Cyolo

A SINGLE SOLUTION FOR SOLVING TODAY'S TOUGHEST MFA AND SSO CHALLENGES

INTRODUCTION

Let's be honest, no matter how much you've moved to the cloud, digitally transformed, or Agile-d your processes, you still rely on some systems that are either custom-built or else so dated that modernizing them is a non-starter.

Though these systems dangle outside the bounds of security best practices, they would simply be too expensive and disruptive to replace.

Even modern identity and access management solutions can't extend multi-factor authentication (MFA), single sign-on (SSO), and other key security measures to these digital hinterlands.

To date, the risks created by such gaps have been outweighed by the cost of modernizing those parts of your infrastructure.

It is what it is, right?

A study by HYPR on the state of authentication in the finance industry found that the average financial institution suffered 3.4 breaches per year to the average tune of $2.19M. Yet over 60% of respondents didn't upgrade their authentication systems after a breach.

- 75% reported IT complications like management complexity and integration issues.
- 62% cited user experience deterioration, which caused resistance from employees.
- 57% said remote employees were significantly harder to authenticate.

Sound familiar?

But the stakes of legacy vulnerabilities grow higher each day. Your most critical business processes live and rely on digital infrastructure. Threats that used to be IT-specific now impact the business at large. Though the enterprise world is slow to modernize, bad actors most certainly are not.

Even if you think a catastrophic cyberattack is unlikely to befall your organization, consider the rising costs of cybersecurity insurance. Today's underwriters take great care to assess an applicant's cybersecurity posture. Those without the basic security fundamentals—MFA being one of them—may be denied insurance or face increased premiums.

And merely enabling MFA when it's convenient isn't enough. MFA must be used for all services, applications, and users. Cloud and on-premise. Legacy and modern. Least and most privileged.

Can you meet that requirement?

Practically no organization can, so no matter the maturity of your cybersecurity practice, you're vulnerable to higher rates and risks than you should be.

THE CHALLENGE OF FLEXIBILITY

Today's digital infrastructure allows team members to work in myriad ways – in-office or remotely, from their company or personal device, using a range of operating systems, web browsers, etc. To do so, they must access a veritable jungle of apps, systems, and so forth.

At a point, this landscape intended to optimize work begins to complicate work. When connections become barriers, users take shortcuts that create security vulnerabilities and make it difficult to implement basics like MFA and SSO.

You know what these behaviors look like. In fact, you've probably taken a shortcut or two yourself at some point in your life.

"WHO THE HECK IS USER 1?"

MANY USERS SHARING ONE ACCOUNT

There's plenty of grumbling in the IT space about how idiotic business users can be, but users aren't account-sharing because they're dumb, lazy, or malicious.

Account sharing may save costs if the app's license prices by headcount.

Team members may use a single account to access and collaborate on a particular project.

The account may serve a specific function, rather than a specific user, so many users may inhabit that account to perform a particular task.

A shared account may be simpler to manage than keeping track of individual accounts and passwords, creating and eliminating them as team members come and go.

Like most shortcuts, account-sharing is harmless until something goes wrong. Then, you have no traceability into who did what. **From the inside of your IT systems, User 1 is one person.** Determining the real-life team member who made a mistake or committed an infraction is like solving a crime in a town where everyone has the same fingerprint, blood type, and DNA; the same height, weight, and shoe size.

CONSIDER THE RISKS OF CONVENIENCE.

Sharing a Netflix account with your mom is one thing. But account-sharing may expose sensitive information from trade secrets to payment information to customer data. This results in failed security assessments and compliance audits, triggering hard costs like higher insurance rates, fines, and penalties.

Account-sharing also lends itself to other lax security controls like weak passwords that are never rotated out. If that's you, then every employee who has ever acted as User 1 can still do so from wherever they are.

That's why 81% of hacking incidents utilize weak and stolen passwords.

IT'S IMPOSSIBLE TO IMPLEMENT MFA WHEN EMPLOYEES SHARE ACCOUNTS.

If your MFA structure sends a token via text to a user's phone number, whose phone does the token go to when multiple people use the account? If someone receives a token they didn't request, they can't tell if it's another team member or a bad actor trying to gain access.

You could give each employee their own individual credentials and let them install the appropriate MFA on their devices, but this ends up requiring you to set up hundreds of individual credentials and install MFA hundreds of times for a single user, let alone a whole team of them. A modern validation framework allows the priorities of security and productivity to play on the same team, each enhancing the other, rather than existing as diametrically opposed forces.

"HONEY, HAVE YOU SEEN MY KEYS?"

ONE USER, ONE PASSWORD, MANY ACCOUNTS

For bad actors, weak passwords are the lowest-hanging fruit.

It sounds like a no-brainer, but **a 2017 report from LastPass** revealed the breadth of password sprawl. The average business user has 191 passwords and types out their credentials over 150 times per month.

Apps generate an astounding amount of data that is then exchanged across the cloud and between devices and people. The result can be overwhelming for IT and security departments, who must continuously put out security fires.

It's only logical to speculate that those numbers have gone up in the intervening years. Think of all the physical identities you maintain. Library cards, health insurance cards, driver's licenses, passports, gym membership cards, season passes for your baseball team, that redemption slip from the dry cleaners—it's a lot to keep up with.

Your digital keychain is loaded down even more. For all of our digital transformation, you probably still occasionally fall into a spiral of login screens while trying to accomplish a basic task. Using the same password for everything is like having one card that works at the doctor's office, the library, and the airport check-in line, or one key for your car, your house, and your lockbox at the bank. Of course, if you lose that card or key, you're screwed. That's the risk of convenience. But for a business user, productivity trumps security. A complicated user experience imposes a drag on their productivity, which, at scale, translates to drag on business progress and agility.

IDENTITY PROVIDERS AREN'T A SILVER BULLET

To enable MFA and SSO for every single application, you need multiple sources of identity and validations. You're probably using several to meet different validation measures—CyberArk or Delinea for PAM, Okta or Duo for IdP, and Zscaler or Axis for ZTNA.

A "validation stack" like this is helpful and necessary. But it isn't complete. It isn't a singular, seamless experience. It's like reducing your 20 forms of identification down to three, but sometimes users are still forced to sign in to all of them. Which would you rather have, a keychain with 20 keys, but you could use one key at a time, or a keychain with three keys, but you had to use all three keys to unlock your house, car, etc.?

Plus, these identity tools can't extend MFA and SSO to legacy applications. It's like you've lost the key to your garage, so you just leave it unlocked and hope no one comes along and jiggles the handle.

"HELLO? IS SOMEONE IN THERE?"

THE CHALLENGES OF THIRD-PARTY ACCESS

Target famously suffered a breach in 2013 that exposed the credit card and personal data of over 110 million customers, resulting in a settlement of $18.5 million.

Target's security posture was robust, comprising over 300 dedicated info-sec staff members, an outside team of network monitoring experts, and state-of-the-art malware detection software. Yet the malware involved in the breach amounted to a run-of-the-mill Trojan Horse that would have been identified immediately by any commercial-grade antivirus software.

So how did it happen?

In a nutshell, Target gave remote network access to a third-party HVAC vendor to monitor temperature fluctuations and save energy costs. One of the vendor's employees fell for a phishing email, unleashing malware into the vendor's systems. This malware obtained the employee's login credentials to Target's network. With this access, the hackers uploaded another piece of malware to Target's cash registers and point-of-sale (POS) devices to collect credit card data in real time, all during the height of the holiday shopping season.

So what can we learn?

- Target's top-of-the-line security was compromised by a third-party vendor's sub-par security.
- There is no reason the vendor's credentials should have had access to Target's payment infrastructure—yet they did.

People are the new network perimeter.

