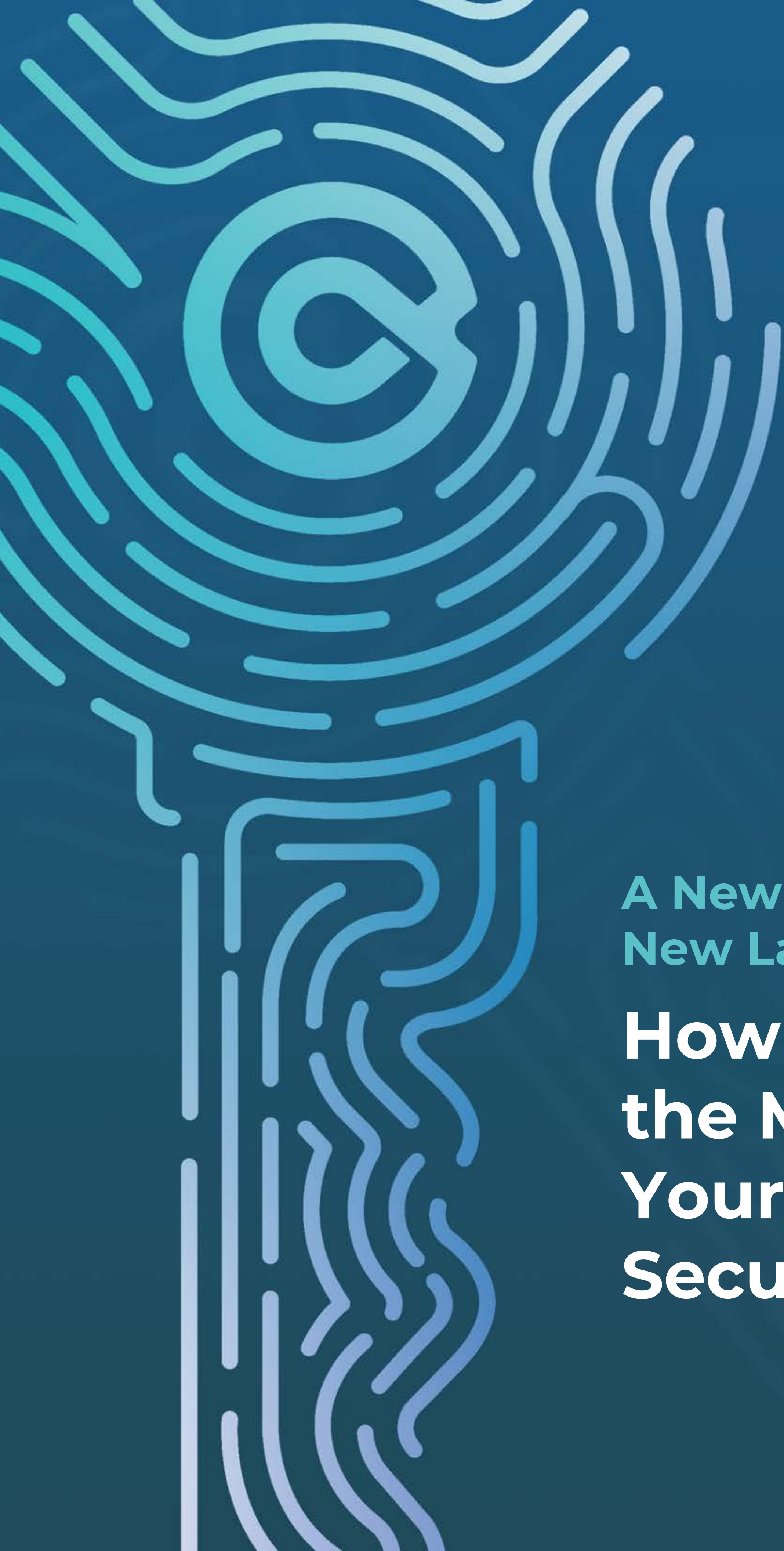


Cyolo

A New Lens for a New Landscape

How to Make the Most of Your Next Security Audit

The cybersecurity landscape has shifted at a tectonic scale over the past few years.

As we approach 2023, the world is finally settling into something resembling normalcy.

