WHITEPAPER

Zero Trust for OT, explained

Why operational environments need a new approach to cybersecurity – and how to make it happen

SECOMEA

About Secomea

Secomea is a Secure Remote Access (SRA) solution purpose-built for operational environments and cyber-physical systems (CPS).
Over 8,000 customers around the world use it every day across thousands of sites to manage remote access to industrial equipment, reduce cybersecurity risks, and prevent downtime.

Table of Contents

01

The problem with perimeter-based security

In the past, many organizations relied on what's known as the **perimeter model**, and the most common way of securing infrastructure and applications was to **protect the perimeter.**

The perimeter model, often referred to as the "**trusted subsystem**", assumes that anything inside the perimeter (i.e., the subsystem) is safe.

The idea was simple: build a strong perimeter – like a castle wall – and trust anything inside.

Why is perimeter security no longer enough

The problem? Once someone breached that wall and got inside the perimeter, they often had free rein and could access resources they shouldn't. No additional checks. No oversight.

This "implicit trust" becomes dangerous when just one device or user is compromised, as they'd have broader access across the network.

The model created a false sense of security, leaving systems vulnerable to insider threats, lateral movement, and undetected compromise. But also, it couldn't account for the growing sophistication of today's cyberattacks.

Zero Trust starts where perimeter security stops

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

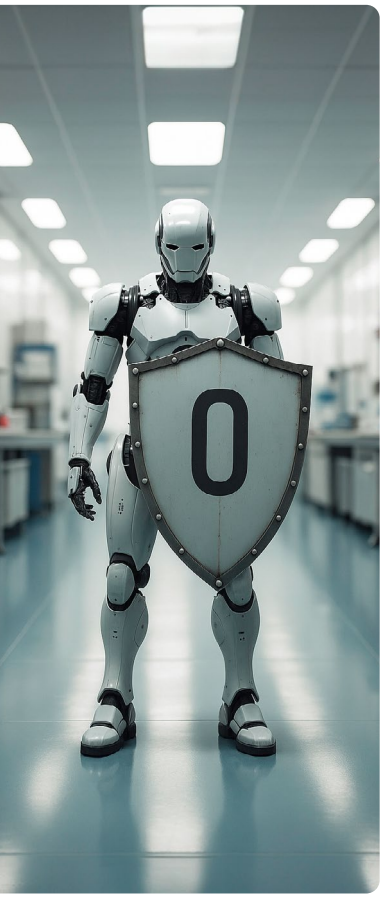
Zero Trust replaces implicit trust with continuous verification – for every user, every device, every session.

But shifting away from a perimeter mindset isn't always easy – especially if you've spent years building systems around it.

So, let's make this more tangible. How can you implement Zero Trust in operational environments where legacy systems, flat networks, and availability concerns still dominate?

This guide helps you find out. We'll break down what Zero Trust really means, how it applies to OT environments, and how to move from theory to action.

Read on and feel free to reach out to us should you still have questions or if you want to be supported in your own OT Zero Trust implementation.



02

What is Zero Trust and why OT needs it now

Zero Trust was created to fix the flaws of perimeter-based security. Its core idea is: "**never trust, always verify**".

No trust is granted by default based on familiarity with the user or location of the device.

Every user, device, or system **must prove it can be trusted – every time.**

To this end, Zero Trust includes practices like:

- strong user authentication,
- network segmentation to limit movement,
- least privilege access (giving users and systems only access to what they need),
- constant monitoring and validation of access permissions.

It uses modern tools like risk-based multi-factor authentication, endpoint protection, and cloud security to ensure that access is secure in real-time and based on context.

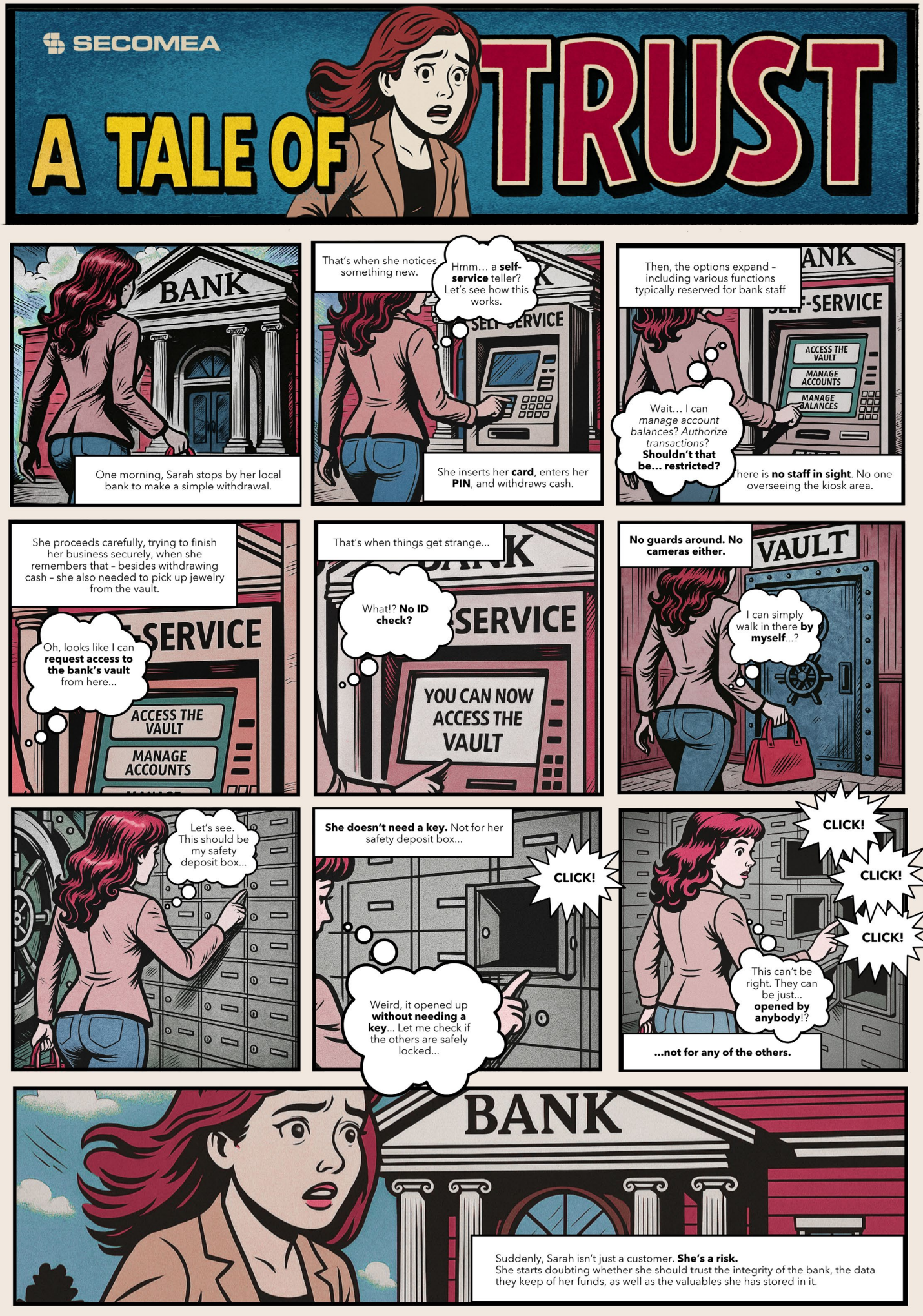
Ultimately, Zero Trust is more than a security tactic – it's a comprehensive approach to keep up with the threats we face today.

While it may sound complex, when implemented correctly, ***Zero Trust not only strengthens security but also simplifies it.***

Why Zero Trust matters, and how a trip to the bank can help explain it

Being used to working with "trusted subsystems," many of us might find it hard to grasp what Zero Trust is and why we need it. Yet, we're already familiar with the concept in the physical world – where locked doors, ID checks, and access restrictions are normal safeguards.

To show you what we mean, let's take the example of Sarah.


SECOMEA
A TALE OF TRUST
BANK
One morning, Sarah stops by her local bank to make a simple withdrawal.
That's when she notices something new.
Hmm… a **self-service** teller? Let's see how this works.
She inserts her **card**, enters her **PIN**, and withdraws cash.
Then, the options expand – including various functions typically reserved for bank staff
ACCESS THE VAULT
MANAGE ACCOUNTS
MANAGE BALANCES
Wait… I can *manage account balances? Authorize transactions?* **Shouldn't that be… restricted?**
There is **no staff in sight**. No one overseeing the kiosk area.
She proceeds carefully, trying to finish her business securely, when she remembers that – besides withdrawing cash – she also needed to pick up jewelry from the vault.
Oh, looks like I can **request access to the bank's vault** from here...
ACCESS THE VAULT
MANAGE ACCOUNTS
That's when things get strange...
What!? **No ID check?**
YOU CAN NOW ACCESS THE VAULT
No guards around. No cameras either.
VAULT
I can simply walk in there **by myself**...?
Let's see. This should be my safety deposit box...
She doesn't need a key. Not for her safety deposit box...
CLICK!
Weird, it opened up **without needing a key**... Let me check if the others are safely locked...
CLICK!
CLICK!
CLICK!
This can't be right. They can be just... **opened by anybody**!?
...not for any of the others.
BANK
Suddenly, Sarah isn't just a customer. **She's a risk.**
She starts doubting whether she should trust the integrity of the bank, the data they keep of her funds, as well as the valuables she has stored in it.

If that sounds absurd, it's because it is. And yet, this is exactly what happens in a trusted subsystem: once inside the network, users (or attackers) often have access to far more than they should. That's why the perimeter model no longer works – and why Zero Trust is essential.

Verify explicitly	Trust is never assumed based solely on the location of the user or device. Every access request must be authenticated and verified before being authorized based on all available data points (user identity, location, device health, etc.), regardless of whether it originates from inside or outside the network.
Enforce the least privilege principle	Users and devices are granted only the minimum level of access needed to perform their tasks. With just-in-time and just-enough-access, if an account is compromised, the attacker's ability to move laterally within the network is limited.
Assume breach	Instead of assuming your network is secure just because it's behind a firewall or VPN, Zero Trust operates with the mindset that a breach has either already happened or is inevitable. Implementing encryption ensures that data transmitted over the network remains secure, even if intercepted. Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide multiple forms of identification before accessing the network.
Micro-segmentation	This involves dividing the network into smaller zones with strict controls to limit lateral movements across segments and minimize the potential damage of a security breach. So that, even if one segment is compromised, the rest of the network remains protected.
Continuous monitoring and validation	Zero Trust networks employ continuous monitoring and analytics to keep re-evaluating access requests and anomalous behaviors and detect potential security threats in real-time. This helps in identifying and responding to security incidents promptly.

Let's now try to rewrite the story with the **5 core principles of Zero Trust** in mind:


SECOMEA
REWRITING THE STORY
THE ZERO TRUST WAY


When Sarah arrives at the new branch office of her bank, she encounters a stringent yet reassuring **Zero Trust approach**.
BANK
To gain access, she must **validate her legitimacy**.


BANK
Okay… need to tap my card just to get in.
Card tap: one-factor authentication – "**something she has**".

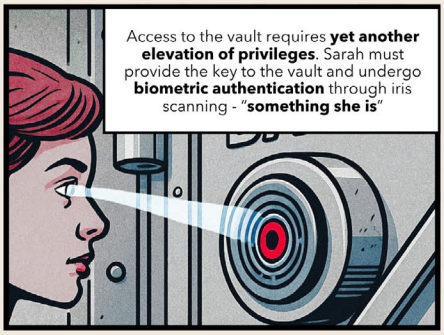

INPUT YOUR PIN
Inside, her access is restricted. Only the ATM is available. And she needs to re-authenticate herself with card and **PIN** - "something she has" and "**something she knows**."


