Can Cybersecurity Drive Growth?

The Strategic Role of Secure Remote Access in Manufacturing

Authored by Takepoint Research
Commissioned by Cyolo

Research

Cyolo

Table of Contents

Click to jump to desired section

Executive Summary

As industrial systems and market expectations evolve, the need to securely connect people to critical operational technology (OT) assets – whether internal staff or third-party vendors – has shifted from optional to essential.

Secure remote access (SRA) is now a foundational capability in industrial cybersecurity, enabling resilience, agility, and operational continuity across globally connected environments.

Safely and securely enabling remote access to OT environments is inherently complex, requiring support for diverse user groups while minimizing risk to legacy systems. Despite these challenges – and contrary to the long-held assumption that cybersecurity hampers productivity and efficiency – **this survey reveals that organizations implementing secure remote access are achieving measurable operational and business gains:**

- **67% cited improved third-party collaboration as the top benefit of secure remote access**
- **58% reported increased efficiency or productivity**
- **50% realized cost savings**
- **42% saw compliance improvements**
- **Only 0.4% reported no benefit**

This report examines how manufacturing organizations across North America and EMEA are reframing cybersecurity as a business enabler. Data was collected from 535 qualified respondents—including CISOs, CIOs, OT security leads, operations managers, and plant engineers—and supported by analyst insights.

Topics covered in the research include:

- **Who is accessing critical OT systems – and how that access is controlled**
- **How security essentials like multi-factor authentication (MFA), role-based access controls (RBAC), and Zero Trust are being put to work**
- **The role of user experience (UX) and artificial intelligence (AI) in driving SRA adoption and performance**
- **Recommended next steps for how to demonstrate the business value of SRA to key stakeholders**

To further illustrate how SRA not only safeguards critical operations but also supports strategic business goals, the report concludes with 2 global manufacturing case studies:

Case study 1 **A Global Food Manufacturer's Journey to Scalable, Secure Remote Access**

Case study 2 **Modernizing Secure Remote Access for a Global Automotive Manufacturer**

Key Survey Takeaways

01

Secure remote access is a strategic enabler that delivers broad business value.

Demonstrating SRA's key role in ensuring uptime and productivity, 64% of respondents use SRA to enable secure real-time access to critical systems, 63% use it for vendor access, and 43% use it to support remote maintenance and troubleshooting. Additional reported benefits include increased efficiency (58%), and cost savings (50%).

Why it matters:

For CISOs: Demonstrating clear ROI on secure access helps justify ongoing investments and aligns cybersecurity with business performance objectives and enterprise KPIs.

For OT leaders: SRA enables faster maintenance and reduced downtime, directly supporting production continuity. Outcomes like improved collaboration and efficiency translate to measurable improvements in operational performance, uptime, and responsiveness.

58%

cited **increased operational efficiency and/or productivity** as a major benefit of SRA.

Key Survey Takeaways

02

Enabling remote third-party access to OT environments is widely accepted, while internal use of SRA is less common.

88% of respondents report their organization authorizes remote third-party access to OT environments, and 60% allow such access for more than 100 external parties (including contractors, vendors, suppliers, OEMs, etc.). By marked contrast, only 54% allow employees to remotely access OT systems.

Why it matters:

For CISOs: Expanding access requires stricter identity and access management controls to prevent supply chain-driven breaches and other security incidents. At the same time, failing to implement SRA for employees can raise risk and limit a company's appeal to top talent seeking flexibility.

For OT leaders: Heavy reliance on external vendors demands strong access controls to protect operational integrity and minimize potential disruptions. Enabling SRA for internal employees also boosts agility, speeds up issue resolution, supports flexible workflows, and could help attract talent to organizations struggling to fill open positions.

32%

authorize more than 250 third parties to access their OT environment.

88%

allow remote third-party access to OT environments.

Key Survey Takeaways

03

Despite broad adoption, satisfaction with current SRA for OT solutions – and especially with user experience – is low.

42% of respondents rated their current SRA security measures as ineffective for protecting OT environments, and the average user experience (UX) satisfaction score is just 2.5 out of 5. Less than 7% are very satisfied with their existing SRA for OT measures.

Why it matters:

For CISOs: Low satisfaction and poor usability can reduce adoption and adherence, limiting the effectiveness of even well-architected security controls.

For OT leaders: Low satisfaction can slow response times and complicate support efforts, while poor UX can lead to workarounds and resistance from frontline users, undermining secure access policies.

Less than

7%

call their current SRA solutions "very effective."

Key Survey Takeaways

04

Security best practices are finally gaining traction in OT: MFA is now common and Zero Trust is emerging.

69% have deployed multi-factor authentication (MFA) and 47% have adopted role-based access control (RBAC). Smaller but still significant numbers have started Zero Trust implementation (34%) or continuous monitoring and auditing of user activities (28%). All survey respondents have adopted at least one of the aforementioned practices, signaling important progress toward adaptive security models – with room for ongoing improvement.

Why it matters:

For CISOs: Strong authentication and other security best practices are foundational for enforcing least privilege access and reducing lateral movement in OT and hybrid IT/OT environments.

For OT leaders: These measures support compliance without overcomplicating workflows for technicians and engineers.

05

Compliance requirements still drive secure remote access adoption — especially in Europe.

Regulatory compliance acts as a powerful catalyst for SRA adoption, particularly in more tightly governed regions. In EMEA, where cybersecurity mandates are more stringent, 30% of respondents cite compliance requirements as a primary driver for SRA implementation. By contrast, only 19% of North American respondents call compliance a core motivation – underscoring a regionally varied regulatory influence. Still, the data affirms that regulatory pressure is triggering security investments that might otherwise be deferred.

Also noteworthy is the bidirectional relationship between compliance and SRA. While compliance drives SRA adoption, SRA itself enables organizations to meet and sustain compliance obligations. 42% of surveyed organizations report that SRA has helped improve or maintain compliance post-deployment. Looking ahead, 47% believe AI will play a crucial role in advancing compliance posture and strengthening risk management capabilities.

Why it matters:

For CISOs: Compliance remains one of the few levers that reliably drives investment in OT cybersecurity. Aligning SRA initiatives with compliance goals not only helps secure executive buy-in but also builds the foundation for stronger risk governance and measurable outcomes.

For OT leaders: Regulatory pressure can be a catalyst for security maturity. Even when compliance is the starting point, effective SRA solutions can yield broader benefits – from reducing unauthorized access to improving audit readiness and operational resilience.

06 Manufacturing leaders are betting on AI to strengthen secure remote access.

The manufacturing industry shows clear enthusiasm for the role of AI in secure remote access. Organizations report realized or expected benefits including improved real-time threat detection and response (61%), better compliance and risk management (47%), and proactive identification of issues before they escalate (38%). Fewer than 4% have no plans to incorporate AI into their remote access security strategy.

Why it matters:

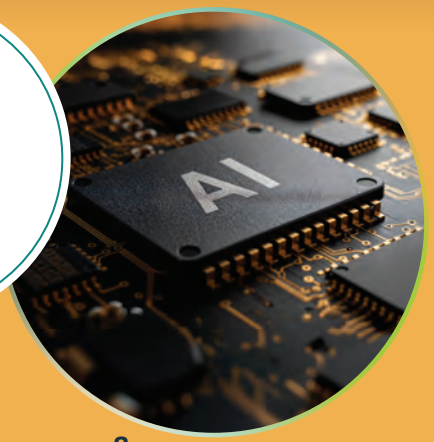
For CISOs: With rising pressure to improve both security and compliance outcomes, AI offers a path to scalable, risk-informed decision-making. CISOs can use these early success signals to build a roadmap for AI adoption aligned with business and regulatory priorities.

For OT leaders: AI is emerging as a practical enabler of operational resilience – helping identify anomalies faster, minimize downtime, and reduce the burden on limited resources. OT leaders should prioritize use cases where AI enhances visibility without adding complexity.

Over

96%

are using or plan to use AI to strengthen SRA



How Stakeholders Can Use This Report

The report is desiged to support all types of stakeholders as they benchmark maturity, identify gaps, and take informed next steps to strengthen both secure remote access strategies and overall resilience in their manufacturing environments.

CISOs & security leaders: Benchmark your existing security program, identify high-impact investments, and more effectively align cybersecurity with business risk. Use the findings to guide strategy, justify budgets, and strengthen board-level conversations.

OT leaders & operations/engineering managers: Get practical insights to align cybersecurity with operational goals. Learn how peers are handling key security tasks, reducing downtime, and maturing their programs – even with limited resources.

Security as a Business Driver

SRA has evolved into a strategic enabler for manufacturers, with 48% directly identifying it as a foundational element supporting business growth. Beyond risk mitigation, SRA supports uptime, resilience, and innovation, helping businesses move faster and operate more intelligently in a decentralized, connected world.

Operational Efficiency as the Starting Point

Most organizations adopt SRA to improve operational performance. According to the survey:

- **64% use SRA for real-time system access to critical systems and assets**
- **63% use SRA to enable third-party support from vendors and contractors**
- **43% use SRA to minimize downtime through remote troubleshooting**

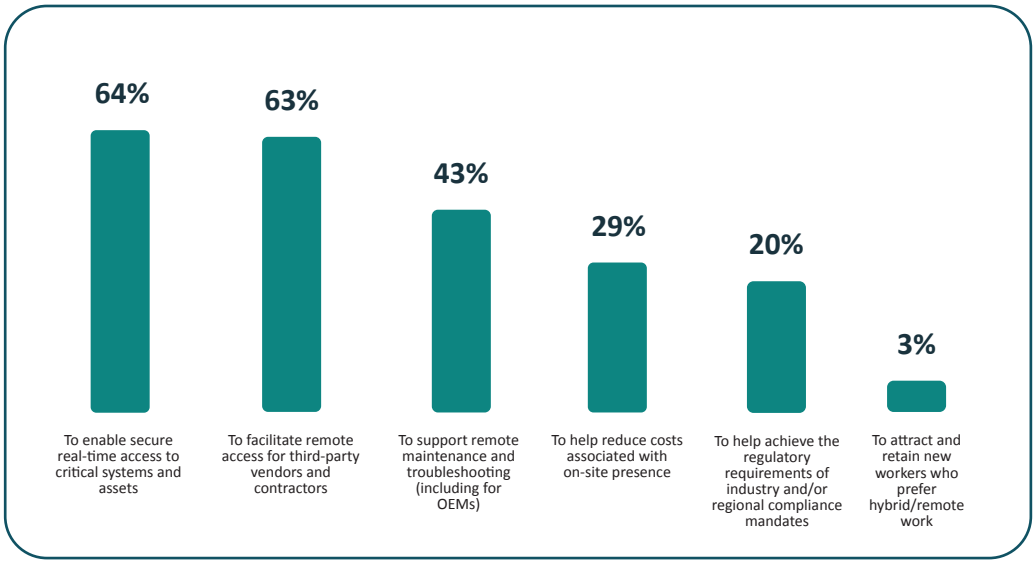
Crucially, these are not IT priorities – they are production imperatives.

And they deliver results: **58% reported increased efficiency, and 50% cited cost savings from reduced travel and faster resolution.**

Figure 1

What are the primary reasons why your organization allows remote access to the OT environment?

(Select up to 3 answers.)



Resilience and Continuity

From global disruptions to site-level failures, distributed access is now central to continuity planning. **42% of respondents reported that secure remote access has helped maintain or improve regulatory compliance**, underscoring its value in supporting operations under pressure while staying audit-ready.

Enabling Innovation

SRA is also a launchpad for digital transformation. By opening secure pathways for AI tools, industrial internet of thing (IIoT) platforms, and remote visualization systems, organizations unlock new efficiencies. **29% reported enhanced user experience** – a signal that well-executed SRA drives both usability and innovation.

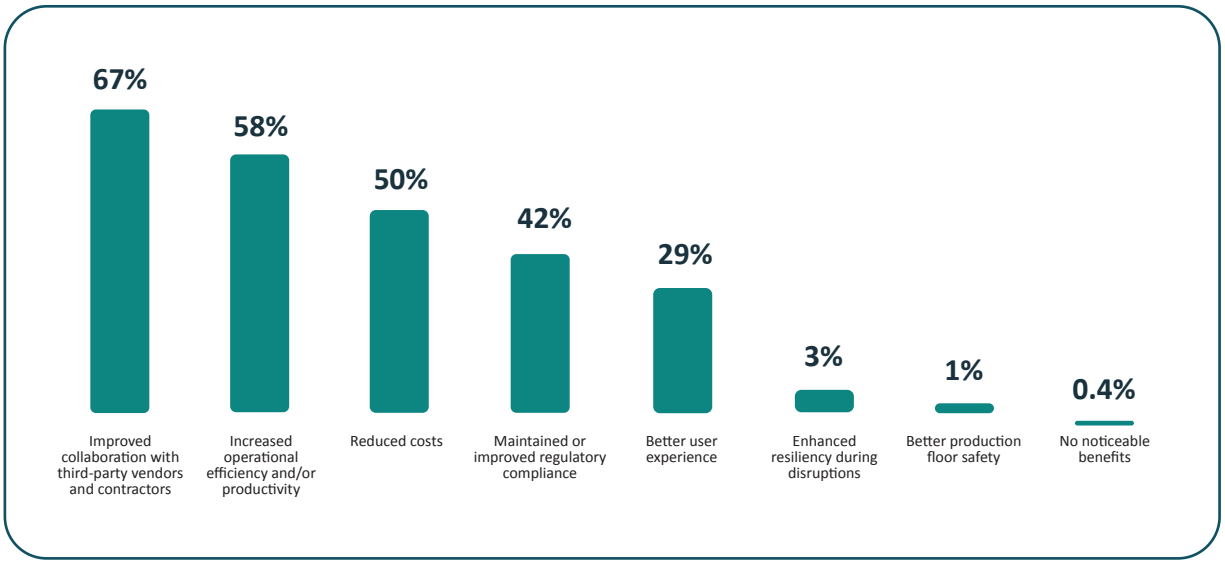
Collaboration Without Compromise

With external vendors essential to plant operations, scalable third-party access is non-negotiable. **67% cited improved third-party collaboration** as the top benefit of SRA. These connections, however, require visibility and control, something legacy SRA solutions like VPNs and jump servers often cannot provide. By contrast, more modern SRA platforms that are specifically built for OT can secure third-party connections without slowing down productivity or opening new areas of risk.

Figure 2

What benefits has your organization experienced by adopting secure remote access?

(Select up to 3 answers.)



Aligning Security with Strategy

Compliance frameworks like IEC 62443 and NIS2 are putting pressure on manufacturers to improve their security posture. SRA done right plays a central role in meeting a range of regulatory mandates through access controls, logging, and user validation. However, stakeholder alignment remains challenging: **68% said it's difficult to show how SRA supports business goals, with an average difficulty rating of 3 out of 5.**

To achieve more positive outcomes, security leaders must reframe SRA as a business enabler, not a technical add-on. Those who do are already realizing not just risk reduction but also operational momentum.

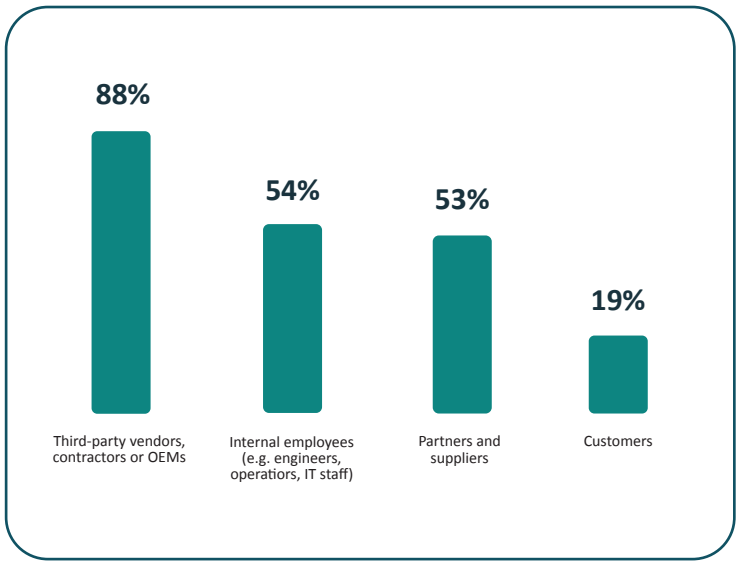
People, Policies, and Practices in Secure Remote Access

Secure remote access is at its core a human issue. Every connection represents a real person – an engineer, technician, or vendor – trying to get work done. To manage these connections securely, organizations must understand who needs access, why, and under what conditions.

Figure 3

Which types of users does your organization allow to remotely access its OT environments?

(Select all that apply)



Expanding the Access Footprint

Access requirements in today's manufacturing environments are broad and complex:

- **Internal employees** (engineers, operators, IT) often manage systems across multiple sites.
- **Third-party vendors and OEMs** are critical for diagnostics, updates, and support – so much so that **88% of organizations grant them access.**
- **Partners and suppliers** require visibility to maintain supply chain continuity – **53.5% grant them remote access.**

Notably, 78% of organizations manage over 50 third-party connections, with a third (32%) managing more than 250 – well beyond what legacy perimeter-based security models can support.

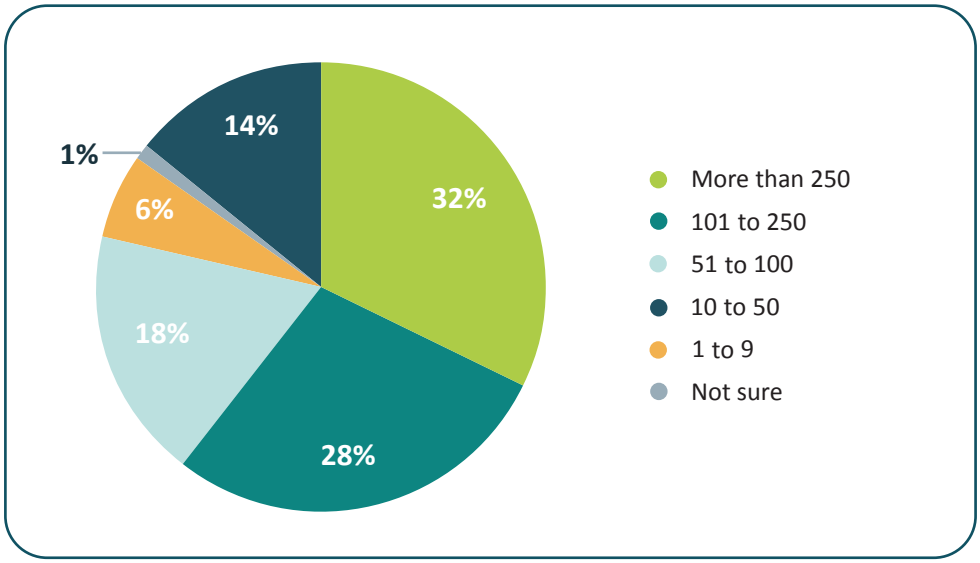
In addition, 14% of respondents report being unsure of how many third parties are authorized to access OT systems, suggesting the real number is likely even higher.

60%

of organizations manage **over 100 third-party connections**

Figure 4

How many third-party vendors, contractors, or OEMs are authorized to connect to your organization's OT environments?



The remarkable degree to which manufacturers rely on third-party support does not negate the fact that vendors and contractors pose a substantial security risk. Third-party access at this scale demands adaptive modern controls to enforce not just identity-based access but also to enable visibility throughout the entire connection.

From Controls to Context

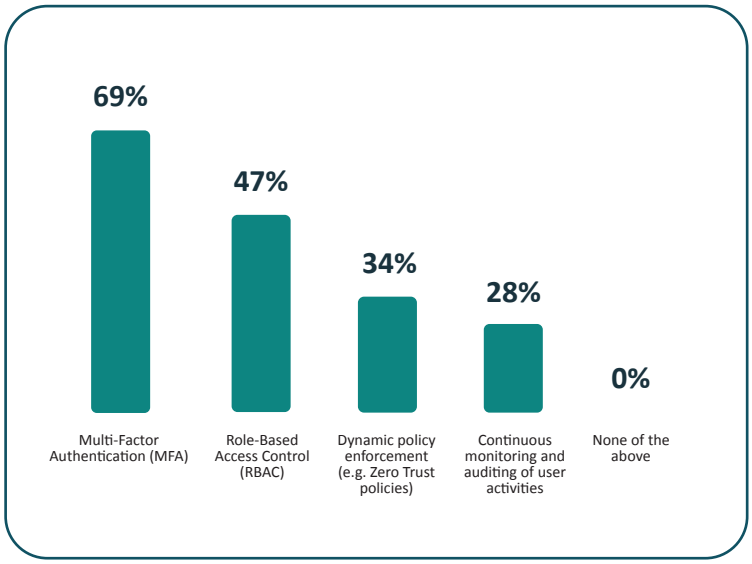
To govern this complex web of users and access policies, organizations need adaptive access strategies:

- MFA (used by 69%) and RBAC (47%) provide foundational controls.
- Dynamic policy enforcement and Zero Trust, adopted by 34%, allow contextual decisions based on risk and behavior.

Figure 5

What approaches does your organization currently employ to manage and secure remote access?

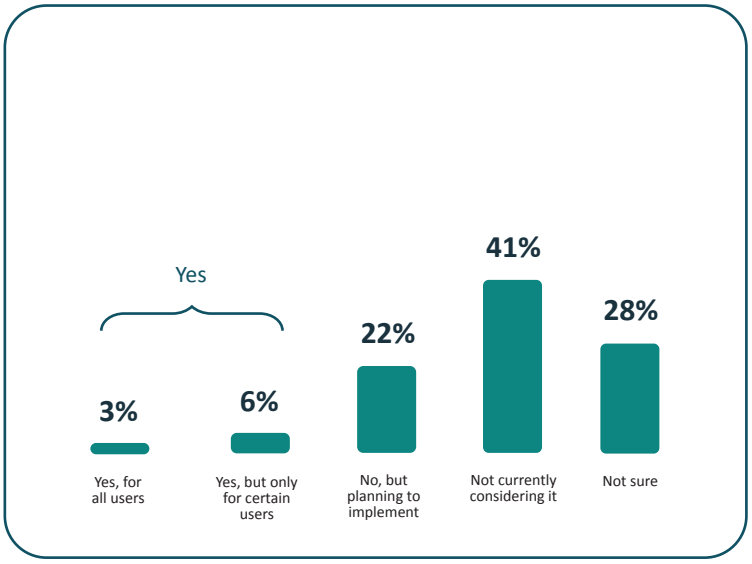
(Select all that apply.)



Yet advanced personalization – such as risk-based access scoring – remains relatively uncommon. This approach dynamically evaluates access requests based on contextual factors such as user role, device posture, location, and behavior, enabling organizations to prioritize and control connections where risk is highest.

Figure 6

Does your organizations assign risk levels or scores to remote users to tailor security controls?



Despite its value in securing instances of privileged access and limiting exposure to threats such as compromised credentials or lateral movement, **only 9% of respondents currently use risk-based access scoring, while 41% are not even considering it** – revealing a significant gap between emerging best practices and current or planned adoption.

Visibility, Training, and the Maturity Gap

Just **28% of organizations actively monitor and audit sessions in real time**, meaning most still lack full visibility into what users are doing after access is granted. Without such visibility, it is difficult to detect misuse of access permissions, enforce accountability, or respond swiftly to suspicious activity – leaving organizations exposed to insider threats, policy violations, and other threats.

Meanwhile, only a few respondents mentioned user training, suggesting many organizations are underinvesting in awareness programs, even as human behavior remains a top vulnerability.

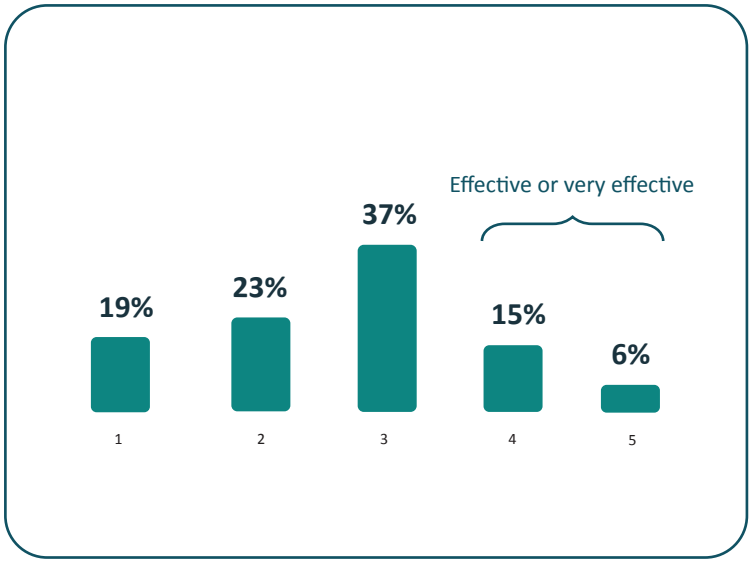
Solution Effectiveness in Question

Despite widespread SRA adoption, confidence in current controls is remarkably low:

- **The average effectiveness score for current SRA solutions was 3 out of 5**
- **42% rated their controls as ineffective or minimally effective (1 or 2 out of 5)**
- **Less than 7% called their current protective measures "highly effective" (5 out of 5)**

Figure 7

On a 1-5 scale, how effective do you consider your organization's current remote access security measures in protecting OT environments?



