Cybersecurity of IoT video surveillance systems

kaspersky

KasperskyOS

According to expert forecasts, by 2022 there will be more than 45 billion video surveillance cameras throughout the world, and most of them will be smart cameras. The capabilities of such cameras make them attractive not only to regular users but also to cybercriminals.

State-of-the-art video surveillance cameras provide multiple ways to connect to wired or wireless data networks. Thanks to their capabilities for recognizing faces, counting people, creating thermal maps, and detecting motion, these smart cameras can also identify the behavior and identity of a person, read vehicle license plates, and much more.

However, security researchers regularly find numerous vulnerabilities in smart cameras. Cybercriminals can exploit these vulnerabilities to spy on the camera owners, manipulate the overall security of networks, or even impact an entire corporate infrastructure.

The importance of cybersecurity

State-of-the-art video cameras are extremely smart and highly functional devices that are also vulnerable to hacker attacks just as other internet of things devices. For example, in 2019 researchers showed that the Mirai worm, which combined its infected devices into botnets, most often attacked cameras and routers. In 2021, hackers compromised 150 thousand video surveillance cameras in the U.S., U.K., and China. Some of these cameras were even installed in schools, hospitals, police departments and prisons. The cybercriminals were able to gain access not only to the cameras but also to entire video archives of these organizations.

Local video surveillance systems

In local video surveillance systems, the greatest risk is any potential physical connection to the system through the camera directly at the facility.

Video surveillance cameras are not normally designed for security mechanisms to be installed directly on them. This means that a camera is normally not protected against the following:

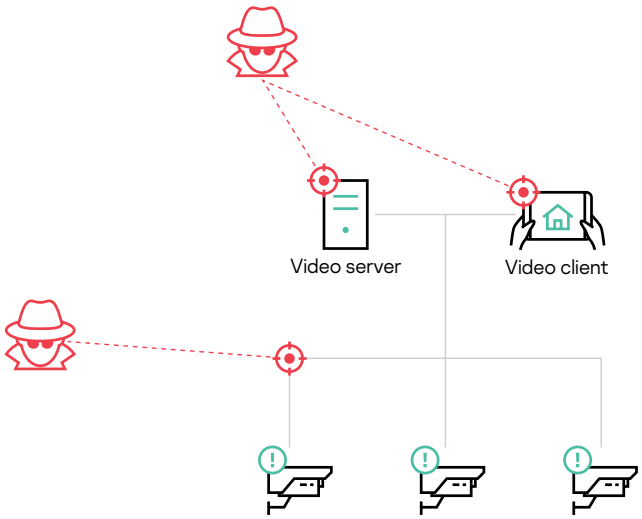
- Unauthorized connection
- Exploits and other malware
- Network attacks
- No visibility of activity on the local network.

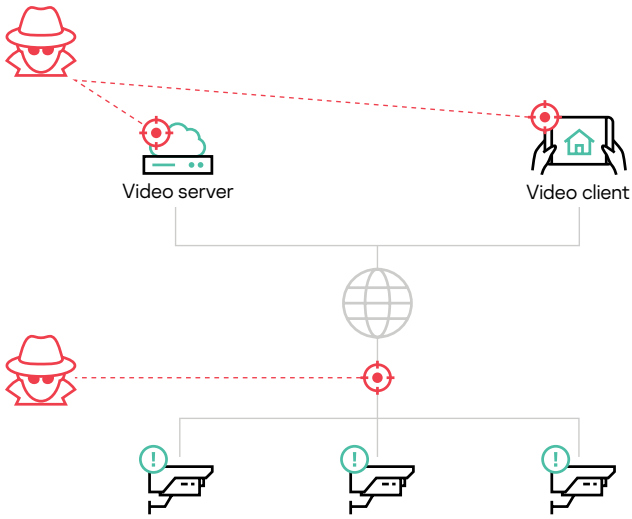
Cloud-based video surveillance systems

The main risks for cloud-based video surveillance systems are caused by their internet connection. This connection is used to transmit the video stream from cameras to a video server, and this is when the data is most vulnerable.

If hackers gain access to a video surveillance system through the internet, they can do the following:

- Exploit vulnerabilities
- Conduct network attacks, including DDoS attacks
- Intercept the video stream
- Infect the system with malware





A video server and video client are vulnerable to the same threats as any other device running Windows or Linux

Potential security threats in video surveillance systems

- Video archives and databases:
  - Unauthorized access
  - Compromise (hacking, gaining access, modifying configurations, data spoofing/leakage)
- Communication channels:
  - Failure
  - Unstable data transfer (not directly related to malicious interference)
  - Man-in-the-Middle (gaining access, capturing and spoofing data)
  - DDoS (channel inaccessibility)
- Cameras:
  - Firmware reflash
  - Modified configuration
  - Password change
  - SSL certificate spoofing
  - Malware installation
  - Unauthorized connection

Solution

To secure the IoT infrastructure of video surveillance systems, Kaspersky is offering a solution called Kaspersky IoT Infrastructure Security whose key component is **Kaspersky IoT Secure Gateway (KISG) 1000 β*** based on the KasperskyOS operating system. KISG 1000 runs on the Advantech UTX-3117 hardware platform, is managed by **Kaspersky Security Center**, and has functions for monitoring and protecting against cyberattacks. This comprehensive solution helps maintain the security of systems, track their state and manage events from a single center.

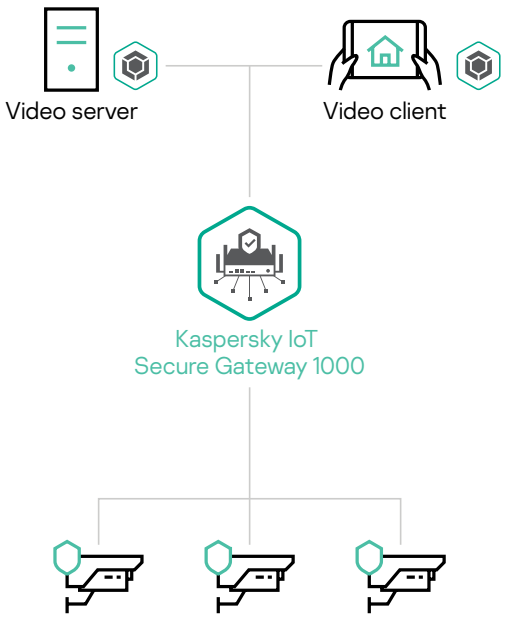
Kaspersky IoT Secure Gateway 1000 lets you restrict access between cameras and the video server in local video surveillance systems, and lets you protect the perimeter of cloud-based systems against threats from the internet.

Functions of KISG 1000:

- Blocks all unauthorized interactions between the video server and cameras.
- Blocks any attempts to attack cameras from a video server or video client.
- Generates a list of cameras and provides notifications about any appearance of an unauthorized device on the local network (which could also indicate that a camera has been replaced).
- Provides a notification if a camera is disabled.

* The current version of the product is intended for non-commercial piloting

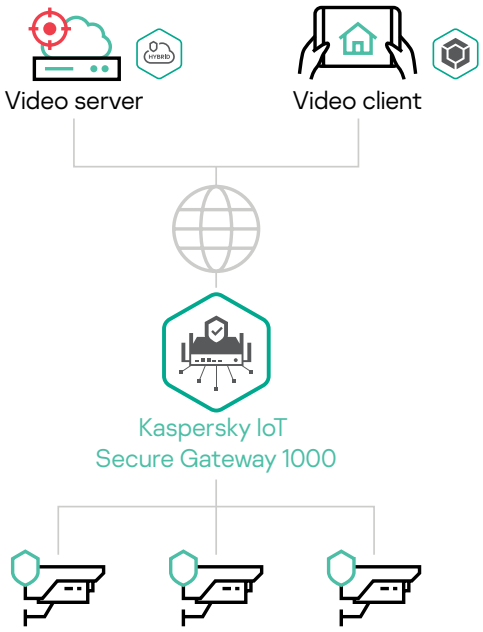
Local video surveillance systems



Kaspersky Total Security for Business secures the video server and video client.

Kaspersky IoT Secure Gateway 1000 protects the video server against potential threats coming from cameras, and protects cameras against potential threats coming from the video server and the video client.

Cloud-based video surveillance systems



Kaspersky Total Security for Business secures the video client.

Kaspersky Hybrid Cloud Security protects video servers residing in the cloud.

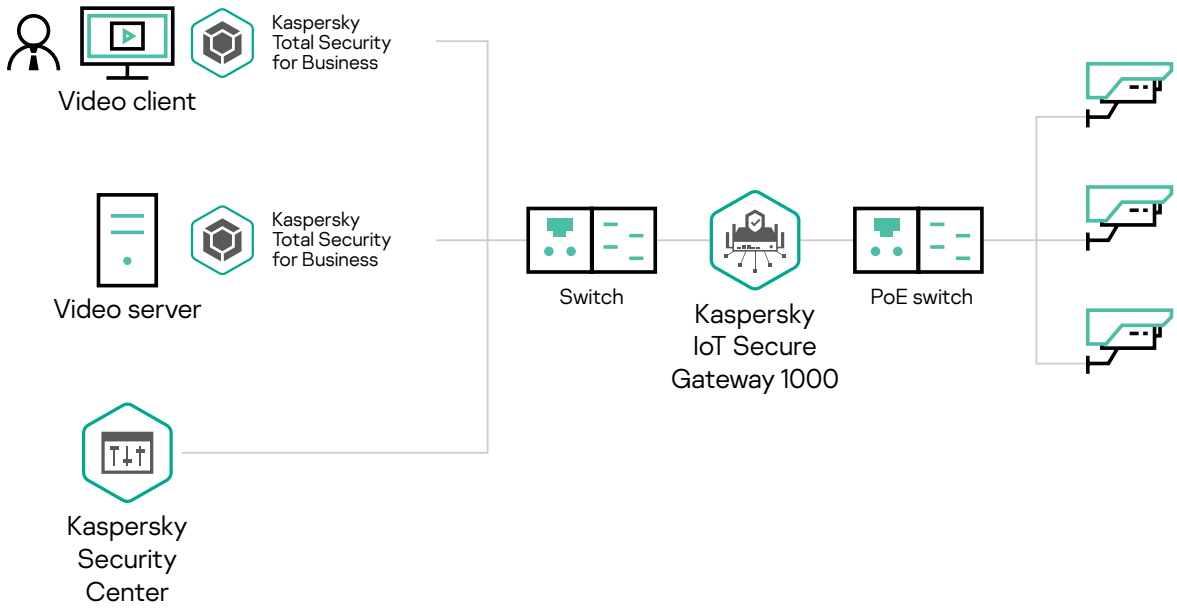
Kaspersky IoT Secure Gateway 1000 protects the video server against potential threats coming from cameras, and protects cameras against potential threats coming from the video server, video client and the internet.

Result

Cybersecurity of video surveillance systems is a task that requires a comprehensive approach. Protection of all architectural components of a video surveillance system (cameras, IoT gateways, video server and video client) reduces the capability of cybercriminals to exploit potential vulnerabilities.

The Kaspersky approach to protecting **local video surveillance systems** includes the following:

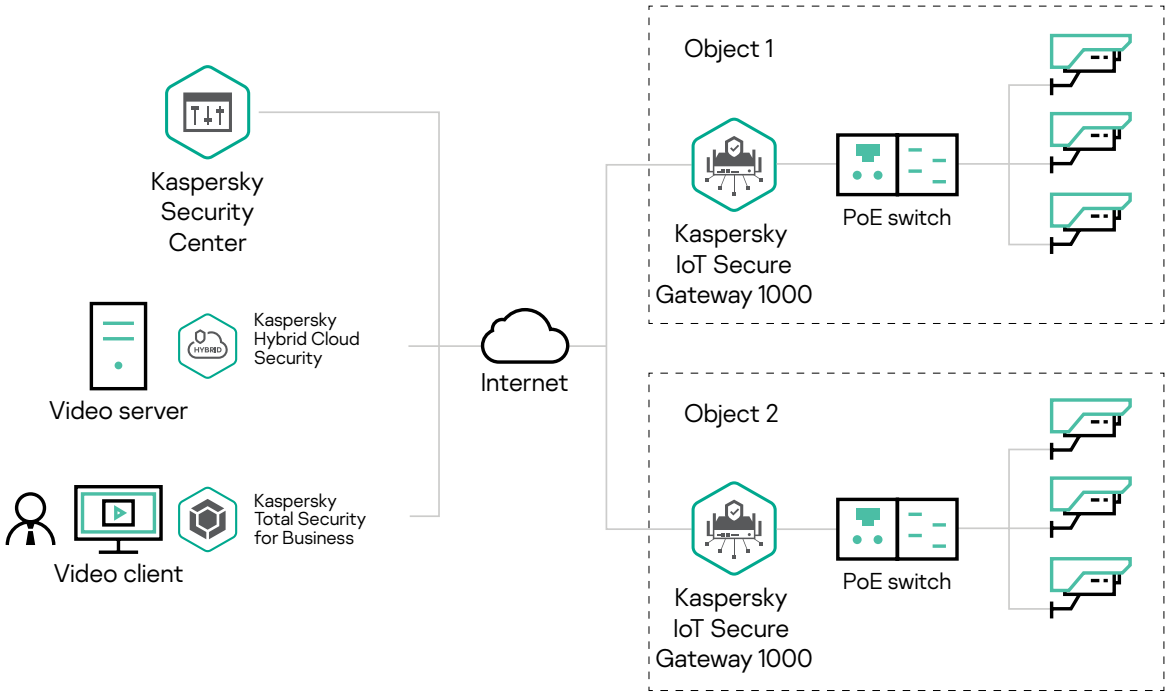
- Kaspersky IoT Infrastructure Security:
  - Kaspersky IoT Secure Gateway 1000
  - Kaspersky Security Center
- Kaspersky Total Security for Business



Levels	Threat vectors	Kaspersky products and solutions
Management of the video surveillance system infrastructure	• Difficulty monitoring IoT infrastructure security (lack of a comprehensive picture of the security situation in real time) • Delayed response to information security incidents (late notification/detection of a problem)	Kaspersky Security Center
Data transmission channel	• Man-in-the-Middle (gaining access to data and substituting it)	Kaspersky IoT Secure Gateway 1000
Gateway	• Network attacks on publicly available devices (devices with a public address or that have been set up for access from public networks)	
Cameras	• Network attacks on connected devices (hacking passwords, gaining access, modifying software configurations, data spoofing/leakage) • New unauthorized connections to the network (a cybercriminal connects additional devices and turns them on instead of cameras)	

Kaspersky's comprehensive approach to protecting **cloud-based video surveillance systems** includes the following:

- Kaspersky IoT Infrastructure Security:
  - Kaspersky IoT Secure Gateway 1000
  - Kaspersky Security Center
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky DDoS Protection



Levels	Threat vectors	Kaspersky products and solutions
Management of the video surveillance system infrastructure	• Difficulty monitoring IoT infrastructure security (lack of a comprehensive picture of the security situation in real time) • Delayed response to information security incidents (late notification/detection of a problem)	Kaspersky Security Center
Cloud	• DDoS attacks (service unavailability) • Compromised video surveillance platform (hacking, gaining access, modifying configurations, data spoofing/leakage)	Kaspersky DDoS Protection Kaspersky Hybrid Cloud Security
Data transmission channel	• DDoS attacks (channel inaccessibility) • Man-in-the-Middle (gaining access to data and substituting it)	Kaspersky DDoS Protection Kaspersky IoT Secure Gateway 1000
Gateway	• Network attacks on publicly available devices (devices with a public address or that have been set up for access from public networks)	
Cameras	• Network attacks on connected devices (hacking passwords, gaining access, modifying software configurations, data spoofing/leakage) • New unauthorized connections to the network (a cybercriminal connects additional devices and turns them on instead of cameras)	

Kaspersky's comprehensive approach to protecting local and cloud-based video surveillance systems provides the capabilities to protect video cameras, cloud platforms and IoT devices, and monitor their security from a single console.
The KasperskyOS-based Kaspersky IoT Secure Gateway 1000 serves as the ultimate security gatekeeper for your network at its frontiers, while Kaspersky Security Center helps you centrally configure your gateways and manage their events.

KasperskyOS

Kaspersky
IoT Infrastructure
Security

Learn more on os.kaspersky.com

www.kaspersky.com