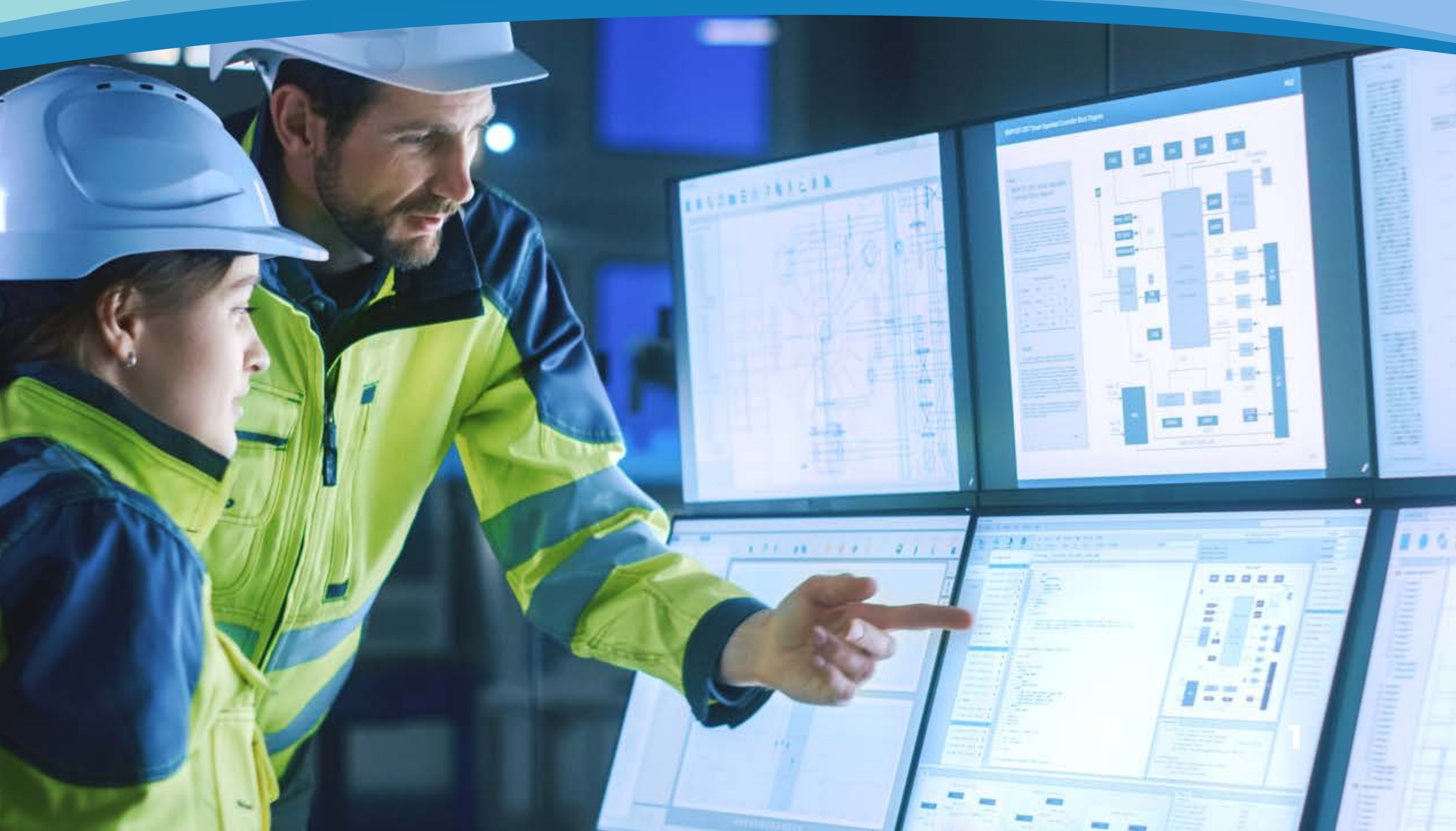
For the first time since 2019, your end-of-year audit can fully assess the vulnerabilities created by the triage-heavy pandemic years.

Between legacy applications, over-permissioned vendors, and remote workers, the results of this year's audit may be rough.

But take heart. This year, your audit is not your finish line — it will serve as your baseline for moving forward.

It's also the perfect opportunity to outline mid- and long-term objectives for your security program.

This is the year to right-size the technology and processes that kept your organization afloat, refocusing them into contributors to strategy, business agility, and innovation, rather than barriers to advancement.



A New Lens for a New Landscape

The way businesses operate today could hardly be more different than the way they ran just three years ago.

