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 were simplicity and scalability:

- **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 speak 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 24

> 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.

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