Rhebo
a Landis+Gyr company

OT Security Made Simple

Rhebo OT Security

Simple & Effective ICS Threat Detection & Monitoring For Electrical Utilities

REDUCE THE RISK OF OT CYBER INCIDENTS

through asset discovery, vulnerability detection and network monitoring

ENABLE FAST MITIGATION OF OT ATTACKS

through early warning of suspicious network activity

BRIDGE THE OT SECURITY SKILLS GAP

with services tailored to your needs

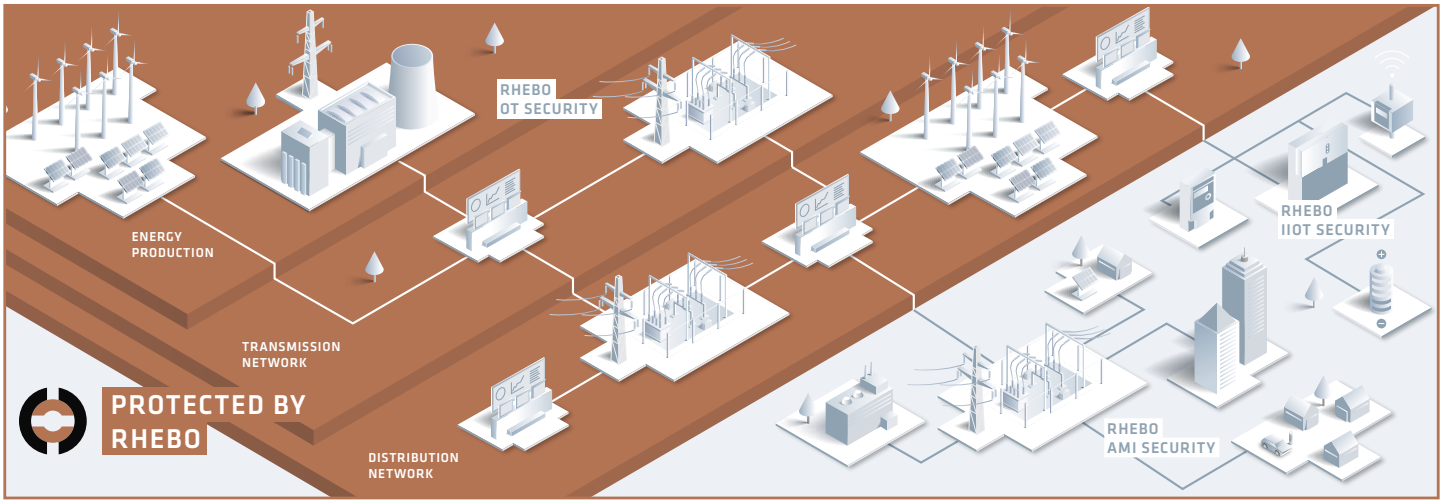
»With Rhebo we can actively make sure that our Industrial Automation & Control System (IACS) is stable and secure. Rhebo provides the detailed visibility into our IACS to rapidly identify and mitigate novel attacks and misconfigurations that have been invisible to us in the past.«

Dipl.-Ing (TU) Sven Hanemann | IT Security Manager | e-netz Südhessen AG

Rhebo provides simple and effective cybersecurity and intrusion detection »Made in Germany« for Operational Technology (OT) and distributed industrial infrastructure. The solution continuously monitors ICS and OT and reports any anomaly within the networks.

Rhebo fully supports companies from the energy sector along the industrial cybersecurity lifecycle from the initial risk analysis to managed OT monitoring with threat & intrusion detection.