Despite having multiple accounts, she can only view and access funds tied to the account linked to the presented card, and certainly not anyone else's.
WITHDRAW FROM THIS ACCOUNT
CHECK ACCOUNT BALANCE
PLEASE ASK FOR ASSISTANCE FROM THE BANK STAFF FOR ADDITIONAL SERVICES
That's **least privilege** and **micro-segmentation** in action.


After withdrawing cash, she remembers that she also needs to pick up jewelry from the vault. So she **heads inside the branch office**, when only existing customers are permitted entry.
BANK OFFICE
Looks like I need to tap my card, *again*...
EXISTING CUSTOMERS ONLY


As Sarah enters the bank, she encounters the bank teller, who recognizes her from previous visits. However, **familiarity doesn't override verification**.
Good to see you again, Sarah. May I see your **ID**?


SECURITY
Sarah's trip to the vault is accompanied by a **security escort**, and she is under **constant video surveillance** - exemplifying the **continuous monitoring** and **physical security** components of Zero Trust.


Access to the vault requires **yet another elevation of privileges**. Sarah must provide the key to the vault and undergo **biometric authentication** through iris scanning - "**something she is**"


Meanwhile, the bank's security personnel is **monitoring her activities in real-time**.


BANK
Sarah leaves the bank, feeling confident about the security measures protecting her financial assets.

03

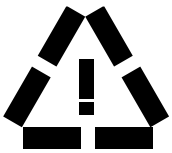
How Zero Trust works in OT – and how it differs from IT-centric Zero Trust

Imagine a factory where every employee, contractor, and vendor uses the same badge to enter the building.

Once inside, that badge gives them access to everything – the production floor, the control room, the server rack, even the executive office. No additional checks, no restrictions.

It's convenient, but risky.

If someone loses a badge or if an attacker gets inside, they can move freely throughout the facility, accessing sensitive equipment, systems, or data they shouldn't touch. **That's what perimeter-based security looks like:** strong at the edge, but wide open once you're in.



Now, picture the same factory, but with a Zero Trust approach. Everyone still enters with a badge, but that badge only gets them into the areas they're authorized to work in. A maintenance technician can access the shop floor but not the control room. A contractor can inspect a machine, but can't plug into the network. Access to high-risk areas like the control room or PLC cabinets requires multi-factor authentication, temporary access tokens, and real-time approval.

Rigorous verification mechanisms should be employed at every access point to mitigate the risk of unauthorized access and potential security breaches.

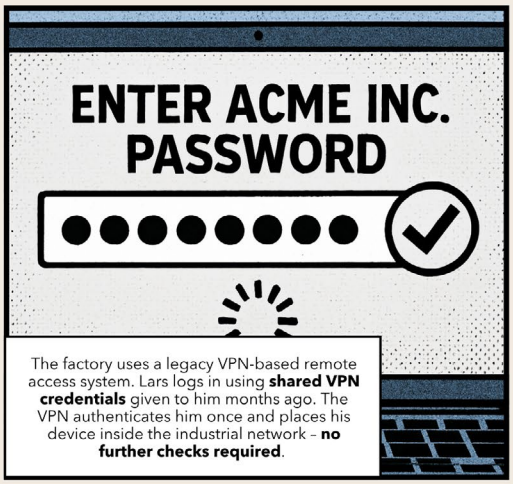
Even once inside, activity is monitored – not because people aren't trusted, but because systems shouldn't assume trust based on perceived legitimacy or origin. If someone tries to access something outside their role, the system flags it or blocks it altogether.

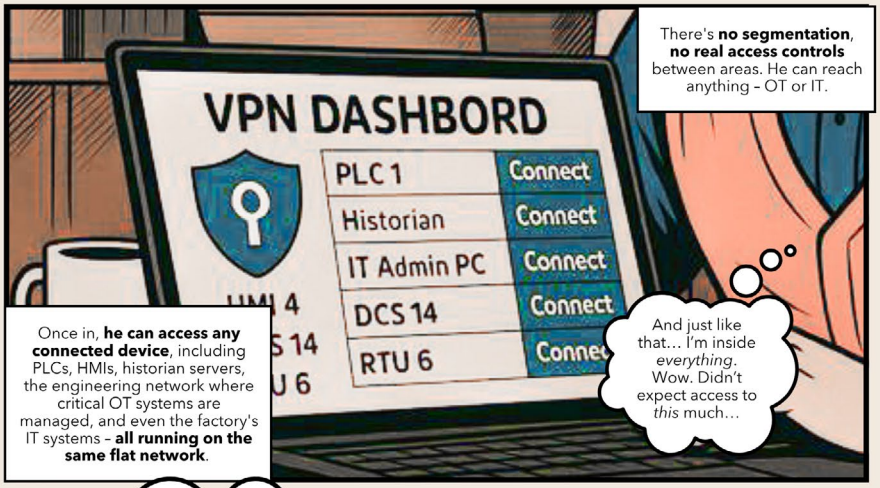
Let's now see how the two security models differ when applied to a common OT remote access use case.

