LANDIS+GYR HES SECURITY
24/7 THREAT & INTRUSION DETECTION FOR HEAD END SYSTEMS

MONITOR HES CYBER SECURITY 24/7/365

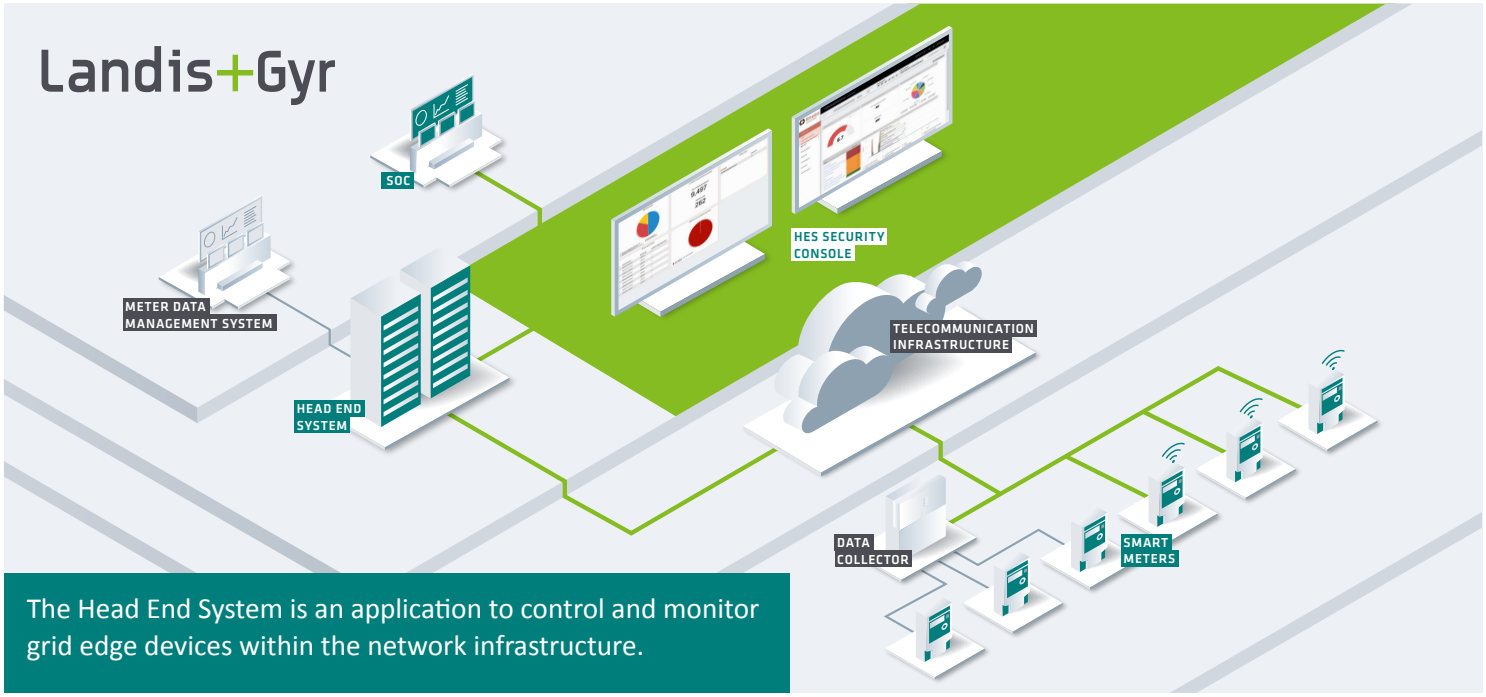
DETECT HES AND SMART METER COMPROMISE IN REAL TIME

ENSURE COMPLIANCE WITH NERC CIP STANDARDS

Energy providers and smart grid operators are under pressure to keep their Head End System operational at all times. Unexpected downtimes due to cyber security incidents or technical errors will result in high costs due to revenue loss, system failure, and legal fines from the NERC and other regulators.

Landis+Gyr HES Security is a dedicated, centralized and easy security monitoring and threat detection solution for Head End Systems. It continuously monitors incoming network communications and configuration changes without requiring changes to the network or devices. Any anomaly is detected, assessed and reported in real time and at all times.

PROTECTING THE HEART OF YOUR AMI INFRASTRUCTURE



The Head End System is an application to control and monitor grid edge devices within the network infrastructure.

CHALLENGE #1: SECURING A DIGITIZED ENERGY INFRASTRUCTURE

2023 has been a record year for cyber incidents in the US and the world:

- 33% increase of ransomware attacks[1];
- US remains #1 target, surpassing 2nd placed UK by a nearly ten-fold victim count[2];
- Appearance of Pipedream, a complete toolkit for disrupting industrial infrastructure;
- 415 industrial control system advisories by CISA.

At the same time, US American and Canadian energy companies are taking big steps in modernizing and digitizing their power distribution infrastructure. This will enable fast remote control of bulk power systems, easy integration of new smart grid applications like smart meters and DER devicesas well as the optimization of monitoring and delivering energy. It also means that critical infrastructure is connected to the outside world and susceptible to external manipulation or disruption. Landis+Gyr devices and systems for advanced energy management have always been designed with cyber security in mind. However, as 2023 has shown the threat landscape is rapidly evolving. With life cycles of 15+ years in industrial environments, a device's security posture today might already be outdated tomorrow.

In particular, the emergence of AI-powered attack techniques and procedures as well as the rise of supply chain compromise have made a company's cyber security a field of high uncertainty. Perimeter security and signature-based prevention is not enough anymore to be prepared for novel attack patterns. The focus of cyber security needs to widen from prevention to the early detection of perimeter breach, compromise and anomalous behavior within the Head End System.

"Our goal is to provide our customers with a compliant and hardened Head End System that is is continuously monitored for cyber threats emerging from zero-day vulnerabilities, supply chain compromise and APTs."

Todd Wiedman | CEO of Landis+Gyr security portfolio Rhebo

CHALLENGE #2: COMPLYING TO SECURITY REGULATIONS

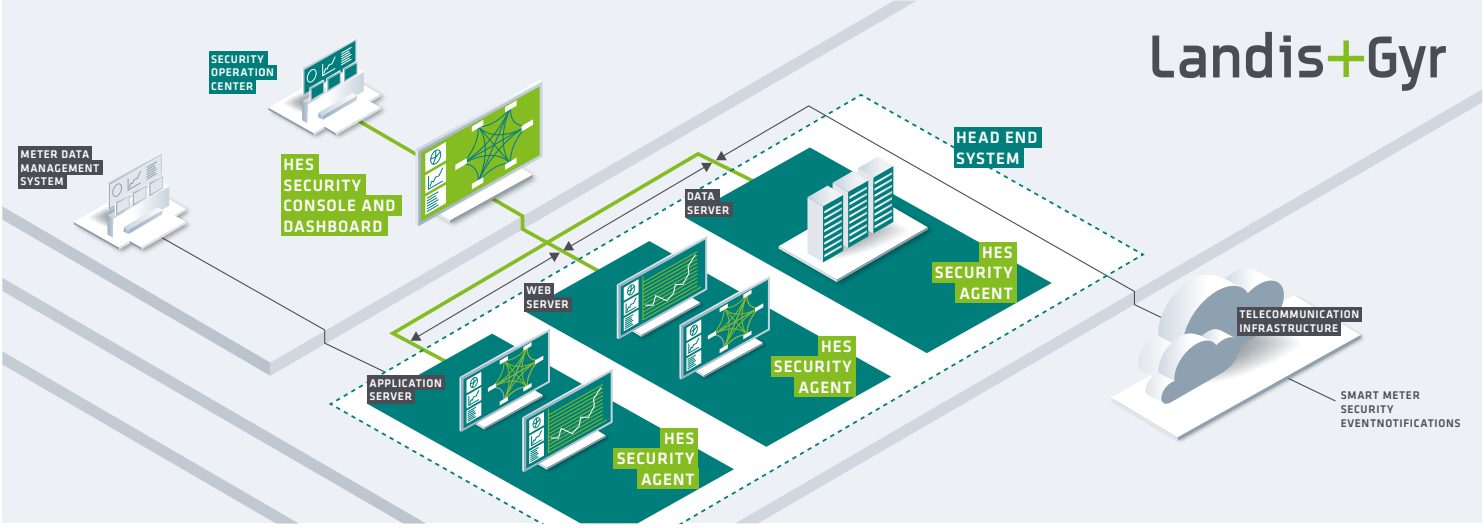
Additionally, energy distributors must comply with a growing set of cyber security regulations. Amongst others, the NERC CIP standards have become the mainstay for securing bulk electric systems (BES) including smart meters and the Head End System. NERC regularly updates its CIP standards, though provides little specific technical guidance. Thus, compliance can become overwhelming when facing the prevailing OT security skills gap, uncertain attack developments and a large variety of technological options. Given that compliance with legally-binding CIP standards is a top priority and necessity for energy companies, the solutions should be simple, manageable and future-proof to fulfill the minimum requirements.

CIP	TASK
CIP-002	▪ identify and categorize all BES Cyber Systems
CIP-007	▪ detect malicious activities, unsuccessful log-in attempts, unauthorized access ▪ identify outdated firmware and known vulnerabilities of BES Cyber System assets ▪ detect inefficiencies of signature-based detection methods
CIP-008	▪ identify, categorize and respond to security incidents ▪ retain records related to reportable security incidents
CIP-009	▪ log and preserve data to determine the cause of the security incident

1 https://www.techzine.eu/news/security/115557/thirty-percent-more-cyber-attacks-in-2023

2 https://cybernews.com/security/ransomware-landscape-overview-2023

CYBER SECURITY IS AT THE HEART OF LANDIS+GYR ENERGY MANAGEMENT SYSTEMS



LANDIS+GYR'S HES SECURITY FOR RELIABLE AMI OPERATIONS

Landis+Gyr HES Security provides enterprise-ready security monitoring and intrusion detection for your Landis+Gyr Head End System. The dedicated OT endpoint intrusion detection system of Landis+Gyr's Rhebo security portfolio continuously monitors and analyzes data collected from the servers and the application. Any activity indicating malicious intent or operational errors is detected, risk assessed and reported for further investigation and informed mitigation.

WHAT?

- security against novel attacks, inside threat actors and intrusion spillover;
- real-time detection of attacks and tampering on your HES, incl. login attempts and configuration changes;
- real-time detection of compromises within your advanced metering infrastructure;
- immediate availability of all details of a security incident for forensic analysis and incident reporting;
- strengthened regulatory compliance.

HOW?

- 24/7/365 security monitoring of the HES solution;
- behavioral analysis of communication using deep packet inspection;
- passive, non-intrusive anomaly detection;
- integration of smart meter security event messages;
- immediate notification about any security incident with pcap files,
- defense-in-depth through hardened systems, perimeter security and endpoint monitoring.

WHY?

- easy, cost-efficient installation and operation as integrated agents;
- comprehensive support 24/7/365 incl. managed services and forensic analysis;
- advanced security solution by leading energy management system developer Landis+Gyr;
- strong track record of more than 300 SaaS Landis+Gyr Head End System customers;
- strong track record of OT-dedicated Rhebo security portfolio in the energy sector.

"We know about the challenge of integrating OT security into the already overwhelming daily workload of security managers. That's why HES Security is a targeted monitoring tool that is effective in detecting known and novel cyber threats to Head End Systems while keeping deployment and operation simple and time-efficient."

Todd Wiedman | CEO of Landis+Gyr security portfolio Rhebo

SECURE YOUR HEAD END SYSTEM AGAINST CYBER THREATS AND TAMPERING

LEARN MORE ABOUT EFFECTIVE AND SIMPLE SECURITY AND ANOMALY MONITORING FOR YOUR HEAD END SYSTEM AND GET IN TOUCH WITH YOUR LANDIS+GYR CONTACT PERSON NOW.

SECURITY@LANDISGYR.COM | +1 855 3455 454

WWW.LANDISGYR.COM/SOLUTION/CYBERSECURITY

ABOUT LANDIS+GYR

Landis+Gyr is the leading global provider of integrated energy management solutions for the utility sector. Offering one of the broadest portfolios, we deliver innovative and flexible solutions to help utilities solve their complex challenges in smart metering, grid edge intelligence and smart infrastructure. With sales of USD 1.8 billion, Landis+Gyr employs approximately 5,600 people in over 30 countries across five continents, with the sole mission of helping the world manage energy better.

www.landisgyr.com

ABOUT RHEBO

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The 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.

www.rhebo.com

Landis+Gyr 30000 Mill Creek Avenue, Suite 100 | Alpharetta, GA 30022 | USA
www.landisgyr.com

HES Security solution brief 2024-02 v01