These numbers expose a **major disconnect between solution adoption and the ability to manage OT access in a safe, secure manner**. Many manufacturers may have implemented remote access out of operational necessity – but seemingly without the processes, visibility, or governance to support it securely and sustainably.

The Bottom Line

Many organizations have adopted core tools to support secure remote access, but few have advanced to risk-aware, behavior-driven access management. Bridging this gap will be key to effectively securing remote operations at scale.

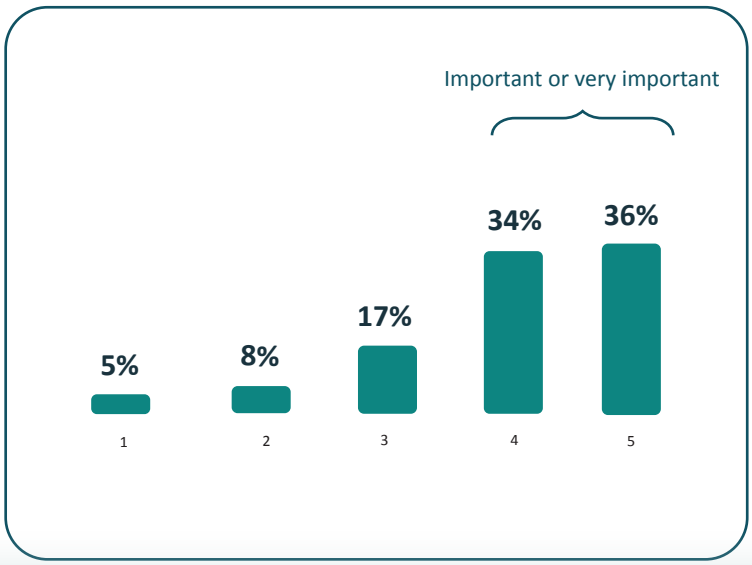
The Impact of User Experience on Security and Business Outcomes

User experience (UX) is often treated as an afterthought in industrial cybersecurity, but it shouldn't be. In operational environments, where remote access is used by a diverse set of users – from field engineers and control room operators to IT staff and third-party vendors – clarity, simplicity, and speed are just as important as security.

And the data backs this up: **70% of respondents rated user experience as a high priority** when selecting SRA solutions, with a mean importance score of 4 out of 5. This signals a growing recognition that security can't succeed in isolation. It must work *with* people, not against them.

Figure 8

When choosing secure remote access solutions, how important is user experience for your organization?



Usability as a Security Imperative

Many users in industrial environments aren’t deeply technical. They're focused on doing their jobs – responding to alarms, checking systems, troubleshooting machines – not navigating layered authentication processes or confusing portals. When security controls become obstacles, users will often find workarounds, which can paradoxically introduce avoidable risk to the organization.

> **If something adds too many clicks, people won’t use it. That’s why seamless integration and a native user experience are so important.**
>
> Senior technical lead at Global Automotive Manufacturer

Figure 9

From the perspective of user experience and ease of use, how satisfied are you with your organization's current solutions for remotely accessing OT environments?

The consequences of poor user experience are reflected in the **low satisfaction scores** for current SRA tools. Even as user experience is deemed important, the average satisfaction score was just **3 out of 5**, with only **5% of users saying they are “very satisfied” with their current tools from a UX perspective.** This gap between expectations and reality is a red flag – but also an opportunity.

When SRA systems are intuitive and efficient, they not only reduce frustration but also improve security outcomes.

66% of respondents said user-friendly access solutions improve productivity, and a further **59% noted enhanced compliance** with security protocols. In other words, usability drives better behavior, which drives better results.

While

70%

said user experience is important or very important when choosing security solutions, **just 5% rated their current SRA tools as "very satisfactory" from a UX perspective.**

The Hidden Costs of Friction

Poor user experience doesn't just inconvenience users – it erodes security posture over time. If systems are difficult to navigate or too slow to use in high-pressure situations, users may share credentials, bypass authentication, or delay important tasks like applying patches or conducting remote diagnostics. This ultimately leads to worse security outcomes.

57% of respondents recognized better adherence to security protocols as a top benefit of user-friendly tools, indicating that a smooth experience is integral to ensuring that good security habits are actually followed.

Even more telling is that only **2% of respondents reported no benefit from improving the user experience.** That means 98% see a clear ROI – operationally, technically, or culturally – from investing in user-centric SRA solutions.

Design Principles for Industrial SRA Success

To be effective, secure remote access must be:

- **Simple and streamlined:** Users should not have to guess how to connect or which credentials to use. Single sign-on (SSO), clear navigation, and fast onboarding are crucial. Agentless access and password-free log-in can also markedly improve user experience.
- **Context-aware:** To minimize noise and reduce error rates, interfaces should present only the tools and information needed for the specific task or role.
- **Integrated with workflow:** Access processes should align with how users work, not force them to adjust to rigid systems. This includes mobile-friendly experiences, real-time feedback, and the ability to work offline where needed.
- **Built with feedback loops:** Security teams should continuously gather user input and behavioral data to refine UX. Survey and telemetry feedback loops create a virtuous cycle of improvement.

The Human Element of Secure Access

A secure access system that frustrates users becomes a liability. A system that supports users becomes an asset.

In today's industrial environments, where uptime, safety, and speed are non-negotiable, **user experience is a critical differentiator.** It shapes adoption. It shapes behavior. And ultimately, it shapes security and business outcomes.

