kaspersky BRING ON THE FUTURE

Kaspersky IoT Infrastructure Security

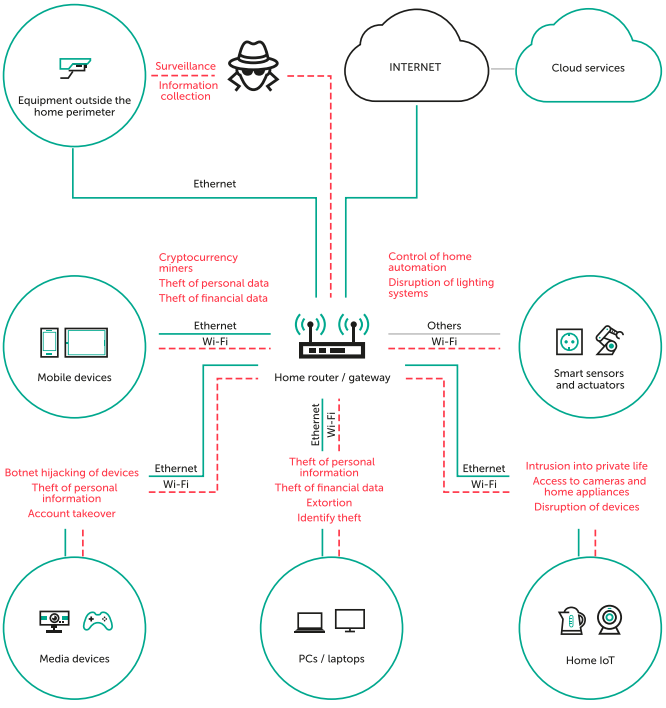
Comprehensive protection for Internet of things infrastructure

The Internet of things (IoT) is changing the world right before our very eyes. It can make it safer and more convenient, help conserve resources and efficiently manage entire production lines.

The IoT concept encompasses an enormous amount of devices, technologies, software, and data transmission protocols. However, the diversity of this environment also brings with it a variety of risks that could threaten the security of various aspects of life.

The complexity of an IoT infrastructure provides cybercriminals with a multitude of opportunities to conduct various attacks. Unfortunately, manufacturers of endpoint smart devices often ignore the main principles of cybersecurity. For example, a lot of hardware fails to ensure the integrity of its firmware, and devices are often delivered with predefined passwords (including default administrator passwords) along with their already weak network security settings or outdated and vulnerable software versions.

The infrastructural and technological complexity of the IoT combined with its exceedingly high rates of growth has unfortunately **turned the Internet of things into a hotbed of potential threats.**



Risk vectors for IoT

Kaspersky IoT Infrastructure Security is a comprehensive solution for protecting and monitoring an IoT infrastructure at all levels, covering everything from endpoint smart devices, gateways and cloud platforms to the actual data transmission channels. Its main component is **Kaspersky IoT Secure Gateway**, which provides security for systems at the gateway level. Monitoring and management is provided through **Kaspersky Security Center**.

Kaspersky
IoT Secure Gateway

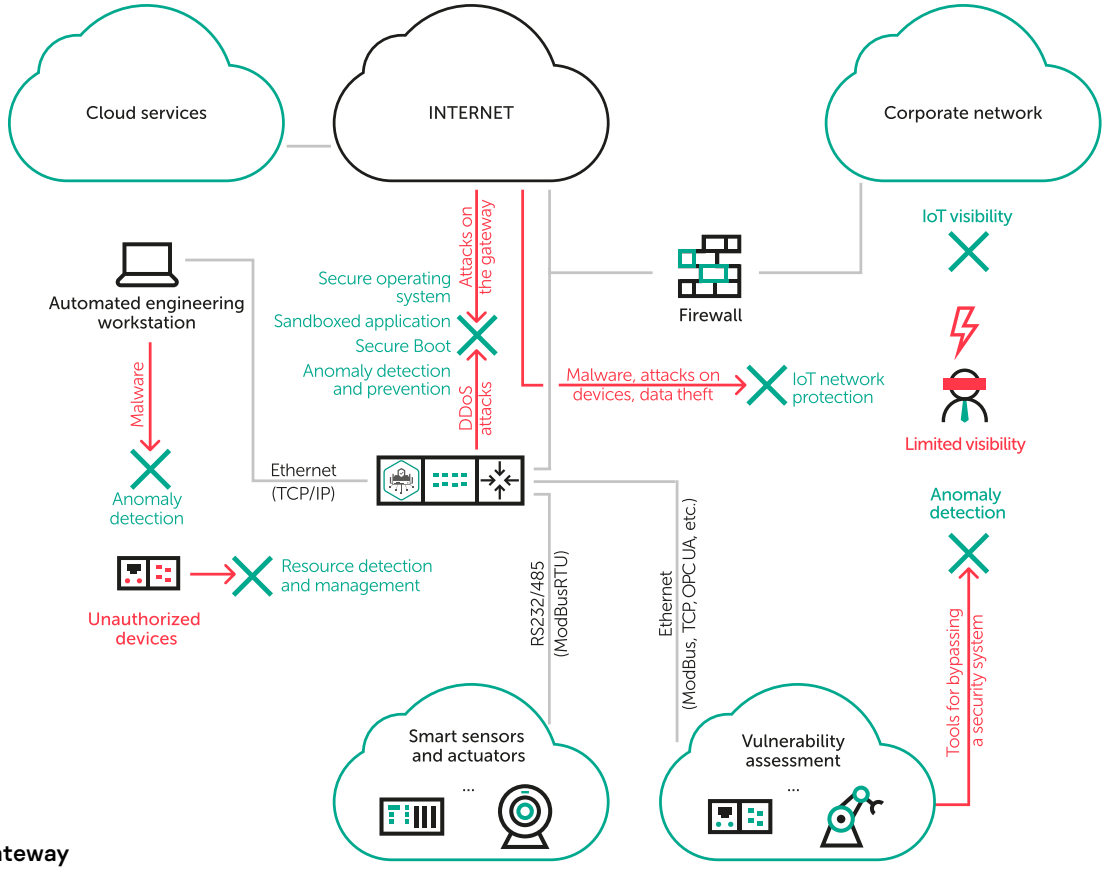
Kaspersky IoT Secure Gateway β*

Secure gateway for protected Internet of things

Some of the most important yet most vulnerable devices in an IoT network are gateways. Their connection to external networks and frequent use of outdated firmware make gateways a prime target for attacks and malware infiltration. Cybercriminals can also exploit a gateway's computing power. For this reason, the gateway of an IoT infrastructure should be secured first of all before any other components of the infrastructure.

Kaspersky IoT Secure Gateway based on KasperskyOS is a product designed for building secure IoT systems. It protects data at the gateway level by receiving, verifying and distributing sensor messages received over the MQTT protocol, and by relaying control commands to actuators. The main security features of the product include detection and classification of devices, registration of security events in IoT systems, and protection against network attacks (IDS/IPS).

Kaspersky IoT Secure Gateway can also be configured and complemented with some features of partner products.



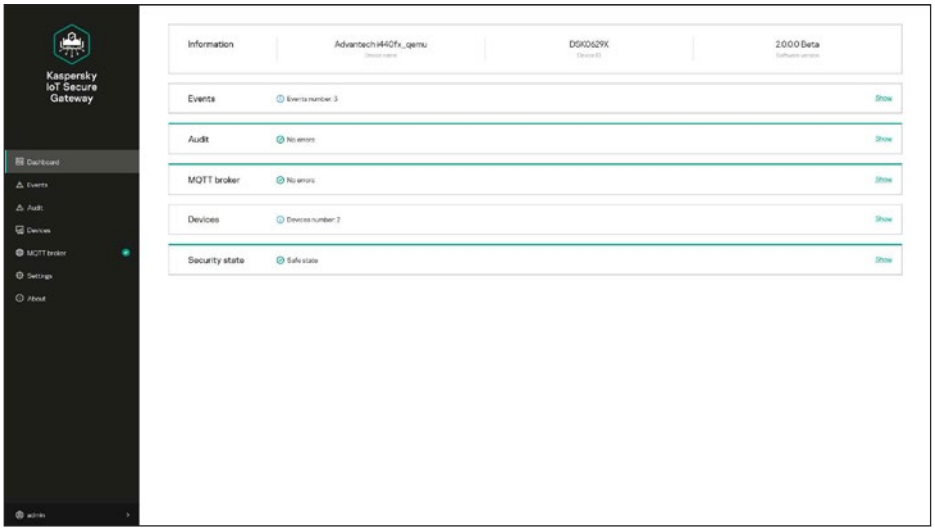
IoT protection with Kaspersky IoT Secure Gateway

* The current version of the product is intended for non-commercial piloting

Features and benefits

Connection	
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 against cyberattacks	
Core security	Security at the level of the operating system kernel (KasperskyOS)
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 (IPS/IDS) 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 β* interface



Supported hardware specifications

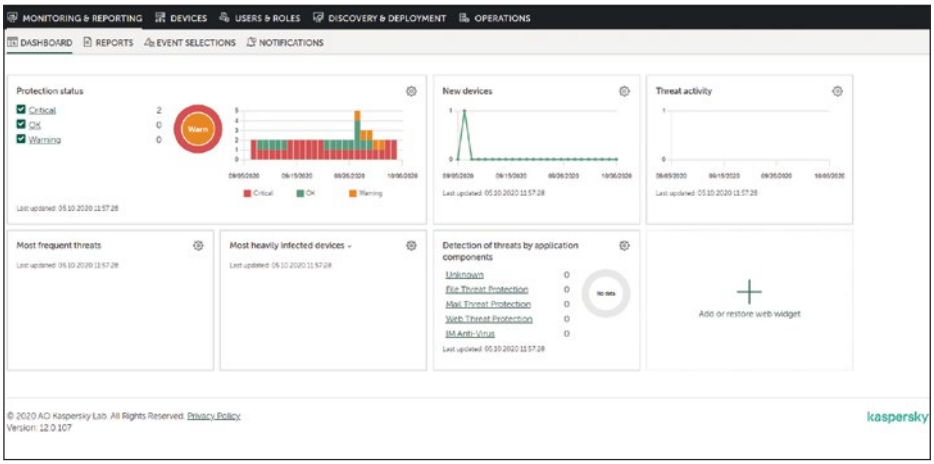
Advantech UTX-3117	
Processor	Intel Apollo Lake E3900 & N series processor, 2MB L2 Cache
RAM	Dual channel DDR3L 1867MHz, up to 8GB
Ethernet	Support of Dual 10/100/1000 Mbps LAN LAN1: Intel I210AT LAN2: Realtek RTL8111G
I/O interfaces	1 x RS-232 c 5v/12v 1 x RS-422/485 full duplex with Phoenix connector 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

* The current version of the product is intended for non-commercial piloting

Kaspersky
Security Center

Kaspersky Security Center

Centralized management and monitoring of Kaspersky IoT Secure Gateway and all objects of IoT infrastructure



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

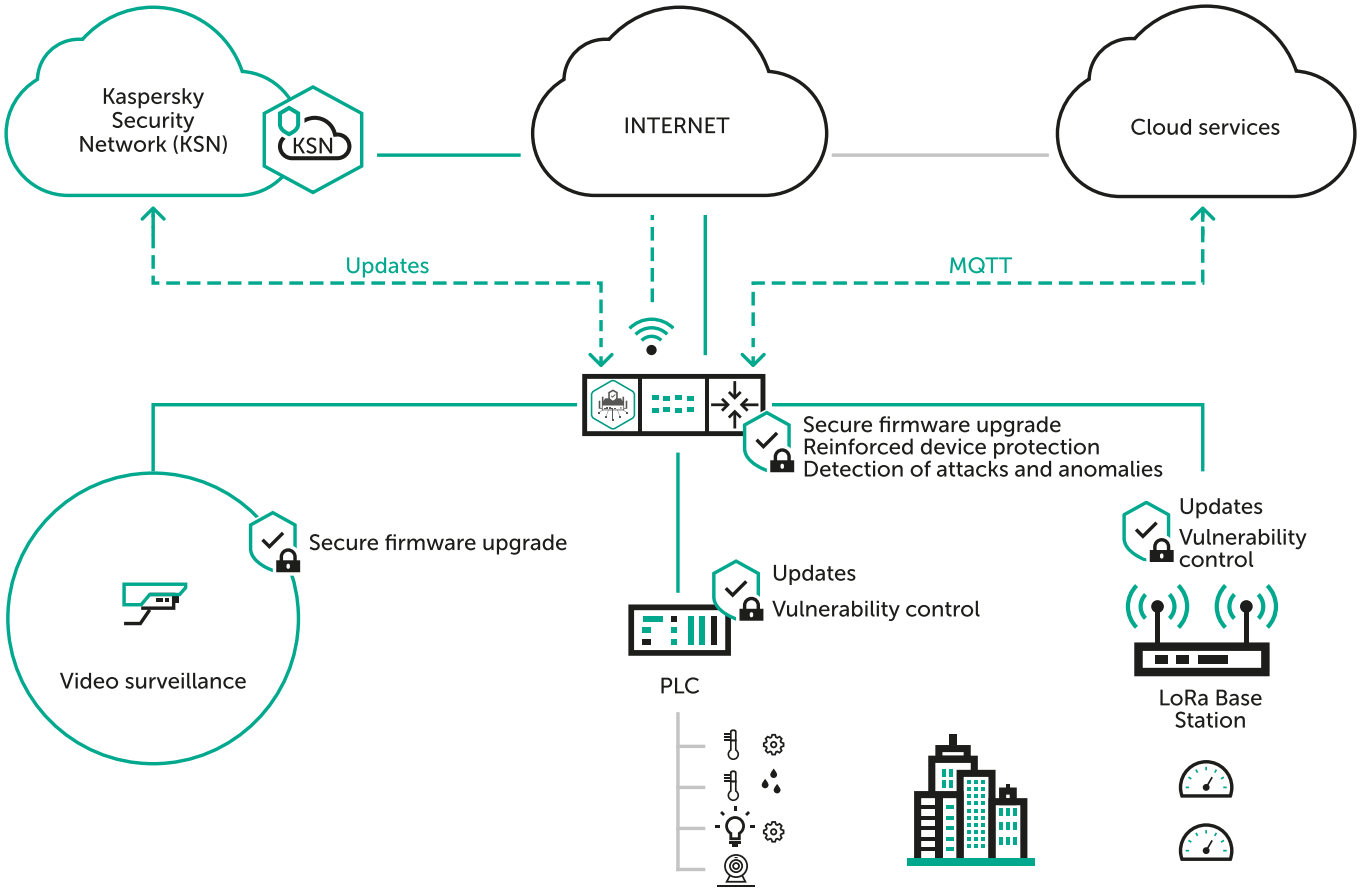
Example implementations of Kaspersky IoT Infrastructure Security

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 wireless protocol known as LoRaWAN.

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,** 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 while monitoring its security and promptly responding to incidents.

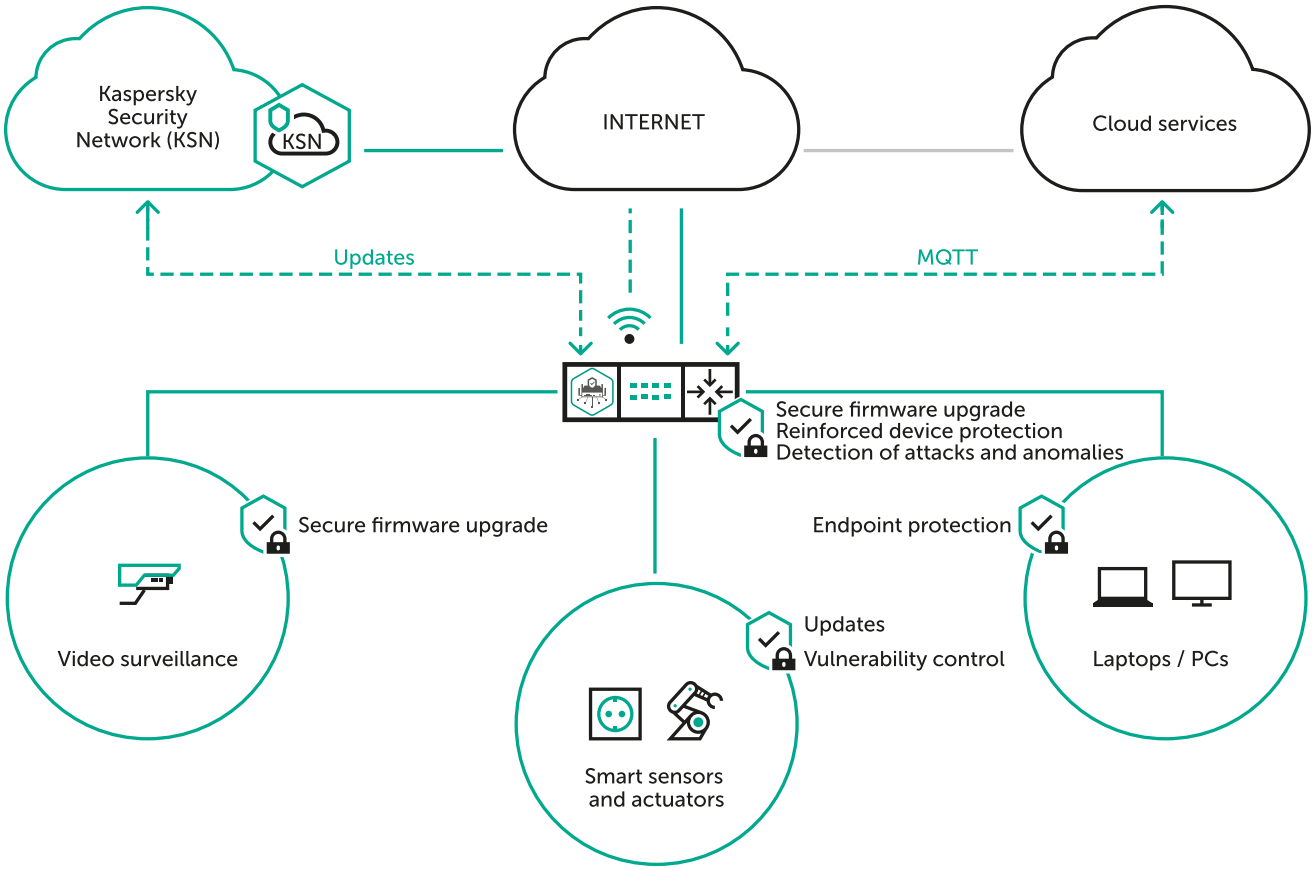


Smart Warehouse

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**, 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 while monitoring its security and promptly responding to incidents.



KasperskyOS®

Kaspersky
IoT Infrastructure
Security

Learn more on os.kaspersky.com

www.kaspersky.com