You need maximum visibility into the most business-critical systems and apps, and you must be able to manage access on a privileged, untrusted basis to those systems. Doing so is more complicated than simply creating an Active Directory account for your vendor, then disabling that account after the work is complete. Here's why:

TOO MUCH ACCESS FOR SERVICE ACCOUNTS

Vendors often require Domain Admin rights, even when they don't need to perform the total range of admin functions. If these credentials are compromised, the attacker has the added power of admin-level privileges. Truthfully, the Domain Admin profile is overpowered, even for leaders within your company. By default, it grants rights to Active Directory, Domain Controllers, workstations and servers, Group Policy, and more. A best practice is to have one Domain Admin account in case of emergency, but it shouldn't be active. Outside vendors should definitely not be granted this profile.

MANAGEMENT COMPLEXITY

Out-of-the-box settings for groups in Active Directory are too lax because they are meant to be customized to your organization. However, a lack of understanding, planning, and execution can result in a messy, over-privileged Active Directory instance. To accurately grant the appropriate rights, the admin must gain insight into what is actually needed and grant access based on those requirements. You also need a system for regularly auditing and monitoring Active Directory. Otherwise, vendors will retain access long after the work is done.

ACQUISITION FRICTION

Merging or consolidating an acquired organization's infrastructure is a massive endeavor. Undoubtedly, the acquiree will bring their own legacy applications and system complications, and the acquirer can proceed in one of two ways:

The acquiring organization operates both infrastructures, over-permissioning new users and existing ones—an extremely unsecure and fragmented user experience.

The acquirer replicates the users, privileges, roles, and authentication sources within their existing system—a huge IT undertaking.

Traditional MFA and SSO measures depend on a broader dexterity in your security system than is commonly found in today's landscape. A modern authentication structure serves both security and business teams, hardening your security posture while increasing flexibility and systems simplicity.

RETROFITTING LEGACY SYSTEMS TO SUPPORT MFA AND SSO

Total modernization is simply outside the reach of most organizations – practically all of them.

The explosion of remote workers, connected devices, and identities is shaking the legacy foundations of today's enterprise world, but most "transformation" solutions simply ignore the reality of legacy systems. Organizations are left exposed to security threats, lapses in business-critical processes, and compliance risk.

Cyolo meets you where you are to extend cloud-based SSO and adaptive MFA to your traditional applications—affordably, quickly, and easily.

A SINGLE LOGIN EXPERIENCE

Cyolo provides a single identity-based connection linking to all IdPs. A team member will use a single set of credentials to log into the Cyolo platform and receive an MFA/SSO verification.

Cyolo will then verify that identity through your existing identity tools and log the user into the apps they need using a different, secure password that Cyolo rotates periodically.

GREATER DEXTERITY AND FLEXIBILITY

Cyolo grants access on an individual app basis, rather than a network basis. This lets your team define access with greater precision and granularity.

Unlike perimeter-based solutions that struggle to connect beyond-network users to the applications they need, **Cyolo's keyless, agentless platform can adapt to any system topology.** We'll build your organizational cloud and implement it wherever you need, allowing you to scale and leverage your existing tech stack more effectively.

RISK-PROOF THIRD-PARTY ACCESS

Cyolo lets you connect third-party users to your environments while keeping sensitive content, data, keys, tokens, and passwords within your full ownership and data center. Features like ongoing identity-based authentication and verification, session recording, and supervised access to resources and applications all work together to reduce your attack surface without compromising the user experience.

We don't even ask you to trust us. **Cyolo is the only zero-trust access platform that doesn't keep copies of your keys or store your data.** That's right—even we don't know the passwords used by our platform.

A PARTNER TO MEET YOU WHERE YOU ARE

At Cyolo, we value practicality as much as we value innovation. **Our platform is the first and only zero-trust access solution that can retrofit your existing technology to deliver a modern identity infrastructure.**

For most organizations, the rip-and-replace transformation model is a fantasy. But that doesn't mean you should subject yourself to higher insurance rates, tightening compliance regulations, or rising external threats. And you shouldn't have to choose between security and productivity, between safety and speed.

No matter where you are on your zero-trust access journey, we'll help you secure every enterprise digital asset, from edge to cloud.

To discover how Cyolo can help modernize your security, tell us more about your goals and challenges.

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 them most exposed to risk, including third-party workers, remote OT operators, and post-M&A employees and applications.

cyolo.io