



PT Container Security

Безопасность облачных приложений

Контейнеры и безопасность*



69%

организаций
используют Kubernetes

31%

разработчиков во всем мире
используют Kubernetes

25%

команд не сканируют
образы на наличие уязвимостей

74%

организаций применяют
в работе методы DevSecOps

94%

специалистов столкнулись
хотя бы с одним инцидентом безопасности,
связанным с контейнерами или Kubernetes

50%

специалистов по DevOps и ИБ
откладывали развертывание приложений
из-за проблем с безопасностью
контейнеров или Kubernetes

Как работают контейнеры



← Сборка — Доставка — Выполнение →

Развертывание в кластере
Kubernetes



Каждый этап можно атаковать



Если контролировать только один этап жизненного цикла, риск просто переедет на следующий

Контейнерная защита сложнее классической



1

Объектов слишком много

Образы, манифесты, контейнеры
и узлы множатся быстрее проверок

Атака растёт

2

Изменения идут постоянно

Версии и настройки попадают
в контур быстрее ручных проверок

Контроль запаздывает

3

Контейнеры живут недолго

Нагрузка исчезает раньше,
чем команда собирает следы

Следы теряются

4

Изоляция не абсолютна

Общее ядро повышает
цену ошибки

Сбой затрагивает хост

5

Риск приходит из поставки

Уязвимость в образе
или манифесте доезжает до кластера

Риск проходит этапы

6

Ответственность размыта

Команды видят разные
фрагменты одной картины

Риск не виден целиком

Контейнерную безопасность не закрыть смежными средствами защиты



Смежные средства и платформы
контейнеризации полезны,
но видят только часть картины:

код, сеть, узел или отдельное событие

Нужен контейнерный
контекст:

связать образ, настройки,
контейнер и событие

Какие угрозы возникают



Образы

Уязвимости, дефекты конфигурации, встроенное ВПО



Реестры

Незащищенные соединения с реестрами, устаревшие образы в реестре, компрометация (подмена) образа, нарушение доступа к чувствительным данным



Узел кластера Kubernetes

Большая плоскость атаки, уязвимости компонентов ОС, некорректные права доступа, взлом файловой системы ОС, ошибки конфигурации ОС, побег из контейнера на узел



Контейнер

Запуск вредоносного кода, извлечение чувствительных данных из контейнера, эксплуатация уязвимостей в запущенных контейнерах



Оркестратор

Неограниченный доступ администратора, несанкционированный доступ, нарушение сетевой изоляции контейнеров, нарушение размещения приложений



Полный базовый контур контейнерной безопасности в PT Container Security



Supply chain

- Сканирование образов и интеграция с реестрами
- Проверка подписи
- SBOM и экспорт отчетов
- CI/CD и плановые проверки



Deployment control

- Проверки Dockerfile и Kubernetes-манифестов
- Admission controller
- Policy-based-блокировки
- Анализ на соответствие стандартам безопасности



Runtime

- eBPF- и WASM-обнаружение инцидентов
- Реакция и инструменты расследования
- Готовые сценарии угроз



Platform

- Поддержка мультикластерности и карты кластера
- RBAC, LDAP, API и нотификации
- Метрики, аудит, поддержка закрытого контура

