aprotech Kaspersky IoT company

KasperskyOS Operating system

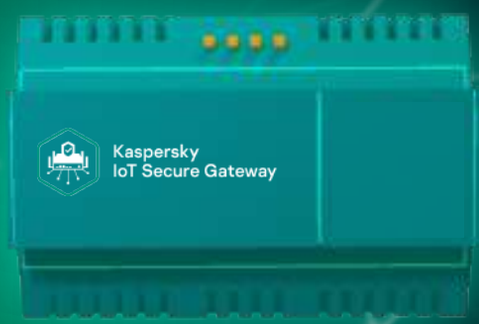
Kaspersky IoT Secure Gateway

Cyber Immune gateways for connecting **ENERGY EQUIPMENT** to clouds and business systems

Scenario №1

Gateway as a software data diode (one-way data transmission)

- **Safe and secure transport** of previously unavailable data for business
- **Trusted data received from the gateway help** to build digital analytics and equipment operation forecasting services
- **Universal software data diode converter** to transmit telemetry data to CIS*
- **Telemetry data collection** in the networks of distributed generation and distribution
- **Monitoring** of gas and steam turbine parameters to optimize operation and foresee equipment breakdowns
- **Monitoring and data collection** of a superchargers' infrastructure



*Corporate Information System

Scenario №2

Gateway as a router (two-way data transmission)

- **Sending security events** via the Syslog protocol
- **Safe and secure two-way data transport** of previously unavailable data for business
- **Analysis of industrial protocols (with intrusion detection/prevention functions)** to provide protection from external threats
- **Gateway** as a part of M2M systems
- **Cyberprotection of infrastructure,** equipment, APCS and SCADA systems when connected to IT systems and during data collection
- **Local storage** of collected data (buffering), emergency data buffer
- **Data protection and transmission** for Technological Information Exchange System (TIES) with Electrical Network Service Operator Automated System
- **Data collection** from digital substations to control, monitor and optimize load
- **Remote access to generation nodes** (for example, DGS*), retranslation of control instructions

*Diesel generator system

Additional notes:

- Creation of ecosystem using Kaspersky Lab products such as KISG+KUMA+KSRW+ KICS+KSC to provide an end-to-end protection of an infrastructure
- Centralized management of Kaspersky Lab products via Kaspersky Security Center