

**DON'T LET YOUR  
GUARD DOWN:  
FORTIFY THE LAST  
MILE OF ACCESS  
SECURITY**



If you're even a casual basketball fan, you know that the final minutes of a high-stakes game can feel like the longest. Part of the reason is that they are. The last few minutes on the clock are agonizingly drawn out by time-outs, strategic fouls, video reviews of close calls, etc.

Back in 2014, the [sports website Deadspin](#) set out to determine how long it takes to play the final 60 seconds of an NCAA basketball game during the March Madness college tournament. They analyzed 52 games and came up with some profound insights.

- The last 60 seconds took an average of 5:57 to play out. The longest final minute of all went to the Tennessee-Michigan game, at 18:09. For those crunching the numbers at home, that final minute took up 14% of the entire game, including the 15-minute halftime.
- The closer the score, the longer the final minute lasted. In other words, the final minute takes longer when the game is still competitive. In the Oregon-Wisconsin game of the tournament, the last minute began with a two-point differential and ended with an eight-point win for Wisconsin.



To bring this analogy around to the subject at hand, the “last mile” of your systems landscape is the most difficult to secure. And just as it is in basketball, football or ice hockey, the last mile is also the most important one. Winning 85% of the minutes in a basketball game isn’t enough to guarantee victory, and securing 85% of your systems isn’t enough to reliably guard against cyberthreats and bad user hygiene.

**In this ebook, we’ll help you pinpoint the obstacles standing in the way of your goal — total organizational coverage — and position you to extend modern security practices to the most challenging aspects of your systems and operations.**



# Extending Your Identity Providers

Every organization struggles to manage their users' digital identities, i.e., verifying that users are who they say they are and restricting their access based on role and function.

In the past, organizations managed identities with clunky on-premises directory servers that required substantial, specialized resources to maintain and secure.

As organizations grew larger, digitized more business processes, and shifted to cloud technologies, the pinch point of managing these legacy, on-premises directories became an outsized burden for engineers and security teams.

For example, mergers and acquisitions became immensely more complicated — and high-risk. Combining two mission-critical systems that follow completely different organization-specific policies can take years. Security teams struggle to integrate new environments into their infrastructure, especially regarding the establishment of trust. The end result still creates a schizophrenic user experience and numerous security inefficiencies.



# The Challenge:

## Agility Comes at the Expense of Identity Security

With the popularity of cloud and software-as-a-service (SaaS) applications like Salesforce, Zoom, and O365, businesses had to scale their identity directories to the cloud, as well. Cloud-based identity providers (IdPs) like Okta, Ping, Jumpcloud, and others, emerged with a similar function: the ability to move all users to their directory services for better management, security, and consistency across the entire tech stack.

While this move enabled organizations to retire hardware and legacy software to fulfill their cloud-forward vision, cloud directories built for cloud apps neglected to consider one integral component — *mission-critical on-premises applications*.



## **What traditional IdPs cannot cover is the “last mile” of application security.**

Whether it is an enterprise resource planning (ERP) system, payroll, or customer resource management (CRM) platform, practically all organizations still rely on at least a few legacy applications hosted in their data centers. These applications pre-date the widespread adoption of multi-factor authentication (MFA) and the existence of security assertion markup language (SAML).

Consequently, even the best IdP will struggle to communicate with such applications. They just don't speak the same language. At best, this “last mile” gap is accounted for by complex yet half-baked workarounds. At worst, these systems are completely unprotected.

It's no wonder that this gap in security coverage has caused numerous newsworthy security incidents in recent years. The need to protect it is more critical than ever, as more cyberattacks threaten critical infrastructure systems running on vulnerable legacy software.

A woman with dark curly hair, wearing a white button-down shirt and a blue lanyard, is standing in a server room. She is holding a tablet computer and looking towards the server racks. The room is dimly lit with blue and green lights from the equipment.

**And yet, the prospect of updating or modernizing legacy systems is often a non-starter for two significant reasons:**

### **1. DISRUPTION**

The organization's operational workflow is simply too dependent on its legacy systems to press "pause" on them. The disruption required for maintenance or migration would incur monetary losses and could impact worker safety, the local environment, and even regional or national economies.

