Rhebo & Barracuda Networks
Integrated Cybersecurity in IACS and IoT Networks

Barracuda
Your journey, secured.

With the integration of Rhebo Industrial Protector, Barracuda combines powerful firewall functionality with an integrated monitoring and anomaly detection in Industrial Automation and Control Systems (IACS). Operators can thus not only secure the individual segments at the network boundaries, but also guarantee continuous cybersecurity within the segments.

Integrated OT Cybersecurity In Accordance With IEC 62443

Connected systems require new concepts for cybersecurity and process stability of Operational Technology (OT). Due to the convergence with the enterprise IT and the use of IoT components, the risk of disruptions caused by cyberattacks grows. In addition, increasing vendor heterogeneity makes it more difficult to implement a holistic cybersecurity strategy. It also increases the risk of technical error states.

OT cybersecurity and condition monitoring must be implemented across multiple plants and layers as Defense-In-Depth. They must monitor communication between OT and IT as well as between equipment within the OT. The growing importance of machine-to-machine communication requires an automated solution that reliably identifies suspicious processes. This requires a smooth integration of all security components in order to consolidate relevant data.

The integrated OT cybersecurity solution from Rhebo Industrial Protector and Barracuda CloudGen Firewall and Secure Connector detects any deviation in the OT communication. Suspicious processes are reported or blocked before malfunctions occur.

360° Security From Network To The Edge Device

Barracuda CloudGen firewall and Secure Connector provide up-to-date security measures at network and segment boundaries as well as industrial IoT devices. The solution analyses incoming and outgoing network traffic and reliably detects attacks and malware. Rhebo Industrial Protector monitors and analyses the communication within the OT via IACS monitoring. The anomaly detection identifies and evaluates any deviation in real-time. Thus, even novel attack patterns and technical error states are reliably detected. The data is collected via mirror ports or network taps without interference of OT processes. In distributed environments, the integration takes place directly on the Secure Connector from Barracuda. This enables cost-efficient deployment and at the same time maximum visibility.

The integration of Rhebo Industrial Protector and Barracuda CloudGen Firewall allows the proactive adjustment of security measures. For this purpose, the anomaly detection system transmits security-relevant activities to the firewall, which immediately blocks them. This prevents lateral movement of attacks to other OT segments and prevents communication to the Internet. Thereby, even zero-day vulnerabilities can be effectively secured, where no immediate patching is possible.

Your Advantages
with Rhebo and Barracuda

- **OT TRANSPARENCY** with comprehensive asset inventory of all systems and connections.
- **INCREASED PLANT AVAILABILITY** through localising technical error states in the network.
- **SECURE NETWORKING** for production plants, OT components and IoT devices.
- **ENHANCED INTRUSION DETECTION** through firewall and anomaly detection on one device.
- **FIELD LEVEL VISIBILITY** through integration of Rhebo sensor technology on Barracuda Secure Connector.
- **EFFICIENT OT CYBERSECURITY** without rebuilding or maintenance windows.

Three Use Cases for Integrated OT Cybersecurity

Prevent Malfunctions On Fieldbus Level

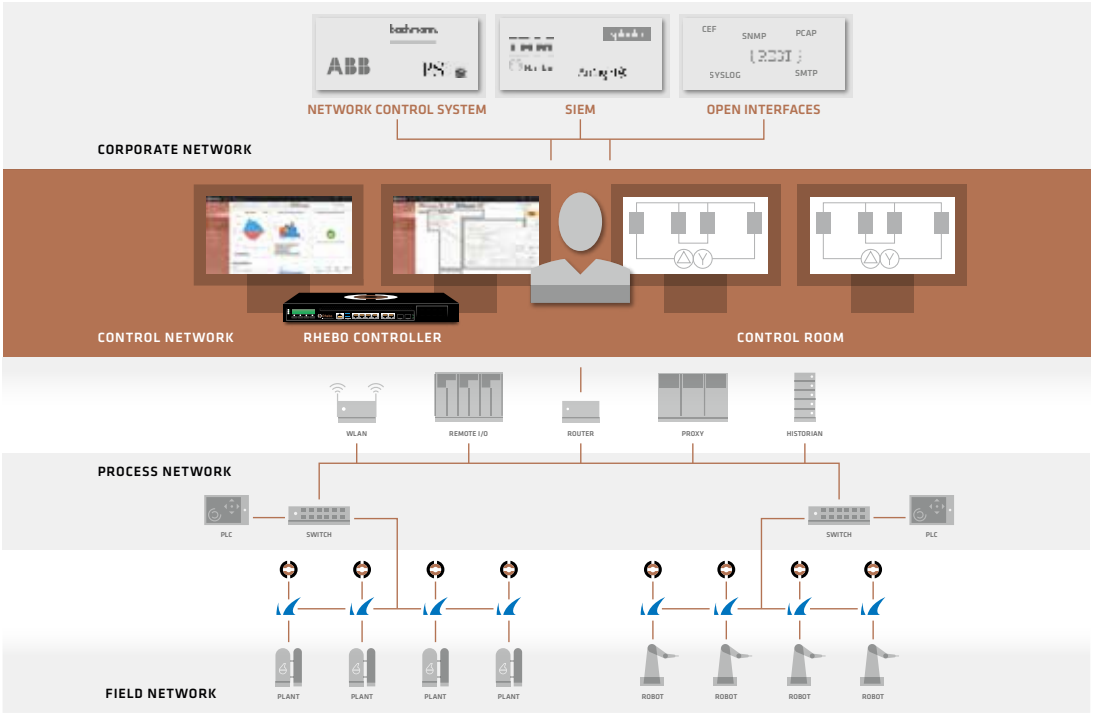
The integration of the Rhebo IACS monitoring with anomaly detection on the Barracuda Secure Connector enables lean and straightforward monitoring of all processes at fieldbus level. Malicious software, for example, introduced to a system via a USB stick, is detected in the production cell before it can laterally spread to the entire network.

Actively React To Anomalies

Rhebo Industrial Protector creates a daily and detailed overview of the systems and equipment communicating in the OT as well as the protocols and commands used. This allows fast identification of anomalies, malfunctions or redundant processes as well as the active adjustment of the Barracuda firewall policies.

Detect Cyberattacks Early On

The anomaly detection of Rhebo Industrial Protector also reports events that occur before a cyberattack (reconnaissance phase). This includes address-, port- as well as Profinet discovery scans. With this information, the Barracuda Firewall can automatically block exploration activities and prevent lateral movements.



Rhebo
Industrial Network Continuity

Barracuda
Your journey, secured.

Rhebo is the only vendor-independent provider of industrial monitoring solutions ensuring both cybersecurity and stability of ICS and IoT infrastructures. The German company's solutions monitor all communication within the ICS and on distributed critical IoT devices. Any attacks, vulnerabilities as well as technical error states are reported in real-time. Thus, Rhebo vendor-neutrally supports industrial, energy and water companies to increase cybersecurity, productivity and availability of their systems and plants to safeguard their digital transformation.

Barracuda Barracuda is committed to making the world a more secure place and believes that every organisation should have access to cloud-ready, enterprise-wide security solutions that are easy to acquire, deploy and use. Barracuda protects email, networks, data and applications with innovative solutions that grow and adapt as the customer journey continues. More than 200,000 companies worldwide trust Barracuda to help them focus on growing their business.
www.barracuda.com

CATARINA WEIDIG
Inside Sales Manager

Phone +49 341 393790202
Email catarina.weidig@rhebo.com