Kaspersky Container Security

12 сентября, 11:00 МСК

СТРИМ

На одной волне с DevSecOps

Безопасность контейнерных сред с Kaspersky Container Security 1.2. Обзор обновления

Программа стрима

- Контейнеризация: преимущества и риски
- Краткий обзор Kaspersky Container Security
- Версия 1.2. Что нового?
- Планы на 2025 год
- Kaspersky Container Security как часть комплексной защиты облачных рабочих нагрузок
- Демонстрация новых возможностей
- Сессия вопросов и ответов

Тайминг: ~1 час

Антон Русаков-Руденко,
PMM по Kaspersky Container Security

Андрей Ветров,
Старший тренер по продуктам

Контейнеры

Использование контейнеров

84%

компаний используют контейнеры в различных средах*

85%

компаний сталкиваются минимум с одним инцидентом в среде Kubernetes в течение года**

Контейнеры многократно увеличивают преимущества CI/CD

- Ускорение написания, отладки и запуска релиза
- Повышение стабильности работы приложения
- Снижение требований к инфраструктуре как разработчика, так и заказчика
- Удобное масштабирование

*CNCF, Annual Report 2023, 2024
** Kaspersky. Managing Geo-Distributed businesses, 2024

Основные риски ключевых компонентов контейнерных сред

Образы

Открытые внешние источники

Уязвимости ПО

Ошибки в конфигурациях

Вредоносное ПО

Секреты в открытом виде

Использование недоверенных образов

Реестр образов

Незащищенное подключение

Наличие устаревших образов с уязвимостями и вредоносным ПО

Недостаточные ограничения на аутентификацию и авторизацию

Оркестратор

Не ограничен административный доступ

Доступ без авторизации

Отсутствует или слабое разделение трафика между контейнерами

Не разнесены по хостам контейнеры с разным уровнями защиты данных

Ошибки в конфигурации оркестратора

Контейнеры

Уязвимости среды выполнения

Неограниченный доступ контейнеров к сети

Небезопасные конфигурации

Уязвимости приложений в контейнерах

Незапланированные контейнеры в среде выполнения

ОС хоста

Большая площадь атак

Общее ядро ОС для всех контейнеров

Уязвимости компонентов ОС

Некорректная настройка прав доступа пользователей

Возможность доступа контейнеров к файловой системе

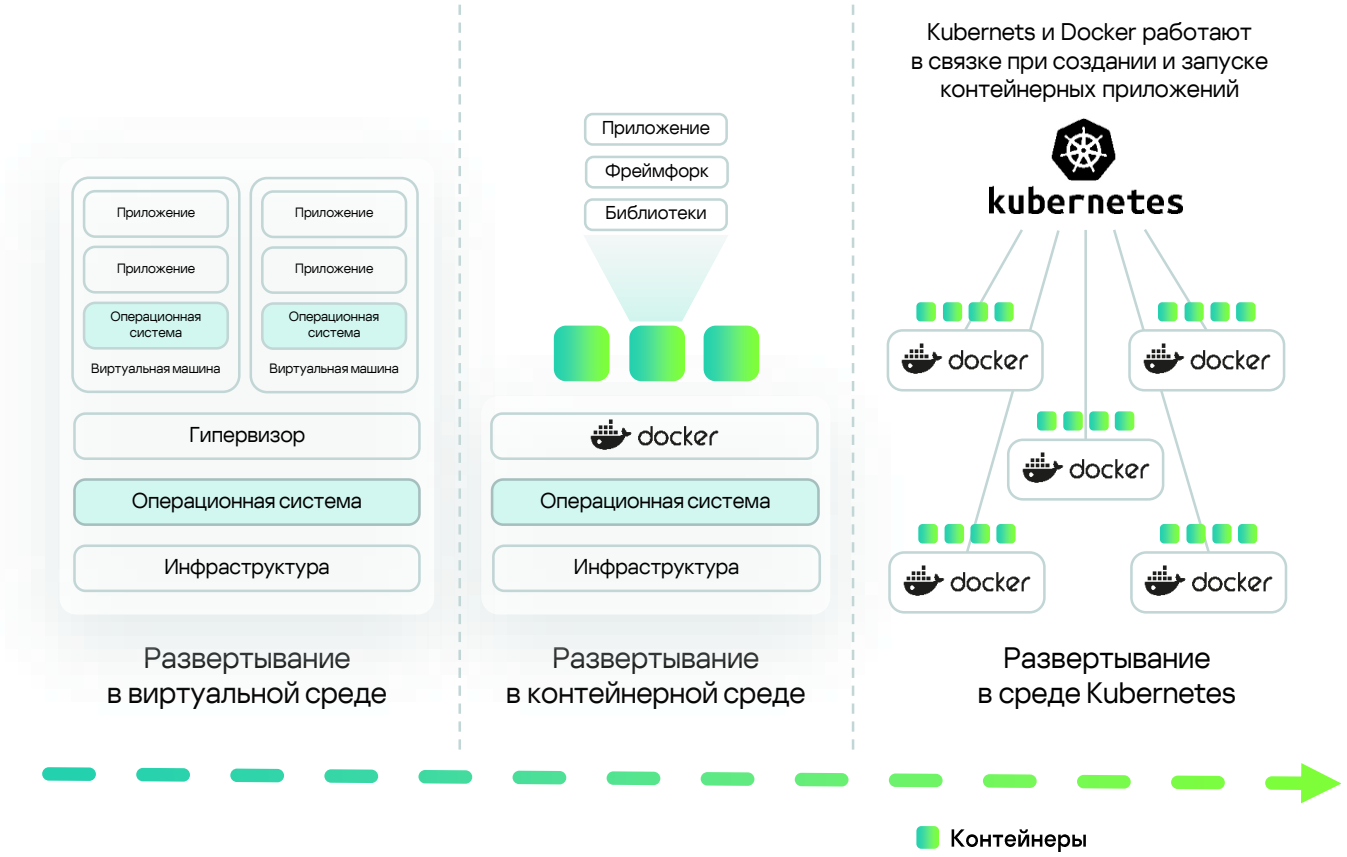
Сравнение Container Security и VM security

