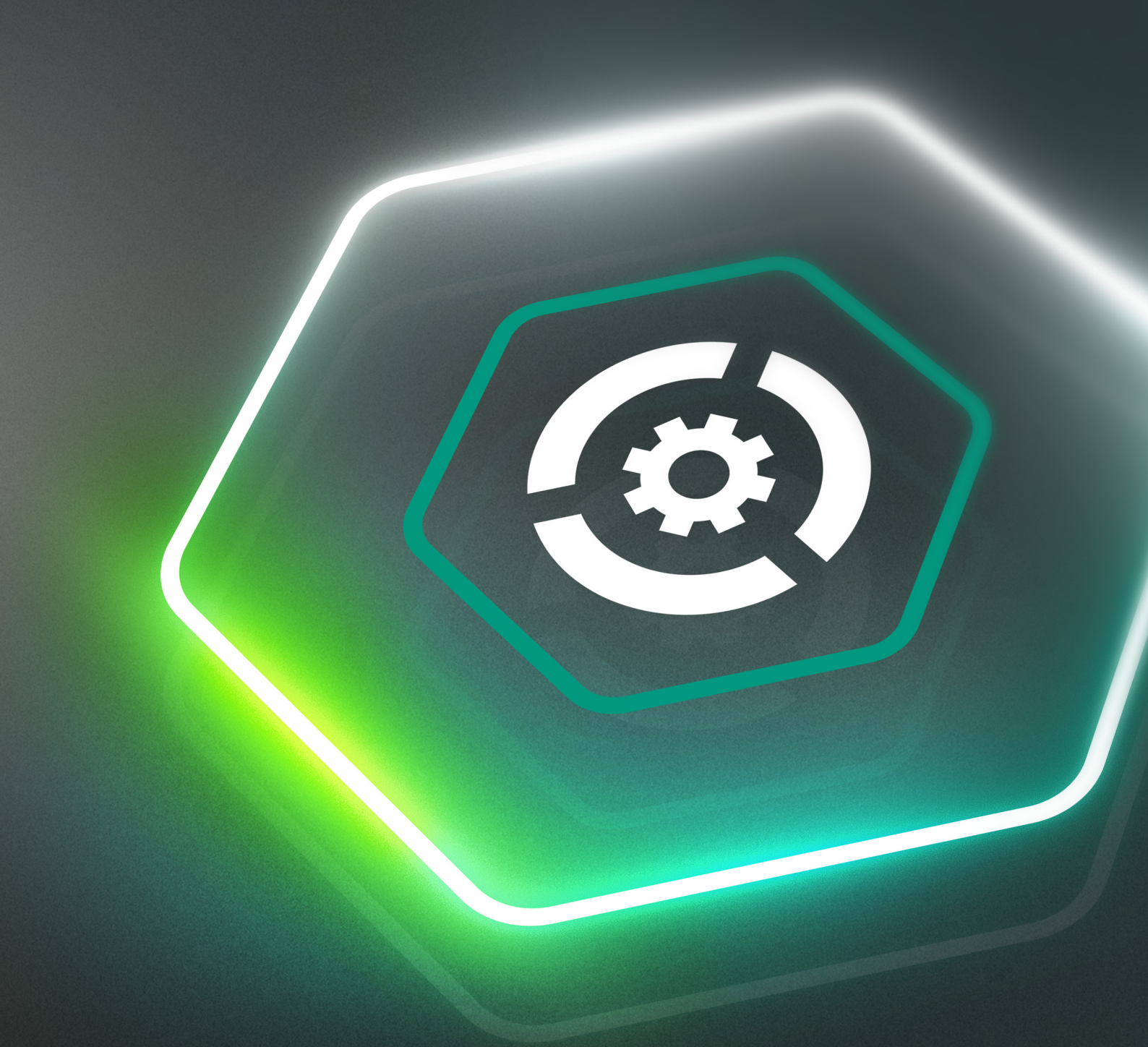


Решение для обнаружения
и блокировки киберугроз

Kaspersky Scan Engine

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Введение

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.

Отечественное ПО

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

Сценарии интеграции

- Веб-порталы и облачные серверы
- Файловые серверы
- Сетевые хранилища данных
- Почтовые серверы
- Сетевые шлюзы и прокси
- Магазины приложений и маркетплейсы

Основные возможности

Два режима работы

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.

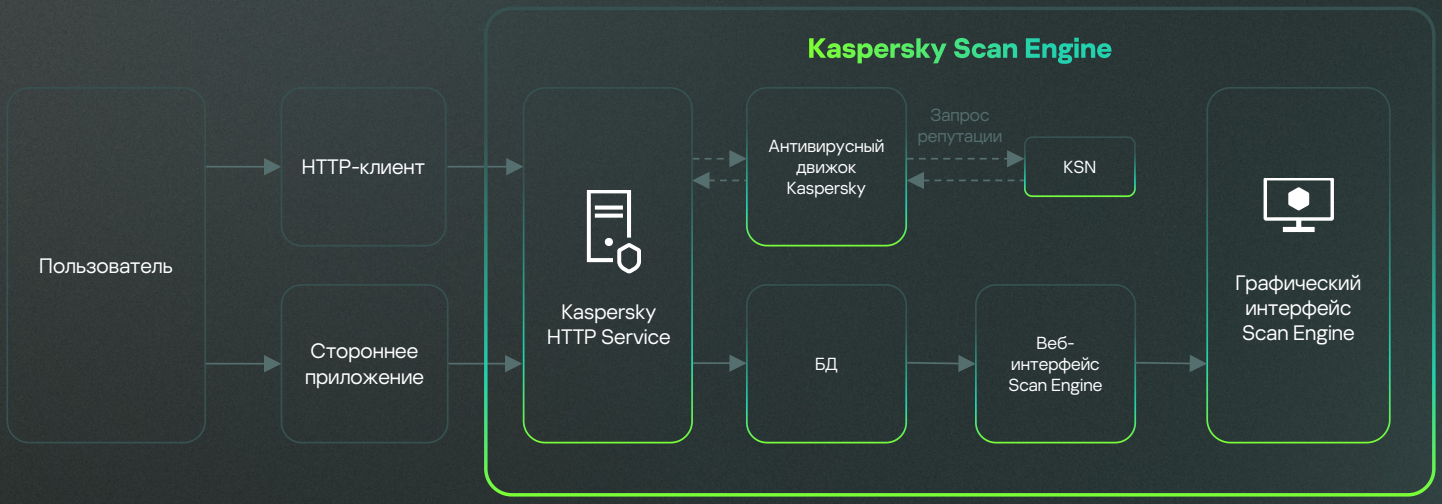
KSEn для Linux

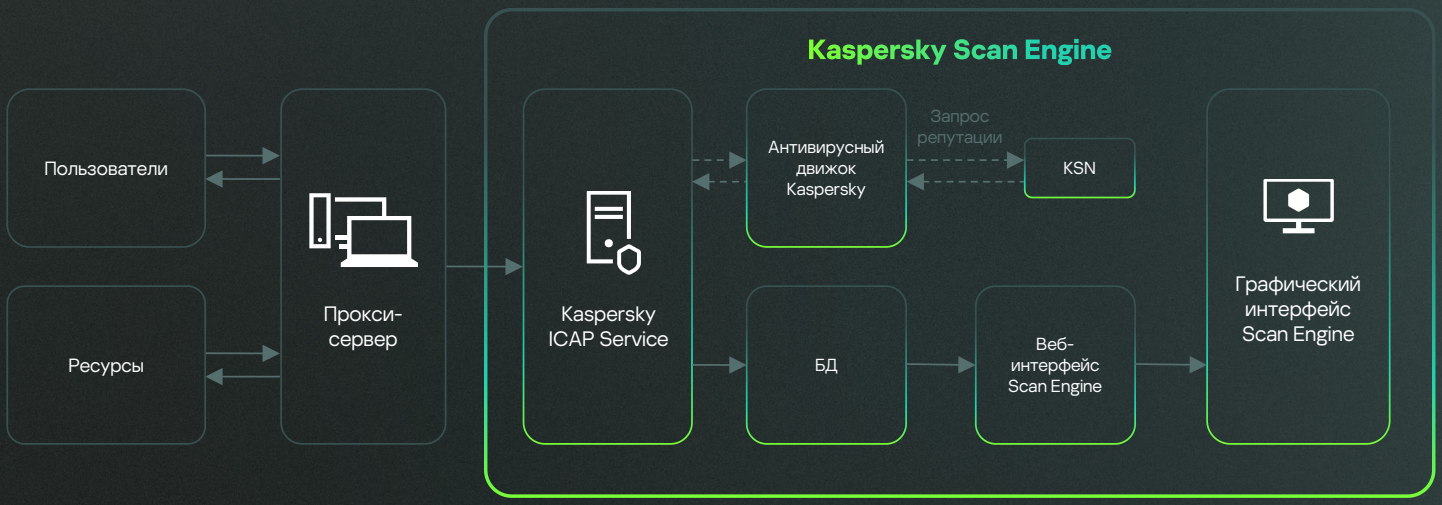
Также доступен в виде docker-контейнера (в HTTP- и ICAP-режимах) и может быть развернут в виде отдельного контейнера или в Docker Swarm, Kubernetes, AWS EKS, или любых аналогичных облачных средах.

