МКБ (Московский кредитный банк) выходит на новый уровень защиты разработки с Kaspersky Container Security

В рамках процесса импортозамещения МКБ внедрил решение Kaspersky Container Security для обеспечения защиты контейнерной разработки. Это позволило сохранить высокий уровень безопасности разработки и усилить защиту данных пользователей.

kaspersky

МКБ

Контекст

МКБ (Московский кредитный банк) входит в топ 5 крупнейших банков России по размеру активов, а также в список системно значимых финансово кредитных институтов, утверждённый ЦБ РФ.

МКБ рассматривает удобство и комфорт клиентов как одну из ключевых задач. Особое внимание уделяется вопросам безопасности, что позволяет поддерживать доверие пользователей — важный элемент успешной работы финансовой организации.

МКБ — универсальный банк, предоставляющий широкий спектр продуктов и услуг всем основным категориям клиентов: крупнейшим и крупным компаниям, среднему и малому бизнесу, а также физическим лицам, в том числе в сегменте private banking.

Банк активно развивает цифровые сервисы, используя передовые методы и инструменты разработки, включая технологии контейнеризации. В МКБ функционируют собственное подразделение R&D и команда DevSecOps, которая отвечает за безопасность процессов разработки.

В банке уже используют решения и сервисы «Лаборатории Касперского», включая Kaspersky Security для бизнеса, виртуальных и облачных сред, Anti-Targeted Attack, KEDR Expert, защиту для почтовых серверов и Kaspersky Thin Client.

Выбор решения

В рамках развития контейнеризации и обеспечения безопасности банк стал оценивать и тестировать несколько отечественных решений.
В результате МКБ выбрал **Kaspersky Container Security** как наиболее соответствующее предъявляемым требованиям.

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 надёжного 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 даёт гибкость и независимость от Open-Source и сторонних инструментов;
- **Предоставление информации об эксплойтах** 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 лёгких 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 и отзывы

Особенности внедрения

Адекватная оценка рисков и понимание угроз, связанных с использованием контейнеров, диктовали высокие требования к средствам защиты. Особое внимание уделялось проверке образов перед их развёртыванием и запуском в рабочей среде. Переход на Kaspersky Container Security позволил банку обеспечить необходимый уровень безопасности как в процессе разработки, так и для самих приложений.

МКБ протестировал несколько решений отечественной разработки и в итоге остановился на Kaspersky Container Security как наиболее соответствующем предъявляемым требованиям.

Решающими факторами выбора решения Kaspersky Container Security для МКБ стали:

- **Уникальная функциональность:** защита в режиме выполнения (Runtime) и поддержка интеграции с основными реестрами, такими как Harbor, Nexus, GitLab.
- **Высокое качество клиентской поддержки:** оперативная помощь в решении возникающих вопросов в ходе реализации пилотного проекта оказывалась несколькими командами «Лаборатории Касперского».
- **Гибкость и клиентоориентированность:** команда разработчиков внесла необходимые функциональные доработки в соответствии с конкретными требованиями банка.

В результате замена решения по защите контейнерных сред прошла успешно. Kaspersky Container Security эффективно выполняет свои защитные функции и способствует развитию программных продуктов.

«Финансовые данные наших клиентов требуют максимальной защиты, поэтому мы используем только проверенные решения. Тестирование Kaspersky Container Security подтвердило его эффективность в обеспечении безопасности контейнеризации и интеграции в наши процессы».

ВЯЧЕСЛАВ КАСИМОВ,
директор департамента информационной безопасности МКБ

«Kaspersky Container Security — важный элемент экосистемы решений для бизнеса, ведь в конечном итоге наша цель — защита всех видов цифровых активов наших заказчиков. Популярность технологии контейнеризации влечёт за собой развитие специализированных угроз, которые не могут быть отражены стандартными средствами. Kaspersky Container Security эффективно отвечает на вызовы времени, позволяет клиенту сосредоточиться на функциональном развитии собственных продуктов, сократить время релизов за счёт автоматизации и не переживать за вопросы безопасности».

МАРИНА УСОВА,
руководитель управления корпоративных продаж «Лаборатории Касперского»