kaspersky BRING ON THE FUTURE

Kaspersky Scan Engine

Kaspersky Scan Engine provides you with the best-in-class threat detection solution that can be integrated into almost any application.

Kaspersky Scan Engine (KSEn) provides comprehensive protection for web portals and applications, proxy servers, network attached storage and mail gateways. It is easy to manage and deploy through HTTP and ICAP as a standalone service, scalable cluster, or Docker container.

KSE uses the latest detection methods for detection and removal of malware including Trojans, phishing threats, worms, rootkits, spyware and adware.

Key Functionality

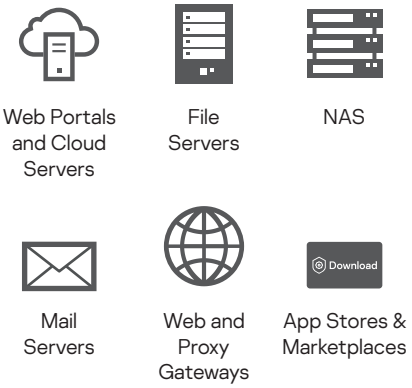
Kaspersky Scan Engine can work in Windows & Linux environments in one of two modes:

- **REST-like service** that receives HTTP requests from client apps, 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 / NGFW / any other solutions communicating through ICAP protocol. This integration model also allows scanning the URLs requested by users; web pages with malicious, phishing or adware content are then filtered out.

Kaspersky Scan Engine is also available as a Linux Docker container (in HTTP & ICAP mode). It can be deployed as an individual container, to Docker Swarm, to Kubernetes, to AWS EKS, and any similar cloud environments.

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

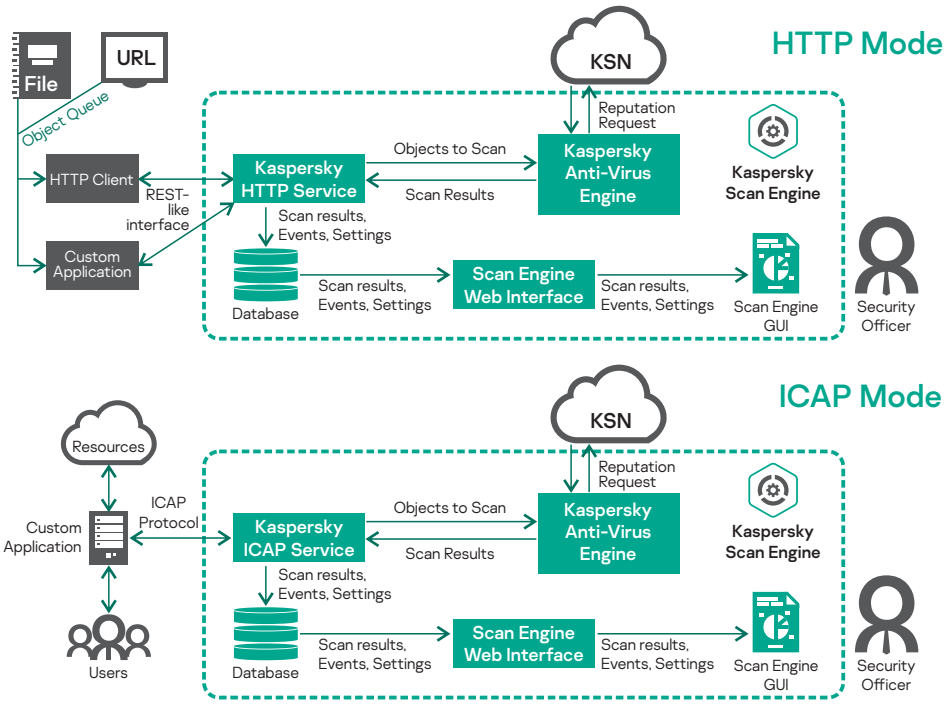
Integration Scenarios



Usage Scenarios

Thanks to a feature-rich REST-like API and open source code, you can easily integrate Kaspersky Scan Engine with almost any solution in your network.

- Web portals protection from malware upload
- Protection of public (AWS S3 bucket, Azure Blob Storage, etc.) and private (Nextcloud, ownCloud, more upcoming) cloud storage from malicious content upload
- Protection of app stores and software marketplaces from malicious apps upload
- Scanning of container images for malware
- Scanning of Windows/Linux file storage for malware
- Anti-malware plugin for third-party web/mail gateways. The list of completed integrations is available upon request and is constantly updated.
- Anti-malware module to corporate document management system, software development pipeline, and other systems which require files to be checked for malware.



Recent Kaspersky Product Awards from Independent Testing Labs

...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. Greatest number of packer and archive formats supported.
- Advanced heuristics analyzer and machine learning-based detection technologies.
- Disinfection of infected files, archives, and encoded objects. Any detected threat can be either removed altogether, or, if possible, only malicious payload can be removed, leaving the rest of the file safe.
- Updatable Anti-Virus engine: detection technologies and processing logic can be upgraded or modified through regular updates of the anti-virus database.
- 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 provides top-notch performance and scales very easily.
- Kaspersky Scan Engine can run in cluster mode: several instances of Kaspersky Scan Engine can be deployed in the same network and administered through Web UI.
- 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.

New features in Kaspersky Scan Engine 2.1 (released in June 2022)

Security and compliance features:

- Multi-user mode and Role-based access control
- Operations audit
- Support of HTTP clients authentication via API tokens
- Protection from password brute-forcing in Web-UI

Cluster mode improvement:

- Idle nodes are automatically removed from the cluster
- Support of heterogenous (HTTP and ICAP) clusters

Operational improvement:

- `systemd` is fully supported for work with the services (start/stop/status/restart)

Documentation improvement:

- Manuals for integration with SIEMs (MicroFocus ArcSight, Splunk)
- Manuals for integration with Oracle Solaris VScan, F5 Application Security Manager, GoAnywhere MFT, Dell Isilon OneFS.

Changes in syslogging:

- Multiple destinations
- Filter of events to be sent

Architectural change:

Scan Engine is divided into 2 modules which can be released separately:

- AV engine (KAV SDK)
- main product functionality (Scan Engine as a wrapper on KAV SDK)

This will allow to release new versions of ScanEngine faster and easier.

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

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

www.kaspersky.com

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