The digitization of business processes has increased your organization's attack surface more than ever.

People have become the new network perimeter. Identity-based access control will be key to shoring up your security posture, especially for remote workers and third-party vendors.

Today's rate of innovation and systems complexity has widened the gap of modernization between new and legacy tools, creating higher-stakes vulnerabilities.

An intense regulatory environment is only growing more rigorous, making compliance harder to achieve and driving the need to accommodate existing and emerging standards.

Cybersecurity insurers are increasing due diligence, requiring security basics like Multi-Factor Authentication (MFA) and Single Sign-On (SSO). Companies that cannot comply face drastically higher premiums, if not outright denial of coverage.

Evaluating your security controls and posture the same way you did in 2019 won't give you the clarity you need to make the most impactful decisions moving forward.

We're here to help you get the most out of your next audit by helping you assess your challenges with fresh eyes.

Legacy Applications

Gartner predicts that [by 2025, 90% of current applications will still be in use] and have insufficient modernization investment to take them forward.

Even as these applications become increasingly inefficient, maintenance-heavy, and risky, they are still impossible to replace or modernize.

Let's face it: many of these legacy applications aren't going anywhere, but the stakes of maintaining them grow higher almost daily.

Your audit should accurately assess the current risks these systems pose, as well as their growing risk over time in today's landscape.

Common Vulnerabilities

- *No native support for SSO or MFA*
- *Can't support modern use cases and methodologies*
- *Heavy maintenance burden and high technical barrier*

The Perils of Continued Support

For years, packaged applications like SAP, Oracle, and Sharepoint endeavored to push customers onto their cloud-based platforms by phasing out legacy products.

Though organizations promised continued support for legacy applications, they will soon stop investing in full-scale security upgrades and innovative features for them.

The tradeoff is, this continued support gave enterprises more runway to plan and execute their digital transformations. Before the pandemic, it was a tradeoff many organizations were willing to accept.

But today, this tradeoff might not work in your organization's favor. The rush of digitization widened the gap between your infrastructure's most modern systems and its most outdated ones.

The wider this differential, the more dangerous it becomes. What was once a chink in the armor is now a gaping hole.

The Homegrown Application Trap

When existing applications in the market can't meet your organization's specific needs or use cases, it's only natural to build them yourself. But homegrown applications take a lot of work to keep up-to-date and can quickly become a maintenance sinkhole.

Here are just a few of the reasons why:

- They were built to facilitate outmoded methodologies like waterfall.
- Updates must be performed manually, in a difficult-to-obtain maintenance window.
- Extending identity protocols like remote access, zero-trust identity checks, MFA, and SSO are difficult and costly to achieve.
- If the original coders have moved on, updating and securing your homegrown application becomes that much more difficult.

Legacy and homegrown applications are likely crucial to the functioning of your business. Unfortunately, the security stakes around them have risen substantially in recent years. Your next audit should accurately assess the risk of legacy applications in light of the post-pandemic “new normal.”

As your organization evolves, the gap between these legacy applications and more modernized parts of your infrastructure will grow wider until they eventually become untenable.

Your audit should suggest what that breaking point may look like and when it is likely to occur.

Air-Gapped Networks

Common in environments like manufacturing lines, financial services, energy, and military contexts, an air-gapped network is a system cut off from the internet and other networks.

Air-gapped networks offer security through isolation—they can only be accessed in person. Think of Mission Impossible (1996), when Tom Cruise's character drops down through the ceiling to physically access a terminal.

Audits often don't include air-gapped networks because we place so much faith in the air-gap approach. But conventional wisdom is starting to falter here, too.

No air-gapped system is totally isolated. As organizations strive to create more synergies between IT and OT, that bridge may compromise the security of your air-gapped networks.

More broadly speaking, OT systems are becoming a favored target among bad actors.

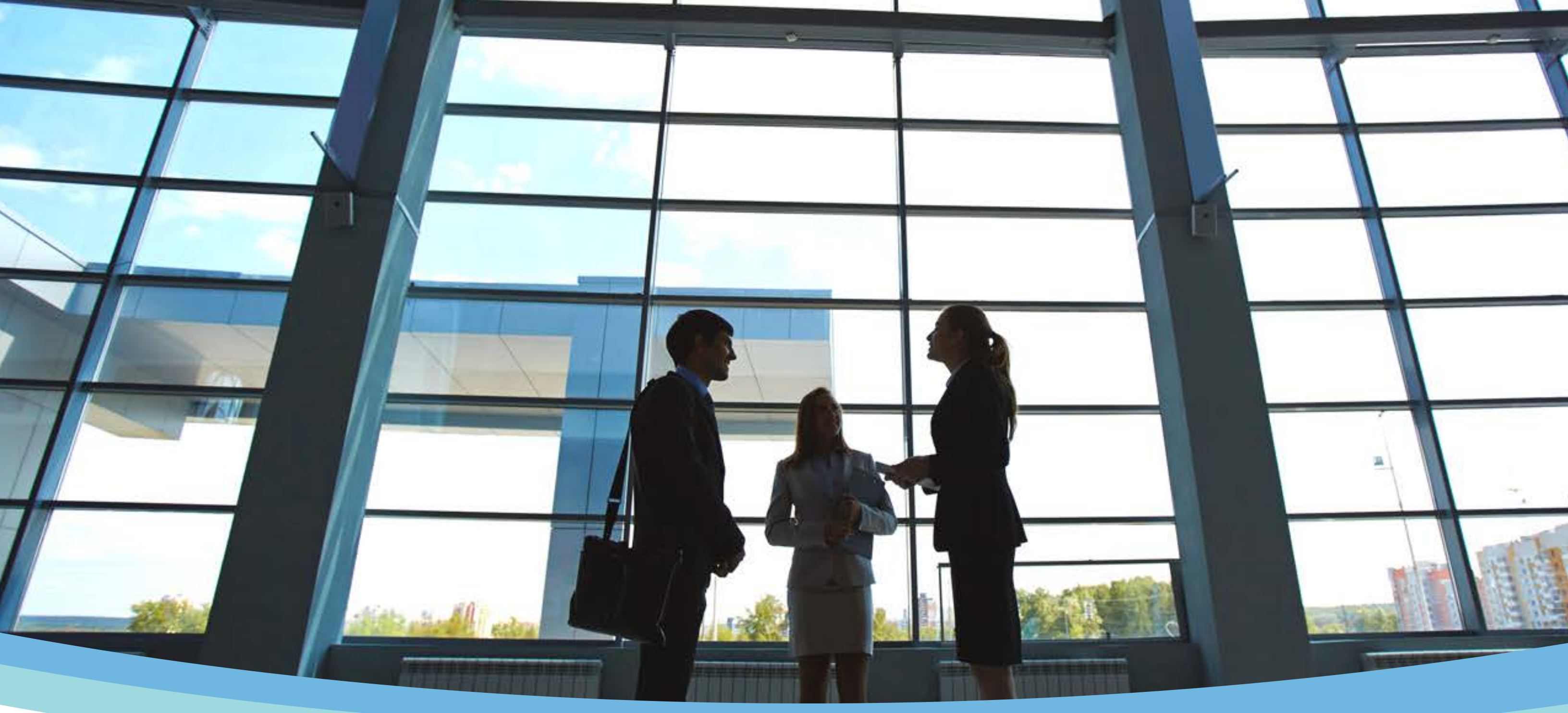
Once accessed, the tactics, techniques, and procedures for cyber-physical systems are incredibly easy to use, allowing an attacker to inflict damage quickly and easily.

In today's landscape, we must put our previous assumptions aside and interrogate even the most rigorous security controls.

As you conduct your audit, make sure to include air-gapped and other offline environments in your assessment.

Important questions to ask include:

- How are you reporting and monitoring access to your air-gapped networks?
- What layers of the Purdue model can external connections access?
- What are the potential cost-savings of enabling remote access to these systems?



Over-Permissioned Vendors & Third-Party Applications

The inside of your system's landscape is a crowded place. To enable or accelerate business operations, organizations hastily adopted a vast patchwork of third-party applications and vendors before and during the pandemic.

Now is the time to take a step back and ask, do you know who's who and what they have access to?

You're probably using more third-party applications than ever.

And business users are using a greater share of these applications than IT. What's more, 79% of third-party applications are never updated after being added to your codebase.

The security posture of these third-party applications can compromise your own. Each integration point represents a potential point of entry for a cyber attack, in addition to adding unnecessary systems complexity.

Vendors May Be Over-Permissioned with Admin-Level Access to Your Most Critical Systems.

