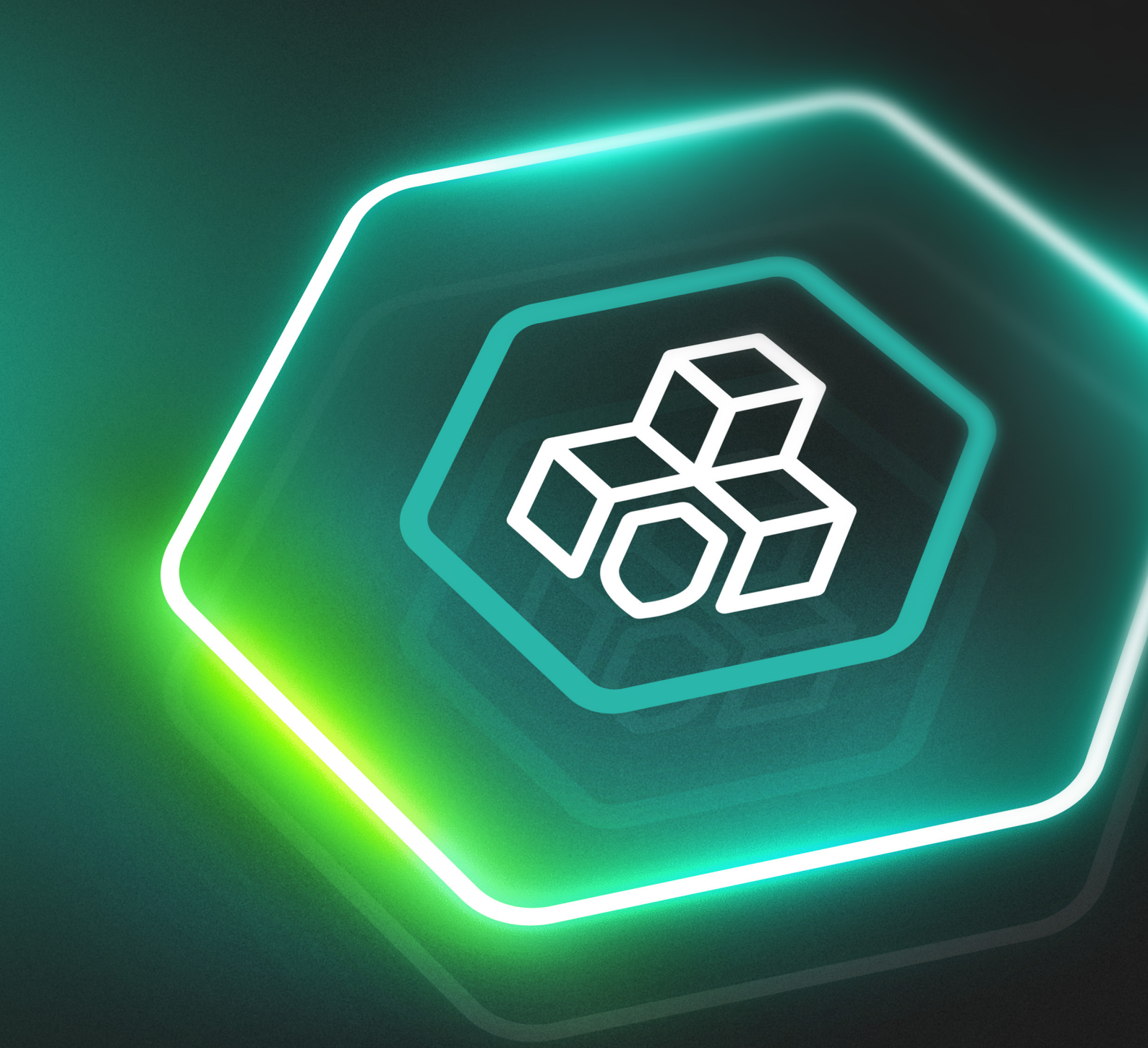


Лицензионное руководство

Февраль' 25

Kaspersky Container Security

Входит в

Kaspersky Cloud Workload Security

kaspersky активируй будущее

Контейнеризация

Один из главных мировых трендов в области разработки ПО. Большинство ведущих мировых компаний уже используют контейнеры в архитектуре приложений. Применение новой технологии позволяет ускорять процесс создания и доставки приложений пользователям, а также повышать отказоустойчивость продукта. Однако архитектурные особенности контейнерных сред не позволяют обеспечить защиту приложений традиционными или open-source-решениями анализа кода и защиты конечных точек.

Kaspersky Container Security

Kaspersky Container Security — 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 помогает 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, вне зависимости от их локального или облачного расположения, и обеспечивает защиту на разных уровнях: от образов контейнеров до ОС хоста.

Kaspersky Container Security является частью комплексного решения для всеобъемлющей защиты облачных нагрузок от киберугроз - Kaspersky Cloud Workload Security.

Уровни лицензирования

Kaspersky Container Security

Standard

Предлагает защиту образов контейнеров, интеграцию с реестрами образов, оркестраторами и CI / CD-платформами, а также с SIEM-системами

Base | Base Premium | Base Premium Plus

Kaspersky Container Security

Advanced

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

Base | Base Premium | Base Premium Plus

Base — лицензия с базовой технической поддержкой

Base Premium и Base Premium Plus — лицензии с сертификатом на расширенную техническую поддержку

Возможности и уровни лицензирования

Возможности	Standard	Advanced
Релиз 2.0		
Анализ конфигурации компонентов контейнерной платформы на предмет соответствия лучшим практикам Повышение уровня безопасности среды и готовности организации к угрозам	●	●
Анализ уязвимостей оркестратора Проверка кластеров и компонентов Kubernetes на соответствие политикам безопасности и мониторинг состояния кластера	●	●
Интеграция с реестрами образов Интегрируется с Docker Hub, JFrog Artifactory, Sonatype Nexus OSS, GitLab Registry, VMWare Harbor, Red Hat Quay, Amazon ECR	●	●
Поддержка сред оркестрации Поддерживает Kubernetes, Red Hat Openshift, Azure AKS, Amazon ECS	●	●
Интеграция с публичными облаками Поддерживает AWS, Microsoft Azure, Yandex Cloud	●	●
Сканирование образов на вредоносные объекты, уязвимости, секреты Сканирование может осуществляться вручную или автоматически на основе заданных параметров	●	●
Оценка рисков для образов контейнеров и конфигурационных файлов (IaC) Автоматизированная проверка образов на основе уровней критичности	●	●
Сканирование конфигурационных файлов (IaC) Обнаружение ошибок конфигурации и проверка на соответствие лучшим практикам	●	●
Набор критериев в UI для создания индивидуальных и редактирования предустановленных политик Автоматизированная проверка образов на основе уровней критичности	●	●
Интеграция с платформами CI/CD и проверка образов и IaC на стадии разработки Интегрируется с Jenkins, Team City and Circle CI для блокировки образов и контейнеров при обнаружении угроз безопасности	●	●
Инструменты визуализации Визуализация информации об образах, контейнерах и других элементах инфраструктуры	●	●
Система отчетности Создание отчетов и возможность загрузить их из логов	●	●
Интеграция с внешними системами безопасности и уведомлений Интеграция с SIEM (через системный журнал), LDAP, e-mail, Telegram	●	●
Открытое API для ключевой функциональности продукта (Swagger) Повышение удобства интеграции и установки	●	●

Релиз 2.0

Поведенческий анализ контейнеров

Формирование нормального профиля поведения контейнера как в автоматизированном, так и в ручном режиме

●

Контроль работы с файлами (eBPF)

Выявление изменения файлов (например, изменения прав и владельца, создание, модификация, история сохранения и т. д.)

●

Логирование системных вызовов хоста

Улучшение возможностей расследования событий, произошедших в системе до и после нарушения политики

●

Передача журналов событий напрямую из контролируемых кластеров в SIEM-системы

Помощь SOC-командам при расследовании сложных инцидентов

●

Специальная страница уязвимостей

Позволяет сфокусироваться на конкретных уязвимостях вне зависимости от их расположения в контейнерной среде

●

Мониторинг и контроль запуска образов контейнеров в соответствии с политиками безопасности

Решение может запрещать запуск нелегитимных образов, незарегистрированных образов и образов с привилегиями, а также устанавливать определенные хранилища данных в контейнеры

●

Обнаружение и сканирование образов в кластере

Может сканировать образы в рантайме

●

Контроль целостности контейнеров

Мониторинг целостности отсканированного образа и образа, из которого запущен контейнер

●

Защита от файловых угроз в контейнерах в рантайме (eBPF и KESL)

Предотвращение потенциальных атак на оркестратор через контейнеры в рантайме

●

Контроль запуска приложений и сервисов внутри контейнеров

Обнаружение и блокировка подозрительной активности внутри контейнеров

●

Мониторинг трафика запущенных контейнеров

Обнаружение и блокировка подозрительной активности между контейнерами в кластере и между кластерами

●

Анализ конфигурации компонентов контейнерной платформы на соответствие нормативным требованиям

Анализ инфраструктуры на соответствие внутренним и регуляторным требованиям безопасности

●

Визуализация ресурсов в кластере

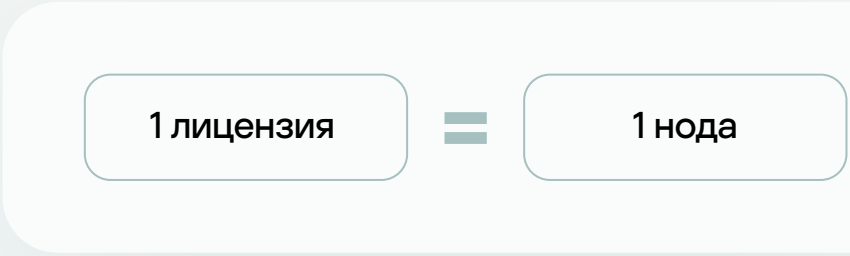
Просмотр ключевой информации о состоянии кластера и его компонентов

●

Объекты лицензирования

Количество нод (узлов) в рантайме

Учитываются ноды контейнерной инфраструктуры организации, на которых разворачивается агент защиты KCS Агент



Расширенная техническая поддержка

Для Kaspersky Container Security доступны два варианта расширенной технической поддержки: Premium и Premium Plus.

	Premium	Premium Plus
Прием запросов по инцидентам	Уровень критичности 1 — в режиме 24×7, остальные — с 10:00 до 18:30 (по Москве)	Уровень критичности 1 и 2 — в режиме 24×7, остальные — с 10:00 до 18:30 (по Москве)
Время реагирования на инциденты	Уровень критичности 1 — 2 часа* Уровень критичности 2 — 6 рабочих часов Уровень критичности 3 — 8 рабочих часов Уровень критичности 4 — 10 рабочих часов	Уровень критичности 1 — 30 минут* Уровень критичности 2 — 2 часа Уровень критичности 3 — 6 рабочих часов Уровень критичности 4 — 8 рабочих часов
Контактные лица	4 — возможное количество контактных лиц со стороны клиента	8 — возможное количество контактных лиц со стороны клиента Персональный технический менеджер Предоставление отчетов клиенту по открытым инцидентам

* В нерабочее время необходимо дополнительное обращение по телефону.

Примеры расчета количества лицензий

Сценарий 1

Необходимо обеспечить безопасность ТОЛЬКО контейнерных образов

Сценарий 2

Необходимо обеспечить безопасность не только контейнерных образов, но и запущенных приложений (рантайм) и проверку на соответствие

Всего у заказчика 810 нод, на 500 из которых планируется развернуть контейнеры.
Для расчета лицензий учитываются только те ноды, на которых разворачиваются контейнеры.

500 нод = 500 лицензий

500 нод = 500 лицензий

500 лицензий Kaspersky Container Security Standard Base / Premium / Premium Plus (MSA)*

500 нод = 500 лицензий

500 лицензий Kaspersky Container Security Standard Base / Premium / Premium Plus (MSA)*

Преимущества для бизнеса

Защита мирового уровня

- Возможности продукта отражают лучшие мировые практики защиты контейнерных сред
- Качественная защита, подтвержденная международными наградами
- Проверка на соответствие лучшим практикам безопасности

Соответствие требованиям регуляторов

- В Реестре отечественного ПО (№16222)
- Анализ уязвимостей по БДУ ФСТЭК

Простое управление – надежная защита

- Визуализация угроз в режиме реального времени
- Экономия ресурсов команд ИБ и ИТ за счет автоматизации проверок безопасности

Всеобъемлющая безопасность контейнерных сред

- Защита на разных уровнях архитектуры контейнерных сред
- Безопасность приложений на всех этапах жизненного циклажизненного цикла: от разработки до эксплуатации

