kaspersky BRING ON THE FUTURE

Kaspersky Security System

Kaspersky Security System

Kaspersky Security System is an innovative framework intended to secure a wide range of computer systems.

Introduction

Kaspersky is creating a portfolio of security solutions for critical infrastructure as part of a global initiative. One of those solutions is KasperskyOS – the secure operating system. KasperskyOS was developed using the best design practices and de-facto security standards. Adherence to these practices and standards will better assure the confidentiality and integrity of the data in the computer system.

Kaspersky Security System was initially implemented as a part of KasperskyOS with a view to supporting diverse security models. However, during development it became clear that Kaspersky Security System fits the needs of many other operating systems and hypervisor-based solutions. As a result, it has evolved into a standalone project and can now be embedded into other systems that demand high levels of security.

Purpose

While some threats can be mitigated by developing dedicated security software, Nowadays all computer systems, including cyber-physical systems used in critical infrastructure, are prone to numerous cyber threats. These computer systems are often protected by add-on tools that are incapable of addressing their specific security requirements. These security tools don't have adequate means of defining the appropriate security policy for every system or for enforcing these policies exactly as defined. This is why Kaspersky has created an embeddable solution that meets current security requirements.

Features

- Applies access control rules based on the separation of security domains.
- Adjusts interaction of components related to different security domains.
- Classifies informational resources according to a given security policy.
- Computes security verdicts to authorize each action in the system.
- Logs and audits security events.
- Provides additional security services.

Integration

Integration of Kaspersky Security System into the existing operating system or solution can be undertaken in two phases:

1. Pre-project phase
   - Analyze the existing solution (operating system or hypervisor-based solution, specific hardware features).
   - Devise a plan to adapt Kaspersky Security System to the existing solution.
   - Create appropriate security policies.
2. Integration phase
   - Integrate Kaspersky Security System into the existing system.
   - Deploy security policies.

Implementation

Kaspersky Security System is an innovative framework intended to secure a wide range of computer systems, such as:

- Enterprise systems
- Special-purpose computer systems
- The Internet of things
- Smart grids
- Industrial systems
- Transportation systems
- Critical Infrastructure

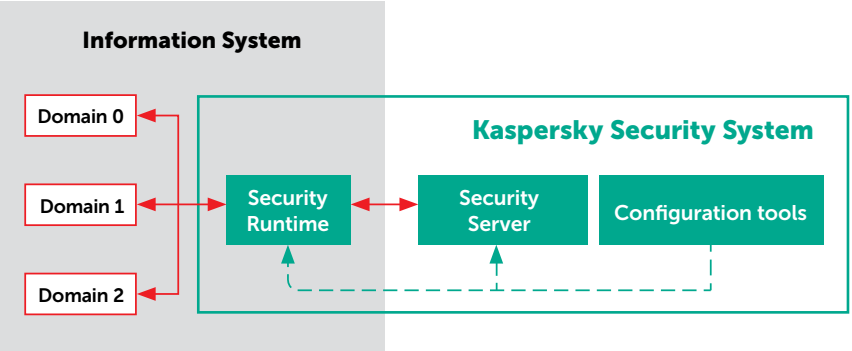
Kaspersky Security System is implemented as an OEM component for operating systems or hypervisor-based solutions.

Compatibility

- KasperskyOS[1]
- PikeOS
- Linux
- Support for other (including real-time) operating systems is in progress

1 The deep integration of KasperskyOS and Kaspersky Security System creates a sustainable, versatile and high performance platform to support security in different systems, including industrial networks.

Figure 1. An example of Kaspersky Security System managing three security domains of an Information System under a single security policy. The Security Runtime component of Kaspersky Security System mediates communications between security domains and enforces predefined security rules that are set by configuration tools. Security Server includes a customizable database of security policies and provides decisions to Security Runtime based on the current state of the system.



The architecture of Kaspersky Security System means specific security rules for every given system can be defined, removing unnecessary controls and complex configurations.

Components

- **Security Runtime** is the module that enables interaction between the existing system's internal components and Kaspersky Security System. It delivers every request to the security verdict engine and returns the computed verdict to the system.
- **Security Server** is the security engine that computes the security verdict (whether an interaction should be permitted or not). It provides its verdict using the following factors:
  - The set of security rules implemented in the security policy for the system.
  - The security context that describes the current state of the system.
- **Configuration tools** are used to adjust security policies and rules and deploy them in the system.

Advantages

- The Kaspersky Security System paradigm is based on the strict separation of security features from the functional components of the computer system. Security is provided regardless of how the system is implemented. Because of this, trusted systems can be built using untrusted components and Kaspersky Security System. Security rules and policies can be varied without changing any functional components.
- Kaspersky Security System allows a combination of different security models, such as connecting basic and customized security policies.
- Under specific conditions Kaspersky Security System can be used in real-time operating systems.
- The architecture of Kaspersky Security System means specific security rules can be defined for every given system, removing unnecessary controls and complex configurations from the overall solution.

Operating modes

There are two operating modes for Kaspersky Security System:

- The basic mode includes a wide range of security policies, sufficient for most usage scenarios.
- The customized mode builds on the basic mode with specialized security policies necessary to comply with the specific objectives of the target solution.

Target Audience

- Vendors of operating systems and hypervisor-based solutions
- Vendors of IT systems demanding enhanced security levels
- System integrators

Patents
The technologies that form the basis of KasperskyOS and Kaspersky Security System are covered by a set of 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.

Read more on os.kaspersky.com

www.kaspersky.com