Kaspersky IoT
Secure Gateway 3.0

kaspersky aprotech Kaspersky IoT company

Kaspersky IoT Secure Gateway 3.0 supports two different operating modes:

Unidirectional gateway (data diode)

Router/firewall

Below are descriptions of the core capabilities of Kaspersky IoT Secure Gateway 3.0 when operating in each mode, and the shared capabilities of both operating modes.

Core specifications of Kaspersky IoT Secure Gateway 3.0 when operating as a unidirectional gateway

Unidirectional data transport

Ethernet, 3G/LTE. The gateway ensures unidirectional transfer of data via Ethernet and 3G/LTE networks, thereby enabling reliable transmission of data from industrial equipment to cloud platforms. This configuration enhances system security by preventing reverse data streams and cyberthreats.

Unidirectional data transport

- **DHCP server.** The built-in DHCP server automates the process of assigning IP addresses and other network settings, which simplifies network management and reduces the likelihood of configuration errors.

Connect to cloud services via third-party applications. The gateway lets you connect to various cloud services, thereby ensuring flexibility and scalability when transmitting data from industrial equipment to cloud platforms for subsequent data processing and analysis. Applications are available on the Kaspersky Appicenter™ platform.

Security

- **Encrypted TLS channel.** The gateway encrypts data when it is transferred over a network using the TLS protocol, ensuring that information is protected from interception or unauthorized access.

VPN client. The device supports the installation of third-party VPN clients, which ensures a secure connection with remote networks and servers and enhances the security of data when transmitted over the internet.

— application is available in Kaspersky Appicenter

Core specifications of Kaspersky IoT Secure Gateway 3.0

when operating as a router/firewall

Bidirectional data transport

Ethernet, 3G/LTE. The gateway ensures bidirectional transmission of data over Ethernet and 3G/LTE networks, enabling flexible connections to various networks and adaptability to varying connectivity conditions. This makes the device ideal for use in industrial or other sectors that require reliable and fast data transfer.

Network functions

- **Routing.** The gateway supports routing functions that enable effective management of network streams and reliable transfer of data between various network segments. This helps improve network performance and manageability.
- **NAT and Port Forwarding.** Support for NAT and port forwarding lets you conceal internal IP addresses and manage access to network resources. This functionality improves network security and provides flexible management of network connections.
- **VRRP clustering.** Support for clustering via VRRP (Visual Router Redundancy Protocol) ensures high availability and fault tolerance of the network, minimizing downtime and data loss.
- **DHCP server.** The built-in DHCP server automates the process of assigning IP addresses and other network settings, simplifying network management and reducing the likelihood of configuration errors.
- **MQTT broker.** Support for an MQTT broker lets you effectively manage publication and subscriptions to data in IoT networks and ensure quick and reliable transfer of messages between devices.

Security

- **Firewall (Default Deny).** The Default Deny firewall policy ensures a high level of security by blocking all unauthorized connections and preventing unauthorized access.
- **Filter (block) traffic of application protocols.** Deep Packet Inspection (DPI) functionality lets you filter and block traffic of application-layer protocols (FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3) to improve control over network traffic and prevent potential threats.
- **Additional firewall functionality.** This functionality was implemented using the Network Protector application that is available in Kaspersky Appicenter.
  - **Firewall at the industrial network level.** Kaspersky IoT Secure Gateway 3.0 supports control and filtering of industrial protocols (MQTT, Modbus, BACnet, DNP3, MMS, OMRON-FINS, ENIP/CIP, TriStation, S7comm), ensuring protection of critical infrastructure against cyberthreats.
  - **Analysis of industrial protocols with intrusion prevention and detection functionality** provides active network protection against attacks and guarantees data security.
- **Integration with SIEM.** Integration with security information and event management (SIEM) systems ensures centralized monitoring and analysis of security events, enhancing general awareness about the state of the network and accelerating responses to incidents.

— application is available in Kaspersky Appicenter

General specifications for both operating modes of Kaspersky IoT Secure Gateway 3.0

Flexible gateway management

- **Centralized management.** Kaspersky IoT Secure Gateway 3.0 can be centrally managed through Kaspersky Security Center (KSC), which lets you easily and efficiently configure, monitor and manage devices from a single console. This simplifies administration and improves control over the network.
- **Web interface.** The convenient web interface of Kaspersky IoT Secure Gateway 3.0 provides direct access to device configuration and management from the LAN using a web browser. Access to the web interface is protected by TLS certificates.
- **Role-based access control (User and Administrator).** The gateway supports role-based access control, which lets you restrict the rights of users and administrators. This ensures secure access to device configuration and functionality, and prevents unauthorized changes.
- **Support for third-party applications.** The gateway can use third-party applications that are available on the Kaspersky Appicenter platform. For example, you can use applications designed to work with the OPC UA and Modbus TCP protocols (for receiving data) and the MQTT Publisher protocol (for sending data to a cloud platform). These applications ensure efficient and reliable conversion of data between protocols, simplifying integration and interaction of devices in an IoT network.
- **Management of third-party applications.** Irrespective of your specific approach to device management, Kaspersky Appicenter functionality lets you find, install, update and remove applications in any interface.

Gateway protection against cyberattacks

- **Cyber Immunity (Secure by Design).** The gateway was developed based on the principles of Cyber Immunity, which means it has built-in protection against vulnerabilities and cyberattacks that was incorporated at the development stage. This significantly reduces the risk of successful attacks and enhances device reliability.
- **Secure boot.** The gateway's secure boot functionality ensures that the authenticity and integrity of software is verified at startup, thereby preventing unauthorized and potentially malicious applications from being loaded.
- **Secure update.** The gateway supports the secure update of software, which lets you reliably update the system while minimizing the risk of installing illegitimate or compromised updates. This helps keep the device up to date and secure during its entire service life.