Kaspersky IoT Security

KASPERSKY lab

KasperskyOS®

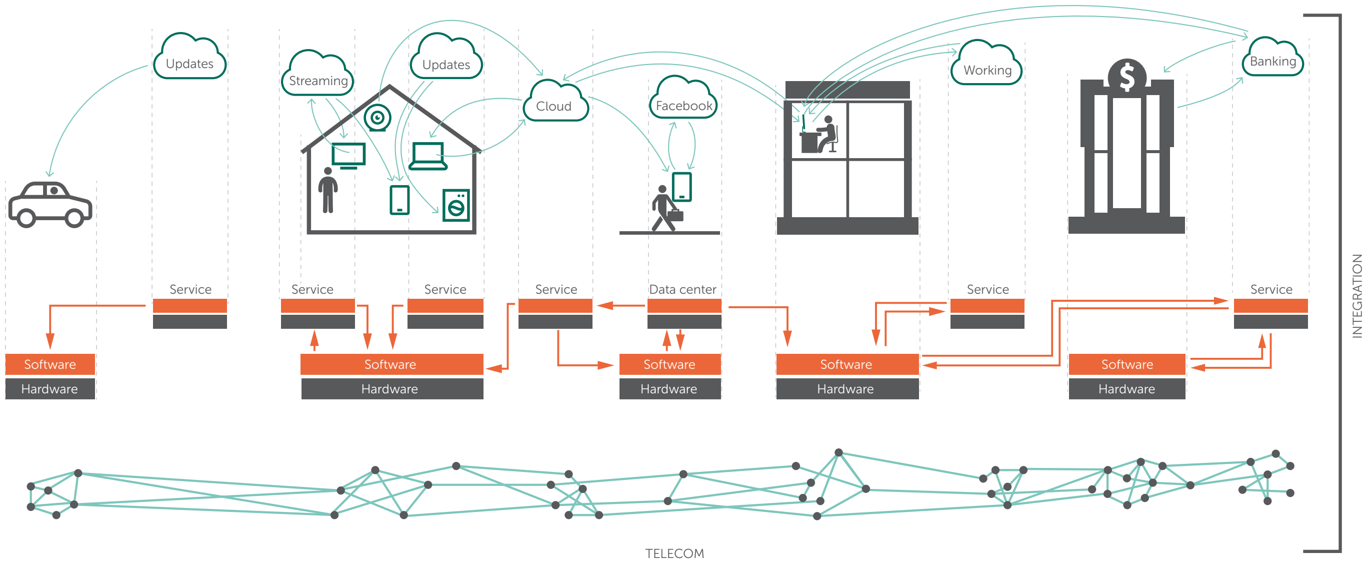
Kaspersky IoT Security

Customers of IoT solutions not only want their connected devices and services to function stably – they want them to be secure.

Developing the internet of things – security as a priority

Solution security has traditionally been associated with the security of personal data. In the IoT era, however, it has transformed into the security of privacy. Violations of user privacy such as remote surveillance via smart home cameras, multimedia or baby monitors; interference in the functioning of household devices; unexpected shutdowns and the failure of everyday services that are normally available – all of this is unacceptable to the end user.

At the same time, the internet of things provides tremendous opportunities for device manufacturing (including hardware components and software), telecom services and the integration market. A lack of trust in IoT solutions among end users could block or significantly slow down the realization of these capabilities. That's why end-to-end security of IoT solutions is the main priority for all those involved.