Традиционные средства защиты VM не эффективны для контейнеров

Традиционные средства защиты приложений разрабатывались под другие платформы (VM, bare metal) и не могут обеспечить защиту контейнерных платформ ввиду различий в архитектуре, в частности отсутствие операционной системы в каждом контейнере

Только специализированное решение Container Security обеспечивает полную безопасность данных сред

CS способен обеспечить безопасность современных приложений, построенных с использованием контейнеров и оркестраторов



Kaspersky Container Security

Закрывает проблемы безопасности контейнерных сред на всех этапах

KCS обеспечивает безопасность всех компонентов контейнерных платформ: образы, реестры образов, оркестраторы, контейнеры, ОС хоста

Позволяет интегрироваться в процессы безопасной разработки

Встраивается в CI pipelines и интегрируется в инфраструктуру

Закрытие рисков ключевых компонентов контейнерных сред

Образы

Проверка на уязвимости

Проверка на ошибки в конфигурациях образов

Проверка на вредоносное ПО

Проверка на секреты

Оценка рисков и выявление потенциально опасных образов

Реестр образов

Интеграция с реестрами и проверка образов в соответствии с политиками сканирования

Использование актуальных безопасных образов

Оркестратор

Обнаружение ошибок конфигурации и выдача рекомендаций по их исправлению

Визуализация ресурсов в кластере

Мониторинг трафика

Обнаружение и сканирование образов в кластере

Контейнеры

Контроль запуска и работы только доверенных контейнеров

Мониторинг трафика

Контроль целостности контейнеров

Контроль запуска приложений и сервисов внутри контейнеров

Поведенческий анализ на основе шаблонов

ОС хоста

Обнаружение ошибок конфигурации и рекомендации по исправлению

Уменьшение рисков за счет контроля запуска и работы контейнеров

Сценарии использования Kaspersky Container Security

При разработке приложений на микросервисной архитектуре

Безопасность приложений/сервисов в контейнерах, среды выполнения и платформ оркестрации

