Kaspersky Industrial Cybersecurity Conference 2023

Kaspersky Container Security:

защита современной разработки.

Василий Сарычев,

руководитель группы продуктового маркетинга, Network & Cloud Security

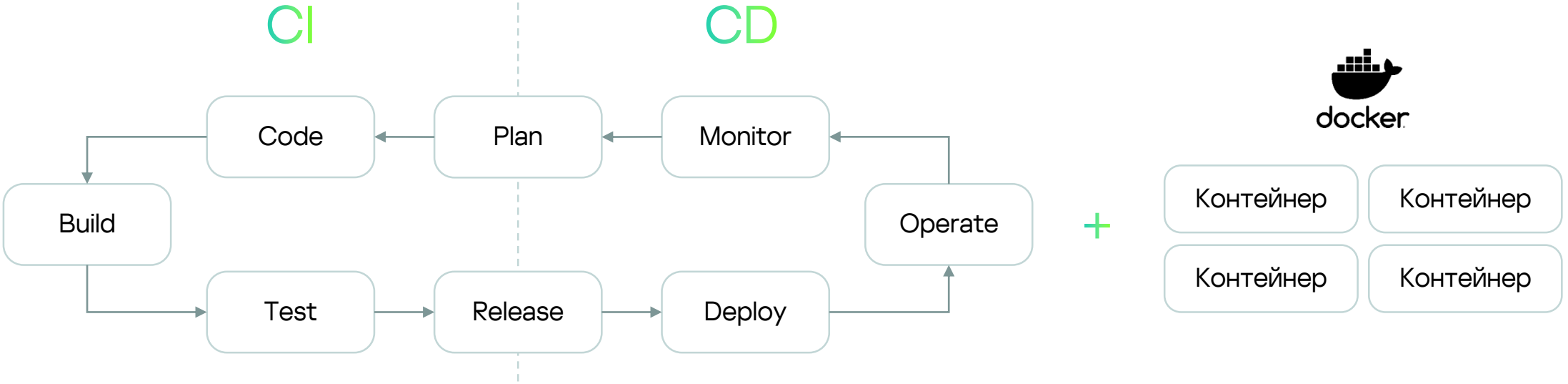
kaspersky

В компании «Роснефть» рассказали о разработке собственного ПО для нефтегазовой отрасли

У нас коммерциализированы и доступны для приобретения 10 программных продуктов. Еще 13 продуктов находятся в стадии разработки и внутренней апробации. Мы сейчас готовы помочь и уже помогаем всем коллегам из нефтегазовой отрасли в импортозамещении того ПО, которое необходимо для разведки и добычи. Они уже тестируют его и покупают

РИА “ФедералПресс” (Rambler Finance, 22) , Сергей Кувшинов, Роснефть

Контейнеры многократно увеличивают преимущества CI / CD



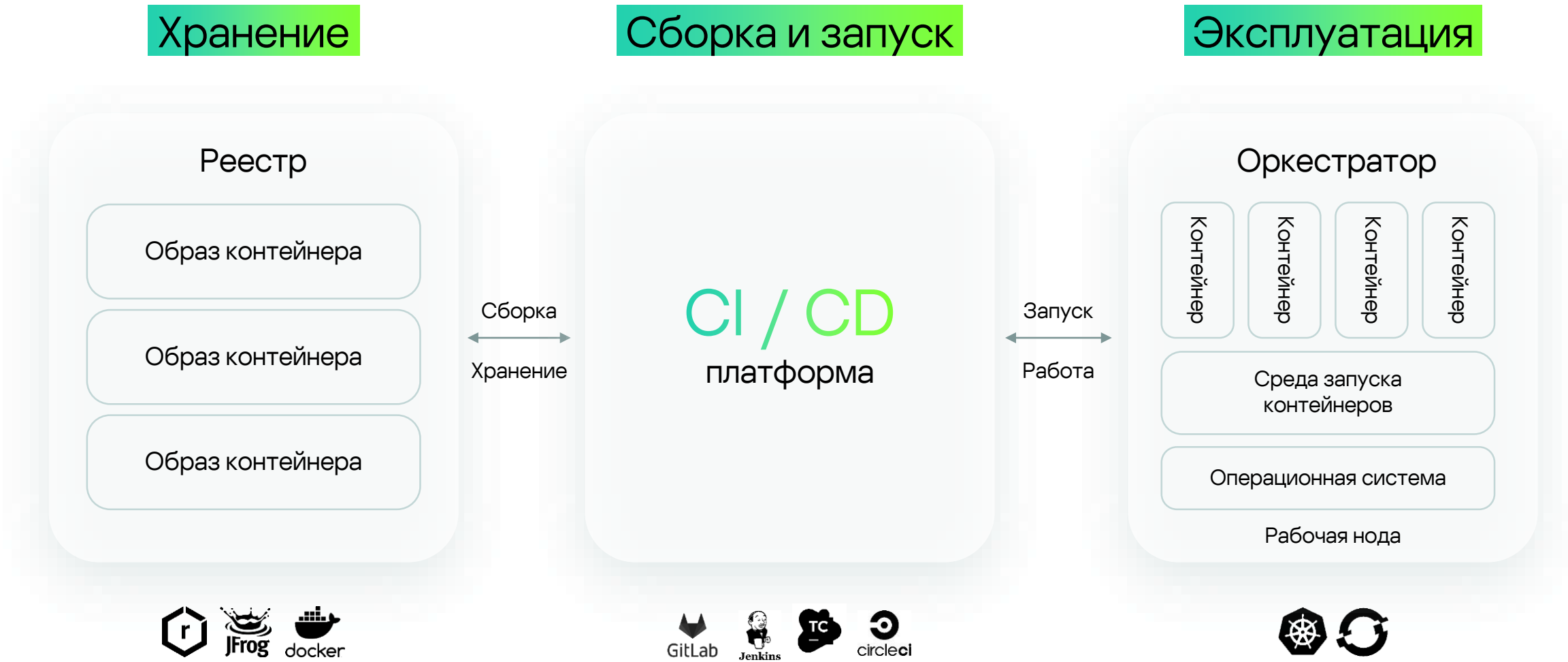
Ускорение написания, отладки и запуска релиза

Повышение стабильности работы приложения

Снижение требований к инфраструктуре как разработчика, так и заказчика

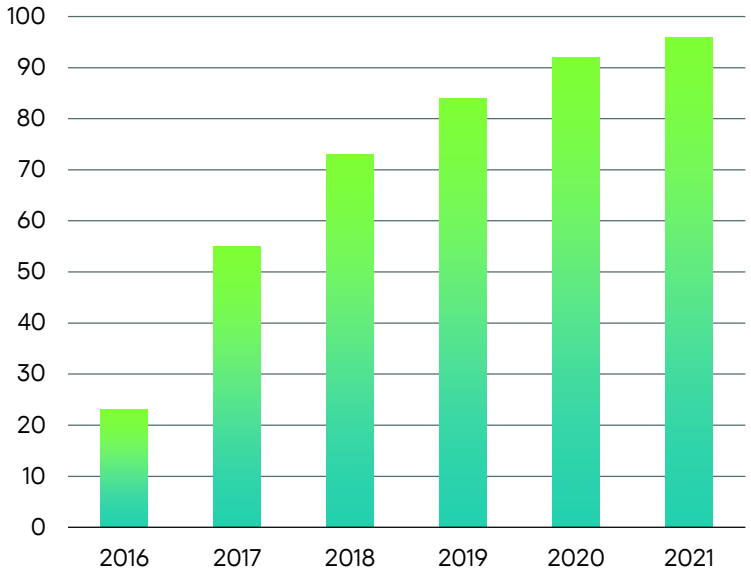
Удобное масштабирование

Компоненты контейнерной инфраструктуры



Использование контейнеров

В мире по данным CNCF*



38% респондентов из Европы,
33% из Сев. Америки, 23% из Азии

*CNCF (Cloud Native Computing Foundation), 2022

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

*** RedHat Datalog 2022

В России среди компаний Топ-500 РБК**

93%

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

~78%

компаний финансовой сферы используют контейнеры в разработке

~56%

компаний используют контейнеры в разработке

Уровень контейнеризации в России ниже, чем в западных странах. Однако, высокие темпы роста говорят о скором применении решения большинством российских компаний.

