Cyolo

What IT Teams Gain From OT-First Secure Remote Access

Table of Contents

When “Built for OT” Meets IT Reality

You lead IT at a large global manufacturer, and consistency is what keeps your world manageable. When every plant uses the same tools and processes, support is simpler, training and licensing costs stay under control, and security gaps don’t sneak in through local exceptions or one-off configurations.

As in many industrial organizations, your team has recently taken responsibility for OT security as well as IT. Maintaining consistency across both worlds is a new and difficult challenge.

OT environments have different priorities than you’re used to. Safety and uptime outrank everything, and any tool that affects system availability or slows down production will provoke resistance. You’re no longer surprised when OT engineers push back on traditional IT security solutions for being too restrictive, too slow, or too complex.

But their frustration doesn’t diminish the risk you’re tasked with managing. A single security misstep could quickly ripple across the entire business, and an OT incident would have the most serious consequences of all – possibly jeopardizing safety in addition to revenue.

So the minute a new request from OT reaches your desk, you’re immediately on alert.

A small lump rises in your throat as an OT engineer tells you excitedly, “I’ve found the perfect secure remote access solution. It’s built for OT and is a much better fit for us than the VPN we use now.”

You know better than anyone that VPNs aren’t perfect. They were never designed for the kind of large-scale, cross-site remote access that today’s industrial enterprises require. But still, they mostly work – and your team has spent years integrating your current VPN solution with your identity provider (IdP), your network, your SIEM, and all your meticulously tuned workflows.

When you hear “secure remote access solution built for OT,” your first thought is, “bad for IT.”

And you’re not alone in this concern. Many CISOs and IT leaders face the same challenge: balancing operational needs with hard-won IT stability. You want to support the OT team, but not by breaking what your own team has painstakingly built.

Fortunately, there’s good news: misalignment between IT and OT isn’t inevitable.

The right Secure Remote Access (SRA) tool can serve both team’s needs — equally and elegantly**.** It can reduce disruption and elevate rather than replace your existing firewalls and security stack, including network security, identity and access management, and SIEM tools.

That’s the principle behind Cyolo PRO (Privileged Remote Operations), a secure remote access solution for the cyber-physical world. **But while Cyolo PRO is designed to satisfy the distinctive needs of OT environments, it also provides IT leaders with greater visibility, stronger control, and fewer headaches.** It does this by building on the strong foundation you’ve already laid – instead of forcing you to rip it all out and start from scratch.

In this guide, you'll discover how an SRA solution made for OT can also advance IT's goals by helping you:

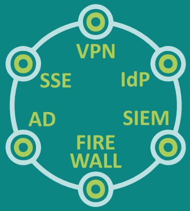
Deploy without network changes. Cyolo PRO fits neatly alongside your existing architectures, eliminating firewall rework, policy redesign, and other time-draining rearchitecting projects.

Avoid hardware refresh cycles. Lightweight, containerized deployment runs on what you already own, from edge compute platforms to virtual appliances, without new hardware purchases.

Enforce consistent identity governance across IT and OT. Use any IdP to extend identity governance into OT environments without requiring new directories, accounts, or workflows.

Reduce support tickets. Browser-based access and intuitive workflows let OT teams manage their own connections, dramatically reducing routine IT troubleshooting.

Centralize logging and oversight. Consolidate OT access activity into your existing SIEM for unified monitoring, investigation, and compliance reporting.



Leverage and even augment your existing enterprise security stack instead of ripping it out. Continue using the Active Directory (AD), IdP, VPN/SSE, and network tools your team already trusts for first-mile connectivity, rather than managing a parallel OT-specific set of technologies.

Lower operational and licensing costs. Simplify contractor access and reduce AD sprawl without adding new infrastructure or identity management burdens.

Strengthen overall cyber resilience. Consistent identity management, centralized visibility, and zero-trust access controls reduce lateral movement risk and contain IT incidents before they spill over into OT.

Now let's explore exactly what a modern, OT-ready SRA solution like Cyolo PRO can do for you and your team as IT professionals.

How IT Benefits from Secure Remote Access for OT

The team at Cyolo began with a straightforward goal: to create a remote access solution that minimizes both risk and disruption – and improves both security and operational efficiency.

This balance is what makes Cyolo PRO work for IT as well as OT.

Because modern OT security isn't just about enabling operators in the field to safely access critical resources. It also means giving IT the visibility, control, and operational stability needed to secure the entire enterprise.

After all, even if a tool meets every OT requirement, it will likely never be deployed if IT isn't on board. And getting IT on board means considering what you prioritize – consistency, visibility, governance, ease of integration and day-to-day use – even while developing features and capabilities focused around OT needs.

Simply put, a secure remote access tool built for OT should actively improve life for IT teams by reducing your workload, lowering the cost and complexity of managing identities, tightening governance, increasing cross-organization visibility, and strengthening cyber resilience.

Cyolo PRO does exactly this, proving that an OT-centric solution can deliver tangible benefits for IT and security teams as well.

Let's look now at a few of those benefits in more detail:

01 Reduced IT Workload

How much time does your team spend granting and revoking OT access, onboarding new users, or putting guardrails in place so third-party vendors don't leave your organization at risk? Probably more than you'd like.

And that's before you factor in a task that's even more time-consuming: network rearchitecting.

Most secure remote access tools (including those not specifically built for OT) require new firewall rules, new zones, or redesigned connectivity paths before they can even be deployed. Each one of those changes adds risk, consumes hours of planning and approvals, and increases the chance of misconfigurations. You also lose valuable time that you could be devoting to the other projects on your endless to-do list.

Cyolo PRO eliminates all of these burdens.

First, deployment does not demand network reworking or firewall restructuring – immediately removing a major source of IT overhead.

Learn More About Cyolo PRO Deployment

And following deployment, OT team can manage their own access needs without relying on IT to constantly configure connections and reset credentials. This is possible because Cyolo PRO's simple, secure design makes access intuitive and prioritizes ease of use and self-service.

The ultimate result for IT teams like yours is:

- Fast deployment with no network rearchitecting. Cyolo PRO works alongside your existing architecture, simplifying deployment, lowering the risk of misconfigurations, and preventing operational delays.
- Seamless user rollout. Users (both internal and external) access approved applications via a browser-based, self-service portal with no need for agent downloads or other installations that could require support and troubleshooting.
- Fewer support tickets and interruptions. Simple, agentless access minimizes day-to-day IT help desk requests.
- Simpler infrastructure management. Reduced firewall rules and streamlined configuration reduce the IT workload.
- A smaller attack surface. Identity-based, zero-trust access and stronger protocols minimize the weak points that IT needs to monitor and maintain.

- Faster user lifecycle management. Simplified provisioning and deprovisioning of user accounts, including potentially risky third-party vendor accounts, improves security and further reduces IT overhead.

When your ticket queue isn't filled with OT support requests, you get more time to concentrate on strategic initiatives that move the business forward. Plus, both IT and OT can rest assured that critical environments are accessed in a safe, secure, and controlled manner.

What makes Cyolo PRO so adaptable?

Cyolo PRO is a decentralized solution consisting of two distinct parts: The Identity Access Controller (IDAC) and a gateway, which can be either private or global. This unique architecture allows organizations to adjust access and security controls in the way that best fits their needs and network structure.

The IDAC

The "brain" of Cyolo PRO. This lightweight software component remains on-prem within the organization's trusted boundaries and holds all configuration, secrets, policies, and keys. The IDAC can be deployed in any environment and has no inbound connection, only a TCP 443 outbound connection to the gateway.

The Gateway

The point of access for users. The gateway can sit anywhere (on-prem, on-cloud, or both), allowing it to integrate seamlessly without requiring infrastructure changes.

Cyolo PRO is also designed with built-in high availability and failover. If the IDAC a user is connected through becomes unavailable, Cyolo PRO immediately and automatically reconnects through another available IDAC. As long as another IDAC is reachable, the user session continues without requiring reauthentication. This redundancy ensures continuity, reliability, and consistent security.

