Cyolo

The ‘Last Mile’ of Application Security:
Extending Your Identity Providers

Every organization faces one consistent problem – managing their user’s digital identities. For years this was done with clunky, on-premises directory servers that required special resources to manage and secure. This model worked well in a non-distributed environment, where companies could anchor their security behind large perimeter firewalls and restrict access outside their organizations. But, as organizations grew larger and adopted more digital and cloud technologies, the pinch point of managing legacy, on-premises directories became too much for engineers and security teams.

Merger and acquisition scenarios were delayed by trying to establish directory trust between remote organizations, and this left security teams with even more gaping holes. Combining two mission-critical systems that follow completely different organization-specific policies is a process that in many cases can span years.

With the popularity of cloud and software as a service (SaaS) applications like Salesforce.com, Zoom, and O365, businesses needed to scale their identity directories to the cloud as well. Cloud-based identity providers (IdPs), such as Okta, Ping, Jumpcloud, and many more, all emerged offering similar functionality – the ability to move all users to their directory services for better management, security, and consistency across the entire tech stack. At the same time, this meant organizations could retire hardware and legacy software to better suit their cloud-forward vision. This worked well in theory, but **cloud directories made for cloud apps left out an integral component – mission-critical on-premises applications.**

> *Even the best IdPs find themselves unable to communicate with legacy applications, as they simply do not speak the same language.*

‘LAST MILE’ APPLICATIONS

- Leave systems unprotected
- Create vulnerability
- Compomise security controls
- Allow for cyberattacks
- Cause security incidents

The gap of what traditional IdPs are able to cover is the ‘last mile’ of application security. Whether it is an enterprise resource planning (ERP) system, payroll, or customer resource management (CRM), most if not all organizations still rely on at least some legacy applications hosted in their data centers.

These applications were built before multifactor authentication (MFA) was an expected norm, and long before security assertion markup language (SAML) was even thought of. Practically speaking, this means even the best IdPs find themselves unable to communicate with such applications, as they simply do not speak the same language. At best, this ‘last mile’ gap has a complex but half-baked solution in place; at worst, these systems are entirely unprotected.

This ‘last mile’ has caused numerous newsworthy security incidents of late, and the need to protect it is more important than ever. Cyberattacks are increasingly threatening critical infrastructure, such as water and nuclear energy plants, which run on vulnerable legacy, out-of-date software. Downtime for maintenance or migration would result in enormous monetary losses and could potentially even impact the local environment and workers' safety – rendering it a non-stater.

Enter the Cyolo zero-trust access solution,

which brings all your existing identity infrastructures into a single platform to manage and secure application access. Thanks to its ability to deploy even in highly regulated offline environments and securely interface with legacy resources, Cyolo can make identity modernization a reality. Extend MFA and single-sign-on (SSO) with secure connectivity to any legacy, thick-client, or on-premises resource while still leveraging your multiple cloud providers. While secure access is critical, MFA and SSO alone are not enough.

Cyolo is the extension of existing identity infrastructure that allows you to create a singular digital identity to be used across your entire organization, including the ‘last mile.’ Cyolo facilitates the connectivity from users to applications, without granting network access (like a VPN), by way of an identity-aware proxy solution. With a trustless architecture, Cyolo can “glue” multiple identity providers together and establish zero-trust application access and connectivity, without ever leaving your secure boundaries.

At last, you can securely connect people to work, without compromising security controls – even for ‘last mile’ applications.

Cyolo