kaspersky

Kaspersky Cloud Workload Security

Содержание

- Цифровая трансформация
- Вкратце о наших продуктах:
  - Kaspersky Security для виртуальных и облачных сред
  - Kaspersky Container Security
- Kaspersky Cloud Workload Security: новое решение в портфолио
- Демо: комплексные сценарии защиты облачных сред с помощью Kaspersky Cloud Workload Security
- Вопросы

Тайминг: ~1 час

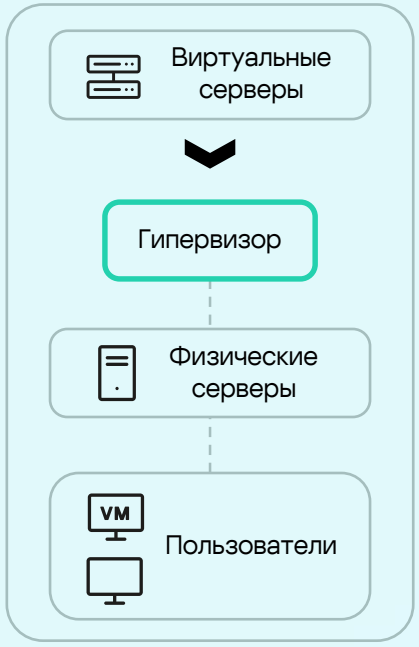
Антон Русаков-Руденко
PMM Cloud Workload Security

Вячеслав Старшинов,
Solutions Expert, Endpoint Security

Основные типы ИТ-инфраструктур

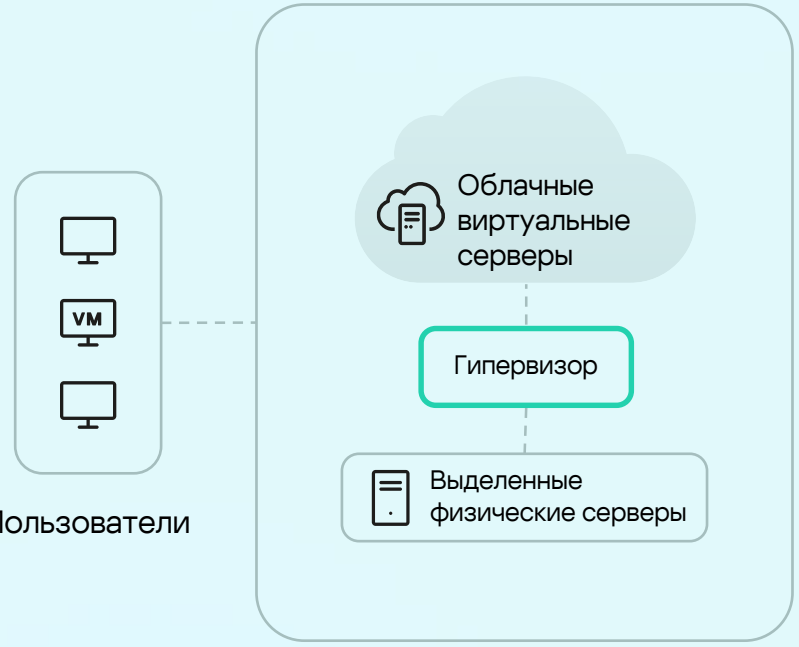
Типовые инфраструктуры

On-premise



IT-инфраструктура организации

Частное облако



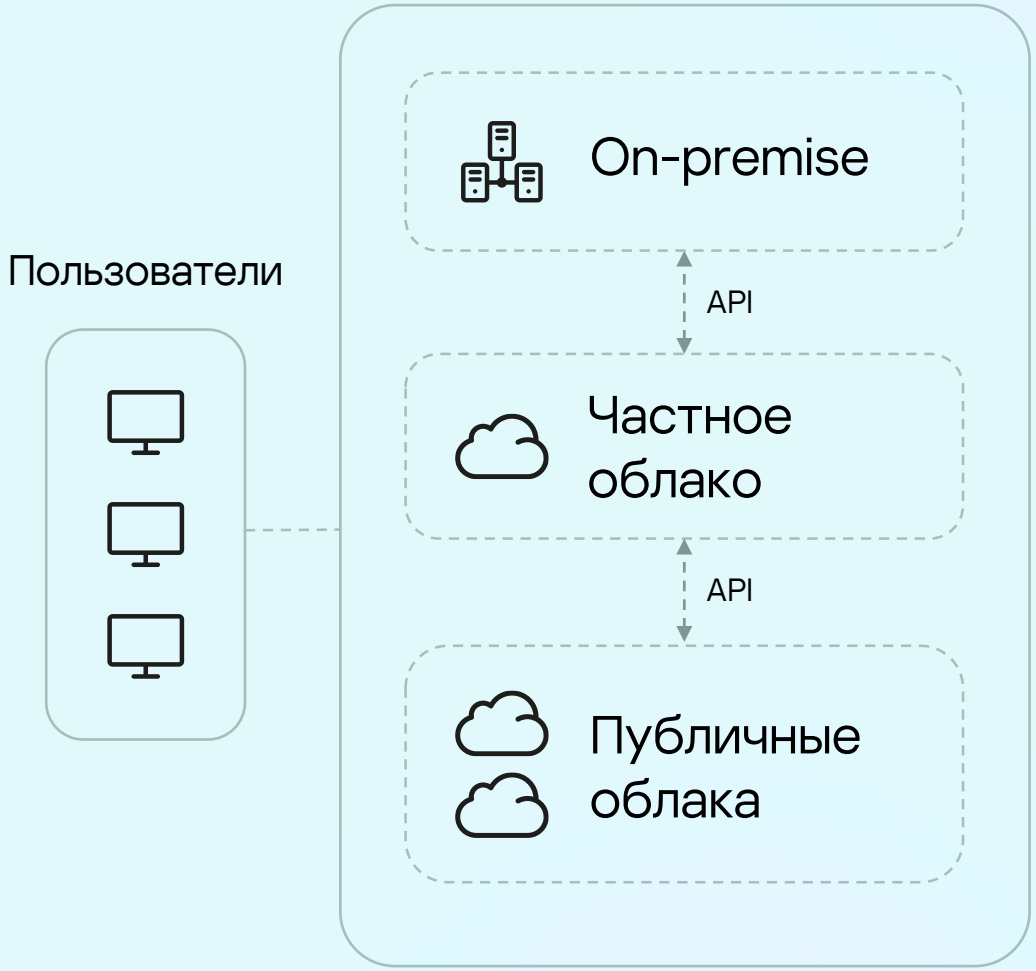
Организация

Поставщик облачного сервиса

Публичное облако

Инфраструктура поставщика облачного сервиса

Гибридная облачная инфраструктура



Преимущества

- Доступность данных
- Гибкость и масштабируемость
- Скорость

Недостатки

- Сложность
- Непрозрачность
- Контроль расходов

Миграция
в облако

Облака уже обыденность

>90% организаций используют тот или иной тип облачных сред*

72%

организаций используют гибридные облачные среды**

75%

организаций считают миграцию в облака эффективной***

28%

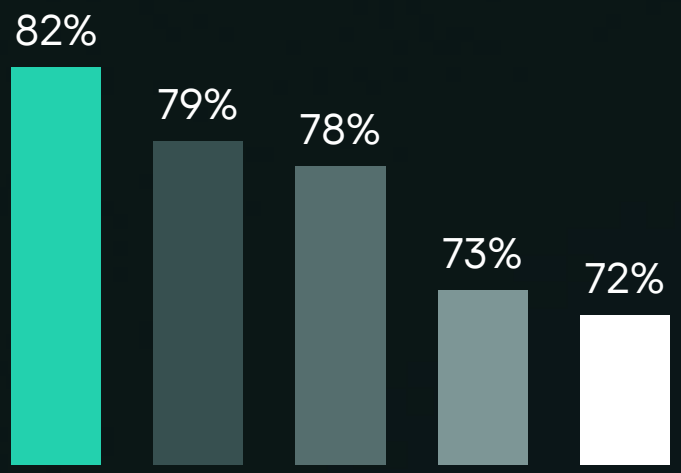
инвестиций в публичные облака были неэффективны **

