Новинки Palo Alto Networks.
PAN-OS 10 и новые сервисы.

Igor Bondarev
Product Manager Palo Alto Networks

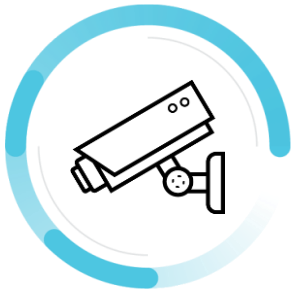
PAN-OS 10.0
Самое важное на одном слайде

Моментальная защита от угроз на основе ML

До 95% неизвестных файловых и веб-атак предотвращаются моментально

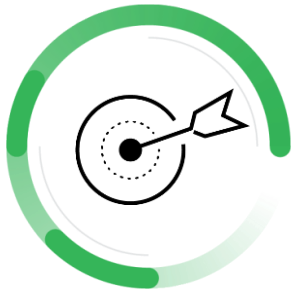
Непрерывный стриминг сигнатур

Доставка сигнатуре менее чем за 10 секунд, что снижает 99.5% число зараженных систем



Комплексная встроенная защита IoT

Выявлено в три раза больше IoT устройств (итоги бета-теста у заказчика)



Автоматические рекомендации политик

Ошибки в конфигурации – причина 99% взломов (Gartner)

IoT Security

Доверяйте каждому устройству в вашей сети

paloalto NETWORKS

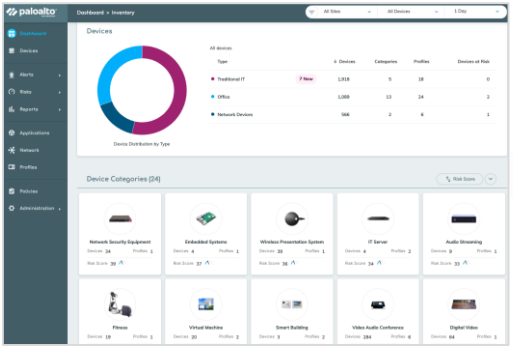
Почему это важно?
Масштабное увеличение количества устройств

Рынок устройств IoT к 2026 году

Подключенных устройств к 2025 году

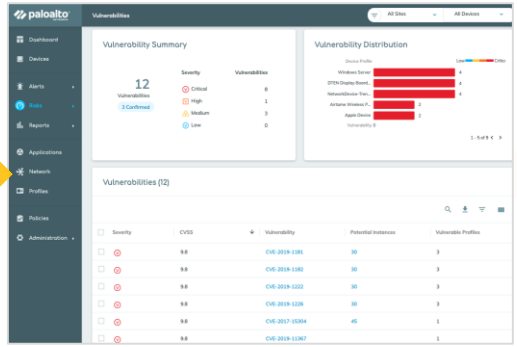
Организаций считают это риском

Новый сервис: IoT Security



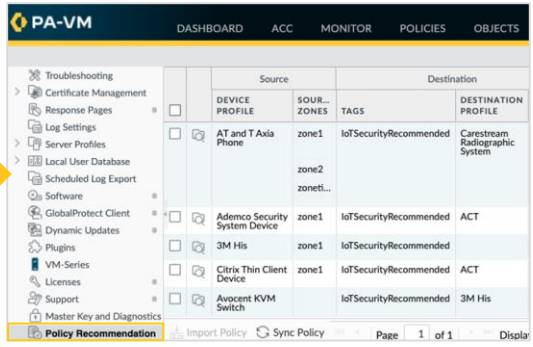
Понимание обстановки

Точная идентификация и классификация любых устройств с ML, в том числе тех, которые встречаются впервые



Глубокий анализ рисков

Быстрое принятие решений на основе понимания аномалий, уязвимостей и критичности



Встроенные действия

Безопасная автоматизация политик защиты на NGFW с новым квалификатором политики Device-ID