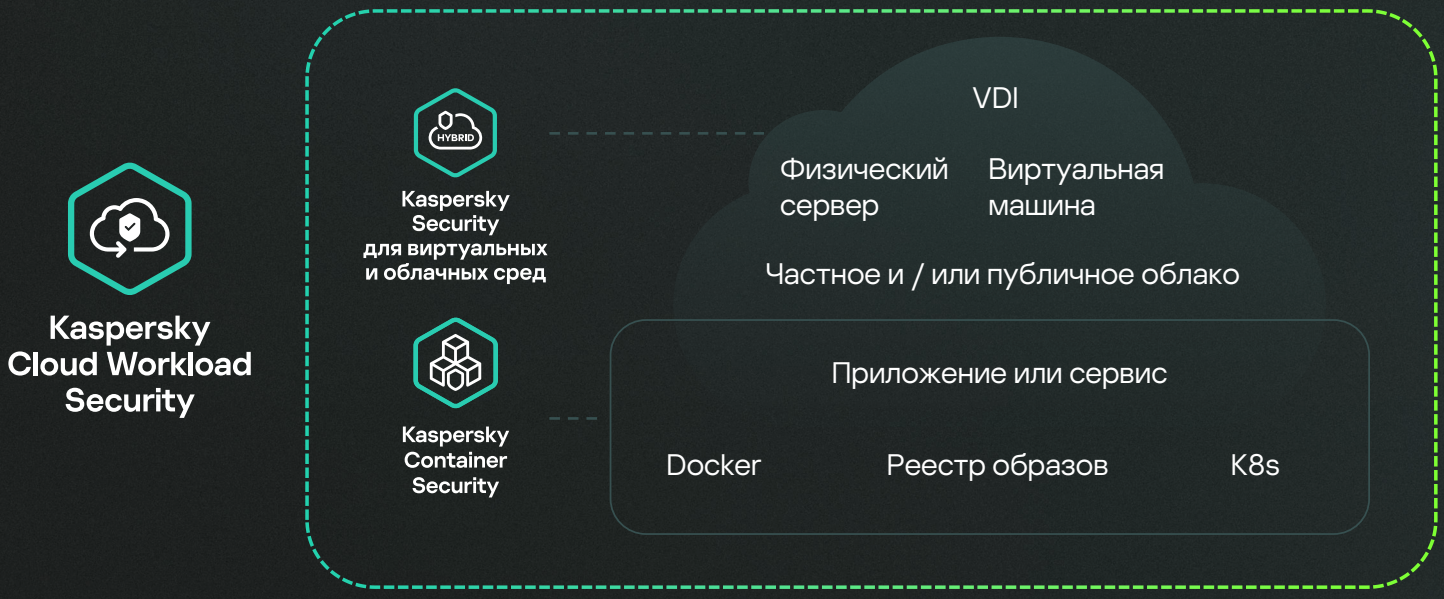
Технологическое лидерство и экспертиза мирового уровня

Kaspersky Cloud Workload Security опирается на знания, технологии и профессионализм трех из пяти Центров экспертизы компании (Центр исследования угроз, Центр исследования технологий искусственного интеллекта, Центр сервисов по кибербезопасности), предлагая реализацию методологий SSDLC и Secure-by-Design, защиту от продвинутых угроз и помощь SOC-командам.

* Лицензия с включенным соглашением о сервисном обслуживании (MSA) предлагает варианты расширенной и премиальной поддержки, позволяющие решать проблемы в области ИТ-безопасности с высоким приоритетом и обеспечивать непрерывность бизнес-процессов в вашей организации.

Компонент Kaspersky Cloud Workload Security

Kaspersky Container Security вместе с Kaspersky Security для виртуальных и облачных сред входят в состав решения для всеобъемлющей защиты облачных нагрузок Kaspersky Cloud Workload Security. Комплексное решение обеспечивает безопасность всей гибридной и облачной инфраструктуры клиентов: хостов гипервизоров, виртуальных машин, контейнеров, оркетраторов и других компонентов.



Система управления состоянием безопасности облака (CSPM)*

Совместимость

Kaspersky Hybrid Cloud Security

Публичные облачные платформы

Google Cloud, aws, Microsoft Azure, Yandex Cloud

Платформы виртуализации

vmware, PROXMOX, Red Hat Enterprise Linux, Microsoft Hyper-V, HUAWEI, AOS, KVM

Инфраструктура виртуальных рабочих столов (VDI)

vmware, citrix, TERMIDESK

Kaspersky Container Security

Оркестраторы

kubernetes, Deckhouse, Amazon ECS, OPENSHIFT

Реестры образов

dockerhub, Red Hat Quay, GitLab, Amazon ECR, HARBOR, JFrog, nexus repository

Платформы CI / CD

Jenkins, TeamCity, GitLab, circleci

* В перспективе

Kaspersky Container Security

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее