

Trusted Network Equipment by Kaspersky Lab and Eltex



Kaspersky®
Security System

www.kaspersky.com
os.kaspersky.com



eltex-co.ru/en/

Two Leading Russian Companies Join Forces to Create Trusted Telecommunications Equipment

«Though targeted attacks on corporate and industrial targets are often carried out via vulnerabilities in system software, this is exactly the sort of software that doesn't have sufficient protection.»

Andrey Doukhvalov,
Head of Future Technologies,
Kaspersky Lab

«The number of cyberthreats is growing every year. As a device developer and manufacturer, our company understands that it's crucial to use the most up-to-date protection technologies to ensure secure and reliable functioning of those devices on our customers' networks. By using KSS from Kaspersky Lab we have given the devices manufactured by Eltex a new level of security.»

Mikhail Moiseev,
Commercial Director Deputy,
Eltex

Challenge

Modern telecommunications systems have extensive functionality, but these capabilities come hand in hand with cyberthreats that jeopardize the stability of the equipment itself and the security and confidentiality of the data that's transferred or stored using these systems.

For example, implants surreptitiously embedded in system software that controls telecoms equipment enable attackers not only to control devices and remotely put them out of operation but also to intercept the data they handle, compromising its integrity as well as confidentiality.

That's why modern communications equipment, in addition to its primary functions, has to ensure the cybersecurity of the device itself and the data it transmits. End users also need to be sure that the device doesn't contain any undocumented functions. Taking into account all the above, it is necessary to create a basic software package with built-in protection against cyberthreats, and to install that package on trusted hardware.

The Kaspersky Lab solution

Eltex and Kaspersky Lab combined efforts to create a trusted solution for telecommunications that completely meets these cybersecurity requirements. The solution is based on hardware and software products by Eltex and Kaspersky Security System – a special security module from Kaspersky Lab.

The main principle behind Kaspersky Security System is that of 'default deny', which means blocking anything that is not explicitly allowed. This approach prevents penetration by malicious programs and any negative consequences. In addition, all the security settings, including denying execution of any particular processes or actions, take into account the characteristics of the Eltex equipment and its security requirements.

Integration of KSS into Eltex's solution was implemented at the same time as modifications to the architecture. In this regard, several components can be emphasized:

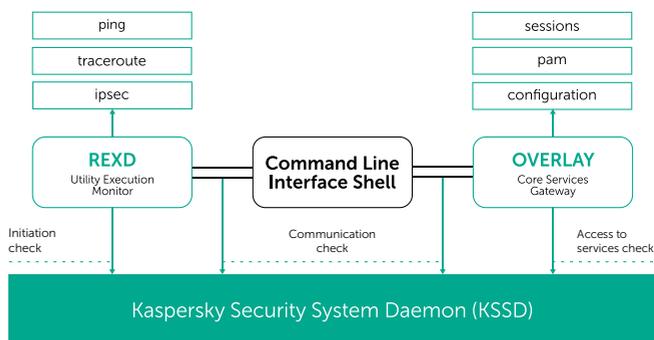
Kaspersky Security System provides control over interactions between program components inside an information system based on predefined security properties and communication rules. With KSS it is also possible to detect and block misbehavior caused by internal errors or attempts to gain unauthorized access.

CLI Shell – a complex component interacting directly with a remote user.

Main features of KSS/Linux:

- isolation of individual components of the solution using containerization technology
- formal description of the interfaces for all components and validation of transmitted messages to ensure compliance with those interfaces
- means of controlling all component interactions to ensure compliance with the specified security policy
- tools to specify a security policy as a combination of a broad range of security properties set in declarative style in the terms of the subject area.

- **CLI Shell:** a command line interface shell used by system users for device configuration tasks, launching auxiliary utilities, analyzing logs, etc.;
- **OVERLAY:** core device services such as authentication, configuration, logging, etc.;
- **REXD:** an initiation service for auxiliary commands. CLI Shell accesses it to run a large number of utilities such as ping, traceroute, tcpdump and lots more;
- **KSSD:** messaging service and access checks in accordance with a security policy.



The main aim of integrating KSS is to prevent the unauthorized escalation of privileges, even if CLI Shell is fully compromised. In other words, CLI Shell is classified as an untrusted component.

For each newly connected user a new CLI Shell instance starts, which is assigned a specific privilege level (ranged from 0 to 15). While working, a user can increase their privileges using the 'enable' command, but this requires additional authorization. At any point in time KSSD knows the privilege level for all CLI Shell instances that have gone through authorization.

In accordance with the restrictions imposed by the security policy, each command has a minimal privilege level that is necessary for its execution. For each request from CLI Shell, KSSD checks if the current privilege level is enough for the requested command.

Result

The range of measures employed means that a user with a privilege level of less than 10 cannot execute a single privileged command even if a critical vulnerability is found in CLI Shell and exploited.

Thanks to the mutual efforts and collaboration of these two industry leaders, a new product has been created based on the latest technological developments by Eltex and Kaspersky Lab's trusted KSS module. Now, customers can be sure their equipment contains no vulnerabilities and their data is reliably protected. The new product is already available for purchase.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company celebrating its 20-year anniversary in 2017. The company's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe.

Kaspersky Lab's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

About Eltex

Eltex is a leading Russian developer and manufacturer of telecommunications equipment.

The company was founded in 1992 and today it is a huge, dynamically developing enterprise with more than 600 employees. Eltex has its own high-tech manufacturing facilities that include all the necessary technological cycles and equipment as well as seven software development labs.



The image illustrates service routers ESR-1200, ESR-1000 and ESR-12VF. For the full list of trusted equipment visit the Eltex website: https://eltex-co.ru/catalog/service_gateways/



KasperskyOS®

Find out more at
os.kaspersky.com

www.kaspersky.com

© 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.