kaspersky BRING ON THE FUTURE

Kaspersky Scan Engine

Kaspersky Scan Engine is a server-side security solution that provides anti-virus protection, HTTP traffic scanning, and file and URL reputation checking for third parties' client-side solutions.

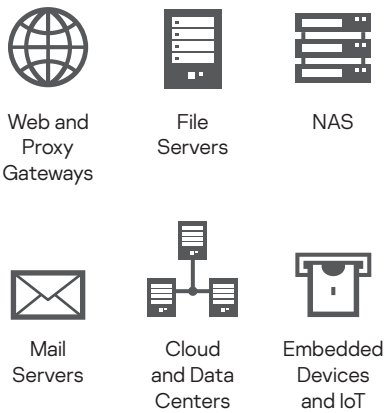
Kaspersky Scan Engine (KSE) delivers comprehensive protection from malware, Trojans, worms, rootkits, spyware, and adware for a wide range of applications. It can be used with various products and services including desktop applications, server solutions, proxy servers, and mail gateways.

KSE employs all the newest methods of detection and removing various types of malware. The solution is very easy to install and configure, and no development is needed with out-of-the box installation.

Usage Scenarios

- Protection of data repositories and workflow systems from malware.
- Scanning of files uploaded by the end-users to the customer's web portal. KSE enables the embedding of uploads scanning procedure into any segment of the chain of files delivery from the end-users to the customer.
- Automated users' file scanning via ICAP protocol. Both the files and the links the users try to access are scanned.
- Deployment of a local web service for scanning of files and links. Objects scanning doesn't require the presence of a client on the endpoints.
- Integration with any third party object scanning applications.

Integration Scenarios



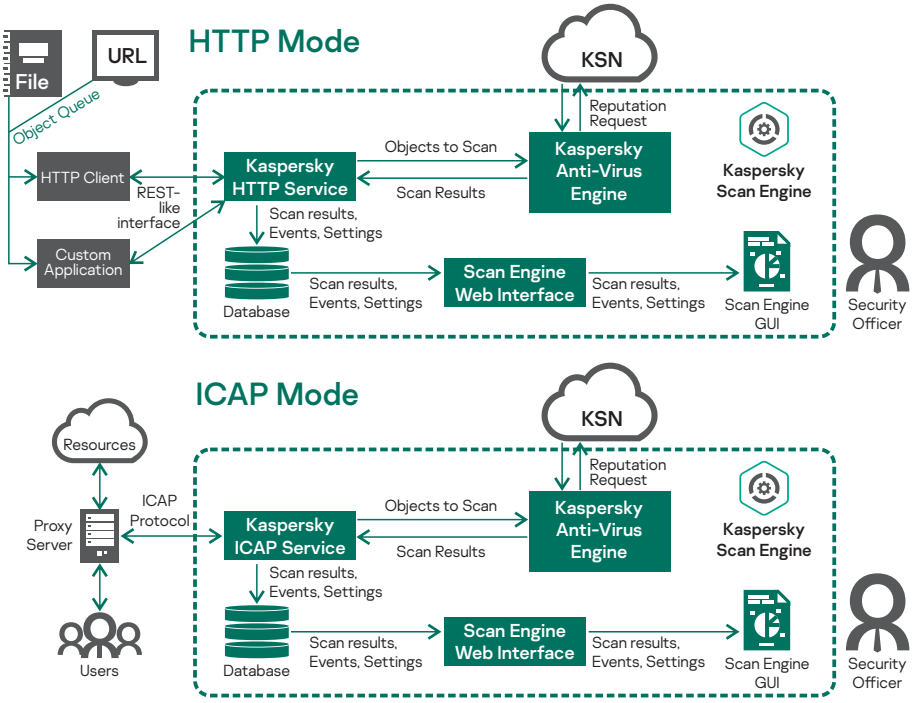
Key Functionality

Kaspersky Scan Engine can work in Windows & Linux environments in one of two modes:

- **REST-like service** that receives HTTP requests from client applications, scans objects passed in these requests, and sends back HTTP responses with scan results.
- **ICAP server** that scans HTTP traffic that passes through a proxy server / NAS / Web Application Firewall / NextGen Firewall / any other solutions communicating through ICAP protocol. This integration model also allows scanning the URLs requested by users; web page that contain malicious content are then filtered out.

Kaspersky Scan Engine is also available as a Linux Docker container (in HTTP & ICAP modes). It can be deployed as an individual container, to Docker Swarm, to Kubernetes, or to AWS.

Kaspersky Scan Engine includes a graphical user interface that allows you to easily configure the product behavior, review its service events, and scan results.



Recent Kaspersky Product Awards from Independent Testing Labs

Kaspersky
Endpoint Protection

...and more – for details see www.kaspersky.com/top3!

Product Features

- **Award-winning Kaspersky anti-malware technology** provides the best-in-class malware detection rates and can instantaneously react to emerging threats.
- Filters out malicious, phishing, and adware URLs.
- Detection of multi-packed objects and objects packed using "grey" compression utilities (frequently used for hiding malicious programs from anti-virus software).
- Advanced heuristics analyzer and machine learning-based detection technologies.
- Disinfection of infected files, archives, and encoded objects.
- Updatable Anti-Virus engine: detection technologies and processing logic can be upgraded or modified through regular updates of the anti-virus database.
- Kaspersky Scan Engine can be provided as a Linux Docker container. Deployment as an individual container, to Docker Swarm, to Kubernetes, and to AWS EKS environments.
- Powered by Big Data: Kaspersky Security Network provides information about the reputation of files and Web resources, ensuring faster and more accurate detection.
- Kaspersky Scan Engine natively supports multithreading and can process several tasks simultaneously. You can adjust the number of scanning processes and threads to increase performance of Kaspersky Scan Engine.
- Several instances of Kaspersky Scan Engine can be deployed in the same network and administered through Web UI.
- Kaspersky Scan Engine can run in cluster mode. This means that if the customer has several instances of KSE, they can use the Web UI of any instance to review the scanning results for any instance, check the status (on/off, database version), or update the settings.
- Communication via TLS protocol is supported when running in REST-like service mode.
- Additional filtering layer is made possible by the Format Recognizer component. You can use this component to recognize and skip files of certain formats during the scanning process. Dozens of formats are supported, including executable, office, media files, and archives.
- **Graphical user interface (GUI) for management and monitoring:**
  - Lets you configure application settings and manage the application.
  - Lets you monitor the application operating status, status of the used key file or activation code, and the number of scanned and detected objects.
  - Provides information about all scanned objects on a dashboard. Scan results can be imported in CSV format.
- **Reporting features:**
  - Important application events are sent to Syslog in CEF format.
  - All service events are visible on the GUI dashboard.
- **Maintenance features:**
  - Anti-virus database updates are automatic. Kaspersky Scan Engine automatically restores corrupted databases.
  - Easy collection of product traces with the GUI.
  - Option to use online activation. With online activation, licensing information for Kaspersky Scan Engine is updated automatically.
- Fault-tolerant and resilient architecture.
- Source code for HTTP client and ICAP service are provided in the distribution kit for customization.
- Comprehensive documentation and cross-platform API support. Similar APIs for Linux/UNIX and Windows versions.
- Option to minimize external traffic by creating local mirror server for the anti-virus database (additional tool needed).

30-day Free Trial is available! Please scan the QR code and make a KSE trial request. Or else, click here: www.kaspersky.com/partners/technology/contact

Kaspersky Technology Alliances

Kaspersky technologies are available for integration into third party hardware and software security products and services. All solutions are backed by professional technological partnership support.

Learn more at www.kaspersky.com/oem

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

©2021 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.