KasperskyOS

Secure OS for Telecoms Equipment
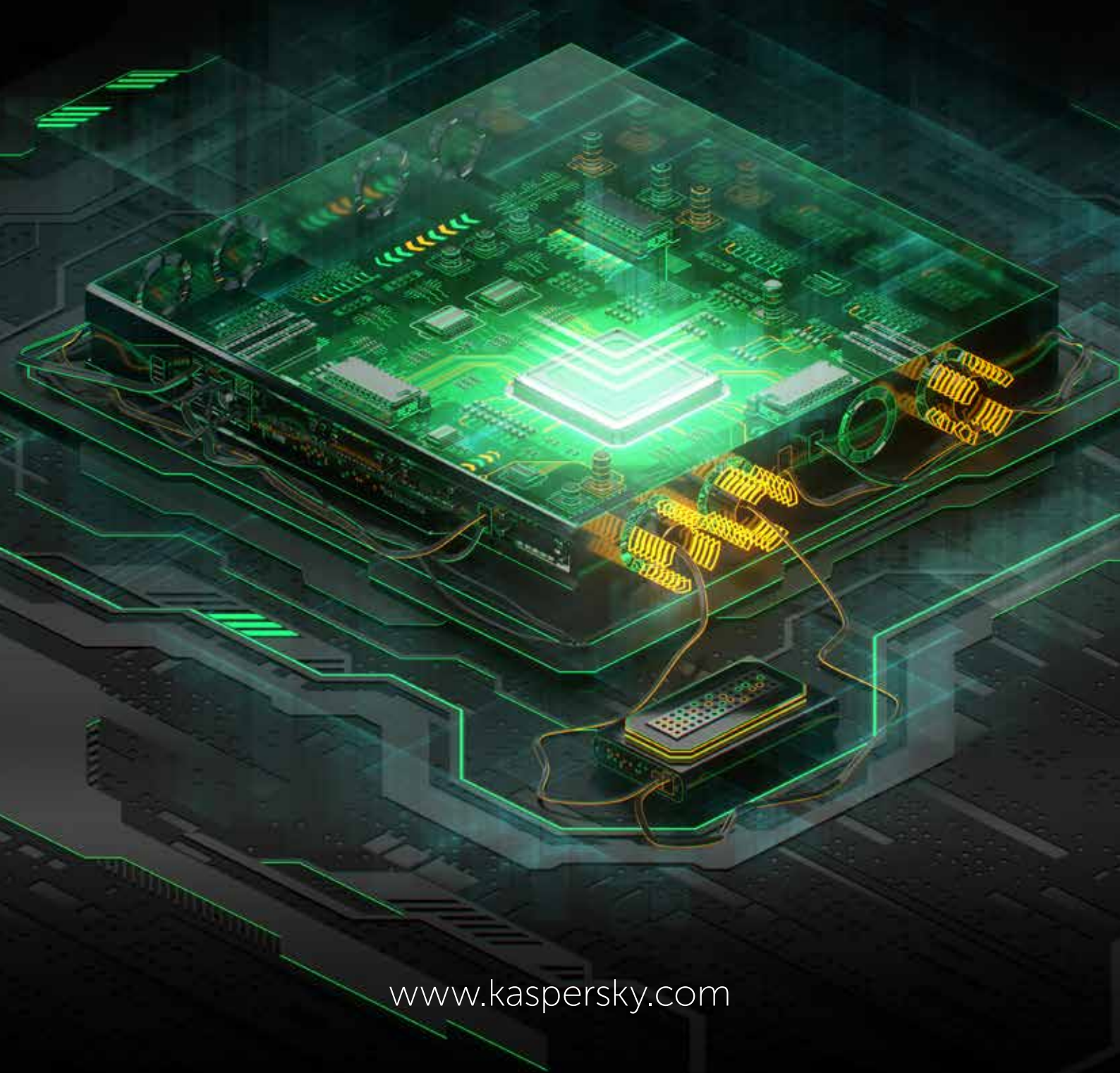
As a system for exchanging diverse information, the Internet has become part and parcel of our everyday lives. Many traditional businesses are transforming themselves into IT and technology companies. We often don't realize to what extent our work, life and leisure are dependent on the Net.

At the same time, new opportunities give rise to new risks. In the case of the Internet, the risks are primarily associated with cyber threats that can affect the stability of the Internet's infrastructure, and how stably the Internet operates depends on telecommunications service providers and telecoms equipment.

Among the cyber threats targeting telecommunications equipment, the following are particularly significant:

1) Threats associated with unintentional actions:

    a. Employee actions resulting in complete or partial equipment failure, switching off or changing the operation mode.
    b. Unauthorized installation and use of programs that are unaccounted for.

2) Threats associated with intentional actions:

    a. Remote attacks on hardware aiming to change its configuration or modify its built-in software (firmware).
    b. Exploiting built-in backdoors or known software and hardware vulnerabilities in order to intercept traffic or gain control of equipment or an automated system.
    c. Unauthorized installation and use of programs that are unaccounted for.

While some threats can be mitigated by developing dedicated security software, reliable protection from other threats can only be achieved by installing a trusted computer appliance providing guaranteed protection against unauthorized software installation or execution of undocumented functions.

This means that equipment manufacturers face a difficult dilemma. On the one hand, the equipment they produce must provide extensive functionality; on the other, its firmware should be sufficiently compact to make checking it for vulnerabilities and backdoors feasible. The equipment should also be reliable and provide faultless operation, but at the same time it should have excellent cyber-security characteristics.

It should also be kept in mind that protecting telecommunications equipment against cyber threats is further complicated by a number of factors, including: (1) the need for the equipment to operate autonomously without maintenance or software updates for extended periods of time; (2) specialized hardware; (3) proprietary built-in software; (4) permanent direct connection to the internet; (5) not being able to install additional protection designed for general-purpose systems.

The only way is to develop a cyber-secure integrated software suite that includes an operating system, as well as system and application software.

To address the issue of cyber security for telecoms equipment, while minimizing the time required to develop security features, we offer KasperskyOS, a secure operating system based on an architecture that is designed to ensure software is executed securely, including non-secure applications. In addition, KasperskyOS provides protection in the event of random software errors and faulty user actions.

KasperskyOS benefits

Inherent security. KasperskyOS is an operating system that is secure by design and we intend to keep it that way by using the best practices of software development.

Versatile modular architecture. Building the system based on loosely coupled modules helps to minimize the amount of trusted code and tailor each solution to the customer's specific needs.

Well-designed applications. The component-based approach to creating secure applications makes developing them relatively easy and convenient, helping to reduce the amount of time needed to take new products to market.

Flexible security configuration. Well-designed configuration tools make it easy to create declarative rule definitions and combinations of rules to control interactions in the system.

Separation of application features from security functions. The security architecture is designed to separate security functions from application business logic, making both configuring security policies and developing applications easier.
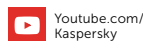
Full-fledged security for attached devices. KasperskyOS is a reliable platform for embedded systems that have special cyber-security requirements.

Supported hardware:
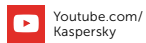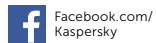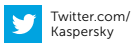Currently KasperskyOS may run on Intel x86, x64, ARMv7 (i.MX6)

Patents:
US 7386885 B1, US 7730535 B1, US 8370918 B1, EP 2575318 A1, US 8522008 B2, US 20130333018 A1, US 8381282 B1, EP 2575317 A1, US 8370922 B1, EP 2575319 A1, US 9015797 B1, DE 202014104595 U1.

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY⁙lab

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab