Rhebo
a Landis+Gyr company

OT Security Made Simple

Rhebo IIoT Security

Angriffserkennung und -abwehr für kritische verteilte IIoT-Geräte und -Anlagen

RISIKO VON IIOT-CYBER-VORFÄLLEN REDUZIEREN

durch Kommunikationsüberwachung und Schwachstellenerkennung

IIOT-NETZWERK-SCHÄDEN ABWEHREN

durch Anomalieerkennung und Sicherheitsautomatisierung

FACHKRÄFTEMANGEL ÜBERBRÜCKEN

durch auf Sie zugeschnittene IIoT-Sicherheits-Services

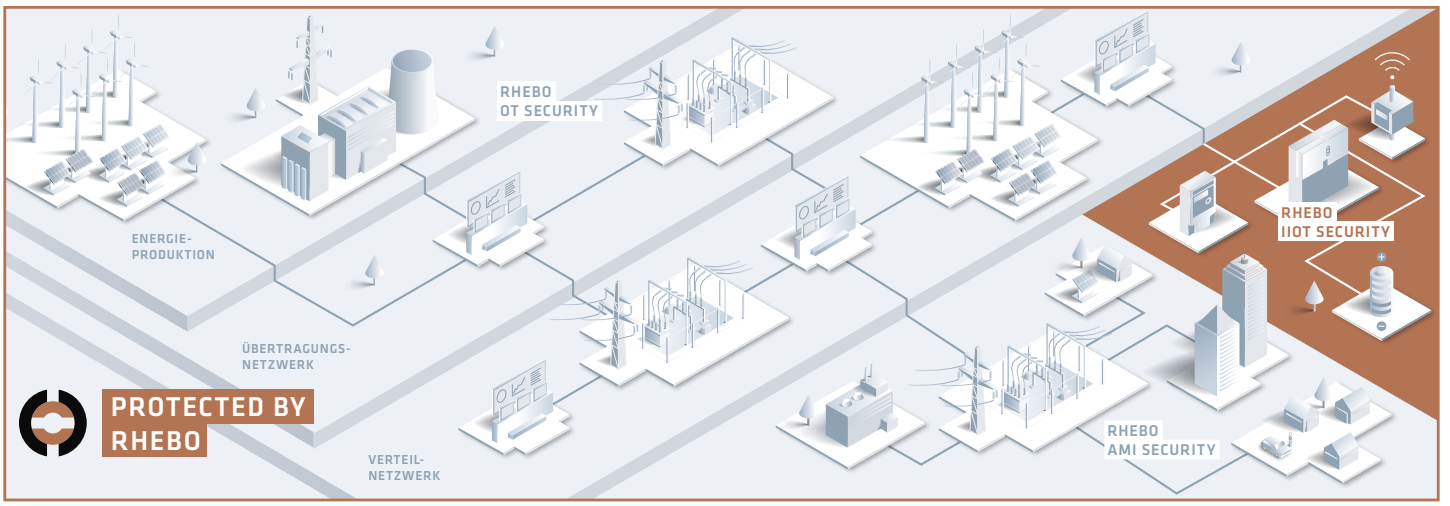
»Uns war bei der Auswahl der Lösung besonders wichtig, dass Monitoring und Sicherheitsautomatisierung konkret auf unsere Geräte zugeschnitten werden und jederzeit erweitert werden können. Denn sowohl unsere Technologie als auch die Gefährdungslage entwickeln sich ständig weiter.«

Daniel Ackermann | Leiter Software Development | Sonnen

Rhebo IIoT Security ermöglicht es herstellenden und betreibenden Unternehmen, ihre kritischen IIoT-Anlagen und -Netzwerke zu sichern, Sicherheitsvorschriften einzuhalten und Kosten für Ausfallzeiten zu sparen. Die Lösung wurde entwickelt, um eine effektive industrielle Cybersicherheit für Energiespeichersysteme, elektrische Ladestationen und andere hochwertige verteilte IIoT-Anlagen zu schaffen.

Sie bietet alle Funktionalitäten, um Angriffe von Anfang an zu stoppen und Gefährdungen zu erkennen, bevor es zu Störungen kommt. Rhebo bietet einfache und effektive Cybersecurity-Lösungen »Made in Germany« für die Operational Technology (OT), verteilte industrielle Anlagen in industriellen IoT-Netzwerken (IIoT) sowie für die Advanced Metering Infrastructure.

Rhebo IIOT Security Gezielt & Einfach



Verteilte IIoT-Geräte sind smart,
aber stark gefährdet

Die Zahl der smarten Geräte in industriellen Umgebungen nimmt zu. Dies beschränkt sich nicht nur auf Komponenten in klassischen industriellen Umgebungen, die mit Rhebo OT Security leicht gesichert werden können. Immer mehr stark verteilte Infrastrukturen wie Energiespeichersysteme, elektrische Ladestationen und intelligente Demand-Site-Response-Systeme nutzen smarte Funktionen. Oft kommunizieren sie über das öffentliche Internet und Clouddienste mit der zentralen Betriebsplattform. Darüber hinaus sind die Anlagen zugänglich für physische Eingriffe und involvieren eine Vielzahl von Nutzergruppen, darunter Wartungsunternehmen und Privatpersonen. Die IIoT-Anlagen sind somit besonders exponiert. Ein einziges kompromittiertes Gerät kann zudem bei fehlenden Sicherheitsmechanismen die gesamte Flotte infizieren. Das ist insbesondere bei neuartigen Angriffsmustern, Advanced Persistent Threats oder Zero-Day-Schwachstellen wahrscheinlich. Die unübersichtliche Risikoexposition macht die verteilten kritischen IIoT-Ressourcen somit besonders anfällig für groß angelegte Attacken wie Ransomware, DDoS-Angriffe, Botnets oder orchestrierte Störungen. Ein erfolgreicher Angriff kann erhebliche negative Folgen für den Betrieb und die Kundenbindung weltweit haben. Herstellende Unternehmen von verteilten kritischen IIoT-Geräten benötigen daher ein intelligentes, automatisiertes Angriffs- und Anomalieerkennungssystem, das selbst neuartige Angriffsmuster detektiert und das Flottenrisiko durch intelligente und lokale Sicherheitsautomatisierung minimiert.

»Die Sicherheit unserer Energiespeicher bedeutet zugleich Sicherheit für unsere Kunden weltweit«.

Daniel Ackermann | Leiter Software Development | Sonnen

Endpoint Detection & Response
für globale IIoT-Netzwerksicherheit

Rhebo IIoT Security ermöglicht es herstellenden und betreibenden Unternehmen kritischer IIoT-Geräte, die Verfügbarkeit, Integrität und Sicherheit ihrer verteilten, hochwertigen Infrastruktur zu gewährleisten. Rhebo IIoT Security basiert auf dem etablierten dedizierten industriellen Monitoringsystem mit Anomalieerkennung von Rhebo und schneidet die Lösung auf die spezifischen Anforderungen von IIoT-Geräten zu:

- minimale Nutzung des CPU;
- minimale Bandbreitennutzung;
- lokale Sicherheitsautomatisierung (z.B. Blocklisting);
- einfache globale Distribution;
- Fernwartung.

Rhebo IIoT Security ist direkt auf dem IIoT-Gerät als Endpoint-Detection- und Response-Lösung integriert. Diese Implementierungsarchitektur ermöglicht die lokale Erkennung und Abwehr von Angriffen und verhindert so laterale Bewegungen, Spill-over und progressive Ausbreitung von Gefahren. Die integrierte Anomalieerkennung lernt hierzu binnen weniger Stunden die autorisierte Kommunikation aller Geräte innerhalb des IIoT-Netzwerks. Während des Betriebs wird die gesamte Kommunikation sowohl auf als auch zwischen den IIoT-Geräten und der cloudbasierten IIoT-Management-Plattform überwacht. Die Erkennung spezifischer sicherheitsrelevanter Vorfälle auf einem IIoT-Gerät löst die lokale Sicherheitsautomatisierung aus und blockiert die bösartige Kommunikation direkt auf dem betroffenen Gerät. Darüber hinaus wird jede Abweichung von der autorisierten Kommunikation, z. B. aufgrund von Konfigurations- oder neuartigen Kommunikationsänderungen sowie technischen Fehlerzuständen, als Anomalie gemeldet. Dies ermöglicht es der Betriebsführung, Verfügbarkeitsrisiken zu lokalisieren und schnell und zielgerichtet über effektive Abhilfemaßnahmen zu entscheiden. Rhebo IIoT Security ist sowohl als selbst betriebene Anwendung als auch als Managed Service von Rhebo erhältlich. So können sich herstellende und betreibende Unternehmen verteilter IIoT-Assets beruhigt auf ihr Kerngeschäft konzentrieren.

Einfach & Effektiv
3 Schritte zur sicheren IIoT

1

Der erste einfache Schritt
zu umfassender IIoT-Sicherheit:
Rhebo Industrial Security Assessment

Cybersicherheit beginnt mit Sichtbarkeit.

Die Risikoanalyse und Reifegradbeurteilung des **Rhebo Industrial Security Assessment** liefert ein detailliertes Verständnis der IIoT-Assets, Netzwerk- und Kommunikationsstruktur sowie bestehender Sicherheitsrisiken. Abhängig von den Anforderungen umfasst der Schritt eine Risikobewertung der IIoT-Assets und der Betriebsplattform mittels Kommunikationsmonitoring sowie einen Pentest ausgewählter IIoT-Geräte.

Sie profitieren von

- der Analyse der Kommunikationsmuster zwischen den IIoT-Geräten und der Betriebsplattform inklusive der Protokolle, Verbindungen und des Kommunikationsverhaltens;
- der detaillierten Analyse bestehender Schwachstellen nach CVE;
- der Identifikation von Cyberrisiken und Sicherheitslücken;
- Handlungsempfehlungen mit Abschlussbericht und Workshop.

2

Der nahtlose Übergang zu
durchgängiger IIoT-Sicherheit:
Rhebo Industrial Protector

Maßgeschneiderte Cybersicherheit, die lokal wirkt, um global zu schützen.

Die Rhebo IIoT Security Lösung **Rhebo Industrial Protector** ist ein industrielles Sicherheitsmonitoring mit integrierter Angriffs- und Anomalieerkennung sowie -abwehr. Es läuft direkt auf den IIoT-Assets und erkennt alle Kommunikationsabweichungen. Entsprechend der individuellen Sicherheitsrichtlinien des betreibenden Unternehmens werden Anomalien entweder aktiv auf dem betroffenen Gerät blockiert oder an das Kontrollzentrum zur weiteren Bewertung gemeldet.

Sie profitieren von

- einer IIoT-Sicherheitslösung, die auf Ihre Anforderungen an die Sicherheitsautomatisierung zugeschnitten ist;
- Echtzeit-Transparenz des Kommunikationsverhaltens aller IIoT-Assets (Protokolle, Verbindungen, Frequenzen);
- Echtzeit-Meldungen von Sicherheitsereignissen und technischen Fehlerzuständen;
- Angriffsabwehr auf Geräteebene, um die Ausbreitung im Netzwerk zu verhindern;
- hohe Skalierbarkeit durch containerisierte Software.

3

Wir überwachen, damit Sie sich
um Ihr Kerngeschäft kümmern können:
Rhebo Managed Protection

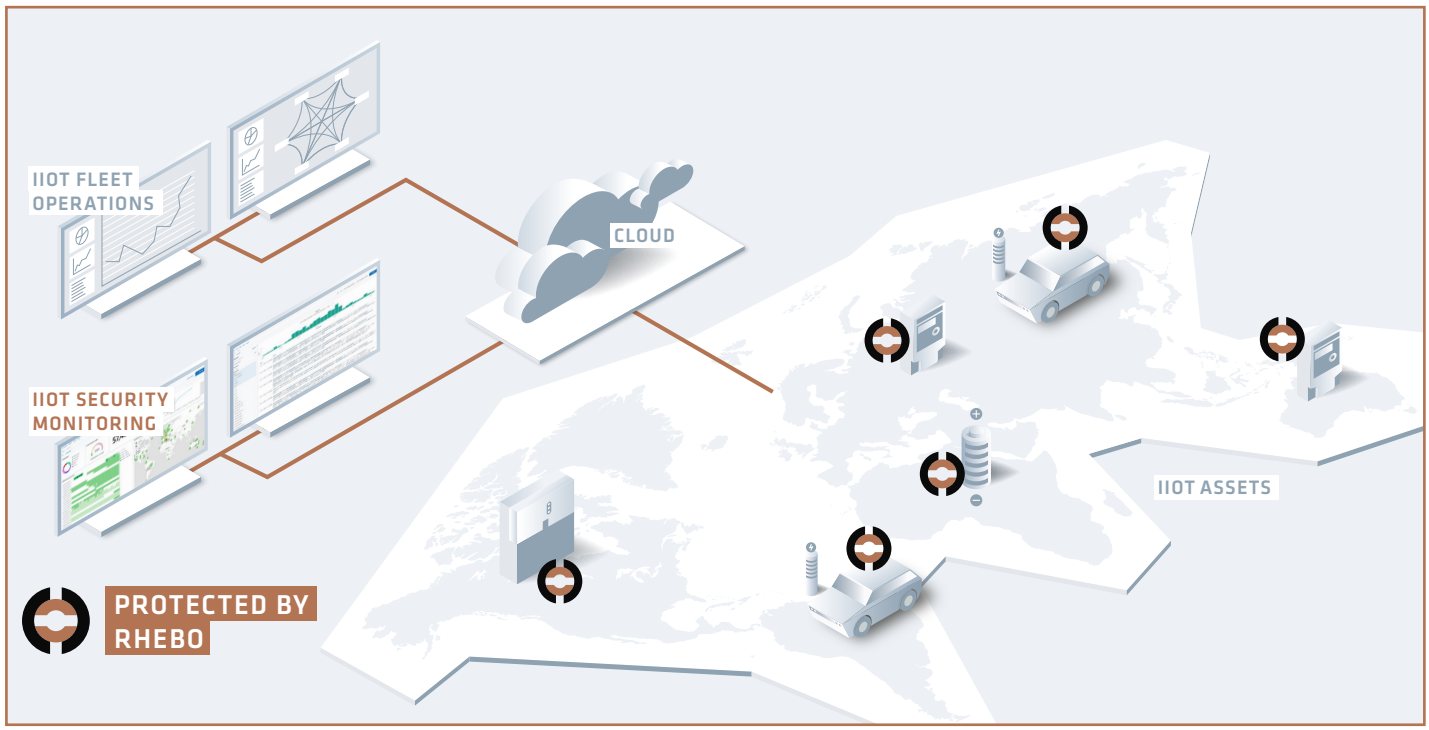
IIOT-Sicherheit braucht Ressourcen und Know-How.

Rhebo unterstützt Sie mit **Rhebo Managed Protection** beim Betrieb des IIoT-Sicherheitsmonitoring, insbesondere bei der Auswertung und Reaktion auf Vorfälle sowie der kontinuierlichen Überprüfung und Verbesserung der Abwehrmechanismen.

Sie profitieren von

- der Unterstützung unserer Expert:innen beim Betrieb des IIoT-Sicherheitsmonitoring;
- der schnellen forensischen Analyse und Aufklärung von IIoT-Anomalien;
- der schnellen Handlungsfähigkeit bei Vorfällen;
- der kontinuierlichen Verbesserung durch regelmäßige IIoT-Risikoanalysen und Pentests.

Beispiel-Deployment von Rhebo IIoT Security
in einer IIoT-Infrastruktur



Schlanke und maßgeschneiderte Cybersicherheit
für Ihre IIoT-Assets

Rhebo IIoT Security funktioniert als voll integrierte, individuell zugeschnittene IIoT-Sicherheitslösung. Sie nutzt das bewährte industrielle Monitoring- und Anomalieerkennungssystem Rhebo Industrial Protector und ergänzt es um IIoT-spezifische Funktionen wie aktive Angriffsabwehr und Software-Containerisierung. Die Lösung wird auf Geräteebene über Softwarepakete implementiert, die per Fernzugriff und vollständig automatisiert installiert und verwaltet werden können.

Was?

- Echtzeit-Erkennung und -Abwehr von Cyberangriffen und kritischen Cybervorfällen auf Geräteebene;
- Echtzeit-Meldung jeder Auffälligkeit an die Betriebsführung;
- Volle Transparenz vom IIoT-Netzwerk bis zum Gerät in Bezug auf Risiken, Schwachstellen und technischen Fehlerzuständen;
- optionale Managed Services durch Rhebo-Expert:innen.

Wie?

- lokale Überwachung der gesamten Kommunikation auf den IIoT-Geräten;
- kontinuierliche Analyse des Verhaltens jedes Geräts und seiner lokalen Schnittstellen wie Web-Interfaces und Systemprotokolle;
- Deep Packet Inspection bis auf Werteebene;
- auf die Sicherheitsrichtlinien des Kunden zugeschnittene Sicherheitsautomatisierung.

Warum?

