



Домклик усиливает безопасность разработки и эксплуатации приложений в контейнерах с помощью Kaspersky Container Security

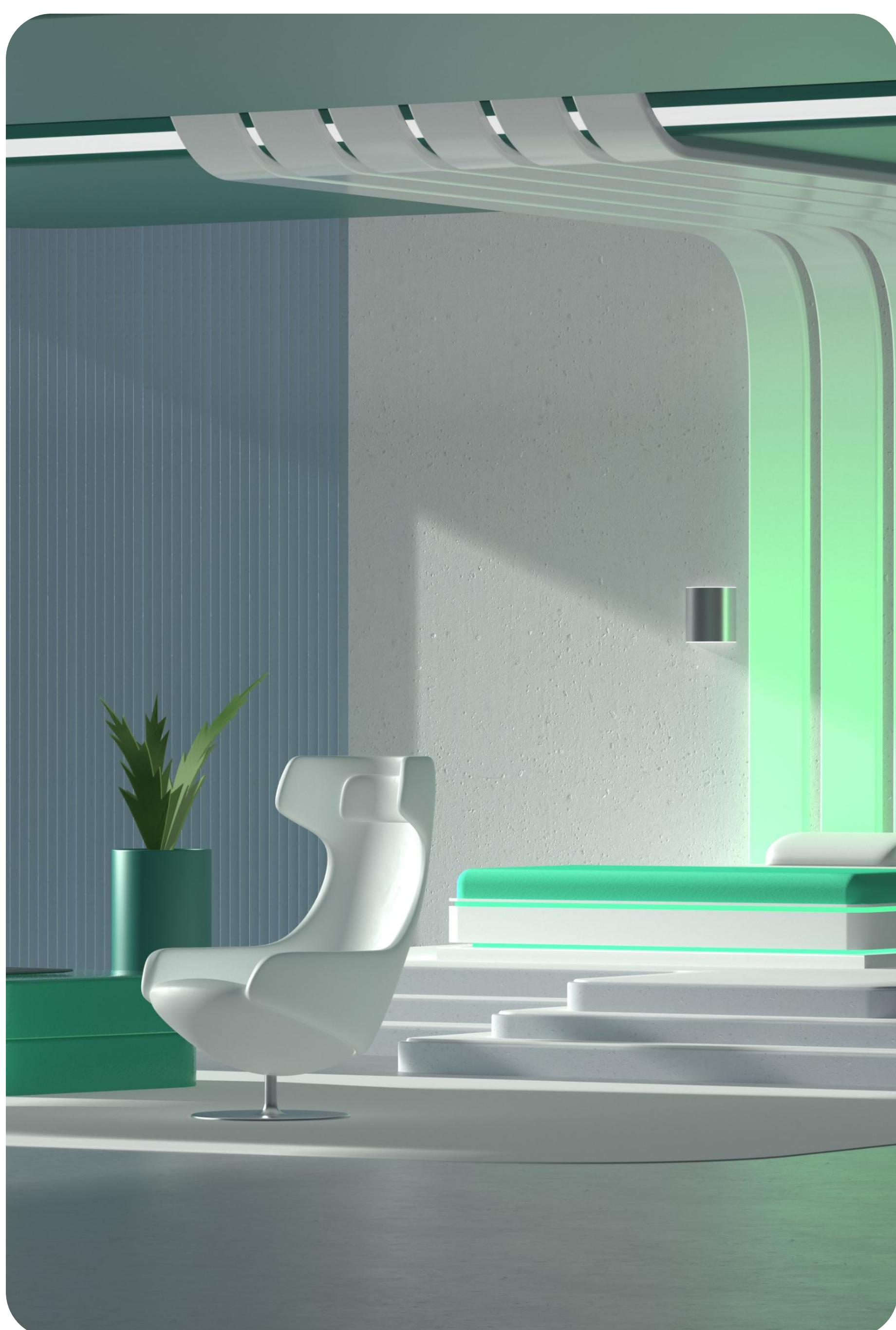
Интеграция Kaspersky Container Security в процессы DevOps и эксплуатации позволила Домклик модернизировать защиту контейнерной инфраструктуры от проверки образов до мониторинга и защиты приложений.

kaspersky





Контекст



Домклик от Сбера — сервис полного цикла в сфере недвижимости. Домклик помогает оптимально и комфортно решить любой вопрос с недвижимостью, оставаясь на стороне человека — клиента, агента, застройщика. Онлайн можно купить или продать недвижимость, снять или сдать её в аренду посуточно или на долгий срок, оформить ипотеку, зарегистрировать сделку и безопасно провести расчёты, следить за динамикой стоимости недвижимости и заботиться о доме с ремонтом, уборкой, заказом мастеров и другими услугами.