Моментальное предотвращение угроз с ML

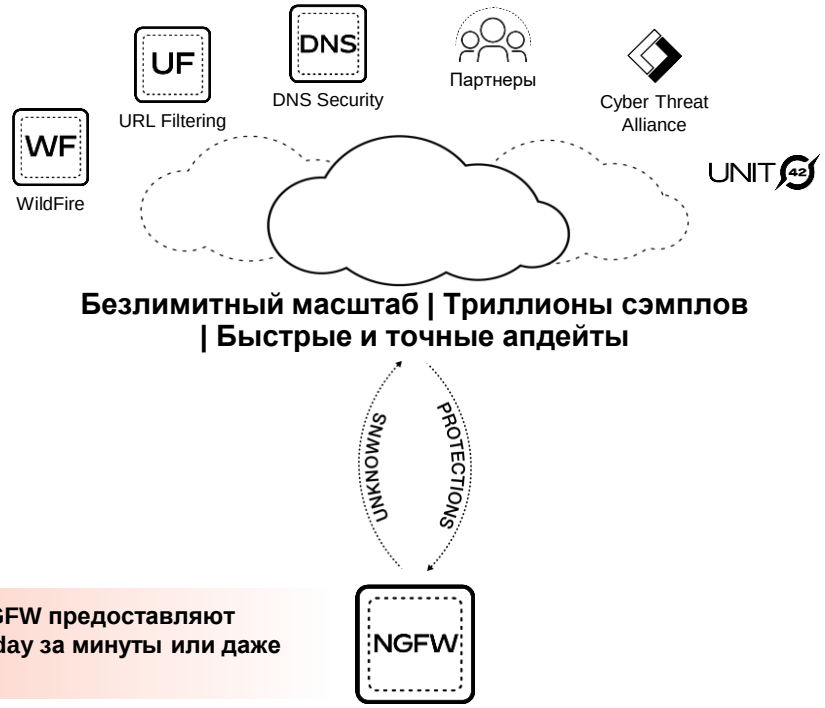
Каждая секунда имеет значение

paloalto NETWORKS

У злоумышленников 2 критических преимущества…

Скорость распространения и полиморфизм

Предотвращение атак сегодня полагается на облако



Подписки NGFW предоставляют защиту от 0-day за минуты или даже быстрее

Облачные сигнатуры **ускоряют предотвращение** атак

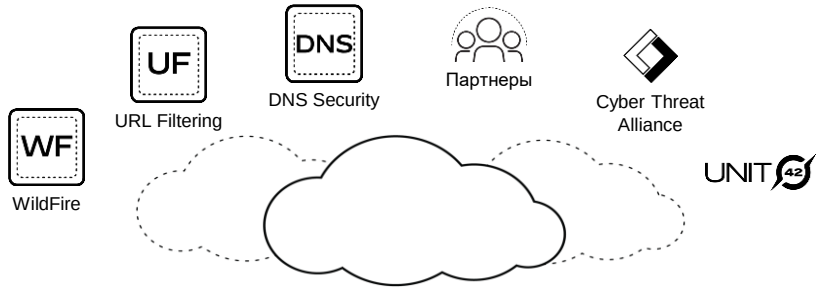
Общий пул сигнатур помогает **быстро распространять** защиту

Файлы: **5 минут**

URL: **1 минута**

DNS: **моментально**

Новое поколение защиты: безсигнатурые вердикты для 0-day моментально на NGFW



До 95% **Предотвращение типичных файловых и веб-угроз**

NGFW
- **Моментальный WildFire**
- **Моментальный URL Filter**

Облачные сигнатуры **ускоряют предотвращение** атак

Общий пул сигнатур помогает **быстро распространять** защиту

- Файлы: **моментально**
- URL: **моментально**
- DNS: **моментально**

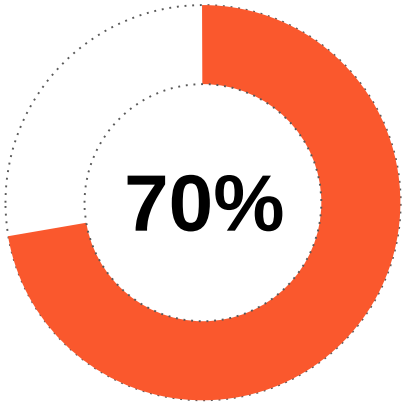
Расшифрование TLS

Критичность анализа шифрованного трафика

Серьезные риски с шифрованным трафиком

Шифрование уже норма

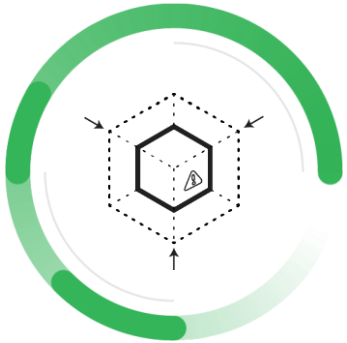
И хакеры пользуются этим



Более 70% вредоносных кампаний в 2020 году будут использовать шифрование для скрытия вредоносной активности (Gartner)

