Find out more about this product and the successful projects that use it os.kaspersky.com/solutions/kaspersky-iot-secure-gateway

Kaspersky IoT Secure Gateway

Next-generation Cyber Immune data gateway running the eponymous KISG software platform based on the KasperskyOS operating system.

Main application areas:

- Smart cities/buildings
- Transportation and logistics
- Manufacturing
- Petrochemical
- Energy
- Other industries

Purpose

Data gateways connect the world of operational technology (OT) with the world of information technology (IT). You can use them to connect industrial equipment and facility monitoring and automation systems to various data storage, processing and visualization systems, ranging from standard corporate MES/ERP systems to advanced IoT platforms with digital analytics services.

Two main modes

The device connects to the internet via Ethernet or 3G/LTE technologies and can operate in two different modes:

Data Diode mode – collects data over industrial protocols with subsequent conversion and unidirectional transmission to corporate and cloud systems. A connection via the MQTT IoT protocol has already been implemented. This functionality will be extended in the future.

Router mode – serves as a router with firewall functionality, analysis and filtering of industrial protocols (with intrusion prevention and detection function), and MQTT broker.

Key benefits of KISG

Secure data transport

The Cyber Immune gateway ensures reliable data transport and protection of the network infrastructure against cyberthreats. Its additional network security functions enable control of network interactions and timely responses to incidents.

Centralized management

Gateways are managed through Kaspersky Security Center (KSC), a unified management console. The console lets you track security events registered by KISG and remotely configure and update system components.

Third-party applications from Kaspersky Appicenter™

The Kaspersky Appicenter platform includes all the necessary tools to create, distribute and work with third-party applications on a device, including applications with edge computing functionality. Applications are delivered to devices through management consoles such as Kaspersky Security Center, which guarantees the authenticity of applications and their safe installation.

Edge computing

The gateway supports applications with edge computing capabilities that enable:

- unification of field equipment while supporting sensor diversity;
- unification of communication interfaces with information systems;
- reduction in traffic and cloud resources via on-premises analytics;
- zero-latency management;
- secure installation and update of applications.

Cyber Immunity

Kaspersky's approach to developing structurally secure systems. The Cyber Immune data gateway performs critical functions even in aggressive environmental conditions and is protected not only from known threats but also from currently unknown threats at the architectural level without the need for externally sourced security tools.

Distinctive features of KasperskyOS:

- All OS entities/domains are strictly isolated from each other and interact only through the microkernel.
- The KasperskyOS microkernel is responsible for functions that can be performed only in privileged mode. All other OS functionality, including drivers, file systems and network stacks, has been relegated to user mode.
- All interprocess communication is strictly controlled by the Kaspersky Security Module and checked for compliance with security policies. In accordance with the Default Deny principle, anything that is not explicitly allowed by security policies is prohibited.

KISG technical specifications and functionality

Hardware platform specification

Processor type	Intel Pentium N4200, 1.1 GHz, 2 MB L2 Cache
Storage	SATA II SSD (32 GB)
Type of memory	DDR3L, 1600 MHz
RAM	8 GB
Interfaces	2x100/1000Mbps Ethernet RJ45
Cellular connection	3G/4G modem (optional)
Operating temperature range	+5°C to +35°C
Storage temperature range	From -40 to +85°C
Relative humidity	up to 80% at 25°C (without condensation)
Input voltage	DC 12...48 V AC 110...220 V (optional)
Energy consumption	20 W (max)
Mount	DIN rail, 19" RACK
Dimensions	165 x 220 x 44 mm (D x W x H)
Weight	1.2 kg

Network functions

Ethernet	Two interfaces for connecting to different network segments via twisted pair (LAN and WAN).
3G/LTE	Ability to use the mobile data network as the primary or backup communication channel.
Routing and NAT	Configuration of static routing. Port forwarding (Destination NAT), masquerading.
VRRP	Combining multiple gateways into a fault-tolerant network cluster. Virtual gateway on a LAN interface.
DHCP server	Automated distribution of network configuration settings to devices residing in the LAN.
MQTT broker	The Mosquitto MQTT broker enables centralized data collection from IoT devices.
TLS	Support for common cryptographic protection mechanisms for data transmitted via MQTT and Syslog.
⬡ VPN	VPN support.
Integration with cloud services	Work with IoT platforms over the MQTT protocol. Extend functionality using applications from Kaspersky Appicenter.

⬡ — application is available in Kaspersky Appicenter

Network infrastructure protection

Firewall	The firewall works according to the default deny principle. The administrator can be sure that only permitted network communications will pass through the gateway.
⬡ Firewall at the industrial network level	• Control and filtering of industrial data transfer protocols: MQTT, Modbus, BACnet, DNP3, MMS, OMRON-FINS, ENIP/CIP, TriStation, S7comm. • Scan traffic of the MQTT and Modbus protocols for anomalies (deviations).
⬡ Industrial protocol filtering with intrusion detection and prevention function	Module blocks malicious and suspicious network activity and forwards incident notifications to Kaspersky Security Center and the SIEM system.
DPI	Filter (block) traffic of application protocols: FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3.
Reports and notifications (MQTT, Syslog, KSC)	An administrator can receive KISG security events in a unified enterprise security management console such as Kaspersky Security Center, and can forward events to recipient systems (SIEM, cloud platforms, etc.) via the Syslog and MQTT protocols.

Flexible gateway management

Web interface	Informative dashboard that lets you quickly get all the up-to-date information you need. Convenient IoT network setup and monitoring, visibility and transparency thanks to WebGUI.
Centralized management system	The Kaspersky Security Center management console works with events received from all KISG instances deployed in an enterprise infrastructure. It can also be used to track the status of gateways and manage their configuration.
Application management	Irrespective of your specific approach to device management, Kaspersky Appicenter functionality lets you find, install, update and remove applications in any interface.
RBAC	Role-based access control.
Backup	Restore your system configuration from a previously saved backup.

Gateway protection against cyberattacks

Cyber Immunity (Secure by Design)	The KasperskyOS operating system eliminates the possibility of the device ever being compromised and helps protect the enterprise infrastructure from cyberattacks.
Secure boot	The integrity and authenticity of the gateway firmware is verified using cryptographic methods before uploading the image. Firmware that is altered without authorization will not be loaded.
Secure update	Used in conjunction with secure boot, this technology only allows firmware updates with properly signed and encrypted images.

⬡ — application is available in Kaspersky Appicenter

os.kaspersky.com **www.kaspersky.com**