



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 As part of a broader digitalization and network segmentation effort, the company recognized the growing risk posed by outdated access models – especially as more OEMs, service providers, and internal teams required remote connectivity to plant systems.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.



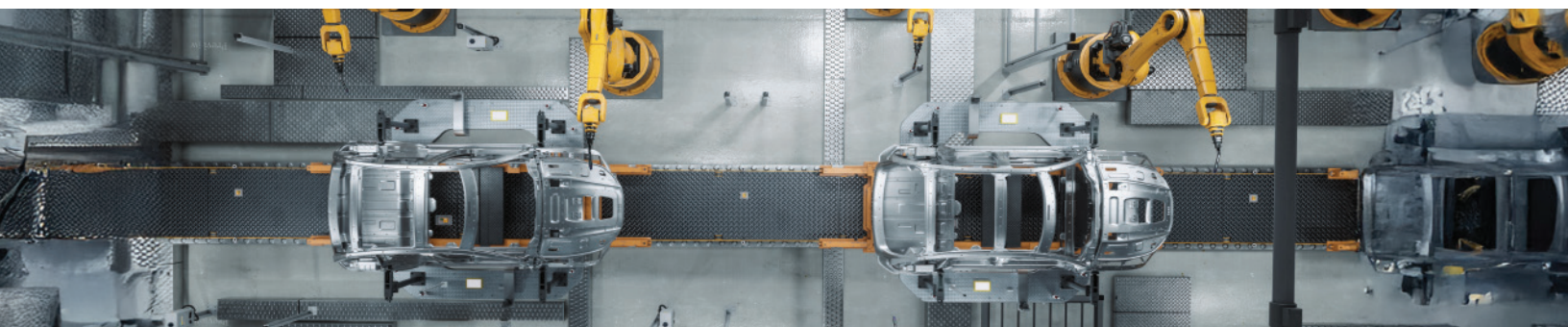
Agents on OT machines were a non-starter – it just wasn't viable in our environment.



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,” the lead explained. 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.



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

Request a demo to learn more:

cyolo.io/demo