

Kaspersky Container Security

kaspersky

Компания приобретает
компанию разработчика
платформы для защиты
контейнерных сред Ximi Pro

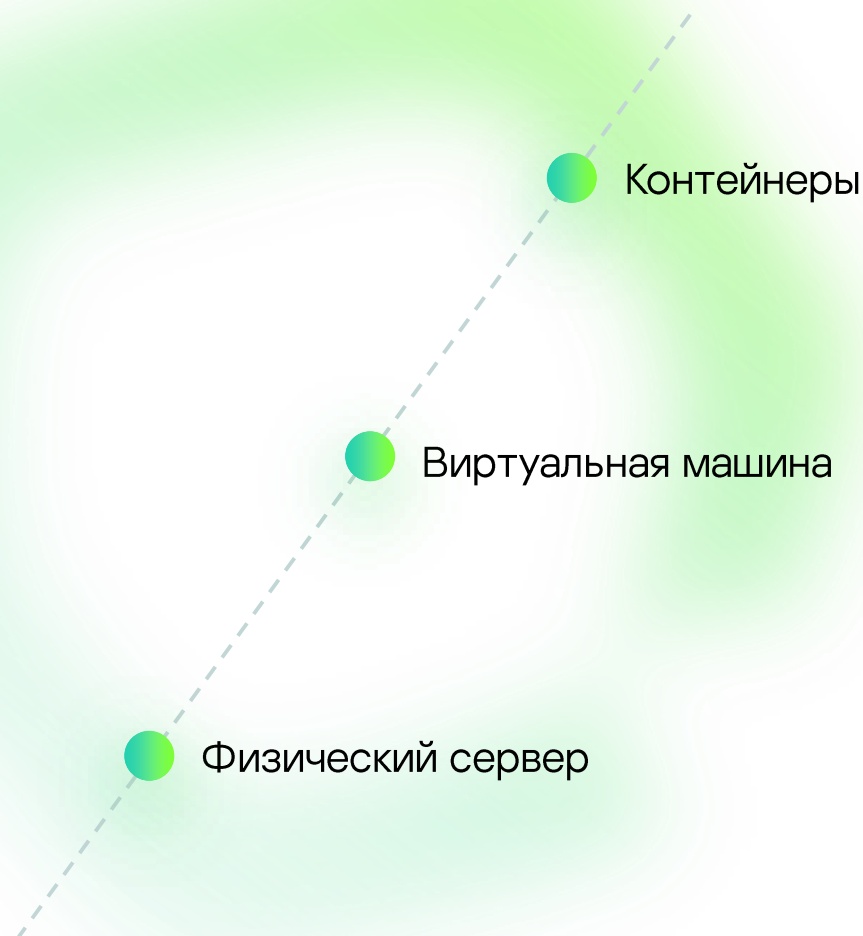
Что такое контейнеры?

Что это?

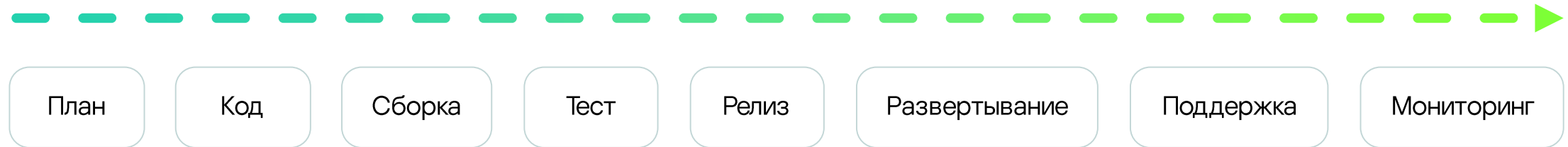
Контейнеризация является более легкой альтернативой виртуальным машинам. В классической схеме: один контейнер – одно приложение или сервис (микросервис)

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.



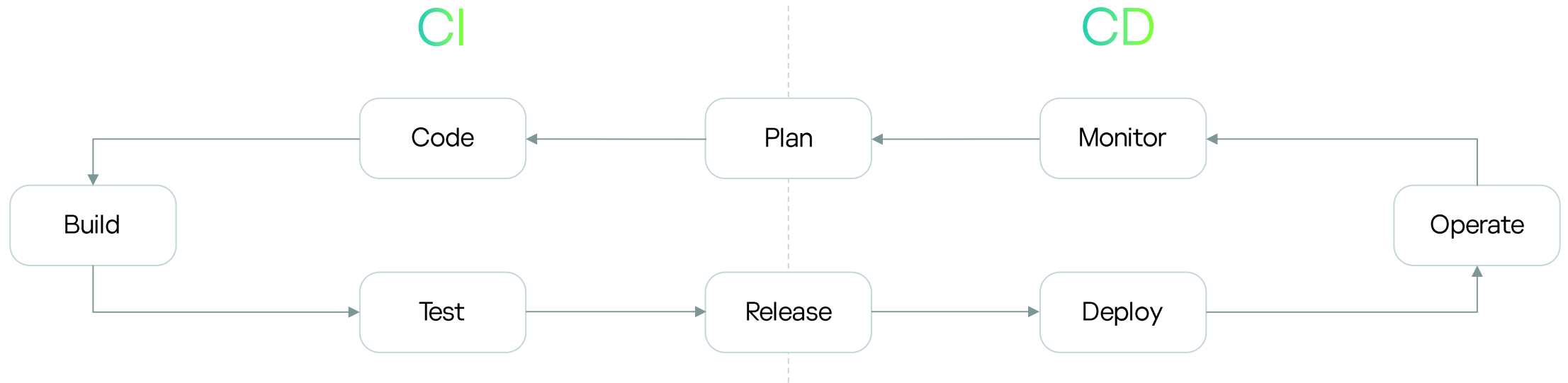
Традиционный цикл разработки (каскадная модель)



Ручной труд и много рутинных операций
Высокая цена ошибки
Простой команд из-за поэтапной работы

Разобщённость команд разработки и эксплуатации
Долгий цикл разработки и выпуска (до нескольких месяцев)

Непрерывная разработка / Непрерывное развертывание



Автоматизация рутинных действий

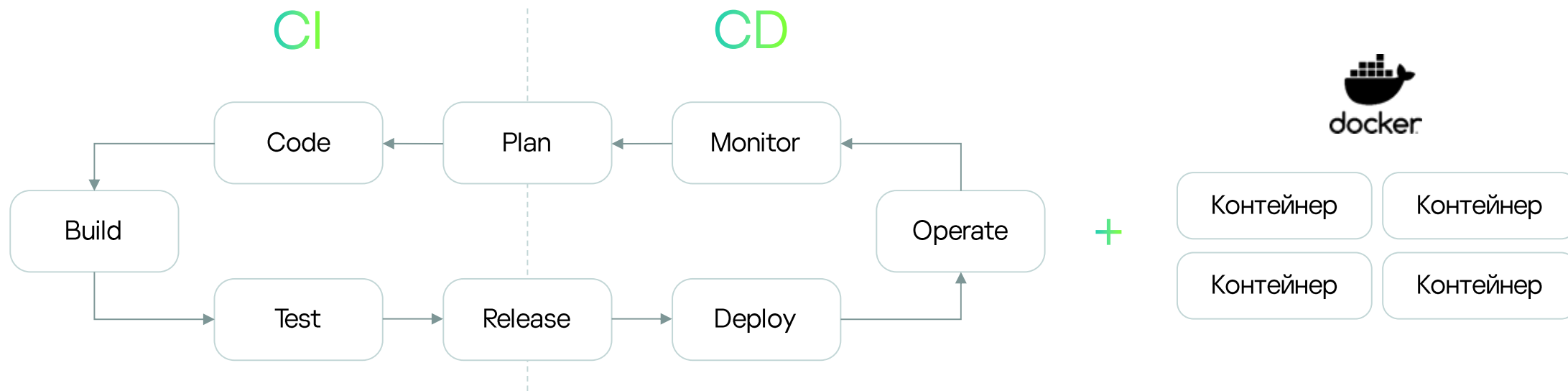
Короткий цикл разработки и выпуска, до нескольких недель