- umfassende Cybersicherheit gegen Cyberangriffe und lokale Manipulation;
- keine Beeinträchtigung der Anlagenleistung durch Design, das auf die CPU- und Speicherbeschränkungen von IIoT-Geräten zugeschnitten ist;
- hohe Skalierbarkeit durch ferngesteuerte und automatisierte Bereitstellung und Wartung;
- umfassender Rhebo-Support vom Entwurf bis zum Betrieb.

Rhebo OT Security Made Simple

Rhebo unterstützt Industrieunternehmen bei der **Einsparung von Millionenbeträgen** durch Security Compliance und Reduzierung von Ausfallzeiten.

Rhebo ermöglicht die **schnelle Inbetriebnahme** von 10.000 bis 100.000 Geräten und mehr mit einer äußerst skalierbaren IIoT-Sicherheitslösung.

Rhebo bietet eine **kosteneffiziente Installation und Administration** ohne lokale Technik- oder Wartungsteams.

SICHERHEIT VOR BESTEHENDEN SCHWACHSTELLEN
durch regelmäßige IIoT-Risikobewertung und Reifegradbeurteilungen.

SICHERHEIT VOR BEKANNTEN UND NEUARTIGEN ANGRIFFEN
durch IIoT-Angriffserkennung und -abwehr mit Monitoring, Asset Discovery, Anomalieerkennung und Sicherheitsautomatisierung.

ENDE-ZU-ENDE-SICHERHEIT
durch Anomalieerkennung zur Vermeidung der Bedrohungsausbreitung über die OT, IIoT und Advanced Metering Infrastructure.

»Mit Rhebo können wir unsere landesweite Energieversorgung zentral und zuverlässig absichern – auch für die von uns betreuten Stadtwerke und über 16.000 dezentralen Erzeuger. Die neu gewonnene Transparenz und kontinuierliche Überwachung steigert sichtlich unsere Netzwerkqualität«.

Dipl.-Ing Daniel Beyer | ISB und Fachgebietsleiter Systemtechnik | Thüringer Energienetze GmbH & Co. KG

(I)IOT SECURITY MADE SIMPLE
durch IIoT-fokussierte Analyse, Vorfallvisualisierung und aktive Abwehr spezifischer Angriffsvektoren.

SICHERSTELLUNG DER HANDLUNGSFÄHIGKEIT
durch Rhebo-Unterstützung bei Risikobewertung, Betrieb und forensischer Analyse.

SYSTEMSICHERHEIT
durch flexible, kosteneffiziente Integration und Wartung der Lösung als containerisierte Software.

SICHERHEIT VOR INTRANSPARENTEN KOSTEN
durch einfache Lizenzpakete und unkomplizierte Lösungsintegration.

COMPLIANCE SICHERSTELLEN
durch System zur Angriffserkennung für IIoT nach ITSiG 2.0 und einschlägigen Sicherheitsstandards.

VERTRAUENSVOLLE SICHERHEIT MADE IN GERMANY
nach den Anforderungen der European Cyber Security Organisation (ECSO) und DSGVO.

Machen Sie Ihre IIoT-Geräte und Anlagen kugelsicher. Kontaktieren Sie uns für eine Demo.

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

Überzeugen Sie sich selbst. Fragen Sie unsere Kunden!

↗ Erfahren Sie, wie die renommierte Sonnen GmbH ihre 60.000+ weltweit verteilten privaten Energiespeichersysteme mit Rhebo IIoT Security sichert.

Geschützt durch Rhebo

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

OT Sicherheit 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 bietet einfache und effektive Cybersicherheitslösungen für die Netzleit-, Fernwirk- und Steuerungstechnik sowie verteilte industrielle Anlagen in Energieunternehmen, Kritischen Infrastrukturen und Industrieunternehmen. Das deutsche Unternehmen unterstützt Kunden auf dem gesamten Weg der OT-Sicherheit von der initialen Risikoanalyse bis zum betreuten OT-Monitoring mit Anomalie- und Angriffserkennung. Rhebo ist seit 2021 Teil der Landis+Gyr AG, einem global führenden Anbieter integrierter Energiemanagement-Lösungen für die Energiewirtschaft mit weltweit rund 7.500 Mitarbeiter:innen in über 30 Ländern. Als vertrauenswürdiges Cybersicherheitsunternehmen ist Rhebo nach ISO 27001 zertifiziert sowie Partner der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und offizieller Träger des Gütesiegels »Cybersecurity Made In Europe«.

www.rhebo.com

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

SOLUTION BRIEF RHEBO IIOT SECURITY 02-2025