

FROM FRAGMENTED SUPPLIER ACCESS
TO A GLOBAL OT SECURITY STANDARD

SECOMEA

How one of the world's largest brewers standardized Secure Remote Access across 100+ production sites

THE BACKGROUND

"We felt almost totally blind, and that was a big security threat."

Global scale, local complexity

Operating more than 165 production facilities across 70+ countries, one of the world's largest brewing companies depends on a broad ecosystem of OEMs, integrators, and service partners to maintain and optimize production.

But over time, remote connectivity had evolved organically across sites and regions:

- Different plants used different access methods
- Suppliers brought their own remote access tools
- VPNs provided connectivity but limited visibility
- User management and audit logs were inconsistent

From a central governance perspective, critical questions became difficult to answer:

→ Who is connected to production systems?
→ Which suppliers have access – and to what?
→ Are sessions approved, logged, and compliant?

Managing dozens of supplier-specific tools was no longer viable. The company needed one model – no more exceptions.

The objective: one global standard

The brewer defined a clear ambition: establish a single, secure, and scalable remote access model that could be deployed globally without slowing down local operations.

Key requirements included:

- One standardized platform across 100+ sites and 90+ vendors
- Central control over third-party and supplier access
- Fast, repeatable deployment at plant level
- Identity-driven login integrated with enterprise IAM
- Zero Trust–aligned security with encrypted, outbound-only connections
- Full session approval, logging, and traceability
- Global visibility combined with local execution flexibility

THE SOLUTION

A platform that suppliers would actually adopt

Because the new standard directly affected external partners, suppliers were involved early in the selection process.

The chosen solution needed to balance governance with usability across diverse technical environments.

Secomea was selected for its ability to:

- Integrate cleanly with both IT and OT architectures
- Scale consistently across highly diverse production sites
- Centralize governance without blocking local operations
- Be deployed quickly – again and again

*"Onboarding most of our suppliers has been really easy. The majority of our machine builder **suppliers loved the solution**"*

THE EXECUTION

From custom projects to consistent rollouts

Rather than treating each plant as a bespoke project, deployments followed a structured, repeatable pattern that could be adapted locally – resulting in:

- 26 sites live in the first month – nearly double within two months
- 100+ sites active today across 70 countries
- 90+ suppliers onboarded

*"We were able to fully implement Secomea at a production site and onboard 20 technicians as users in **15 minutes**."*

THE RESULT

A structural shift in total cost of ownership

The ROI was not defined by a single savings metric but rather in architectural clarity, structural simplification, and risk reduction.

Remote access moved from a fragmented collection of tools and exceptions to a standardized, governed capability embedded into global operations.

The organization gained a model that scales predictably across sites, suppliers, and regulatory environments – without multiplying complexity.

One tool, one standard, one operating model

The organization established centralized visibility into all remote connections, enforced Zero Trust principles, and implemented audit-ready logging aligned with IEC 62443, NIS2, and NIST.

- ✓ Control replaced improvisation.
- ✓ Consistency replaced exceptions.
- ✓ Governed access replaced inherited risk.

Structural change	Operational effect	Strategic impact
Consolidated dozens of vendor-specific tools into one global OT access platform	Eliminated security exceptions, workarounds, and compensating controls	Reduced third-party risk exposure and simplified governance at scale
Integrated enterprise IAM via SCIM for automated credential lifecycle management	Removed manual provisioning, deprovisioning, and access clean-up	Ensured consistent identity governance across 100+ sites without increasing administrative overhead
Enforced granular, least-privilege, time-limited access with mandatory approvals and full session logging	Improved traceability and reduced audit preparation time and effort	Established a scalable foundation that prevents future rework as regulations evolve

THE BUSINESS OUTCOME

- No more operational friction
- Supplier onboarding accelerated from weeks to minutes
- Infrastructure complexity reduced at scale
- Full global oversight across all remote sessions
- Compliance embedded into daily operations

"Remote access is now simple. Secomea enables us to have logs of everything, so if you access the environment, I have proof of it: I know who you are, what you are asking, and when you access what. That is really important for us"

ABOUT SECOMEA

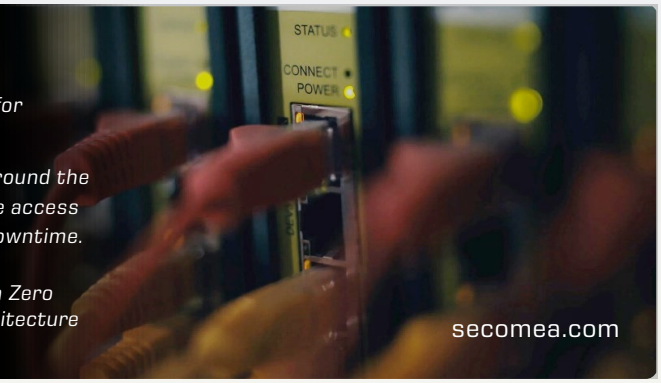
Secomea is a Secure Remote Access (SRA) solution purpose-built for operational environments and cyber-physical systems (CPS).

Over 8,000 manufacturers and critical infrastructure operators around the world use it every day across thousands of sites to manage remote access to industrial equipment, reduce cybersecurity risks, and prevent downtime.

Built for OT, trusted by IT

IEC 62443-certified

Based on a Zero Trust architecture



secomea.com