Что уже умеет PT Container Security



Безопасность образов

уязвимости, ВПО, подпись, регулярные проверки

Контроль допуска

блокировка небезопасных действий до запуска

Среда выполнения

eBPF, детекторы, правила реагирования

Карта кластера

поды, неймспейсы, ноды и события

Конфигурации

пайплайн и кластер: мiskonфигурации, риски, стандарты

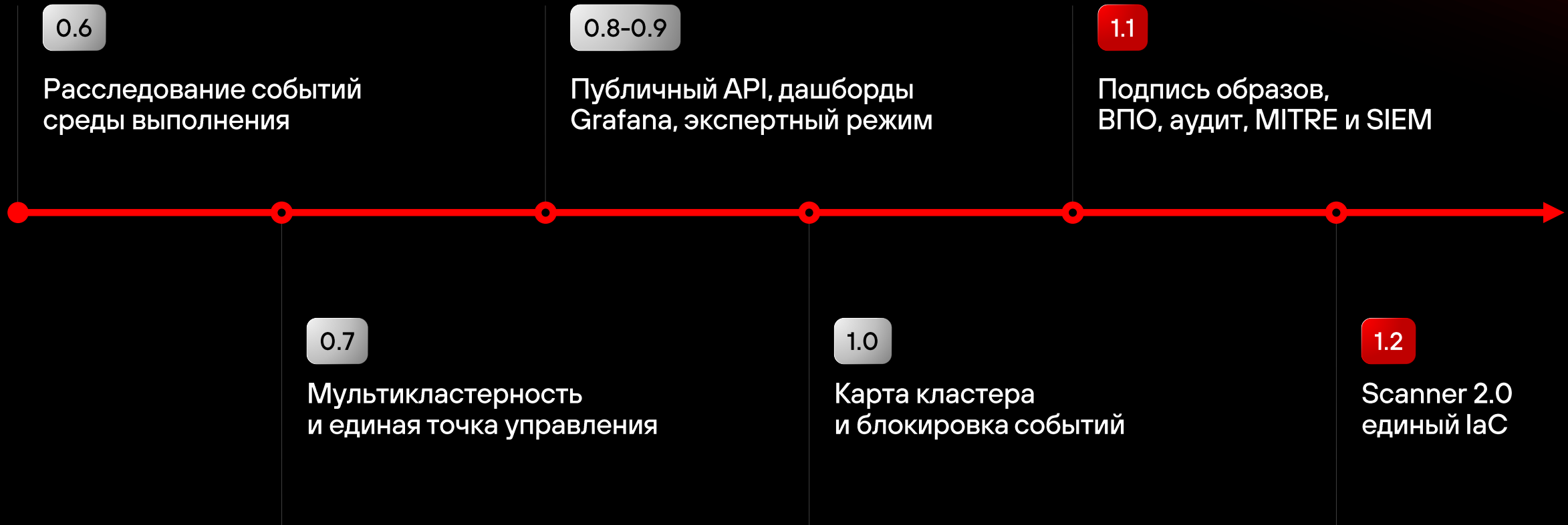
Интеграции

командная строка, API, вебхук, syslog, SIEM

Эксплуатация

LDAP, роли, токены, аудит, Grafana, Loki

Таймлайн развития продукта



Почему PT Container Security



Детекторы под нагрузку

Расширение рантайма
под полезные процессы



Open-source Runtime Radar

Старт без долгой бюрократии



Экосистема Positive Technologies

MaxPatrol SIEM
и смежные продукты



Гибкость настройки

Настройка глубины
наблюдения



Экспертиза команды

Помощь при внедрении
и эксплуатации



Сертификация

Начало 2027 года

Вектор развития: Q3–Q4 2026



Q3 2026

добавляем видимость
и помощников

Инвентаризация кластера

табличный вид карты: поды, события,
уязвимости и ошибки конфигурации

Docker как отдельная платформа

мониторинг контейнеров и контроль
операций с ними

LLM-помощник

быстрее разбирать инциденты,
уязвимости и проводить расследования

Детекторы в допуске

кастомные срабатывания до применения манифеста

Q4 2026

упрощаем управление
и снижаем шум

Поиск секретов в образах

находим чувствительные
данные до запуска

Единые политики и история

одни правила и единая картина
на несколько кластеров

Автотюнинг мониторинга

меньше ручной настройки и ниже
потребление ресурсов

Вектор развития: H1–H2 2027



H1 2027

Анализ сети и управление сетевыми политиками

Сертификация ФСТЭК

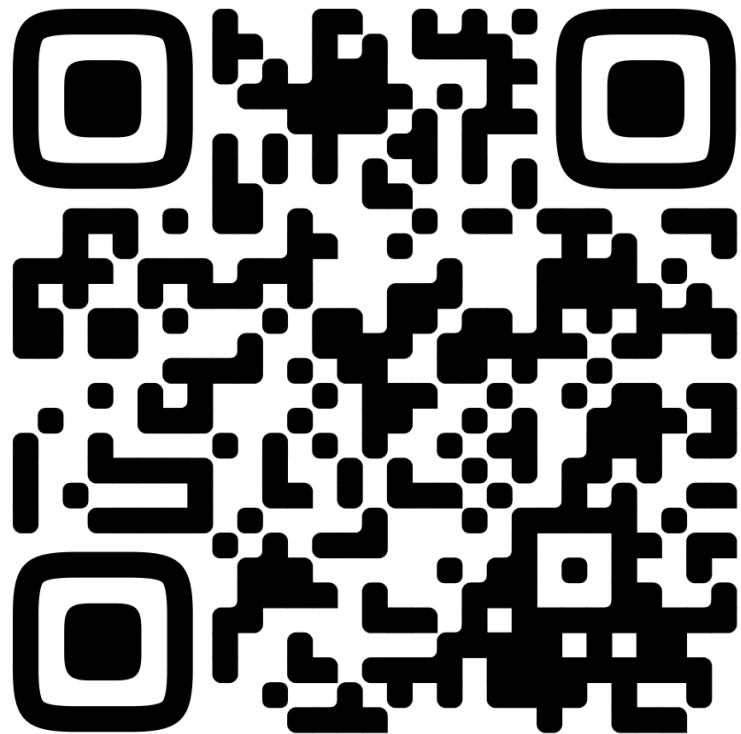
Подана заявка на сертификацию продукта

H2 2027

Защита узлов от файловых угроз

На текущий момент закрывается отдельным продуктом
Positive Technologies — MaxPatrol EDR

PT Container Security



@runtimeradar

Мы разработали
первое **открытое
решение**
для мониторинга
безопасности
и реагирования
на инциденты
в контейнери-
зированных средах

Open source



@pt_containersecurity



Спасибо!