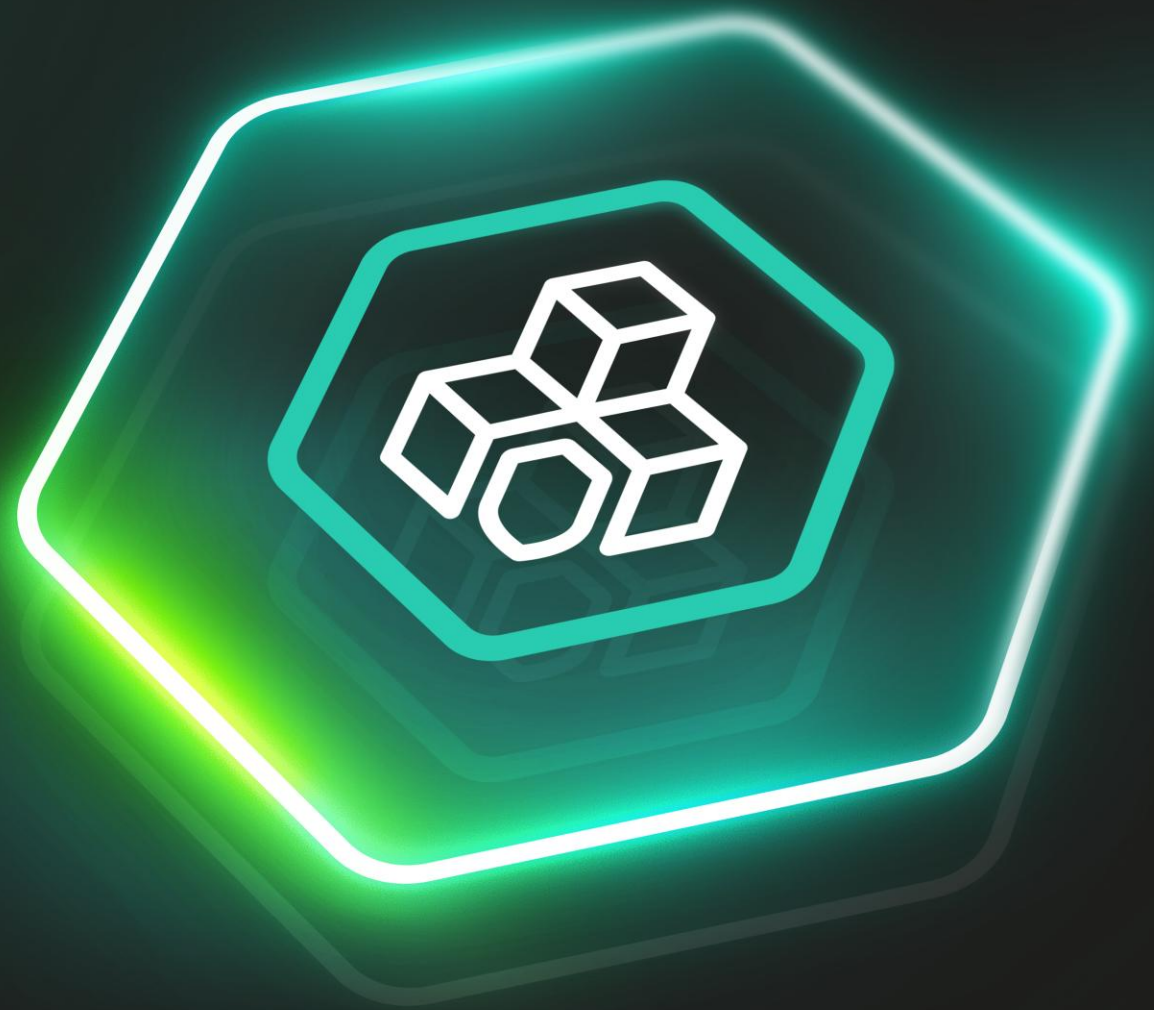
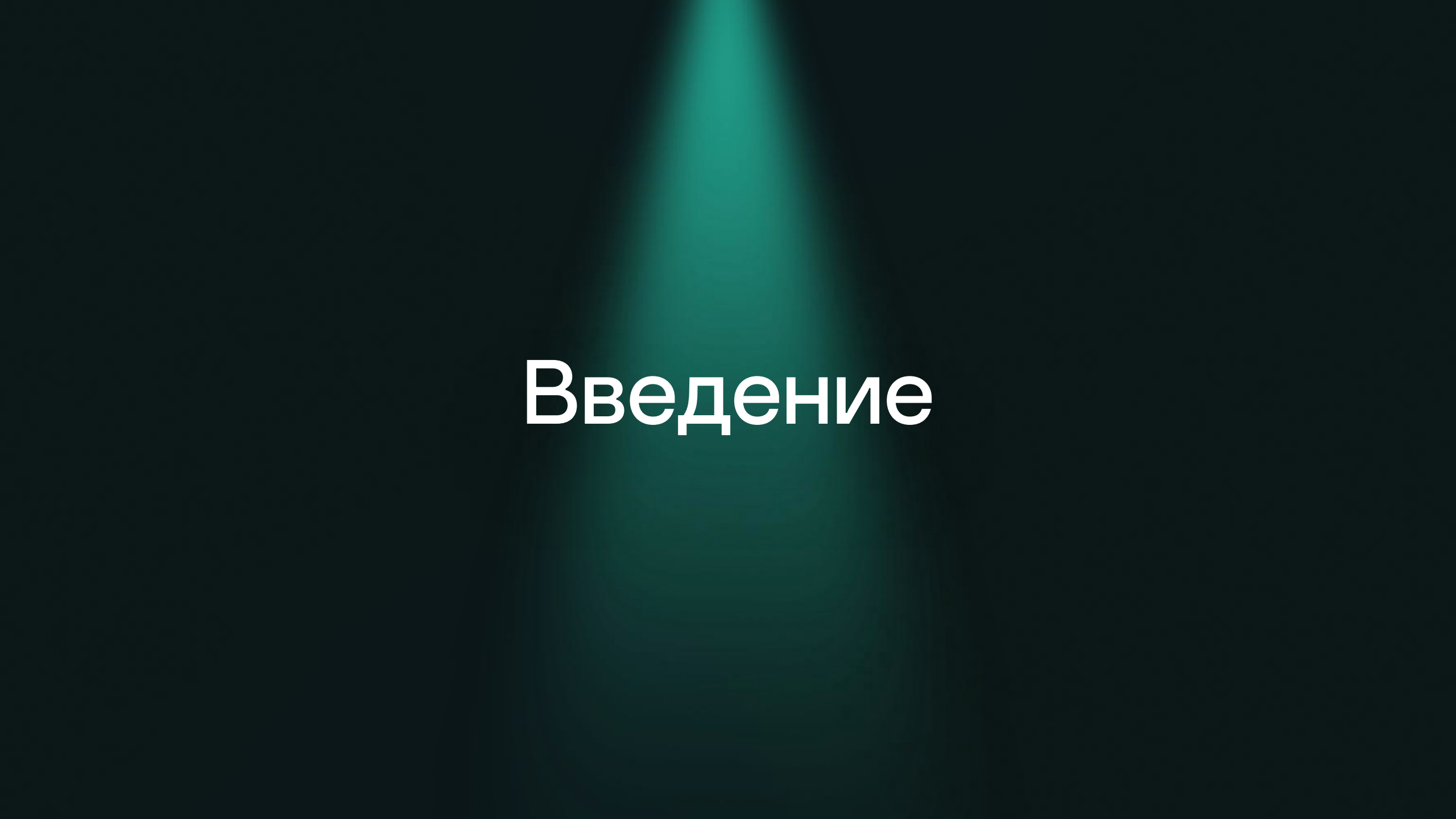