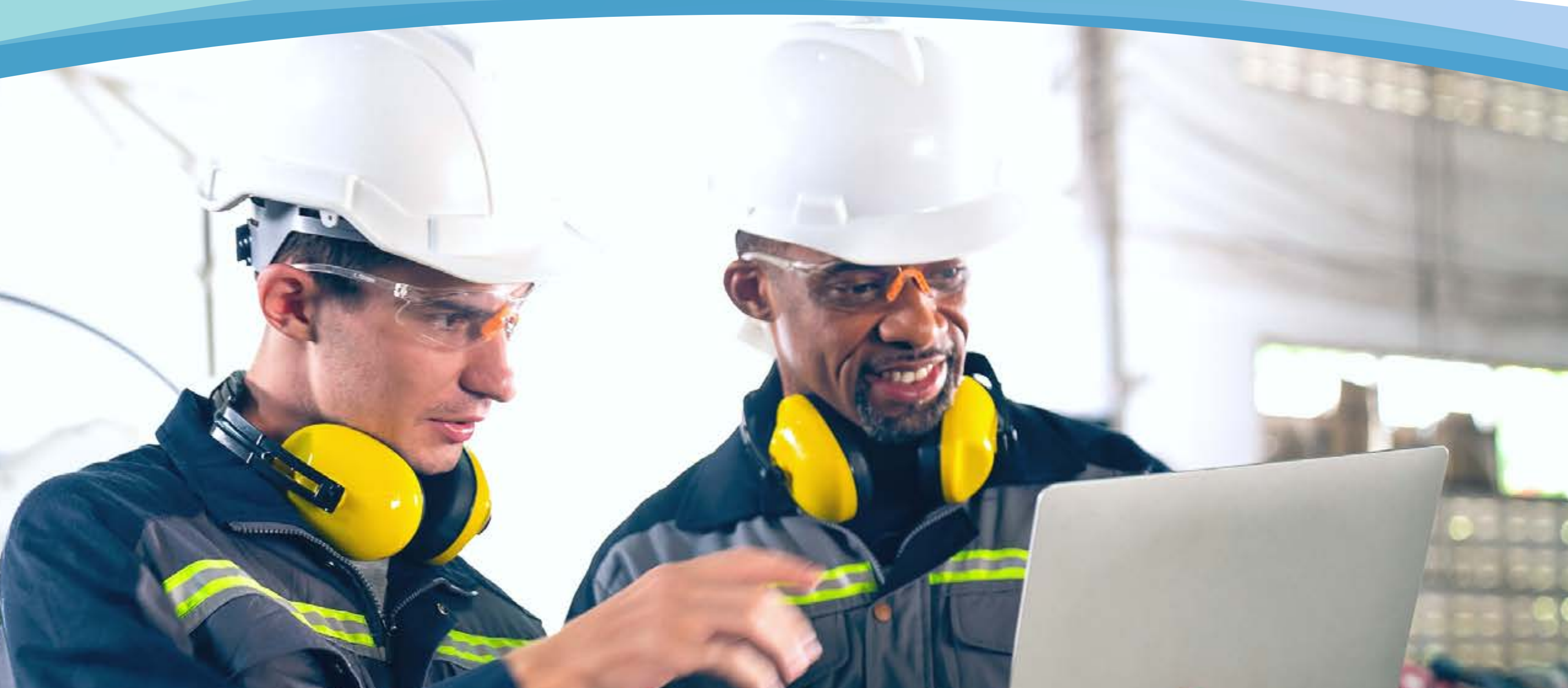
To get new vendors on-boarded and working toward your business goals as quickly as possible, they may have been granted inflated permissions or even admin-level access. A compromised admin account can wreak havoc on your entire system in a remarkably short period of time.

Active Directory needs to be maintained as vendors come and go with good onboarding and off-boarding processes in place. Otherwise, anyone who's ever been given credentials to your system can return or get hacked.

In your audit, take stock of all third-party users who still have a foot in the door of your infrastructure.

Inspection of firewall rules and Virtual Private Network (VPN) connections might reveal additional gaps in third-party security posture that should be closed.

Consolidate tools and applications when possible, tailor your vendor profiles according to the principle of least privilege (giving users no more access than what is needed to do their jobs), and outline a process for deactivating them once their work is complete.



Shadow IT & Problematic User Behaviors

Many organizations had a solid role-based access system in place, but when the pandemic sent everyone home to work, IT teams were forced to over-permission users to maintain business continuity.

Users don't work the same way.

No organization can say they resumed operations exactly as they were before. Users have more or different applications to tackle their work in new ways.

For instance, when users share accounts or use the same weak password across dozens of applications, it isn't done to spite your security strategy — they're just trying to be productive.

Security controls must reflect the real workflow of your organization's users, so use your audit to get a grasp of exactly how users are working.

Your audit should assess the exact level of access every role needs and offer a plan for implementing that schema in a way that facilitates productivity, rather than slows it down.

Shadow IT Is Simply a Reality.

When users work in the office on company-owned and monitored devices, IT policies can be easily enforced — but that isn't the world we live in anymore.

Users have taken their workflows beyond your network perimeter, to realms you can't always see, let alone control. In the comfort of their own home, on their devices, users are going to employ the tools they feel most comfortable with to get their work done.

Shadow IT is nearly impossible to fully prevent.

So, instead of asking how to stop users from deviating from your policies, ask why they deviate and what tools they are using most.

The answers will provide valuable insight into users' behaviors and preferences.

Your audit should capture these behaviors and consider adopting the tools that users most prefer using. By meeting them where they are, you'll mitigate deviation from policy (aka, risk).

M&A Activity

The financial uncertainty of the pandemic drove a higher rate of Merger and Acquisition (M&A) activity than we saw before 2020, and for businesses with strong balance sheets, M&A stands as a crucial component of any growth strategy.

From a security standpoint, M&A is a complex marriage of two previously independent systems. At worst, IT simply duct tapes the systems together, and at best, the identities and user profiles of the acquired company are duplicated in the acquirer's system. Either way, you're left with a conundrum of vulnerability and redundancy.

If your organization executed a merger or acquisition, your ability to perform due diligence may have been limited. Your end-of-year audit is the perfect chance to review these systems with a fine-toothed comb.

- How many identity providers do you use?
- How many other access management and network security tools are you using?
- Should you plan to federate these tools?
- Do you have duplicate user identities across multiple identity providers?

Your audit should account for these complexities and suggest strategies for fully integrating the acquired company into your systems.

Then, these recommendations can serve as the basis for evaluating future M&A possibilities.

People Are the New Network Perimeter

Securing your organization is no small order. You must:

- Manage the human element — the habits, preferences, and priorities of non-security stakeholders.
- Minimize the drastically expanded attack surface created by cloud technologies and remote work.
- Adapt to the emerging regulatory rigor of compliance mandates and cybersecurity insurance requirements.
- Recast security as a contributor to company-wide innovation, rather than a speedbump to progress.

If this year's audit is predominantly red, that's ok. Red is real.

To execute your go-forward security strategy, your audit must assess the current reality of your organization's posture.

The old conventions of the traditional network perimeter are never coming back.

People are the new perimeter, and the best way forward is to enable identity-based access that validates every digital transaction without imposing a drag on users' productivity.

We'd all prefer to wave a magic wand and instantly solve the conundrums of legacy applications and bad user behaviors, but it unfortunately isn't that simple.

Your audit findings and recommendations must be rooted in the hard reality of your organization. There's no use making a plan for the future that's based on incomplete or inaccurate data.

Digital Trust for the Real World

At Cyolo, we meet organizations where they are to extend modern security practices like MFA and SSO to every corner of the systems landscape.

Our solution is the only fully trustless zero-trust platform built for the realities of modern enterprises.

- Cyolo retrofits existing systems and processes to bring MFA and SSO to legacy applications, OT systems, and remote workers.
- Cyolo consolidates numerous identity providers into a single-click experience that secures users without adding steps to their process.
- Cyolo is the only zero-trust vendor on the market that you don't have to trust. That's right, even *we* don't know your password.

No matter where your organization is in its security or digital transformation journey, we'd love to help you achieve the benefits of identity-based access and connectivity.

Reach out to us [here to arrange a demo] or [visit our website] for more information.

About Cyolo

Critical assets and systems remain exposed because traditional secure access solutions have not been able to protect the legacy and custom apps that make up the last mile. Cyolo's purpose-built Identity-Based Access Control platform works alongside any and every existing security software to bring secure, frictionless and agentless user access to the edge. Within minutes of configuring, the last mile for IT, OT, and other critical infrastructures are protected with no change management. Now work can happen everywhere without compromising any security controls.

cyolo.io

Cyolo