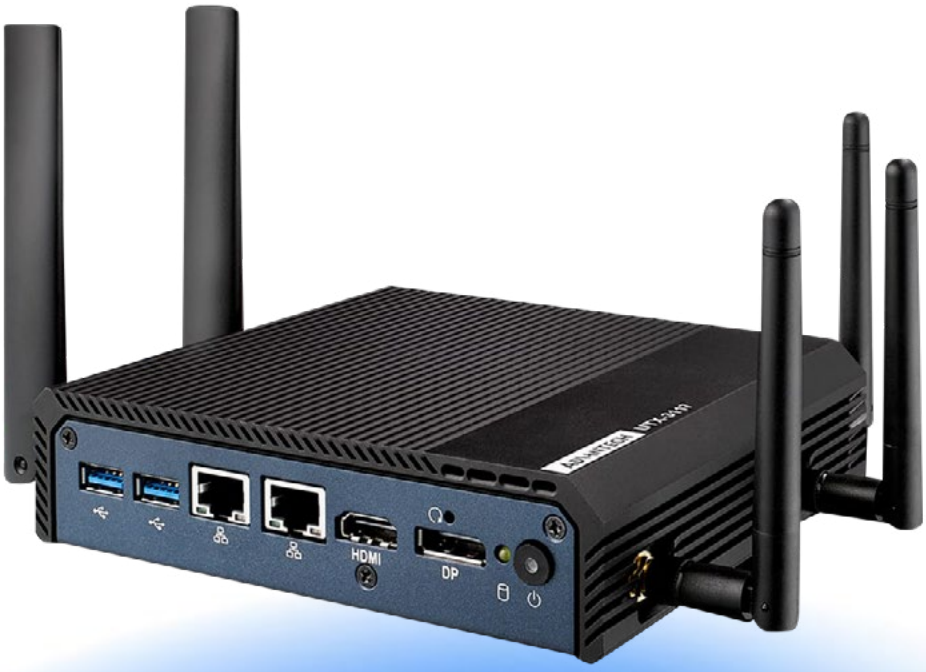
aprotech Kaspersky IoT company KasperskyOS Be Immune ADVANTECH

Kaspersky IoT

Secure Gateway 1000

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.

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



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. It can be used in industry, smart homes, CCTV and other fields.

Centralized management and web interface

The Kaspersky Security Center (KSC) administration console provides device management and allows you to monitor KISG 1000 events. Gateway configuration is also possible via the web interface.

KasperskyOS operating system	· All OS entities/domains are strictly isolated and therefore cannot affect 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 flexible configuration
Protocol	· MQTT. Secure TLS connection and data transmission between gateway and cloud platform
Connection to IoT platform	· Works with any cloud platforms using the MQTT protocol

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

Let's start your Cyber Immune digitalization together!

start@aprotech.ru
+7 495 970 71 17

www.aprotech.online

aprotech Kaspersky IoT company KasperskyOS Be Immune ADVANTECH

Hardware platform

Advantech UTX-3117 technical data

Technical data	
Processor type	Intel Pentium N4200, 1.1GHz, 2MB L2 Cache
Storage	SATA II SSD (32GB)
Type of memory	DDR3L, 1600MHz
RAM	4GB
Interfaces	2x100/1000 Mbps Ethernet RJ45
Additional communication device	3G/4G modem (optional)
Operating temperature range	From 0 to +55 °C
Storage temperature range	From -40 to +85 °C
Relative humidity	Operating: up to 95% at 40 °C (non-condensing)
Input voltage	12...24 V DC
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)
3G/4G modem	Ability to use the cellular 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 parameters to IoT and other devices operating 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 platforms using MQTT protocol
Monitoring	
Device detection and classification	Discovers devices 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, including unauthorized ones
Reports and notifications (MQTT, Syslog, KSC)	The administrator can receive KISG 1000 security events in the unified enterprise security management console – Kaspersky Security Center – as well as transfer events to third-party systems (SIEM, cloud platforms, etc.) via Syslog and MQTT protocols
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 console 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 penetrate 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