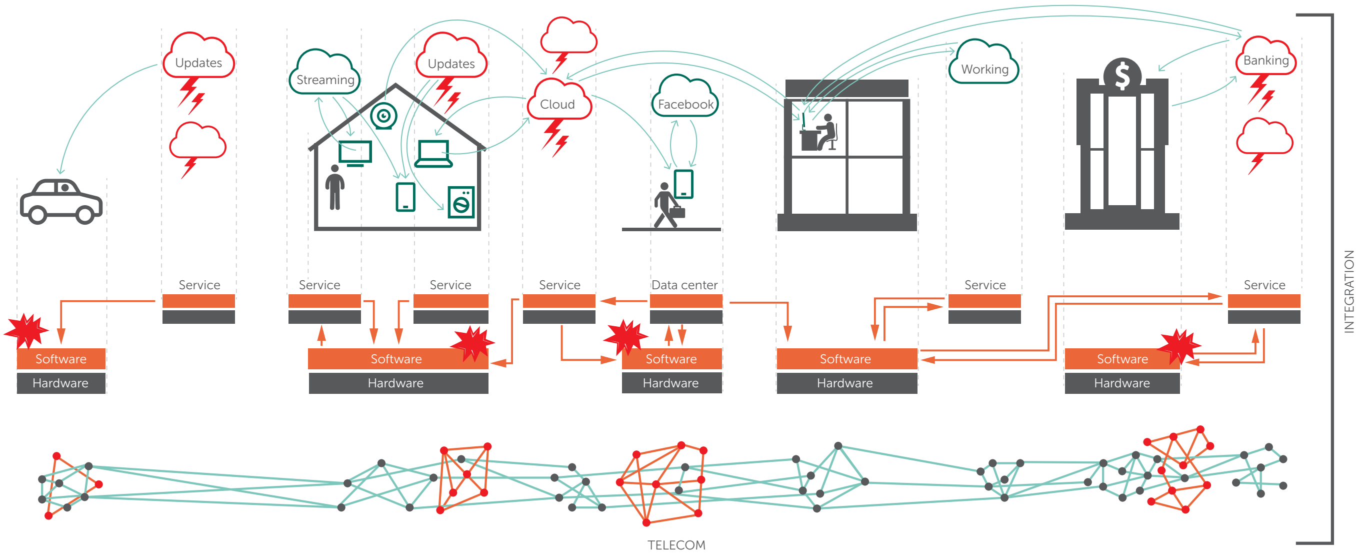
Home users presume their TV is only connected to the servers of their service provider – for example a digital TV or a streaming video provider. However, in reality a device connects to dozens of servers for the transfer of telemetry data, voice processing, receiving updates, etc.

What threatens the internet of things

At the end of 2016, the home routers of a European telecom provider were successfully attacked by a specially developed version of the Mirai worm. It turned all the compromised devices into an army of bots that later participated in massive DDoS attacks[1].

After analyzing this incident we came to the conclusion that the users had no idea their household devices had been compromised and were part of an enormous botnet. They also didn't know about the network activity of their connected devices such as TV sets, baby monitors, washing machines and so on.

The complexity of the infrastructure for providing IoT services presents a number of opportunities for carrying out a variety of attacks. It's easy to hide data sent by an intruder among a large number of network requests. It's always possible to find a vulnerable function among the huge number of those executed by a device or a service.



Strange as it may seem, the main source of threats to the internet of things is the IoT itself – its infrastructure and technological complexity combined with the speed at which it's developing.

In many cases, the manufacturers of IoT edge devices and telecom equipment ignore the main principles of cybersecurity. The hardware doesn't control the integrity of the firmware, devices are shipped with preinstalled passwords, including administrator passwords, not to mention weak network security settings or the use of old and vulnerable software versions. Moreover, a software update process is not always provided, meaning vulnerable devices can work for years without updates. It's just a matter of time before such devices are successfully attacked.

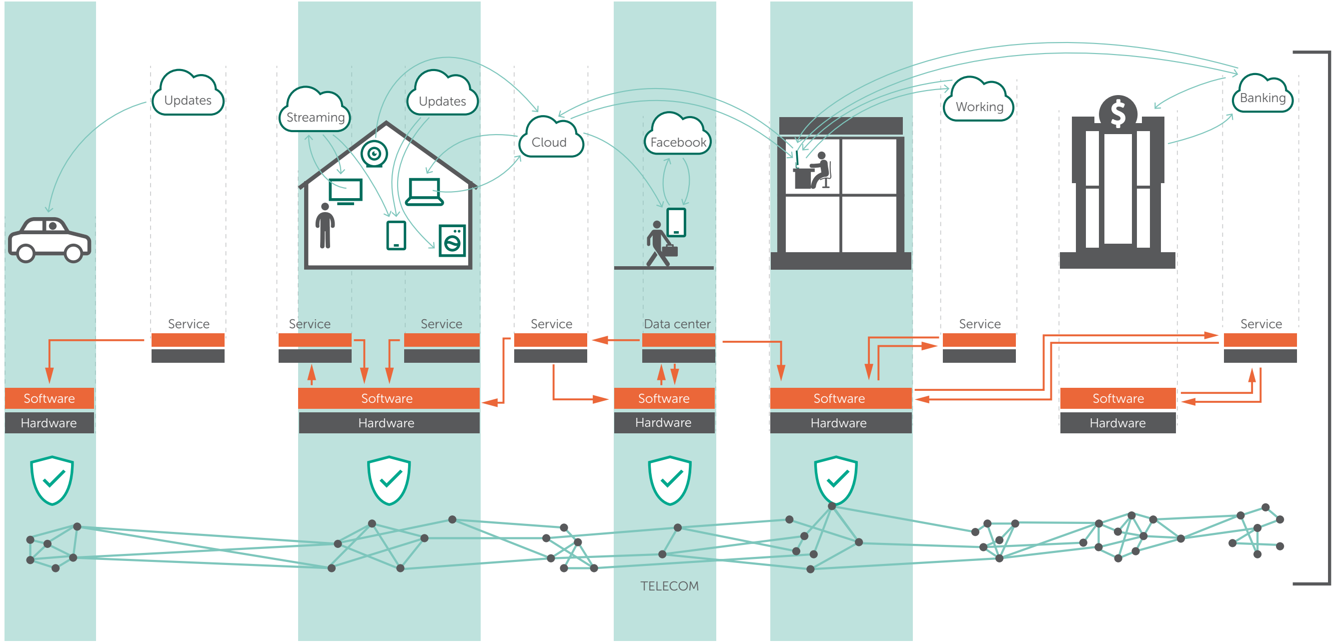
Who's responsible for protecting the IoT