Rhebo OT Security Dedicated & Simple



New Security Challenges
For Complex Energy Supply Systems

The **power grid is becoming increasingly fragmented** due to the integration of municipal utilities, renewable energy resources and the construction of new substations. The individual stations are often located far away from the central control room. Therefore, control is increasingly carried out digitally via remote access. To secure these peripheral systems, distribution and transmission system operators often rely exclusively on firewalls. These reliably detect known malware. **However, firewalls are blind to novel attack patterns and professional attacks that often run for months or years.** With several hundred of thousands of new malware variants each day[1] cybersecurity limited to identifying known signatures becomes highly unreliable. **Protection mechanisms in operational technology (OT) and industrial control systems (ICS) are minimal.** On-site personnel are rarely trained and authorized to look after the ICS. Communication within the plants often is a black box the central control room. Incorrect or corrupted communications within substations and other remotely controlled power systems can not be detected until they have already impacted the power supply. **This makes it easy for cybercriminals** scout OT networks as part of the reconnaissance, move laterally within the infrastructure, advance threat propagation as well as cause and sustain disruption.

[1] Federal Office For IT Security (BSI)

»The audit has given us a clearer picture of all processes in our complex industrial control system. This enabled us to analyze all communication traffic extensively and check the ICS specifically for vulnerabilities. We were impressed by the smooth process. The direct development of effective measures optimally prepared us for future cyber security risks.«

Falk Fischer | Team Leader IT-Systems and Applications | Leipziger Wasserwerke

End-to-End OT Cybersecurity
for Critical Infrastructures

Rhebo supports energy and water sector companies along the **entire lifecycle of establishing and maintaining thorough OT cybersecurity.** With Rhebo OT Security, critical infrastructures can rely on the strong Rhebo expertise from the initial OT risk analysis to integrating an OT intrusion and anomaly detection system to (optionally) the continuous operation of the security system.

Rhebo's **Next Generation OT Intrusion Detection System combines passive OT monitoring with non-intrusive anomaly detection.** The system is a dedicated solution for OT cybersecurity covering the entire critical infrastructure from the control rooms and central power plants to substations and renewable energy resources to enable reliable **end-to-end monitoring of the distributed infrastructure.**

Cyberattacks, manipulation, scans and technical error states occurring in the facilities are detected and reported in real time on the basis of the associated communication changes.

Rhebo OT Security supports all common platforms and **can be integrated cost-efficiently** into any industrial automated network via:

- **dedicated** industrial hardware for physical setups;
- **virtual** appliances for the operation in VMware, Hyper-V and other virtual environments;
- **software-based** sensors for common security gateways, edge computing devices and substation servers e.g. by Barracuda, Cisco, INSYS icom Smart Devices, RAD, Siemens RUGGEDCOM and Welotec.

The solution **fully supports specific substation protocols** such as OPC, IEC 60870-5-104, IEC 61850-8-1 and DNP3, amongst others. With Rhebo OT Security, **resilience and system hardening are improved** as threats can be mitigated quickly, and attacks can be prevented from spreading to other sites or the central systems.

Simple & Effective
3 Steps To Uncompromising OT Security

1

The first easy step
to OT security:
Rhebo Industrial Security Assessment

Cybersecurity starts with visibility.

The **Rhebo Industrial Security Assessment** is an OT cyberrisk and vulnerabillity analysis that provides a deep understanding of your ICS / OT assets, risk exposure as well as recommendations for effective measures for hardening the systems.

You profit from

- the identification of all devices and systems within the OT including their properties, firmware versions, protocols, connections and communication behavior (Asset Discovery & Inventory);
- an in-depth analysis of existing CVE-documented vulnerabilities;
- the identification of risk exposure, security gaps and technical error states;
- a detailed audit report and workshop with actionable recommendations.

2

The seamless transition
to comprehensive OT security:
Rhebo Industrial Protector

Cybersecurity does not end at the network perimeters.

The OT monitoring with next generation OT threat and intrusion detection **Rhebo Industrial Protector** provides enterprise-ready OT-dedicated security. It advances the existing perimeter firewall security by integrating holistic anomaly detection that does not interfere with the critical industrial processes.

You profit from

- real-time visibility of communication behavior of all OT and ICS assets (protocols, connections, frequencies);
- real-time reporting and localization of events (anomalies) that indicate cyberattacks, manipulation or technical error states;
- early identification of attacks via back-doors, previously unknown vulnerabilities and internal adversaries that firewalls fail to detect (defense-in-depth).

3

The recipe to peace of mind.
We monitor so you don't have to:
Rhebo Managed Protection

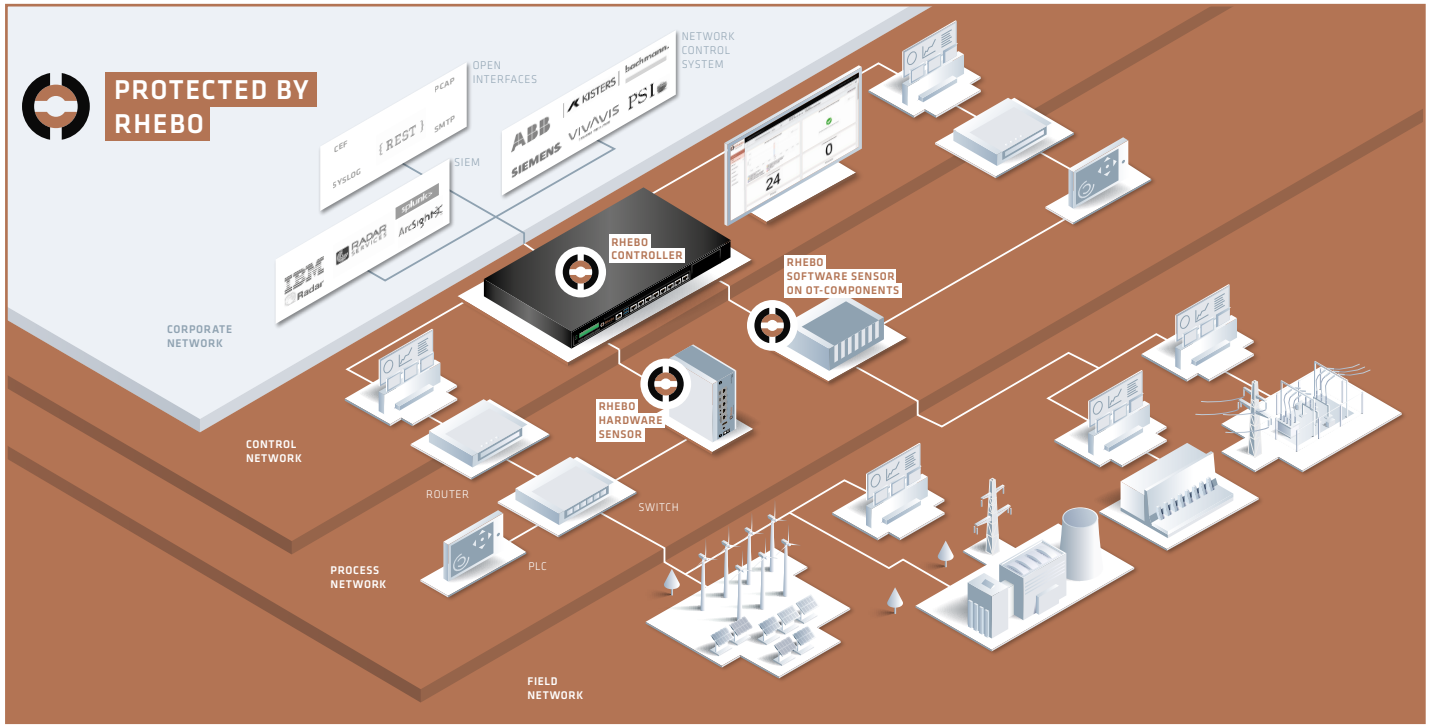
Cybersecurity needs resources and know-how.

With **Rhebo Managed Protection,** we support you in operating the OT security monitoring with anomaly detection, in particular in evaluating and responding to incidents, as well as continuously reviewing and improving mitigation mechanisms.

You profit from

- expert support for the operation of the OT security monitoring system;
- fast forensic analyses and assessment of OT anomalies;
- fast actionability in case of incidents;
- regular OT cyber risk analyses and maturity assessments for continuous improvement.

Sample Controller & Sensor Deployment
In OT Infrastructure



Rhebo Industrial Protector
Your lean and dedicated OT intrusion detection

Rhebo Industrial Protector provides **enterprise-ready OT-dedicated security.** It advances the existing perimeter firewall security by integrating network-based OT monitoring with anomaly detection. Any communication that indicates cyberattacks, tampering, espionage or technical error conditions is reported in real time. This allows early detection of multi-step attack patterns as outlined by the MITRE ATT&CK for ICS framework.

