Cyolo

The Manufacturers' Guide to Secure Remote Access for OT

8 Tips for Choosing a Future-Proof Solution

Secure Remote Access for OT: Everything You Need to Know Before Selecting a New Solution

Manufacturing is evolving, fast. Digitalization, automation, remote connectivity, and increased interfacing between information technology (IT) and operational technology (OT) are driving huge opportunities for manufacturers.

72% of manufacturers are actively pursuing IT/OT convergence.[1]

55% have increased their security budget for industrial controls systems (ICS) and OT, with the biggest spend on defensible network architecture.[2]

But, like with all technological revolutions, new challenges – and in this case, new security risks – have also emerged.

Manufacturing is the #1 target for cyberattacks, making up 26% of all global attacks – more than any other sector for three years straight.[3]

60% of manufacturing companies have already been hit with an attack – at an average cost of $1 million per breach.[4]

As Internet of Things (IoT) adoption surges, risks are continuing to climb – with a 30% increase in security incidents.[5]

As manufacturers strive to address growing cybersecurity threats, too many are taking security solutions built for the world of IT and trying to force them into the OT environment. In the end, this creates a messy and ultimately ineffective patchwork system full of security gaps.

But fear not, because there is good news! **With the right Secure Remote Access (SRA) approach and solution, your organization can enjoy the many benefits of connectivity – all without exposing your OT environment or the critical systems within it to unnecessary danger.**

The first and most crucial point to determine before you commit to an SRA platform is whether the solution is designed specifically for OT.

An SRA solution built for OT will address the realities of your OT environment as well as your unique priorities. Security matters, of course. But so do safety, operational agility, productivity, and real-world usability.

Why Choosing a Secure Remote Access Solution Built for OT is Critical

Why is it so important to choose an SRA solution that's purpose-built to overcome OT challenges?

Just think – would you use a wrench to hammer in a nail? Technically it might work, but it's not what it was designed for – and it may even cause damage in the process.

In the same way, IT-built remote access tools might seem like they can handle OT needs. In reality, however, they're not fit for the job – and are likely to leave you more frustrated than satisfied. Here are just a few of the reasons why:

They don't prioritize availability: IT security tools almost always require downtime for patching and upgrades. In manufacturing and the broader OT world, systems availability is essential. Even a short period of downtime could cause chaos for a plant, so such solutions are far from ideal.

They depend on cloud connectivity: IT security solutions often rely heavily on the cloud. However, OT systems aren't always connected to the internet, and some compliance mandates may prohibit cloud connectivity. As a result, tools requiring a cloud connection will provide patchy coverage at best for OT environments.

They're not adaptable to OT needs: OT environments tend to be highly complex, and IT security solutions often struggle to adapt to their unique configurations, requirements, and compliance needs.

Security policies are typically implemented with the best of intentions. But **forcing OT teams to access systems and resources using IT solutions can lead to more problems than it solves** – from clunky interfaces that irritate users, to operational disruptions that create ever-widening security gaps.

This is why choosing an SRA platform built for OT - rather than an IT-focused tool shoehorned into the OT environment – is vital.

But how do you know you're getting a solution that's made for OT and will truly meet your needs?

It starts with asking the right questions.

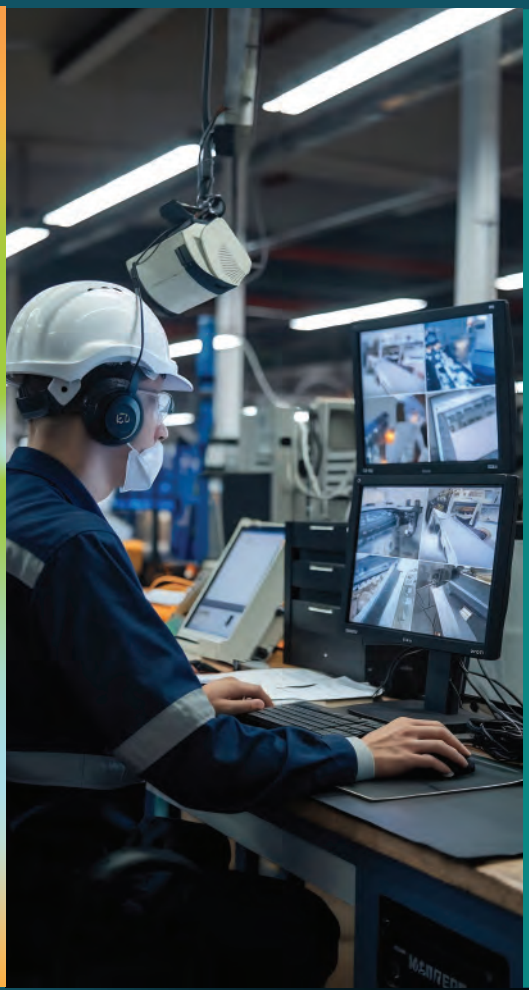
This handy guide breaks everything down into eight essential questions to ask before making a decision – so you can invest with confidence and start seeing real results. Let's begin!

But First: Why Privileged Access Matters (A LOT) in OT Security

As you go through this guide, you'll notice one phrase popping up again and again – **privileged access**.

That's no coincidence.

In IT, privileged accounts usually bring to mind system admins. But in OT, and specifically in manufacturing, the list of privileged users goes far beyond that – likely including third-party contractors, remote employees, and even on-prem operators directly accessing key production systems or other critical resources.



Why securing privileged access matters:

Privileged access = direct access to your most critical systems and assets.
The fewer people who have it (and the better protected they are), the better.

The compromise of privileged accounts can spell disaster.
Most of today's cybercriminals aren't brute-forcing their way in – they're stealing your credentials via phishing, social engineering attacks, and other advanced techniques. And if they gain control of a privileged account, they could potentially manipulate machinery, disrupt production, and even endanger lives.

Securing just a tiny fraction of your users can make a mountain of difference to your risk mitigation. Some estimates suggest that privileged accounts typically make up around 10% of the user base but can account for up to 90% of risk. This means that ensuring secure access for privileged users and devices will deliver huge results for your organization with minimal investment.

Simply put, an SRA solution shouldn't just control who gets in. It should prioritize securing privileged access scenarios from start to finish and make these connections seamless, secure, and efficient.

The right platform will ensure that the people who need access get it – fast, safely, and without friction – while keeping everyone else locked out.

Managing remote privileged access isn't just a security checkbox. It's the key to protecting your OT environment from both external and internal threats.

Did you know? Securing instances of privileged remote access is so crucial that in December 2023, Gartner® introduced a new solution category: Remote Privileged Access Management (RPAM).[6]

The key features of RPAM are divided into 4 areas:

1) Identity administration

2) Authorization and least privilege

3) Access and authentication

4) Recording and auditing

A robust RPAM solution will allow organizations to more effectively manage the entire lifecycle of a privileged remote connection – from the initial verification of identity through to the termination of the session.

Ask These 8 Questions to Find the Perfect Secure Remote Access Solution

01

ONE

Will it work in any environment – or just add another solution to your towering security stack?

02

TWO

Can you deploy it without infrastructure changes?

03

THREE

Does it provide controls for connectivity, oversight, *and* access?

04

FOUR

Does it secure the legacy systems you depend on?

05

FIVE

Does it deliver true zero trust – or is your security vendor a security weak spot?

06

SIX

Does it improve operational agility, not slow you down?

07

SEVEN

Does it boost productivity – or give you more work?

08

EIGHT

Will it scale with your manufacturing operations – or leave them feeling bloated?

01 Will it work in any environment – or just add another solution to your towering security stack?

For various reasons, most manufacturing organizations have a number of different access solutions in their current tech stack. But adding a new tool to fulfill each specific access need that arises can feel like building a house of cards on a windy day – fragile, risky, and bound to topple sooner or later.

In the past, there was no good alternative to this cobbled-together leaning tower of secure access tools. Today, there's a much better way.

The ideal SRA solution will be deployable in every type of environment, eliminating the need to juggle multiple tools for different setup scenarios.

Already migrated some applications to the cloud? Great.

Have a few systems you prefer to keep on-prem only or even entirely offline? No problem.

There's absolutely no reason to move to the cloud, change IP addresses, or overhaul your existing architecture just to enable secure remote access.

In short, your SRA solution should work seamlessly across all environments – on-prem, cloud-connected, and offline. This isn't just common sense – it's also the only way to gain a full picture of what users (and especially privileged users) are doing inside your systems.

Choosing an adaptable solution today helps you prepare for the future.

No one knows exactly what the future of manufacturing holds. A generation ago, the ability to control operations remotely was the stuff of science fiction.

The only certainty is that your systems architecture will continue to evolve. Your security should, too. Instead of tacking on a new solution every couple of years, why not invest now in a flexible SRA tool that will evolve with you?

The shift is already underway: 37% of automotive manufacturers are planning cloud adoption in the next five years, and 16% are already seeing ROI from their cloud and SaaS investments by improving connectivity and efficiency in their plants.[7]

By choosing an SRA solution that's adaptable across all environments, you can simplify your overall remote access strategy, gain unprecedented cross-system visibility, and prepare for whatever systems architecture the future may hold.

02 Can you deploy it without infrastructure changes?

Nothing slows down operations like a forced overhaul. When a new security solution requires massive adjustments to your existing infrastructure, it's frustrating as well as risky.

Plus, isn't it a little presumptuous of a vendor to ask you to change just to accommodate their product?

The right SRA tool will adapt to your needs, not the other way around.

Production disruptions? Not an option. Large-scale changes almost always mean downtime. And in manufacturing, that's a direct hit to productivity, efficiency, and profitability.

Safety risks? Unacceptable. ICS/OT environments, unlike IT systems, interact with the physical world. This makes them uniquely vulnerable to threats where a security incident can cause potentially dangerous operational failures, environmental damage, or even put lives at risk.[8]

Human error? A major threat. We humans aren't great at handling change. Change leads to stress, which then leads to mistakes. In manufacturing, 70% of breaches stem from internal vulnerabilities – primarily, human error.[9] A complicated, disruptive product rollout only adds to that risk.

When a new solution integrates seamlessly with your existing systems, you see results faster while avoiding deployment headaches. You also get these additional benefits:

Transition at your own pace. Don't get forced into cutting the cord on existing systems before you're ready. And on the other hand, gain the flexibility to replace tools that may no longer be needed.

Scaling made simple. Beyond fast, frictionless deployment, an adaptable SRA solution built on a decentralized architecture can grow or contract alongside your business.

Less disruption, lower stress, faster ROI. Teams stay focused on their jobs, not wrestling with new tools.

The best security is seamless, simple, and stress-free – because safety, efficiency, and productivity should never be a trade-off.

What do we mean by 'decentralized architecture'? Rather than relying on a single centralized point to manage access or data flow, decentralized architecture is spread across multiple gateways or nodes. The best part? A solution built in this unique way has no single point of failure and no single point of compromise. This gives you stronger security against attackers – thanks to encrypted data and zero visibility across your wider system – plus faster connections for users, who can be automatically rerouted to another gateway without disruption.

03 Does it provide controls for connectivity, oversight, *and* access?

Letting someone into your network with access controls but no oversight is like intensely screening them with James-Bond-level fingerprint, retina scanning them at the door… and then giving them free rein to rifle through anything they find inside.

Yet, that's exactly what happens with many remote access solutions – they focus on getting users inside securely, but fail to offer any control over what happens next.

But going to all the trouble of securing the point of access makes little sense if you won't have any visibility or control during the actual connection.

Sure, SRA might have 'access' in the name, but you need a tool that provides more than just access.

When you're responsible for securing critical assets and keeping production lines moving, your SRA tool simply must be able to secure full remote connections from start to finish.

After all, in manufacturing, unauthorized access isn't just a data risk. A breach could disrupt operations, harm the environment, or even endanger lives.

This makes oversight controls crucial for security – and also for ensuring compliance with many industry and regional regulations.

So, look for an SRA solution that puts you in control of what users can and cannot do while they're connected:

Centralized management. Know exactly who's accessing your systems, exactly what they're doing, and when they're doing it– in real-time, across all systems and environments.

Supervised access. Maintaining a record of all connections is often required for compliance, and can also be extremely beneficial during incident response efforts.

Action policy controls. Visibility into what users are doing while connected is key, but actual control over their activities is even better. The right solution will allow you to restrict or block risky behaviors by a privileged user during a session – such as uploading or downloading files, using the clipboard (copy/paste), or activating a webcam.

To ensure the highest possible level of security, your SRA solution should give you full control not just at the point of access, but for the entirety of the connection.

Want an example? One global food and beverage giant implemented automatic session monitoring across their OT systems. The results? Their security team went from receiving 1.5 million alerts to just a handful each day, discovered and triaged over 30 OT ransomware infections, and protected over $42 million of revenue by remediating compromised assets.[10]

04 Does it secure the legacy systems you depend on?

The IT world is all about racing to find and adopt the next-big-thing in technology, with companies who embrace the latest flavor of the week phenomena often earning the biggest competitive advantage.

But, at least in this particular sense, OT moves at a slower pace.

Your factory very likely depends on at least a couple systems that haven't been updated since the previous century. And for the sake of keeping your operations running, such legacy systems aren't going anywhere – they remain essential for your day-to-day operations, even as they pose a growing security threat as a vulnerable point of entry for attackers.

But unfortunately, most security vendors and solutions don't handle legacy OT very well. They expect you to upgrade everything or just accept the risk. Neither is a good option.

Updating or replacing legacy infrastructure with more modern systems isn't realistic in most cases. But why should that mean you have to live with the risks?

Your best option? An SRA solution that retrofits your legacy systems to accommodate modern security protocols, draping them in protection without infrastructure updates or production slowdowns.

And let's not forget: some of the most vulnerable connections in your entire environment are the privileged ones into legacy systems. These high-risk access points are prime targets for attackers – and without the proper protections in place, they're wide open.

Securing these connections isn't just important – it's critical.

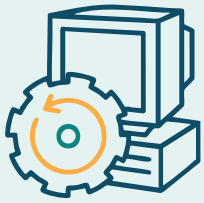
So look for a solution that provides:

MFA for identity verification. Your SRA solution should be able to overlay common legacy manufacturing systems, adding identity-based authentication and other security best practices without major upheaval.

Security that works within your whole setup. In the same way that an SRA tool should be deployable in any environment, it should also be able to enforce identity-based authentication to every type of system - from your newest cloud-based apps to the dependable old mainframe still handling inventory management.

Cyberattackers are betting that you'll treat security for your legacy OT systems as an afterthought. Don't prove them right.

Instead, secure every part of your environment, without ever forfeiting productivity for protection.



Did you know?

Most legacy OT systems don't support modern identity authentication – a key requirement for remote privileged access management (and also for many compliance mandates)! The right SRA solution will sit on top of your legacy systems, securing privileged access scenarios without updates or disruptions.

05

Does it deliver true zero trust – or is your security vendor a security weak spot?

Ever had a vendor promise zero trust, only to then demand full access to your data? Forget zero trust – that's zero *logic*.

Let's get the facts about zero trust straight:

Zero-trust access means:

Identity-based verification, not IP-based. IP addresses can be shared, spoofed, or compromised. When zero-trust access is enforced, users are verified according to their identity, not their location or IP address.

Least privilege = maximum security. Zero-trust security is built on the principle of least privilege, meaning users and devices get access to only what they need – nothing more. This is especially important in OT, where privileged accounts need access to operate and control mission-critical systems.

No full-network access – *ever.* A zero-trust access solution provides application-level access, not blanket network access, to minimize exposure to ransomware and other malware that can quickly spread across an open network. This is a crucial step in protecting instances of privileged access, preventing unauthorized users from gaining dangerous network-level access.

Trust no one – including your vendor. If a vendor claims to offer zero-trust security but then asks you to hand over your secrets, that's a big red flag. A true zero-trust architecture means you own and control your sensitive information – not your vendor or any other third party.

Vendors that request your passwords or encryption keys don't have malicious intentions for your data – they most likely just overestimate their own security capabilities or don't see themselves as part of the zero-trust ecosystem.

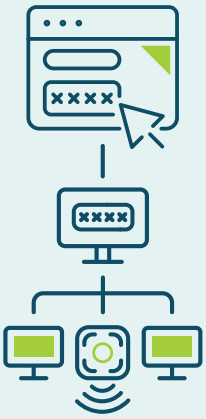
But security vendors should know better than anyone that every organization has vulnerabilities.

When vendors break the zero-trust model by holding and storing sensitive customer data, that data is left at serious risk of exposure if the vendor is breached or otherwise attacked. And why would you work with a security vendor who's going to increase your risk?

One sub-industry that's no stranger to cybercriminals is food and beverage manufacturing. With a combined annual revenue of $3 trillion across the US[11] and EU[12], it's an attractive target for cybercriminals. Any vendor that pools sensitive data from their food and beverage customers all in one place creates a tempting buffet of opportunity for threat actors – one that's often too tempting to ignore.

To take that buffet off the table, manufacturers need an SRA solution that goes beyond perimeter security and enforces strict zero-access controls, like:

- **Multi-factor authentication (MFA)** to help keep unauthorized users away from sensitive systems.
- **Continuous authorization** throughout the entire connection for added security.
- **Application-level access** (based on the principle of least privilege) to limit lateral movement inside the network.
- **Keeping all sensitive data and secrets within the organization's trusted boundary** to prevent access or unintentional exposure by the SRA vendor.
- **Alignment with manufacturing industry standards**[13] like NIS2, IEC 62443, and EU Machinery Regulation 2023/1230.



Need a scenario in context? Let's say you're a global manufacturer. Instead of granting network-wide access via VPN, you implement a zero-trust architecture that enforces application-level access for privileged users, like remote maintenance engineers. This lets you authenticate each user through identity-based controls, before granting access only to the specific HMI or SCADA system needed for their work.

Voila! You've now limited lateral movement within the network, preventing unauthorized access to other production systems and drastically reducing the attack surface.

06 Does it improve operational agility, not slow you down?

Remote access should make your operations smoother and faster rather than creating additional friction and slowing you down.

If an SRA tool makes it harder to carry out your essential work, chances are it was not built for OT. It's probably an IT-focused solution with a couple of OT capabilities stuck on afterward.

The SRA solution you're looking for will fit into your OT environment seamlessly and boost your operational agility in some – if not all – of the following ways:

Simple to deploy and scale. An adaptable solution that doesn't require major infrastructure changes will be a game-changer for the teams responsible for deployment and scaling. Agentless deployment is another bonus – so nobody's stuck installing and updating software on every device in the organization.

Easy to manage every day. No one has time for a tool that creates more work than it saves. The right SRA solution won't pile extra tasks on supervisors and IT teams.

One dashboard for less hassle. When users can access all the systems and applications they need via a single dashboard, that means more time doing actual work and less time searching for MFA codes (or screaming internally when it takes 5 log-ins to access a single resource).

User experience that's so good, you don't even notice it. A clunky interface doesn't just turn security into a migraine – it also leads users to find unauthorized and possibly problematic workarounds. A well-designed UI, by contrast, makes it easy to get work done – without IT constantly stepping in. That's fewer support tickets and happier teams.

Visibility and control, minus the friction. It's not only access your SRA solution should provide – it's also visibility and control over what users are doing once they're inside your critical systems. Need to monitor privileged connections in real-time for compliance purposes? Or want to make sure third-party vendors can't copy or paste data within certain sensitive systems? The right platform will include a range of easy-to-manage connectivity and supervisory controls in addition to standard access controls like MFA and continuous authorization.

AI-powered efficiency. Granular controls are great, but not if they overwhelm admin and support teams with endless manual tasks. A modern SRA solution should reduce manual work, enabling you to instantly see who's accessing what, flagging suspicious activity, and giving you better security, accountability, and compliance-readiness. This also gives security teams more time to focus on tasks that AI can't assist with. Whether it's through smart automation or AI-driven security features, your SRA should help you stay ahead of threats – without the extra legwork.

The bottom line? **Your SRA platform should adapt to your workflow, keep your critical assets secure, and then get out of your way – allowing you to work smarter and safer than ever.**

Did you know? 80% of all OT outage events are unintentional [14], either due to routine jobs, unscheduled changes, or device misconfigurations by an organization's OT and IT personnel. Having an easy-to-use interface that streamlines access and workloads for privileged users could help to reduce OT outages – key for safety and efficiency in manufacturing scenarios!

07

Does it boost productivity– or give you more work?

Every workplace seeks to be as productive as possible, but in manufacturing, time truly is money.

Whether it's hitting production targets or keeping the supply chain moving, remote access should empower your team to work more quickly, not hold them back.

Yet too many solutions – looking at you, VPNs – do exactly that.

Latency, cumbersome login requirements, and rigid workflows can slow work routines when every second counts. They can also frustrate users, who simply want to do their jobs.

The SRA solution you choose should prioritize productivity as well as security. Instead of creating roadblocks, it will streamline access, speeding up work by making it easier to connect securely. Benefits to look for should include:

Easy adoption, zero disruptions. The right solution will integrate with how you currently work. Users already have native experience with familiar applications, so there's no need for time-consuming and potentially costly retraining. Quicker time to ROI and happier teams.

One unified dashboard, everything you need. A centralized access hub means less friction, fewer logins, and more time doing actual work.

No agents, no delays. Manufacturers depend on a variety of third-party contractors, from original equipment manufacturers (OEMs) to specialist technicians, to keep operations running smoothly and safely. Securing these privileged users is key – but so is getting them working as quickly as possible. An agentless SRA solution will get vendors to work faster, while also making life easier for the security teams and admins who manage user onboarding. That's security plus maximum productivity.

When an SRA tool is built for OT productivity, it's not just safer – it's smarter, faster, and easier to use.

Did you know? With older workforces retiring and manufacturers expanding capacity, the manufacturing industry needs to find and train up 3.8 million new employees by 2033 – especially in metalworking and textiles.[15] When time is of the essence to onboard new workers, having an SRA solution that's easy to use and streamlines privileged access can make all the difference to your productivity.

08

Will it scale with your manufacturing operations – or leave them feeling bloated?

Would you buy an entire toolkit if you only needed a hammer, or a screwdriver? Probably not.

So why invest in a secure access solution that's oversized, inflexible, packed with features you don't need (or worse, lacking ones you do)?

To avoid unnecessary systems bloat while ensuring you can scale freely as needed, the solution you choose should:

Focus on what actually matters. Roughly 10% of users carry about 90% of your risk. Your SRA tool should prioritize securing these privileged accounts, rather than unnecessary bells and whistles that won't help your bottom line or don't comply with industry regulations.

Deploy and scale easily without draining your resources. Manufacturers often operate across dozens, even hundreds of sites. Solutions with decentralized architecture, centralized management, and automated controls reduce daily workloads by making scaling simple. No logistical nightmares in sight.

Flex with your needs. Whether you're securing one facility or a global network, your SRA solution should be built for OT from the ground up. No clunky IT-first tools reverse-engineered for industrial environments.

The right SRA solution makes scaling across your entire organization easy, whether you're expanding, evolving, or just keeping things running at peak efficiency.

Key takeaway: Treating all users as 'privileged' and saddling them with the most stringent access and connectivity controls can be a bit inconvenient when your operations are smaller. But, as you grow, you could be creating unnecessary restrictions for hundreds or thousands of employees. That's why it's best to choose a flexible remote access solution with controls that adapt to fit the needs of each worker and device.

Revealed: The SRA Solution that Checks Every Box for Your OT Secure Access Needs

Let's take a full look through the checklist one more time:

- ☐ Will it work in any environment?
- ☐ Can you deploy it without infrastructure changes?
- ☐ Does it provide controls for connectivity, oversight, *and* access?
- ☐ Does it secure the legacy systems you depend on?
- ☐ Does it deliver true zero trust?
- ☐ Does it improve operational agility?
- ☐ Does it boost productivity?
- ☐ Will it scale with your manufacturing operations?

If the SRA solution you're evaluating doesn't check all these boxes, it likely isn't built for OT and it's definitely not the right fit for ensuring secure remote access to your critical systems and resources.

The Next Step: Tick Every Box and More with Cyolo

Cyolo is a leading cybersecurity innovator dedicated to helping manufacturers connect privileged users to critical OT assets in a way that's secure, safe, and surprisingly simple.

Meeting the needs of both security and OT teams, the Cyolo PRO (Privileged Remote Operations) access solution is adaptable to any environment and deploys without causing disruptions or requiring change management.

Here's what manufacturers can expect with Cyolo PRO on the factory floor and beyond:

An SRA solution designed specifically for OT. Cyolo PRO is purpose-built to provide secure access to operational environments and cyber-physical systems.

No more patching together different tools for every access scenario. Cyolo PRO integrates seamlessly into your existing tech stack and can be deployed in every type of environment – cloud-connected, on-prem, or air-gapped/offline.

Focus protection where it matters most. Cyolo PRO helps manufacturers achieve meaningful security gains by securing remote access for privileged users and devices – without adding unnecessary complexity.

Decentralized architecture, centralized management. Security should move at the pace of your operations. Cyolo PRO is built for the physical world – secure by default, effortless by design, and agile enough for any environment.

Cyolo delivers improved security, productivity, and operational agility – without compromise.

Ready to see how easy it can be to ensure secure remote access to your OT environment?

SCHEDULE A DEMO TODAY

References

1 Ponemon Institute, 2024.
2 SecurityWeek, 2025.
3 IBM Threat Intelligence Report, 2024.
4 DataGuard, 2024.
5 DataGuard, 2024.
6 Gartner, 2023.
7 Rockwell Automation, 2024.
8 OPSWAT, 2025.
9 DataGuard, 2024.
10 EY.com.
11 IndustrySelect, 2023.
12 FoodDrinkEurope, 2023.
13 IndustrialCyber, 2024.
14 SANS Institute, 2023.
15 USA Today, 2024.

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