

SECURE REMOTE ACCESS FOR
CYBER-PHYSICAL SYSTEMS (CPS)

Built for OT. Approved by IT.

One single platform for secure, compliant, and auditable vendor access
– without adding to your IT workload.

SECURE REMOTE CONNECTIONS

Q

Are remote connections really **outbound-only**?

A

Yes. The gateway initiates all traffic from inside the OT network to a central, cloud-based Access Management Server – meaning no inbound connections are required or accepted.

Q

Can a hacker **intercept traffic** between the gateway and the access management server?

A

The Secomea Access Management Server has a unique TLS certificate and key to which a Secomea gateway binds the first time it connects (also known as “ToFu or “Trust-on-first-use”) and against which any subsequent connections are verified.

Q

What does it mean that Secomea’s remote access connections are **firewall-friendly**?

A

All communication is established from within the OT network outward on allowed ports – 11444 and, if necessary, standard web ports 443 (HTTPS) or 80 (HTTP upgraded to TLS), to maintain connectivity.

Q

Are remote connections always **encrypted**?

A

Yes. Secomea’s encryption methods are built on TLS 1.3 connections using x.509 certificates (with 1024-bit keys) and AES256 encryption.

How this helps you

This greatly **simplifies deployment** because it works with most corporate firewall policies by riding over existing outbound web connectivity. IT administrators don’t have to carve out special inbound access exceptions.

How this protects you

To change the server the gateway trusts, one must manually reconfigure the M2M server settings in the gateway. An attacker cannot do this through interception alone. By requiring manual reconfiguration for any changes, **unauthorized redirections (and MitM attacks) are prevented.**

How this helps you

This multi-method approach ensures that remote access will work even under strict network rules, **without requiring manual intervention** from IT.

How this protects you

AES256 encryption secures data **confidentiality**, preventing unauthorized access, while x.509 certificates and TLS 1.3 protocols guarantee **integrity** by protecting data against tampering or corruption in transit, and ensure **authenticity** by verifying all communication endpoints.

Q

How are privileges **managed** with Secomea?

A

Access clearance is managed at the individual level with granular permissions and hierarchy-based user roles following the least privilege principle.

Q

How is access **controlled** with Secomea?

A

Remote access sessions are identity-bound, time-limited, must be explicitly approved, and are logged and recorded.

Q

How is access **monitored** with Secomea?

A

Access sessions can be monitored in real-time, and you can interrupt or terminate them at any time. All user activities are tracked and documented in audit logs, and you can review session recordings to see exactly what users did.

Q

Will it work with **legacy OT** equipment?

A

Yes. Secomea natively supports PLC, HMI, SCADA, DCS, RTU, and all ICS equipment – regardless of age or brand – via USB, Ethernet, UDP/TCP, Layer 2, Layer 3, web proxy, and even serial communication protocols.

Q

Can it **integrate** with our existing IT systems?

A

Yes. Secomea can easily be integrated with your Identity and Access Management system (Microsoft Entra ID, Okta, Azure B2C), your SIEM system (Splunk, Syslog, etc.), your ticketing tools, and other platforms via API.

Q

What does it mean that Secomea is **compliance-ready**?

A

Secomea is certified under IEC 62443-4-1 and compliant with IEC 62443-4-2 and IEC 62443-3-3 standards, and our organizational security measures are based on ISO 27002 and certified in an ISAE 3402 report.

How this protects you

Users can only see the assets they're explicitly allowed to access. If they don't have access permission, it's as if the machine doesn't exist. This **reduces exposure, prevents accidental access, and stops lateral movement**.

How this protects you

No vendor can initiate a remote access session without **prior approval** and **secure identity verification**.

How this protects you

You are **always in control** and can check who accessed which asset, when, and what they did (for **troubleshooting** or **audit purposes**).

How this helps you

You can connect all your industrial equipment, regardless of age or brand, without the need for upgrades or workarounds. Deploy Secomea with **no changes to the existing infrastructure** and use it right away without needing hours of training.

How this helps you

Through our robust **API connections**, you can integrate Secomea with all the tools you already use to run your operations enabling interoperability and ensuring that your daily workflows on the factory floor remain efficient and hassle-free.

How this helps you

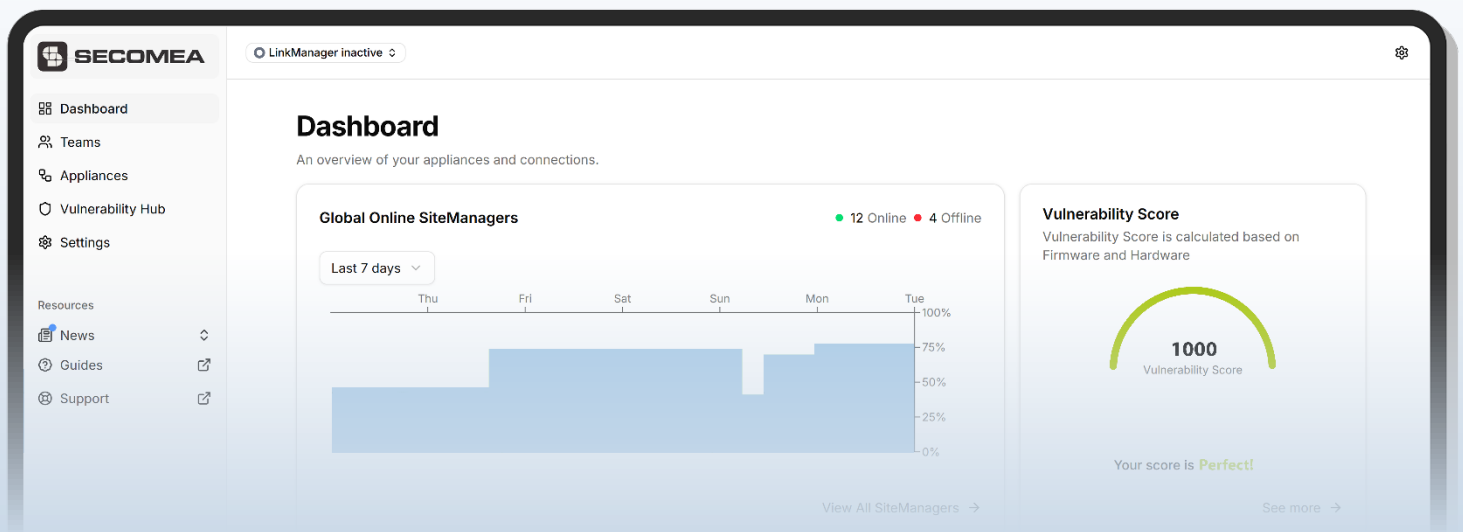
We provide users with features meant to ensure their own compliance with regulatory standards (**NIS2, CRA, NIST 2.0, and ISO 27001**). Audit logs and session recordings are exportable for review and inspection.

Say bye to

- * Vendor chaos from multiple uncontrolled tools (VPNs, TeamViewer, etc.)
- * Audit gaps and compliance headaches
- * Security risks from open inbound connections
- * OT workarounds that bypass IT policies

How it works

SECOMEA Prime



CONNECT
YOUR OT
EQUIPMENT



EDGE GATEWAY

Plug-and-play Industrial IoT gateway (hardware or software) installed on the factory floor and enabling secure remote access and data collection

- ✓ All connections are outbound only

MANAGE USER
PERMISSIONS AND
OVERSEE THEIR
ACTIVITIES



ACCESS MANAGEMENT SERVER

Centralized platform for user access management, approvals, oversight, and auditing – cloud-based, accessible via browser

- ✓ Access is scheduled, approved, and time-limited

ACCESS EQUIPMENT
REMOTELY,
SECURELY AND
COMPLIANTLY



REMOTE ACCESS PORTAL

Lightweight client for remote access using the equipment's native protocols (Modbus, Profinet, Ethernet/IP, etc.) and clientless remote access via RDP, VNC, SSH, and HTTPS

- ✓ Actions done during sessions are logged and exportable

Why IT teams trust Secomea

- 
Central control: Manage all remote access operations in one place, across all sites and vendors
- 
Security by design: Zero Trust architecture, outbound-only traffic, MFA, and no open ports
- 
Audit ready: Full session tracking, role-based permissions, and audit logs and session recordings for compliance
- 
Compliance out of the box: IEC 62443, NIS2, CRA, NIST 2.0, ISO 27001 alignment.
- 
Seamless IT/OT Integration: Prevent silos and bridge teams by connecting Secomea to your IAM (Entra ID, Okta, Azure B2C), SIEM (Syslog, Splunk), support systems – and more.

? Without Secomea

- ✖ Multiple tools, no oversight
- ✖ VPN admin overhead
- ✖ Manual, slow, incomplete audits
- ✖ IT bottlenecks

✓ With Secomea

- ✓ One platform for all vendors and sites
- ✓ Zero Trust, no VPN needed
- ✓ Instantly exportable logs
- ✓ Role-based OT autonomy
= lighter IT workload

EMERSON
MITSUBISHI ELECTRIC
B&R
OMRON
Schneider Electric
P&G
NOVARTIS
Upfield
MQWI
BUHLER

The proven choice for secure OT connectivity



8,000+ customers in 100+ countries



17+ years securing OT remote access



IEC 62443-certified

Standardize, secure, and simplify your remote access



Book a 30-minute technical demo or start a Proof of Concept today.