aprotech Kaspersky IoT company KasperskyOS Operating system

start@aprotech.ru
aprotech.online

Kaspersky IoT Secure Gateway

The device is based on the KasperskyOS operating system

Cyber Immune data gateway of a new generation for creating a secure communication channel between technological and corporate data networks including system protection of industrial internet of things (IIoT) from cyberattacks

Main applications:

- Industry
- Petrochemistry
- Smart cities/buildings
- Transport and logistics
- Energy
- and other fields

Application

Data gateways bring together operational technologies (OT) with information technologies (IT). With the help of these devices, it is possible to connect industrial equipment and monitoring and automatization systems to different systems of visualization, data storage and processing: starting from standard corporate systems MES/ERP and ending with advanced IoT platforms with digital analytical services.

Two modes of operation

The device can be connected to the Internet through the Ethernet or 3G/LTE and can operate in two modes:

«Router» - router with functionality of firewall, analysis and filtration of industrial protocols (with intrusion detection/prevention functions) and also MQTT broker

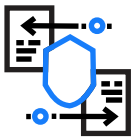
«Data diode» - data collection by industrial protocols with further converting and one-way transmission to corporate and cloud systems through IoT-protocol MQTT with future expansion of functionality

aprotech Kaspersky IoT company

KasperskyOS Operating system

Let's go digital together!

KISG key features

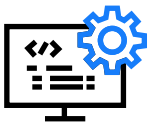


Secure data transmission

Cyber immune gateway provides a safe data transport and protection of the network infrastructure from cyberattacks. Additional functions of a network security (firewall, analysis of industrial protocols) allow to control network communications and respond promptly to incidents.

Centralized management

Management of gateways is provided from the single Kaspersky Security Center (KSC) administration console. The console also helps to monitor security events registered by KISG, set up devices remotely and update system components.



Support of third-party applications

It is possible to develop your own apps for the KasperskyOS operating system that will be added to a public app store. The delivery to a device is carried out through the Kaspersky Security Center that ensures application authenticity and their safe installation.

Cyber Immunity

Cyber Immunity – is the approach of Kaspersky Lab applied to the development of the secure by design systems. Cyber Immune data gateway will perform critical functions even in hostile environments. It is protected not only from known but also from unknown cyberattacks at the level of architecture without additional security features.

Advantages of the KasperskyOS operating system:

- All OS entities/domains are strictly isolated and interact only via microkernel
- Microkernel KasperskyOS is responsible for the functions that can be performed only in a privileged mode. All other functions of OS (including drivers, file systems and networking stacks) are carried out in a user mode
- Each interprocess communication is strictly controlled by Kaspersky Security Module and is verified in accordance with security policies

aprotech Kaspersky IoT company

KasperskyOS Operating system

Hardware platform Specifications

Technical data

Processor type	Intel Pentium N4200, 1,1GHz, 2MB L2 Cache
Storage	SATA II SSD (32GB)
Type of memory	DDR3L, 1600MHz
RAM	8GB
Interfaces	2x100/1000 Mbps Ethernet RJ45
Cellular service	3G/4G modem (optional)
Operating temperature range	From +5 to +35 °C
Storage temperature range	From -40 to +85 °C
Relative humidity	Up to 80% at 25 °C (non-condensing)
Input voltage	DC 12...24V AC 110...220V (optional)
Mount	DIN rail

Connection

Ethernet	Two interfaces for connecting to different network segments via twisted pair (LAN and WAN)
3G/LTE	Ability to use the cellular network as the primary or backup communication channel
Routing and NAT	Configuration of static routing. Port forwarding (Destination NAT), masquerading.
VRRP	Two or more KISG 1000 devices can be grouped into VRRP failover cluster (virtual router on LAN interface)
DHCP server	Automatic distribution of network configuration parameters to other devices operating in the local network
MQTT broker	MQTT broker based on Mosquitto enables centralized data collection from IoT devices
TLS	Support for common cryptographic protection mechanisms for data transmitted via MQTT and Syslog
Integration with cloud services	Works with IoT platforms using MQTT protocol
VPN	VPN support

aprotech Kaspersky IoT company

KasperskyOS Operating system

Infrastructure protection

Firewall	The firewall works according to the “Deny by Default” principle. The administrator can be sure that only permitted network communications will pass through the gateway.
Firewall of the industrial network level	• Control and filtration of the industrial communication protocols: MQTT, Modbus, BACnet, DNP3, MMS,OMRON-FINS, ENIP/CIP, TriStation, S7comm • Anomaly inspection for MQTT and Modbus TCP
Analysis of industrial protocols (with intrusion detection/prevention functions)	The intrusion detection/prevention module issues alerts and blocks malicious activity and also sends a notification about the incident to Kaspersky Security Center and SIEM-system
DPI	Filtration (blocking) of the application protocols’ traffic: FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3

Monitoring

Reports and notifications (MQTT, Syslog, KSC)	The administrator can receive security events in the unified enterprise security management console – Kaspersky Security Center – as well as transfer events to the third-party systems (SIEM, cloud platforms, etc.) via Syslog and MQTT protocols

Flexible security and gateway management

Web interface	Informative dashboard quickly allows to get all the required information. Convenient IoT network setup and monitoring, visibility and transparency using WebGUI.
Centralized management system	The Kaspersky Security Center administration console makes it possible to handle events from all KISG deployed in an organization's infrastructure. It also allows you to monitor the status of gateways and manage their configuration.
RBAC	Role-based access control
Backup	The ability to restore system configuration from the previously saved backup copy

Gateway protection against cyberattacks

Cyber Immunity (Secure by design) OS	The KasperskyOS operating system eliminates the possibility of device compromise and helps to protect the infrastructure of the organization from cyberattacks
Secure boot	The integrity and authenticity of the gateway firmware is verified using cryptographic methods before uploading the image. Firmware that is damaged or altered without authorization will not be loaded.
Secure update	Working in conjunction with secure boot, the technology allows firmware updates only when properly signed and encrypted images are used