To ensure security on the IoT, it's necessary to combine the forces of several parties:

- Edge device manufacturers;
- Telecom device manufacturers;
- IoT core equipment and telecom device suppliers;
- Telecom providers;
- IoT application service providers;
- System integrators working in the field of IoT and connected devices.

Due to their business needs, all these parties are interested in the secure and predictable behavior of edge devices. The greater the attention to quality and the more reliable the solutions and services are in the eyes of customers, the better the implementation of this behavior.

[1] https://securelist.com/ddos-attacks-in-q4-2016/77412/



What guarantees are there to ensure trust on the internet of things?

This trust is based on guarantees that a supplier – the manufacturer of part or all of a solution, or an integrator – is making an effort to avoid malfunctions and mitigate attacks on IoT infrastructure in their area of responsibility. This sort of supplier has a reliable reputation that allows them to retain and consolidate the relevant part of the market for IoT solutions and integration services.

Trusted IoT

Guarantees of trust on the device level

The principle of a chain of trust forms the basis for guarantees of secure IoT device functioning, including edge devices and infrastructure elements (gateways). This principle begins with the use of a root of trust on the hardware level that ensures the secure boot of an operating system.

This technology carries out a trusted boot of an operating system, including the integrity of OS image checking, applying cryptography and mechanisms of hardware-assisted secure storage for key information. Trusted boot is crucial for key IoT infrastructure devices such as gateways, ensuring the operating system is booted from predefined media and only after the equipment has successfully passed special integrity checks.

The next important element in the chain of trust is a secure operating system capable of ensuring the proper execution of software that is not considered to be trusted. Modern developments in computer technology make it possible to implement an environment on the OS level that restricts the behavior of applications that cannot be considered trusted.

If an application violates the limits of the preconfigured behavior, its execution will be restricted – something that is not always acceptable. To avoid this, the developers of applications and services, being interested parties, tend to avoid unforeseen behavior by program code where possible. As a result, secure applications become the final element of the root of trust. Their development should take into account secure coding practices to prevent malfunctioning on the scenario level and implement additional security services.

Because the internet of things represents a complex heterogeneous environment where devices of varying levels of trust interact with one another, the cumulative security of this environment can be breached by compromised or untrusted components.

Guarantees of trust on the infrastructure level

To increase the level of trust in an internet-of-things infrastructure, it is necessary to apply a set of technologies enabling detection, isolation and denial of malware content.

At the current time the following list of technologies are key:

- Managing security updates helps strengthen untrusted edge components. Secure updates have to be implemented securely, meaning updates should be downloaded from a trusted source, they should be tested and shouldn't damage the device or its virtual and physical environment.
- Detection and blocking of malicious code on infrastructure and edge components of the internet of things helps stop random attacks like ransomware, as well as targeted attacks using malicious software to penetrate the target system and become part of it.
- Content filtering, behavior analysis and advanced exploit prevention makes it possible to monitor and block popular attack vectors targeting edge components.
- Technologies for detecting and preventing network attacks (IDS/IPS) based on signature detection and anomaly analysis make it possible to analyze a situation on the communication channel level and protect the entire network infrastructure.
- Anti-DDoS technologies ensure the continuity of business processes and continuous functioning of the internet of things' online resources and services at the infrastructural level.
- Proactive threat protection based on cloud technologies makes it possible to stay one step ahead of the attackers, automatically neutralizing attacks that have just started to spread on the internet or local networks.
- Security of cloud infrastructure.
- Artificial intelligence, including machine learning as an obligatory attribute that helps handle the growing volume of data.