02 Better Visibility and Reporting Capabilities

Letting go of day-to-day OT access responsibilities doesn't mean that IT teams are cut out of the loop completely. To ensure security across the organization, it's crucial to know who's connecting to the OT network and what they're doing while connected.

Unlike VPNs and other traditional SRA tools that only protect the initial point of access, Cyolo PRO includes session monitoring, recording, and logging capabilities to secure each connection from start to finish. This gives everyone more visibility into what users are doing inside your OT environment. And, most importantly for IT teams, it's easy both to add more controls and to track user activity.

With Cyolo PRO, you get:

- **SIEM integration.** Connect seamlessly with Splunk, QRadar or any existing monitoring platform to see all logging and telemetry data in one place.
- **Identity-linked logs.** Every action maps back to a verified user for complete traceability. No more wondering who's the actual identity behind Operator1.
- **Credential vaulting.** Cyolo PRO's built-in vault eliminates the risk posed by weak or shared OT credentials.

Visibility, Control, and True Zero Trust Make Compliance Smoother

Gaining clearer visibility into how users access OT systems doesn't just boost security – it also simplifies the work of evaluating, proving, and maintaining compliance across regulatory and security frameworks.

Secure, Auditable Data Handling and Storage

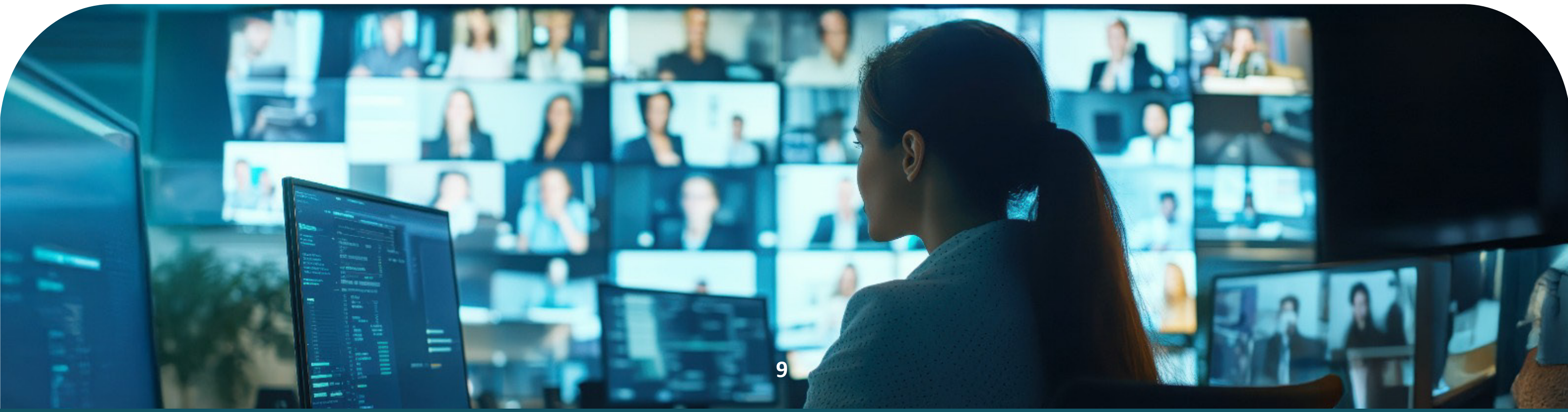
Cyolo PRO adheres fully to the zero-trust security model.

The solution's decentralized architecture keeps all identities, policies, and secrets inside your trusted boundaries and under your control. This eliminates the risk of exposure if Cyolo were to be breached and makes it easier to demonstrate compliance with identity governance requirements and data protection standards like GDPR and the California Consumer Privacy Act (CCPA).

Stronger Authentication and Credential Management

Identity-based access, multi-factor authentication (MFA), and credential vaulting with secure injection help organizations meet key controls required by SOC 2, NIST CSF, ISO frameworks, and other compliance programs.

Cyolo PRO ensures every user action is tied to a verified identity – providing clean, auditable records for internal and external assessments.



03 Lower Burden of Managing Contractors, Plus Cost Savings

Contractors and OEMs are essential to OT operations, but managing them directly in AD is complex and risky – not to mention, expensive. Every extra license drains both budget and time.

With Cyolo PRO, you can:

- **Create a dedicated OT directory for vendors and service providers,** enabling easier management of third-party access and eliminating the need for additional AD licenses.
- **Automate the previously manual work of creating, provisioning, and managing users** by integrating Cyolo PRO with your existing third-party directories.
- **Instantly revoke access** when contracts end or accounts go dormant.

The result is, again, less work for IT as well as less strain on your budget, plus a significantly easier and more secure way to manage and monitor access for third-party vendors.

04 Protection of Critical OT Systems from IT Security Incidents

Despite all the hard work IT teams put in, misconfigurations, malware, and credential compromises still happen. In critical industries like manufacturing or energy & utilities, it's vital is to contain these issues so that an IT problem is never able to take down OT operations.

Yet in many organizations today, a single misconfigured VPN or compromised admin credential on the IT side can create a direct pathway into the OT environment. That's often all an attacker needs to move laterally into production systems and cause real, physical damage.

With the right access architecture, that pathway simply doesn't exist – keeping critical OT infrastructure protected even in the case of an IT incident.

Cyolo PRO makes this possible by separating the control plane from the data plane. This isolates the two environments and prevents an IT breach from becoming a company-wide outage. IT teams maintain oversight across both domains – and gain the peace of mind that an IT security threat won't spill over into OT.

So… What Does an IT-Friendly OT Security Tool Look Like?

As attacks on OT intensify and IT teams take on greater responsibility for OT security, the benefits outlined above are shifting from “nice to have” to essential. Clearer visibility, consistent identity controls, and stronger containment between IT and OT aren’t optional when you’re accountable for safeguarding both digital and physical operations.

But not all SRA solutions can provide these benefits. Some tools offer remote connectivity for operators yet create more work for IT through network redesigns, rigid infrastructure requirements, complex integrations, or fragmented identity models. Others may satisfy OT workflows but fall short on identity governance, auditing, and centralized control – leaving IT with blind spots and added operational risk.

This is why solution architecture matters. The right design will reduce IT burden and strengthen overall enterprise security; the wrong one will magnify inconsistencies, increase costs, and introduce potential new attack paths.

When evaluating any SRA solution built for OT, IT leaders should look for these key architectural principles:

01 No Network Changes – No Rebuilds, No Added Risk

For IT security leaders, architectural change equals risk and potential downtime. Every firewall modification or new tunnel introduces potential misconfigurations, human error, and compliance drift. Plus, network changes can cause small latency increases in time-sensitive industrial systems. Even a delay of a few milliseconds may activate safety mechanisms that shut down production.

Given that most remote access solutions require some level of network reconfiguration, it’s no wonder that IT teams often prefer to stick with the status quo. And, for what it’s worth, OT teams aren’t typically thrilled about change either, as it’s usually slow and disruptive to their established processes and routines.

Faster user lifecycle management. Simplified provisioning and deprovisioning of user accounts, including potentially risky third-party vendor accounts, improves security and further reduces IT overhead.

When your ticket queue isn't filled with OT support requests, you get more time to concentrate on strategic initiatives that move the business forward. Plus, both IT and OT can rest assured that critical environments are accessed in a safe, secure, and controlled manner.

To overcome these key hurdles, Cyolo PRO was designed to sit *alongside* your existing architecture, not *inside* it. Your firewalls, network policies, and other configurations stay intact and untouched – while Cyolo PRO adds an extra layer of protection and visibility.

It's like an adaptable, invisible suit of armor that protects what's underneath without disturbing or disrupting the core.

This allows you to:

- Maintain your existing network and tech stack – no re-architecting required.
- Avoid configuration-related downtime and human error.
- Gain visibility into who's accessing OT systems without compromising IT's governance model.
- Use existing network tools like MPLS, SD-WAN, or SSE to connect to OT more securely than their native capabilities allow

02 Deploy Anywhere – Full Flexibility, No New Hardware

Deployment flexibility is more than a matter of convenience for IT teams. It also directly affects cost, scalability, and long-term operational stability. But many SRA tools tie you to proprietary appliances, fixed virtual machine (VM) footprints, or costly cloud dependencies.

In stark contrast to the usual model, Cyolo PRO is delivered as a lightweight, containerized component that can run virtually anywhere: on an application server, a virtual appliance, or even a physical appliance when a black-box form factor is required. And because it's containerized, it can be clustered for high availability and performance.

This deployment flexibility gives you several meaningful advantages:

- **No hardware plans or refresh cycles**, eliminating cost, disruption, and procurement delays.
- **Runs on existing infrastructure,** including edge compute platforms, switches, routers, and firewalls.
- **Easy to scale.** Cluster as needed for performance or high availability.
- **Lower total cost of ownership**, with no new compute budget required just to begin deployment.
- **Faster rollouts everywhere**, from isolated plants to cloud-connected sites.

03 Retain the Tools You Trust – Integrate Without Disruption

IT teams like yours have spent years or even decades finding the right products and perfecting the processes that keep your business running. This includes first-mile connectivity tools like MPLS, (SD)WAN, ZScaler, Citrix, and other VPNs.

So, it's more than a little frustrating when an SRA solution requires its own end-to-end connectivity and can't integrate easily with your existing ecosystem of connectivity tools.

Cyolo takes a different approach that allows IT teams to keep their familiar tools and workflows. The Cyolo PRO solution activates only when a user crosses from an IT setting into the OT environment. Up to that point, your existing first-mile connectivity tools operate exactly as they always have.

Whether your organization relies on cloud-native connectivity or more traditional network setups (or both), Cyolo PRO adds secure, identity-based access beyond the first mile – all without disrupting your current tech stack or work routines.

This lets you:

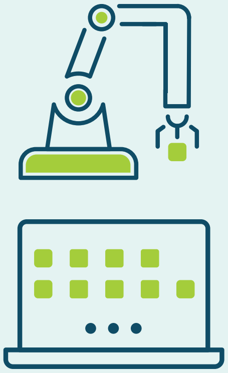
- Preserve existing connectivity strategies and vendor relationships.
- Prevent expensive "rip-and-replace" projects or retraining cycles.
- Enhance your overall security posture with zero-trust access controls past the first-mile boundary.

04 Add Visibility and Control While Enabling OT Autonomy

IT and OT teams work differently – and that's okay. Trying to force both into a single operational model leads to friction and can even introduce new security risks. Still, many traditional remote access platforms lock everyone into a rigid structure that doesn't fully satisfy anyone.

IT/OT Misalignment in Action

IT teams typically want to enforce a single, cloud-based VPN or remote desktop gateway for all users. From your perspective, this centralization simplifies management, enforces consistent identity controls, and aligns with corporate cybersecurity policies.



But for your OT colleagues, this same solution can be problematic. A cloud-based VPN may not meet latency or uptime requirements for critical control systems. It might require software agents that can't be installed on legacy HMIs or engineering workstations. And perhaps worst of all, it can expose too much of the network, giving remote users broader access than they need and increasing the risk of lateral movement and downtime.

OT engineers are left frustrated and either disconnected from critical assets or else forced to work around the system entirely – undermining both productivity and security. And even while IT got its desired tool, policy exceptions from the OT side pile up, adding to an already towering workload.

Ultimately, no one is happy, and security is not measurably improved.

Unlike conventional remote access tools that force IT and OT to conform to a single way of working, Cyolo PRO is designed for both worlds. IT gains a complete, centralized view of who can access what across the organization, while OT retains autonomy over how access is granted and governed within their environment.

