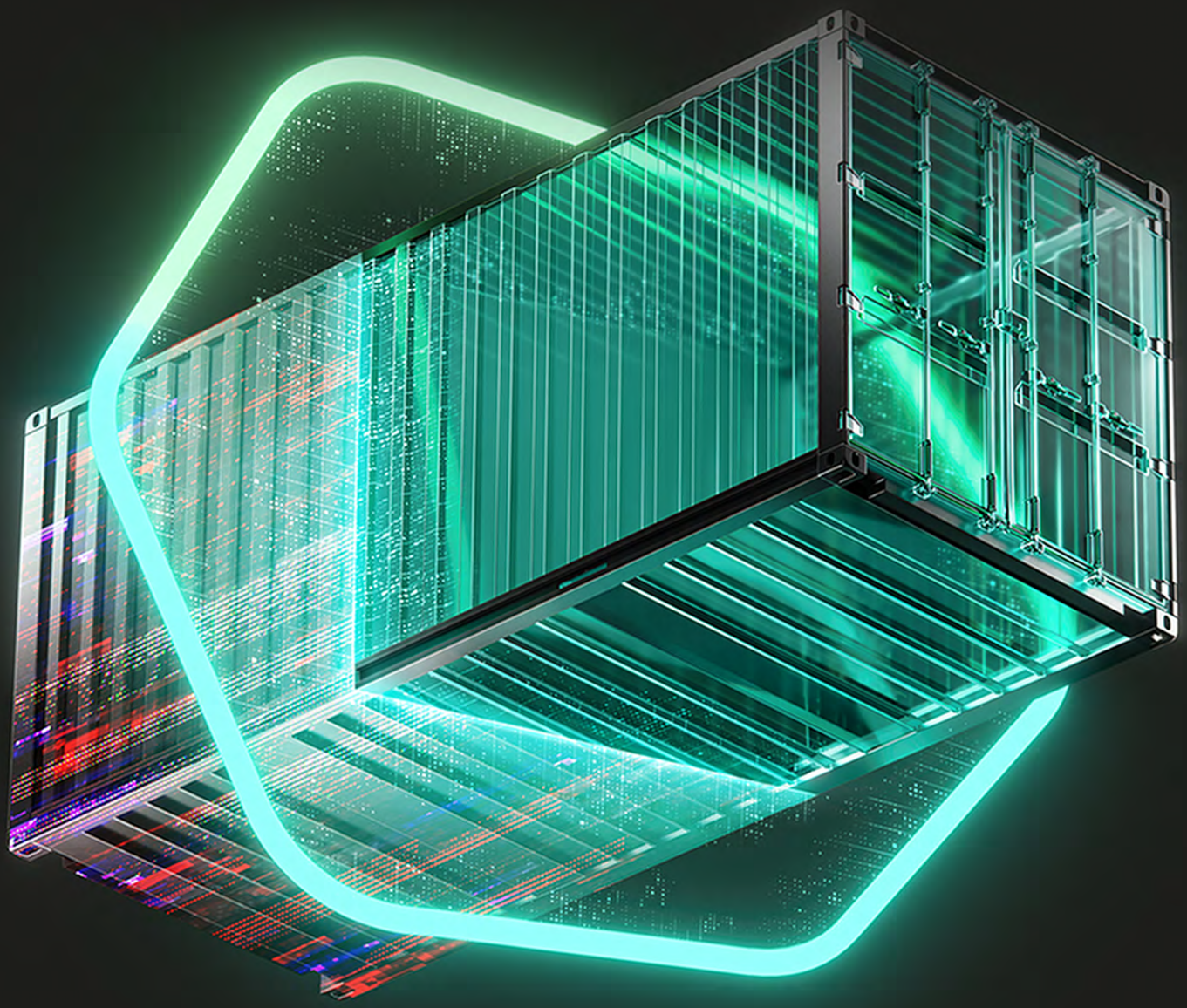
kaspersky



Отраслевые сценарии защиты контейнеров

Риски, примеры инцидентов и специализированная защита контейнерной среды в финансах, страховании, ритейле и телекоме

Содержание

#1

Облака и контейнеры — доверие в России растет

В России облачной инфраструктурой уже пользуются 64% компаний[1]. По оценкам «Лаборатории Касперского» примерно такой же процент размещают свои приложения в контейнерной инфраструктуре. Их число растет: по оценкам Gartner, к 2026 году применять контейнеры будут 90% крупных компаний в мире.

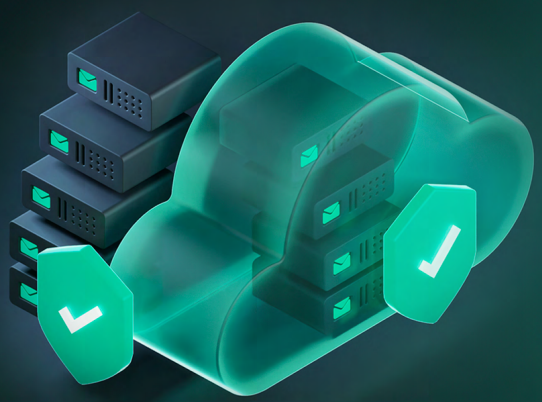
Предприятия, использующие облачную и контейнерную инфраструктуры, охватывают самые разные сферы — от IT и ритейла до промышленного производства. Бизнес доверяет облачным решениям наиболее важные приложения и сервисы, включая базы данных, клиентские сервисы и коммуникационные платформы.

В России наиболее активно в облака переносятся

Исследование CNEWS и «Лаборатории Касперского» «Курс на облачную безопасность в России – 2024», 2024 г.

80% компаний планируют расширять применение облачных технологий в разработке ПО в перспективе ближайших трех лет. Современное ПО, как правило, разрабатывают на основе микросервисной архитектуры с последующим развёртыванием в контейнерах. Микросервисную архитектуру и контейнерные технологии используют уже более половины компаний в России и мире[2].

Преимущества контейнеров очевидны: они позволяют запускать приложения в изолированных друг от друга средах, что повышает их отказоустойчивость и надежность. При этом контейнеры пользуются ОС, установленной на хосте, и работают только тогда, когда они нужны, что позволяет уменьшить потребление ресурсов. Однако, применение микросервисов и контейнеров принесло и новые риски в сфере ИБ. Они усугубляются тем, что **безопасность контейнерной среды невозможно обеспечить традиционными инструментами защиты**.



Мнимая безопасность контейнеров

В большинстве статей и исследований на тему безопасности контейнеров под безопасностью понимается устойчивость к инфраструктурным проблемам – критическим сбоям контейнеров, потерям данных. Изолированность контейнеров создаёт ложное ощущение безопасности. На практике каждый компонент инфраструктуры — от образов контейнеров до ОС хоста — это возможный вектор атаки. Угрозы могут возникать как в образах, так и позже при сборке и запуске. Ошибки в конфигурации инструментов также могут привести к проблемам.

Статистика «Лаборатории Касперского» показывает, что более **85%** компаний, использующих методы контейнерной разработки, сталкивались с киберинцидентами[1]. Компания Red Hat (вендор безопасных решений в области контейнеризации ПО), считает, что угроза еще серьёзнее: по их данным[3], в течение года **90%** организаций по всему миру сталкиваются хотя бы с одним инцидентом, связанным с безопасностью контейнеров или средой Kubernetes.

В России ситуация с безопасностью контейнерных сред осложняется уходом иностранных компаний и сворачиванием ими технической поддержки своих решений. Но даже с учётом этих обстоятельств **50%** компаний уже внедрили средства защиты контейнеров, а **80%** из тех, кто планирует расширять применение облачных технологий, намерены укреплять защиту каждого уровня стека контейнера[1].

Среди проблем в обеспечении информационной безопасности облаков российские компании называют:

32%

Невозможность выявить в облачной среде «слепые зоны» даже путём постоянного сканирования.

32%

Проблемы интеграции, связанные с существующими протоколами безопасности CSP.

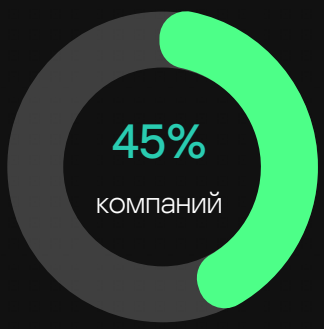
27%

Невозможность отслеживания и предотвращения использования неправильной конфигурации облачных сервисов во время их работы.

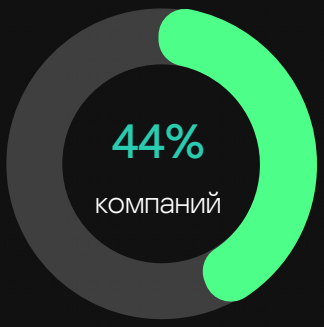
24%

Отсутствие возможностей анализа сценариев угроз.

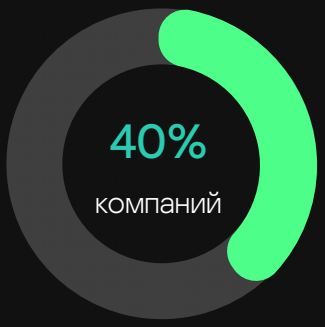
Организациям необходимо учитывать, что для защиты контейнерной инфраструктуры недостаточно не только традиционных средств кибербезопасности, но и проверенных методов, эффективных для виртуальных машин. К примеру, внутри контейнера в принципе нельзя запустить EDR- или VM-агент, а происходящие в нём процессы остаются практически невидимыми для стандартных систем защиты на хосте. Это делает невозможным обеспечение полноценной безопасности на этапе разработки и эксплуатации приложений и сервисов.



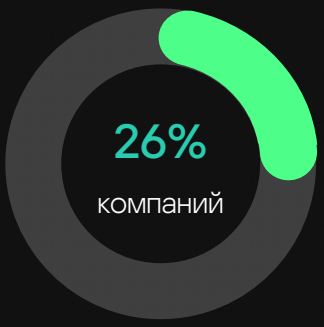
Сталкивались с инцидентами во время выполнения приложений в течение года



Столкнулись с проблемами на этапах сборки и развёртывания



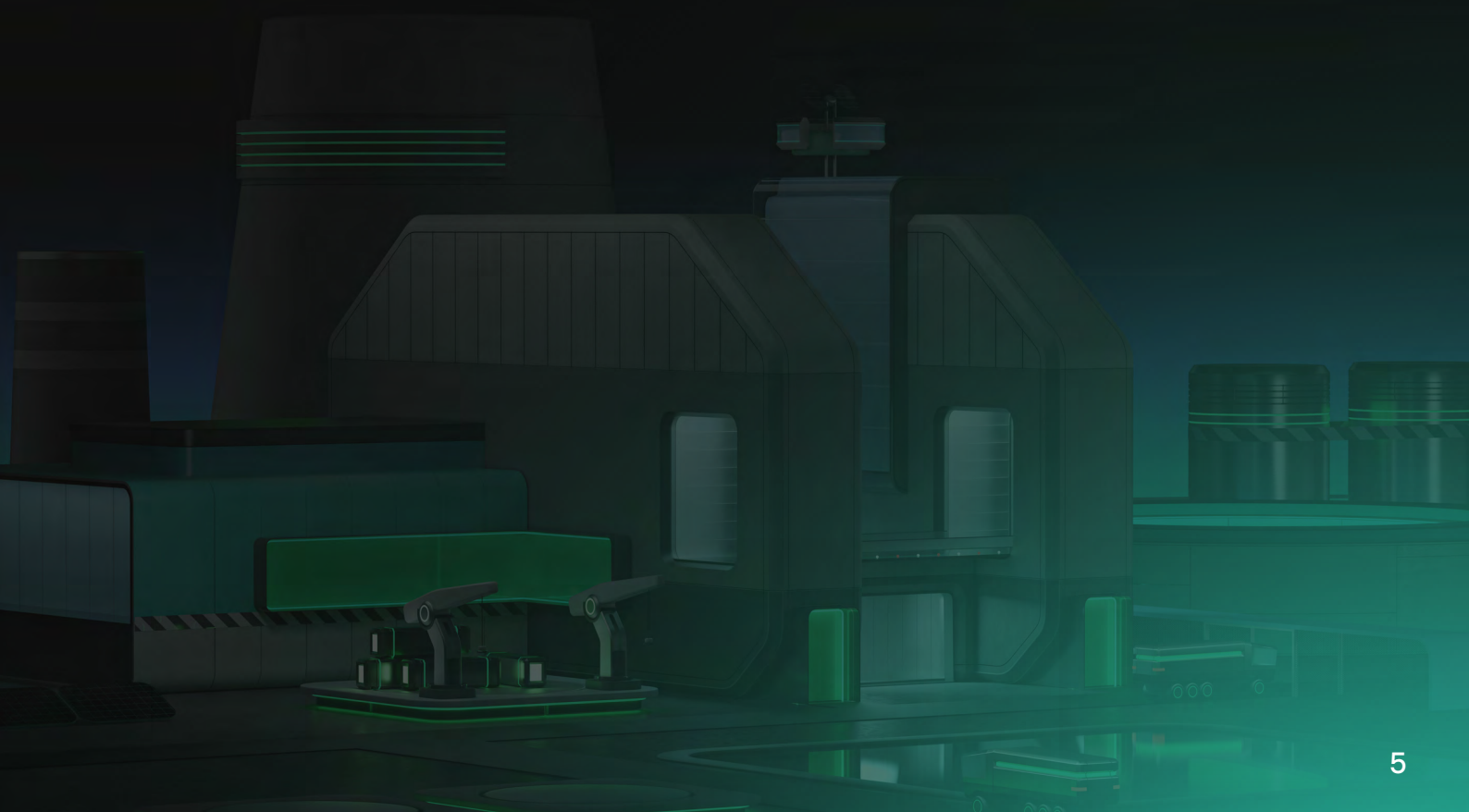
Обнаружили неправильную конфигурацию в своих контейнерах или средах Kubernetes



Не прошли аудит на соответствие нормативным требованиям

Исследование Red Hat «The state of Kubernetes security report», 2024 г.

Чтобы свести к минимуму риски ущерба от киберинцидентов в контейнерных средах и контейнеризированных приложениях, для начала вам нужно лучше понять уязвимости этой инфраструктуры и возможные векторы угроз. Как правильно расставить приоритеты при защите контейнерной среды на вашем предприятии? Какие угрозы будут наиболее опасны именно для вашей инфраструктуры и какие средства помогут максимально обезопасить её? Ответим на это ниже.



#2

Сценарии, при которых необходима специализированная защита контейнерной среды

Контейнеры — это не просто новый формат упаковки приложений. Это принципиально иная методология разработки и эксплуатации ПО с собственной архитектурой, жизненным циклом и уникальными угрозами. Это требует соответствующей адаптации подходов к информационной безопасности.

Все больше критических бизнес-систем переносят в облачную среду. Эти приложения могут быть изначально созданы по контейнерной технологии и поступать к клиентам уже в виде образов контейнеров. Поэтому важно не сопротивляться новой технологии, а выстраивать процессы ИБ с учетом её специфики.

Рассмотрим сценарии, когда защита контейнерной среды становится необходимостью, а также примеры применения контейнеризации в различных отраслях и сопутствующие риски.

2.1 Самостоятельная разработка приложений с микросервисной архитектурой

Крупные организации сегодня часто разрабатывают, обновляют и поддерживают свои сервисы силами собственных подразделений R&D. Чтобы обеспечить безопасность этих сервисов, средства проверки и защиты контейнерных приложений должны быть интегрированы в процесс разработки.

Риски

- Киберпреступники могут взломать конвейер CI/CD и внедрить бэкдоры в образы контейнеров
- При разработке в ПО могут остаться уязвимости, незамеченные разработчиками, но эксплуатируемые злоумышленниками
- Если разработчики используют готовые образы сторонней разработки, есть вероятность нарваться на образ, содержащий уязвимости или вредоносный код

Как поможет решение для защиты контейнеров

Комплексное решение для защиты контейнеров интегрируется с CI/CD-конвейерами для автоматического сканирования образов контейнеров и IaC на наличие уязвимостей, вредоносного ПО, неправильной конфигурации и конфиденциальных данных и останавливает конвейер, если не соблюдаются определенные условия соответствия. Сопутствующим преимуществом становится оптимизация разработки и сокращение времени выхода на рынок за счет автоматизации проверок на требования ИБ.

2.2 Миграция приложений в облачную среду

Организация может принять решение о миграции уже существующих приложений в облачную среду для повышения отказоустойчивости и гибкости инфраструктуры. При этом весь инструментарий контейнеризации также должен переместиться в облако. Особенное внимание стоит уделить переносу оркестраторов – в облаке их нагрузкой будет легче управлять, но и ошибки в конфигурации или при рефакторинге могут стоить дороже.

Риски

- При рефакторинге кода в нем могут появиться уязвимости, которые затем могут эксплуатировать злоумышленники
- Неправильно сконфигурированный кластер Kubernetes может дать злоумышленникам доступ к данным компании, в том числе конфиденциальным

Как поможет решение для защиты контейнеров

Комплексное решение для защиты контейнеров, такое как Kaspersky Container Security, может проактивно обеспечивать проверки файлов настройки и инфраструктуры Kubernetes для выявления неправильной конфигурации системы безопасности. Кроме того, решение автоматически сканирует образы запускаемых контейнеров, чтобы обеспечить полную видимость рисков еще до развёртывания.

2.3 Импортозамещение

Организации, использующие контейнерные технологии и практикующие зрелый подход к безопасности облачных инфраструктур, после 2022 года столкнулись с проблемой ухода зарубежных вендоров защитных решений с российского рынка. Для таких компаний важно найти отечественное решение для обеспечения защиты контейнеров, которое позволило бы сохранить высокий уровень безопасности с учетом российских трендов перехода на отечественные системы – оркестраторы, ОС и т.д.

Риски

- Продолжение использования иностранного решения без поддержки со стороны вендора грозит проблемами с безопасностью из-за отсутствия обновлений
- Продолжение использование иностранного решения вместо отечественного может противоречить требованиям законодательства РФ (в частности, Указу Президента №250) и стать причиной наложения штрафа на организацию
- Отечественное решение может не покрывать все риски, охваченные прежде использовавшимся решением от иностранного вендора
- Отсутствие поддержки отечественных ОС западными решениями

Как поможет решение для защиты контейнеров

Решение Kaspersky Container Security создано на базе лучших мировых практик и предлагает защиту для всей контейнерной инфраструктуры и процессов:

- среды оркестрации,
- реестров образов и самих образов,
- контейнеров,
- контейнеризированных приложений,
- конвейеров микросервисной разработки.

Функциональность решения соответствует уровню лучших иностранных аналогов и уже успешно внедряется крунейшими российскими компаниями и международными клиентами за пределами России. При этом «Лаборатория Касперского» готова вносить необходимые доработки в индивидуальном порядке в соответствии с конкретными требованиями организации-заказчика и обеспечивать его поддержкой в режиме 24/7.

2.4 Выполнение требований регуляторов

Российские регуляторы устанавливают современные и строгие требования в области информационной безопасности, включая обязательное оперативное устранение известных уязвимостей. Поэтому решения для обеспечения контейнерной безопасности должны отслеживать уязвимости не только по западным источникам, таким как NVD, но и по БДУ, поддерживаемой ФСТЭК.

Кроме того, действующие в России законы требуют определенного уровня защиты чувствительных данных и систем, относящихся к критической информационной инфраструктуре (КИИ). Например, закон №152-ФЗ «О персональных данных» предписывает меры по обеспечению информационной безопасности систем, обрабатывающих и хранящих персональные данные. Контейнерные приложения, которые часто обрабатывают персональные данные клиентов, должны выполнять требования 152-ФЗ.

Приказ ФСТЭК №118 содержит требования к безопасности средств контейнеризации, обязательные для госструктур и организаций (в том числе относящихся к КИИ), работающих с гостайной и важными данными. Документ регламентирует не только управление доступом, но и предписывает обязательные функции защиты, такие как мониторинг уязвимостей в контейнерах, проверку конфигурации и контроль целостности контейнеров и их образов.

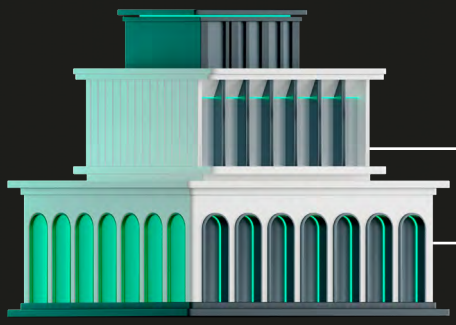
Риски

- Несоблюдение требований законодательства в сфере защиты информации грозит административным и уголовным наказанием
- Возможен отзыв лицензии на осуществление банковских операций

Как поможет решение для защиты контейнеров

Решение Kaspersky Container Security позволяет обнаруживать нарушения требований регуляторов в разных компонентах контейнерной среды и выполнять проверку в соответствии с отечественными и международными стандартами. Продукт использует более 30 баз уязвимостей, включая БДУ ФСТЭК, NIST, собственную БДУ «Лаборатории Касперского», в также позволяет подключать собственные базы заказчиков.

#3 Применение технологии контейнеризации и защиты для контейнеров в различных отраслях



ФИНАНСОВЫЕ И СТРАХОВЫЕ УСЛУГИ

Облачные технологии и контейнеризация предоставляют финансовым организациям гибкость, необходимую для ускоренной разработки и внедрения новых продуктов и услуг, масштабируемость для обработки изменяющихся объемов транзакций, а также повышают отказоустойчивость критически важных систем. Финансовые учреждения применяют контейнеры для банковских и клиентских сервисов, включая приложения, обеспечивающие бесперебойное обслуживание клиентов.

IT-системы банков, размещаемые в контейнерной среде

- Дистанционное банковское обслуживание (ДБО) физических и юридических лиц: мобильный банкинг, интернет-банкинг
- Платежные сервисы
- Дополнительные сервисы для продажи продуктов банковской экосистемы (страхование, продажа туристических туров и т.п.)

Последствия для финансовых организаций, связанные с недостаточной безопасностью контейнерной среды

Финансовое мошенничество

Манипулирование транзакциями, кража средств клиентов или компрометация торговых систем ведут к потере средств клиентами или банком.

Утечки данных

Кража финансовых данных клиентов, информации о счетах или данных кредитных карт грозят репутационным ущербом и штрафами со стороны регуляторов.

Нарушение работы банковских онлайн-услуг

Означает финансовые потери из-за простоя и ущерб репутации.

Примеры атак:

1

Злоумышленник получил доступ к записям клиентов из-за неправильно настроенного кластера Kubernetes. Неверные настройки WAF привели к получению им доступа к кластеру, а уязвимости побега контейнера – к боковому перемещению в пределах инфраструктуры.

Внедрение Kaspersky Container Security сделает возможным заблаговременное проведение аудита и проверки соответствия конфигурации и инфраструктуры Kubernetes. Это поможет выявлять неверные настройки безопасности, а также политики контроля запуска (Admission Control). Таким образом, развёртывание любого потенциального привилегированного контейнера будет заблокировано.

2

Атакующие внедрили вредоносный код в образ контейнера, используемый в банковском конвейере CI/CD. При развёртывании зараженные контейнеры связывались с командными и управляющими серверами злоумышленников, и в дальнейшем использовались для майнинга криптовалюты.

- При внедрении, Kaspersky Container Security интегрируется прямо в конвейер CI/CD и может автоматически проверять собираемый образ на наличие уязвимостей и вредоносов. При обнаружении таковых, решение останавливает процесс сборки.
- Используя политики контроля процессов на этапе эксплуатации, Kaspersky Container Security может блокировать запуск нежелательных процессов, например, криптомайнеров.

FSI: Реальный кейс от исследователей «Лаборатории Касперского»

Docker-контейнеры европейского банка взломаны с помощью вредоносного образа Redis (2024)

Что произошло?

Европейский банк, использующий Dockerized Redis для кэширования, был скомпрометирован после извлечения троянизированного образа Redis из публичного реестра.

Вектор атаки

Вредоносный образ, извлеченный из публичного реестра, содержал бэкдор, который передавал учетные данные на внешний сервер C2.

Злоумышленники получили доступ к внутренним банковским API и смогли проводить несанкционированные денежные транзакции.

Последствия

Прежде чем взлом был обнаружен, злоумышленники совершили мошеннические переводы на сумму $2,7 млн.

Сбои контейнера вызвали простои в приложениях мобильного банкинга.

Распространенные риски для контейнерной среды в финансовой сфере

Митигация риска

Небезопасные образы контейнеров

Использование ненадежных или плохо поддерживаемых базовых образов (например, из публичных реестров) может привести к появлению уязвимостей или неправильной конфигурации.

Необходимо сканировать образы на наличие уязвимостей.

Управление идентификацией и доступом

Несанкционированный доступ к конфиденциальным банковским данным и ресурсам в контейнерных средах из-за отсутствия надежных политик IAM.

Средство для защиты контейнерной среды должно уметь проводить аудит, чтобы выявлять неправильные политики контроля допуска.

Риски во время выполнения (runtime security)

По данным исследования «Лаборатории Касперского», почти треть (32%) киберинцидентов в контейнерной инфраструктуре происходит во время выполнения. На этом этапе контейнеры наиболее уязвимы для таких атак, как повышение привилегий и уязвимости нулевого дня.

Необходимо средство защиты, способное отслеживать и контролировать процессы, файловые операции и сетевую коммуникацию, а также политики контроля допуска (admission control) – для предотвращения развёртывания потенциально привилегированных контейнеров или контейнеров с особыми возможностями.

Проекты из практики «Лаборатории Касперского»

МКБ — универсальный банк, предоставляющий широкий спектр продуктов и услуг крупному, среднему и малому бизнесу, а также физическим лицам. В МКБ функционируют собственное подразделение R&D и команда DevSecOps, которая отвечает за безопасность процессов разработки.

МКБ (Московский кредитный банк)

Сценарий применения:

- Самостоятельная разработка приложений
- Импортозамещение иностранного решения для защиты контейнеров

Задача

В рамках процесса импортозамещения МКБ искал решение, которое позволило бы обеспечить защиту контейнеров и сохранить высокий уровень безопасности разработки.

- Импортозаместить иностранное решение для защиты контейнеров
- Реализовать глубокую проверку образов перед их запуском в контейнерной среде, а также интеграцию с реестрами (Harbor, Nexus, GitLab) и автоматизацию процессов проверки реестров и образов внутри
- Обеспечить защиту в режиме выполнения (Runtime)
- Предусмотреть возможность доработки защитного решения в соответствии с конкретными требованиями банка

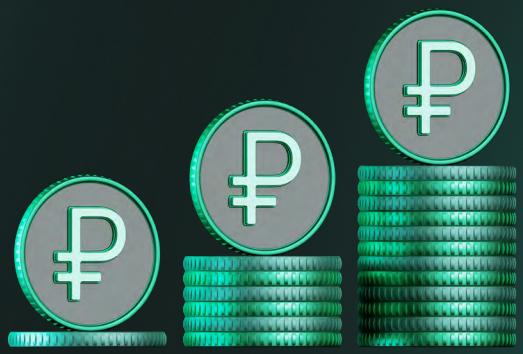
Выбор

Банк протестировал несколько отечественных решений. Наиболее полно предъявляемым требованиям соответствовал Kaspersky Container Security. Решающими при выборе стали следующие преимущества:

- Kaspersky Container Security – комплексное решение, охватывающее всю инфраструктуру и процессы в контейнерной среде. В решение заложено максимальное количество сценариев автоматизации и одновременно гибкости для заказчика.
- Клиентоориентированность: «Лаборатория Касперского» всегда чутко реагирует на обратную связь от заказчика и вносит необходимые изменения в функциональность решения. Команда поддержки готова оперативно прийти на помощь и непрерывно сопровождает команду заказчика в ходе реализации пилотного проекта.

Результат

Переход на Kaspersky Container Security позволил банку обеспечить необходимый уровень безопасности как в процессе разработки, так и для самих приложений. Замена решения по защите контейнерных сред прошла успешно.



Крупный банк в Египте

Сценарий применения:

- Миграция приложений в облачную среду

Банк стремится войти в топ-10 банков Египта по показателю рентабельности собственного капитала (ROE). Обслуживает клиентов через 35 филиалов по всей стране и постоянно расширяет клиентскую базу, открывая новые отделения и банкоматы.

Задача

Банк преобразует собственные сервисы в облачные нативные приложения и использует Red Hat OpenShift в качестве платформы оркестрации. Команда кибербезопасности банка хотела оценить решение, способное защитить их облачные приложения и инфраструктуру, однако не имела общей стратегии в отношении полной защиты среды.

Исходное требование: обеспечить сканирование уязвимостей в облачной среде.

Результат

«Лаборатория Касперского» провела для клиента консультации, где команду ИБ ознакомили с ландшафтом угроз для контейнеров и описали, какие уровни и возможности необходимы для полной защиты их среды. Банк реализовал пилотный проект, охватывающий часть его инфраструктуры. Клиент доволен достигнутым результатом и планирует расширения до полного охвата среды.

Kaspersky Container Security

Почему клиент выбрал Kaspersky Container Security:

- Высокое доверие к технологиям «Лаборатории Касперского» в сочетании с комплексными возможностями решения помогли выделиться на фоне конкурентов.
- Всеобъемлющий подход, сочетающий передовые технологии и многолетнюю экспертизу.

РИТЕЙЛ

Облачные нативные платформы обеспечивают ритейлерам масштабируемость для работы в пиковые сезоны покупок и стабильную производительность платформ электронной коммерции. Контейнеризация упрощает развёртывание различных приложений для розничной торговли, от управления запасами до управления взаимоотношениями с клиентами, помогая быстрее обновлять сервисы и более гибко реагировать на запросы рынка.

IT-системы ритейлеров, размещаемые в контейнерной среде

- Платформа электронной коммерции
- Мобильное приложение для клиентов: интернет-магазин, каталог товаров, рекомендательный сервис
- Программы лояльности для клиентов
- Внутренние сервисы складского учета
- Приложения, связанные системой управления цепями поставок (SCM): планирование спроса, поставок, логистика

Последствия для ритейлеров, связанные с недостаточной безопасностью контейнерной среды

Утечки данных клиентов

Кража платежной информации, личных данных или данных программы лояльности наносят ущерб репутации, приводят к оттоку клиентов и штрафам от регуляторов.

Нарушение работы платформ электронной коммерции

Перебои в работе влекут прямые финансовые потери и ущерб репутации.

Компрометация систем точек продаж (POS)

Кража платежных данных клиентов – это репутационный ущерб и штрафы за утечку персональных данных.

Примеры атак:

1

Злоумышленники захватывали секреты Kubernetes, используя ошибки в настройках системы логирования/аутентификации. Захваченные секреты были использованы для развёртывания вредоносного контейнера, а затем – для кражи данных кредитных карт на страницах оформления заказов.

Внедрение Kaspersky Container Security позволит проверять настройки Kubernetes на предмет наличия рисков ИБ, включая хранение секретов в открытом виде. Вдобавок, возможности проверки образов и контроля их запуска помогут предотвратить нелегитимные действия. Например, заблокировать запуск непроверенного или не соответствующего актуальным политикам образа.

2

Злоумышленники запускали скрипты для DDoS атак на портале электронной коммерции в пиковые часы продаж, используя уязвимые контейнерные микросервисы и незащищённый API.

Внедрение Kaspersky Container Security поможет настроить политики безопасности среды исполнения. Применение политик позволит замечать попытки запуска нелегитимных процессов и блокировать их исполнение.

Распространенные риски для контейнерной среды в ритейле	Митигация риска
Неправильно настроенная система оркестровки контейнеров (Kubernetes, Docker) Настройки по умолчанию, открытые панели инструментов и чрезмерные разрешения позволяют злоумышленникам захватывать кластеры.	Необходимо средство защиты, которое будет проактивно проводить проверки настройки системы оркестрации контейнеров, чтобы выявлять небезопасную конфигурацию системы.
Уязвимые образы контейнеров (устаревшие/из публичных репозиториев) Ритейлеры часто используют готовые образы с незакрытыми уязвимостями и торопятся с развёртыванием контейнеров, не уделяя должного внимания мерам защиты.	Необходимо сканировать образы на наличие уязвимостей.
Контейнеры с избыточными полномочиями (избыточные роли IAM) Приложения для розничной торговли часто предоставляют контейнерам широкий доступ к облаку, увеличивая поверхность атаки.	Средство для защиты контейнерной среды должно уметь проводить аудит, чтобы выявлять неправильные политики контроля допуска.

Проект из практики «Лаборатории Касперского»

Розничная сеть «Магнит»

МАГНИТ

Уникальная компания в российском ритейле с базой клиентов более 16 млн и 360 тыс. сотрудников. Наряду с продажей товаров розничная сеть занимается производством продуктов питания. Компания управляет 20 собственными предприятиями по выращиванию овощей, грибов, производству бакалеи и кондитерских изделий, которые выпускают продукцию под собственной торговой маркой «Магнит»

Сценарий применения:

- Импортозамещение иностранного решения для защиты контейнеров

Задача

С 2008 года в «Магните» используют продукты для защиты рабочих мест и серверов от «Лаборатории Касперского» Kaspersky Endpoint Security для бизнеса, в последующие годы к ним был добавлен Kaspersky Security для виртуальных и облачных сред. Уход иностранных вендоров из России подтолкнул «Магнит» к построению единой системы защиты на базе решений от одного вендора.

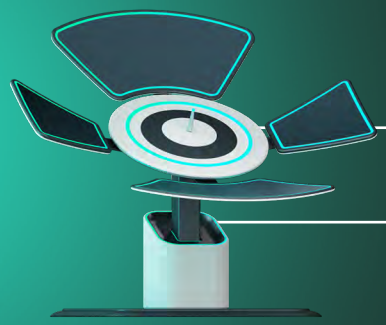
Выбор

Когда компания «Магнит» столкнулась с необходимостью изменения своего подхода к построению ИБ-системы, выбор был сделан в пользу расширения набора используемых продуктов и сервисов от «Лаборатории Касперского». Ключевым преимуществом для компании стало то, что экосистема продуктов «Лаборатории Касперского» представляет собой комплексный подход к защите бизнеса, где компоненты интегрированы друг с другом: обнаружение из одного решения становится доступным для всех остальных защитных решений. Гибкая настройка прав и разворачиваемых компонентов позволяет подстраивать продукты под инфраструктуру компании. Сокращается время обнаружения и реагирования за счет автоматизации и унификации действий. Также работу службы ИБ упрощают единая техническая поддержка высокого класса и клиентоориентированность, которую особенно отметили в «Магните».

Результат

«Магнит» стал одной из первых компаний в России, протестировавших и внедривших решение Kaspersky Container Security (KCS), представленное российскому рынку летом 2023 года. KCS динамично развивается, в том числе благодаря обратной связи от пользователей. В 2025 году уже обладает уникальной функциональностью по обеспечению безопасности разработки и эксплуатации контейнерных приложений с учетом специфики российских организаций. «Магнит» использует KCS для повышения эффективности и безопасности процессов разработки и эксплуатации контейнерных приложений, включая важные внутренние и внешние клиентские сервисы.

Подробнее



ТЕЛЕКОММУНИКАЦИИ

Облачные технологии и виртуализация сетевых функций (NFV) помогают телекоммуникационным компаниям оптимизировать инфраструктуру: повышают гибкость, масштабируемость и снижают затраты. Дополнительным преимуществом становится контейнеризация, которая радикально ускоряет внедрение новых сервисов.

Телекоммуникационные сети – критически важная инфраструктура, что делает их мишенью для атак, которые могут нарушить связь и скомпрометировать конфиденциальные данные.

IT-системы телекоммуникационных компаний, размещаемые в контейнерной среде

- Операционные (OSS) и бизнес-поддерживающие (BSS) системы, такие как биллинг, CRM, активация услуг
- Виртуальные сетевые функции, такие как маршрутизация, балансировка нагрузки, межсетевые экраны
- Edge Computing – контейнеры используются для обработки данных на границе сети

Последствия для телекоммуникационных компаний, связанные с недостаточной безопасностью контейнерной среды

Сбои в работе коммуникационных сетей

Перебои или ошибки в функционировании сервисов наносят ущерб репутации компании и приводят к потере клиентов.

Компрометация данных

Утечка записей звонков, геолокационных данных или персональной информации подрывает доверие клиентов и может повлечь штрафные санкции от регуляторов.

Кибершпионаж

Перехват сообщений или несанкционированный доступ к конфиденциальной информации наносят репутационный вред и создает юридические риски.

Примеры атак:

1

Злоумышленники использовали уязвимости функций ядра сети 5G (UPF, AMF) для перехвата и манипулирования трафиком абонентов. Таким образом, осуществлялось прослушивание звонков, перехват СМС или DDoS-атаки сервисов 5G.

Внедрение Kaspersky Container Security позволит выявлять уязвимости в пакетах на самых ранних этапах. Также, решение предоставляет детальную информацию об эксплуатируемости выявленных уязвимостей.

2

Злоумышленники воспользовались уязвимостью прокси-сервера (Envoy Proxy), чтобы встроить вредоносный контейнер в инфраструктуру. Контейнер затем использовался для проведения MITM-атаки.

Внедрение Kaspersky Container Security позволит использовать возможности визуализации всей инфраструктуры. Функционал контроля запуска не пропускает образы, не соответствующие политикам, а контроль сетевой активности позволяет ограничивать как внутренние, так и внешние сетевые взаимодействия.

Telco: пример атаки от исследователей «Лаборатории Касперского»

Работа 5G-сети азиатского поставщика телекоммуникационных услуг нарушена программой-вымогателем для Kubernetes (2024)

Что произошло?

5G-сеть крупной азиатской телекоммуникационной компании, которая использовала Kubernetes для оркестрации контейнерной инфраструктуры, подверглась атаке программы-вымогателя.

Вектор атаки:

Злоумышленники использовали уязвимость повышения привилегий в Kubernetes (CVE-2023-5528) для шифрования баз данных etcd.

В записке о выкупе требовалось $5 млн в биткоинах для расшифровки баз данных и восстановления нормальной работы сети.

Последствия:

Отключение 5G-сети на более чем 12 часов, затронувшее миллионы клиентов.

Утечка метаданных абонентов (хотя никакие финансовые данные не утекли).

Распространенные риски для контейнерной среды в телекоммуникационной сфере	Митигация риска
Уязвимые образы контейнеров (устаревшие/из публичных репозиториев) Если использовался образ, не проверенный на уязвимости, злоумышленники могут воспользоваться ими для компрометации контейнера. Известен случай, когда киберпреступники использовали уязвимость в контейнеризированной сетевой функции (CNF) для внедрения вредоносного ПО, скрытно майнящего криптовалюту.	Необходимо сканировать образы на наличие уязвимостей. Оптимальный вариант – решение для безопасности контейнеров интегрируется в CI/CD-конвейер нативно и автоматически сканирует образы контейнеров и инфраструктуру на уязвимости, вредоносное ПО, ошибочные конфигурации и наличие чувствительных данных.
Небезопасные конфигурации ключевых компонентов Например, если база etcd в Kubernetes (хранит токены сервисных аккаунтов, конфигурации сетевых политик) не защищена шифрованием или аутентификацией, то злоумышленники могут воспользоваться ею для изменения настроек Kubernetes и запустить вредоносное ПО.	Для защиты etcd необходимо включить шифрование трафика для etcd-клиентов и серверов, а также аутентификацию и авторизацию через сертификаты. Для обеспечения максимальной безопасности необходимо решение, которое будет проводить проактивный аудит и контроль соответствия требований для конфигураций Kubernetes, выявляя небезопасные настройки.
Обход механизмов контроля допуска (Admission Control) Кастомный контроллер может иметь ошибки или недостаточную валидацию входящих запросов. Злоумышленники могут воспользоваться уязвимостью в пользовательском Admission Controller для развёртывания контейнеров с опасными возможностями, включая доступ к сети хоста и привилегированный режим.	Решение, которое проверяет политики контроля допуска для блокировки развёртывания потенциально опасных привилегированных контейнеров.

Kaspersky Container Security

О решении Kaspersky Container Security

Для защиты контейнерных сред от описанных выше отраслевых рисков и повышения безопасности гибридных инфраструктур, а также для митигации рисков через цепочку поставок (со стороны поставщиков цифровых сервисов и услуг) команда «Лаборатории Касперского» рекомендует использовать специализированное решение Kaspersky Container Security.

Kaspersky Container Security обеспечивает безопасность контейнерных приложений на всех этапах жизненного цикла: от разработки до эксплуатации. Продукт позволяет защитить бизнес-процессы организации, соответствовать стандартам и нормам безопасности, а также помогает реализовать принцип безопасной разработки ПО (DevSecOps).

С помощью Kaspersky Container Security можно высвободить ресурсы ИБ-службы для решения других задач и сократить время вывода продуктов на рынок благодаря всеобъемлющей защите от актуальных киберугроз и автоматизации проверок на соответствие требованиям.

Kaspersky Container Security спроектирован с учетом особенностей контейнерных сред и обеспечивает защиту на разных уровнях: от образов контейнеров до ОС хоста. Kaspersky Continer Security является частью комплексного решения по защите облачных рабочих нагрузок Kaspersky Cloud Workload Security. Оно надежно защищает от кибератак и сокращает время обнаружения угроз и реагирования на них в облачных средах.

Подробнее

[1] Исследование CNEWS и «Лаборатории Касперского» «Курс на облачную безопасность в России – 2024», 2024 г.

[2] Исследование агентства CNews Analytics и компании «Инфосистемы Джет» «Проникновение технологий контейнеризации в ИТ-ландшафт крупных компаний 2020», 2020 г.

[3] Исследование Red Hat «The state of Kubernetes security report», 2024 г.

www.kaspersky.ru