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

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 $	docker	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 Tesla • Утечка чувствительной информации	TESLA	Arstechnica
Контейнеры	Проникновение через незакрытый API и запуск контейнера с привилегированными правами	Получение доступа к любому устройству сети	Cybersecurity Action Team *	Trailofbits
ОС хоста	Проникновение в систему за счет присвоения прав администратора Docker-хоста	Получение доступа к serverless-системам	INTEZER *	Intezer

* Исследование уязвимостей

Сравнение Container Security и VM security

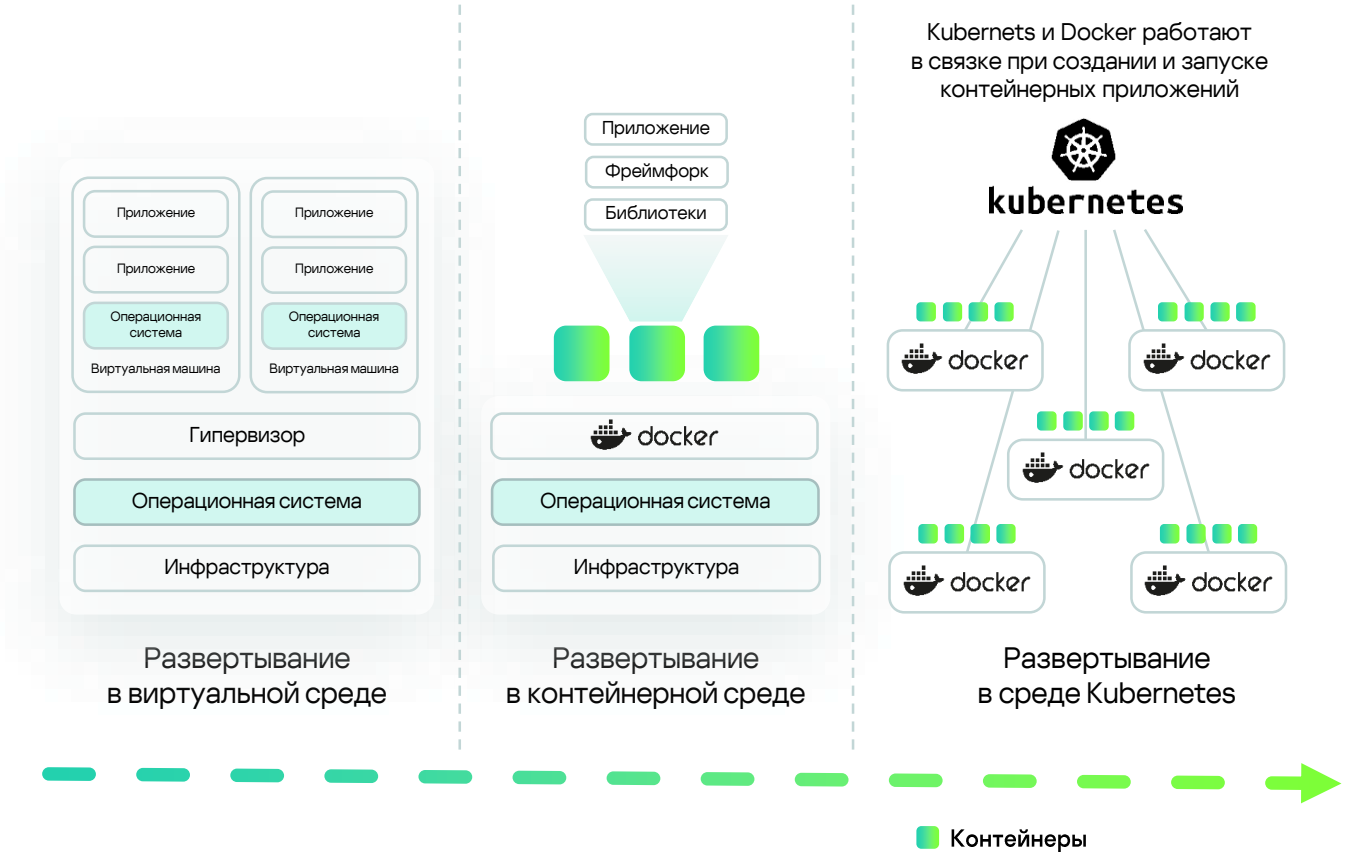
Традиционные средства защиты VM не эффективны для контейнеров

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

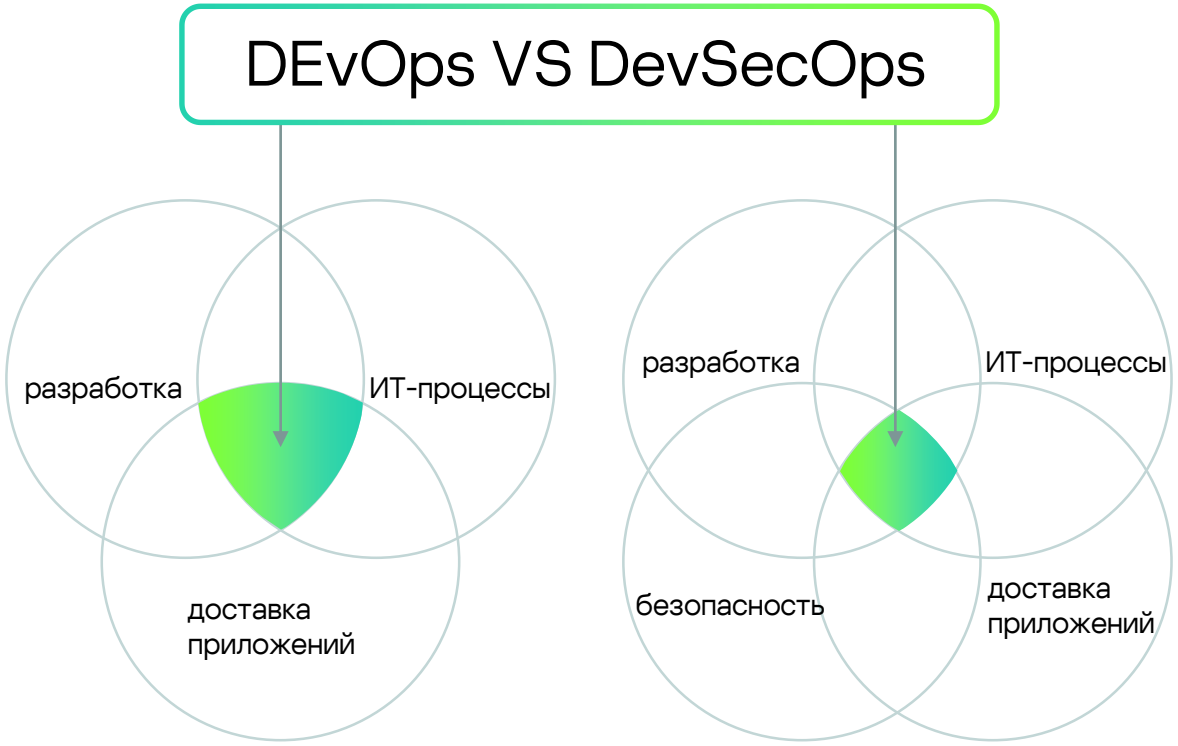
Подробнее



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

Эволюция решений Kaspersky для защиты облачных, виртуальных и гибридных нагрузок

2012
Запуск Kaspersky Security for Virtualization

2014
Выпуск технологии KSV Light Agent (US patent 9,009,836)

2016
Light Agent для Linux; новые платформы виртуализации

2018
Запуск Kaspersky Security для виртуальных и облачных платформ

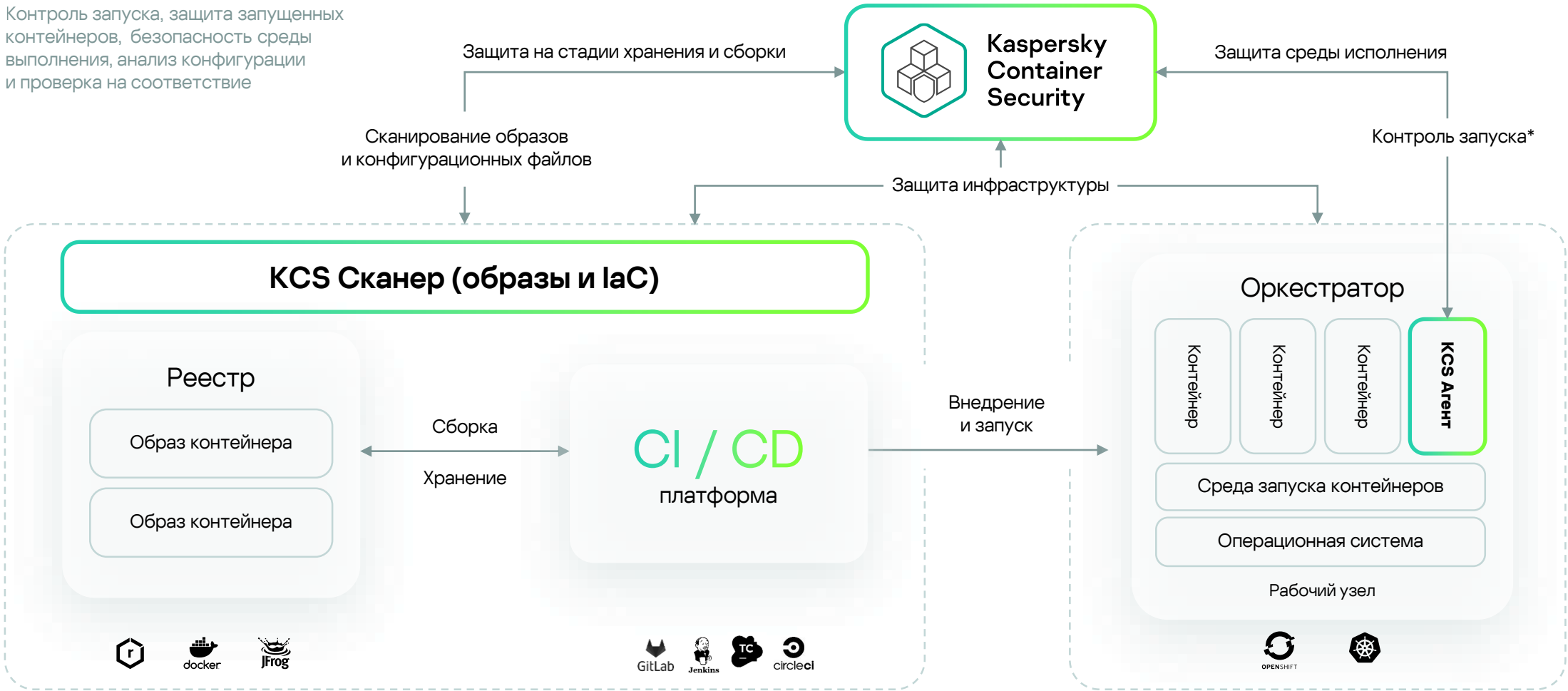
2020
Поддержка API интеграций с AWS, Azure и GCP

2023
Kaspersky Container Security

docker
Jenkins
kubernetes
amazon web services
Google Cloud
vmware
nsx
Microsoft Azure
KVM
CITRIX
Microsoft

Архитектура KCS – защита на всех этапах

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



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

Обнаружение и сканирование образов в кластере

Контейнеры

Контроль запуска и работы только доверенных контейнеров

Контроль целостности контейнеров

Контроль запуска приложений и сервисов внутри контейнеров*

Контроль трафика контейнера*

ОС хоста

Обнаружение ошибок конфигурации и рекомендации по исправлению

Уменьшение рисков за счет контроля запуска и работы контейнеров

* Планируется в версии 1.1.

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

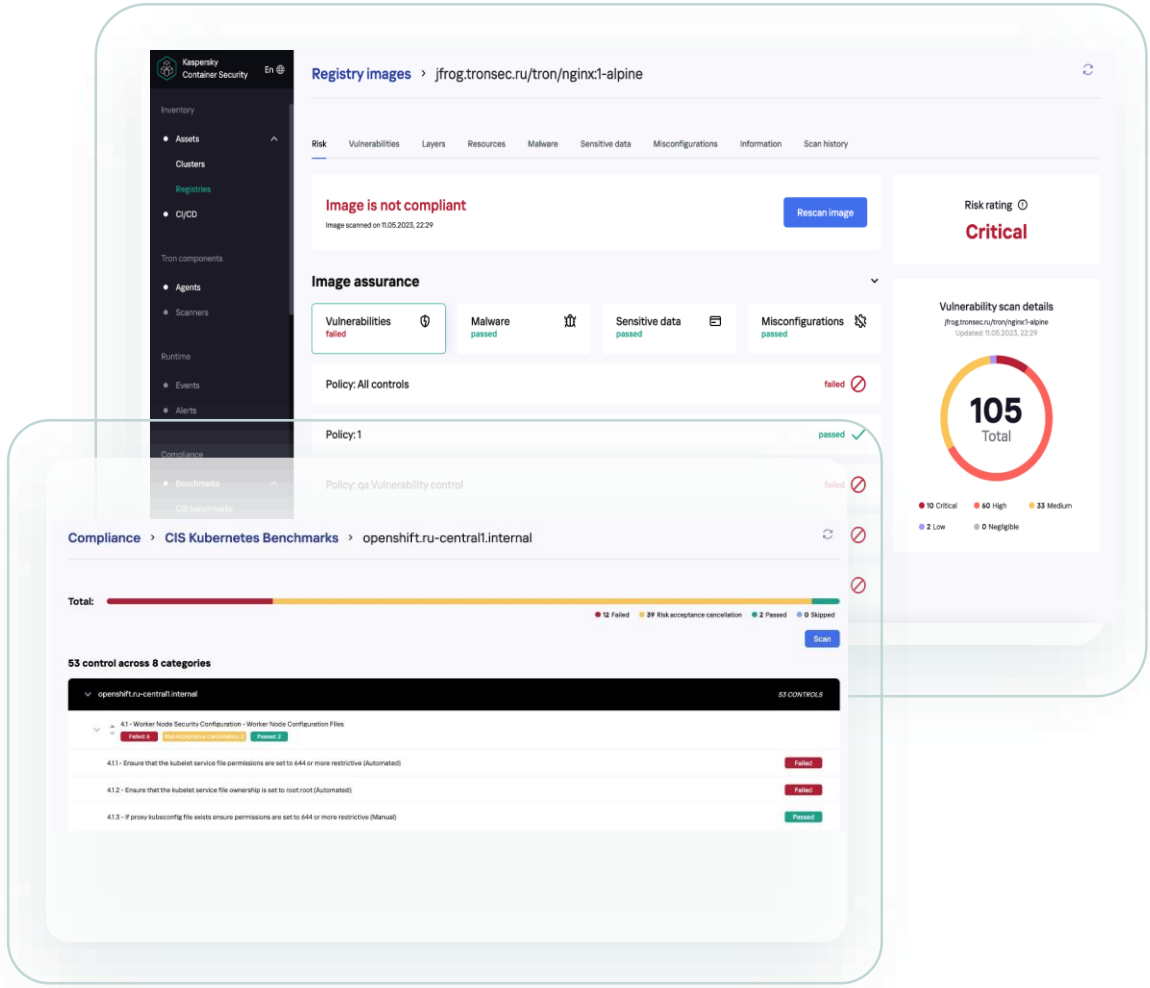
Добавление «quality gate» требует проверки собираемых контейнеров

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



Версия 1.0 – выпущена

OAS и ODS сканирование образов контейнеров

Проверка образов на наличие:
уязвимостей, вредоносных объектов и секретов

Интеграция с реестрами образов контейнеров
и платформами оркестрации

Интеграция с CI/CD платформами
и проверка образов на стадии разработки

Оценка рисков для образов по результатам
сканирования

Функционал принятия рисков для образов

Визуализация в интерфейсе продукта информации об образах,
элементах контейнерной инфраструктуры, их взаимосвязи,
найденных проблемах и связанных рисках

Возможности интеграции с внешними системами
безопасности и уведомлений

Анализ среды исполнения на наличие ошибок конфигурации
и проверка на соответствие стандартам

Сканирование образов в кластере

Контроль запуска доверенных контейнеров

Kaspersky Container Security - roadmap

Q3 2023

Версия 1.0

- Сканирование образов контейнеров на различных стадиях
- Контроль запуска доверенных контейнеров
- Анализ и обнаружение ошибок конфигурации компонентов контейнерной платформы

Q4 2023

Версия 1.1

- Контроль запуска приложений и сервисов внутри контейнеров
- Визуализация, мониторинг и контроль трафика между контейнерами, компонентами платформы контейнеризации, внешними сервисами и ресурсами
- Улучшенные технологии защиты на стадии запуска и работы контейнеров

2024

Новые версии*

- Улучшенные технологии защиты на стадии запуска и работы контейнеров
- Интеграция с другими защитными решениями
- Интеграция с публичными облаками

* Возможны изменения

Решение проблем с помощью KCS

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 IT инцидентов

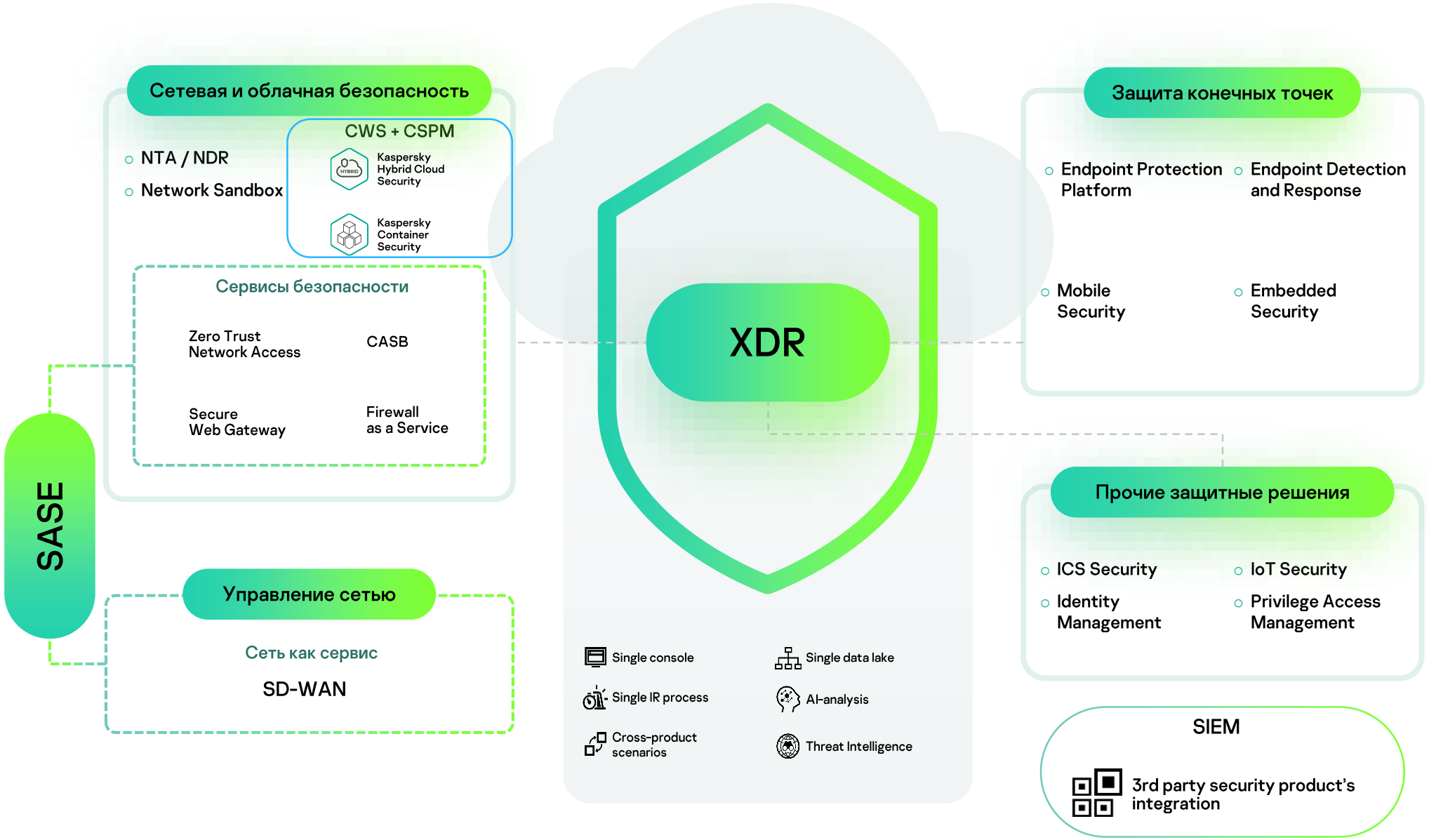
Наглядность для всех компонентов контейнерной инфраструктуры и связанных рисков

Container Security – Уровни и Лицензирование

	Возможности	Standard	Advanced
Безопасность образов контейнеров	Интеграция с реестрами образов и платформами оркестрации	●	●
	Интеграция с CI/CD платформами и проверка образов на стадии разработки	●	●
	Сканирование образов на вредоносные объекты, уязвимости и секреты	●	●
	Оценка рисков для образов и инструментарий принятия рисков	●	●
	Сканирование конфигурационных файлов (IaC)	●	●
	Интеграция с внешними системами безопасности и уведомлений	●	●
	Политики соответствия для образов по результатам сканирования	●	●
Безопасность запущенных приложений и соответствие требованиям регуляторов	Мониторинг и контроль запуска контейнеров в соответствии с политиками безопасности		●
	Обнаружение и сканирование образов в кластере		●
	Защита от файловых угроз для запущенных контейнеров*		●
	Поведенческий анализ контейнеров (на основе шаблонов)*		●
	Контроль трафика запущенных контейнеров*		●
	Контроль целостности для контейнеров		●
	Контроль запуска приложений и сервисов внутри контейнеров*		●
	Анализ конфигурации компонентов контейнерной платформы на соответствие лучшим практикам и требованиям регуляторов		●

* Планируется в версии 1.1.

Container Security – развитие направления Cloud Workload Security и часть XDR стратегии



Демо

Запишитесь
на демонстрацию
продукта через своего
аккаунт менеджера!

Спасибо!

kaspersky