

Kaspersky IoT Secure Gateway 1000

Product data sheet



Kaspersky
IoT company

Kaspersky IoT

Secure Gateway (KISG) 1000

Based on the KasperskyOS operating system and Advantech UTX-3117 hardware platform.

A Cyber Immune data gateway for a secure, transparent and functional internet of things. A key tool for building reliable end-to-end digital services in industry, smart cities, CCTV and other fields.



Cyber Immunity + network protection

Inherent security at the OS architecture level plus firewall functions. The device will perform critical functions even in hostile environments and will detect and prevent intrusions into an organization's network.

Secure data transport

The gateway collects data from IoT devices and transmits it securely to digital platforms.

Centralized management and web interface

The Kaspersky Security Center (KSC) platform makes it easy to monitor and manage KISG 1000 events. Gateway settings are accessible via the web interface.

KasperskyOS operating system:

- All OS entities/domains are strictly isolated and therefore cannot impact each other
- Proprietary microkernel blocks unauthorized interactions based on security verdicts by default
- Verdicts are determined by the Kaspersky Security System engine based on security policies enabling finely tuned configuration

Protocol

- MQTT. Secure connection and data transmission between gateway and cloud platform

Cloud platform connection

- Works with any cloud systems using the MQTT protocol

Combined use of KISG 1000 and KISG 100

KISG 100 connects industrial equipment via the OPC UA protocol and transmits data to a cloud-based IoT platform. In this scenario, KISG 1000 acts as a network router and also monitors and protects other devices from external network attacks.

KasperskyOS is open for development. KISG 1000 components can be supplemented with new ones as required.

Hardware platform

Advantech UTX-3117 technical specifications

Specifications

Processor type	Intel Pentium N4200, 11GHz, 2MB L2 Cache
Storage	SATA II SSD (32GB)
Type of memory	DDR3L, 1600MHz
RAM	4GB
Interfaces	2xGbE LAN, 2xMiniPCle
Additional communication device	3G/4G modem (optional)
Operating temperature range	From -20 to +60 °C
Storage temperature range	From -40 to +85 °C
Relative humidity	Operating: up to 95% at 40 °C (non-condensing)
Input voltage	12 ~ 24V
Average power consumption	12V * 0.35(A), 4.2W
Maximum power consumption	12V * 0.61(A), 7.32W
Dimensions	Length 128mm, width 152mm, height 37mm

Connection

Ethernet	Two interfaces for connecting to different network segments via twisted pair (LAN and WAN)
Cellular modem	Ability to use the mobile data network as the primary or backup communication channel
Routing and NAT	Automatically configurable routing between KISG 1000 interfaces. Ability to control NAT operation (masquerading)
DHCP server	Automatic distribution of network configuration to IoT and other devices located in the local network
MQTT broker	MQTT broker based on Mosquitto enables centralized data collection from IoT devices
OpenSSL/TLS	Support for common cryptographic protection mechanisms for data transmitted via MQTT and Syslog
Integration with cloud services	Works with any cloud systems using the MQTT protocol

Monitoring

Device detection and classification	Discovers devices located in the local network based on their network activity. The user interface displays all network devices communicating with the KISG 1000, and new devices will be detected within 60 seconds
Reports and notifications (MQTT, Syslog, push notifications, KSC)	The administrator can receive KISG 1000 security events in the unified enterprise security management system – Kaspersky Security Center – as well as transfer events to third-party systems (SIEM, cloud platforms, etc.) via Syslog and MQTT protocols. KISG 1000 supports integration with Google Firebase for push notifications to mobile devices

Flexible security and gateway management

Web interface	Convenient IoT network setup and monitoring, visibility and transparency thanks to WebGUI. Informative dashboard allows you to get all the information you need quickly
Centralized management system	The KSC platform makes it possible to handle events from all KISG 1000s deployed in an organization's infrastructure. It also allows you to monitor the status of gateways and manage their configuration

Gateway protection against cyberattacks

Cyber Immunity (secure by design)	The KasperskyOS operating system eliminates the possibility of device compromise, making it impossible to leak data or infiltrate enterprise infrastructure
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 only allows firmware updates using properly signed and encrypted images

IoT infrastructure protection

IDS/IPS and 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. The IDS/IPS (intrusion detection and prevention) module issues alerts and blocks malicious activity detected by a set of signatures prepared by Kaspersky specialists
----------------------	--

**ADAPTIVE PRODUCTION
TECHNOLOGIES LLC**

**Contact us, and we'll start
digitalization together!**

**start@aprotech.ru
+7 (495) 970-71-17**

**aprotech.online
os.kaspersky.com**