Cyolo

Ensuring Secure Access to Work: Overcoming Identity Challenges After M&A

Merging or consolidating an acquired organization's infrastructure is a massive endeavor that presents numerous challenges. Chief among these challenges is the fact that integrating two large-scale networks with many users is difficult - but must nonetheless be done as quickly as possible. The faster this integration takes place, the sooner the acquiring company can start realizing the benefits of the M&A.

Unfortunately, complications often arise because both organizations use multiple business-critical tools to get work done. Each user is accustomed to certain workflows for accessing their work, but as systems combine, or specific users need access to tools on the other company's system, these workflows begin to break down. The resulting user headache can easily become an IT nightmare. **With systems merging and the acquiree bringing in their own legacy applications and tools, the acquirer will be forced to proceed in one of two ways:**

> Cyolo securely connects people to work by ensuring the right level of access and connectivity to resources, applications, or services.

1. The acquiring organization operates both infrastructures and gives blanket access to new and existing users, creating an extremely unsecure and fragmented user experience.

2. The acquiring organization replicates the users, privileges, roles, and authentication sources within their existing system—a huge and time-consuming IT undertaking.

A modern authentication structure serves both security and business objectives, hardening your security posture while increasing flexibility and systems simplicity. Traditional multi-factor authentication (MFA) and single sign-on (SSO) measures depend on a broad dexterity in your security system. Typical MFA and SSO strategies break down when combining users from multiple merging companies.

HOW CYOLO CAN HELP DURING M&A

Cyolo securely connects people to work by ensuring the right level of access and connectivity to resources, applications or services. This access is designed to follow the zero-trust model, with identity serving as the key for unlocking any given resource. In a merger or acquisition, the large number of identity sources creates the bulk of the challenge. In such situations, Cyolo works as an Identity Federation tool. When a user requests access to a resource, **Cyolo will administer access and connectivity by validating the user's identity and their level of authorization for the specified resource.** Identity federation supports the ability to leverage all existing identity sources, including the acquired companies' identity providers (IDPs), privileged access management (PAM), and active directories (ADs), among many others.

With the ability to federate multiple identity sources, even those from different organizations, the Cyolo platform extends a zero-trust relationship to all assets. Now a user can be granted access to an application within one organization, with identity validation provided by the other. Instead of consolidating two disparate systems, IT can focus on extending the right level of access so users can get their work done without compromising security controls.

Cybersecurity concerns can derail mergers, with 53% of deals encountering critical cybersecurity issues such as:

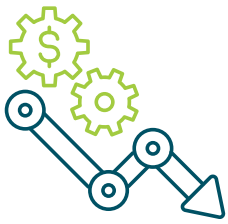
- Compliance Mandates
- Lack of System Control
- Network Convergence
- Lack of Visibility
- Legal and Financial Consequences

SECURE THIRD-PARTY USERS

GAIN FULL VISIBILITY AND CONTROL

ACHIEVE COMPLIANCE

DEPLOY AND SCALE WITH EASE



REDUCE OPERATIONAL COSTS