What?

- real-time detection of cyber attacks and technical error states within the OT and SCS,
- full visibility of OT components for asset inventory,
- documentation of asset properties incl. protocols, connections and vulnerabilities,
- optional managed services.

How?

- continuous network-based monitoring of communication in, to and from the OT*,
- behavioral analysis of network traffic using deep packet inspection,
- immediate notification about any communication anomaly including pcap files for forensic analysis,
- passive, non-intrusive monitoring and detection.

Why?

- tried-and-tested OT cybersecurity against sophisticated threat actors and zero-day exploits,
- OT security made simple even for small teams,
- easily scalable to multiple sites with one central point of control,
- comprehensive support from initial risk analysis to IDS operation.

*A complete list of supported protocols can be found in the **Rhebo Industrial Protector Spec Sheet.**

Rhebo OT Security Made Simple

STRONG TRACK RECORD
of industrial security solutions for the energy and water sector.

DEDICATED AND SIMPLE SOLUTION
for cost efficient implementation of OT, Advanced Metering Infrastructure and IIoT cybersecurity.

COMPREHENSIVE SUPPORT
for increasing industrial resilience fast and uncomplicated.

SECURITY AGAINST PREVAILING VULNERABILITIES
through periodic OT cyber risk and maturity assessments.

SECURITY AGAINST KNOWN AND NOVEL ATTACKS
through continuous OT monitoring, asset discovery and anomaly detection.

SECURITY AGAINST INTRUSION SPILL-OVER
through end-2-end security monitoring with anomaly detection of the OT, IoT and the Advanced Metering Infrastructure.

»With Rhebo, we can centrally and reliably secure our energy supply as well as the municipal utilities and over 16,000 decentralized energy producers we serve. The newly gained transparency and continuous monitoring visibly increases our network quality«.

Dipl.-Ing Daniel Beyer | Head of System Engineering & Information Security Manager | Thüringer Energienetze GmbH & Co. KG

OT SECURITY MADE SIMPLE
through OT-focused analysis & intelligent event visualization.

SECURING ACTIONABILITY
through Rhebo expert support for risk analysis, operations and forensic analysis.

SYSTEM SECURITY
through flexible and cost-efficient integration of Rhebo solutions on IIoT devices and network components.

SECURITY AGAINST UNPREDICTABLE TCO
through simple license schemes and easy, low-footprint installations.

SECURING COMPLIANCE
through Next Generation IDS for OT based on national security laws and international security standards.

SECURITY OF TRUST MADE IN GERMANY
compliant with European Cyber Security Organisation (ECSO) and GDPR.

Order your custom OT network security assessment or book a demo

www.rhebo.com | sales@rhebo.com | +49 341 3937900

Explore More Rhebo Solutions

↗ Rhebo AMI Security

↗ Rhebo IIoT Security

Secured By Rhebo

Stromnetz Hamburg · Leipziger Wasserwerke · Thüringer Energienetze · Landis+Gyr · BayWa r.e. · MITNETZ STROM

OT Security Made In Germany

OT SECURITY Made in Germany · Information Security Management System DNV ISO/IEC 27001 · bitkom · Cybersecurity Made in Europe (Initiated by ECSO. Issued by eurobits e.V.) · Allianz für Cyber-Sicherheit · Plattform Industrie 4.0

Rhebo OT Security Made Simple

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The German company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. Since 2021, Rhebo is part of the Landis+Gyr AG, a leading global provider of integrated energy management solutions for the energy industry with around 7,500 employees in over 30 countries worldwide. As a trustworthy cybersecurity provider, Rhebo is ISO 27001 certified, and was awarded the »Cybersecurity Made In Europe« label for its strict data protection and data security policies.

www.rhebo.com

Rhebo GmbH Spinnereistr. 7 | 04179 Leipzig | Germany
rhebo.com

SOLUTION BRIEF RHEBO OT SECURITY 02-2025