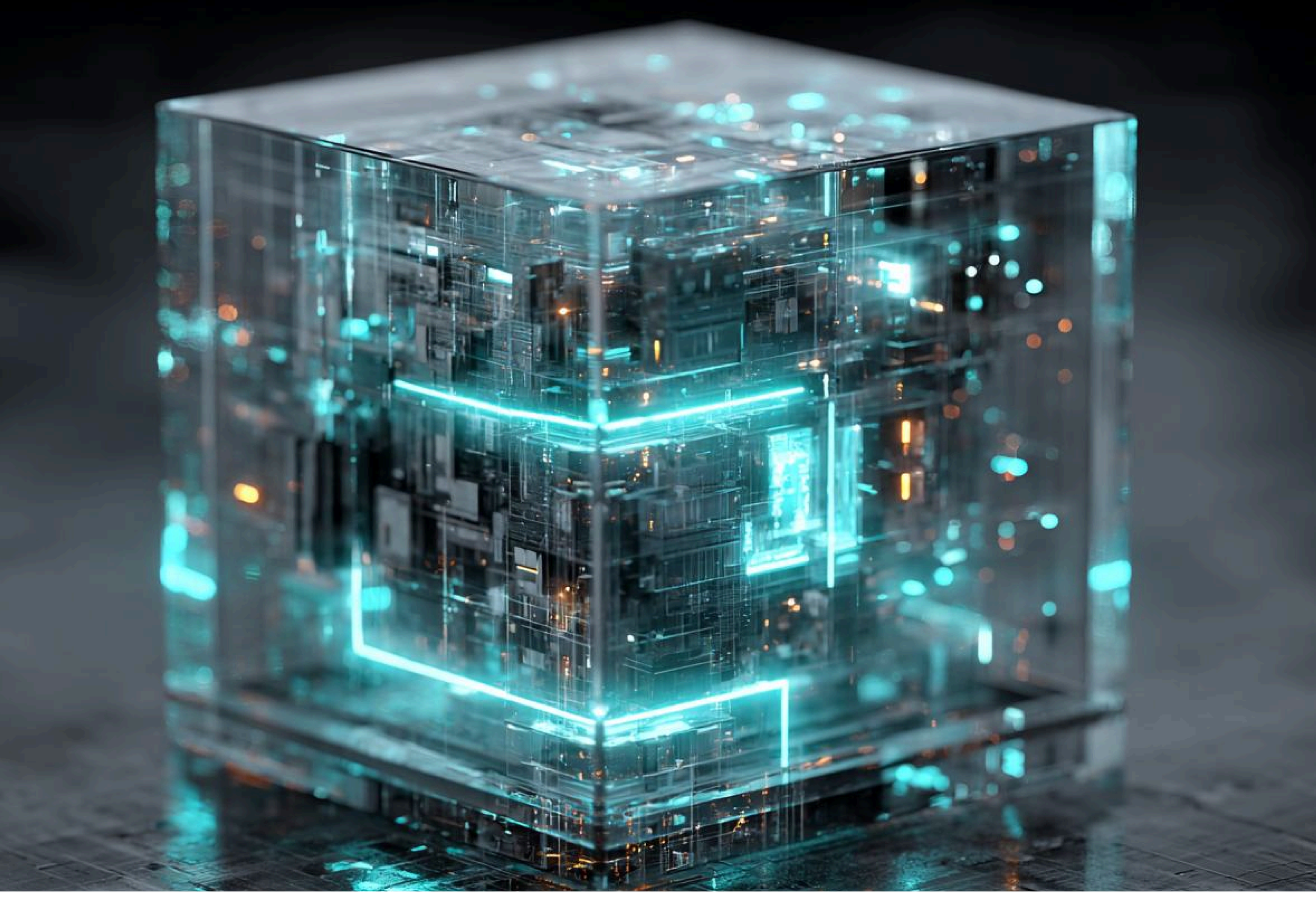


НПФ «БУДУЩЕЕ» построил контейнерную инфраструктуру под защитой Kaspersky Container Security

НПФ «БУДУЩЕЕ» обеспечил надежность и защищенность внутренних сервисов с помощью решения «Лаборатории Касперского»

kaspersky

БУДУЩЕЕ
ПЕНСИОННЫЙ ФОНД

Контекст

Поиск решения

Внедрение контейнерных сервисов на фоне агрессивного ландашфта киберугроз создали для команды Фонда новые вызовы безопасности. Необходимо было обеспечить надлежащий уровень защищённости и надежности новых сервисов и их дальнейшей эксплуатации.

НПФ «БУДУЩЕЕ» обозначил потребность в зрелом отечественном решении с поддержкой российских платформ оркестрации (в фонде используется одна из версий платформы «Штурвал», хостовые системы RedOS и «Астра»), широкими возможностями защиты в режиме эксплуатации (Runtime), понятным планом развития.

«БУДУЩЕЕ» — российский негосударственный пенсионный фонд (НПФ), созданный в 2014 г. Осуществляет деятельность в области негосударственного пенсионного обеспечения (НПО), обязательного пенсионного страхования (ОПС) и формирования долгосрочных сбережений (ПДС).

- **4 место** на рынке НПФ по объему активов
- **788 млрд рублей** активов под управлением
- **более 8,5 млн.** клиентов доверили фонду сбережения

Деятельность «БУДУЩЕГО» предполагает работу с данными миллионов клиентов, в том числе персональными и финансовыми. Этот факт кратно усиливает требования к защите ИТ-инфраструктуры и процессов организации: как со стороны регуляторов, так и со стороны рынка и пользователей. Поэтому **кибербезопасность – стратегический актив НПФ «БУДУЩЕЕ» как организации финансового сектора.**

У фонда есть опытная команда информационной безопасности. С 2019 года НПФ «БУДУЩЕЕ» обеспечивает информационную защиту фонда и данных клиентов решениями «Лаборатории Касперского».

Относительно недавно в организации началось внедрение технологий контейнеризации, в первую очередь для внутренних сервисов.

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.**

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

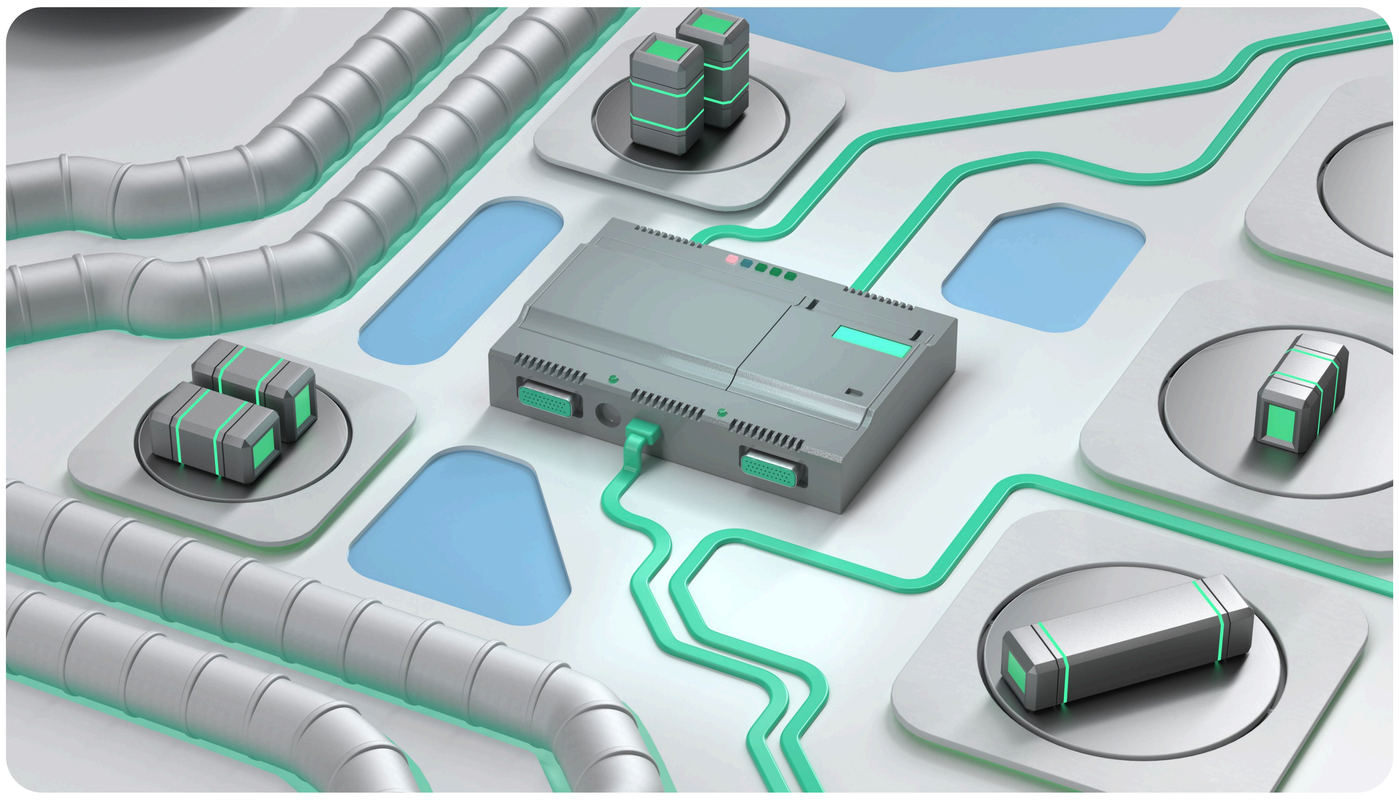
- Интеграция с платформами оркестрации
- Поведенческий анализ контейнеров на основе множества критериев
- Режимы блокирования и аудита нелегитимных активностей

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

По итогам тестов KCS показало себя наиболее зрелым и функциональным решением среди конкурентов и закрыло все потребности НПФ «БУДУЩЕЕ».