* AAG. The Latest Cloud Computing Statistics, 2023
** Flexera. State of the Cloud Report, 2023
*** Infosys. Cloud radar, 2023

Миграция в облако не всегда проходит гладко

Вызовы*

- Управление затратами на облако
- Безопасность
- Недостаток ресурсов или экспертизы
- Соответствие требованиям
- Управление лицензиями ПО



* Flexera. State of the Cloud Report, 2023

Как решают задачу

Размещают критичные приложения и сервисы в локальной инфраструктуре

Откатываются назад к полностью локальной инфраструктуре

Мигрируют в национальное облако

Основные риски облачных сред

- Ошибки в конфигурациях
- Несанкционированный доступ
- Небезопасные API
- Перехват учетных записей
- Отсутствие прозрачности происходящих процессов
- Незащищенный обмен данными с внешними пользователями
- Целевые кибератаки
- DoS-атаки
- Человеческий фактор

Требования к решениям по защите облаков

	Open source	Встроенная безопасность в бизнес-решения	Решения типа EDR	Решения по защите гибридных облаков	CWS (CWPP)
Интеграция с облаками (частными/публичными)	в зависимости от решения	в зависимости от решения		•	•
Поддержка мультиоблачной инфраструктуры				•	•
Защита контейнеров	частично			частично	•
Интеграция с защитными решениями	частично	• (по API)	•	•	•
Визуализация облачных нагрузок	частично			•	•
Защита бессерверных вычислений					•
Единая консоль мониторинга и управления				в зависимости от решения	•
Соответствие требованиям регуляторов	частично	частично	•	•	•

Kaspersky Security для виртуальных и облачных сред

Решение, специально созданное для гибридных облачных сред

Многоуровневая защита от угроз

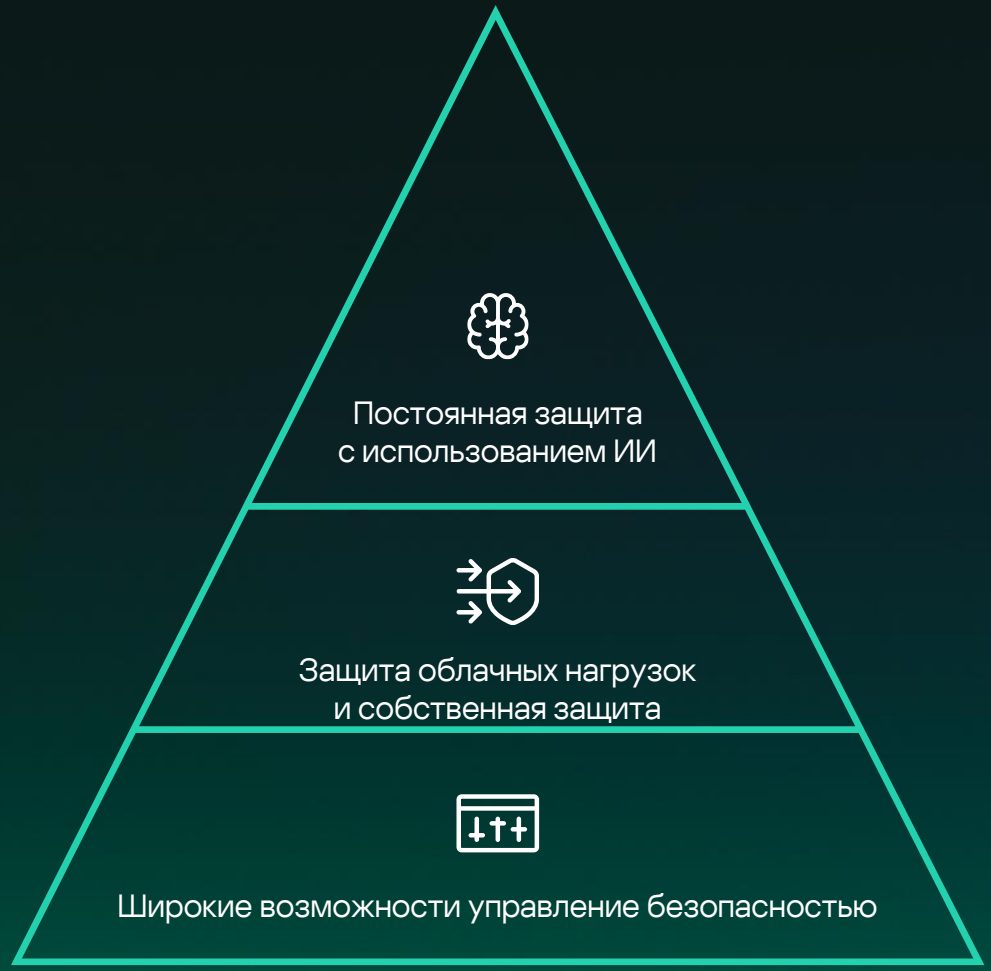
Проактивно противодействует большинству кибератак, в том числе вредоносному ПО, фишингу и другим угрозам.

Алгоритмы машинного обучения

и богатый опыт наших экспертов обеспечивают высокий уровень обнаружения угроз при минимальном количестве ложных срабатываний.

Данные об угрозах, получаемые в реальном времени

позволяют защитить инфраструктуру от новейших эксплойтов.



Поддержка любых платформ

Защита всей облачной инфраструктуры, вне зависимости от варианта размещения рабочих нагрузок – физические и виртуальные среды, частные, публичные и гибридные облака.

Публичные облака — Google Cloud, aws, Microsoft Azure

Частные облака — vmware, KVM, Red Hat Enterprise Linux

VDI — vmware, citrix, TERMIDESK

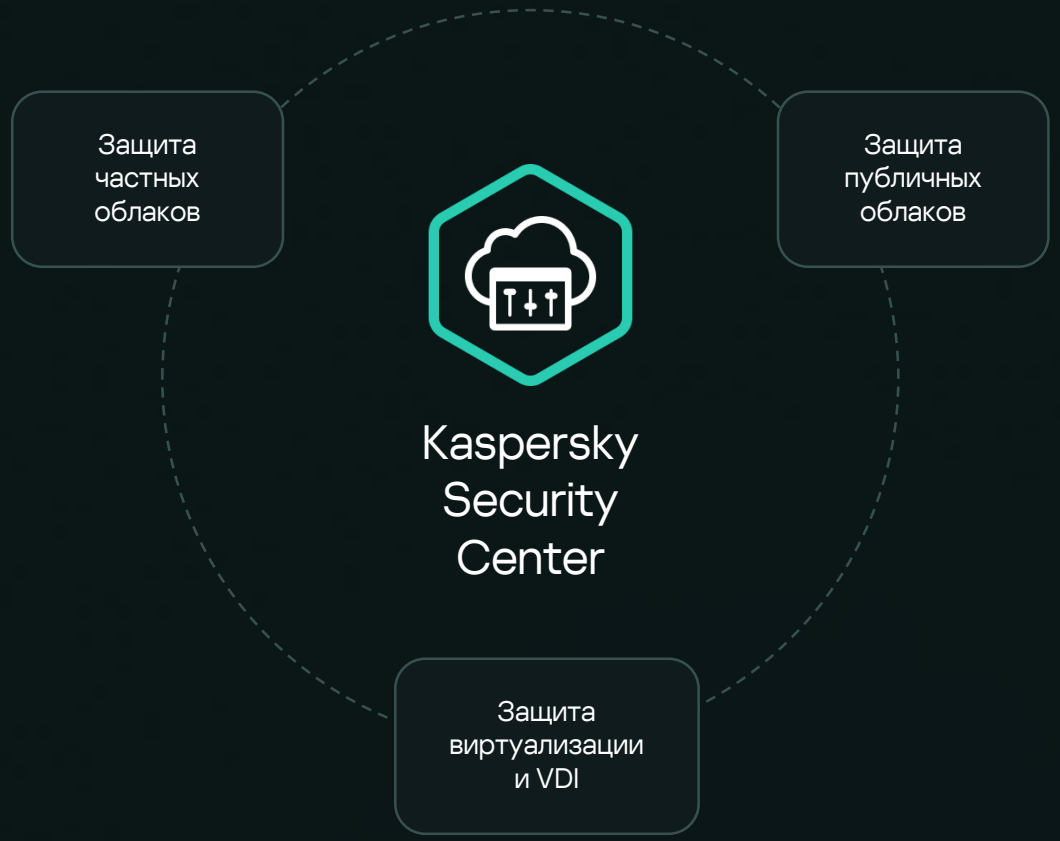
Минимальное воздействие на производительность

- Легкие агенты, оптимизированные для работы с каждой ОС, снижают потребление ресурсов виртуализации на 30%.

×3	×2	×2
Эффективнее использование CPU	Эффективнее использование памяти	Эффективнее использование HDD

- Использование общего кеша, в котором хранится информация о проверках файлов, позволяет сократить объем обрабатываемых данных и количество выполняемых действий.
- Интеграция с публичными облачными службами через API и политики автоматического масштабирования позволяют существенно сэкономить время и ресурсы

Без слепых зон



Единая консоль
управления всеми облачными ресурсами

Делает управление безопасностью всей инфраструктуры более простым, сохраняя время и ресурсы ИТ/ИБ-команд.

Технологии комплексной защиты

от самозащиты агентов до оценки уязвимостей и автоматизированной установки исправлений, непрерывно обеспечивают соответствие нормативным требованиям.

Широкий набор возможностей

позволяет управлять рисками и выполнять нормативные требования.

- Иерархия управляющих серверов
- Несколько вариантов развертывания
- Отчетность и анализ журналов
- Контроль доступа на основе ролей
- Самозащита агента и его защита паролем
- Оценка уязвимостей и автоматизированная установка исправлений
- Прозрачное для пользователя шифрование, сертифицированное по стандарту FIPS 140-2
- Укрепление системы
- Контроль устройств
- Настраиваемая защита от вредоносного ПО и персональные сетевые экраны

Kaspersky
Container Security

~80%

компаний в мире используют контейнеры в различных средах*

~90%

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 (Cloud Native Computing Foundation), 2022
** Red Hat Datalog 2023

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

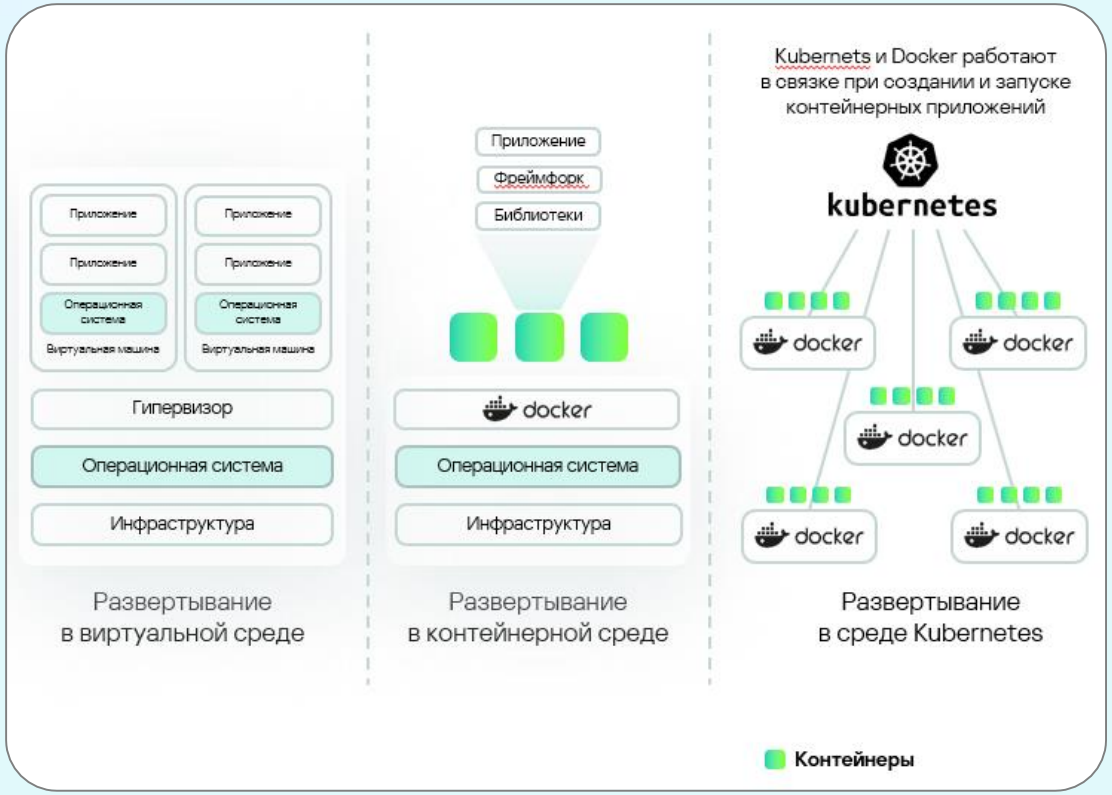
Сравнение Container Security и VM security

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



Решение контейнерной безопасности

Закрывает проблемы безопасности контейнерных сред на всех этапах

Kaspersky Container Security 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

IИнтеграция 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

Kaspersky Container Security - roadmap

Q2 2024

Версия 1.2

- Повышение надежности работы продукта
- 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
- Run-time защита контейнеров от файловых угроз с использованием агента защиты (KESL)
- Открытое API для ключевого функционала продукта
- Поддержка работы с публичными облаками

Q4 2024

Версия 1.3*

- Расширение интеграционных возможностей как с защитными решениями, так и с облачной и контейнерной инфраструктурой
- Улучшенные технологии защиты на стадии запуска и работы контейнеров
- Улучшение и расширение возможностей визуализации
- Логирование всех syscalls хоста
- Улучшение политик безопасности

* Возможны изменения

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

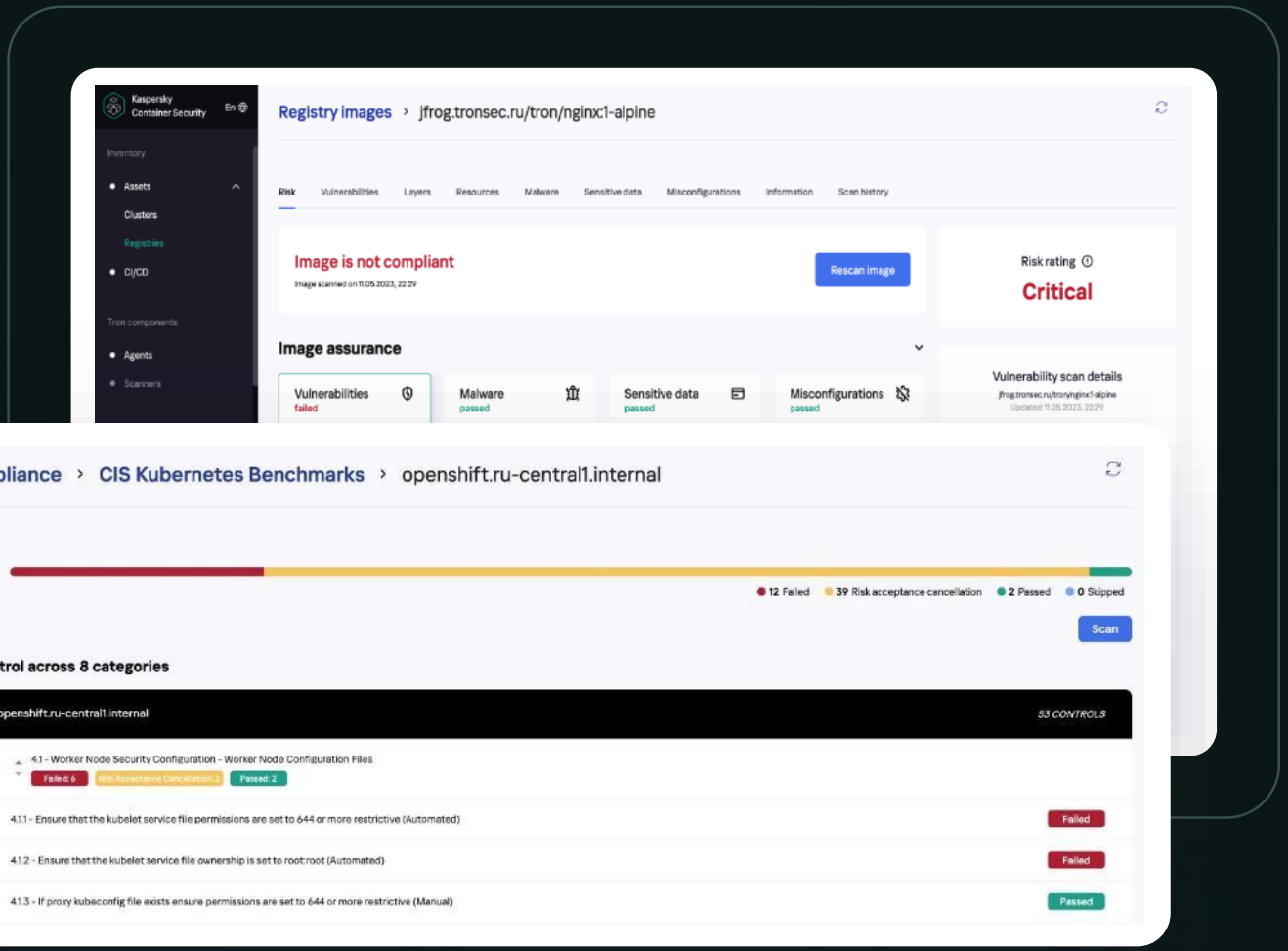
Добавление «quality gate» требует проверки собираемых контейнеров

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



Kaspersky
Cloud Workload Security

Kaspersky Cloud Workload Security: обзор

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

Ключевые возможности

- Контроль приложений
- Управление уязвимостями
- Защита от файловых угроз
- Защита памяти
- Сегментация сети
- Контроль целостности
- Система предотвращения вторжений
- Расширенное обнаружение и реагирование
- Поведенческий анализ
- Защита от эксплойтов
- Защита от вредоносного ПО и фишинга
- Защита DevOps

Как Kaspersky CWS решает проблемы целевой аудитории

Для ИБ-команд

Безопасность облачной инфраструктуры

Повышение прозрачности процессов

Автоматизация рутинных операций

Поддержка соответствия требованиям регуляторов

Для ИТ-команд

Оптимизация вычислительных ресурсов

Увеличение производительности

Повышение прозрачности всей инфраструктуры

Сокращение количества ИТ-инцидентов

Для команд разработки

Подход Shift-left

Защита в рантайме

Автоматизация проверок

Прозрачность и кооперация

Гибкое лицензирование

Примеры сочетания продуктов

Kaspersky Security для виртуальных и облачных сред

Kaspersky Container Security

Уровень защиты	Standard	Enterprise	Standard	Advanced
	Базовая защита гибридных сред	Всеобъемлющая защита гибридных облачных сред и соответствие требованиям	Безопасность образов контейнеров	Защита в рантайме и соответствие требованиям
Базовая защита ВМ + защита образов контейнеров	•		•	
Базовая защита ВМ + защита контейнеров в рантайме	•		•	•
Продвинутая защита ВМ + защита образов контейнеров	•	•	•	
Продвинутая защита ВМ + защита контейнеров в рантайме	•	•	•	•

Возьмите курс на облачную безопасность

Сокращение затрат

- Выбирайте и используйте только те возможности, которые необходимы именно вам
- Сокращение потребления ресурсов с помощью специальных функций и технологий

Обзор 360° в облаках

- Единая консоль
- Визуализация Kubernetes

Защита сред разработки

- Защита в рантайме
- Подход Shift-left

Соответствие требованиям

- Укрепление защиты (self-hardening) и самозащита
- Широкий набор функций

Демонстрация

Kaspersky Cloud Workload Security