При выстраивании процессов DevSecOps

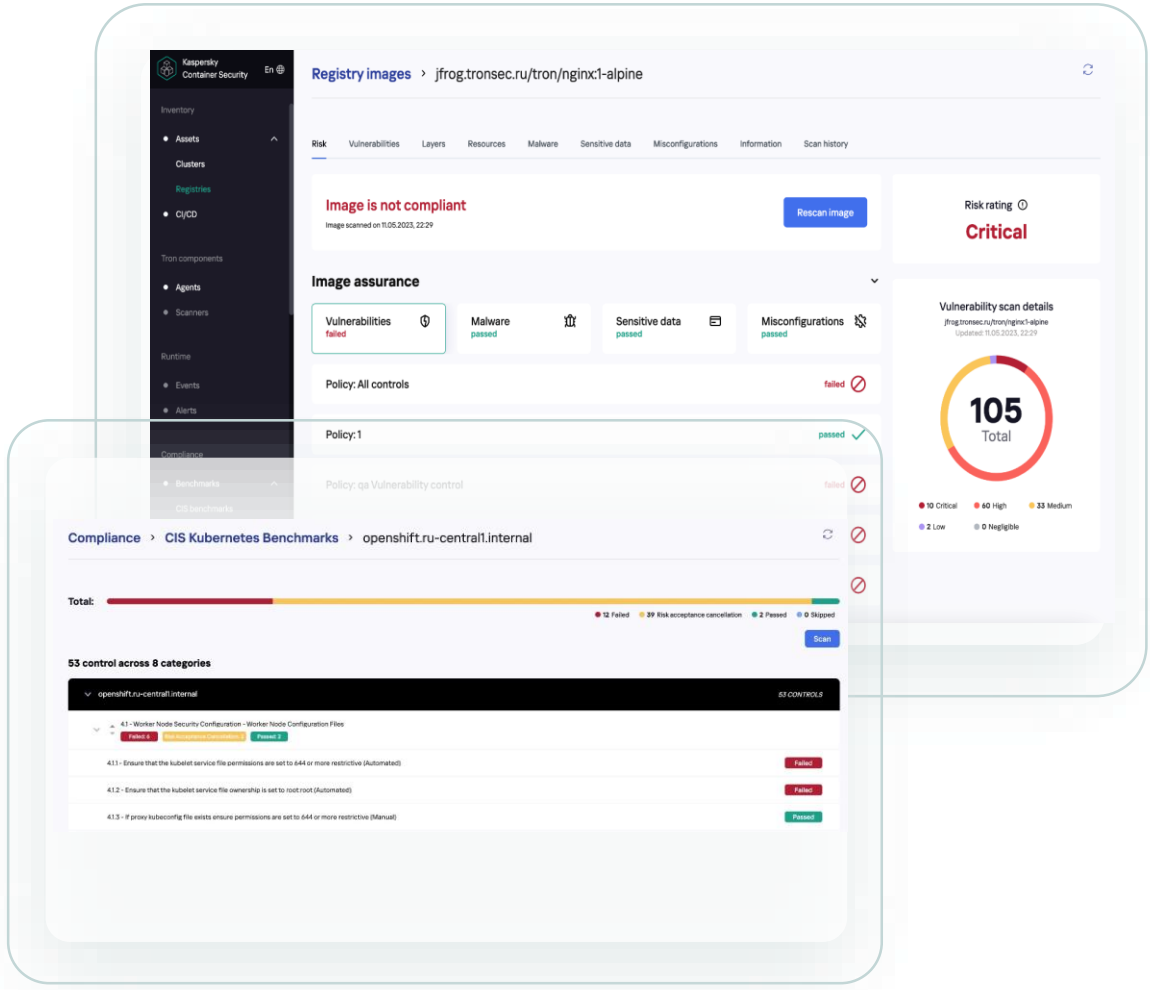
Добавление «quality gate» требует проверки собираемых контейнеров

При необходимости соблюдения Compliance

KCS позволяет автоматизировать процесс проверки на соответствие стандартам и требованиям регуляторов

Для инвентаризации и визуализации

Компонентов контейнерной инфраструктуры и ресурсов в кластерах



Обзор новых возможностей и планов

Новые возможности Kaspersky Container Security

Q2 2024

Версия 1.2

- Runtime защита контейнеров от файловых угроз с использованием агента защиты (KESL)
- Открытое API для ключевых возможностей продукта
- Поддержка работы с публичными облаками
- Поддержка больших инфраструктур
- Скрипт интеграции с CI/CD платформами (для TeamCity, Jenkins)
- Поддержка Harbor Scanner API
- Визуализация трафика между контейнерами, компонентами платформы контейнеризации, внешними сервисами и ресурсами

Runtime защита контейнеров от файловых угроз с использованием агента защиты (KESL)

Возможности

- Проверка файлов, контейнеров, образов и пространств имен как в реальном времени, так и по требованию
- Обнаружение зараженных объектов и автоматическое обезвреживание угроз

Выгода для бизнеса

- Своевременное обнаружение и пресечение вредоносной активности
- Минимизация ущерба продукту, сервису или инфраструктуре
- Предотвращение потенциальной атаки на ПО

Расширение интеграционных возможностей

Открытое API для ключевых возможностей продукта

Возможности

- Проверка образов по запросу
- Создание агент групп
- Получение данных для отображения в собственной BI системе

Выгода для бизнеса

- Ускорение интеграции и развертывания продукта
- Расширенные возможности мониторинга состояния защиты и инфраструктуры
- Поддержка больших инфраструктур

Поддержка работы с публичными облаками

Возможности

- Интеграция с AWS, MS Azure и Yandex Cloud
- Поддержка Yandex Registry и Docker Registry API

Выгода для бизнеса

- Защита облачных инсталляций контейнерной инфраструктуры

Kaspersky Container Security – планы на ближайший релиз

Q4 2024 (TR)