Графический интерфейс

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

Сценарии использования





Интеграция с любым решением в сети

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 и других) облачных хранилищ от загрузки вредоносного контента.

Защита магазинов приложений и облачных маркетплейсов от загрузки вредоносных приложений.

Защита Microsoft SharePoint Server от загрузки вредоносного контента 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.

Основные функции

Знаменитые технологии защиты

Знаменитые технологии защиты «Лаборатории Касперского» эффективно обнаруживают вредоносное ПО и мгновенно реагируют на угрозы

Фильтрация

Фильтрация вредоносных, фишинговых и рекламных URL-адресов

Обнаружение

Обнаружение объектов, которые упакованы несколькими разными упаковщиками. Поддерживаются тысячи различных форматов и версий упаковщиков и архиваторов

Взаимодействие с платформами

Поддержка взаимодействия с множеством сторонних платформ, в том числе Amazon S3, Nextcloud, ownCloud, Kubernetes и т.д.

Обезвреживание файлов

Обезвреживание зараженных файлов, архивов и зашифрованных объектов. Найденные угрозы можно как удалять полностью, так и, при возможности, «лечить» зараженный файл, удаляя лишь вредоносную часть кода

Обновление

Обновление антивирусного движка: технологии обнаружения и алгоритм обработки обновляются или модифицируются в ходе обычных обновлений антивирусных баз

Передовые функции

Передовые функции эвристического анализа и технологии обнаружения на базе машинного обучения

Big Data

Эффективность Big Data: глобальная распределенная сеть Kaspersky Security Network предоставляет информацию о репутации файлов и интернет-ресурсов, обеспечивая более быстрое и надежное обнаружение угроз

Масштабирование

Kaspersky Scan Engine обладает отличной пропускной способностью с возможностью быстрого масштабирования

Настройки фильтрации

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

TLS в режиме REST-Like

Возможность взаимодействия по TLS при работе в режиме REST-like сервиса

Кластерный режим

Поддерживается кластерный режим работы, когда заказчик ставит в свою сеть несколько экземпляров KSEn и управляет ими через веб-интерфейс

Новые возможности Kaspersky Scan Engine 2.1

Запущен в июне 2022 года

Безопасность и комплаенс

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

Изменения в архитектуре

Scan Engine разделен на 2 модуля с возможностью их независимого релиза: AV-движок (KAV SDK) и продукт с полным функционалом (Scan Engine как обертка над KAV SDK) Это изменение упростит и ускорит запуск новых версий Scan Engine

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

Улучшенный функционал

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

Улучшенный кластерный режим работы

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

Изменения системного журнала

Возможность отправки нескольким адресатам. Фильтрация отправляемых событий

Наши награды

Недавние высшие награды от независимых тестовых лабораторий

Подробнее

Kaspersky Scan Engine

Бесплатная 30-дневная пробная версия!
Перейдите по ссылке и получите пробную версию KSEn

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее