kaspersky

BRING ON THE FUTURE

Kaspersky Private Security Network

Real-time, cloud-assisted cybersecurity for privacy and compliance-restricted networks

Complex and focused threats tend to inflict incomparably greater damage than mass malware can generate. In the face of this threat environment, the value of the security intelligence delivered by Kaspersky Security Network cannot be overestimated.

Every object passing through a system protected by Kaspersky solutions is subject to analysis, based on threat intelligence fed with real-time data from tens of millions of global sensors. The highest accuracy and relevance is ensured through interaction between machine learning technologies, big data analysis and leading researchers: Kaspersky HuMachine technology. The result is a consistently high level of protection against real-world, real-time cyberthreats.

Kaspersky Private Security Network allows enterprises to take advantage of most of the benefits of global cloud-based threat intelligence, without releasing any data whatsoever outside their controlled perimeter. It's an organization's personal, local and completely private version of Kaspersky Security Network.

Kaspersky Private Security Network is ideal for:

- Enterprises with strict data access control requirements
- Government agencies
- Telecommunications companies
- Manufacturers and utilities providers with physically isolated networks
- Critical infrastructures
- MSSPs and other service providers

Business Benefits

- Optimum detection of malicious objects
- Real-time access to threat and reputation statistics
- Stops the spread of malicious software
- Reduces risk and minimizes the damage from cybersecurity incidents
- Minimizes false positives
- Allows the addition of your own malicious 'verdicts' for customized security
- Supports full compliance with regulatory requirements for the security of isolated systems and environments

All the benefits of cloud-assisted security – without the need to share information outside your controlled infrastructure

- Enables you to harness the power of cloud intelligence without the need to transfer data outside the organization
- Helps deliver the exceptionally high detection rates and low number of 'false positives' for which Kaspersky security solutions are so widely known
- Designed for full compliance with regulatory and security standards
- Real-time awareness of the latest, most sophisticated attacks, delivered within your controlled, local network
- Integration with third-party applications via HTTP protocol
- Adapted for critical networks isolation – including 'air gap' requirements
- High availability and clustering
- Flexible deployment options

True Cybersecurity

With the demand for cloud-assisted security for critical and isolated networks growing, most solutions respond by using 'caching proxies' - limited data or predefined reputation databases without updates. Kaspersky Private Security Network is unique in its ability to deploy cloud-based security entirely locally, within the organization's own data center, involving zero outbound transactions with third-party servers.

Solution requirements

To install Kaspersky Private Security Network, a dedicated server with the following specifications is required:

Hardware requirements

- 8-core 2 GHz processor
- 96 GB RAM
- 500 GB SSD

Software requirements

- RHEL 7.6
- CentOS 7.5
- Browser: Google Chrome, Mozilla Firefox or Opera
- JAVA-plugin 7 or higher

Kaspersky Anti Targeted Attack support

When deployed in conjunction with the Kaspersky Anti Targeted Attack Platform, Kaspersky Private Security Network requires data to be placed on an additional dedicated server with the following configuration:

- 10-core 3 GHz processor
- 96 GB RAM
- 600 GB SSD

For other deployment configurations, please refer to the Administrators Guide.

Licensing

Kaspersky Private Security Network Standard

- Support for up to 50,000 protected devices

Kaspersky Private Security Network Advanced

- Support for up to 500,000 protected devices
- Local reputation database (company defined black/whitelists)
- xSP model support
- High availability

How it works

Kaspersky Private Security Network can be installed within your own data center; your in-house IT specialists retain complete control. So your IT infrastructure and SOC can enjoy all the benefits of cloud-assisted security without compromising on privacy, and in compliance with regulatory requirements that no item of data leaves your perimeter.
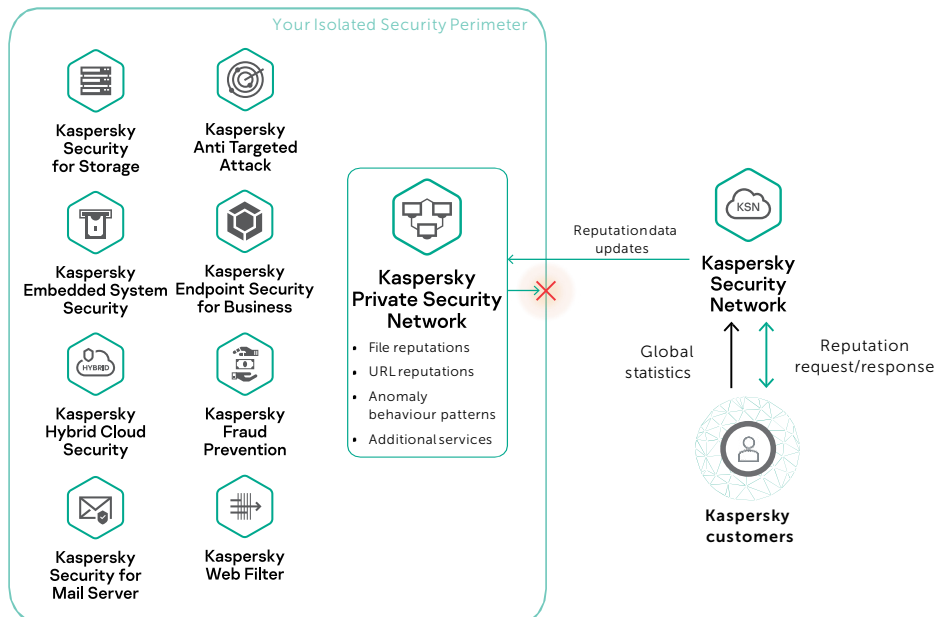
File Reputation Service

This service provides your Kaspersky security solutions with information about the reputation and categorization of files.

URL Reputation Service

This service provides information about the reputation and category of websites.

Anti-Spam

Anti-Spam delivers statistical data for protection against spam.

Anti-APT

When running the Kaspersky Anti Targeted Attack Platform, this component supports Kaspersky Private Security Network with data on the reputations of IP addresses and domain names, for the rapid detection of targeted attacks and advanced threats.

The highest accuracy of information is ensured by the well-oiled mechanism of interaction between robots and experts: Kaspersky HuMachine technologies.

In any organization, it's essential to ensure the Best Possible Outcome for a given situation, and Kaspersky Security Network, together with its "internal" version Kaspersky Private Security Network, achieves this goal.

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at **kaspersky.com/transparency**

Proven.
Transparent.
Independent.