Best expertise

- Unique team of more than 40 world-leading security experts in place in all regions
- Expert support for industry groups, national and global organizations and customers
- World's leading team of recognized anti-malware experts, globally and locally
- Focused on fighting cybercrime by exposing, analyzing and neutralizing IT threats

Kaspersky Lab solutions to ensure trust in the internet of things

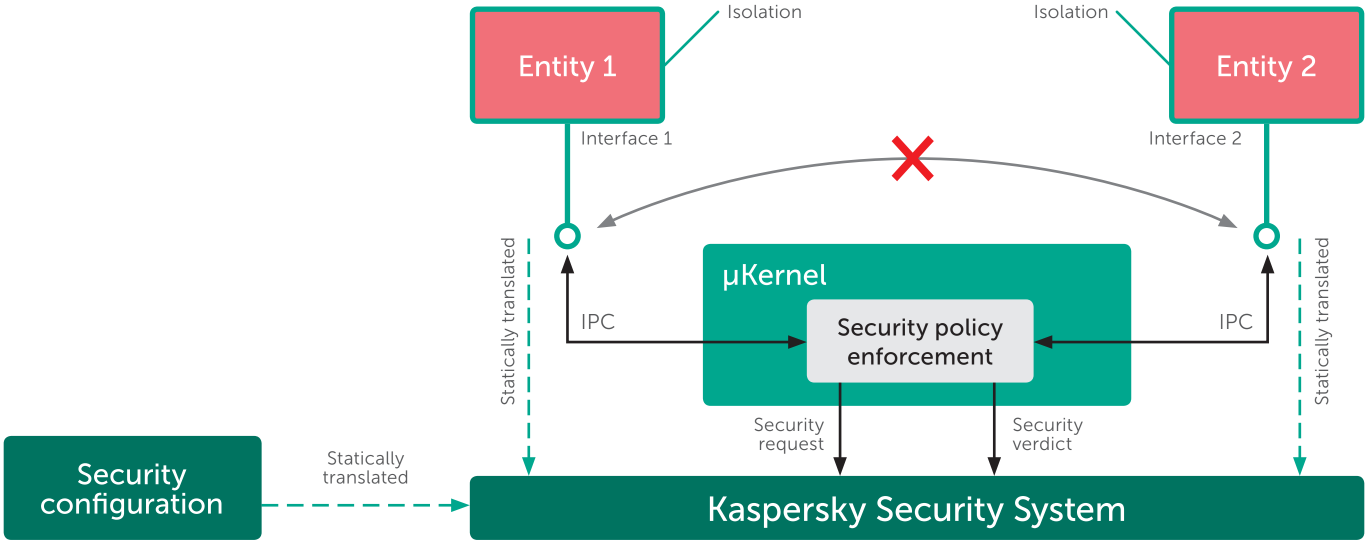
Unique trusted technologies

KasperskyOS

Every day thousands of devices are exposed to malicious code, viruses and hacker attacks. And we don't care about it until it becomes a threat to our devices, or even to our health. In order to protect software and data systems from such threats and to reduce the risk of harm caused by program bugs, unintentional mistakes or premeditated abuse, we recommend KasperskyOS, a secure operating system for embedded connected devices with specific cybersecurity requirements. KasperskyOS creates an environment where a vulnerability or bad code is no longer a big deal. The Kaspersky Security System (KSS) protection component controls interactions across the whole system, rendering the exploitation of vulnerabilities useless.

Kaspersky Security System

Kaspersky Security System is a security policy verdict computation engine capable of working simultaneously with different types of security policies (role-based and mandatory access control, temporal logic, control flow, type enforcement, etc.) and can be customized to meet a client's needs. The more precise the policies, the more control and security afforded the entire system. KSS can be used together with KasperskyOS (the most secure configuration) as well as in a Linux-based solution (secure actions in an unsecure system).



