Cyolo

Avoid M&A Security Risks That Limit ROI: Zero Trust for Post-M&A Access

A merger and acquisition (M&A) is not complete when the ink dries on the deal; in many ways, it is just beginning. Integrating two infrastructures—each with its own complex architectures, policies, and controls—can take years, and even then there is often no clean or easy way to do it.

During an M&A, malicious behavior is more difficult to detect because users are behaving irregularly. They are navigating conflicting policy sets, juggling multiple identity providers, and adjusting to new workflows. To minimize this friction, organizations often lower their defenses and create a wide road via which an attacker could sneak in.

Perimeter-based security strategies are simply not flexible enough to harmonize acquired resources and users. Identity-led zero trust can secure acquisitions and enable them to start creating value faster for the acquiring organization.

The Cyolo zero-trust access platform protects what's connected to your network by continuously authorizing access to applications for all users, including risky post-M&A employees.

- **Over a third of organizations** suffer data breaches related to M&A integration. (*IBM*)
- **55% of M&As** fail to realize their full value due to poor integration. (*Dealroom*)
- **Over 50% of organizations** have encountered a cybersecurity issue during an M&A that threatened the deal. (*Forescout*)
- **65% of organizations** experienced regrets in making an M&A deal due to cybersecurity concerns. (*Forescout*)

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 customer personally identifiable information (PII). As an acquiring company performs a security audit of the acquired company, these assets can easily be missed, especially 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. These tools often come with over-permissioned default settings that attackers use to disable other controls and upgrade their own access permissions. The complexity of an M&A further compounds these vulnerabilities.

M&A 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.

MARRIOT-STARWOOD, 2018

Marriott acquired the Starwood chain of hotels in 2016, but had not yet migrated its networks and systems when a breach released hundreds of millions of private records in 2018. An investigation discovered that Starwood's network had been compromised for two entire years before the acquisition took place.

EQUIFAX, 2017

After a 10-year acquisition spree comprising 18 companies, Equifax failed to patch systems when vulnerabilities were discovered and stored personal information on legacy systems. As a result, almost 150 million Americans' personal information was exposed, resulting in fines and settlements nearing $1B.

M&A CHALLENGES

TECHNICAL DEBT

The acquiring organization takes on the vulnerabilities and attack surface of the acquired organization. It can take years to configure and integrate poorly-architected and poorly-maintained systems.

IDENTITY PROVIDER SPRAWL

Incorporating an additional set of identity providers (IdPs) from an acquired domain burdens IT teams with the need to configure them all to work together and may demand an update to authentication protocols and workflows.

CONNECTING TO UNIQUE IP ADDRESS RANGES

Overlapping IP addresses post-merger can obscure visibility into user activity and make it harder for users to access the resources they need. The workload of IP range mapping and de-duplicating prolongs time-to-value on an acquisition.

MASS-ONBOARDING

Determining user groups and necessary permissions for all acquired employees is a huge endeavor. Most organizations simply allow traffic from the acquired firewall into their network, but this presents far more risk.

DEVICE SECURITY

Provisioning new devices for acquired employees can prolong ramptime, but enforcing security on their personal devices is very difficult. It is impossible to know the state of an employee's personal device or environment.

USER UNKNOWNS

The people inherited in an acquisition present the biggest unknown of all. They may adopt shadow IT, bring bad hygiene, or simply take too much time to conform to the organization's established policies and processes.

MAXIMIZE M&A VALUE WITH CYOLO

In today's security landscape, people are the new network perimeter. With its identity-based approach to secure access, the Cyolo platform is able to authenticate and extend connectivity post-M&A to newly onboarded users with no added risk. Cyolo validates and continuously authorizes all users according to identity and then provides 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 permissions for specific user groups and enforce the principle least privilege to ensure maximum productivity with minimal risk. With Cyolo, organizations can position security as an enabler of progress and scale rather than a hindrance.

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

Cyolo has developed a uniquely architectured zero-trust access platform to help companies across industries gain the control they need to effectively merge two distinct companies into one.

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

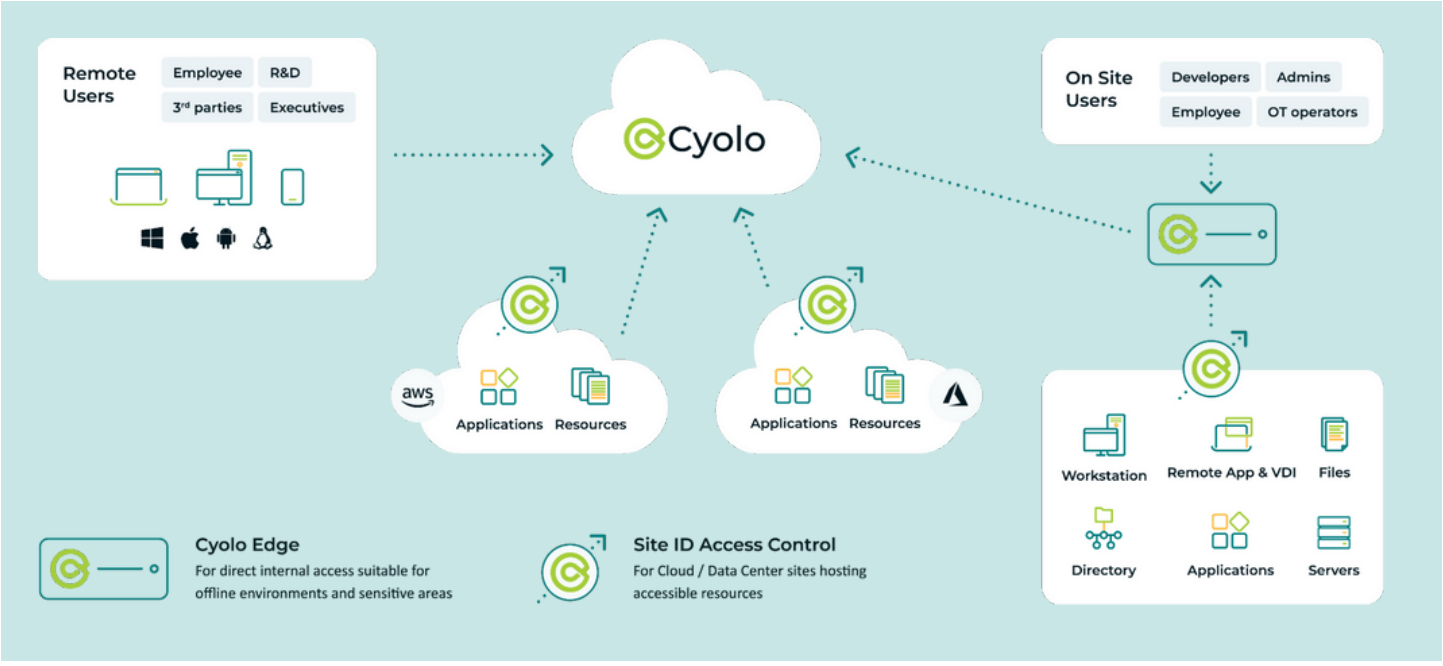
Edges are on-premises brokers that route users' requests based on a Server Name Indication (SNI) header to the relevant IDAC. In all deployment models, the Edge routes traffic from the users to the IDACs. Edges can operate without any external connections, which makes Cyolo an ideal secure access solution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

The on-premises deployment can be fully isolated and non-IP connected for additional security, as needed. 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).

BRIDGE THE GAP WITH ZERO TRUST

Organizations will almost always choose growth over security. Zero trust gives you the best of both.
Security should contribute to innovation and growth, rather than slow it down. A zero-trust security strategy mitigates the security risks from M&A activity while empowering organizations to streamline onboarding and integration to achieve better outcomes and faster time-to-value.

WITH CYOLO, ZERO TRUST MEANS ZERO EXCEPTIONS

Unlike other zero-trust 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

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.