kaspersky

Kaspersky Container Security





Введение

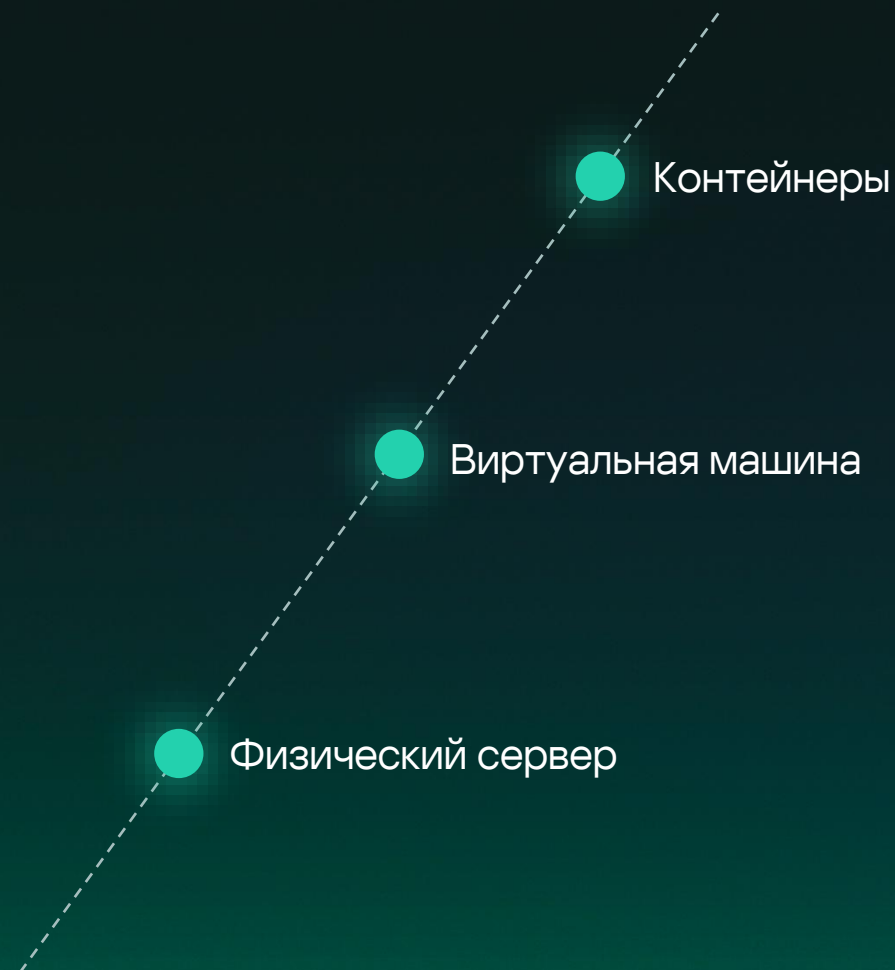
Что это?

Контейнеризация является более легковесной альтернативой виртуальным машинам.

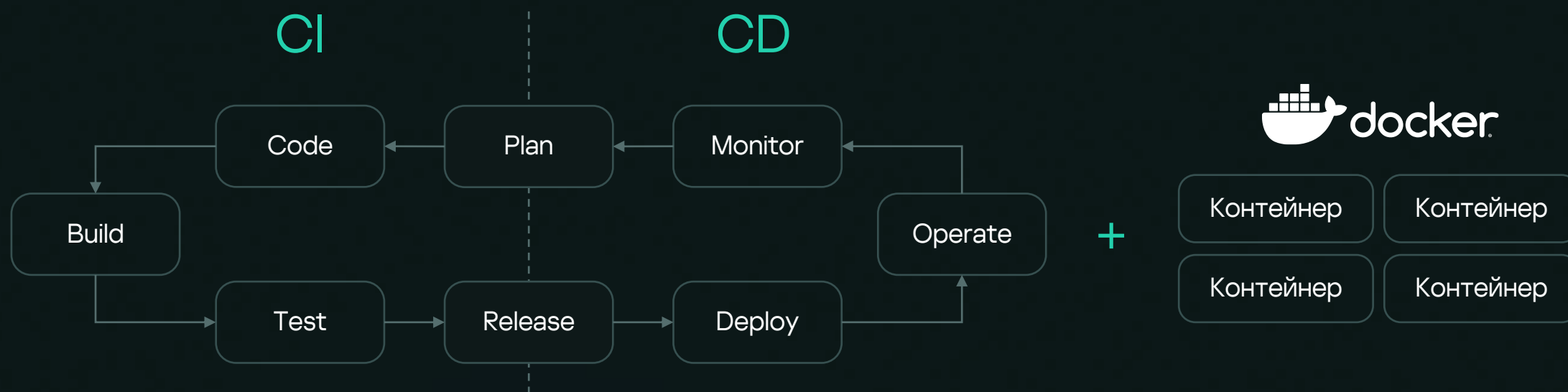
В классической схеме: один контейнер – одно приложение или сервис (микросервис)

Пример

Приложения, построенные на микросервисной архитектуре – проигрыватель видео на сайте, сервисы заказа/оплаты и доставки в интернет магазинах, музыкальное приложение в соцсетях, прогноз погоды и т.п.



Контейнеры многократно усиливают преимущества CI / CD



Ускорение написания, отладки и запуска релиза
Повышение стабильности работы приложения

Снижение требований к инфраструктуре
как разработчика, так и заказчика
Удобное масштабирование





Облачные технологии и контейнеризация — ..., это новый образ мышления, философия, постигнув которую, можно значительно расширить свои возможности.

Александр Мольский,
ИТ-директор компании «Ренессанс Жизнь»***



... Мы изначально строили свою облачную инфраструктуру на базе контейнеров, потому что это промышленный стандарт.

Антон Степаненко,
технический директор компании Ozon***

84%

компаний в мире используют контейнеры в различных средах*

~85%

компаний сталкиваются >1 одним инцидентом в среде Kubernetes в течение года**

~78%

компаний финансовой сферы используют контейнеры в разработке***

* CNCF. Annual Survey 2023, 2024

** Kaspersky. Managing Geo-Distributed businesses, 2024

*** Исследование CNews Analytics и «Инфосистемы Джет», 2020

Основные риски ключевых компонентов контейнерных сред

[Подробнее](#)

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

Примеры инцидентов контейнерной безопасности

	Инцидент	Результат	Компания	Источник
Образы	Размещение в сообществе образов с вредоносным ПО	До закрытия уязвимости (30 дней) с помощью образов было похищено до 90 000 \$	ИТ-компания	Bleepingcomputer
Реестр образов	Размещение реестра образов в открытом доступе	Потенциальная эксплуатация уязвимости для получения доступа к персональным данным	Авиакомпания	The Register
Оркестратор	Проникновение в систему через незащищенную консоль администратора K8s	• Майнинг криптовалюты на серверах компании • Утечка чувствительной информации	Автопроизводитель	Arstechnica
Контейнеры	Проникновение через незакрытый API и запуск контейнера с привилегированными правами	Получение доступа к любому устройству сети	ИТ-компания*	Trailofbits
ОС хоста	Проникновение в систему за счет присвоения прав администратора Docker-хоста	Получение доступа к serverless-системам	ИТ-компания*	Intezer

* Исследование уязвимостей

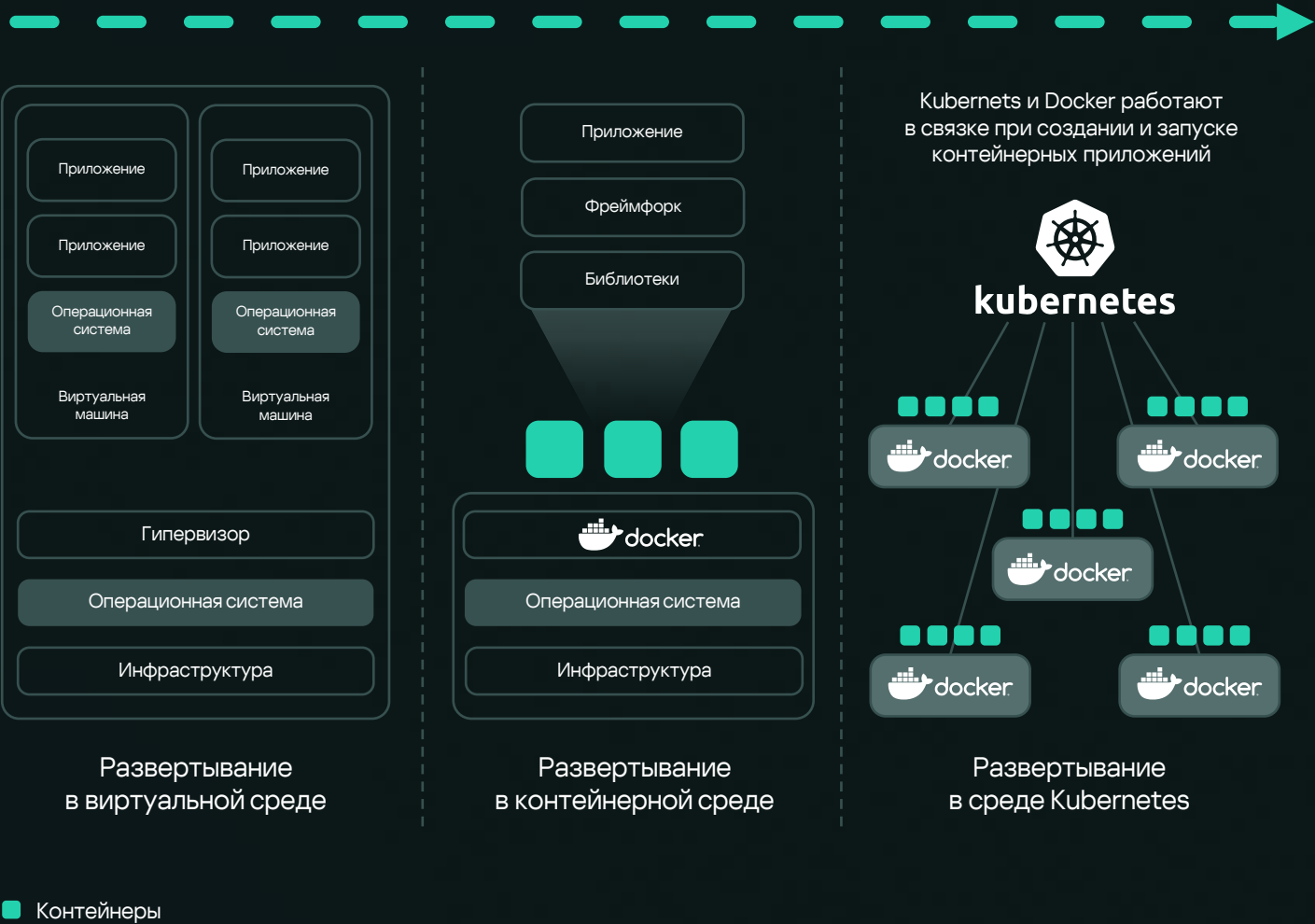
Традиционные средства защиты VM не эффективны для контейнеров

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

[Подробнее](#)

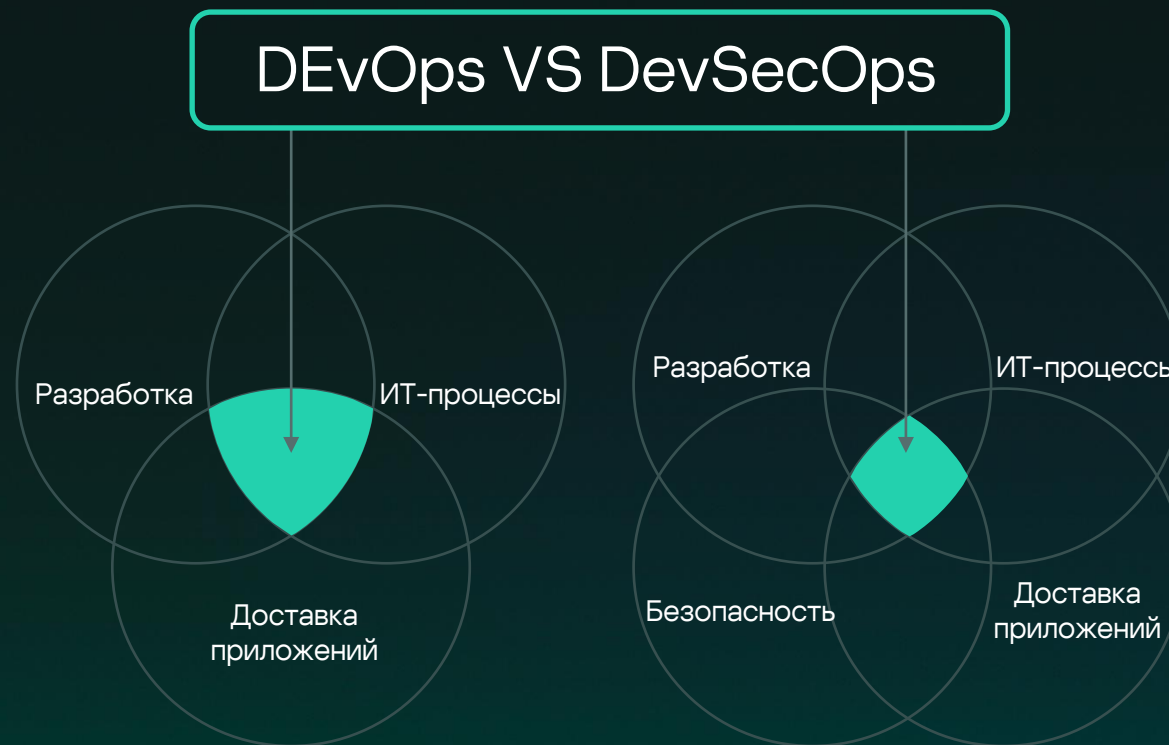


Container Security как часть процессов подхода DevSecOps

Решение должно **интегрироваться**
в процесс создания микросервисных
приложений, работающих
в контейнерных средах



Комплексный инструмент для команд
разработки и безопасности





Kaspersky Container Security

Решение контейнерной безопасности

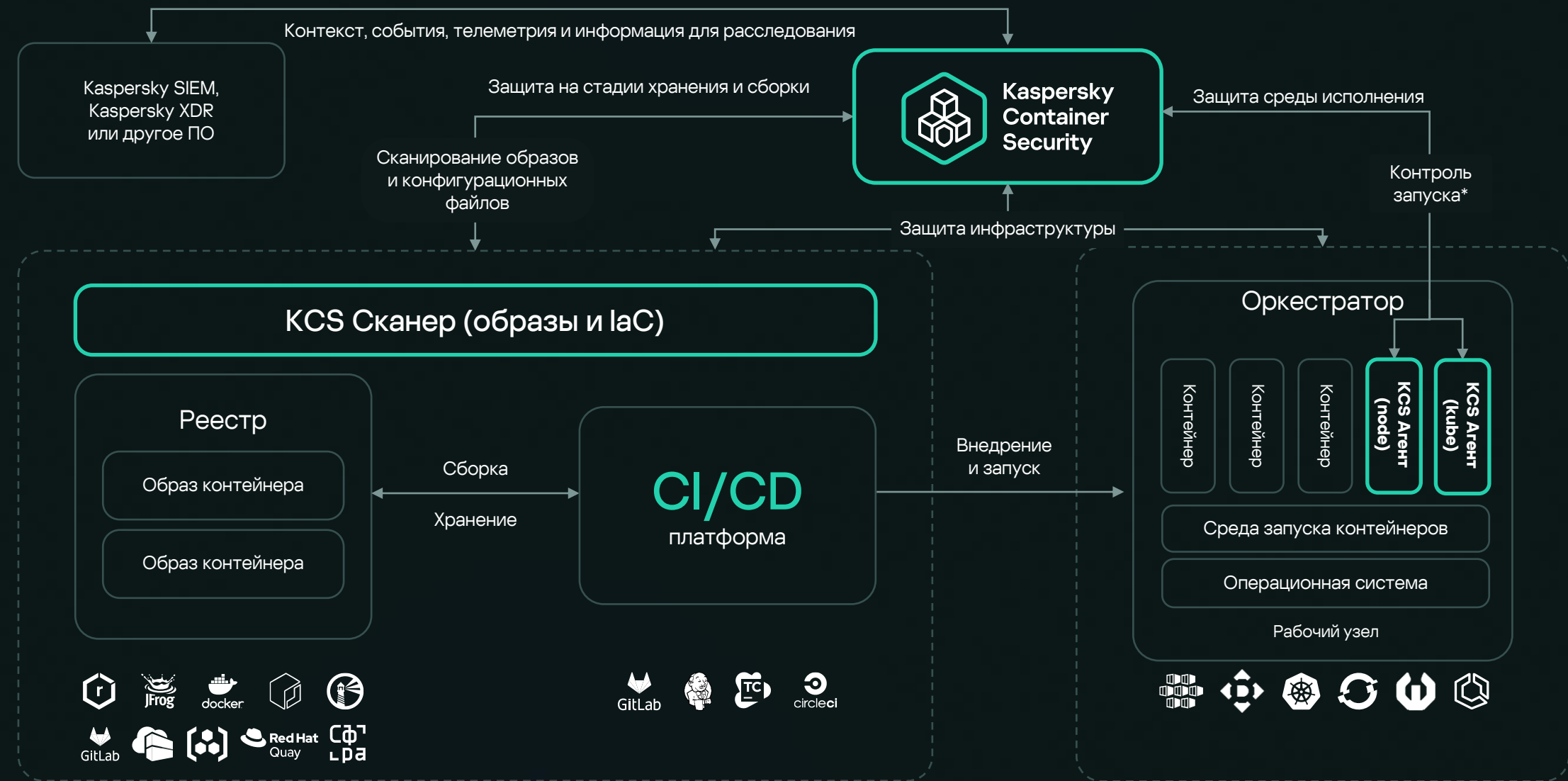
Закрывает проблемы
безопасности контейнерных
сред на всех этапах

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

Позволяет интегрироваться
в процессы безопасной
разработки

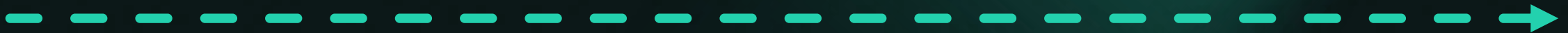
Встраивается в CI pipelines
и интегрируется в инфраструктуру

Архитектура KCS – защита на всех этапах



* Контроль запуска, защита запущенных контейнеров, безопасность среды выполнения, анализ конфигурации и проверка на соответствие

Интеграция в процесс разработки



VCS & Реестр

Исследование

Проверка образов из реестра

Сканирование конфигурационных файлов (IaC, Dockerfile) на наличие ошибок и секретов

CI инструменты

Создание и тестирование

Сканирование образов на уязвимости, вредоносное ПО и наличие секретов

CD инструменты

Доставка и развертывание

Обеспечение доставки образов соответствующих политикам безопасности

Оркестратор

Выполнение

Проверка сетевого взаимодействия на соответствие политикам безопасности

Поведенческий анализ контейнеров

Защита от уязвимостей и файловых угроз

Заккрытие 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 и визуализация трафика

Обнаружение и сканирование образов в кластере

Проверка на уязвимости

Защита узлов от файловых угроз

Контейнеры

Контроль запуска и работы только доверенных контейнеров

Мониторинг и визуализация трафика

Контроль целостности

Автоматизированный поведенческий анализ

Контроль запуска приложений и сервисов внутри контейнеров

Защита от файловых угроз

Отслеживание операций с файлами

ОС хоста

Обнаружение ошибок конфигурации и рекомендации по исправлению

Уменьшение рисков за счет контроля запуска и работы контейнеров

Проверка на уязвимости

Защита от файловых угроз

- Интеграция с KIRA (Kaspersky Investigation and Response Assistant) – нейросетевой моделью на базе GigaChat
- Интеграция с любой используемой нейросетевой моделью с помощью OpenAI API

Принцип работы:

- Просканируйте любой образ
- Нажмите «Описать с помощью ИИ»
- Получите описание образа с анализом найденных рисков и рекомендацией по их устранению
- Ускорьте время принятия решений и экономьте ресурсы

Анализ рисков

Загрузка бинарных файлов напрямую из внешних ресурсов

- Строка:

```
bash
curl -o /tmp/code-server.tar.gz -L "https://github.com/coder/code-server/releases/download/v${CODE_RELEASE}/code-server-${CODE_RELEASE}-linux-amd64.tar.gz" && tar xf /tmp/code-server.tar.gz -C /app/code-server --strip-components=1
```
- Риск: Хотя файлы загружаются с официального репозитория GitHub, отсутствие проверки целостности архива может создать условия для атаки типа «man-in-the-middle» при передаче данных по сети. Если атакующий сможет перехватить трафик и заменить оригинальный архив вредоносным файлом, это приведет к компрометации контейнера.
- Митигация: Проверять контрольные суммы (SHA256) перед распаковкой файла и использовать протоколы шифрования (HTTPS).

Использование сторонних скриптов без контроля содержимого

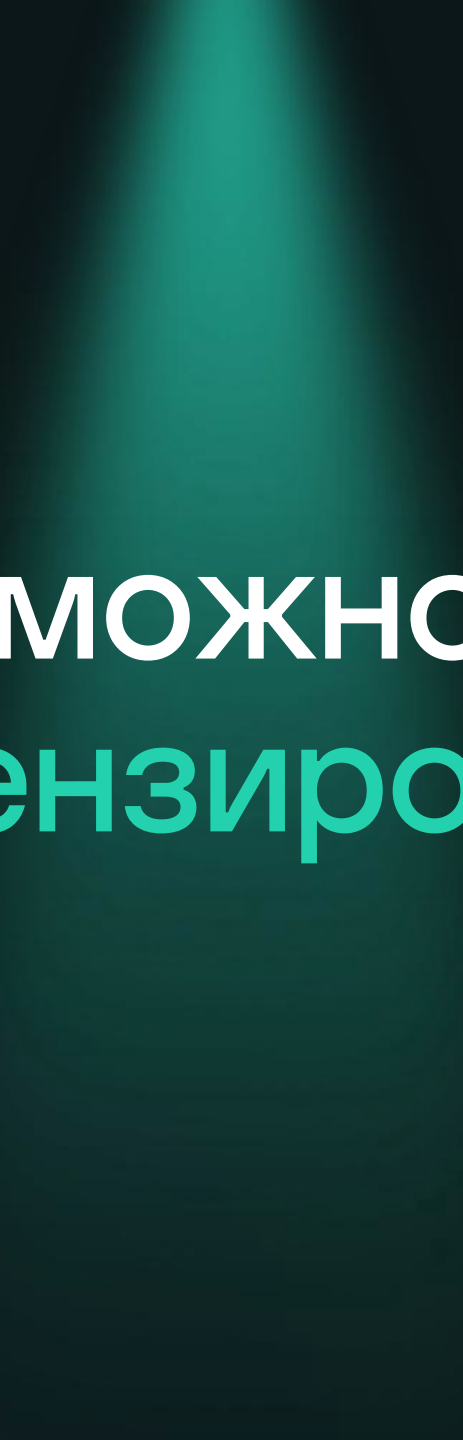
- Строка:

```
bash
ADD --chmod=755 https://raw.githubusercontent.com/linuxserver/docker-mods/mod-scripts/with-contenv.v1 /usr/bin/with-contenv
```
- Риск: Использование удаленных скриптов из публичных источников (GitHub) без предварительной проверки их содержания может представлять опасность. В случае компрометации учетной записи владельца репозитория или случайного внесения изменений посторонними лицами эти сценарии могут выполнять нежелательные действия внутри контейнера.
- Митигация: Всегда проверять содержимое скриптов перед использованием. Рекомендуется забирать копии проверенных версий и сохранять их локально для последующего использования вместо прямой загрузки во время сборки.

Итоговый результат анализа

Обнаружены два потенциальных риска, связанных с отсутствием проверки целостности загружаемых файлов и доверием к сторонним скриптам без предварительного анализа. Это может привести к компрометации контейнера. Необходимо внедрить меры по проверке целостности файлов и контролю используемых скриптов.

 The description provided by the AI Tool is formed automatically and may contain inaccuracies.



Возможности и лицензирование



Версии 2.2/2.3/2.4

Начало сертификации
во ФСТЭК России

Интеграция и применение
ИИ-ассистента KIRA в продукте

Интеграция с SSO

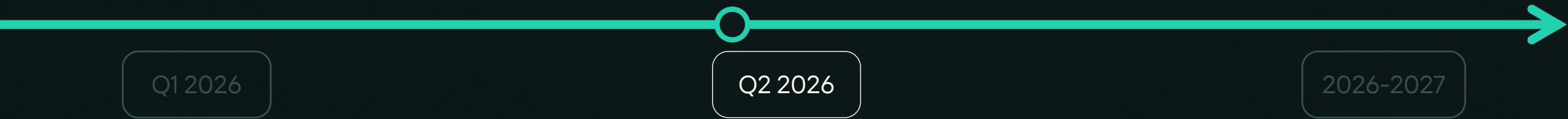
Расширение возможности
анализа RBAC в кластере

Поддержка мультидоменности
AD

Оптимизация работы
с большими образами

Оптимизация процесса
сканирования

Обогащение Assurance-политик



Версии 2.5

Возможность создание
собственных проверок
безопасности кластера

Возможность создания
собственных DAC- и Assurance-
политик

Возможность импорта/экспорта
конфигурации системы

Просмотр SBOM в деталях
анализа образа

Разграничение доступа к
результатам проверок CI

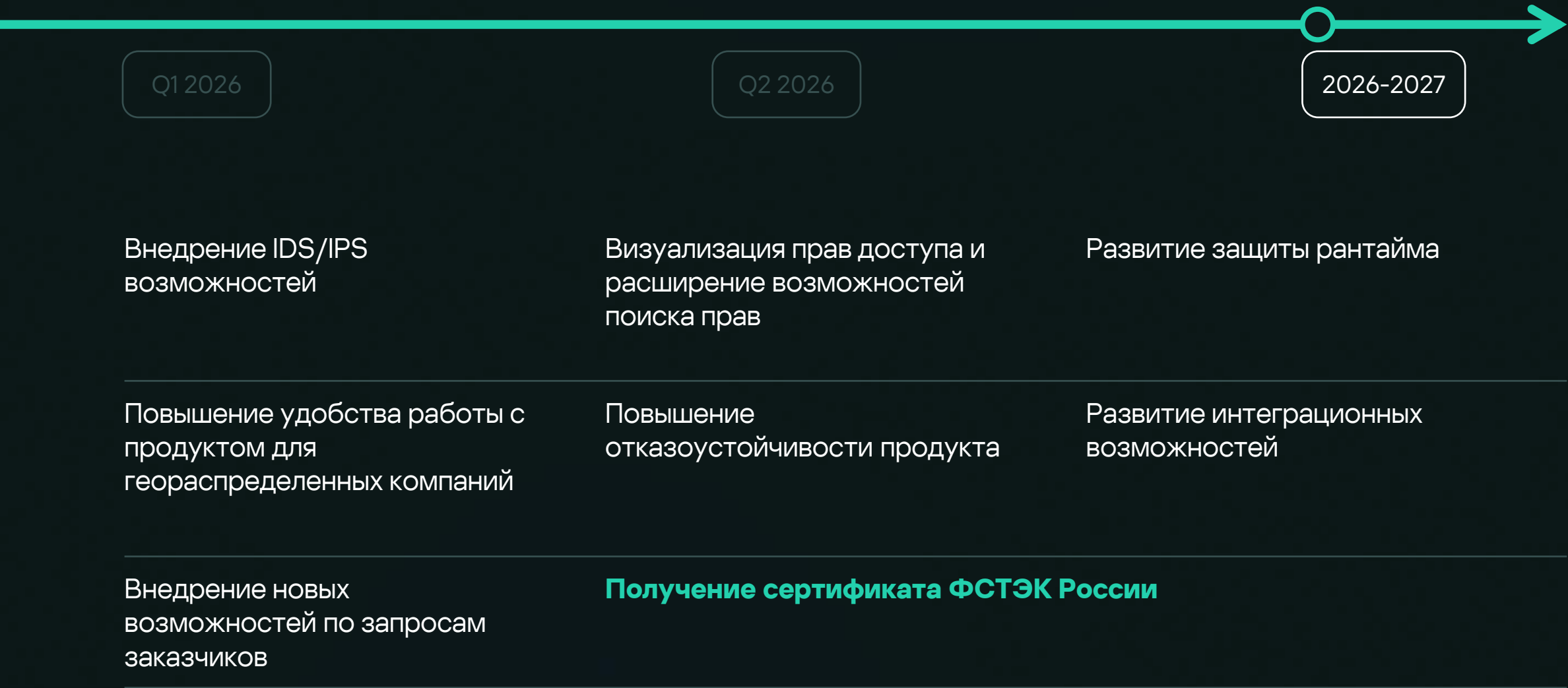
Оптимизация работы
с большими образами

Оптимизация процесса
сканирования

Оптимизация производительности
node-агента

Возможность работы node-agent на
мастер ноде

Другие улучшения



* Возможны изменения

Возможности		Standard	Advanced	Advanced Pro
Безопасность образов контейнеров	Интеграция с реестрами образов и платформами оркестрации	•	•	•
	Интеграция с CI/CD платформами и проверка образов на стадии разработки	•	•	•
	Интеграция с публичными облаками	•	•	•
	Сканирование образов на вредоносные объекты, уязвимости и секреты	•	•	•
	Оценка рисков для образов и инструментарий принятия рисков	•	•	•
	Сканирование конфигурационных файлов (IaC)	•	•	•
	Политики соответствия для образов по результатам сканирования	•	•	•
	Открытое API для ключевой функциональности продукта (Swagger)	•	•	•
	Специальная страница по исследованию уязвимостей (ограниченная функциональность)	•	•	•
	Сбор логов событий и их передача напрямую в SIEM-систему (ограниченная функциональность)	•	•	•
	Анализ оркестратора на соответствие лучшим практикам безопасности	•	•	•
	Инструменты визуализации	•	•	•
	Анализ конфигурации компонентов контейнерной платформы на соответствие отраслевым стандартам и практикам, выявления рисков безопасности (ограниченная функциональность)	•	•	•
	Интеграция с внешними системами безопасности и уведомлений	•	•	•

Возможности		Standard	Advanced	Advanced Pro
Безопасность запущенных приложений и соответствие требованиям регуляторов	Мониторинг и контроль запуска контейнеров в соответствии с политиками безопасности		•	•
	Обнаружение и сканирование образов в кластере		•	•
	Автоматическое построение профиля поведения контейнера и генерация политик безопасности		•	•
	Контроль трафика запущенных контейнеров и построение графа визуализации		•	•
	Защита от файловых угроз для запущенных контейнеров (eBPF, KESL агент)		•	•
	Защита ОС ноды от файловых угроз (KESL агент)		•	•
	Сканирование ОС нод на уязвимости		•	•
	Мониторинг и контроль файловых операций для запущенных контейнеров (eBPF)		•	•
	Сбор логов событий и их передача напрямую в SIEM-систему (полная функциональность)		•	•
	Контроль изменения логов в объектах RBAC кластера		•	•
	Контроль целостности для контейнеров (функциональность проверки подписи)		•	•
	Специальная страница по исследованию уязвимостей (полная функциональность)		•	•
	Контроль запуска приложений и сервисов внутри контейнеров		•	•
	Обогащение информацией о репутации сетевых соединений с помощью пользовательских фидов		•	•
	Визуализация ресурсов кластера		•	•
	Анализ конфигурации компонентов контейнерной платформы на соответствие отраслевым стандартам и практикам, выявления рисков безопасности (полная функциональность)		•	•

Advanced Pro



Интеграция с ИИ-ассистентом KIRA (на базе GenAI) и OpenAI API

Позволяет использовать любых
ИИ-помощников, развернутых
в вашей инфраструктуре
(как локальной, так и облачной)



Прменение пользовательских политик безопасности

Политики безопасности могут быть
адаптированы к стандартам и практикам
безопасности вашей организации.



**Kaspersky
Container
Security**

Standard

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



**Kaspersky
Container
Security**

Advanced

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



**Kaspersky
Container
Security**

Advanced Pro

Расширяет сценарии и удобство работы с продуктом благодаря ИИ-аналитике образов контейнеров и возможности использования пользовательских политик безопасности

1 лицензия = 1 нода с контейнерами

1 лицензия =

1 нода с контейнерами

5100 токенов на ноду в день

Традиционная модель продаж через дистрибьютеров и партнеров

Сценарии использования и преимущества

Сценарии использования Kaspersky Container Security

26

При разработке приложений на микросервисной архитектуре

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

При выстраивании процессов DevSecOps

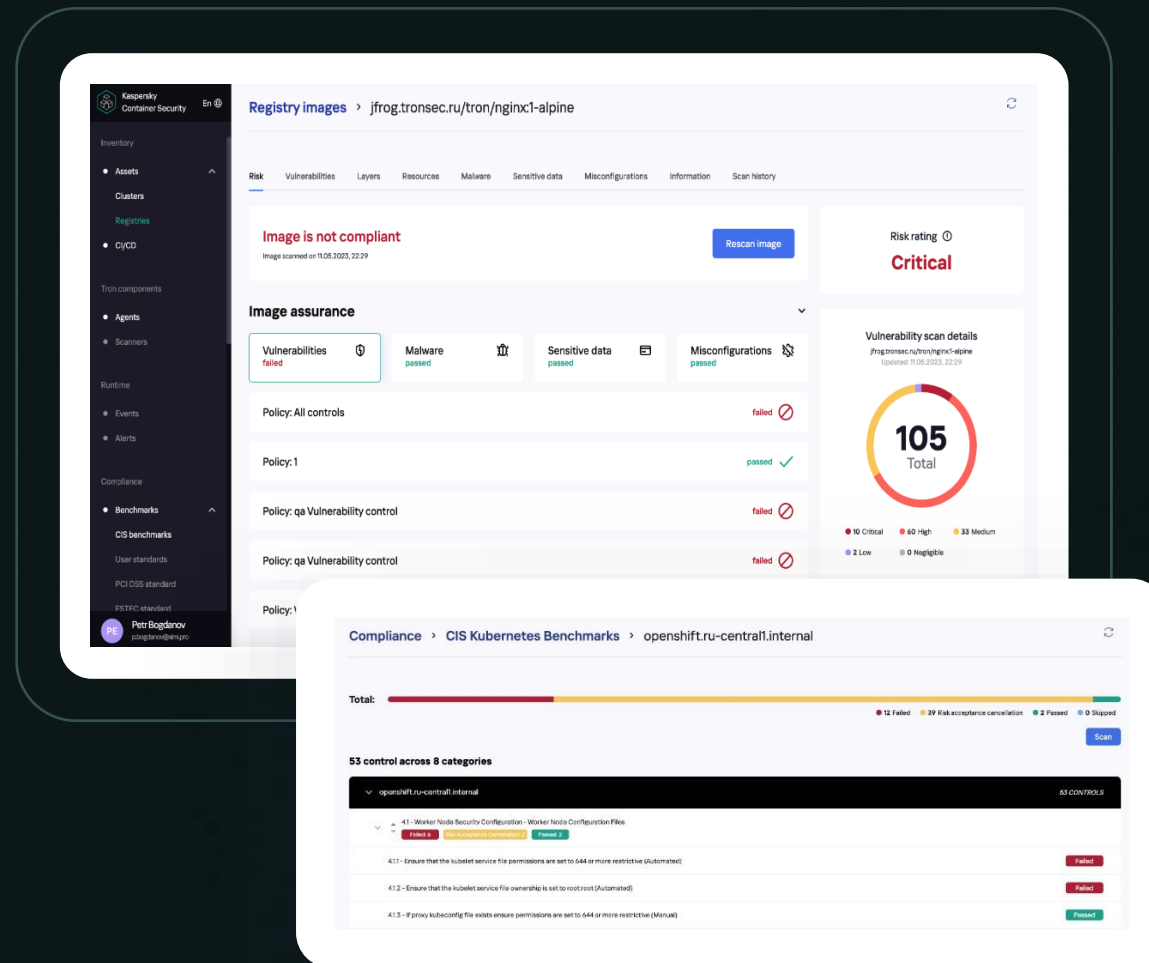
Добавление «quality gate» требует проверки собираемых контейнеров

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



Отрасль	Рейтинг	Описание проекта	Размер инфраструктуры
Финансы	Организации из списка Топ-10 в отрасли	Современная цифровая инфраструктура, как внешняя, так и внутренняя, с микросервисной архитектурой и контейнеризованными приложениями. Строгие промышленные и внутренние стандарты и требования по кибербезопасности. Организации стремятся защитить как цикл разработки клиентских приложений, так и всю инфраструктуру, выполняя требования регуляторов и норм законодательства.	Более 100 000 узлов
Государственная финансовая организация		Современная цифровая инфраструктура с микросервисной архитектурой и контейнеризованными приложениями. Строжайшие требования по кибербезопасности. Организация выстраивает отказоустойчивую и защищенную инфраструктуру согласно требованиям законодательства и регуляторов.	450 узлов (900 в планах на 2026)
Розничная торговля	Организации из списка Топ-5 в отрасли	Приложения для клиентов построены с использованием контейнеров. Любой сбой в работе приложений влечет за собой финансовые потери. Организации стремятся обеспечить безопасность цикл разработки приложений, повышая их отказоустойчивость и обеспечивая безопасность данных клиентов.	800 узлов
Телеком	Организация из большой четверки операторов связи	Микросервисная архитектура используется как для внутренних (корпоративных) решений, так и для большинства клиентских сервисов. Компания стремится заменить иностранного поставщика, а также соблюдать требования по безопасности данных клиентов.	1500 узлов

