ZERO TRUST ISN'T A TREND. IT'S THE FIX.

The most dangerous assumption in OT? Trust.

Because OT can't afford a single mistake

Traditional *perimeter security* assumes that once a user is inside the network, they can be trusted.

No additional checks. No oversight. No limitations on what the user can reach and tamper with.

IT might absorb the risk of trusting by default – OT can't afford to.

OT networks are increasingly targeted through:

- shared or unmanaged vendor access,
- flat, unsegmented networks,
- legacy systems that can't be patched or monitored.

In operational environments prioritizing **uptime**, **safety**, and **availability**, that level of trust opens the door to disaster.

And that's exactly what Zero Trust aims to fix.

Zero Trust flips the model by replacing implicit trust with **continuous verification and scoped access** – for every user, every device, every session.

	IT Zero Trust	OT Zero Trust
Assets	Users, apps, endpoints	PLCs, HMIs, sensors
Priority	Data confidentiality	Availability, uptime, safety
Users	Employees on managed devices	Vendors, contractors on unmanaged devices
Network	Segmented with VLANs and policies	Often flat, segmented via gateways
Patching	Frequent, regular, and automated	Rare, manual, often not possible or limited
Monitoring	Agent-based, SIEM-driven	Agentless, session-based, and device-focused

Not all Zero Trust is built for OT. This one is.

Most Zero Trust tools are built for IT environments, meaning they're designed around different assets, limitations, and priorities than those found in OT.

Secomea delivers a Zero Trust-based Secure Remote Access solution purpose-built for operational environments.

Legacy assets? *No problem.*
Unmanaged vendors? *Scoped and verified.*
Always-on production? *No downtime required.*

With Secomea, you get all the principles of Zero Trust in action – no complexity, no changes to your existing infrastructure.

- Verify explicitly
- Enforce the least privilege principle
- Assume breach
- Micro-segmentation
- Continuous monitoring and validation

ZERO TRUST, ZERO DOWNTIME

Secomea delivers Zero Trust that actually works for OT

Get agentless, session-based, identity-aware remote access that integrates seamlessly with your existing infrastructure – no downtime, no disruptions.

Zero Trust principles	How Secomea's features bring them to life
Never trust, always verify	MFA, SSO, and certificate-based login for all users – internal or external
Least privilege access	Individual, hierarchy-based user roles and granular permissions to limit user access
Just-in-time (JIT) access	Time-limited, approval-based access to specific assets, on-demand or scheduled
Real-time activities monitoring & alerts	Overview of ongoing sessions, notifications for specific events, and automatically triggered actions
Session visibility & logging	Audit logs documenting who did what and when, and session video-recordings auditable for troubleshooting and compliance
Encryption & micro-segmentation	Outbound-only connections with AES 256-encrypted TLS tunnels that can be restricted remotely or via I/O ports.
Legacy system support	Agentless access that works with unpatchable and legacy OT equipment as well as all industrial protocols
Endpoint protection	Scanning of files transferred remotely for viruses or malware to assess their safety before downloading them in industrial assets

Secomea Prime is **built on a Zero Trust architecture**, requiring that all identities and resources be segmented from one another, thereby enabling fine-grained, identity- and context-sensitive access controls.

Our guiding coding principle is "*zero inherent or implicit trust*".

By enforcing a multi-layered approach to security, Secomea aligns with the Defense-in-Depth (DiD) model and powers Zero-Trust-based Secure Remote Access (SRA) for Cyber-Physical Systems (CPS).

Why choose Secomea for OT Zero Trust

- Designed specifically for OT environments
- Requires no changes to your existing infrastructure
- Uptime-first design – no agents, no reboots, no impact on operations
- Supports compliance with IEC 62443, NIS2, and NIST CSF
- Secure-by-design throughout its lifecycle
- Certified under ISA/IEC 62443
- Used by global manufacturers and OEMs in 100+ countries


Authenticate every user


Grant access only to what's needed


Record and log all sessions


Monitor, detect, and respond in real time


Eliminate risky VPN dependencies


Rely on audit trails for compliance


Enable secure and efficient remote maintenance


Support safe IIoT connectivity without sacrificing uptime

THE INDUSTRIAL SHORTCUT TO ZERO TRUST MATURITY

Remote access is your most critical risk – and your easiest win.

From blind spots to bulletproof.
Here's what Zero Trust in OT should look like.

Before and after Secomea

	Legacy VPN-based Remote Access	Secomea Zero Trust Access
Access scope	Full network exposure	Scoped to one machine
User verification	One-time login	MFA + continuous checks
Auditability	None or basic logs	Session recordings + full logs
Risk of lateral movement	High	Contained and segmented
File transfer	Unchecked	Scanned and logged
Control over sessions	None	Time-bound + revocable access

GET STARTED WITH OT ZERO TRUST

01 Align stakeholders across IT, OT, and leadership

02 Map users, devices, and trust assumptions

03 Enforce identity controls (SSO, MFA, RBAC)

04 Enable least-privilege, time-limited access

05 Segment the network with secure gateways

06 Continuously monitor, log, and refine

Don't stop here. Dig deeper.

More resources for you and your team:

- Zero Trust for OT: what it is, and why it matters
- Why is Perimeter Security no longer enough?
- Why OT needs Zero Trust security now
- How does Zero Trust work in OT?
- Zero Trust in OT vs. IT
- How to implement Zero Trust in OT: a guide
- The role of SRA in your OT Zero Trust strategy

Download the full whitepaper for free

Want support in securing your OT operations?
See how simple OT Zero Trust can be.

Book a demo today