kaspersky BRING ON THE FUTURE

Kaspersky Scan Engine

Kaspersky Scan Engine (KSEn) – это лучшее в классе решение для обнаружения и борьбы с киберугрозами, которое с легкостью интегрируется почти с любыми приложениями.

Kaspersky Scan Engine предназначен для комплексной защиты интернет-порталов, веб-приложений, прокси-серверов, сетевых хранилищ данных и почтовых шлюзов. Решение просто в развертывании и эксплуатации, оно работает через протоколы HTTP или ICAP в качестве самостоятельного сервиса, масштабируемого кластера, или контейнера Docker.

KSEn использует новейшие технологии обнаружения для выявления и уничтожения различных киберугроз, в том числе троянов, фишинга, червей, руткитов, шпионских и рекламных программ и т.п.

С апреля 2020 года приказом Минкомсвязи РФ Kaspersky Scan Engine внесен в Реестр отечественного ПО.

Основные возможности KSEn

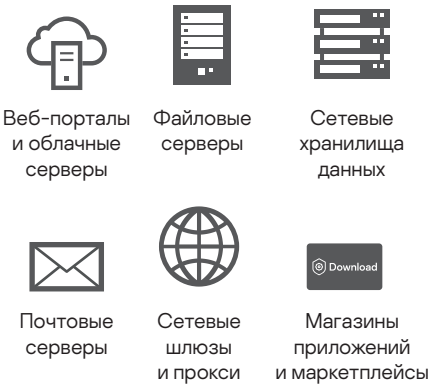
У Kaspersky Scan Engine есть два режима работы в Windows- и Linux-средах.

- REST-like сервис получает HTTP-запросы от клиентских приложений и сканирует передаваемые объекты, затем возвращает HTTP-ответы с результатами проверки.
- ICAP-сервер сканирует HTTP-трафик, проходящий через прокси-сервер, сетевые хранилища данных, межсетевые экраны или любые другие приложения, работающие через протокол ICAP. Данная модель интеграции также позволяет сканировать URL-адреса, которые запрашивают пользователи, после чего отфильтровывать веб-страницы с вредоносным или рекламным контентом.

KSEn для Linux также доступен в виде docker-контейнера (в HTTP- и ICAP-режимах) и может быть развернут в виде отдельного контейнера или в Docker Swarm, Kubernetes, AWS EKS, или любых аналогичных облачных средах.

Решение Kaspersky Scan Engine оснащено графическим пользовательским веб-интерфейсом, где можно легко настроить службу или просмотреть события и результаты сканирования.

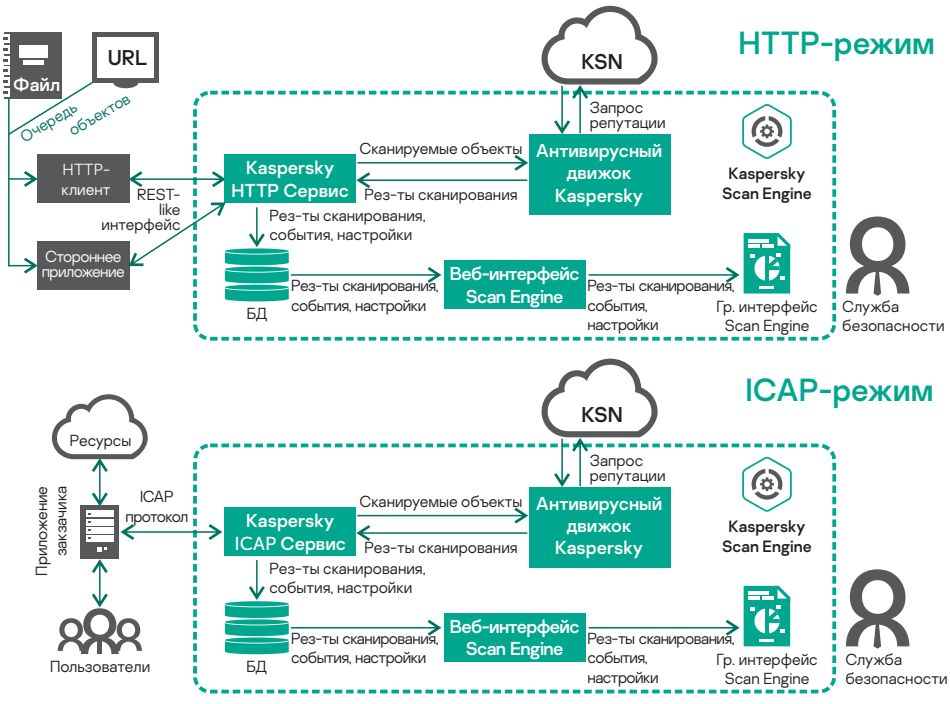
Сценарии интеграции



Сценарии использования

Благодаря богатому REST-API и наличию исходного кода, вы можете выполнить интеграцию Kaspersky Scan Engine с любым решением в вашей сети.

- Защита веб-портала от загрузки вредоносного контента
- Защита публичных (AWS S3 bucket, Azure Blob Storage и другие) и приватных (Nextcloud, ownCloud, возможно другие) облачных хранилищ от загрузки вредоносного контента
- Защита магазинов приложений и облачных маркетплейсов от загрузки вредоносных приложений
- Проверка образов контейнеров на наличие вредоносных объектов
- Защита файлового хранилища на Windows/Linux от вредоносных файлов
- Антивирусный плагин к стороннему веб/почтовому шлюзу. Список готовых интеграций доступен по запросу и постоянно пополняется.
- Антивирусный модуль к корпоративной системе документооборота, к сборочному конвейеру разработки ПО и иным системам, где требуется обеспечить проверку файлов на наличие вредоносного кода.



Недавние высшие награды от независимых тестовых лабораторий

...и многие другие – подробнее см. www.kaspersky.ru/top3!

Основные функции

- **Знаменитые технологии защиты «Лаборатории Касперского» эффективно обнаруживают вредоносное ПО и мгновенно реагируют на угрозы.**
- Фильтрация вредоносных, фишинговых и рекламных URL-адресов.
- Обнаружение объектов, которые упакованы несколькими разными упаковщиками. Поддерживаются тысячи различных форматов и версий упаковщиков и архиваторов.
- Передовые функции эвристического анализа и технологии обнаружения на базе машинного обучения.
- Обезвреживание зараженных файлов, архивов и зашифрованных объектов. Найденные угрозы можно как удалять полностью, так и, при возможности, «лечить» заражённый файл, удаляя лишь вредоносную часть кода.
- Обновление антивирусного движка: технологии обнаружения и алгоритм обработки обновляются или модифицируются в ходе обычных обновлений антивирусных баз.
- Поддержка взаимодействия с множеством сторонних платформ, в том числе Microsoft SharePoint, Amazon S3, Microsoft Azure, Nextcloud, ownCloud, Kubernetes и т.д.
- Эффективность «биг дата»: глобальная распределенная сеть Kaspersky Security Network предоставляет информацию о репутации файлов и интернет-ресурсов, обеспечивая более быстрое и надежное обнаружение угроз.
- Kaspersky Scan Engine обладает отличной пропускной способностью с возможностью быстрого масштабирования.
- Поддерживается кластерный режим работы, когда заказчик ставит себе в сеть несколько экземпляров KSEn и управляет ими через веб-интерфейс.
- Возможность взаимодействия по TLS при работе в режиме REST-like сервиса.
- Возможность настройки фильтрации с помощью модуля Format Recognizer — он может определять и пропускать файлы определенных форматов в процессе сканирования. Модуль поддерживает десятки форматов, в том числе исполняемые файлы, файлы Office, медиафайлы и архивы.

Новые возможности Kaspersky Scan Engine 2.1 (запущен в июне 2022 г.)

Безопасность и комплайенс:

- Многопользовательский режим и контроль доступа в зависимости от ролей
- Операционный аудит
- Поддержка аутентификации HTTP-клиентов с помощью API-токенов
- Защита от атаки перебором паролей в Web-UI

Улучшенный кластерный режим работы:

- Автоматическое удаление из кластера простаивающих узлов
- Поддержка гетерогенных кластеров (HTTP и ICAP)

Улучшенный функционал:

- Полная поддержка `systemd` при работе с сервисами (start/stop/status/restart)

Дополненная документация:

- Руководства по интеграции с SIEM-системами (MicroFocus ArcSight, Splunk)
- Руководства по интеграции с Oracle Solaris VScan, F5 Application Security Manager, GoAnywhere MFT, Dell Isilon OneFS.

Изменения системного журнала:

- Возможность отправки нескольким адресатам
- Фильтрация отправляемых событий

Изменения в архитектуре:

Scan Engine разделен на 2 модуля с возможностью их независимого релиза:

- AV-движок (KAV SDK)
- Продукт с полным функционалом (Scan Engine как обёртка над KAV SDK)

Это изменение упростит и ускорит запуск новых версий Scan Engine.

Бесплатная 30-дневная пробная версия!
Отсканируйте QR-код и закажите пробную версию KSEn, или же кликните по ссылке:
www.kaspersky.ru/partners/technology/contact

Новости о киберугрозах:
www.securelist.ru

Новости IT-безопасности:
business.kaspersky.ru

www.kaspersky.ru

Kaspersky Technology Alliances

Технологии «Лаборатории Касперского» предлагаются для интегрирования в сторонние аппаратные и программные продукты и сервисы. Все решения обеспечены профессиональным пред- и послепродажным обслуживанием.

Узнать больше: www.kaspersky.ru/oem

Version 7.0 – January 2024