KasperskyOS

# Cyber Immune operating system for industries with high information security requirements

**KasperskyOS implements a new Cyber Immune approach to protecting IT systems, rendering both known and new types of cyberattacks ineffective.**

**The need for protection:**

According to Kaspersky ICS CERT, 39.61% of ICS computers were attacked by malware in 2021

## Why it matters

With each year, the cyberthreat landscape becomes more complex and the capabilities of the attackers improve. Industrial plants, the energy sector, transport infrastructure, and smart city IT systems are all under attack.

Conventional approaches to the security of IT systems are ineffective in these circumstances, which is why there is increasing demand for operating systems with a high level of security guarantees.

**Advantages:**

- Minimization of cyber-risks
- Reduced costs of purchasing and operating additional IT security products
- Optimization of IT and information security department labor costs
- Flexible configuration to meet individual functionality and security requirements

## Solution

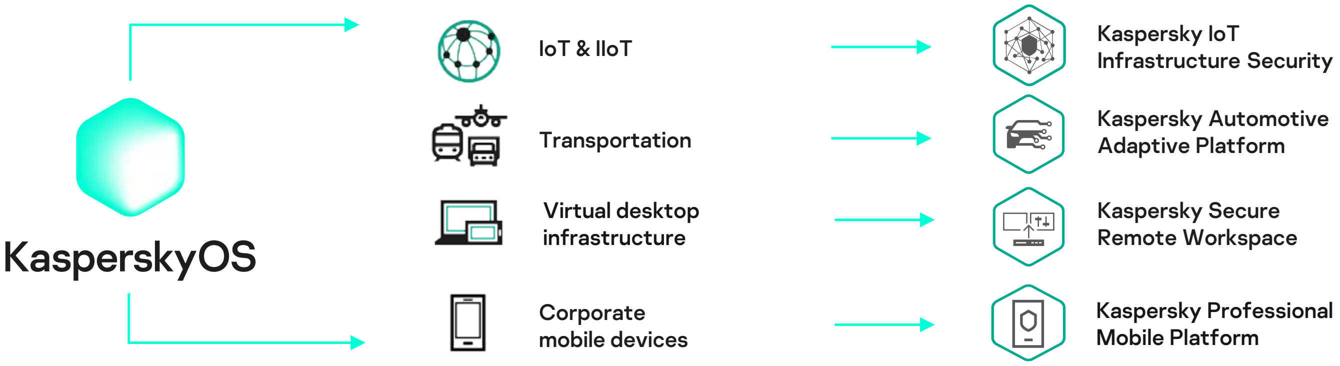
As a response to today's realities, Kaspersky has developed its own operating system KasperskyOS.

The distinctive architecture of KasperskyOS makes it possible to create IT products that are Cyber Immune, i.e., have built-in protection against most types of cyberattacks. It is virtually impossible to hack these products or affect their critical functions, and they continue to function reliably even in hostile environments.

Solutions built on KasperskyOS do not need additional (applied) security features everything you need is already inside the system.

## Areas of application

KasperskyOS is used in areas where IT systems are subject to higher cybersecurity, reliability and predictability requirements, such as manufacturing industries, the energy sector, transport infrastructure, and smart city systems. It ensures the confidentiality and integrity of data and secures it against spoofing.


KasperskyOS
IoT & IIoT
Transportation
Virtual desktop infrastructure
Corporate mobile devices
Kaspersky IoT Infrastructure Security
Kaspersky Automotive Adaptive Platform
Kaspersky Secure Remote Workspace
Kaspersky Professional Mobile Platform

kaspersky

**Key technologies:**

**Kaspersky Cyber Immunity®**
Proprietary methodology for developing secure by design systems that do not require additional security features.

**Microkernel**
Ensures operating system reliability and transparency. The kernel's minimal size ensures strict quality control of the code.

**Kaspersky Security System subsystem**
Monitors all interactions between KasperskyOS components, checks they comply with security policies and prohibits any undesirable behavior.

The operating system kernel was developed from scratch at Kaspersky, without the use of third-party libraries or code.

# What makes KasperskyOS secure?

The 'innate' security of KasperskyOS is embedded in its architecture and philosophy. The operating system is based on Kaspersky's own approach to developing Cyber Immune IT products.

Cyber Immunity is ensured by dividing the system into isolated components and controlling the interaction between them. At the design stage, security policies are defined that specify each permissible action. Only what is allowed by the system administrators and application developers can run and work.

KasperskyOS, together with the methodology for developing IT products, serves as an effective and reliable basis for creating trusted information systems that are immune to cyber threats.

# Architecture features

KasperskyOS was developed in accordance with the proven and extensively documented concepts including MILS and FLASK, with the addition of Kaspersky's own security technologies.

KasperskyOS allows you to flexibly define security policies  rules that the system will follow throughout its lifecycle and that will prevent it from performing potentially dangerous operations.

KasperskyOS components are divided into isolated security domains that cannot interact directly. All their interactions go through the microkernel and are checked by the Kaspersky Security System subsystem, which issues security verdicts to each of them. Any action not explicitly permitted by the security policy will be blocked before it is performed.

This means untrusted components that do not have Cyber Immunity can also be used when developing on our OS. Even if an untrusted component is compromised, the attacker will not be able to escalate the attack and affect the functioning of the system.

# Development methodology

To develop a Cyber Immune product based on KasperskyOS, it is necessary to follow a specific methodology:

- clearly define the security goals (e.g., data confidentiality) as well as the environment in which the system will operate;
- divide solutions into isolated security domains, taking into account the functionality and degree of trust in each of them;
- ensure control of information flows between these domains, permitting only specified types of interactions.

KasperskyOS provides the necessary interfaces, mechanisms and tools for developing cybersecurity solutions, including isolating security domains and controlling interactions between them.

KasperskyOS

Find out more os.kaspersky.com

www.kaspersky.com