Kaspersky IoT Infrastructure Security

KasperskyOS

**Kaspersky
IoT Infrastructure
Security**

Protection of the internet of things on the gateway level based on Kaspersky Cyber Immunity approach

The internet of things (IoT) can make the world safer, more comfortable and productive. It can help conserve resources and efficiently manage digital infrastructures in different areas, from video surveillance to smart cities. It also enables the transformation of manufacturing into Industry 4.0.

The IoT concept encompasses an enormous amount of devices, technologies, software, and data transmission protocols. Such a diverse environment faces many risks at all levels.

It is possible to protect the internet of things **on the gateway level**. The device transfers all the data from equipment to cloud platforms. It means that security of the whole IoT networks depends on its security.

Kaspersky offers secure by design gateways based on KasperskyOS. These gateways are the key elements of the **Kaspersky IoT Infrastructure Security** solution and they help build reliable and functional systems for the internet of things.

The first product with Kaspersky Cyber Immunity to hit the market is **Kaspersky IoT Secure Gateway 100** based on the Siemens SIMATIC IOT2040 hardware. It securely transfers data from industrial equipment to cloud platforms using the OPC UA protocol. It has been created by Kaspersky and its subsidiary, Adaptive Production Technology (Aprotech), which helps industrial companies undergo digital transformation.

Another gateway is also a part of the solution. **Kaspersky IoT Secure Gateway 1000** offers data protection and monitoring features. It is based on the Advantech UTX–3117 hardware, and uses the MQTT over TLS protocol to collect data and manage connected devices. Kaspersky Security Center enables centralized configuration and monitoring of all the events of KISG 1000. Together, the two products protect IoT infrastructures on the gateway level, making it possible to monitor them and manage events from a single console.

In future, the product line of **Kaspersky IoT Infrastructure Security** will continue to expand.
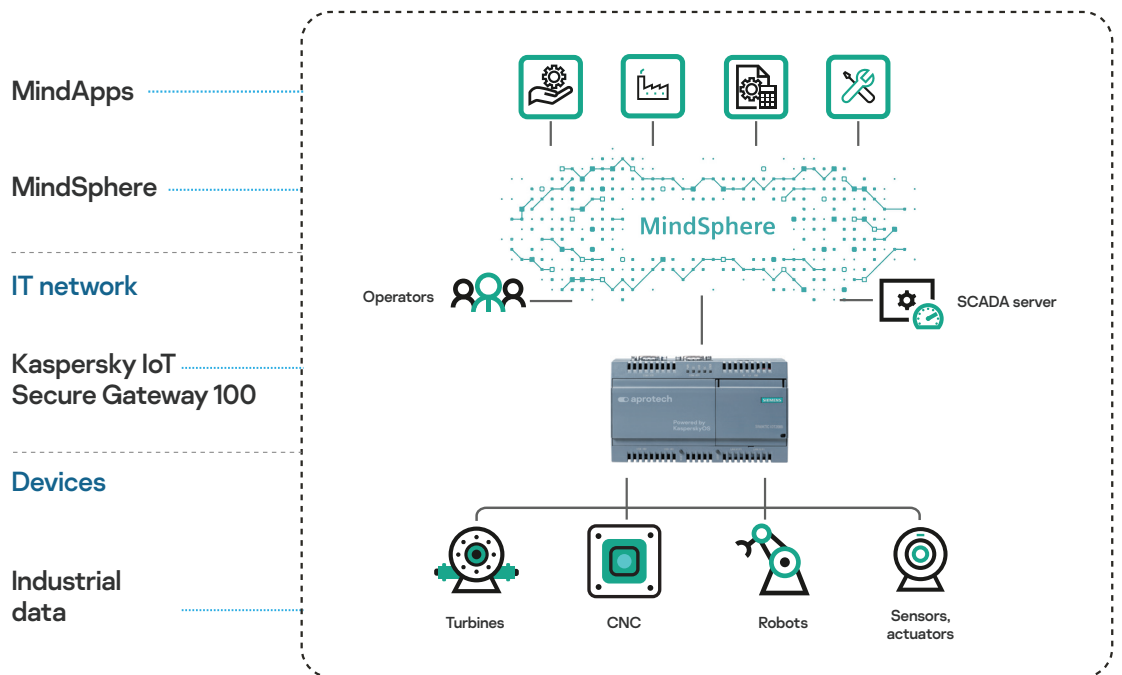
Kaspersky IoT Secure Gateway 100
Cyber Immune gateway for industrial internet of things

Kaspersky IoT Secure Gateway 100 is the first product with Kaspersky Cyber Immunity based on KasperskyOS that is available on the market. The gateway helps industrial companies go through digital transformation: it is a universal bridge for fast and secure connection of OT with corporate IT.

Connecting industrial equipment to a cloud platform enables a detailed understanding of how it works; it allows for better control of production lines, optimizes manufacturing and minimizes downtime, increasing overall business efficiency. Kaspersky IoT Secure Gateway 100 is directly connected to various equipment to securely collect data, converting it to a convenient format and passing it to the Siemens MindSphere cloud platform for storing and processing.

MindApps

MindSphere

IT network

Kaspersky IoT Secure Gateway 100

Devices

Industrial data

MindSphere

Operators

SCADA server

Turbines   CNC   Robots   Sensors, actuators

Kaspersky IoT Secure Gateway 100 in industrial IoT

This IIoT gateway is capable of collecting large volumes of data generated by equipment. A typical SCADA system collects about 10-15% of data from the equipment. This is not sufficient for machine learning, predictive analysis and building math models.

Unidirectional transfer of data through Kaspersky IoT Secure Gateway 100 prevents external access to equipment from the outside. KasperskyOS technologies are the basis of the Cyber Immune gateway; they give it innate protection from cyberattacks. The microkernel of KasperskyOS paired with Kaspersky Security System block all unauthorized processes before execution.

This means that Kaspersky IoT Secure Gateway 100 secures the authenticity of the telemetry from equipment and permits the building of robust user applications on its basis for Siemens MindSphere, as well as working effectively with ERP and MES to control the production cycle.

Features and benefits of KISG 100

Connection	
OPC UA (version 1.04)	Collect and transfer data through proven protocol
Siemens MindSphere	Store and process data in dedicated IoT cloud
Software	
OS	KasperskyOS based on Kaspersky Cyber Immunity principles, SSL/TLS support
Connectivity	Mind Connect API 3.5 Siemens MindSphere

Supported hardware for KISG 100

Siemens SIMATIC IOT2040	
Processor	Intel Quark X1020
Size	53 (L) x 144 (W) x 90 мм (H)
RAM	1 GB DDR3-SDRAM
Ethernet	Supports 100 Mbps LAN 2 x Ethernet (RJ45)
I/O interfaces	1 x USB 2.0 1 x USB client 2 x COM ports (RS 232, RS 485)
Data storage	1 x microSD

About Adaptive Production Technology services

Aprotech offers several services in partnership with Siemens to help industrial companies go through digital transformation:

- **BASE 4.0 consulting**
  It makes it possible to determine bottlenecks in the overall technological setup, or in a single technological process of an industrial company. A digital audit simplifies the transfer to new technologies needed for the gradual optimization of business processes. Based on the results of the audit, Aprotech can help implement technologies that can increase business efficiency (e.g. cloud connection).

- **Development of applications for cloud platform (Siemens MindSphere)**
  The IIoT platform has ready-made services for the basic monitoring of connected equipment as well as specialized applications for predictive analytics, big data analysis, as well as manufacturing efficiency analysis.

- **OEE service** (Overall Equipment Effectiveness)
  The service includes analysis of the general effectiveness of equipment as well as creation of tailored recommendations to improve OEE on the level of a single machine/production line. Three factors are assessed: availability of equipment, its productivity, production quality.
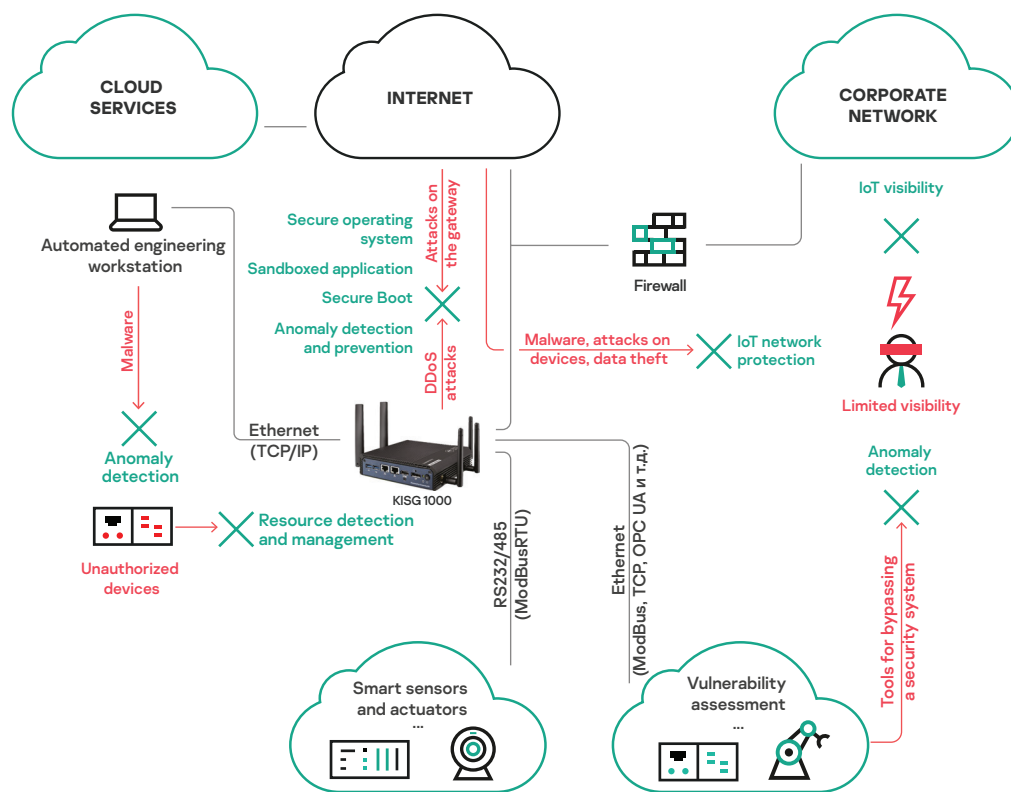
Kaspersky IoT Secure Gateway 1000
Secure gateway for protected internet of things

Kaspersky IoT Secure Gateway 1000 based on KasperskyOS is a product designed for building secure IoT systems. This secure-by-design device provides cybersecurity for the whole IoT infrastructure. The gateway has firewall functions, as well as the technologies of active protection, intrusion prevention and detection. KISG 1000 also helps to securely connect IoT to public or private clouds. Centralized management and monitoring are carried out using the Kaspersky Security Center platform.

Here are the key features of Kaspersky IoT Secure Gateway 1000:

- Can work in other industries as well as manufacturing
- Kaspersky Cyber Immunity — the ability to withstand most types of cyberattacks
- Aggregates data collected via different protocols (Zigbee, LoRa, Modbus, CanBus, PROFINET, OPC UA, etc.), and converts it for transmission over cellular networks and Ethernet (MQTT, CoAP, AMQP, XMPP)
- Not only collects, checks and distributes telemetry, but also transmits control commands received via MQTT to devices
- Performs security functions, such as device detection and classification, logging security events in IoT systems and protection from network attacks (IDS / IPS)

IoT protection with Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 can be used as a security gateway — a specialized border network solution for protection of IoT and IIoT infrastructure from hacker attacks. It's possible to configure it for particular needs, as well as add new functions from partner products.

Features and benefits of KISG 1000

| Подключение	
Ethernet	Connection to data transmission networks over the Ethernet protocol
Routing and NAT	Communication between internal and external networks; use of NAT mechanisms
DHCP server	Building networks of endpoint devices featuring dynamic allocation of their IP addresses
MQTT broker	The Mosquitto-based MQTT broker enables data collection and management of connected IoT devices (sensors and actuators, smart relays, etc.)
OpenSSL/TLS	Support for commonly used encryption mechanisms to secure transmitted data
MQTT over TLS	Secure connection and protected transmission of data between the gateway and the cloud platform
Integration with cloud services	MS Azure, Amazon AWS, IBM Bluemix, and others. Work with any cloud systems using the MQTT protocol; support of simultaneous operation with multiple cloud platforms
Monitoring	
IoT Device Detection & Classification	Detects and categorizes IoT devices based on their network activity. The user interface lets you see all devices in the network, and new devices will be detected within 60 seconds after they are connected
Reports and notifications (MQTT, SYSLOG, Push notifications)	The administrator will be notified each time a new device is connected to the network
Flexible security and gateway management	
Web interface	User-friendly configuration and monitoring of the IoT network, visibility and transparency thanks to WebGUI. Informative dashboard lets you quickly get all the information you need
IoT gateway protection using Kaspersky Cyber Immunity principles	
Core security	KasperskyOS operating system with Kaspersky Cyber Immunity rules out device compromise, thus making a data leak or penetration of the enterprise infrastructure impossible
Secure Boot	Use of encryption methods on IoT devices to verify the integrity and authenticity of the firmware image before booting. Firmware that is corrupted or altered without authorization will not be loaded. Secure Boot can be used together with hardware key storage
Secure Update	Working in conjunction with Secure Boot, this technology lets you upgrade firmware only with correctly signed and encrypted images from trusted sources
IoT infrastructure protection	
IDS/IPS and Firewall	Two mutually complementary mechanisms for protection against network attacks. Firewall protects against unauthorized network access, and malicious activity detection (IDS/IPS) lets you quickly block an attack against nodes of the protected network
Root of trust	This approach is based on a chain of trust. The initial point of trust is chosen based on the specific requirements and can be set at the hardware level in complex cases

Kaspersky IoT Secure Gateway 1000
interface
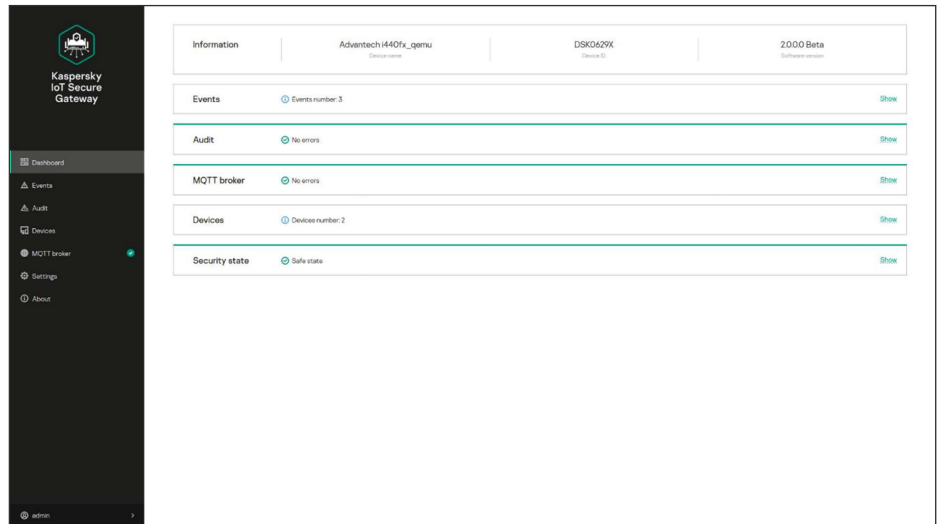
Supported hardware for KISG 1000

Advantech UTX-3117	
Processor	Intel Apollo Lake E3900 & N series processor, 2MB L2 Cache
RAM	Dual channel DDR3L 1867MHz, up to 8GB
Ethernet	Support of Dual 10/100/1000 Mbps LAN LAN1: Intel I210AT LAN2: Realtek RTL8111G
I/O interface	1 x RS-232 with 5v/12v 1 x RS-422/485 full duplex with Phoenix connector 2 x USB3.0 port 1 x SATA interface, on-board support for SSD TPM Infineon chip SLB9665. Support for TPM2.0
Data storage	1 x SATA II SSD bay mSATA 1, used concurrently with H/S MiniPCIE slot
Expansion	1 x Sub1G or mSATA module supporting half-sized Mini PCIE 1 x full-sized Mini PCIE module with 3G/LTE support and SIM slot 1 x Wi-Fi M.2 module that supports electronic keys

Combining KISG 100 and KISG 1000

Kaspersky IoT Secure Gateway 1000 can be used together with Kaspersky IoT Secure Gateway 100 in IIoT by being installed higher — between the IoT and external data networks.
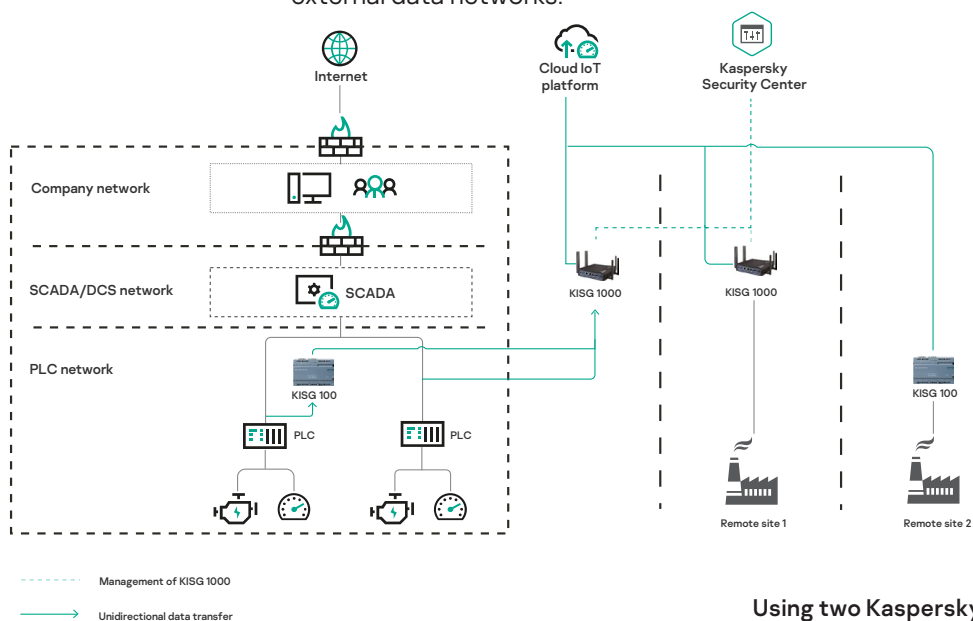

Using two Kaspersky IoT Secure Gateways in IIoT infrastructure

Kaspersky Security Center
Centralized management and monitoring of Kaspersky IoT Secure Gateway 1000

Kaspersky Security Center helps you manage all events of Kaspersky IoT Secure Gateway 1000 β from a single center, track them and conveniently carry out their configuration. These two products form the comprehensive Kaspersky IoT Infrastructure Security solution for transparent, functional and secure internet of things.
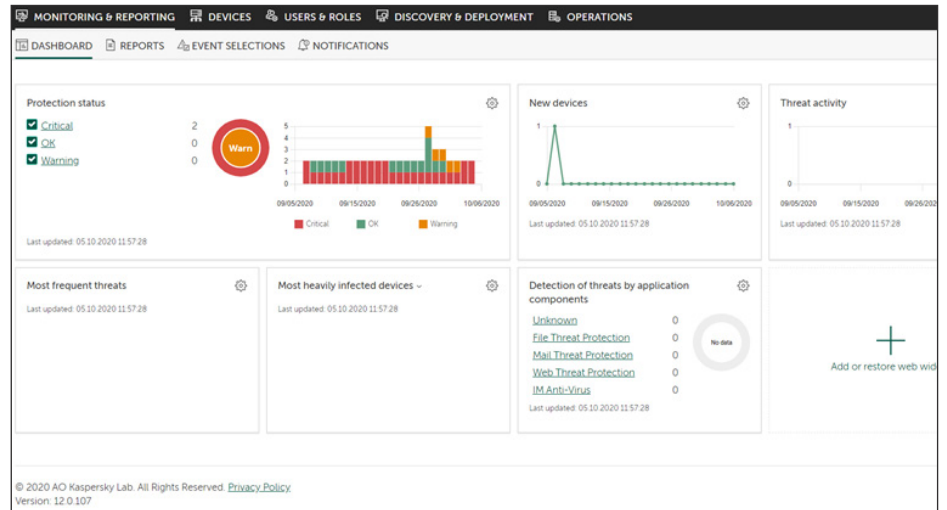
Kaspersky Security Center interface

Features and benefits

Kaspersky Security Center combines tools and technologies to form an advanced integrated platform for centralized administration, monitoring and security of IoT systems.

Expedites routine tasks

Reduces vulnerability to attacks

Helps protect all your endpoints and servers

Simplifies administration

Ensures integrity of systems

Provides a complete picture of the IT environment

Single management console	Automation, transparency, reduced expenses, increased efficiency of administration, and correlation of events from various sources in IoT systems.
	Restricted use of unsuitable or unsecure applications, devices and websites.
	Quick and simple application of security policies on all endpoints
Role-based access	Each administrator can only access the tools and data relevant to their work responsibilities
Easy scalability	Scalability without changing the initial configuration: management of up to 100,000 physical, virtual and cloud-based endpoints using a single Kaspersky Security Center server.
	Optimized backup capabilities

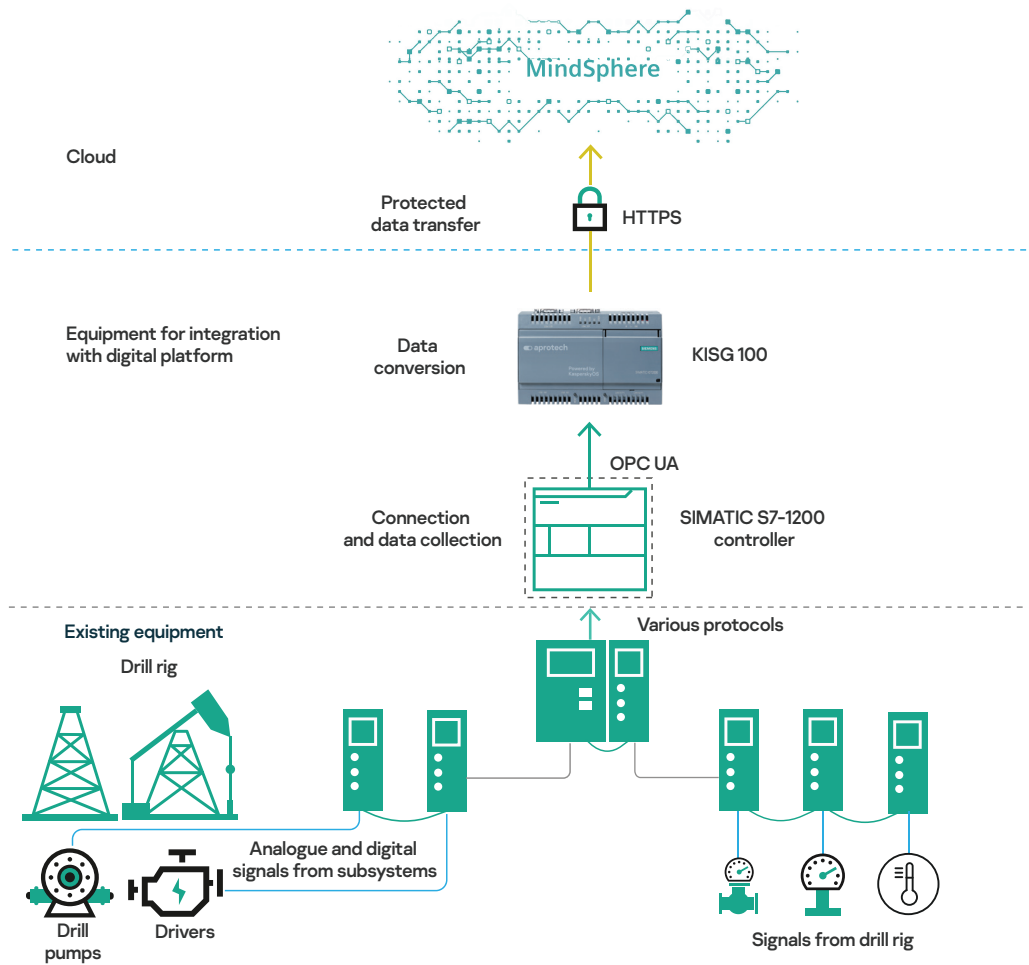|	
Expandable architecture	If a new application is purchased or released, the corresponding extension can be installed without patching or re-installing the console
Convenient alerts	Notifications about incidents through various channels that are convenient for the administrator (text messages, emails, push notifications and others)
Flexible reporting	Customizable and ready-to-use reports with dynamic filtering and sorting by any data field

Use cases for Kaspersky IoT Secure Gateway

Oil & gas industry

An oil producer wants to digitize their technology to implement machine learning and predictive analytics for their equipment. Cloud-based IIoT makes this possible. Equipment (drill rigs, pumps, drives, etc.) is equipped with sensors connected to the gateway which transfers data to a cloud or local storage and processing platform.

Kaspersky IoT Secure Gateway 100 helps build functional IIoT infrastructure, securing trusted telemetry and preparing it for processing. The gateway collects data from all devices using specialized protocols and securely transfers it to the Siemens MindSphere cloud, preventing it from being compromised by external connections to the equipment.

MindSphere

Cloud

Protected data transfer   HTTPS

Equipment for integration with digital platform   Data conversion   KISG 100

OPC UA

Connection and data collection   SIMATIC S7-1200 controller

Existing equipment   Various protocols

Drill rig

Analogue and digital signals from subsystems

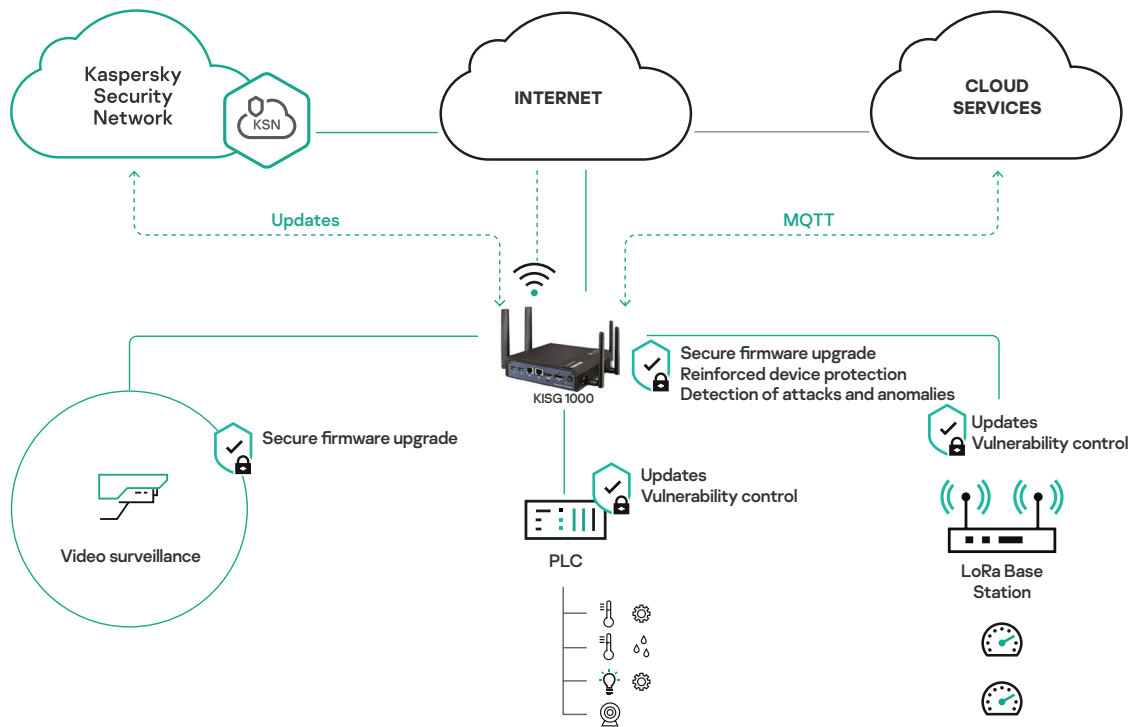Drill pumps   Drivers   Signals from drill rig

Even if there are vulnerabilities in connected IIoT devices, Kaspersky Cyber Immunity in Kaspersky IoT Secure Gateway 100 will prevent attackers from exploiting them and affecting the work of other equipment.

Smart city

A residential building is equipped with systems that monitor the consumption of resources and manage electricity and water supply. The meters inside apartments are connected over the LoRaWAN wireless protocol.

Physical security of the systems is provided through remote-access video surveillance systems, motion detectors and door sensors. Information security is ensured by **Kaspersky IoT Secure Gateway 1000**, which blocks attacks launched against local devices and workstations, identifies unauthorized connections to the network, and protects the network perimeter and cloud communications.

Kaspersky Security Center provides convenient centralized management for the entire IoT infrastructure, helping monitor its security and promptly respond to incidents.

Kaspersky
Security
Network

KSN

INTERNET

CLOUD
SERVICES

Updates

MQTT

KISG 1000

Secure firmware upgrade
Reinforced device protection
Detection of attacks and anomalies

Secure firmware upgrade

Updates
Vulnerability control

Video surveillance

Updates
Vulnerability control

PLC

LoRa Base
Station

Smart warehouse

A warehouse is equipped with climate control systems that can be managed through the cloud to continually maintain and control the climate in the warehouse from any location. Automated warehouse accounting is conducted via RFID sensors and tags and is managed locally (from user workstations on the network) and centrally.

Remote-access video surveillance systems, volume sensors and door sensors provide physical security for the warehouse. Information security is ensured by **Kaspersky IoT Secure Gateway 1000**, which blocks attacks launched against local workstations, identifies unauthorized connections to the network, and protects the network perimeter and cloud communications.

Kaspersky Security Center provides convenient centralized management for the entire IoT infrastructure, helping monitor its security and promptly respond to incidents.
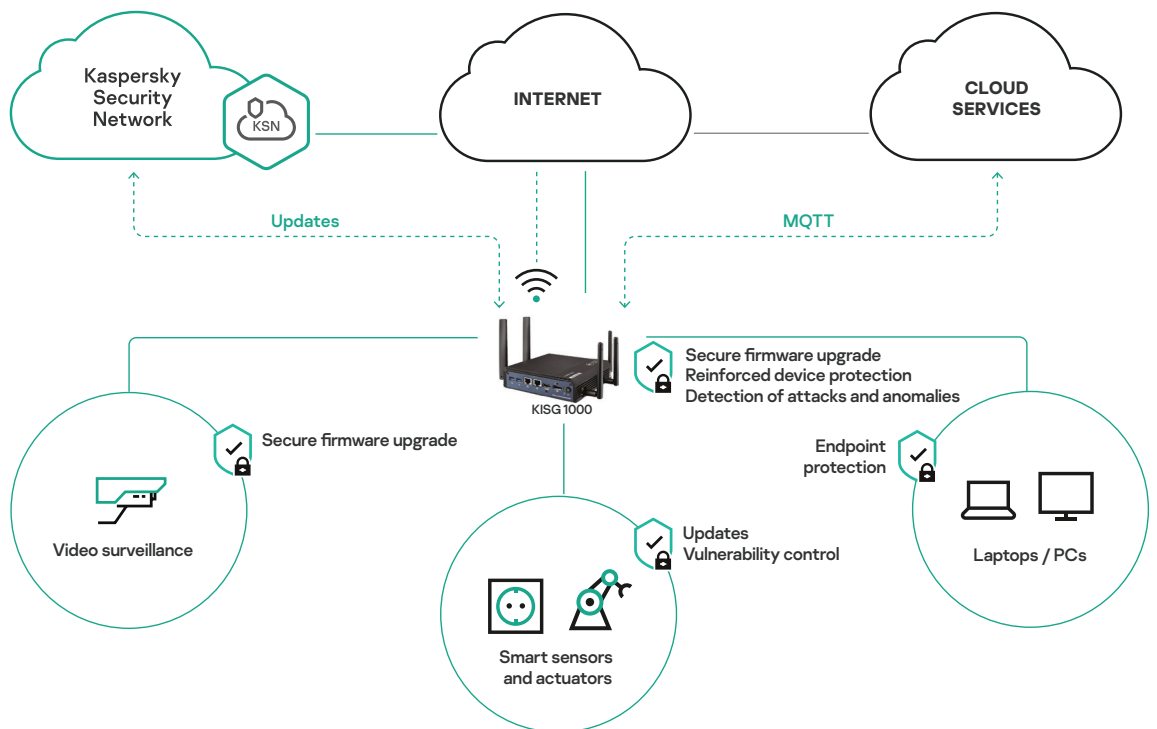

Kaspersky Security Network

KSN

INTERNET

CLOUD SERVICES

Updates

MQTT

KISG 1000

Secure firmware upgrade
Reinforced device protection
Detection of attacks and anomalies

Secure firmware upgrade

Video surveillance

Updates
Vulnerability control

Smart sensors and actuators

Endpoint protection

Laptops / PCs

os.kaspersky.com
www.kaspersky.com

www.aprotech.ru

KasperskyOS
Be Immune

aprotech   Powered by
KasperskyOS