Organizations that want to future-proof their SRA strategies must go beyond technical checkboxes and design for the people using the system every day. This is how you turn secure access from a constraint into a catalyst for productivity.

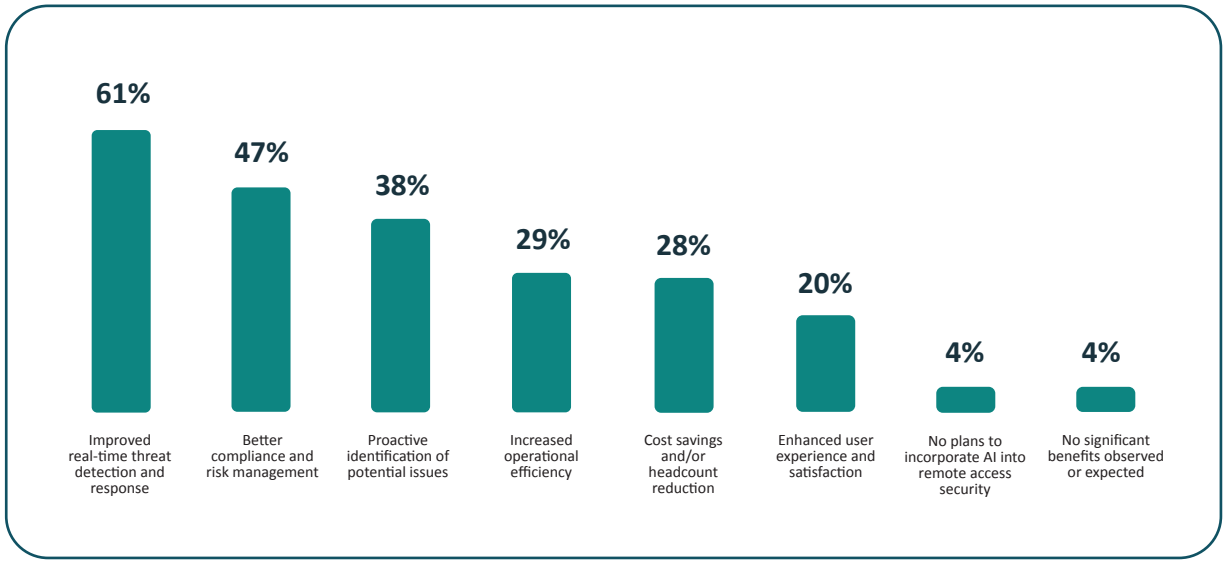
Leveraging AI to Advance Secure Remote Access

AI is reshaping secure remote access in OT environments by delivering real-world value in areas like threat detection, access governance, and user experience. As industrial networks grow more complex, AI is becoming essential to scale securely without adding friction or overhead.

Figure 10

What benefits has your organization realized or do you expect to realize by incorporating AI into remote access security?

(Select all that apply.)



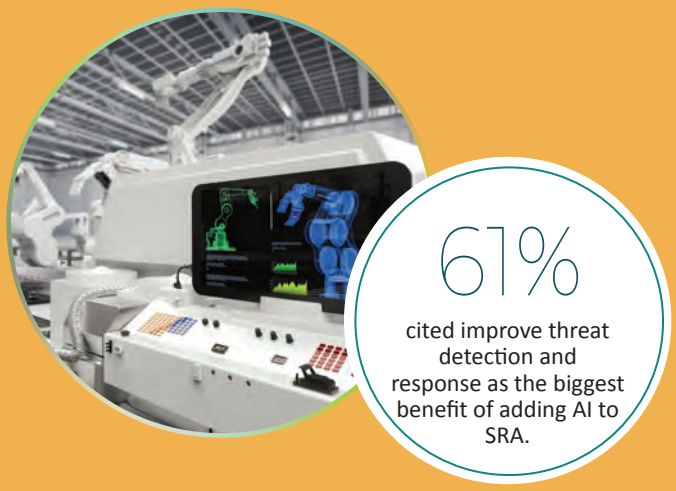
Real-Time Detection and Automated Response

61% of respondents cited threat detection and response as the most valuable AI benefit. AI-powered monitoring enables real-time identification of suspicious activity, reducing dwell time and speeding up remediation. Offloading manual monitoring tasks to AI also allows security teams to focus on higher-value work. While only 9% currently use automated response, adoption is expected to grow as confidence in AI-driven enforcement increases.

Threat Intelligence and Anomaly Detection

When asked what AI capabilities would be most valuable for their organization's SRA needs, **71% selected threat and anomaly detection** – far ahead of all other features. AI systems trained on behavioral patterns and attack data can detect subtle deviations that signal potential threats, offering a significant advantage in OT networks where anomalies often go undetected by traditional tools.

Early detection is particularly crucial in industrial environments, where even minor deviations can escalate into safety incidents, equipment damage, or widespread operational disruption. Timely alerts enable faster containment and response, helping prevent potentially catastrophic consequences.



61%

cited improve threat detection and response as the biggest benefit of adding AI to SRA.

Compliance and Risk Management

AI simplifies compliance by automating policy enforcement, logging, and reporting. **53% prioritize AI for governance** and risk assessment, and **47% cite better compliance as a key benefit**. However, **only 9% use AI-driven risk scoring today**, pointing to a maturity gap with significant growth potential.

Adaptive Access Control

AI enables real-time, context-aware access decisions – adjusting authentication based on behavior, location, or device risk. **50% of respondents prioritize dynamic access control**, reflecting a shift toward Zero Trust models that balance agility and security.

AI can also escalate requirements like MFA during high-risk sessions, improving protection while maintaining ease of use for authorized users.

User Experience as a Strategic Gain

AI enhances usability. **20% of respondents reported improved user satisfaction**. Features like chatbots and smart guidance, though still underused, can help streamline access for both internal and third-party users. As noted above, a positive user experience contributes directly to better security outcomes and improved productivity.

The Bottom Line

The survey responses signal a clear shift toward intelligent, scalable, and adaptive access solutions in industrial environments.

To most effectively harness emerging AI capabilities, organizations should:

- **Prioritize high-value AI use cases**, such as anomaly detection and dynamic access enforcement.
- **Pilot emerging capabilities**, including automated response and risk scoring, in low-risk environments to build confidence.
- **Align AI usage with Zero Trust and compliance goals** to reinforce least-privilege access and continuous risk assessment.
- **Balance AI gains with usability**, ensuring tools enhance the user experience for both internal and third-party users.