### **2. COST**

The cost of modernization is greater than the estimated cost of an incident. However, the dynamics around such cost evaluations are changing in light of modern threats and risk. Too often, organizational leadership takes a position of willful ignorance in the face of rising risk and the substantial cost of an adequate modernization investment.

**But doing nothing has a price, too – and that price is getting higher.**



# The Solution:

## A Universal Identity Infrastructure

If you can't bring your legacy apps and systems into the modern world, you must bring modern practices to them by extending your identity infrastructure across its current gaps.

The right solution gives you the transformation without the disruption, including the ability to:

- Deploy in highly regulated offline environments and legacy systems
- Extend MFA and single-sign-on (SSO) with secure connectivity to legacy, thick-client, and on-premise resources
- Leverages existing cloud identity providers
- Simplifies user workflows by allowing them to work securely with one single identity, rather than juggling several from various IdPs

**Unlike VPNs, a unified identity platform doesn't grant full network access. Its identity-aware proxy solution lets you establish identity-based access and connectivity without ever leaving your secure network boundaries. As a result, you can securely connect people to their work without compromising security controls, all the way through the "last mile."**





# Extending Your Privileged Access Management

If IdPs answer the “who?” question in regards to identity, then Privileged Access Management (PAM) tools answer the question, “how much?”

PAM tools were created to secure, monitor, and control the level of privilege each user receives. A privileged user is someone like an HR staff member who edits payroll information or an Industrial Control Systems (ICS) operator who accesses Programmable Logic Controllers (PLCs) in a plant or factory.

Because these users handle such sensitive information, users can’t choose their own passwords. You can’t operate a nuclear power plant with the password “123456.” PAM solutions manage credentials by centralizing them and layering in capabilities to check in/out and rotate them. By doing so, PAM solutions reduce the number of users who have access to sensitive systems and then secure those who truly do need such access.

# The Challenge:

## PAM Solutions Can't Communicate with "Last Mile" Applications

While PAM solutions have been much needed across several verticals and industries, PAM alone cannot protect your organization's entire tech stack. If a user (or bad actor) can get to the application and present the privileged credentials, they are granted access. PAM cannot validate whether the user arrived at the application through legitimate means before the credentials are entered. Additionally, PAM cannot support password management for legacy, thick-client, or homegrown applications.

**To put it more simply, PAM can't extend modern password security controls to the "last mile" of resources that predate those modern controls.**



# The Solution:

## More Iterative, Granular Validation Steps

PAM solutions can't evaluate the circumstances by which users arrive at apps and submit credentials. Organizations need the ability to integrate policy options into their identity controls, defining what users can access based on risk, geo-location, time of day, and a long list of other factors.

A modern identity solution can also apply controls for file uploads and downloads, clipboard access, and other physical device controls. When paired with an existing PAM tool, such a solution handles the connectivity to PAM-guarded assets with an arms-length interface and easily extends to critical applications that PAM solutions struggle to secure.

The outcome: workers can connect to their applications more securely with no added friction to the user experience. Credentials are securely stored, and broad network access never needs to be granted.





## Extending Your Zero Trust Network Access

The pandemic-driven shift to remote work fundamentally changed our society's attitudes and expectations around where, when, and how work should take place. No matter how the dust ultimately settles on remote and hybrid work, the traditional network-centric approach to security is a thing of the past. This poses new challenges and presents new opportunities for security professionals.



# The Challenge:

## People are the New Access Perimeter

Now that users have left the building, the riskiest threat vector is the users themselves. When everyone worked from the office, it was easy enough to extend trust to users who accessed the corporate network with valid credentials. This castle-and-moat model worked for many organizations for many years.

As the era of digital transformation set in, users needed remote access to corporate resources, which led to the creation of the Virtual Private Network (VPN). VPNs follow the same logic — trusting users based on the validity of their credentials to grant them access to the corporate network as though they were physically present in the office.



# The Solution:


## True Zero-Trust Access to Everything, Everywhere

Zero-trust network access (ZTNA) was designed to replace or augment VPNs as a tool for remotely accessing corporate resources, while simultaneously enforcing advanced security policies. Unlike VPNs, zero-trust access solutions validate who rather than where.

Essentially, zero trust eliminates dependence on the network perimeter by using identity-based criteria to verify users. Even after the initial authentication and login, zero-trust access solutions perform continuous authentication checks to combat session hijacking, prevent the installation of malicious payloads, and stop other nefarious activities.





A man with dark hair and a beard, wearing a dark blue button-down shirt, is shown in profile from the chest up. He is sitting at a desk, looking down at some papers or a device. The background is a blurred office environment with a window showing a grid pattern. The overall lighting is soft and blue-toned.

ZTNA is an important step forward from traditional remote access tools like VPNs, but the first generation of zero-trust access platforms still face significant shortcomings. First, in order to securely route traffic to the needed application, most ZTNA providers typically decrypt the traffic and then, after route determination, re-encrypt the traffic and send it on its way.

**This approach has three main problems:**

1. Each decryption/re-encryption takes up bandwidth and slows down the entire journey.
2. By hosting decryption keys, the ZTNA cloud router violates the zero-trust model and presents a single point of failure. Any breach of the provider could have serious security implications for their customers.
3. ZTNA tools are traditionally designed to support remote workers accessing cloud applications and often struggle to support on-premises users as well as hosted, legacy, or offline applications.

**The uniquely designed Cyolo zero-trust access platform abolishes the need for vendor trust with its trustless architecture. All data, passwords, tokens, etc. remain in the customer's trust boundary at all times, which both prevents the need for lengthy decryption/re-encryption journeys and ensures that a breach of the vendor will not endanger even an iota of sensitive customer assets.**

Beyond having an architecture that allows for faster speeds and greater security, the Cyolo platform is also the only zero-trust access solution purpose-built to enable users to access every type of resource, whether hosted on cloud, on-premises or even offline, as in the case of many operational technology (OT) deployments.

Furthermore, Cyolo can retrofit existing systems, including legacy applications, with the modern authentication infrastructure needed to support zero-trust access.





# Extending Your Secure Access Service Edge

Many organizations are seeing a growing disconnect between the cloud/SaaS-led direction of digital transformation and the legacy-but-necessary processes and realities of today's enterprise. What those in the SaaS camp may not realize is that "legacy" doesn't have to mean a millstone around the neck of your organization.

Traditional assets like on-premises tools, mainframes, and homegrown applications will likely always have a place in your organizational architecture. The solution, of course, is not the elevation of yesterday's tools over tomorrow's but greater synergy and integration between the two.

The Secure Access Service Edge (SASE, pronounced "sassy") is the meeting point between a wide area network (WAN) and cloud-delivered security services, such as Secure Web Gateways (SWG), Cloud Firewalls, and ZTNA.

Gartner predicts SASE strategies to become a high priority for enterprises in the next few years. SASE frameworks can improve business adaptivity and performance, threat detection and mitigation, and cost savings.

**However, SASE strategies also fall short when it comes to the "last mile."**

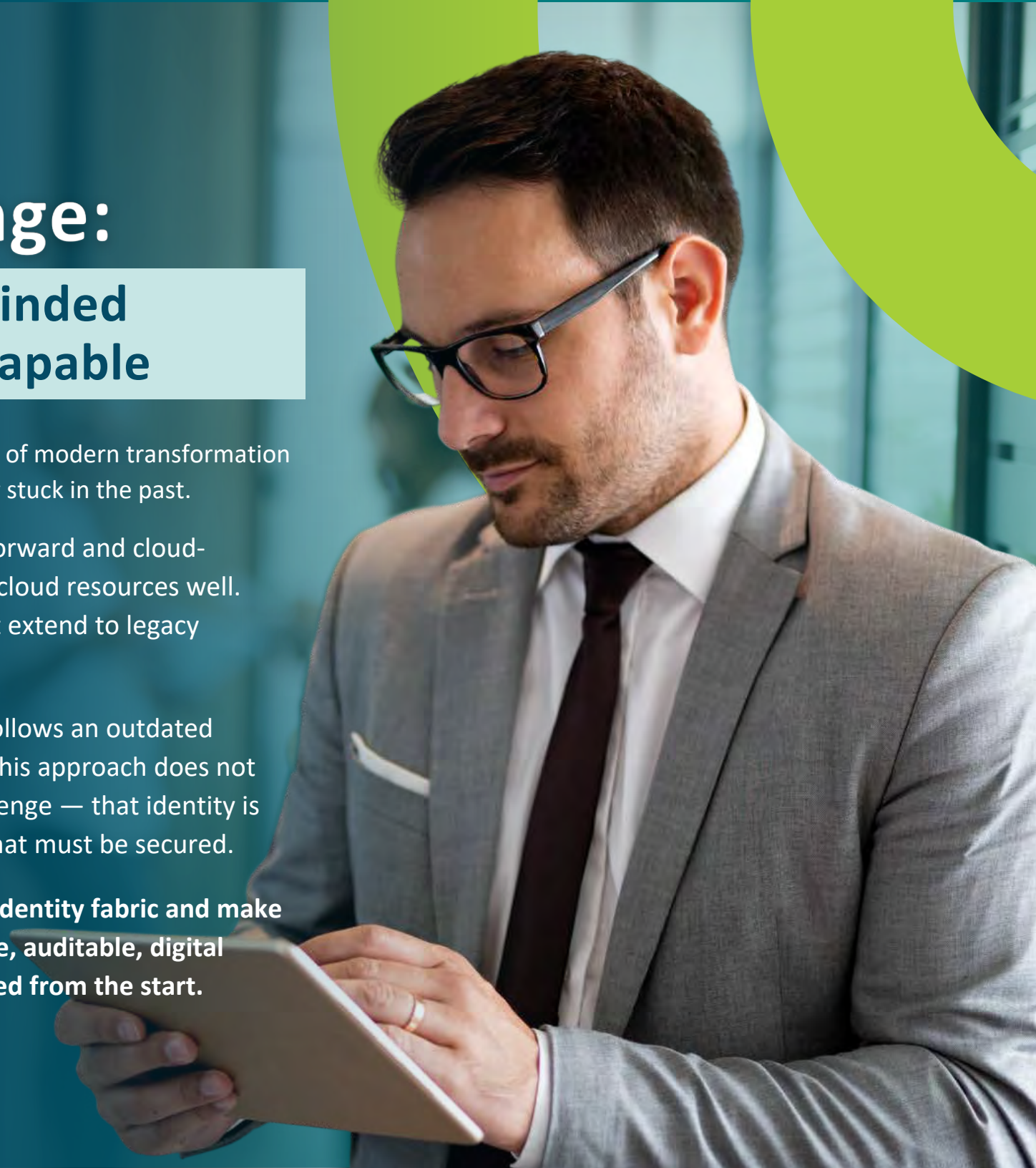
# The Challenge:

## SASE is Legacy-Minded But Not Legacy-Capable

Tactically, SASE has all the trappings of modern transformation methodologies, but it is strategically stuck in the past.

- SASE frameworks are cloud-forward and cloud-delivered, and SASE protects cloud resources well. However, SASE controls don't extend to legacy systems.
- At the same time, SASE still follows an outdated network-focused approach. This approach does not account for a significant challenge — that identity is now the primary perimeter that must be secured.

**Without the ability to weave an identity fabric and make access decisions based on a single, auditable, digital identity, SASE solutions are limited from the start.**



# The Solution:

## SASE Backed by an Identity Solution

SASE solutions have the most success when protecting modern cloud-native resources. To achieve full protection for the last mile of applications, you'll need to augment your SASE tool with a zero-trust access and connectivity solution that covers everything, everywhere, for everyone.

A modern identity solution meets compliance standards by tracing application access back to a single identity. For those overseeing critical infrastructure and OT networks or utilizing other on-premises legacy systems, identity-based connectivity is key to protecting business-critical resources without violating compliance mandates.





# Cyolo: The Full Court Press

Cyolo was built to meet the demands of today's toughest access and connectivity conundrums. Cyolo protects your "last mile" by sitting in front of tough-to-secure applications and brokering connections securely and quickly. Cyolo also adds MFA and SSO to applications that do not natively support these protocols in order to ensure that only verified users can connect to your critical systems.

When combined with existing security tools, Cyolo becomes the single source of truth for digital identity and access policies. With Cyolo, organizations can streamline all existing identity providers, retrofit legacy resources with modern authentication capabilities, and create a single policy enforcement point across all users, applications, and devices.







**Cyolo** helps you leave nothing unguarded so you can defend your organization when and where it matters most. No matter where you are in your access control journey, we're here to help you protect your organization from the first mile to the last.

To tell us more about your goals and learn more about how Cyolo can simplify secure access, [let's talk.](#)



[cyolo.io](https://cyolo.io)