Более низкая цена ошибки

Параллельная работа команд над одним кодом

Снижение или уменьшение простоя команд

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

Хранение

Реестр

Образ контейнера

Образ контейнера

Образ контейнера



Сборка и запуск

CI / CD
платформа



Эксплуатация

Оркестратор

Контейнер

Контейнер

Контейнер

Контейнер

Среда запуска контейнеров

Операционная система

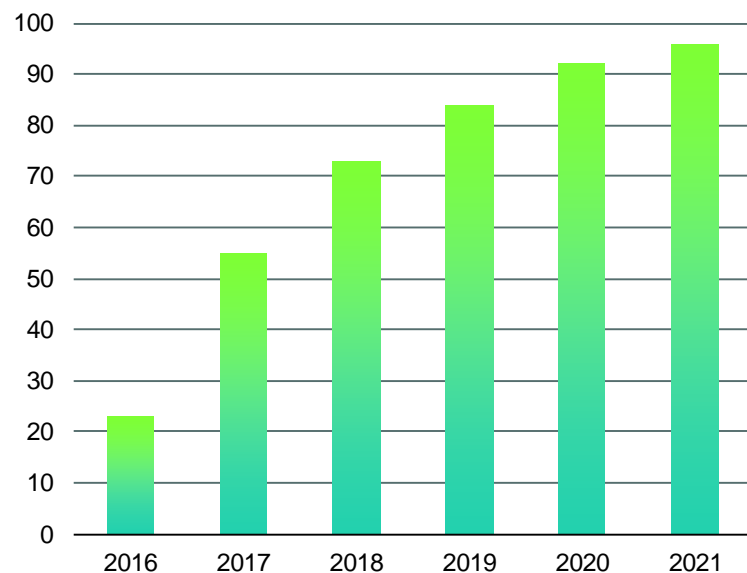
Рабочий узел



Сборка
↔
Хранение

Запуск
↔
Работа

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

В России среди компаний Топ-500 РБК**

~56%

компаний используют
контейнеры в разработке

27%

Компаний, в которых службы
безопасности интегрированы
в процесс разработки

~78%

компаний финансовой
сферы 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

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 или несанкционированные 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		The Register
Оркестратор	Проникновение в систему через незащищенную консоль администратора K8s	Майнинг криптовалюты на серверах Tesla Утечка чувствительной информации		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

Традиционные средства защиты серверов и виртуальных машин неэффективны для контейнеров

1. Необходимость установки агента на ОС хоста: не всегда возможно, сложность развертывания, риски деградации производительности и/или стабильности хоста и развернутых на нем приложений
2. Защита только работающих контейнеров на стадии эксплуатации, без учета специфики работы приложений в контейнерах
3. Нет данных о результатах сканирования образов и конфигурационных файлов, найденных проблемах и оценки рисков.
4. Нет защиты и обнаружения проблем на ранних стадиях работы с контейнерами: хранение, разработка, поставка
5. Нет анализа и контроля ошибок конфигурации контейнерных платформ.
6. Нет интеграции с реестрами образов, CI/CD, платформами оркестрации, отсутствуют возможности встраивания в процессы разработки
7. Нет визуализации всех компонентов контейнерных сред, зависимостей между ними и связанных рисков.

Только специализированное решение Container Security обеспечивает полную безопасность данных сред на всех стадиях работы с контейнерами

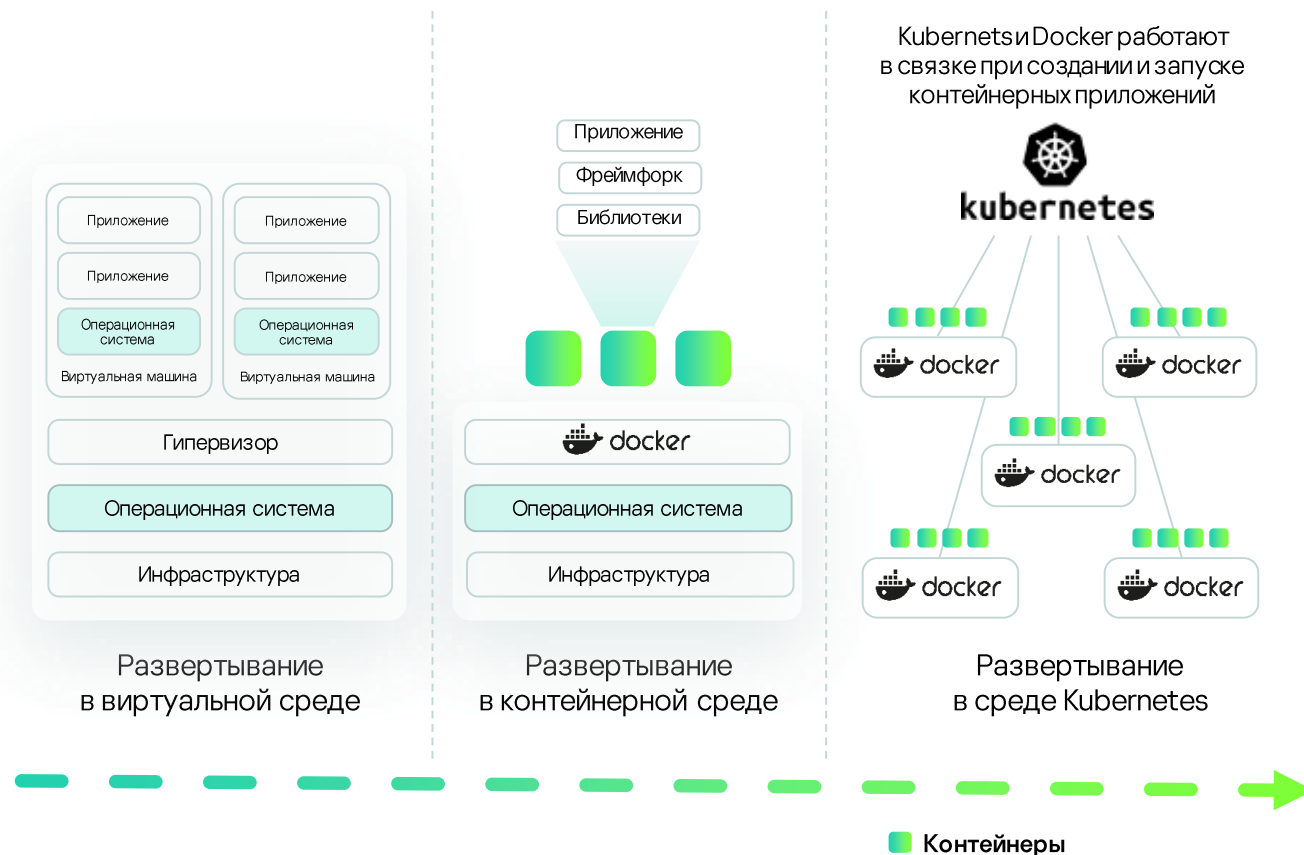
Сравнение Container Security и VM security

Традиционные средства защиты VM неэффективны для контейнеров

Традиционные средства защиты приложений разрабатывались под другие платформы (VM, bare metal) и не могут обеспечить защиту контейнерных платформ из-за различий в архитектуре, в частности отсутствия 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

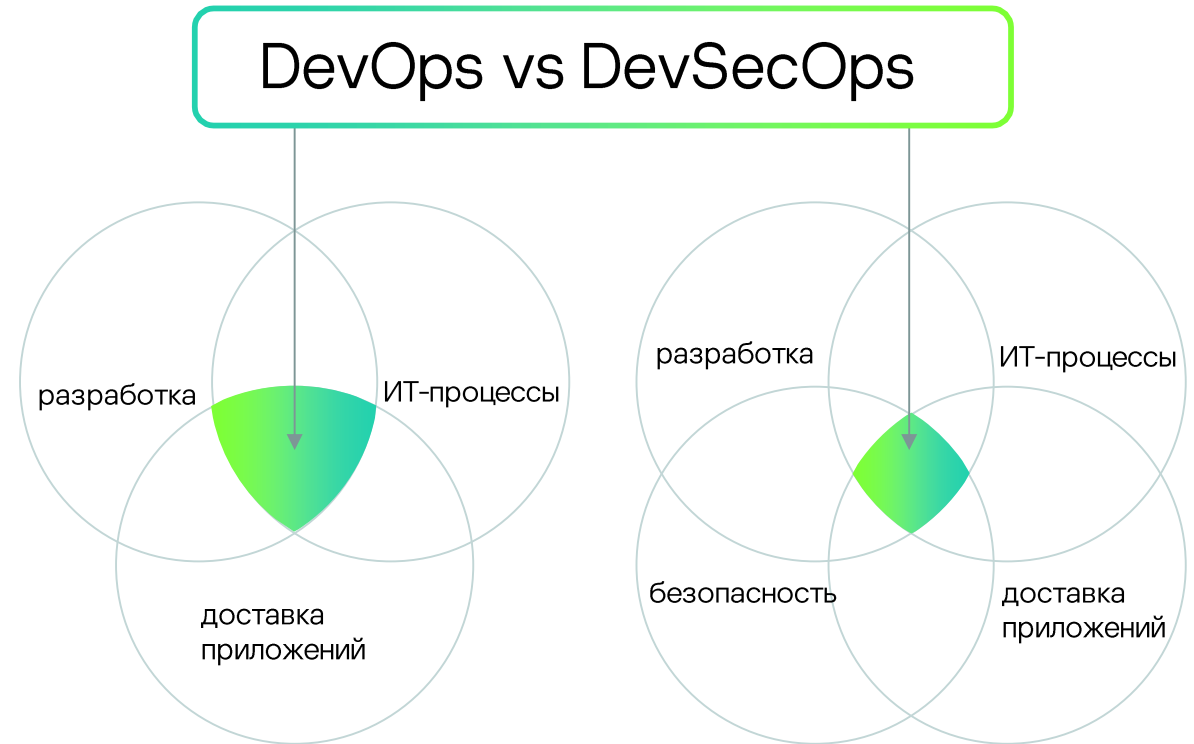


Kubernetes и Docker работают в связке при создании и запуске контейнерных приложений

Container Security как часть процессов подхода DevSecOps

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

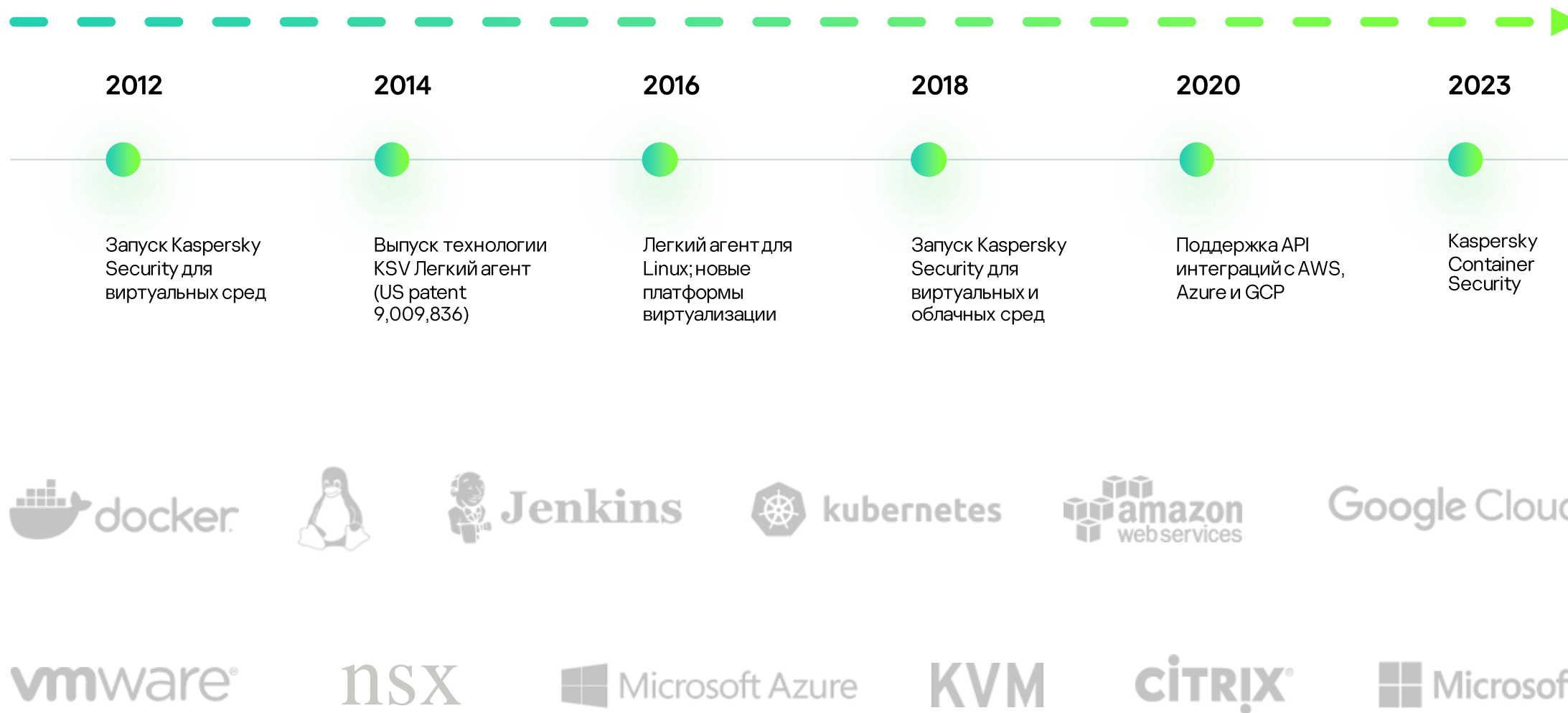
Комплексный инструмент для команд разработки и безопасности



