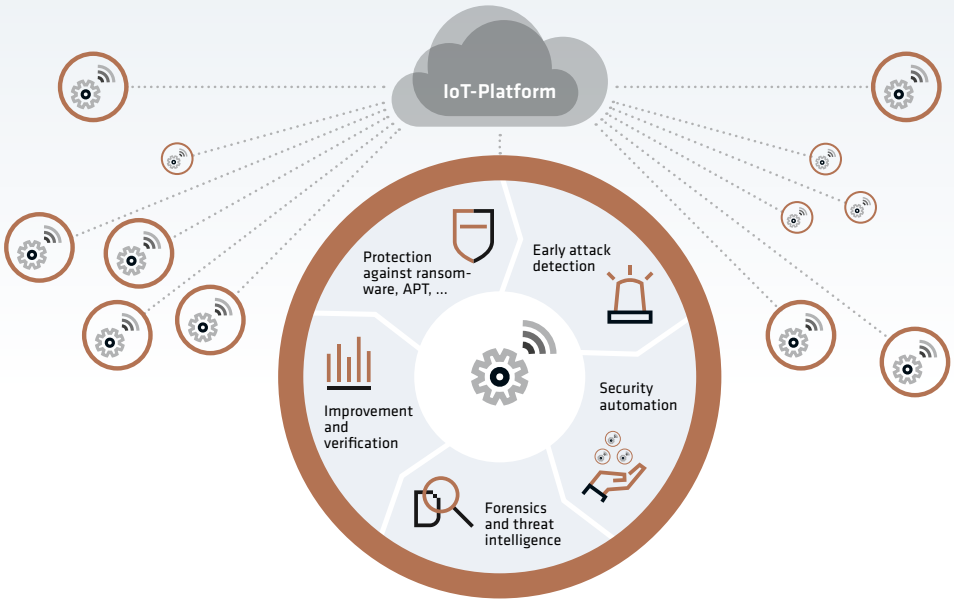
Rhebo IoT Device Protection
The Immune System for Connected Devices

AUTOMATED CYBERSECURITY
for critical
connected devices

FAST SECURITY UPGRADE
for existing devices and
IoT networks

COMPLETE TRANSPARENCY
on the security status of the fleet
and individual devices



Rhebo IoT Device Protection

Your Benefits

- **IMPLEMENT ENDPOINT DETECTION & RESPONSE (EDR)** for connected devices and IoT platforms.
- **PREVENT INFECTION SPREAD** to the cloud and other devices with Security Automation and Defense-in-Depth.
- **IMPLEMENT COST-EFFICIENT SECURITY DESIGN** through seamless integration and minimal CPU and memory footprint.
- **ACHIEVE FINE GRANULAR BEHAVIOUR ANALYSIS & ANOMALY DETECTION** based on device-specific patterns (policies).
- **RESOLVE SOFTWARE ERRORS FASTER** by early detection of error conditions as well as rapid root cause analysis.
- **ENSURE COMPLIANCE AND STATE-OF-THE-ART** by meeting relevant standards such as IEC 62443.

Your Devices Are Smart. But Are They Secure?

The number of IoT devices is growing in industrial networks and especially in decentralised infrastructures with remote access. Manufacturers of **e.g. energy storage systems, automation technology and kiosk systems** are thus also becoming platform operators. The IoT cloud is used to pool the connected devices in order to analyse data flows, optimise performance using AI or implement service level agreements via remote access. The devices are smart and connected, but rarely secure. Large fleets of critical devices in particular pose a risk to trouble-free operation – whether through ransomware, professional attacks, botnets or Advanced Persistent Threats.

Security and stability are at stake both for the users of the devices and for the manufacturers and platform operators. A compromised device can lead to the infection of the entire fleet. This is all the more likely with new attack patterns, Advanced Persistent Threats or unknown vulnerabilities, which are becoming increasingly common. Manufacturers of critical and distributed IoT devices therefore need an intelligent, automated detection and defense system that also reliably identifies unknown attack patterns and minimizes fleet risk through intelligent security automation.

Automated IoT Fleet And Platform Security

Rhebo uses **security monitoring and anomaly detection** to monitor all communication both on and between critical connected devices and the cloud-based IoT platform. Within just a few hours, the system learns the authorised communication pattern of the devices. During operation, all communication is analysed down to the content level of the data packets using deep packet inspection technology.

Any deviations from the authorized pattern are documented, reported and stopped in real-time as an anomaly. A configurable **Security Automation Policy** prevents the further spread of an infection. The fleet protection is maintained. The IoT platform is not affected. Rhebo already supports standard hardware architectures, IoT platforms and operating systems.

IoT Device Protection »Made in Germany«

TeleTrusT Pioneers in IT security. bitkom Allianz für Cyber-Sicherheit PLATTFORM INDUSTRIE4.0 Security made in Germany Trust Seal www.teletrust.de/itsmig

Secure your critical connected devices. Get in touch with us!

ALEXANDER MÜLLER
VP Product Management

Mobile +49 172 1676644
Email alexander.mueller@rhebo.com

About Rhebo

Rhebo is the only provider of industrial monitoring solutions to ensure both cybersecurity and stability of the ICS and IoT infrastructure in industrial, energy and water companies. The German company's solutions monitor all communication within the ICS, and reliably report attacks, vulnerabilities as well as technical error states. Thus, Rhebo supports operators of ICS to increase cybersecurity, productivity and availability of their systems and plants, and to safeguard the digital transformation of their processes. In this role, the company is actively involved in the Alliance for Cyber Security of the Federal Office for Information Security (BSI), the Teletrust – Bundesverband IT-Sicherheit e.V. and the Bitkom Security Management Working Group to develop standards and technical guidance.