Kaspersky IoT Secure Gateway 1000

All data transmitted between devices and cloud platforms passes through IoT gateways, which means that the security of the entire infrastructure depends on the security of these gateways. Kaspersky IoT Secure Gateway (KISG) 1000 is an internet of things data gateway powered by the KasperskyOS operating system. It both collects data from IoT devices and helps to provide reliable cybersecurity.

Data gathering

KISG 1000 can be used in the manufacturing sector and beyond. The gateway provides for centralized collection of data from IoT devices (sensors, controllers, etc.), and secure data transmission to a cloud platform via the MQTT protocol.

OS-level security

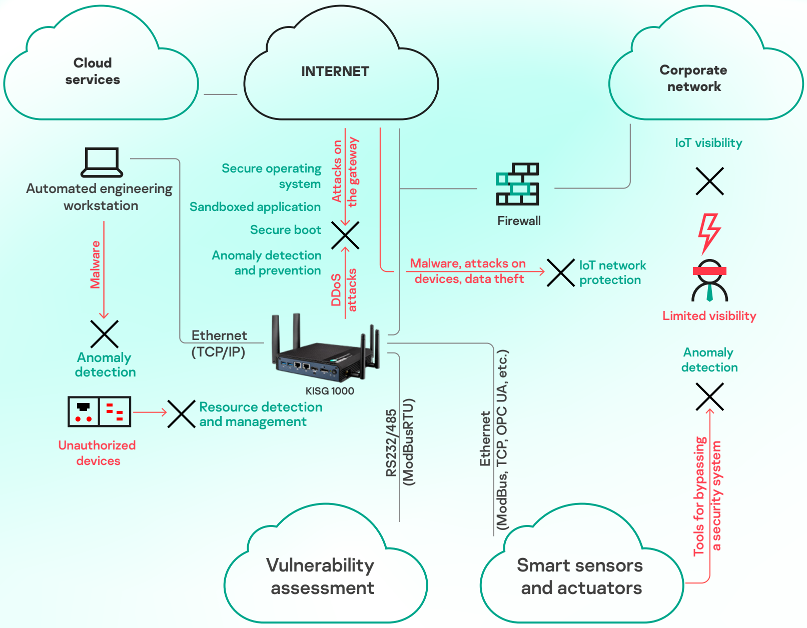
KISG 1000 has Cyber Immunity: OS-level security by design. It means that most types of cyberattacks will not be able to affect the critical functions of the gateway; that is, the device operates reliably even in an aggressive environment.

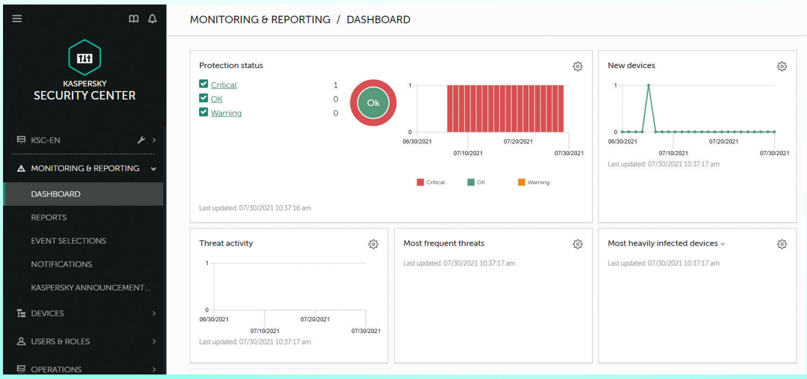
Protecting the IoT from cyberthreats

Kaspersky IoT Secure Gateway 1000 incorporates firewall features, as well as the Intrusion Detection and Prevention technology. It also provides secure transfer of data to public or private clouds.

Centralized management

Centralized monitoring and management of all the KISG 1000 events is provided by the Kaspersky Security Center platform. Together, the two products constitute the comprehensive Kaspersky IoT Infrastructure Security solution.





MONITORING & REPORTING / DASHBOARD

Protection status

☑ Critical 1
☑ OK 0
☑ Warning 0

Last updated: 07/30/2021 10:37:16 am

New devices

Last updated: 07/30/2021 10:37:17 am

Threat activity

Last updated: 07/30/2021 10:37:17 am

Most frequent threats

Last updated: 07/30/2021 10:37:17 am

Most heavily infected devices

Last updated: 07/30/2021 10:37:17 am

Kaspersky Security Center inteface

kaspersky

KasperskyOS

KISG 1000 specifications and capabilities

Specifications	
Processor	Intel Pentium N4200, 1.1GHz, 2MB L2 Cache
RAM	4GB, DDR3L, 1600MHz
Storage	SATA II SSD (32 GB)
Interfaces	2xGbE LAN, 2xMiniPCIe
Dimensions	128x152x37 mm
Operating temperature range	–20 to 60°C
Extras	3G/4G (optional)

Connection	
Ethernet	Two interfaces for connecting to different network segments via a twisted pair (LAN and WAN)
Cellular modem	Mobile data network as the primary or backup data channel
Routing and NAT	Automatic routing between KISG 1000 interfaces NAT managing (masquerading)
DHCP server	Automatic propagation of network configuration to IoT and other devices on the local network
MQTT broker	Mosquitto-based MQTT broker allowing centralized collection of data from IoT devices (sensors and actuators, smart relays, etc.)
OpenSSL/TLS	Support of common mechanisms for cryptographic protection of data transmitted via MQTT and Syslog protocols
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, etc. Works with any cloud systems using the MQTT protocol

Monitoring	
Detection and classification of devices	Detects devices on the local network by their network activity. The user interface can display all the network devices already communicating with KISG 1000, while new ones will be detected within 60 seconds
Reports and notifications (MQTT, Syslog, push notifications, Kaspersky Security Center)	The administrator can receive KISG 1000 security events in a single enterprise security management system (Kaspersky Security Center), and transmit events to external systems (SIEM, cloud platforms, etc.) using the Syslog and MQTT protocols. KISG 1000 supports integration with Google Firebase for sending push notifications to mobile devices

Flexible security and gateway management	
Web interface	User-friendly configuration and monitoring of the IoT network, visibility and transparency thanks to WebGUI. Informative dashboard allows you to get all the information you need quickly
Centralized management system	The Kaspersky Security Center platform allows managing events received from all KISG 1000 units deployed within the organization's infrastructure. It also allows tracking the status of gateways and managing their configuration

IoT gateway protection against cyberattacks	
Secure by design	The Cyber Immune KasperskyOS operating system rules out device compromise, thus making a data leak or penetration of the enterprise infrastructure impossible
Secure boot	Verification of the integrity and authenticity of gateway firmware using cryptographic methods before loading the image. Firmware that is damaged or altered without authorization will not be loaded
Secure update	Working in conjunction with secure boot, this technology allows updating the firmware with properly signed and encrypted images only

IoT infrastructure protection	
IDS/IPS and firewall	The firewall uses the principle of Default Deny. The administrator can rest assured that only allowed network interactions will pass through the gateway The IDS/IPS (Intrusion Detection and Prevention) module blocks malicious activity detected using a signature set prepared by Kaspersky specialists, and notifies the administrator

KasperskyOS

Kaspersky
IoT Secure
Gateway 1000

Learn more on os.kaspersky.com

www.kaspersky.com