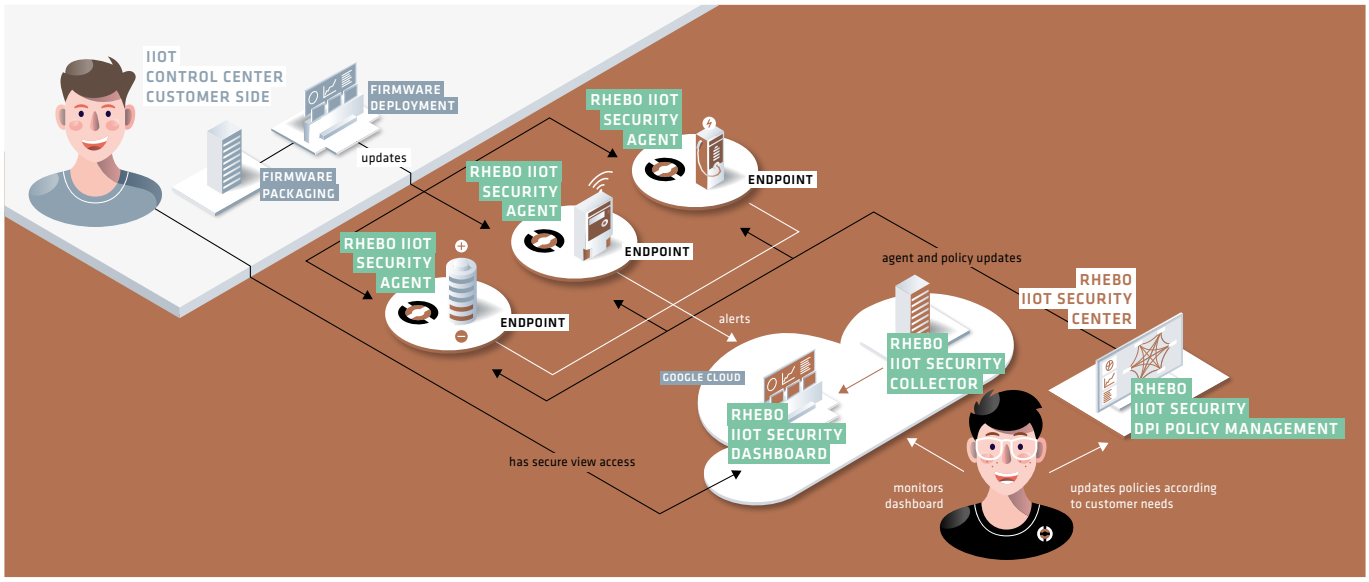
Rhebo IIoT Security agent



KEY COMPONENTS

Rhebo IIoT Security agent
with integrated Deep Packet Inspection (DPI) engine and anomaly detection deployed on each endpoint.

Rhebo IIoT Security collector
on Google Cloud Platform receives all alerts from the Rhebo IIoT Security agents.

Rhebo IIoT Security dashboard, based on the ELK stack, on Google Cloud Platform (Google Marketplace) allows view, search and analysis of alerts.

Rhebo IIoT Policy Management
allows creation, update and deployment of policies to fine tune the alert reporting of the agent DPI engines.

DEPLOYMENT AND CONFIGURATION

Agent deployment

- The agent is deployed as part the endpoint firmware, using the endpoint vendor standard deployment process.
- Once deployed, the agent automatically contacts the collector and establishes a TLS connection to it.

Agent configuration

- Policies can be updated and centrally deployed to agents to configure the type of alerts a fleet of agents reports.
- Policy updates are deployed with a dedicated tool, from the monitoring infrastructure.

TECHNICAL SPECIFICATIONS

Agent specifications

- Linux package embedded in endpoint firmware,
- secure TLS communication to the collector,
- reporting of agent resource use on endpoint,
- integrated DPI engine and anomaly detection for decoding traffic in real time,
- configurable DPI,
- resource usage (example*):
  - <12 MB of RAM
  - <10 % of an ARMv7 CPU
  - ~5 MB of storage.

Alerts (non-exhaustive)**

- port scans,
- unsolicited incoming DHCP response,
- unexpected incoming HTTP request,
- unexpected HTTPS domain,
- unexpected outgoing LAN connections,
- HTTP invalid authentication token,
- SSH connections,
- SSH probing,
- requesting command API without valid auth token.

Alert properties

Alerts include the following information:

- timestamp,
- source IP,
- destination IP,
- protocol,
- port,
- HTTP URL request (where applicable),
- policy ID,
- on-demand traffic capture and pcap download.

DEFAULT PROTOCOLS DETECTED & ANALYZED WITH RHEBO IIOT SECURITY***

ARP	HTTP	McAfee	OpenVPN
CanonBjnp	ICMP	MDNS	SamsungServiceDiscovery
DHCP	IGMP	Modbus	SSDP
DNS	KNX	MQTT	SSH
FroniusDevice	LLDP	NetBOIS	TLS
HopOpt	LLMR	NTP	

* Resource requirements may vary depending on the use case. Typically, the vendor provides the resource usage limits and the agent is adapted accordingly.
** Further incident alerts can be defined based on the use case's requirements.
*** Additional protocols are added to fit our customers use cases while keeping aware of the resource usage.

OT SECURITY Made in Germany · DNV ISO/IEC 27001 · bitkom · CYBERSECURITY MADE IN EUROPE · 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

SPEC-SHEET RHEBO IIOT SECURITY 02-2025