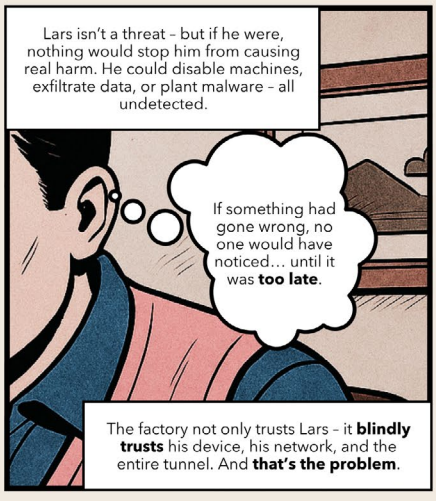
PERIMETER SECURITY VS. ZERO TRUST

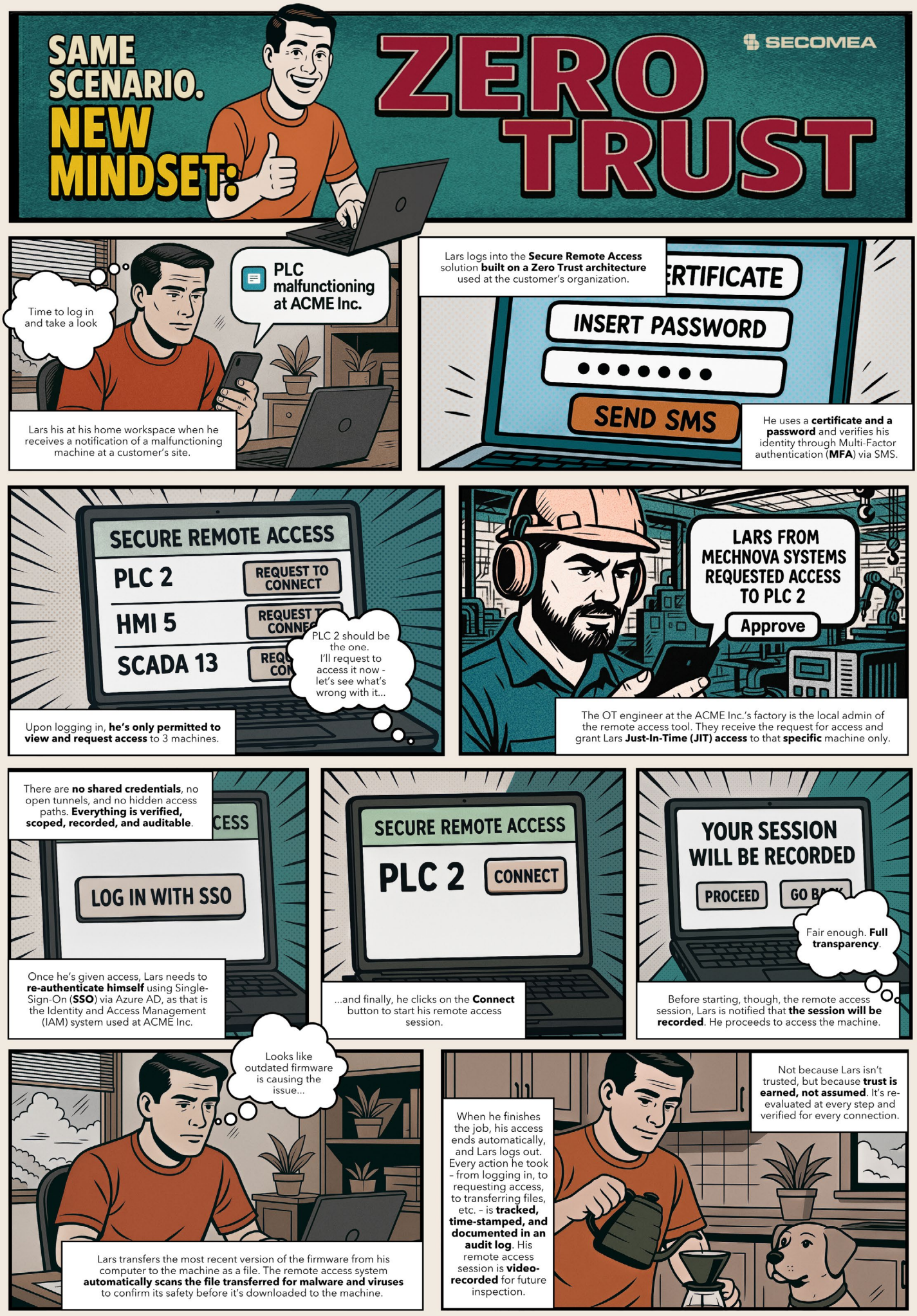
AN INDUSTRIAL REMOTE ACCESS STORY

SECOMEA








SAME SCENARIO.
NEW MINDSET:
ZERO TRUST
SECOMEA
Time to log in and take a look
PLC malfunctioning at ACME Inc.
Lars his at his home workspace when he receives a notification of a malfunctioning machine at a customer's site.
Lars logs into the Secure Remote Access solution built on a Zero Trust architecture used at the customer's organization.
ERTIFICATE
INSERT PASSWORD
SEND SMS
He uses a certificate and a password and verifies his identity through Multi-Factor authentication (MFA) via SMS.
SECURE REMOTE ACCESS
PLC 2
REQUEST TO CONNECT
HMI 5
SCADA 13
PLC 2 should be the one. I'll request to access it now - let's see what's wrong with it...
Upon logging in, he's only permitted to view and request access to 3 machines.
LARS FROM MECHNOVA SYSTEMS REQUESTED ACCESS TO PLC 2
Approve
The OT engineer at the ACME Inc.'s factory is the local admin of the remote access tool. They receive the request for access and grant Lars Just-In-Time (JIT) access to that specific machine only.
There are no shared credentials, no open tunnels, and no hidden access paths. Everything is verified, scoped, recorded, and auditable.
LOG IN WITH SSO
Once he's given access, Lars needs to re-authenticate himself using Single-Sign-On (SSO) via Azure AD, as that is the Identity and Access Management (IAM) system used at ACME Inc.
SECURE REMOTE ACCESS
PLC 2
CONNECT
...and finally, he clicks on the Connect button to start his remote access session.
YOUR SESSION WILL BE RECORDED
PROCEED
Fair enough. Full transparency.
Before starting, though, the remote access session, Lars is notified that the session will be recorded. He proceeds to access the machine.
Looks like outdated firmware is causing the issue...
Lars transfers the most recent version of the firmware from his computer to the machine as a file. The remote access system automatically scans the file transferred for malware and viruses to confirm its safety before it's downloaded to the machine.
When he finishes the job, his access ends automatically, and Lars logs out. Every action he took - from logging in, to requesting access, to transferring files, etc. - is tracked, time-stamped, and documented in an audit log. His remote access session is video-recorded for future inspection.
Not because Lars isn't trusted, but because trust is earned, not assumed. It's re-evaluated at every step and verified for every connection.

Implementing Zero Trust in OT isn't the same as in IT

In both physical and digital industrial environments, you can't rely on trust being inherited **simply because someone** or something **is "inside".**

The story of Lars shows how Zero Trust can transform remote access from an open-ended risk to a tightly controlled, auditable interaction. But it also surfaces a deeper point: applying Zero Trust in industrial environments **isn't just a matter of enforcing the same IT rules in a new setting.**

While the principles are consistent, the **realities of OT networks, devices, and user behavior demand a fundamentally different implementation.**

To understand why, it helps to look at how Zero Trust differs between traditional IT environments and the unique context of OT.

	IT Zero Trust	OT Zero Trust
Assets	Users, apps, endpoints	PLC, 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

Remember Stuxnet? That's what can happen when you don't follow Zero Trust

The **Stuxnet** malware incident stands as a stark reminder of the consequences that can arise from failing to adhere to Zero Trust principles. It was one of the most sophisticated cyberattacks in history, but **all it actually did was exploit trust assumptions.**

Bypassing traditional defenses of industrial networks, the malware targeted SCADA systems, moved laterally to PLCs, and altered operations undetected, sabotaging nuclear centrifuges. Ultimately, it caused significant damage to critical infrastructure and posed a serious threat to global security.

All because internal systems trusted too easily and verified too little.

It's an eye-opener on how **trust *cannot* be a security strategy.** Whether you're protecting a bank, a factory, or a network, Zero Trust gives you the layered defenses needed to stop threats before they escalate.

OT-focused Zero Trust vs. IT-centric Zero Trust

Zero Trust in OT and industrial environments differs significantly from general, IT-centric Zero Trust in goals, constraints, and implementation.

01

The asset types and protocols are fundamentally different

IT Zero Trust focuses on users, cloud apps, laptops, mobile devices, and web access.

OT Zero Trust, instead, deals with industrial assets like PLCs, HMIs, RTUs, sensors – often running proprietary or legacy protocols (e.g., Modbus, OPC UA, PROFINET).

Therefore, **Zero Trust in OT must work with agentless devices and older-generation communication standards** not designed for modern security.

02

In OT, availability takes priority over confidentiality

While IT Zero Trust's top concern is protecting data confidentiality and integrity, the primary goal in OT is availability and uptime.

OT Zero Trust must be designed for non-disruptive enforcement – verifying access without breaking real-time control, introducing latency, or triggering downtime.

03

Users and access patterns are different

In IT, Zero Trust needs to primarily secure employees' access to cloud services from company-managed devices.

In OT, on the other hand, external vendors, service engineers, and subcontractor technicians also need to access industrial systems, mostly from unmanaged devices and unknown networks.

This calls for stronger session control, as well as time-based access and approvals, especially for third parties, **with detailed audit trails.**

04

OT networks are often flat and hard to segment

While network segmentation is standard in IT – using VLANs, firewalls, and identity-based access control – many operational environments still run flat networks with little segmentation. Devices may not support modern identity or access policies.

OT Zero Trust often starts with **micro-segmentation and isolation, using tools that work at the network level rather than at the endpoint level.**

05

Patching and updates aren't always an option in OT

While you can roll out updates, security patches, and new tools frequently in the IT domain, OT devices may be 10+ years old, vendor-locked, or operate in regulated environments where patching is rare or risky.

You need a Zero Trust model that **provides security *around* unpatchable devices, rather than *on* them** – like secure remote access gateways, traffic control, and strong authentication before interaction.

06

Visibility and monitoring must span both IT and OT

While you can monitor user behavior, endpoints, and cloud services via agents and SIEMs in IT, implementing Zero Trust in OT means working across hybrid IT/OT environments, often without agents.

You need tools that monitor remote access, device communications, and human-machine interactions, **bridging IT and OT monitoring and generating logs that are OT-aware** (e.g., who accessed which PLC and what did they change).

04

A practical guide to implementing Zero Trust in operational environments

Implementing Zero Trust in OT environments requires more than applying IT strategies to industrial systems.

OT networks have unique priorities, legacy assets, and availability requirements that demand an approach tailored to operational realities.

Whether you're in manufacturing, critical infrastructure, oil and gas, transportation, or energy – Zero Trust offers a resilient framework for securing systems without compromising uptime.

Moving beyond perimeter-based security

Traditional security models rely on the assumption that everything inside the network – a.k.a., the trusted subsystem – is "whitelisted" as safe, and threats only come from the outside. These models depend heavily on firewalls, VPNs, and static trust zones.

But in modern operational environments, where remote access is common and IIoT devices are proliferating, this approach falls short.

Zero Trust eliminates implicit trust and replaces it with continuous authentication and verification of every user, device, and session. This shift is essential for environments where third-party access, unpatchable systems, and always-on operations are the norm.

Key components of an OT-centric Zero Trust strategy

ZERO TRUST MODEL (ZTM)

Elimination of implicit trust across identity, devices, applications, data, and networks.

ZERO TRUST NETWORK ACCESS (ZTNA)

Session-based, least-privilege access in Software-Defined Perimeters (SDP)

SECURE IDENTITY VERIFICATION

Multi-Factor Authentication (MFA), Single Sign-On (SSO), and role-based access control (RBAC)

ENDPOINT PROTECTION

Vulnerability and patch management, antivirus, transferred file scanning

MICRO-SEGMENTATION

Access boundaries down to each device's IP and port, remotely and on site via I/O ports

CONTINUOUS MONITORING

Real-time tracking of user behavior, device activity, and network traffic

Where to start: a phased, practical implementation approach

Zero Trust is not a one-time project. It's a continuous strategy that should evolve with your operations, technologies, and threat landscape. A phased approach helps minimize disruption while steadily strengthening your security posture.

01

1. Educate stakeholders on Zero Trust principles and OT security fundamentals

- Break down Zero Trust into practical, operational concepts relevant to OT environments
- Highlight the risks of legacy protocols, flat networks, and implicit trust
- Align security messaging with roles across IT, OT, and executive stakeholders

02

2. Assess your current state

- Map critical OT assets, users, data flows, and entry points and prioritize high-risk use cases like third-party access and remote maintenance
- Identify trust assumptions, shared credentials, and unmanaged connections
- Evaluate how remote access, vendor access, and legacy systems are controlled

03

3. Strengthen identity and access controls

- Enforce Multi-Factor Authentication (MFA), Single Sign-On (SSO), and Role-Based Access Control (RBAC)
- Eliminate shared credentials; assign unique, auditable identities to all users
- Centralize identity management across IT and OT environments

04

4. Apply least privilege and Just-in-Time access

- Limit users, machines, and third parties to only the systems and actions they need
- Use time-bound and approval-based sessions for contractors and vendors
- Dynamically adjust permissions based on risk and operational context

05

5. Secure endpoints and legacy devices

- Perform device health checks before granting access
- Use ICS- and IIoT-specific endpoint protection and monitoring tools
- Apply external security controls around unpatchable or outdated devices

06

6. Segment and isolate networks

- Use micro-segmentation to contain threats and restrict lateral movement
- Separate IT and OT environments logically and physically
- Deploy secure access gateways instead of exposing full networks through VPNs

07

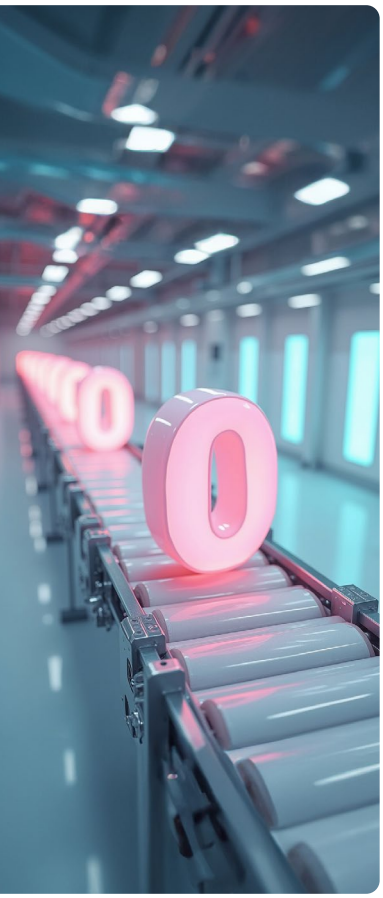
7. Monitor and analyze continuously

- Log all access requests, remote sessions, and critical system interactions
- Use behavior analytics and threat detection to flag anomalies in real time
- Feed data into centralized platforms (e.g., SIEMs) for visibility and compliance

08

8. Iterate and scale

- Refine access policies based on audits, threat intelligence, and regulatory requirements (e.g., NIS2, NIST CSF, IEC 62443)
- Start with a contained deployment, validate its impact, and then expand Zero Trust across more systems, facilities, and user groups
- Align improvements with business goals and operational constraints



05

How Secomea brings Zero Trust to life in your OT infrastructure

Adopting Zero Trust in OT comes with unique obstacles. Common implementation challenges include:

- **Legacy system limitations:** Older devices may not support modern security protocols
- **Downtime risk:** Security must be applied without interrupting production
- **Third-party access:** Vendor and contractor management requires strong governance
- **Skills gap:** Industrial cybersecurity expertise is often scarce

Partnering with OT-specialized vendors can accelerate progress and reduce complexity.

Why do you need an OT-specific solution

Under the Zero Trust framework, systems have to be designed and operated in a way so that *as little as possible can be done with them beyond their intended use*. In other words, **systems should only perform their intended functions** – and nothing more. This helps limit how much damage an attacker can do if they gain access.

However, **that's nearly impossible when using an IT-centric solution** in OT environments, which have very different constraints and requirements – from legacy protocols to limited tolerance for downtime. OT environments require solutions that:

- work without agents or invasive software
- respect operational uptime and safety requirements
- understand industrial protocols and systems
- integrate access control with network isolation

Only with an OT-aware solution can you implement Zero Trust principles without overhauling your existing infrastructure.

Secomea is purpose-built for these needs

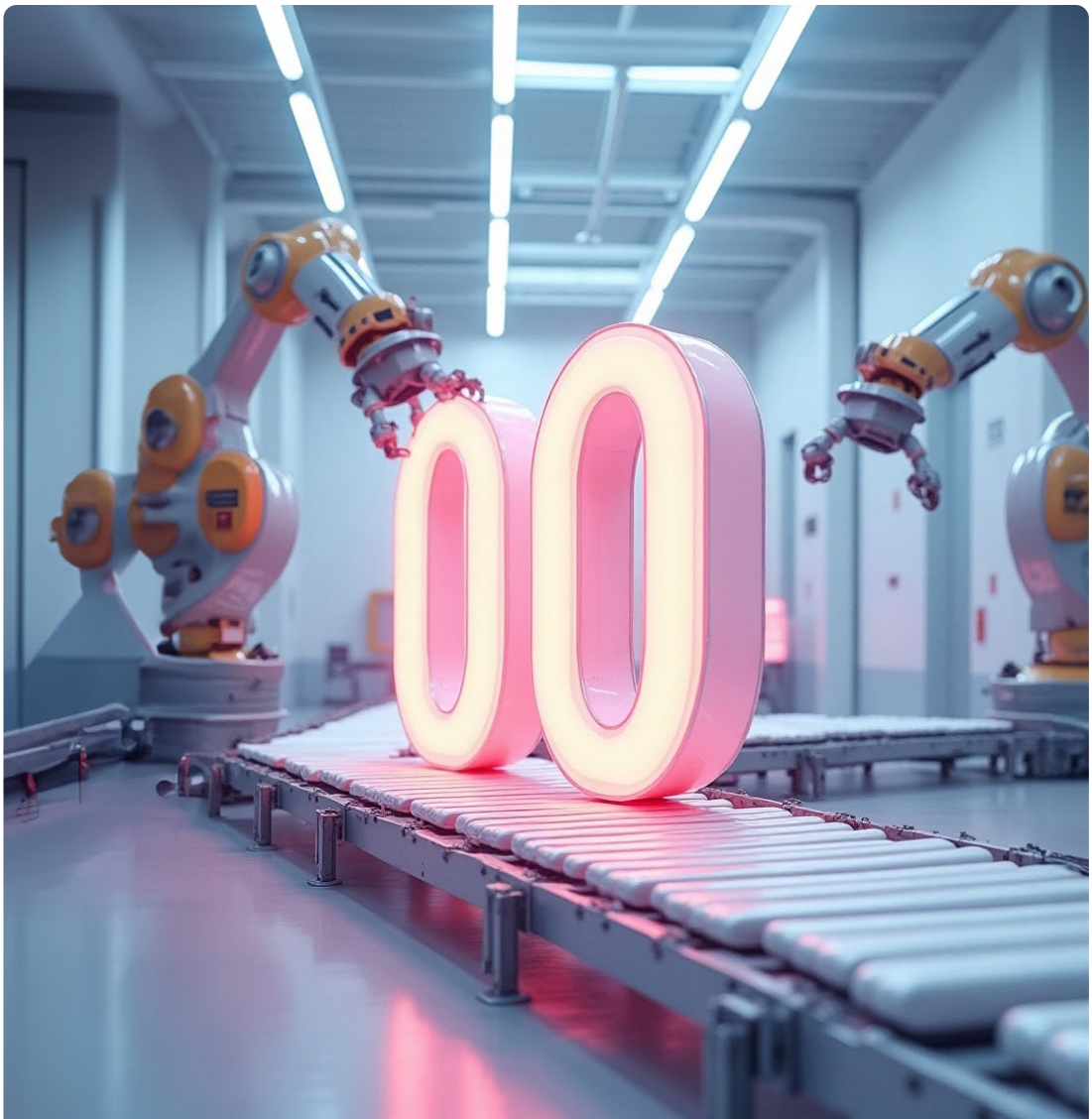
Secomea is custom-made for OT, tailored to support Zero Trust in industrial networks, and secure-by-design throughout its lifecycle for industrial assets and networks. Therefore, our platform can help you implement Zero Trust principles without overhauling your existing infrastructure.

To validate that, Secomea has also been independently audited for compliance with **ISA/IEC 62443-4-1**, the global standard for secure product development in industrial automation and control systems (IACS). This ensures it meets the security and lifecycle requirements **expected in OT**.

More about IEC 62443-4-1

Secomea is securing network, applications, and data resources, with a focus on providing an identity-centric policy model for controlling access, as certified in our third-party attestation of compliance with the ISA/IEC 62443-4-1 standard for Security Development Lifecycle Assurance (SDLA).

This certification confirms Secomea follows secure development lifecycle practices, including secure-by-design engineering, patch management, and product EOL procedures.



How Secomea fits into your Zero Trust strategy

At Secomea, our guiding coding principle is *"zero inherent or implicit trust".*

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

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).

Secomea supports Zero Trust by:

- Enforcing granular, role-based access with Privileged Access Management and grouping features **(ZTNA)** and authenticating users with MFA (via SMS) or Single Sign-On (Azure AD, Okta) before granting access **(Identity verification)**.
- Securing access through approval-based workflows, just-in-time (JIT) access windows, and secure file transfer with built-in malware scanning **(Endpoint protection**
- **Monitoring** sessions in real time, logging all user activity with audit trails and session recordings, and protecting communications with AES 256 encryption and strict **network segmentation.**

This ensures your Zero Trust implementation supports operational continuity while raising your security maturity.

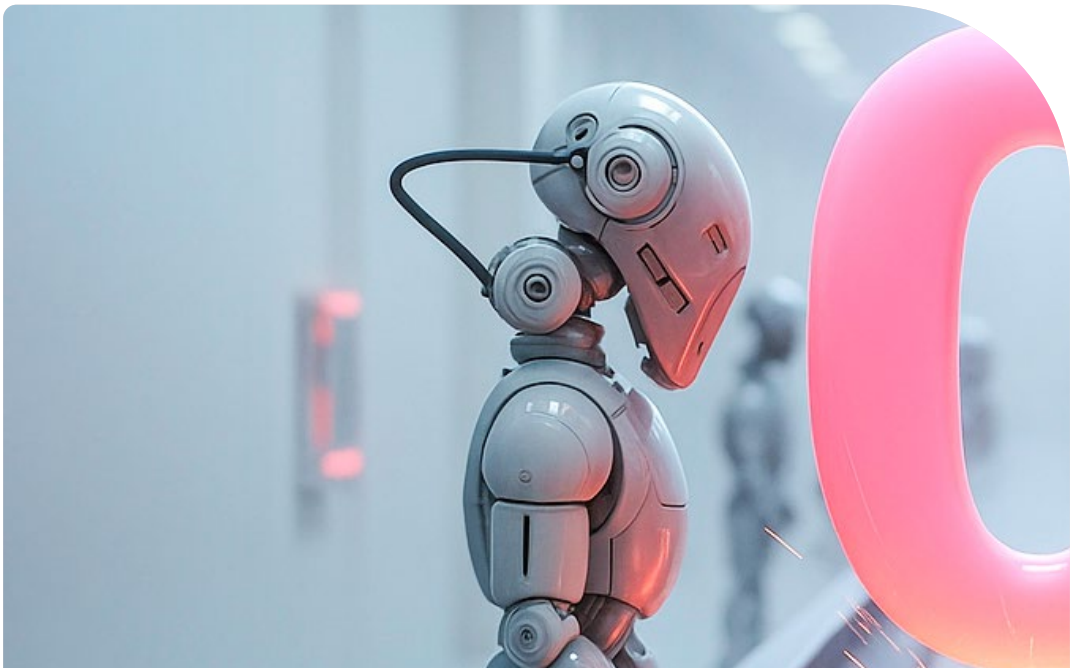
SECOMEA FEATURES POWERING ZERO TRUST IN OT			
	ZTNA & Identity Verification	Privileged Access Management	Set up hierarchy-based user roles individually or use the advanced grouping feature to manage user rights in bulk.
		Granular access control	Control access on an individual level with granular, role-based permissions.
		MFA & SSO	Access is granted only after secure identity verification with MFA via SMS or Single Sign-On (Azure AD or Okta).
	Endpoint protection	Access granted only after request approval	Condition access to the approval of user requests, indicating the session's reason, timing, and duration.
		Just-in-time (JIT) access	Grant temporary, time-limited access to specific assets, on-demand or scheduled.
		Secure file transfer	Scan files transferred remotely for viruses or malware to assess their safety before downloading them.
	Monitoring & Segmentation	Real-time activities monitoring & alerts	View ongoing sessions, receive notifications for specific events, and automate triggered actions.
		Audit logs & session recordings	Track every activity to document who did what and when for troubleshooting and audit.
		Encryption and network segmentation	Secure asset connections with AES 256-encrypted TLS tunnels. Restrict access remotely or via I/O ports.

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

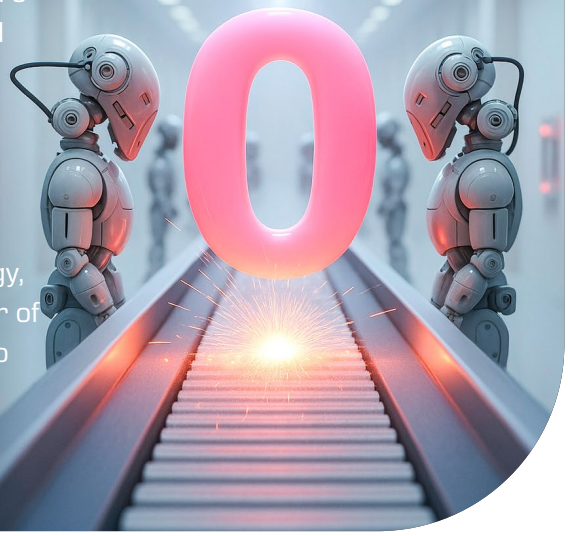


Get started with Zero Trust-based Remote Access today!

Zero Trust isn't about making systems harder to use – it's about making them safer to operate.

Secomea strengthens Zero Trust implementation and helps you meet security and operational goals simultaneously.

With the right strategy and OT-focused technology, security becomes a driver of resilience, not a barrier to productivity.



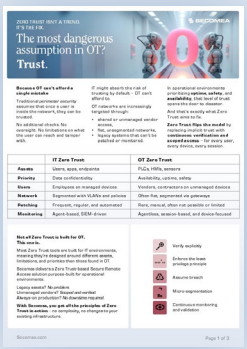
Why choose Secomea for OT Zero Trust

- 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

Want the essentials in one place?

Download our Zero Trust datasheet



Don't stop here. Dig deeper.

- Zero Trust for OT: what it is, why it matters, and how to make it work
- What is Perimeter Security – and why is it no longer enough for OT?
- What is Zero Trust security, and why OT needs it now
- How does Zero Trust work in OT?
- Zero Trust in OT vs. IT – why a one-size-fits-all approach fails
- How to implement Zero Trust in OT: a practical step-by-step guide
- The role of Secure Remote Access in your OT Zero Trust strategy

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

Book a demo today

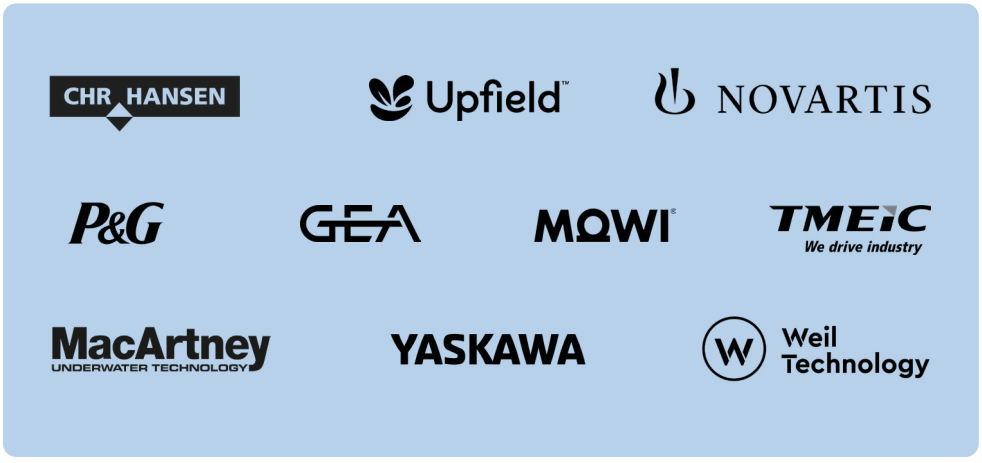
About Secomea

Offices in Denmark (HQ), US, China, Japan

70+
Partners

+8,000
customers worldwide

+250,000
Gateways installed



www.secomea.com