У Домклик собственная команда разработки и высокий уровень зрелости в области DevSecOps. Здесь понимают: **безопасность должна быть встроена во все этапы жизненного цикла приложения** — от написания кода до его эксплуатации в продуктивной среде. Сильная внутренняя экспертиза позволяет компании не только оперативно реагировать на возникающие риски, но и закладывать защиту как неотъемлемую часть архитектуры и функционала продукта.

Выбор решения

Контейнерная инфраструктура Домклик обеспечивает гибкость и масштабируемость разработки и эксплуатации приложений, но одновременно требует специализированной защиты. Рост нагрузки, повышение требований к стабильности сервисов и усложнение киберугроз, нацеленных на DevOps-процессы, привели к необходимости внедрения комплексного решения для безопасности контейнерной среды. После анализа предложений на рынке компания выбрала **Kaspersky Container Security** от «Лаборатории Касперского» — решение, которое **обеспечивает защиту на всех этапах жизненного цикла контейнеров**: от проверки образов и конфигураций до мониторинга и защиты в runtime.



**Kaspersky
Container
Security**

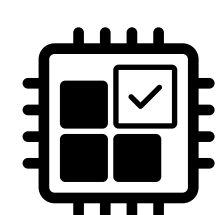
Kaspersky Container Security (KCS) – это специализированное решение для обеспечения безопасности всех ключевых элементов контейнерных сред и контейнерных приложений на всех этапах жизненного цикла: от разработки до эксплуатации

Преимущества Kaspersky Container Security

- **Специализированное решение** от надежного российского вендора на базе лучших мировых практик;
- **Учитывает архитектуру** и специфические риски контейнерных сред;
- **Всё в одном** решении — защита среды оркестрации, реестров, образов, контейнерных приложений, конвейеров микросервисной разработки;
- **Собственная разработка Policy Engine, Admission Controller**, функционала eBPF дают гибкость и независимость от open source и сторонних инструментов;
- **Предоставление информации об эксплоитах** для найденных уязвимостей;
- Решение класса Enterprise с **круглосуточной поддержкой 24/7**;
- Идеально подходит для **импортозамещения**.

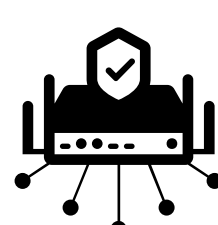
Решение

Ключевые возможности:



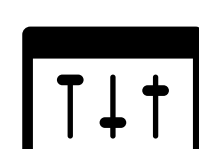
Встраивание в процесс разработки

- Интеграция с реестрами образов и платформами CI/CD
- Интеграция с системами безопасности и уведомлений
- Открытый API для легких интеграций с окружением



Защита контейнеров в рантайме

- Интеграция с платформами оркестрации
- Поведенческий анализ контейнеров на основе множества критериев
- Режимы блокирования и аудита нелегитимных активностей



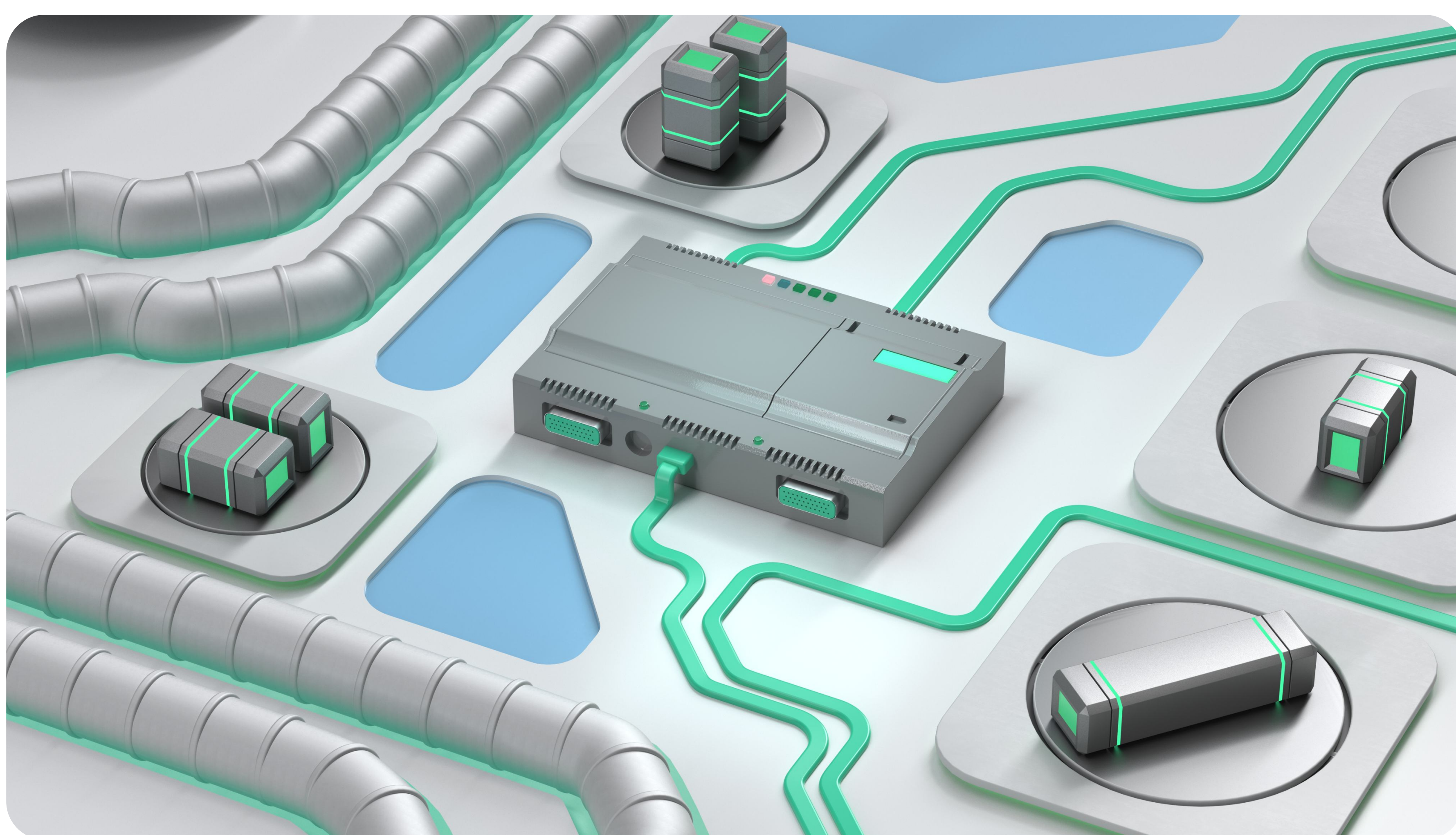
Автоматическая инвентаризация ресурсов в кластере

- Информативные дашборды и виджеты
- Визуализация ресурсов кластера, сетевого взаимодействия, ассоциированных рисков и «отработки» политик прямо на графе



Проверка на соблюдение требований регуляторов

- Проверка на соответствие образов и среды оркестрации стандартам и лучшим практикам ИБ
- Использование 30+ баз уязвимостей, включая БДУ ЛК, БДУ ФСТЭК, NIST
- Автоматизация рутинных проверок и действий



Результат



В инфраструктуре Домклик уже использовались решения «Лаборатории Касперского» для защиты конечных точек, почтового и веб-трафика. Многолетний опыт сотрудничества и доверие к технологиям вендора стали важной основой для выбора Kaspersky Container Security.

Ключевыми аргументами в пользу решения стали **открытый API** и **широкие возможности** по интеграции с внутренними системами Домклик, а также **экспертиза в вопросах ИБ, поддержка 24/7** и **готовность адаптировать продукт** под требования заказчика.

В процессе внедрения агент был **адаптирован для работы под высокой нагрузкой**, с учётом специфики внешних кластеров СУБД. Дополнительно оптимизированы размеры запросов, что позволило обеспечить **стабильную работу** при большом количестве сервисов в контейнерных кластерах.



«Ранее мы использовали open-source-продукты для защиты контейнерной среды, но с ростом масштабов контейнерных кластеров и требований к их надёжности мы столкнулись с ограничениями этих решений. Переход на Kaspersky Container Security позволил нам не только решить вопросы высокой нагрузки и особенностей инфраструктуры, но и значительно усилить защиту CI/CD-процессов без потерь в TTM. Отдельно хочу отметить вовлеченную и экспертную поддержку со стороны специалистов «Лаборатории Касперского» на всех этапах внедрения»

Андрей Лагоденко

директор по кибербезопасности, Домклик

«Мы смотрим на контейнерную безопасность не как на частный технический вопрос, а как на элемент общей устойчивости бизнеса. Если не видеть, что происходит внутри инфраструктуры, невозможно защитить ключевые активы — от клиентских данных до логики сервисов. Благодаря высокой степени автоматизации и прозрачному контролю Kaspersky Container Security позволяет командам выделять больше ресурсов на развитие своих продуктов, сохраняя высокий уровень защиты данных, что в конечном итоге выгодно для бизнеса»

Леонид Кудряшов

менеджер по развитию бизнеса Kaspersky Container Security