Kaspersky Secure Hypervisor

Kaspersky Secure Hypervisor runs on the KasperskyOS microkernel. With KSH, potentially untrusted virtualized guest operating systems can be separated from each other and all communications between them can be controlled and trusted, even though they are physically running on the same hardware platform. An additional benefit of KSH is its ability to reduce expenses on hardware maintenance.

Kaspersky Security Network and Kaspersky Private Security Network

Kaspersky Security Network is a global system created by Kaspersky Lab. KSN contains data about all threats and provides it in real-time mode for protection from cyberthreats and the investigation of all types of incidents.

Kaspersky Private Security Network is a local reputation database that can be installed and used under the customer's full control. The internal IT infrastructure and Security Operations Center benefit from all the advantages of cloud technologies, allowing the customer to meet all the requirements of regulatory authorities by preventing any data from leaving the protected perimeter.

Traditional anti-malware solutions require up to four hours to detect and block malicious software; Kaspersky Private Security Network does so in less than a minute without transferring customer data outside the local network. The very latest analytical technologies allow the solution to detect threats and react to them accordingly.

Multifunctional security framework for IoT gateways

Our solution ensures infrastructure control and the quickest possible reaction to vulnerability detection using our patented technologies and cloud services that help deal with threats before official patches are released.

The IoT infrastructure provider receives information about the types of controlled devices, number of uncontrolled devices, if any, and geolocation information about devices.

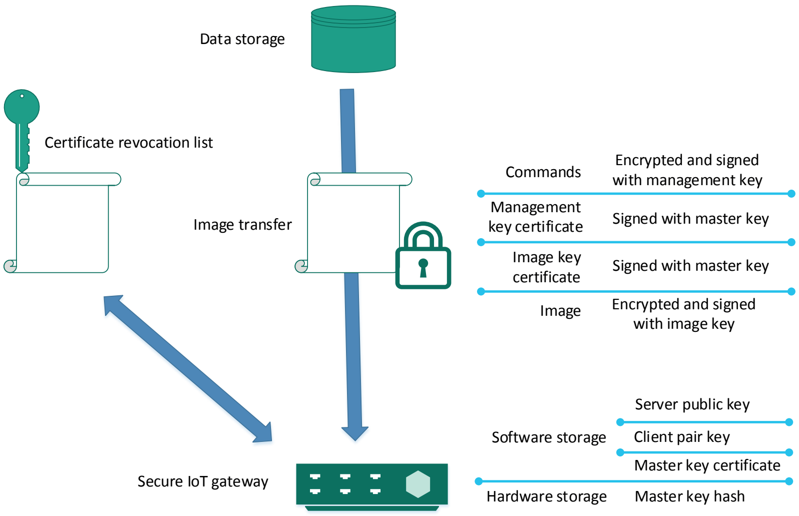
The solution includes lifecycle management for software embedded on devices and provides information about its security, number of vulnerabilities detected and ability to update to previously tested or fully examined versions. It's also possible to flexibly manage firmware and program module updates at the request of the end user or via forced update.

Another important component provides multifunctional monitoring to track events that take place in the system.

One of the priorities of our solution is to reduce the costs of managing IoT infrastructure for customers and services. Kaspersky Lab takes responsibility for maintaining the controlled network and devices in a secure state.

Secure boot

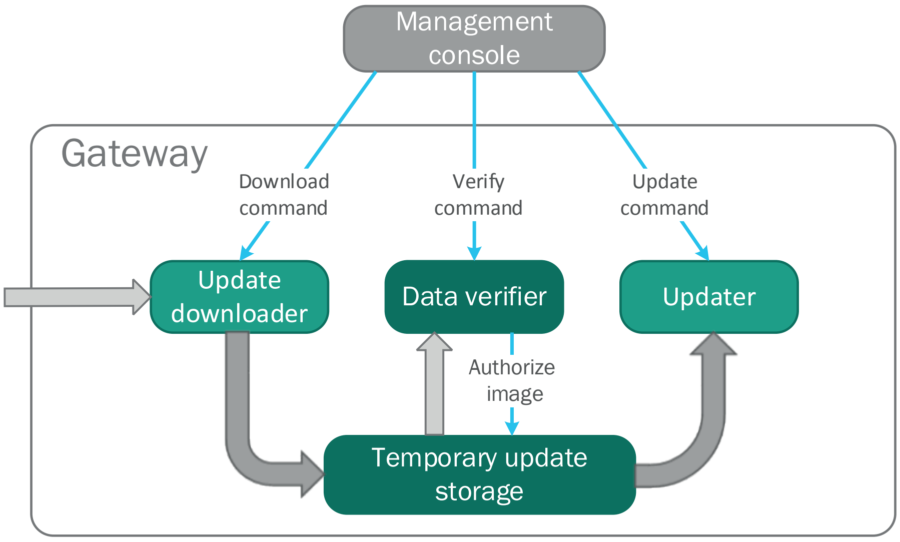
As mentioned above, a secure boot is a basic security technology for embedded systems – the root of trust begins with a secure boot. A secure boot makes it possible to decrypt and check the digital signature of an image of the OS itself (OS core and file systems) and its loaders, and guarantees that an operating system that is damaged or modified by an attacker is not booted.



