visibility and granular controls they need to finely tailor third-party permissions and enforce the principle least privilege to enable vendor productivity with minimal risk.

ACCESS CONTROLS

- **Multi-Factor Authentication (MFA)** to confirm identity
- **Single Sign-On (SSO) & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- **Terminate Connection** once work is complete

OVERSIGHT CONTROLS

- Full **Audit Trail &** complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery for Business Continuity**

TECHNICAL OVERVIEW OF THE CYOLO SOLUTION

The core building blocks of the Cyolo platform are Identity Access Controllers (IDACs) and Edges. The following is a description of each Cyolo platform element and in which environments they are used.

IDENTITY ACCESS CONTROLLER (IDAC)

IDACs terminate the Transport Layer Security (TLS) 1.3 connections and enforce the access policies configured by the Cyolo administrator. As a 'reverse-proxy,' all decryption and enforcement occurs behind organizational firewalls.

EDGE

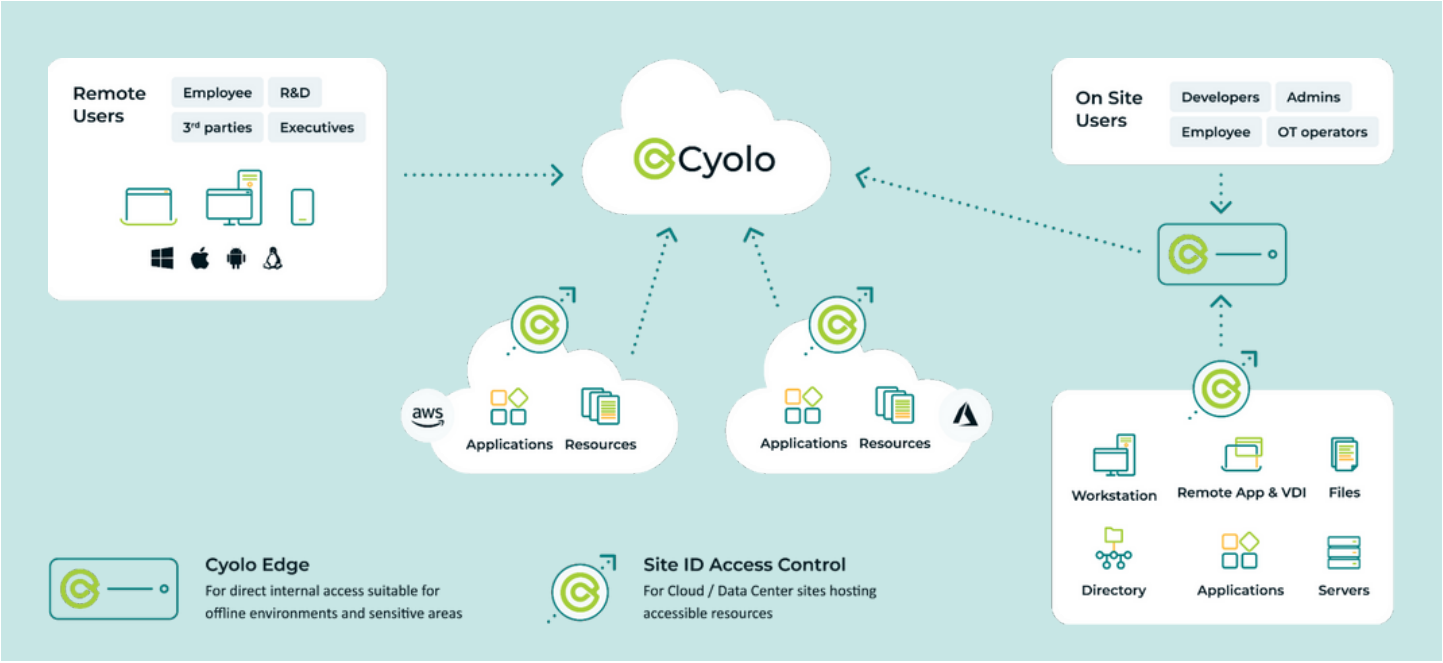
Edges are on-premises brokers that route users' requests based on a Server Name Indication (SNI) header to the relevant IDAC. In all deployment models, the Edge routes traffic from the users to the IDACs. Edges can operate without any external connections, which makes Cyolo an ideal secure access solution for operational technology (OT) environments that are air-gapped or disconnected from the internet.

CLOUD EDGE

The Cloud Edge is a cloud-based broker that routes users' requests based on an SNI header to the relevant IDAC. The Cloud Edge also routes traffic from the users to the IDACs. The Cloud Edge never decrypts any traffic – meaning the Cyolo solution actually upholds the principles of zero trust.

CYOLO CONNECT

Cyolo Connect is an installed agent for domain-joined machines and mobile devices. While most deployment scenarios do not require an agent, Cyolo Connect enables advanced features such as device posture checks and endpoint security integrations.



Cyolo can be deployed in cloud-connected, cloud-averse, and offline environments.

These are the core elements needed for each deployment method:

- **IDP CONNECTION**

  Identity providers (IdPs) ensure the user seeking access is who or what they claim to be across multiple platforms, applications, and networks. Cyolo can integrate with existing IdPs or use Cyolo's local (native) IdP that is included as part of the IDAC setup. The IDAC connects directly to the IdP (not through the Edges).

- **IDAC OUTBOUND COMMUNICATION**

  IDACs always communicate outbound, whether they connect users' sessions coming from the Edges (on port 443) or whether they communicate with the published applications they serve (on their specific port).

The scale of cascading risk introduced by third and fourth parties is impossible to defend against using traditional perimeter-focused security controls. Organizations simply cannot afford to take vendors at their word regarding their own security postures or the security postures of their own partners, who may have access to critical systems and data. The Cyolo remote privileged access solution gives organizations the visibility and granularity of control they need to secure third-party users without impeding their productivity.

WITH CYOLO, ZERO TRUST MEANS ZERO EXCEPTIONS

Unlike other secure access vendors, who rely on a shared infrastructure model that immediately and paradoxically violates the principle of zero trust, Cyolo is built on a unique trustless architecture that stores all customer data securely within the organization's trusted perimeter and never in the Cyolo cloud. This model enables true zero-trust security, with Cyolo having no access to sensitive company information like encryption keys or passwords.

ABOUT CYOLO

Cyolo enables privileged remote operations, connecting verified identities directly to applications with continuous authorization throughout the connection. Purpose-built for deployment in every type of environment, our hybrid secure access solution combines multiple security functions required to mitigate high risk access, including Zero Trust Access for users and devices, MFA for the last mile, IdP, Vault, secure file transfer, supervised access, session recording and much more into a single, cost-effective, easy to deploy, and user-friendly platform.

Consolidate your security stack and experience the power of seamless and secure operations across any application in any environment, from critical infrastructure to cloud.

To learn more, visit cyolo.io.