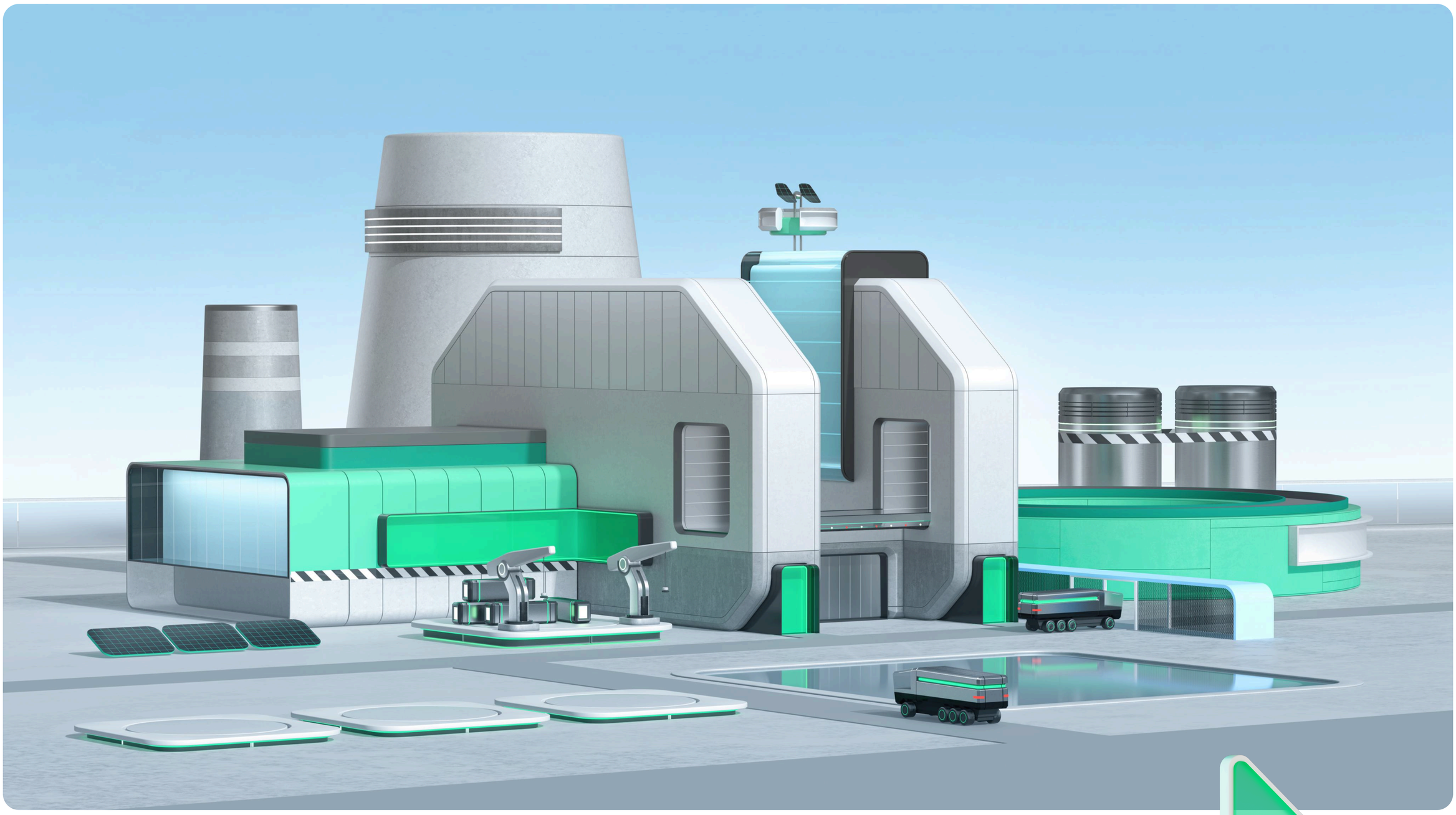
Защита контейнерных сред с помощью Kaspersky Container Security в энергетическом секторе

Крупная российская энергетическая компания выбрала Kaspersky Container Security для централизованной защиты контейнерной инфраструктуры

kaspersky



Предыстория

Выбор решения

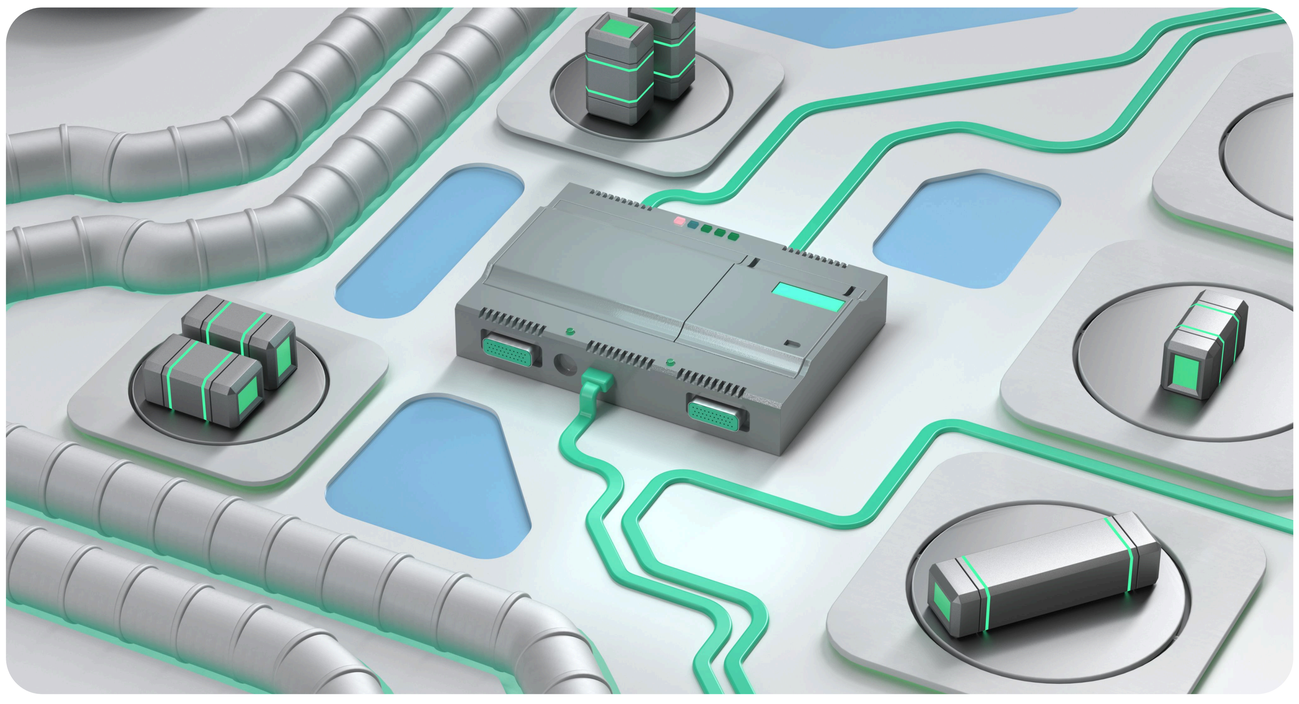
По мере развития контейнерной инфраструктуры и роста требований к безопасности в компании столкнулись с необходимостью перехода от решения, разработанного на основе открытого кода, к более надежному и удобному в использовании отечественному продукту. Основными драйверами стали потребность в оперативных обновлениях, наличии профессиональной технической поддержки и более высоком уровне управляемости процессами безопасности.

Особенно важной задачей для энергетической компании стал **анализ безопасности вновь внедряемых систем и мониторинг возникновения уязвимостей нулевого дня в эксплуатируемых сервисах.** В энергетике любой сбой может иметь критические последствия, поэтому бесперебойность внутренних сервисов — приоритет номер один.

В фокусе внимания - одна из крупнейших российских энергетических компаний, обеспечивающая надежное и качественное тепло- и энергоснабжение по всей стране. В энергетической отрасли бесперебойность работы внутренних сервисов имеет критическое значение, что предъявляет особые требования к защищённости ИТ-инфраструктуры.

Компания обладает высокой зрелостью в области информационной безопасности: собственный ИБ-департамент с глубокой экспертизой, круглосуточный SOC и выделенная команда DevSecOps.

Контейнерная инфраструктура компании развёрнута на российской платформе **Deckhouse** и используется для создания и поддержания внутренних сервисов. Среда включает test и prod окружения, которые требовали надёжной защиты на всех этапах жизненного цикла приложений.



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.

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.**

Контейнеризация — это технология, являющаяся более легкой альтернативой виртуальным машинам. Она позволяет запускать изолированные друг от друга приложения (микросервисы) на операционной системе хостового узла, используя общее ядро ОС. Код приложения упаковывается в контейнер вместе со всеми зависимостями, необходимыми для его запуска и работы.

Технология ускоряет процесс создания и доставки приложений. Однако архитектурные особенности контейнерных сред — например, отсутствие отдельной гостевой операционной системы и высокая динамичность их работы — не позволяют эффективно защищать их традиционными решениями, предназначенными для рабочих станций.

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.

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

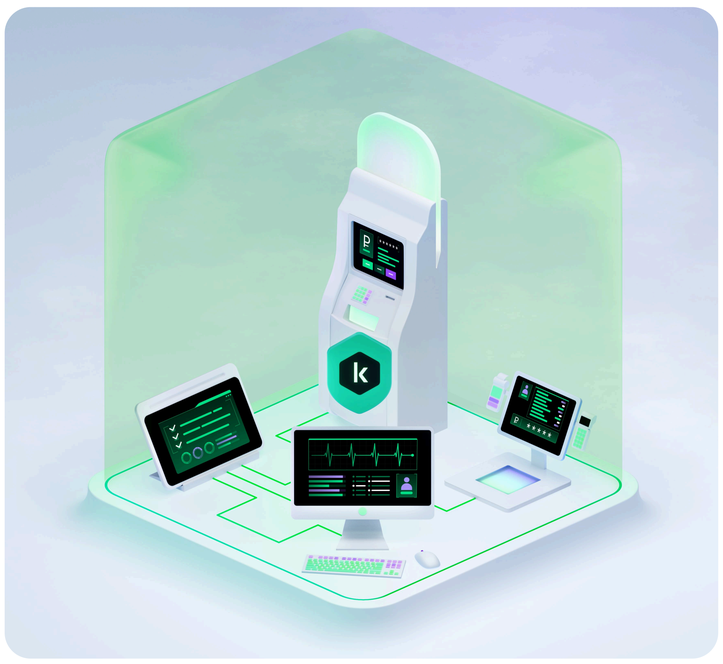
Защита контейнеров в рантайме

- 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

Результатом внедрения стало значительное повышение эффективности работы служб безопасности:

- Повысилась оперативность проведения экспертиз безопасности контейнерных приложений;
- Быстрая интеграция со сторонними сервисами благодаря API сократила время на развёртывание;
- Появился удобный интерфейс для комплексной оценки безопасности образов и кластеров;
- Сократились трудозатраты на организацию защиты в runtime и проведение анализа безопасности;
- Обеспечено централизованное формирование экспертиз безопасности вместо работы в разрозненных системах.

При выборе решения ключевыми факторами стали **репутация «Лаборатории Касперского»** как мирового лидера в области кибербезопасности, которому доверяют крупные отечественные компании во многих сферах деятельности, а также **технические преимущества продукта: поддержка широкого перечня актуальных инструментов,** включая отечественное ПО, **фокус на безопасности**, заложенный в решение на этапе его разработки, и широкие **возможности API для интеграции.**

Также важными аргументами стали **интеграция с распространенными реестрами образов** и CI-системами, наличие механизма работы с рисками и **открытого API** для взаимодействия с внутренними системами компании.

Внедрение прошло успешно, несмотря на необходимость адаптации к российской инфраструктуре на основе Deckhouse, операционных систем семейства Astra Linux и других отечественных решений. В процессе интеграции потребовалось внести изменения в приоритеты загрузки для корректной работы в runtime в сетевой среде Cilium. Пилотный проект длился почти год, но прошёл без серьёзных проблем — все возникавшие вопросы решались оперативно при поддержке экспертов «Лаборатории Касперского».

Одним из важных достижений стала интеграция KCS с корпоративным порталом, посвящённым ИБ. Это позволило централизовать процессы оценки безопасности контейнерных приложений.

«Переход на Kaspersky Container Security позволил нам значительно повысить уровень защиты критически важной контейнерной инфраструктуры. Особенно ценной стала возможность централизованного управления безопасностью и интеграция с нашими внутренними процессами. В энергетической отрасли, где бесперебойность работы систем имеет критическое значение, такой всеобъемлющий уровень защиты и контроля просто необходим»,

Алексей Тимонин
технический эксперт по ИБ

«Kaspersky Container Security успешно интегрировался в существующий процесс SDLC и упростил обеспечение ShiftLeft-подхода при обеспечении безопасности контейнерных сред. Основными достоинствами данного решения является продуманная архитектура, упрощающая его масштабирование, а также богатый функционал, позволяющий гибко реализовывать установленные в организации политики безопасности.»,

Александр Дьяченко
технический эксперт по ИБ