Secure update

The secure update of embedded devices is one of the most important services provided by the Kaspersky IoT framework.

Kaspersky Secure Updater is a technology that ensures two important elements of the secure software update. Firstly, it guarantees that an update isn't compromised and wasn't modified during the transfer. This is done using different cryptography methods. Secondly, the component ensures the update process makes minimal use of trusted code, significantly reducing the attack surface. The security of most of the Updater is not that important because if these pieces of code are compromised, an attacker is still unable to bypass the updater and secure boot security mechanisms and replace the firmware with malware.



Secure audit

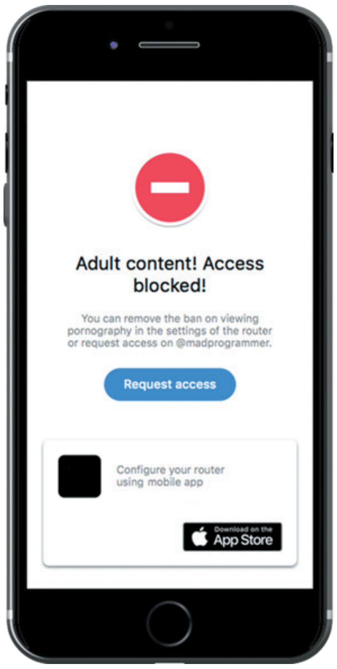
Kaspersky Secure Audit is another important technology that saves security events in a special storage that uses blockchain mechanisms to guarantee the log's integrity and authenticity. If the log is falsified, the operator can determine unequivocally what part of the log was modified and when the modification took place.

IoT device management

IoT Device Management is a system that unifies different components and manages the entire lifecycle of program modules inside the IoT framework, including the secure update, secure boot and vulnerability assessment.

Cybersecurity technologies

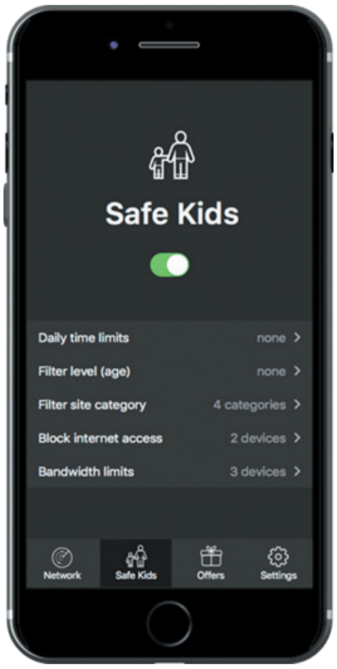
A significant part of our solution is made up of familiar, proven cybersecurity technologies such as the antivirus scanner, firewall, intrusion detection and prevention systems, various content filtering technologies (e.g., parental control and anti-phishing).



Adult content! Access blocked!

You can remove the ban on viewing pornography in the settings of the router or request access on @madprogrammer.

Configure your router using mobile app

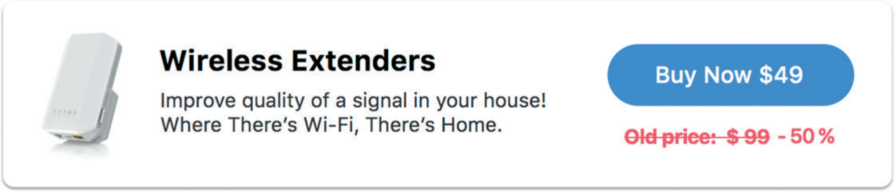


Safe Kids

Daily time limits	none
Filter level (age)	none
Filter site category	4 categories
Block internet access	2 devices
Bandwidth limits	3 devices

Built-in prompts and upselling

Along with the aforementioned cybersecurity technologies, we propose built-in prompts and upselling. Unlike other similar technologies, our approach is based on behavior analysis which helps propose goods and services at the very moment the user needs it. For example, if a user has a weak signal from an internet access point, they see a proposal to buy a wireless extender.



Wireless Extenders

Improve quality of a signal in your house!
Where There's Wi-Fi, There's Home.

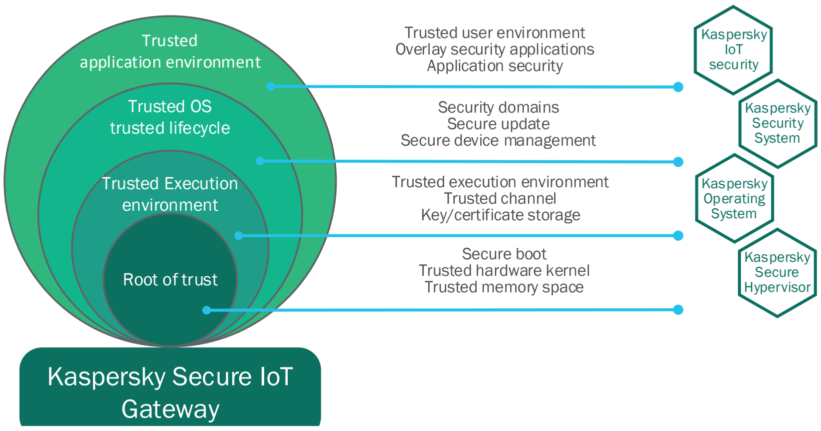
~~Old price: $ 99~~ - 50 %

Architecture of trust

The architecture of trust in the internet of things is based on the gateway – an infrastructure solution that maintains a predefined level of guarantees in relation to the behavior of the controlled area.

Kaspersky Lab offers Kaspersky Secure IoT Gateway, with a qualitatively different approach to ensure infrastructure security for the internet of things. As well as the best technologies for infrastructure security, it implements trusted technologies that guarantee the secure behavior of the gateway itself

Nowadays the market offers numerous gateways that are described as “secure” or “trusted”. These devices provide a wide range of technologies to protect against cyberthreats: antivirus scanners, traffic checking, firewalls, etc. It is important to understand that these technologies are made to protect devices that are connected to the gateway. But who is going to secure the gateway itself? If it’s compromised, all the accompanying security technologies can be deactivated.


Trusted application environment
Trusted OS trusted lifecycle
Trusted Execution environment
Root of trust
Kaspersky Secure IoT Gateway
Trusted user environment
Overlay security applications
Application security
Security domains
Secure update
Secure device management
Trusted execution environment
Trusted channel
Key/certificate storage
Secure boot
Trusted hardware kernel
Trusted memory space
Kaspersky IoT security
Kaspersky Security System
Kaspersky Operating System
Kaspersky Secure Hypervisor

Kaspersky Lab’s solution is designed to embed security modules and technologies in device firmware and can be used to protect devices with varying degrees of customization.

This approach is based on a chain of trust. The initial point of trust is chosen depending on the level of guarantees required, and in the most extreme cases is set at the hardware level. However, this is not the only option: the level of guarantees can be set by the operating system, an additional security subsystem or even by requirements for application implementation. In any of these cases, the gateway will be able to implement functions to protect the infrastructure as well as the specialist services of the IoT framework.

Advantages

Primarily, the advanced cybersecurity technologies offered by Kaspersky Secure IoT Gateway mean a reduction in operational costs and total cost of ownership (and service) for secure devices. This is due to a reduction in customer service calls, a significant decrease in reputational risk as well as the direct and indirect losses caused by cybersecurity incidents.

Another important advantage is the transparency and manageability of the infrastructure thanks to the advanced monitoring and management tools included in the Kaspersky Lab solution.

With the built-in opportunities for the operator or manufacturer to promote additional services, it is also possible to upsell and increase revenue from a user.

End users of the devices will appreciate the concern, resulting in increased loyalty to the operator. Advantages for end users include advanced parental control with flexible settings, IoT device management (for IT and IoT devices), and protection for incoming and outgoing traffic.

www.kaspersky.com

Kaspersky Lab, Moscow, Russia **www.kaspersky.com**
Cyber Threats News: **www.securelist.com**
KasperskyOS®: **os.kaspersky.com**

#kasperskyos
#truecybersecurity