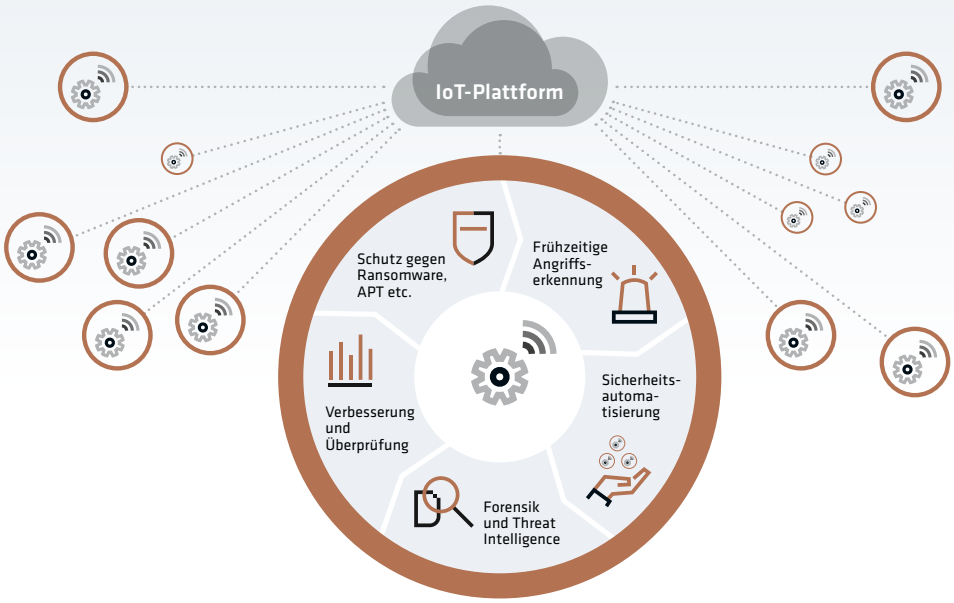
Rhebo IoT Device Protection

Das Immunsystem für vernetzte Geräte

AUTOMATISIERTE CYBERSICHERHEIT
für kritische vernetzte Geräte

SCHNELLES SICHERHEITSUPGRADE
bestehender Geräteflotten

VOLLSTÄNDIGE TRANSPARENZ
über den Sicherheitsstatus
der Flotte und Einzelgeräte



Rhebo IoT Device Protection

Ihre Vorteile

- **ENDPOINT DETECTION & RESPONSE (EDR)** für vernetzte Geräte und IoT-Plattformen.
- **INFEKTIONSAUSBREITUNG AUF CLOUD UND FLOTTE VERHINDERN** durch Security Automation und Defense-in-Depth.
- **KOSTENEFFIZIENTES SICHERHEITSDESIGN** durch nahtlose Integration sowie minimalen CPU- und Speicherbedarf.
- **FEINGRANULARE VERHALTENSANALYSE & ANOMALIEERKENNUNG** basierend auf gerätespezifischen Mustern (Policies).
- **SOFTWAREFEHLER SCHNELLER BEHEBEN** durch Früherkennung von Fehlerzuständen und schnelle Ursachenanalyse.
- **COMPLIANCE UND STATE-OF-THE-ART SICHERSTELLEN** durch Einhaltung relevanter Standards wie IEC 62443.

Ihre Geräte sind smart. Sind sie auch sicher?

Die Anzahl von IoT-Geräten wächst in industriellen Netzwerken und insbesondere in dezentral geführten Infrastrukturen mit Fernzugriff. Hersteller von **z. B. Energiespeichern, Automatisierungstechnik und Kiosksystemen** werden damit auch zum Plattformbetreiber. Über die IoT-Cloud werden die vernetzten Geräte zusammengeführt, um Datenflüsse zu analysieren, mittels KI die Performanz zu optimieren oder Service Level Agreements per Fernzugang umzusetzen. Die Geräte sind smart und konnektiv, jedoch selten sicher. Insbesondere große Flotten kritischer Geräte werden damit zu einem Risiko für den störungsfreien Betrieb – ob durch Ransomware, professionelle Angriffe, Botnets oder Advanced Persistent Threats.

Dabei stehen Sicherheit und Stabilität sowohl für die Nutzer der Geräte als auch für die Hersteller und Plattformbetreiber auf dem Spiel. Ein kompromittiertes Gerät kann zur Infektion der gesamten Flotte führen. Das ist umso wahrscheinlicher bei neuartigen Angriffsmustern, Advanced Persistent Threats oder unbekannten Sicherheitslücken, wie sie aktuell immer häufiger auftreten. Hersteller kritischer und verteilter IoT-Geräte benötigen deshalb ein intelligentes, automatisiertes Erkennungs- und Abwehrsystem, das auch unbekannte Angriffsmuster lückenlos identifiziert und über eine intelligente Sicherheitsautomatisierung das Flottenrisiko minimiert.

Automatisierter IoT Flotten- und Plattformschutz

Rhebo überwacht mittels **Sicherheitsmonitoring und Anomalieerkennung** jegliche Kommunikation, die sowohl auf als auch zwischen kritischen vernetzten Geräten und der cloud-basierten IoT-Plattform erfolgt. Das System erlernt binnen weniger Stunden das autorisierte Kommunikationsmuster der Geräte. Im laufenden Betrieb wird die Kommunikation per Deep-Packet-Inspection-Technologie bis auf Wertebene der Datenpakete analysiert.

Abweichungen vom autorisierten Muster werden in Echtzeit als Anomalie dokumentiert, gemeldet und gestoppt. Mittels konfigurierbarer **Security Automation Policy** wird die Weiterverbreitung einer Infektion verhindert. Der Flottenschutz wird aufrecht erhalten. Die IoT-Plattform wird nicht beeinträchtigt.
Rhebo unterstützt bereits heute die gängigen Hardware-Architekturen, IoT-Plattformen und Betriebssysteme.

IoT Device Protection »Made in Germany«

TeleTrusT Pioneers in IT security. bitkom Allianz für Cyber-Sicherheit PLATTFORM INDUSTRIE 4.0 SecurITy made in Germany Trust Seal www.teletrust.de/itsmig

Sichern Sie Ihre IoT-Geräte. Kommen Sie mit uns ins Gespräch.

ALEXANDER MÜLLER
VP Product Management

Mobil +49 172 1676644
E-Mail alexander.mueller@rhebo.com

Über Rhebo

Rhebo gewährleistet als einziger Anbieter industrieller Monitoringlösungen sowohl Cybersicherheit als auch Stabilität der OT- und IoT-Infrastruktur in Industrie-, Energie- und Wasserunternehmen. Unsere Software und Services überwachen dazu die Datenkommunikation innerhalb der Steuerungstechnik sowie auf kritischen IoT-Geräten. Angriffe, Schwachstellen sowie technische Fehlerzustände werden zuverlässig und in Echtzeit gemeldet. Rhebo unterstützt damit Betreiber von Industrial Control Systems, Automatisierungs- und Netzleittechnik, die Cybersicherheit, Produktivität und Verfügbarkeit ihrer Anlagen zu steigern und die digitale Transformation der Prozesse zu sichern. Das Unternehmen engagiert sich in dieser Rolle aktiv bei der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem Teletrust – Bundesverband IT-Sicherheit e.V. und dem Bitkom Arbeitskreis Sicherheitsmanagement bei der Erarbeitung von Standards und Handlungsempfehlungen.