Тестирование, а затем внедрение KCS происходило одновременно с внедрением платформы оркестрации «Штурвал». Разворачиваемая контейнерная среда предназначалась для новых внутренних сервисов (приложения на основе микросервисов), разработанных подрядчиком Фонда.

Развёртывание KCS осуществила команда ИТ при поддержке специалистов «Лаборатории Касперского». После внедрения управление KCS перешло команде ИБ. Ключевыми сценариями использования стали:

- **контроль безопасности поставляемого ПО**
- **проверка образов перед запуском**
- **контроль контейнеров в среде выполнения**

KCS помогло НПФ «БУДУЩЕЕ» автоматизировать процессы проверки контейнеров, высвободив ограниченные ресурсы команды ИБ, а также обеспечить надежность и прозрачность контейнеров в инфраструктуре.

В результате внедрённые контейнерные сервисы оказались под надёжной защитой, с начала их активной эксплуатации не случилось ни единого серьёзного инцидента. Чувствительные данные клиентов Фонда — в безопасности.

Преимущества Kaspersky Container Security, выявленные в ходе конкурса и эксплуатации:

- **Широкая функциональность.** Важными преимуществами перед конкурентами для НПФ «БУДУЩЕЕ» стали:
  - Возможности защиты контейнеров в среде выполнения (Runtime)
  - Управление множеством кластеров из единого интерфейса
  - Автопрофилирование — автоматическое формирование профилей не только для отдельных контейнеров, но и для множества сущностей, например, групп контейнеров внутри кластера.
  - Встроенный антивирусный движок на основе KES for Linux (без необходимости установки новых агентов), который позволяет обеспечить высококлассную автоматизированную защиту нод.
- **Экономия ресурсов команды.** KCS — решение, доступное из коробки с простым и удобным интерфейсом. Это позволяет внедрить и эксплуатировать его без необходимости расширять штат. Кроме того, пользователям доступна специализированная поддержка вендора 24/7.
- **Удобство контроля и прозрачность.** Высокое качество сканирования контейнеров обеспечивает прозрачность инфраструктуры и ее управляемость, благодаря, например, визуализации рисков на карте кластера.
- **Сильная разработка (RnD)** и амбициозный **Roadmap,** учитывающий запросы и потребности заказчиков. С выходом версии 2.4 команда Фонда рассматривает возможность использования ИИ функционала для анализа образов.
- Помощь в соответствии **требованиям регуляторов.** KCS сканирует контейнеры на основе 30+ угрозных баз, в том числе БДУ ФСТЭК России. В 2026 году ожидается получение сертификатов ФСТЭК России.

Результат

«Контейнеризация становится ключевым инструментом для ускорения разработки и масштабирования сервисов в финансовом секторе. Однако, как любая новая технология, она обладает определенной спецификой. Работая с финансовыми данными миллионов клиентов, мы не можем позволить себе компромиссов в вопросах безопасности, поэтому для нас было важным прорабатывать вопросы защиты контейнерной инфраструктуры на каждом этапе её создания. После тщательного анализа рынка и тестирования нескольких решений мы выбрали Kaspersky Container Security. Оно полностью соответствует нашим требованиям, позволяет реализовать подход Shift-Left, дает возможности надежно контролировать наши сервисы в контейнерных средах»

Андрей Петухов
начальник отдела защиты информации НПФ «БУДУЩЕЕ»

«В финансовом секторе удобство сервисов и безопасность должны идти рука об руку. Kaspersky Container Security предлагает многоуровневую защиту — от статического анализа кода и проверки зависимостей до поведенческого мониторинга и автоматического реагирования на инциденты в среде выполнения. Это позволяет финансовым организациям не просто реагировать на угрозы, а предотвращать их на ранних этапах. Кроме того, он обеспечивает “бесшовную” защиту контейнеров без замедления бизнес-процессов — а это критически важно для организаций, где любой инцидент может обернуться критическими последствиями»

Леонид Кудряшов
руководитель по развитию бизнеса Kaspersky Container Security