Версия 2.0

- Развитие возможностей API:
  - проверка состояния компонентов продукта
  - действия с политиками
  - работа с профилями образов
  - импорт / экспорт конфигураций продукта
- Интеграция с менеджерами секретов (Hashi Vault)
- Логирование syscalls хоста для целей расследования
- Автоматическое построение профилей образов
- Поддержка кластеров с количеством узлов до нескольких тысяч
- Логирование дополнительных полей в событиях рантайма
- Отслеживание файловых операций в рантайме (eBPF)
- Защита от файловых угроз узлов оркестратора
- Анализ на проблемы безопасности параметров оркестратора

* Возможны изменения

Решение проблем целевой аудитории

Выгоды для ИБ

- Наглядность инфраструктуры
- Сокращение рутинных действий
- Соответствие требованиям регуляторов
- Безопасность инфраструктуры

Выгоды для ИТ

- Наглядность инфраструктуры
- Сокращение ИТ-инцидентов
- Оптимизация использования ресурсов
- Повышение производительности приложений и сервисов

Выгоды для разработчиков

- Ускорение релизного цикла
- Защита среды рантайма
- Автоматизация проверок на безопасность
- Поддержка практик DevSecOps

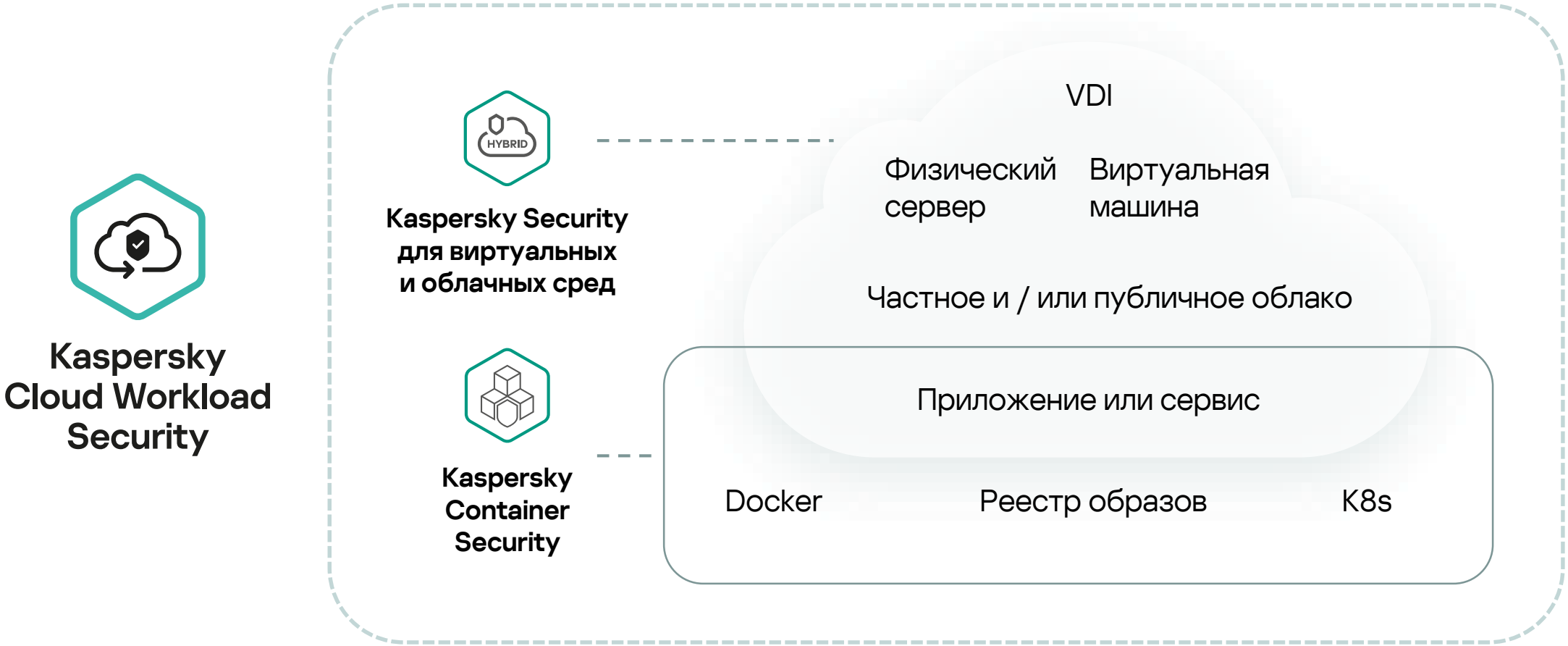
Компонент

Kaspersky Cloud Workload Security

Ключевые возможности

- Обзор 360° как в облаках, так и в контейнерной среде
- Гибкое лицензирование
- Экономия вычислительных ресурсов
- Автоматизация проверок на безопасность
- Всесторонняя защита рабочих облачных нагрузок
- Соответствие требованиям регуляторов

Kaspersky Cloud Workload Security: архитектура



Система управления состоянием безопасности облака (CSPM)
(в перспективе)

Приглашаем продолжить общение