SECOMEA

Empowering manufacturers to gain control across all production lines

SIMPLICITY

1-day setup and ease of use

Record-speed implementation – as fast as one production site per day. Manage user access to assets in a few clicks and onboard non-IT people without needing hours of training.

VISIBILITY

Secure third-party access

Gain control over your vendors' remote access operations. Adjust their access permissions for the desired time span, authenticate their identities, and monitor their activities.

CONTROL

Always be in the know

Maintain ongoing oversight over your OT assets and networks by relying on audit logs and session recordings to verify who accessed which asset, when, and what they did.

PRODUCTIVITY

Ensure uptime and efficiency

Collect machine data to prevent system failures, perform predictive maintenance, and avoid downtime. Leverage insights from your industrial equipment to improve productivity.

PEACE OF MIND

Cybersecurity & compliance

Rely on a secure-by-design, IEC 62443-certified solution with features purpose-built for compliance with regulations (NIS2, Cyber Resilience Act, etc.) and standards (NIST).

In our customer's own words

SECOMEA IN ACTION

How Procter & Gamble standardized remote access and maintenance globally with Secomea

THE CHALLANGE

Enforcing consistent maintenance operations across sites

"When we couldn't connect remotely, production sites would often take big liberties, making changes on their own."

THE SOLUTION

Replacing multiple tools with a single one easy to set up and use

"We got up and running quickly. We did an evaluation, and it worked out of the box. To the end user, it's no different than plugging into the device directly."

THE RESULTS

Global control and centralized user management

"The access management system was a huge win. We can selectively add remote access users at the machine level. This helped us respond quickly, at a low cost"

P&G

"We want to maintain a high level of standardization, not just digitally, but physically. With Secomea, we can support our sites centrally"

Electrical Platform Leader,
Procter & Gamble

SECOMEA Prime

The all-in-one solution for Secure Remote Access purpose-built for OT and industrial networks

CONNECT

Control your OT environments

Easily deploy our plug-and-play Industrial IoT gateway (hardware or software) enabling secure remote access and data collection

ACCESS

Direct and clientless remote access

Access industrial equipment with a lightweight client via direct tunneling over port 443 using native OT protocols or indirectly, from your browser, via RDP, VNC, SSH, Telnet, HTTPS.

MANAGE

Agentless user & asset management

Control individual access based on the least privilege principle. Provide just-in-time, always-on, or on-demand access to users upon secure authentication via MFA or SSO with Azure AD or Okta.

CONTROL

Real-time activities monitoring

Track who accesses which OT asset and what they do. Gain complete visibility over ongoing connections, access audit logs, and review session recordings for incident response and compliance purposes.

DEFEND

Security by design for CPS

Based on the Zero Trust model and the Defense in Depth approach, Secomea integrates into existing infrastructure frameworks such as the Purdue Model and protects Cyber-Physical Systems.

SECOMEA

Enabling machine builders to service customers from anywhere, securely

COST-EFFICIENCY

Avoid long and expensive trips on site

Get the most out of your technicians' time and expertise by letting them access machines remotely from wherever they are instead of traveling, reducing response times.

EASE-OF-USE FOR NON-IT PEOPLE

User-friendly by design

Secomea is intuitive and OT-friendly, so your service engineers can start using it right away without needing hours of training—and new staff can be onboarded easily.

GAIN LONG-LASTING LOYALTY

Be trusted as a security-conscious supplier

Worldwide-known security certifications, such as IEC 62443-4-1, 4-2, and 3-3, give you (and your customers) higher assurance that your machines are protected and reliable.

ENABLE NEW REVENUE STREAMS

Perform predictive maintenance

Collect machine data to monitor their status, detect vulnerabilities, and prevent system failures. Suggest part replacements and unlock your machines' full value.

GIVE YOUR CUSTOMERS PEACE OF MIND

Secure approval for your SRA solution

With features purpose-built to address international regulations (NIS2, Cyber Resilience Act, etc.) and standards (NIST), you can easily abide by your customers' internal policies.

Connect. Protect. Grow.

Instant version upgrades

As an easy to scale cloud-based solution, Secomea instantly adopts new updates, eliminating the complexities of scheduled rollouts across various sites.

Effortless deployment

Being infrastructure-agnostic, Secomea reduces the TCO by removing the need for on-site installations and changes to the pre-existing infrastructure.

Third-party security certifications

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

Customizations and integrations

Integrate Secomea via API with other tools you use to run your operations—SIEM system (Syslog, Splunk, etc.), support system, IAM system (Azure AD, Okta, etc.), cloud solution (Azure IoT Hub, AWS IoT Core, Cumulocity IoT, Aveva Insight, MQTT data servers, etc.), and more.

Protection against MitM attacks

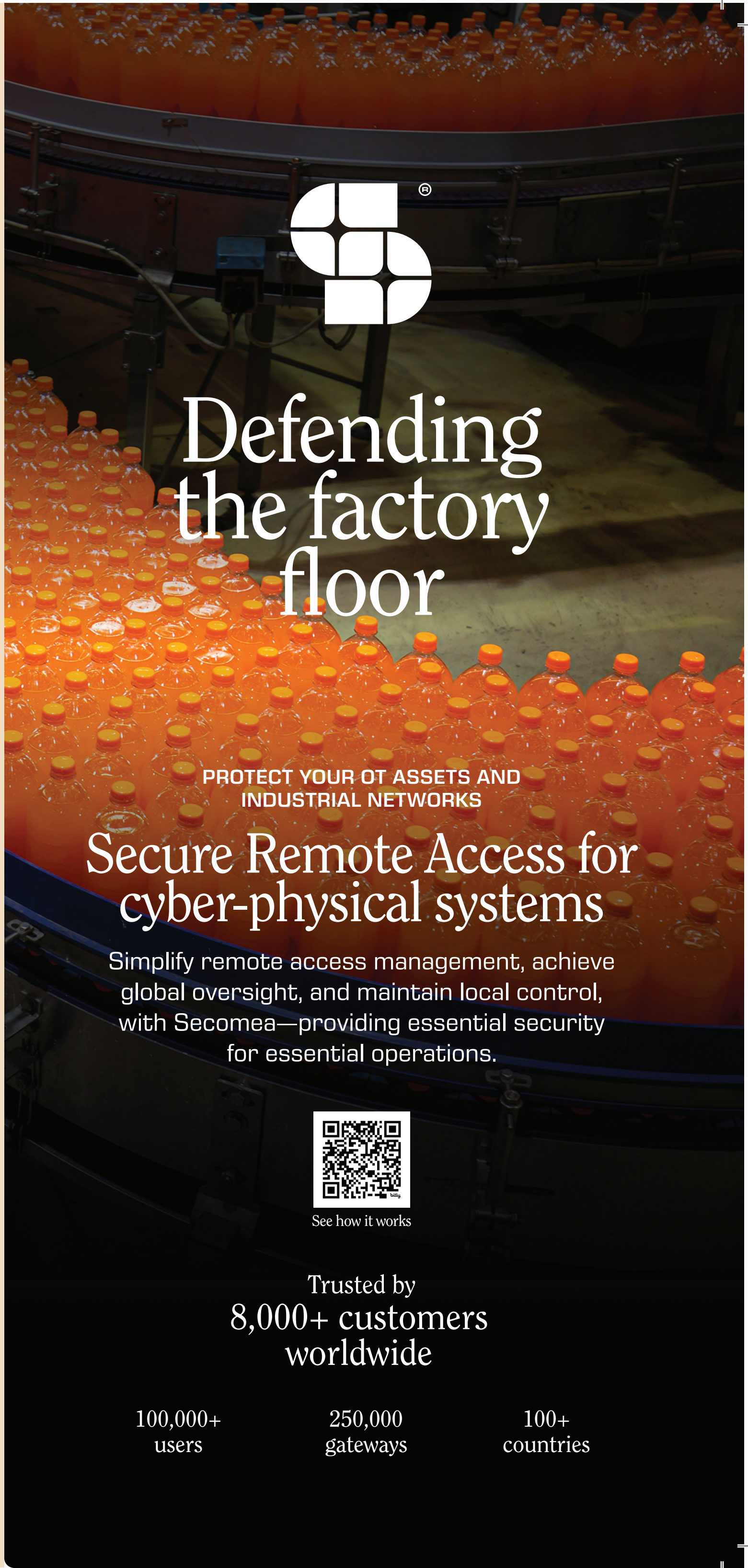
Each Secomea Access Management server has a unique TLS certificate/key, bound on first connection ("Trust-on-first-use," ToFu) and verified for all future connections. By requiring manual reconfiguration for any changes, we prevent unauthorized redirections.

Encryption and network segmentation

Connect your assets via AES 256bit encrypted tunnels based on TLS—aligning seamlessly with the principles of the CIA triad. Restrict connections down to each specific device's IP address and port, both remotely and on-site with I/O ports for physical control.

Crisis management and business continuity

Isolate and contain threats through air gap or island mode configurations. Should a problem arise—e.g., a cyber-attack infecting one or more of your devices—you can use Secomea to cut that machine's access to your network, thereby preventing viruses or malware from spreading to other industrial equipment.



Defending the factory floor

PROTECT YOUR OT ASSETS AND INDUSTRIAL NETWORKS

Secure Remote Access for cyber-physical systems

Simplify remote access management, achieve global oversight, and maintain local control, with Secomea—providing essential security for essential operations.

See how it works

Trusted by
8,000+ customers worldwide

100,000+ users	250,000 gateways	100+ countries