Решение проблем ИБ

- Оценка и контроль рисков на всех стадиях работы с контейнерами
- Контроль конфигурации с точки зрения ИБ
- Обеспечение безопасности приложений в контейнерах
- Безопасность инфраструктуры
- Выявление устаревших и уязвимых компонентов
- Соответствие требованиям регуляторов

Решение проблем ИТ

- Корректная конфигурация всех компонентов в соответствии с лучшими практиками
- Оптимизация использования ресурсов, выявление аномалий
- Повышение производительности приложений и сервисов
- Контролируемое внедрение контейнеризации
- Уменьшение ИТ инцидентов

Наглядность для всех компонентов контейнерной инфраструктуры и связанных рисков

Применение подхода Shift-left

Проверка образов контейнеров и артефактов развертывания в момент их попадания в репозиторий

Контроль образов в реестрах

Возможность обнаружить и исправить ИБ-риск на ранней стадии создания приложения

Контроль процессов в рантайме

Образы, которые не прошли проверки на соответствие требованиям не будут развернуты в среде оркестратора

Прозрачность

Оперативное получение информации о состоянии проектов и проблемах ИБ в своей зоне видимости

Кооперация

Возможность параллельной работы разных команд в одной системе не мешая друг другу

Сила бренда и качество продукта

По результатам более 700 независимых испытаний наши разработки были признаны наиболее эффективными решениями в области кибербезопасности

Легкий старт

Решение имеет удобный интерфейс и не требует сложной настройки или специальных навыков, автоматизированные проверки безопасности сокращают время выхода на рынок и помогают перераспределить ресурсы службы ИБ

Удобен для он-прем инфраструктур

Все возможности продукта доступны для физических инфраструктур и изолированных сетей

Удобное лицензирование

Просто посчитайте ноды, на которых развернуты контейнеры



Kaspersky Cloud Workload Security



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

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



Защита сред разработки

- Защита в рантайме
- Подход Shift-left



Обзор 360° в облаках

- Единая консоль
- Визуализация Kubernetes



Соответствие требованиям

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



Kaspersky Cloud Workload Security

Комплексная защита облачной инфраструктуры и контейнерных сред



Kaspersky Security для виртуальных и облачных сред

Защита гибридной инфраструктуры — физические серверы, виртуальные серверы и VDI, а также публичные облака



Kaspersky Security for Storage

Защита операций с файлами и конфиденциальных данных в том числе от вредоносных программ-шифровальщиков



Kaspersky Unified Monitoring and Analysis Platform

SIEM-система, которая повышает прозрачность инфраструктуры и усиливает эффективность мер защиты



Kaspersky Endpoint Detection and Response Expert

Продвинутое обнаружение угроз, автоматическое реагирование и обзор в реальном времени

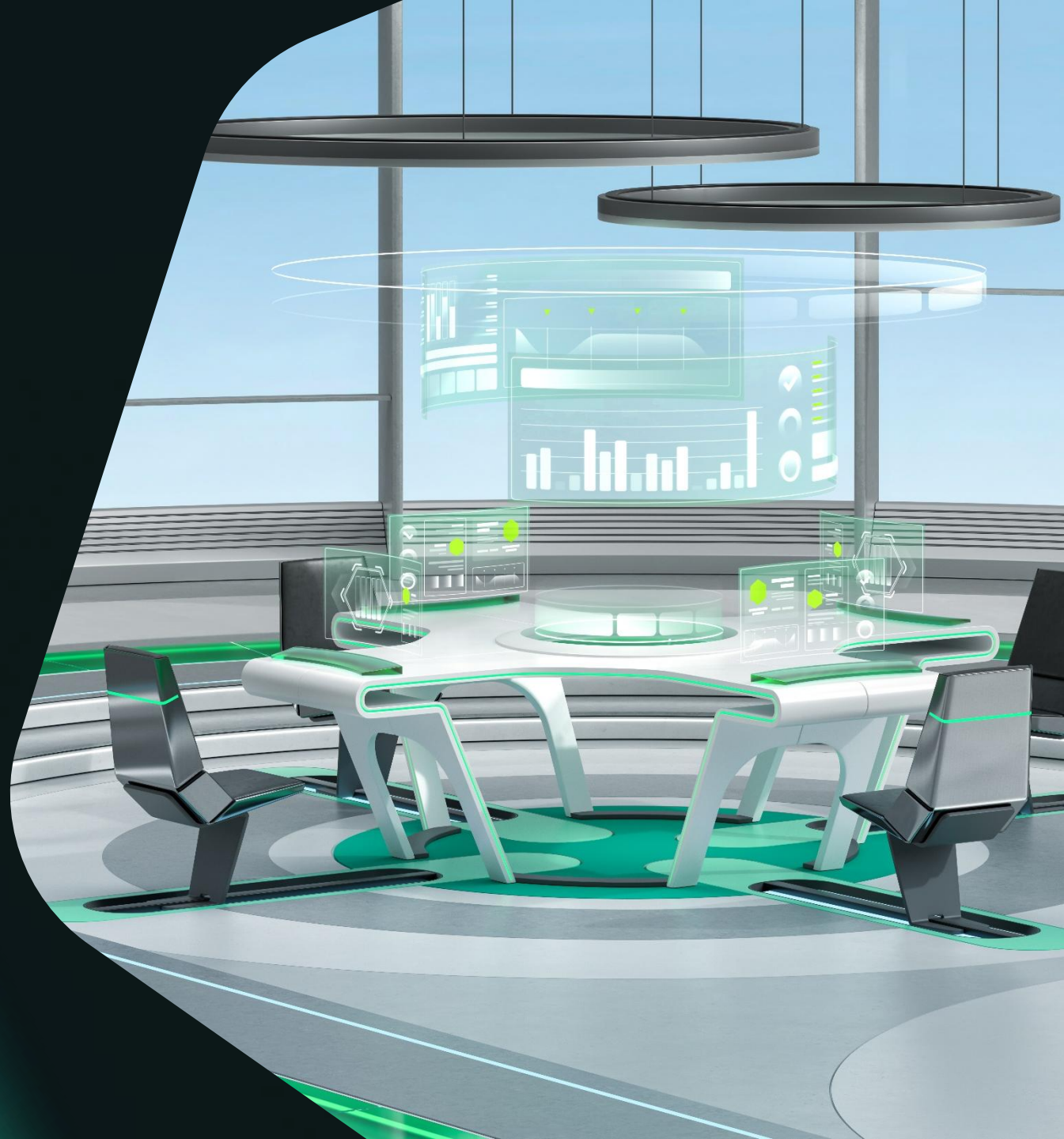


Kaspersky Professional Services

Получите максимум преимуществ от продуктов «Лаборатории Касперского»

Демо

Запишитесь
на демонстрацию
продукта через
своего аккаунт
менеджера!



Спасибо!

