aprotech Kaspersky IoT company

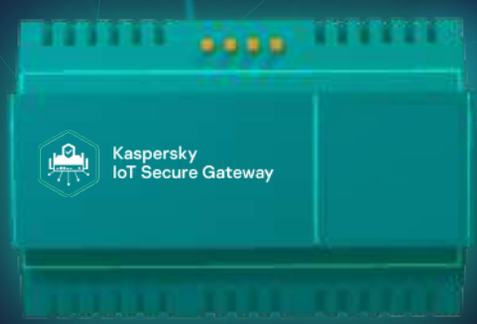
KasperskyOS Operating system

Kaspersky IoT Secure Gateway

Cyber Immune gateways for connecting **PETROCHEMICAL 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
- **Operation monitoring** of drilling rigs to optimize weight and foresee equipment breakdowns
- **Connection and monitoring** of remote technological sites
- **Collection and transmission of parameters** to digitalize an oil terminal

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
- **Cyberprotection of industrial equipment,** DCS, APCS and SCADA systems from cyberattacks when connected to IT-systems and during data collection
- **Data collection and transmission** (CME) received from pumps and well cluster/oil field equipment, to optimize energy consumption and foresee equipment breakdowns, data transmission to demilitarized zone
- **Protection and comprehensive data collection** from processing equipment to create a digital twin of a technological process and an optimal control of a system
- **Local storage** of collected data (buffering), emergency data buffer
- **Secure data collection and transmission** from industrial equipment to DCS

Additional notes:

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