SECOMEA DATASHEET

Secure Remote Access tailored for OT

Advancements in connectivity, automation, and Industry 4.0 technologies are driving significant improvements in operational efficiency for industrial organizations.

However, traditional remote access tools fail to deliver the robust control, visibility, and security required to safeguard critical industrial operations.

As the attack surface expands, threats become more sophisticated, and regulators tighten compliance requirements – outdated IT-designed solutions struggle to keep up with the evolving OT demands.

A modern OT secure remote access solution needs to boost productivity, reduce complexity, and ensure compliance with regulatory standards.

Key challenges

Shorten mean-time-to-repair (MTTR)
Improve efficiency and productivity metrics, reduce unplanned downtime

Inadequacy of IT-centric systems
VPNs, VDIs, jump servers, PAM solutions don't address OT-specific needs

Amplified cybersecurity risks
Broadened attack surface and more frequent and sophisticated cyberattacks

Compliance demands
Increased regulatory pressure to intensify security for critical operations

Secomea's Solution

Our Secure Remote Access solution simplifies remote access while strengthening security and control, improving operational efficiency, and enhancing UX for both internal and third-party users.

SECURITY	Tailored for OT/ICS environments	Secomea's Secure Remote Access solution is specifically designed to meet the unique requirements of complex operational technology (OT) and industrial control system (ICS) environments.
	Architecture-specific security	Secomea combines industry best practices such as the Zero Trust model and the Defense in Depth approach to integrate into existing infrastructure frameworks such as the Purdue Model and protect cyber-physical systems (CPS).
	Regulatory compliance ensured	Secomea is certified under IEC 62443-4-1 and compliant with IEC 62443-4-2 and IEC 62443-3-3 standards; the solution offers features purpose-built to address legal requirements and mitigate the risk of non-compliance.
CONTROL	Simplified user access management	Streamline the credential management process by creating, provisioning, and managing user permissions with an intuitive access management server, reducing the need for extensive administrative resources.
	Mitigation of risk of unauthorized access risks	Authenticate users securely via SSO (Azure AD, Okta, etc.) before connecting them to the equipment they are authorized to access under the least privilege principle, restricting lateral movement to prevent threats from spreading within or across networks.
	Ongoing monitoring and oversight	Gain complete visibility and control over remote access activities. Get an overview of ongoing connections, access audit logs tracking each user action, and review session recordings for incident response and compliance purposes.
EFFICIENCY	Record-speed implementation	Being purpose-built for OT and infrastructure-agnostic, Secomea can seamlessly and quickly be deployed in any operational environment and be used right away without needing hours of training.
	Optimized response time	Secomea's flexible solution ensures consistent performance and seamless access to business-critical assets, even in high-latency environments, no matter the location. Prevent downtime with data-driven predictive maintenance.
	Versatile remote access	Secomea offers a variety of remote access options – ranging from direct remote access via VPN tunneling over port 443 using the equipment's native protocols (e.g., Modbus, Profinet, Ethernet/IP, etc.) to indirect, clientless remote access via RDP, VNC, SSH, Telnet.

Cloud-based solution benefits

Instant Version Upgrades:

Secomea immediately adopts new updates as they become available, streamlining the process and avoiding the complexities of scheduled rollouts across various sites.

Robust Cybersecurity:

Secomea's security by design is based on the Zero Trust model, the Defense in Depth approach, and the Purdue model. Secomea's solution 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.

Effortless Deployment:

An infrastructure-agnostic cloud-based solution reduces the total cost of ownership (TCO) by removing the need for on-site installations and relieving the strain of managing associated infrastructure.

Encryption and network segmentation

TLS 1.2 & AES256

CIA triad security & 3rd-party certifications

Secomea's encryption methods, built on TLS 1.2 connections using x.509 certificates (with 1024-bit keys) and AES256 encryption, align seamlessly with the principles of the CIA triad: confidentiality, integrity, and authenticity.

The use of AES256 encryption ensures confidentiality by securing data from unauthorized access, while the x.509 certificates and TLS 1.2 protocols guarantee integrity by protecting data against tampering or corruption during transmission. Additionally, the robust authentication framework inherent in TLS and x.509 certificates strengthens authenticity, verifying the identities of all communication endpoints to prevent unauthorized entities from accessing the system.

TRUST ON FIRST USE

Protection against MitM attacks

Secomea connects your assets via AES 256bit encrypted tunnels based on TLS. You can restrict connections down to each specific device's IP address and port, both remotely and on-site with I/O ports for physical control.

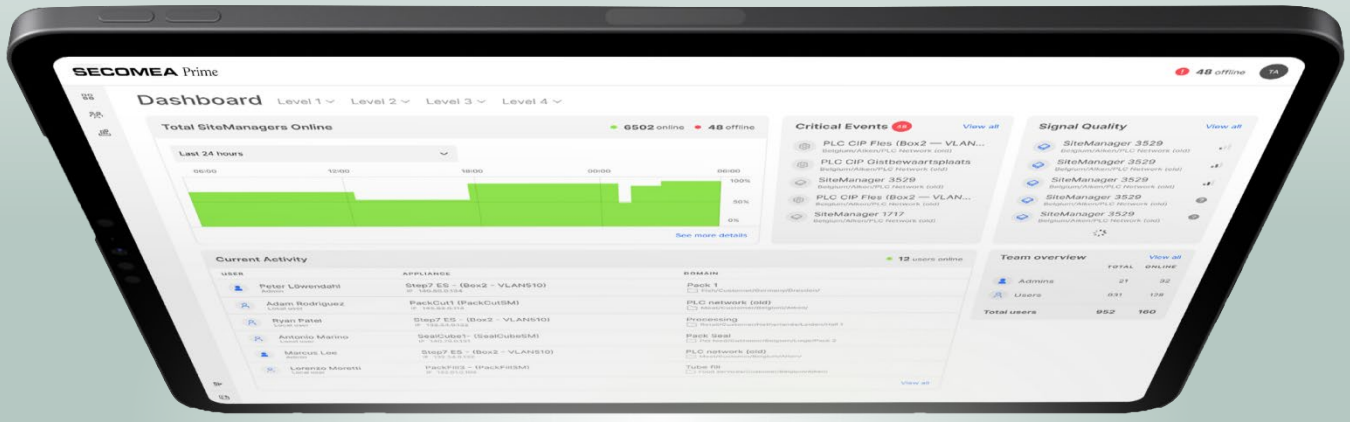
Each Secomea's Access Management server has a unique TLS certificate/key to which a Secomea's gateway binds the first time they connect (a.k.a, "Trust-on-first-use" - ToFu) and against which any subsequent connections are verified. To change the server the gateway trusts, one must manually reconfigure the Access Management server settings in the gateway. An attacker cannot do this through interception alone. By requiring manual reconfiguration for any changes, we prevent unauthorized redirections.

Secomea's Architecture

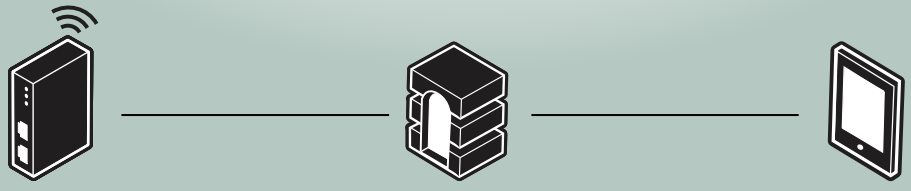
Specifically designed for manufacturing and critical infrastructure sectors, Secomea minimizes cyber risks, strengthens business continuity, and protects vital CPS processes.

The solution includes all the software and hardware components needed for performing your remote access and maintenance tasks—from remote programming and troubleshooting to data-driven decision-making.

Manage user access, control remote sessions in real-time, and collect machine data while enjoying top-notch security for your OT environments.



SECOMEA Prime



SiteManager

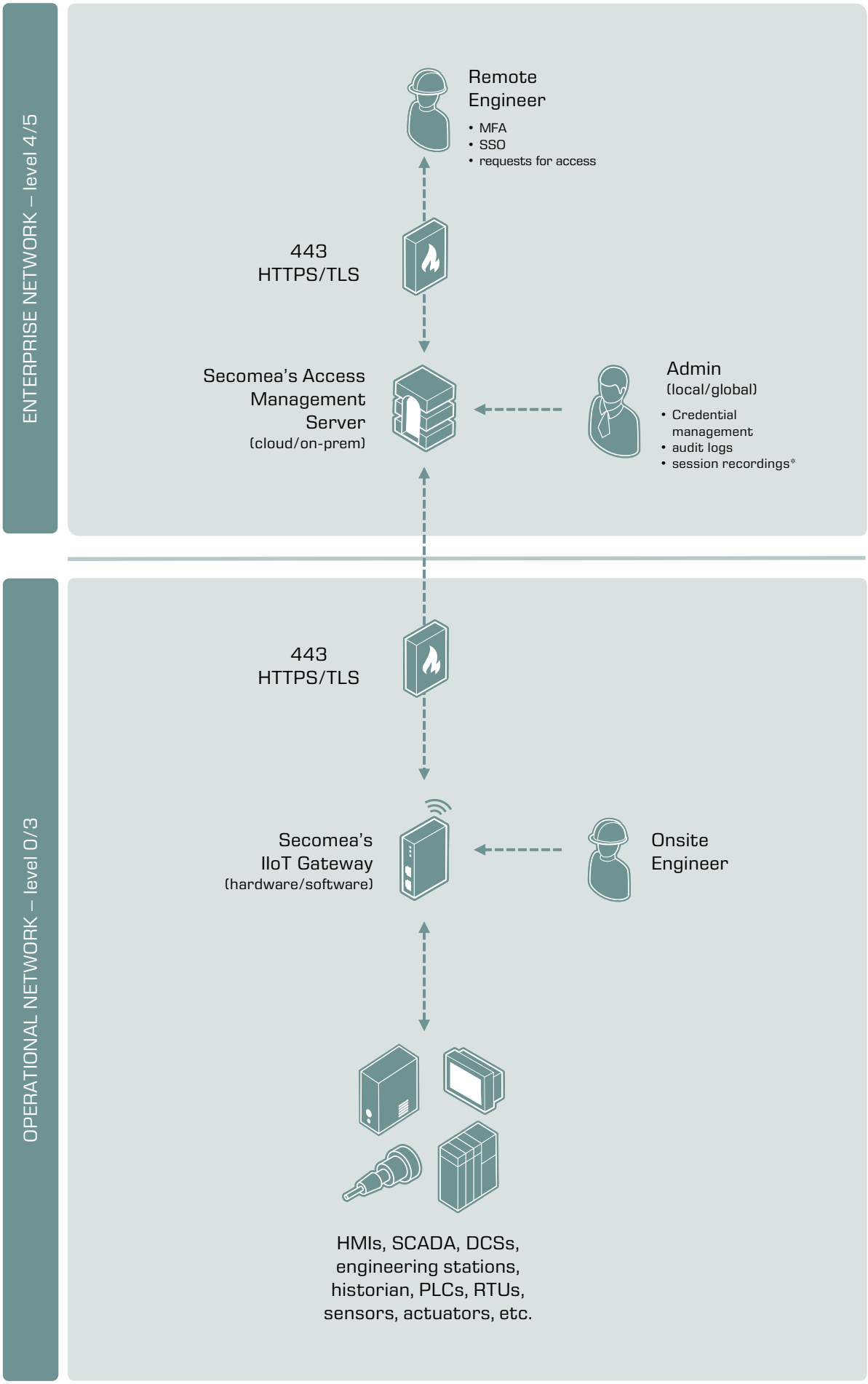
Plug-and-play Industrial IoT gateway (hardware or software) for secure remote access and data collection

GateManager

Centralized Industrial Access Management and M2M Server for user access management and auditing

LinkManager

Clientless remote access client enabling a variety of remote access options from anywhere, via any device



* Feature available in Q4 2024

Secomea's features and capabilities

IDENTITY AND ACCESS MANAGEMENT	Privileged access management	Set up hierarchy-based user roles based on the principle of least privilege
	Granular access control	Control access on an individual level with granular permissions
	Advanced grouping	Perform mass administration of user permissions
	Just-in-time (JIT) access	Grant temporary or scheduled access to specific assets
	Always-on access	Set up a static, persistent tunnel connection between two separate networks
	Request for access	Users can request access to specific assets and admins can approve it in one click
	Multi-Factor Authentication (MFA)	Verify users' identities via MFA with SMS authentication
	Single Sign-On (SSO)	Secure users' authentication via Single Sign-On (SSO) with Azure AD or Okta
REMOTE ACCESS	Agentless, web-based system	Use Secomea directly from your browser – no need to install a plugin or application
	Direct access (lightweight client)	Supporting OT protocols such as Modbus, Profinet, EtherCAT, Ethernet/IP, etc.
	Indirect and clientless access	Supporting remote access from your browser via RDP, VNC, SSH, Telnet, HTTPS
	Secure file transfer	Scan files transferred remotely for viruses or malware to assess their safety
AUDIT & MONITORING	Real-time activities monitoring	Get an overview of ongoing remote access sessions from the Prime Dashboard
	Audit logs	Track every activity performed on your machines to document who did what and when
	Session recordings*	Capture videos of remote access sessions for troubleshooting and audit purposes
	Alerts and automated actions	Get SMS/email notifications for specific events and automate triggered actions
	Access gateways information	Get a centralized overview of all gateways with detailed info (serial number, IP, firmware, last heartbeat). Register info on their physical location and contact details for streamlined operations
	Vulnerability hub	Spot gateways that are not running the latest firmware version and those whose models are approaching End of Life or End of Support to ensure timely updates and replacements
CUSTOMIZATION & INTEGRATIONS	API access	Integrate Secomea with other tools you use to run your operations
	AD integration	Changes implemented in Microsoft Azure Active Directory are synced hourly in Secomea's access management server.
	Security Information and Event Management (SIEM) integration	Integrate your SIEM system (Syslog, Splunk, etc.) with Secomea
	Data Collection Module (DCM) and cloud integration	Collect data from your industrial equipment using its native data collection protocols (OPC UA, Modbus TCP, Siemens S7, Ethernet/IP, MQTT, etc.) and send it to your chosen cloud solution for further processing (Microsoft Azure IoT Hub, Amazon AWS IoT Core, Software AG Cumulocity IoT, Aveva Insight, MQTT data servers, etc.)
	Support system integration	Integrate your support system with Secomea's to centralize tickets management
	Branding	Customize your URL and login page to align it with your corporate brand

* Feature available in Q4 2024