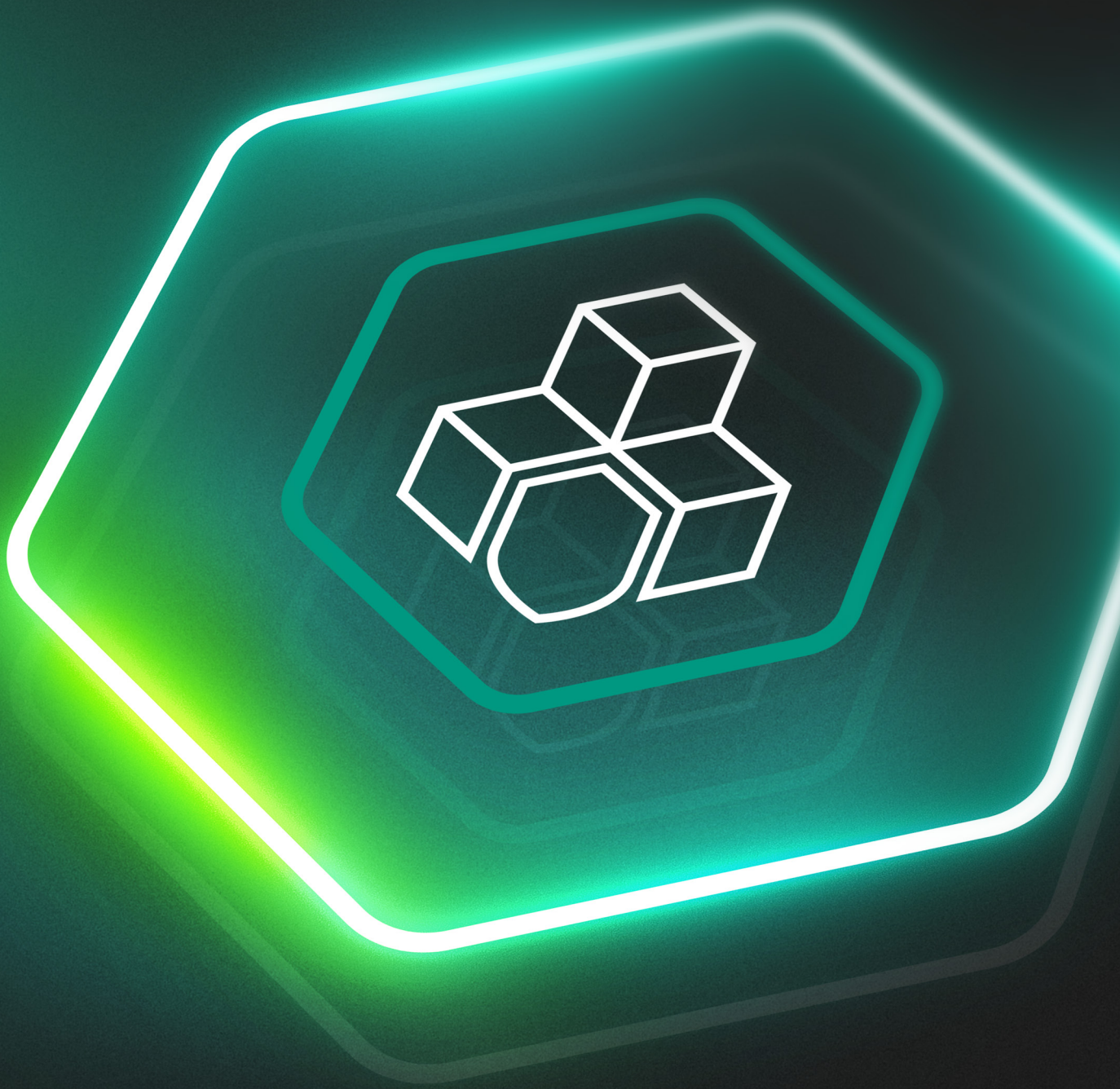

Описание возможностей

Kaspersky Container Security

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Ноябрь 23

Преимущества для бизнеса

Безопасность мирового уровня

- Возможности продукта соответствуют лучшим практикам защиты контейнерных сред
- Качественная защита, подтвержденная международными наградами

Всеобъемлющая защита контейнерных сред

- Защита на разных уровнях архитектуры контейнерных сред
- Безопасность приложений на всех этапах жизненного цикла

Отечественное ПО

- Решение от надежного российского вендора
- Внесен в Реестр отечественного ПО (№16222)

Соответствие требованиям

- Анализ уязвимостей по БДУ ФСТЭК
- Поддержка ОС Astra Linux и РЕД ОС

Введение

Kaspersky Container Security (KCS) — это решение, которое обеспечивает безопасность контейнерных приложений на всех этапах жизненного цикла: от разработки до эксплуатации. Продукт позволяет защитить бизнес-процессы организации, соответствовать стандартам и нормам безопасности, а также помочь реализовать принцип безопасной разработки ПО (DevSecOps).

С помощью Kaspersky Container Security можно высвободить ресурсы ИБ-службы для решения других задач и сократить время вывода продуктов на рынок благодаря всеобъемлющей защите от актуальных киберугроз и автоматизации проверок на соответствие требованиям.

Kaspersky Container Security спроектирован с учетом особенностей контейнерных сред и обеспечивает защиту на разных уровнях: от образов контейнеров до ОС хоста.

Уровни лицензирования

Два уровня защиты:

Kaspersky Container Security

Standard

Предоставляет защиту образов контейнеров, интеграцию с реестрами образов, оркестраторами и CI/CD-платформами, а также отслеживает статус контейнера

Advanced

Обеспечивает защиту контейнеров в среде выполнения, предоставляет улучшенные возможности мониторинга и инструменты проверок на соответствие требованиям регуляторов

Возможности и уровни лицензирования

Возможности	Standard	Advanced
Интеграция с реестрами образов контейнеров Интегрирация с Docker Hub, JFrog, Sonatype Nexus OSS, GitLab Registr, Harbor	●	●
Поддержка работы в средах оркестрации Поддержка работы в Kubernetes и OpenShift	●	●
Сканирование образов на вредоносные объекты, уязвимости и секреты Проверка может осуществляться как вручную, так и автоматизировано по заданным параметра	●	●
Оценка рисков для образов контейнеров и конфигурационный файлов (IaC) Автоматизированная оценка образов на основе уровней критичности	●	●
Сканирование конфигурационных файлов (IaC) Обнаружение ошибок в конфигурации и проверка на соответствие лучшим практикам	●	●
Настройка пользовательских политик и редактирование предустановленных в интерфейсе продукта Адаптация и доработка политик безопасности через UI без необходимости создания сложных правил и написания кода	●	●
Интеграция с CI/CD платформами и проверка образов на стадии разработки Продукт интегрируется с Jenkins, Team City и Circle CI и позволяет блокировать образы контейнеры при обнаружении угроз безопасности	●	●
Инструменты визуализации Визуализация информации об образах, контейнерах и элементах инфраструктуры	●	●
Система отчетности Формирование отчетов и возможность выгрузки из журнала по требованию	●	●
Интеграция с внешними системами безопасности и уведомлений Интеграция с SIEM (через syslog), LDAP, e-mail, Telegram	●	●
Мониторинг и контроль запуска образов контейнеров в соответствии с политиками безопасности Отслеживание образов контейнеров по набору заданных критериев безопасности и предотвращение их запуска при несоответствии политикам		●
Обнаружение и сканирование образов в кластере Возможность сканирования образов в рантайме		●

Возможности	Standard	Advanced
Поведенческий анализ контейнеров (на основе шаблонов) Контроль контейнеров согласно заданным профилям		●
Контроль запуска приложений и сервисов внутри контейнеров Выявление и блокирование подозрительной активности внутри контейнеров		●
Контроль трафика запущенных контейнеров Выявление и блокирование подозрительной активности между кластерами, а также между контейнерам в рамках одного кластера		●
Контроль целостности контейнеров Контроль соответствия просканированного системой образа и образа, из которого запущен контейнер		●
Анализ конфигурации компонентов контейнерной платформы на соответствие лучшим практикам и требованиям регуляторов Анализ инфраструктуры на соответствие стандартам CIS для повышения уровня защищенности среды		●
Визуализация ресурсов в кластере Отображение ключевой информации о состоянии кластера и его компонентов		●

Kaspersky Container Security

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее