

# Kaspersky IoT Secure Gateway



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

## Scenario N°1

Gateway as a **software data diode** with  
functionality of industrial protocols  
converting (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 CNC machines, pressure equipment, oxygen converter, etc.
- **Operation monitoring** of special vehicles (quarry equipment, trucks)
- **Analysis of production chains**, including logistics tracking (RFID)

## Scenario №2

### Gateway as a firewall with data routing functionality (two-way data transmission)



- Sending security events via the Syslog protocol
- Safe and secure two-way data transport of previously unavailable data for business
- Signature-based intrusion and anomaly detection to provide protection from external threats
- Control and management of industrial equipment (CNC machines, PLC, printers, robots), monitoring of remote sites
- Protection of enterprise perimeter, technological data transfer network level protection, creation of a demilitarized zone
- Local network monitoring to detect new connected devices
- Protection of intelligent video surveillance
- Gateway as a part of M2M systems
- Analysis of production chains, including logistics tracking (RFID)

#### 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 line
- Centralized management of Kaspersky Lab products via Kaspersky Security Center