

СберТех усилил безопасность контейнерных сред с помощью Kaspersky Container Security

Решение позволило встроить контроль безопасности в существующую защиту систем без их существенной перестройки и усилить защиту от угроз, характерных для контейнерных сред

kaspersky

SBER TECH



Контекст

Выбор решения

Как крупный и ответственный разработчик СберТех всегда следит за трендами и рисками, особое внимание уделяя безопасности. Рост масштабов контейнерной разработки и повышение требований к контролю образов, кластеров и контейнеров в среде выполнения сформировали потребность в специализированном средстве защиты.

По итогам анализа рынка таких решений и серии пилотных проектов выбор был сделан в пользу **Kaspersky Container Security.**

СберТех (АО «Сбербанк-Технологии») — российская ИТ-компания, входящая в экосистему Сбера. Компания разрабатывает цифровые решения и технологические платформы для Сбера и внешнего рынка.

Основное направление деятельности СберТеха — создание технологических решений, способствующих цифровой независимости и технологическому суверенитету. Компания разрабатывает и поддерживает инфраструктурное программное обеспечение, платформы для управления данными, инструменты аналитики, а также решения в области кибербезопасности.

Одним из основных продуктов СберТеха стала цифровая платформа Platform V — комплекс из более чем 90 инструментов, для разработки программного обеспечения и ускорения вывода продуктов на рынок.

Собственная экспертиза СберТеха в области оценки безопасности программного обеспечения и DevSecOps определяет высокие требования к применяемым средствам защиты. Компания использует комплекс решений корпоративного класса для защиты ИТ-инфраструктуры, в том числе ряд продуктов «Лаборатории Касперского», и последовательно усиливает безопасность на всех этапах разработки и эксплуатации программного обеспечения.

Kaspersky Container Security

Решение

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.

Продукт защищает бизнес-процессы организации, помогает соответствовать отраслевым стандартам и нормам безопасности, а также реализовать принцип безопасной разработки ПО (DevSecOps).
KCS — полностью российская разработка с учетом лучших мировых практик. Решение внесено в Реестр отечественного ПО.

Решение вышло на российский рынок летом 2023 года и динамично развивается, в том числе благодаря тесной работе с заказчиками и обратной связи от них.

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.**

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

Автоматическая инвентаризация ресурсов в кластере

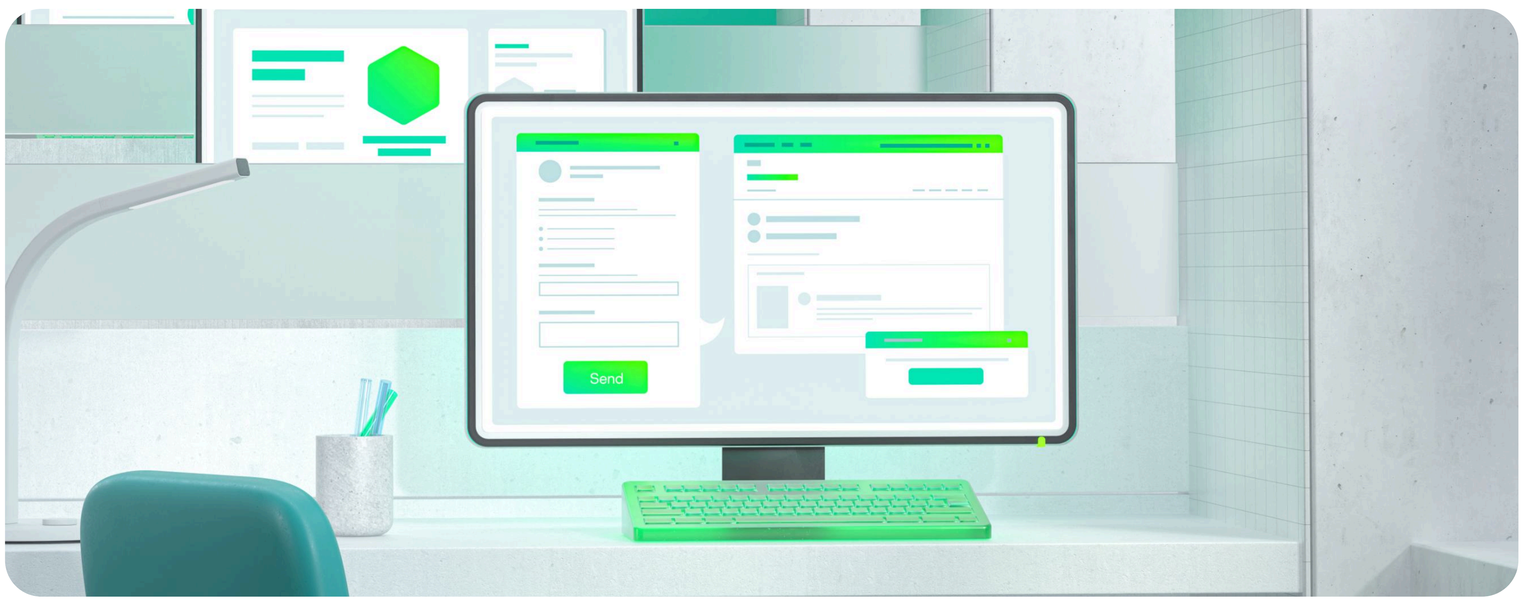
- Информативные дашборды и виджеты
- Визуализация ресурсов кластера, сетевого взаимодействия, ассоциированных рисков и «отработки» политик прямо на графе

Защита контейнеров в рантайме

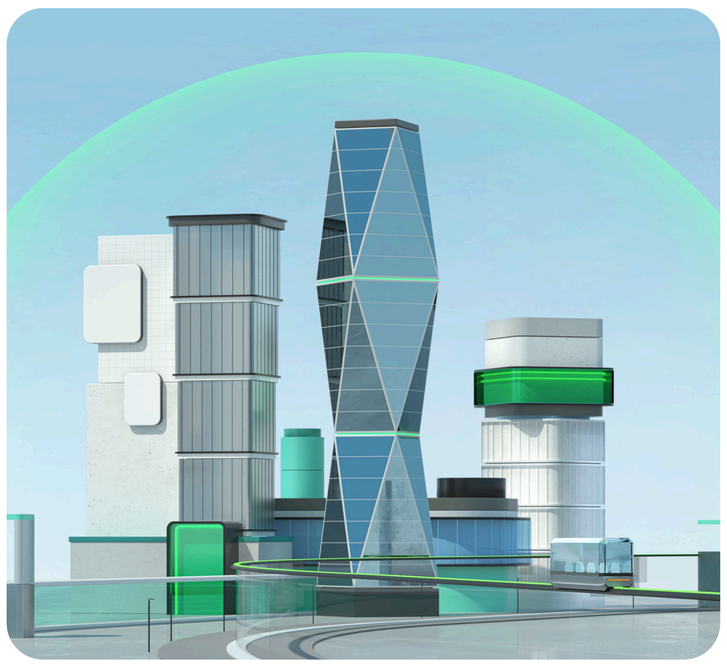
- Интеграция с платформами оркестрации
- Поведенческий анализ контейнеров на основе множества критериев
- Режимы блокирования и аудита нелегитимных активностей

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



KCS vs open source



В связи с уходом иностранных вендоров компании, использовавшие их продукты для защиты контейнерных сред, часто обращаются к open-source-решениям. Это накладывает дополнительные требования к команде ИБ и уровню ее компетенций, так как требует поддержки сразу множества независимых open-source-инструментов, тонкой настройки и интеграции между ними, в том числе через самописные компоненты.

Кроме того, никто не гарантирует отсутствия уязвимостей и багов в open-source-компонентах, регулярных функциональных апдейтов, актуальности используемых БДУ.

Преимущества Kaspersky Container Security в сравнении с open-source-решениями

- **Комплексная защита всех элементов** контейнерной инфраструктуры и защита приложений на всех этапах их жизненного цикла. Это явная экономия ресурсов и времени по сравнению с разработкой собственного решения на основе множества open-source-инструментов
- KCS не увеличивает и **не предъявляет новых требований** к количеству и квалификации сотрудников
- **Единая консоль** для настройки и управления вместо множества интерфейсов.
- Использование **30+ баз уязвимостей**, включая собственные базы «Лаборатории Касперского», БДУ ФСТЭК, NIST, БДУ производителей отечественных ОС (RedOS, Astra Linux и т.д.), Kaspersky Open Source Software Threats Data Feed для выявления уязвимостей и угроз в open-source-компонентах
- **Регулярные обновления** БДУ и информации об эксплоитах и их эксплуатируемости
- **Регулярные обновления** ПО, баг-фиксинг и расширение функционала
- **Подтверждённая экспертиза** «Лаборатория Касперского» в области кибербезопасности, безопасной разработки, антивирусных решений
- **Клиентская поддержка** 24/7 — важный элемент решения класса Enterprise

Результат



Внедрение Kaspersky Container Security позволило СберТеху усилить защиту контейнерных сред на ключевых этапах жизненного цикла информационных систем от формирования и хранения образов до их развёртывания и работы в кластерах.

Благодаря внедрению решения контроль безопасности контейнеризированных информационных систем стал более системным и управляемым, при этом действующие процессы контейнерной разработки не потребовали существенной перестройки.

«От надёжности и защищенности инфраструктуры СберТеха зависит в том числе устойчивость технологических процессов наших клиентов, поэтому к безопасности наших информационных систем и продуктов мы предъявляем самые высокие требования. Нам было важно получить не просто инструмент сканирования контейнеров на уязвимости и вредоносное ПО, а комплексное решение, которое встраивается в существующие процессы и обеспечивает контроль на разных этапах жизненного цикла контейнерных приложений как с точки зрения политик безопасности, так и непосредственно в средах выполнения»

Всеслав Соленик
директор по кибербезопасности, СберТех

«Контейнеры имеют важнейшее значение для разработки, развёртывания и масштабирования программного обеспечения. Они широко используются в нативных облачных средах, DevOps и микросервисной архитектуре, что делает их привлекательной мишенью для кибератак. В ответ «Лаборатория Касперского» активно развивает Kaspersky Container Security и другие продукты для комплексной защиты бизнеса от всех видов компрометации»

Леонид Кудряшов
руководитель по развитию бизнеса Kaspersky Container Security

© 2026 АО «Лаборатория Касперского». Все права защищены.