Kaspersky Container Security



Эволюция решений Kaspersky для защиты облачных, виртуальных и гибридных нагрузок



Решение контейнерной безопасности

Закрывает проблемы
безопасности контейнерных
сред на всех этапах

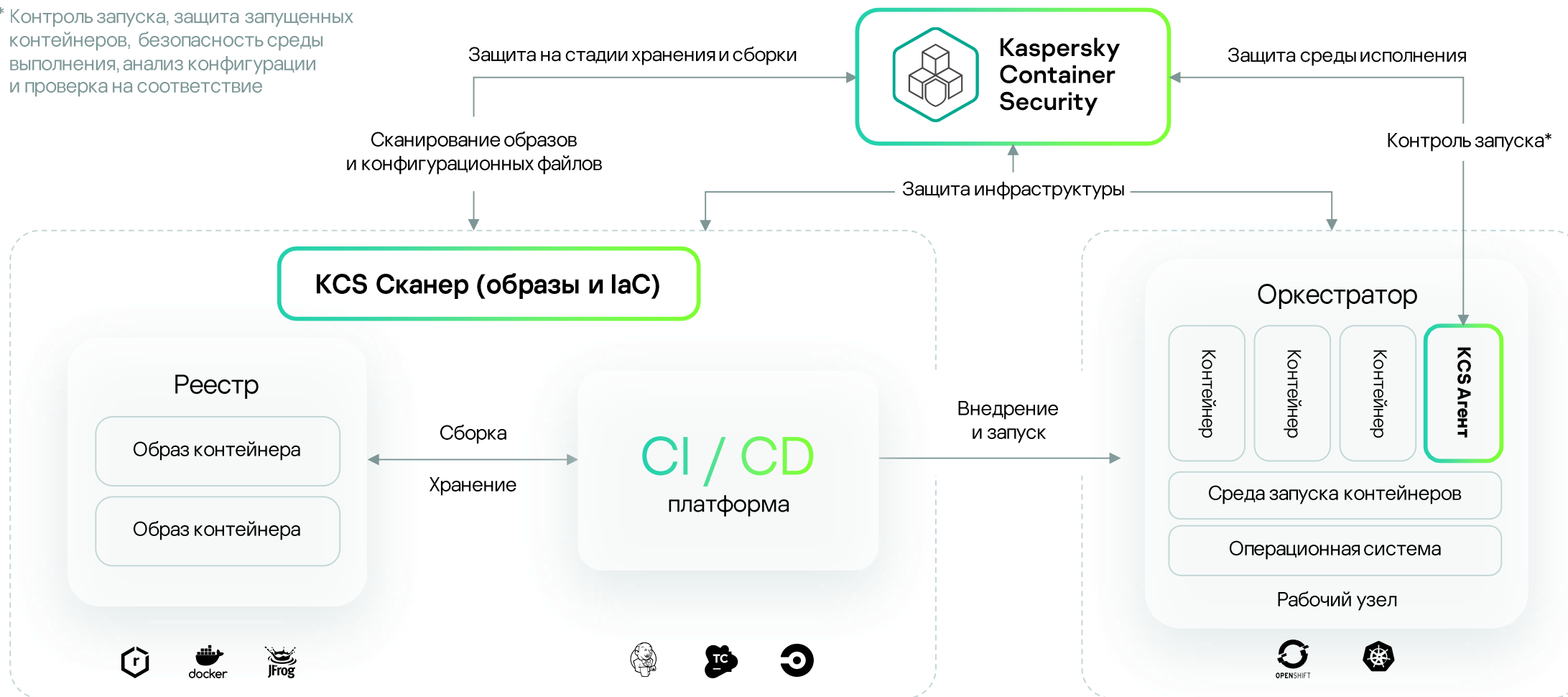
KCS обеспечивает безопасность всех компонентов контейнерных платформ: образы, реестры образов, оркестраторы, контейнеры, ОС хоста

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

Защита от файловых угроз
Проверка сетевого взаимодействия
Контроль целостности и работы приложений и сервисов в контейнере
Поведенческий анализ контейнеров

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 рекомендации по 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

Защита от файловых угроз

Поведенческий анализ

Контроль работы приложений и сервисов внутри контейнеров

ОС хоста

Проверка версий компонентов базовой ОС

Обнаружение ошибок конфигурации и рекомендации по исправлению

Уменьшение рисков за счет контроля 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

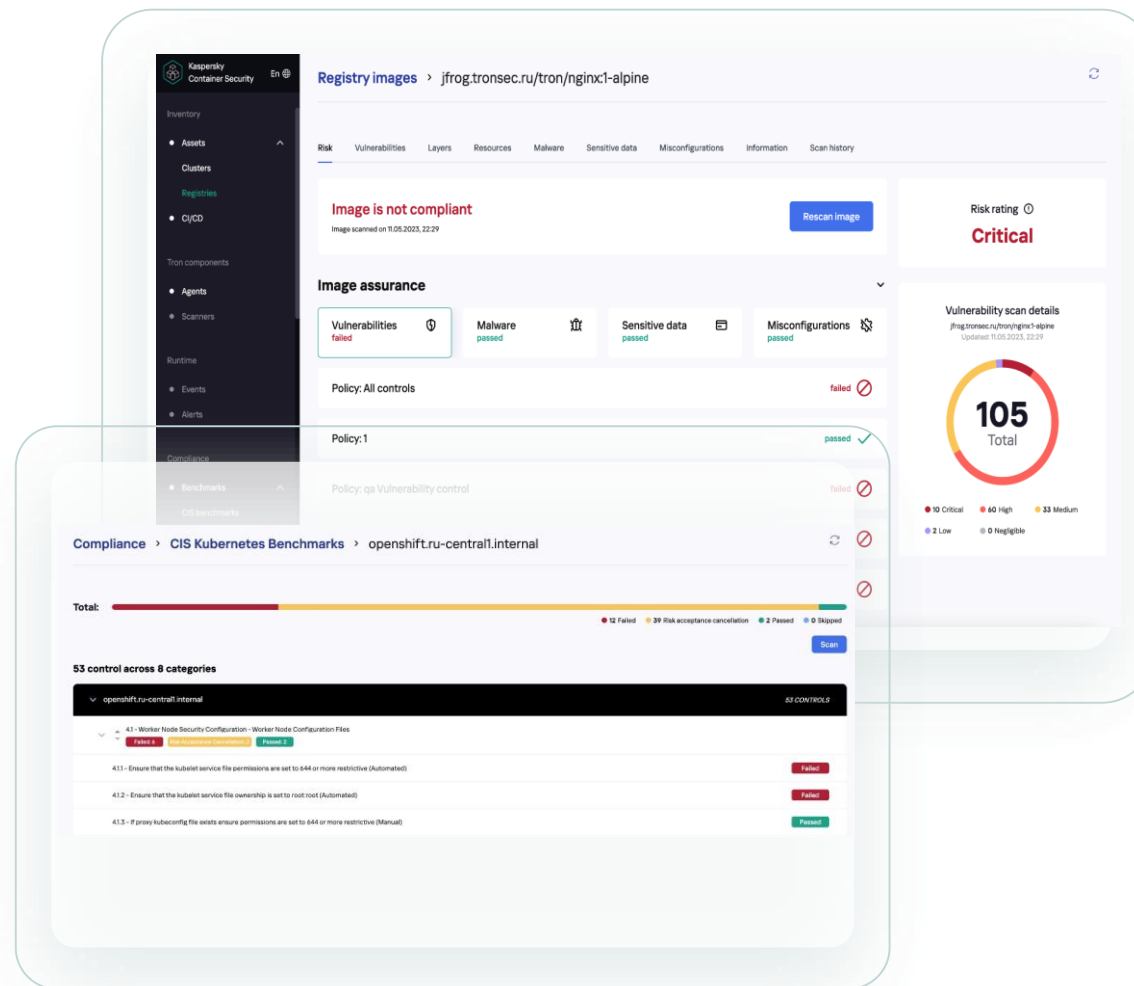
Добавление «quality gate» требует проверки собираемых контейнеров

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



Решение проблем ИБ

Наглядность для всех компонентов контейнерной инфраструктуры и связанных рисков

- Оценка и контроль рисков на всех стадиях работы с контейнерами
- Контроль и обеспечение безопасной конфигурации инфраструктуры, выявление устаревших и уязвимых компонентов
- Обеспечение безопасности приложений в контейнерах
- Соответствие требованиям регуляторов

Решение проблем ИТ

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



Q2 2023

New

Beta версия

- Сканирование образов контейнеров на различных стадиях

Q3 2023

1.0

Версия 1.0

- Функциональность Beta версии

Плюс:

- Защита на стадии запуска и работы контейнеров
- Анализ и обнаружение ошибок конфигурации компонентов контейнерной платформы

Q4 2023

1.1

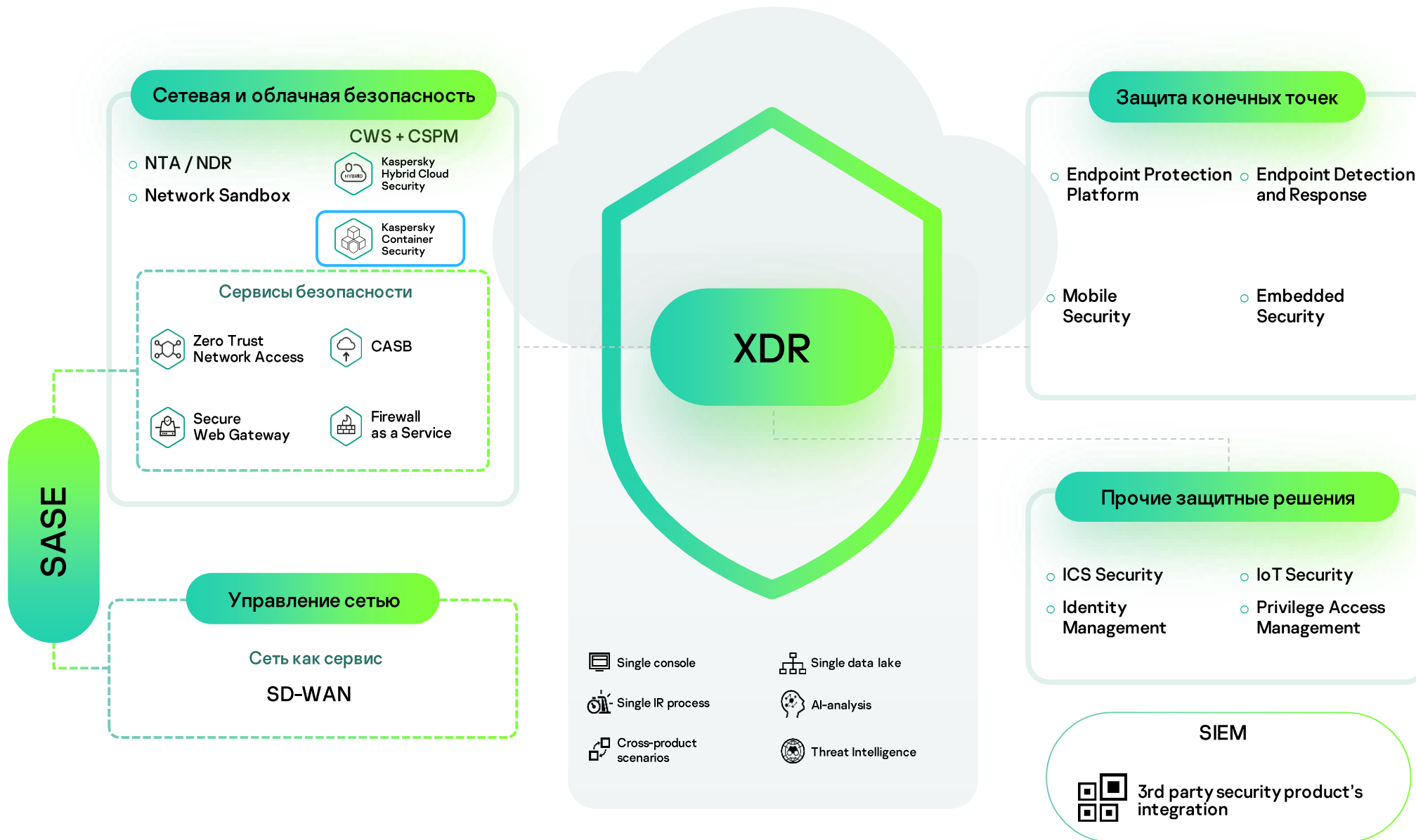
Версия 1.1

- Улучшенные технологии защиты на стадии запуска и работы контейнеров

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	●	●
	Поддержка сценария сортировки образов	●	●
	Сканирование конфигурационных файлов (IaC)	●	●
	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 профилей)		●
	Мониторинг 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		●	

Продукт лицензируется по нодам и просканированным образам контейнеров

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



Демо

QnA

Запишитесь

на демонстрацию
продукта через своего
аккаунт-менеджера,
партнера или на странице:



Вопросы спикерам: rub2b@kaspersky.com



Спасибо!