A phased, strategic approach will help organizations realize AI's potential without adding operational complexity.

Conclusion and Recommendations: From Insights to Action

Secure remote access has evolved from a technical necessity into a strategic business enabler. As this report demonstrates, organizations across the manufacturing sector are recognizing the transformative potential of secure, scalable connectivity – supporting not only cybersecurity objectives, but also productivity, innovation, compliance, and collaboration.

Major Findings

- **The operational value of SRA is clear.** Top benefits of SRA adoption include improved third-party collaboration (67%), increased efficiency (58%), and cost savings (50%), underscoring SRA's role in enabling operational agility, production continuity, and vendor support.
- **SRA is widely adopted but inconsistently implemented.** While 100% of respondents reported enabling SRA, only 28% are satisfied with their current solutions, and many lack visibility, automation, and adaptive access controls.
- **Security maturity remains uneven.** MFA is common (69%), but only 34% have begun adopting Zero Trust, and just 9% use risk-based access scoring to tailor security controls for remote users – indicating a wide gap between best practice and current state.
- **User experience is a critical differentiator.** 70% claim to prioritize UX in tool selection, but satisfaction remains low (2.5/5 average). When UX improves, so do security behaviors and business outcomes.

- **AI adoption is rising – but slowly.** Capabilities like anomaly detection (72%) and adaptive access control (50%) are highly valued, yet practical deployment of AI-driven response and governance remains limited.

To unlock the full business value of secure remote access, organizations should concentrate on the following priorities:

1. **Position SRA as a strategic enabler:** Frame secure remote access as a driver of uptime, agility, and innovation – not just a security tool. This will help align stakeholders and ensure executive sponsorship.

2. **Design SRA strategy for usability and adoption:** Invest in user-centric access experiences, especially for frontline and third-party users. A seamless interface reduces friction, increases adoption, and improves security adherence.

3. **Implement risk-based, adaptive access controls:** Advance beyond static policies by incorporating contextual decision-making – such as device health, user behavior, and location – to support Zero Trust and least privilege principles.

4. **Enhance visibility and monitoring across access paths:** Deploy centralized session logging and real-time monitoring to improve governance, detect anomalies, and enable faster response to potential threats.

5. **Pilot high-value AI use cases:** Start with AI capabilities like anomaly detection or dynamic access control in targeted areas. Use small wins to build trust, refine policies, and scale securely.

Case Study: A Global Food Manufacturer's Journey to Scalable, Secure Remote Access

Background: Scaling with Confidence

A global food manufacturing company with dozens of facilities across Europe, the Americas, and Asia set out to standardize and secure its remote access capabilities. With nearly half of its plant infrastructure located in Europe alone, the organization was under growing pressure to enable safe, seamless collaboration with OEMs, service providers, and engineering partners, without compromising its operational integrity.

The driver? A fragmented approach across plants and regions had created visibility blind spots, inconsistent user experiences, and growing security risks.

The Catalyst: Unifying a Disjointed Access Landscape

Previously, the organization relied on a legacy solution that was functional but far from optimal. The lack of MFA integration, complex logins, and clunky interfaces led to low user satisfaction and reduced adoption.

"The user experience was poor, logins were complex, the platform wasn't stable, and third parties hated it."

Each plant was using its own methods to facilitate third-party access, resulting in significant governance gaps. The business recognized the need for a globally consistent, centrally managed, and operationally efficient platform.

The Evaluation Process: A Collaborative, Cross-Functional Approach

To address these challenges, the organization launched a structured global RFP. Candidates included the incumbent vendor (offering an updated solution), a leading IT services provider with an industrial offering, and a lesser-known remote access provider with strong usability credentials.

The evaluation went beyond the security team. Global OT leads, local plant engineers, security architects, and standards bodies were brought together to assess fit and functionality through live pilots at four to five sites worldwide.

It wasn't just about what the security team thought. We had input from the people in the plants, from our standards team, and from those who would actually use the system every day. That collective validation gave us confidence.

Cyolo – described as “the dark horse” – emerged as the unanimous choice, winning over stakeholders with its usability, compatibility, and flexibility.

What Mattered Most: Usability, Scale, and Trust

What sealed the decision was simplicity and scale:

- **No plugins or installations:** Users accessed the system via browser
- **Cross-device support:** Compatible with managed and unmanaged PCs and tablets
- **Contextual access control:** Users only saw what they were meant to see
- **Minimal onboarding time:** Enabling quick adoption by internal teams and third parties alike

> **It’s the first time we’ve had third parties ask if they could use it for more. Usually, it’s grumbling. But now the reaction is: ‘Oh, this is quite good.**

Administratively, the team deployed a federated, multi-tenant model, delegating control to 100+ OT personnel across regions, replacing the previous bottlenecked model where only a few admins could execute changes.

> **We trusted the team, gave them access, and built in training and documentation. So far, that trust has been rewarded.**

Success Metrics: Cost, Control, and Continuity

The results spoke for themselves:

- **Hundreds of daily users**, including both internal staff and external vendors
- **Rapid onboarding and operational adoption**, even among non-technical users
- **Reduction in support tickets**, login issues, and access delays
- **Compliance alignment** across OT security standards without disruption
- **Cost-effective transition**, with year-one savings exceeding implementation costs

The transition costs were more than covered in the first year. We let the team choose what was best for the business, because we knew we could afford all the options.

The rollout was not only secure and scalable, but it was culturally resonant. Built on trust, collaboration, and transparency, the solution embedded itself into daily operations across the global footprint.

Conclusion: Secure Access as an Enabler of Manufacturing Excellence

This case illustrates a key insight from our broader research: **the value of secure remote access is magnified when solutions are selected collaboratively, aligned to real-world use cases, and designed around the user experience.**

What began as an effort to close security gaps evolved into a platform for **operational resilience, innovation, and trust** – and a textbook example of what it looks like when cybersecurity aligns with business value.

Case Study: Modernizing Secure Remote Access for a Global Automotive Manufacturer

Background: Reducing Risk While Enabling Digitalization

A leading global automotive manufacturer with more than 10 production sites sought to transform how it managed secure remote access to its OT environments. As part of a broader digitalization and network segmentation effort, the company recognized the growing risk posed by outdated access models – especially as more OEMs, service providers, and internal teams required remote connectivity to plant systems.

The Catalyst: Legacy Tools Created Operational Barriers

At the time, the organization relied on a legacy IT-centric remote access tool that required agent installation on both the client and target systems. While functional in office environments, it proved ill-suited for OT contexts, where agents could not be deployed due to vendor restrictions or system limitations.

> **Agents on OT machines were a non-starter – it just wasn't viable in our environment.**

Compounding the problem was the tool's ownership structure: it resided outside the cybersecurity function, limiting visibility and governance. As cyber risks increased, the internal network security team needed a solution they could manage and trust.

The Evaluation: Partner-Assisted Selection and Risk-Aware Rollout

The manufacturer collaborated with its managed security partner to shortlist tools based on real-world OT suitability and operational experience, ultimately selecting Cyolo for a focused proof of concept.

Key decision criteria included:

- **Clientless Access:** No agents on OT assets
- **API Readiness:** Full automation potential
- **Usability:** Both for internal teams and external vendors

The team initially deployed the solution as a global hub, then gradually expanded to new and existing sites using a phased, plant-by-plant approach. This staged deployment helped the team build internal expertise and confidence while minimizing risk.

What Mattered Most: Flexibility, Usability, and Zero Trust Alignment

The Cyolo solution's usability and flexibility emerged as critical differentiators. The platform supported third-party onboarding without friction, and internal users could choose between portal access and integration with familiar tools like PuTTY and RDP.

We learned that if something adds too many clicks, people won't use it. That's why seamless integration and a native user experience were so important.

Operationally, the team retained centralized control but found the platform easy to manage – even with just two core administrators. Automation was the next frontier: server provisioning was integrated with ServiceNow, and plans were underway to auto-publish hundreds of existing assets, closing legacy RDP/SSH gaps in the process.

Measuring Success: Attack Surface Reduction and Operational Confidence

The initiative had clear cybersecurity goals: reduce attack surface, enforce segmentation, and move toward Zero Trust principles. But it also delivered operational value:

- Simplified architecture through reduced IPSec VPN tunnels
- Centralized management without scaling bottlenecks
- Frictionless vendor access and improved governance
- Stronger alignment between manufacturing and cybersecurity teams

The goal is to deny all direct RDP and SSH in firewalls. Cyolo becomes the only way in – and that's a good thing. This isn't just about cybersecurity. It's about doing things in a smarter, more secure way.

Conclusion: Incremental Steps to Zero Trust Success

This case highlights how a manufacturing enterprise can modernize secure remote access through pragmatic steps. Rather than ripping out existing infrastructure, the organization built a hybrid model – using Cyolo where it fits today, while continuing to support other tools as needed.

By starting with a centralized hub, validating user experience, and expanding through automation, the company laid the groundwork for scalable, resilient, and user-centric access – without compromising production or overwhelming internal teams.

Report Methodology

This report was developed by Takepoint Research as part of a focused study into the evolving role of secure remote access in the manufacturing industry. The findings are based on a combination of quantitative and qualitative research conducted in Q1 2025.

Survey Data Collection

A structured survey was distributed to cybersecurity, operations, and engineering professionals across manufacturing sub-sectors. Respondents represented a diverse mix of roles, from CISOs and plant managers to OT security leads and IT/OT architects.

- **Sample size:** 535 qualified respondents
- **Regions covered:** North America and EMEA
- **Manufacturing sub-industries represented:** Discrete and process manufacturing, food and beverage, consumer goods, automotive, and more
- **Respondent roles:** CISO, OT/ICS security, plant IT, engineering leads, risk and compliance

The survey included both multiple-choice and scaled-response questions designed to assess the current state, challenges, and maturity of secure remote access implementations in OT environments.

Qualitative Insights

To complement the survey data, Takepoint Research conducted one-on-one interviews with selected manufacturing organizations. These conversations provided deeper context around decision-making, solution evaluation, and post-deployment outcomes. The featured case study in this report reflects the insights of one global manufacturer with extensive experience deploying secure remote access across its global operations.

Data Validation and Analysis

All responses were reviewed for completeness and relevance. Quantitative data was aggregated and analyzed to identify trends, outliers, and patterns across industry segments and geographies. Qualitative inputs were synthesized to extract practical insights and illustrate real-world applications.

About Takepoint Research

Takepoint Research is a specialized analyst firm focused exclusively on industrial cybersecurity. Founded in 2016, Takepoint delivers practical, bias-free insights that help industrial organizations secure their operations and meet regulatory, resilience, and productivity goals. Its analyst team—comprised of seasoned industry professionals—produces trusted guidance, blueprints, and strategic assessments tailored to critical infrastructure and manufacturing environments.

With a mission to bring clarity and strategic focus to the complex world of Industrial Cybersecurity, Takepoint Research equips stakeholders with the knowledge to act confidently and decisively.

About the Author

Jonathon Gordon is the Directing Analyst at Takepoint Research, where he leads industrial cybersecurity coverage. With over 30 years of experience in cybersecurity, IT, and telecoms, Jonathon delivers clear, actionable insights to help industrial enterprises navigate today's evolving threat landscape. Since joining Takepoint in 2016, he has authored key reports and playbooks on secure remote access, network visibility, asset inventory, perimeter defence, and ransomware resilience. He is also the lead author of the widely referenced Industrial Cybersecurity Buyers' Guide.

About Cyolo

Cyolo provides secure remote privileged access for cyber-physical systems. The Cyolo PRO (Privileged Remote Operations) solution enables industrial enterprises to connect employees and third-party vendors to critical assets in a way that's secure, safe, and surprisingly simple.

Cyolo offers stronger security and more control than traditional secure remote access (SRA), while simultaneously improving operational agility and productivity. Cyolo PRO adapts to any environment, deploys without disruptions or infrastructure changes, and includes capabilities such as privileged access controls, zero-trust connectivity, identity-based access for legacy systems, and centralized management across multiple sites.

Former CISO Almog Apirion co-founded Cyolo in 2020. Frustrated by the limitations of existing SRA tools, he joined forces with industry veterans to build a solution that meets the distinctive access needs of OT environments. With headquarters in Israel and strong presence in the US and EMEA, Cyolo's network of employees, customers, and partners stretches around the world. To learn more, visit https://cyolo.io.

Disclaimer