Cyolo PRO's unique multi-tenant architecture allows IT and OT to operate independently within a shared security framework. IT retains the master tenant, enforcing enterprise-wide identity controls such as MFA, password policies, and centralized user lifecycle management. Meanwhile, OT teams manage their own sub-tenants, defining granular access policies based on local workflows, operational constraints, and safety protocol – without having to create, maintain, or remove user accounts.

Cyolo PRO also integrates seamlessly with any IdP, or even multiple IdPs simultaneously. This enables IT and OT users to authenticate using their existing identities, while access policies remain decoupled from the identity itself. For third-party vendors, IT can decide which IdP they authenticate through – or connect Cyolo PRO directly to the vendor's IdP – without introducing long-lived local accounts into OT systems.

By separating identity from access and policy, Cyolo PRO eliminates one of the most persistent governance challenges in OT environments: orphaned or over-privileged accounts. Even if a user or vendor account still exists in an external IdP, access can be removed instantly by policy, ensuring no residual connectivity to critical assets.

In practice, all of this means:

- **IT gains visibility and maintains policy control**, enforcing consistent security standards enterprise-wide.
- **OT teams gain the ability manage their own access controls** and follow their validated workflows independently – even in air-gapped or latency-sensitive environments.
- **Both teams eliminate manual overhead** from external user management, remote access workflows, and JML (Joiner, Mover, Leaver) processes.

With Cyolo PRO, multi-tenancy isn't just a feature – it's a philosophy: control for IT, autonomy for OT, and efficiency for everyone.

05 Extend Existing Identities Into OT

Identity management is often the hardest and riskiest part of deploying a new access tool. Manual migrations invite configuration errors, prolong go-live timelines, and create compliance headaches.

Cyolo PRO eliminates both the friction and the risk by automatically and securely transferring federated identities from Okta, Microsoft Entra ID, or Active Directory across cloud, on-premises, and hybrid environments.

From day one, OT assets align under the same zero-trust-based identity, access, and compliance controls as IT, with no new directories or user mappings to maintain.

Simply stated, Cyolo PRO gives you a unified identity and governance framework that accelerates rollout timelines, minimizes operational overhead, and maintains policy consistency across the enterprise.

Added Bonus: Keep Your Existing File Scanning Tools – Or Use Cyolo's

In addition to integrating smoothly with any IdP, Cyolo PRO can work with the file scanning tools you're already using today. This removes the need to log in and out of multiple tools and lets you scan every file across OT and IT using the same process.

And if you don't currently have an OT file scanning solution in place, Cyolo PRO's file scanning capabilities – available via an ICAP integration.

Cyolo PRO, the OT SRA Solution That Moves IT Forward

The future of secure remote access (and cybersecurity more broadly) isn't about choosing between IT and OT needs. It's about aligning them.

And crucially, "built for OT" doesn't have to mean "bad for IT."

With the right architecture, an OT-first secure remote access solution can meet the specialized needs of industrial operations and provide measurable benefits for IT and security teams.

The Cyolo PRO remote access solution demonstrates this in practice. It preserves your existing IT architecture and tool stack, extends identity and governance into OT systems without adding complexity, and applies zero-trust access controls consistently across the enterprise. Cyolo PRO also reduces day-to-day administrative workload, prevents IT security incidents from spreading into OT networks, and gives OT teams safe, stable access that never compromises uptime or safety.

With Cyolo PRO, "built for OT" becomes a strategic win for IT. And in a world where connectivity, remote operations, and cyber-physical risks are now the norm, that's exactly the kind of alignment IT and security leaders need to move their businesses forward.

About Cyolo

Cyolo provides secure remote privileged access for cyber-physical systems (CPS). Our solution enables industrial enterprises to simply connect employees and third-party vendors to critical assets.

Cyolo meets the needs of security and operational technology (OT) teams with a solution that's adaptable to any environment and includes capabilities such as privileged access controls, zero-trust connectivity, identity-based access for legacy systems, and centralized management across multiple sites.

Cyolo offers stronger security and more control than traditional secure remote access (SRA) and deploys without causing disruptions or requiring change management. Cyolo delivers improved security, productivity, and operational agility – without compromise.

To learn more, visit CYOLO.IO