Источник: Encrypted Traffic (2016) | Encrypted Traffic (2020) | Encrypted Walwave (Gartner)

Расшифрование теперь стало проще



Устранение рисков безопасности

Контроль использования старых протоколов TLS, небезопасных шифров и ошибочных конфигураций

Простое внедрение политик расшифрования

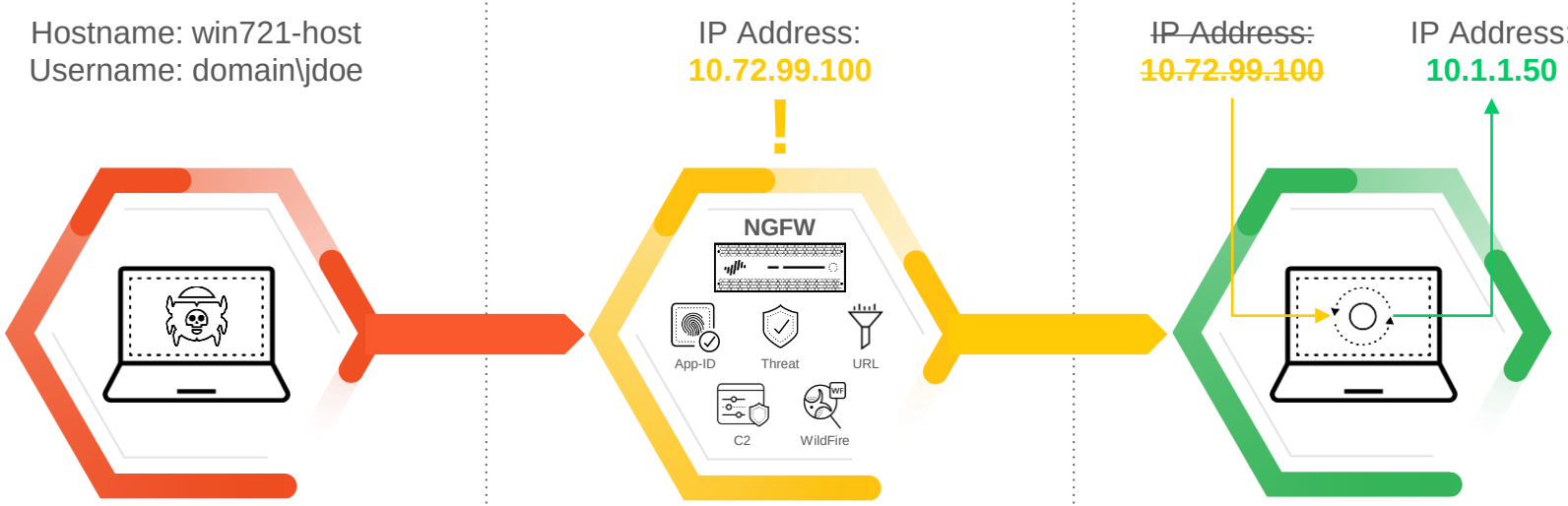
Простая настройка и управление расшифровкой с помощью встроенных средств и мониторинга

Быстрая защита облачных приложений

Защита трафика TLS 1.3 и HTTP/2. Новое криптоускорение дает 2x производительности

Кратко о других новинках

GlobalProtect позволяет держать устройства в карантине, даже если у них поменялся IP



ПК пользователя взломан

NGFW видит вредоносную активность и ограничивает доступы для этой машины

Клиент GlobalProtect автоматически поддерживает карантин даже при смене IP

Подписка DNS Security дополнена категориями DNS-угроз

Категории

DNS-туннели	DGA
C2	Вредоносы
Динамический DNS	Новые домены

Command & Control

Уровень: Критический

Синкхолинг

Политика

- Синкхолинг C2 доменов со значением “critical”
- Запуск автоматического процесса карантина

Вредонос

Уровень: Средний

Политика

- Блокировать вредоносные домены с “medium”
- Не требует дополнительных действий

Аналитика по DNS-трафику

Мониторинг DNS

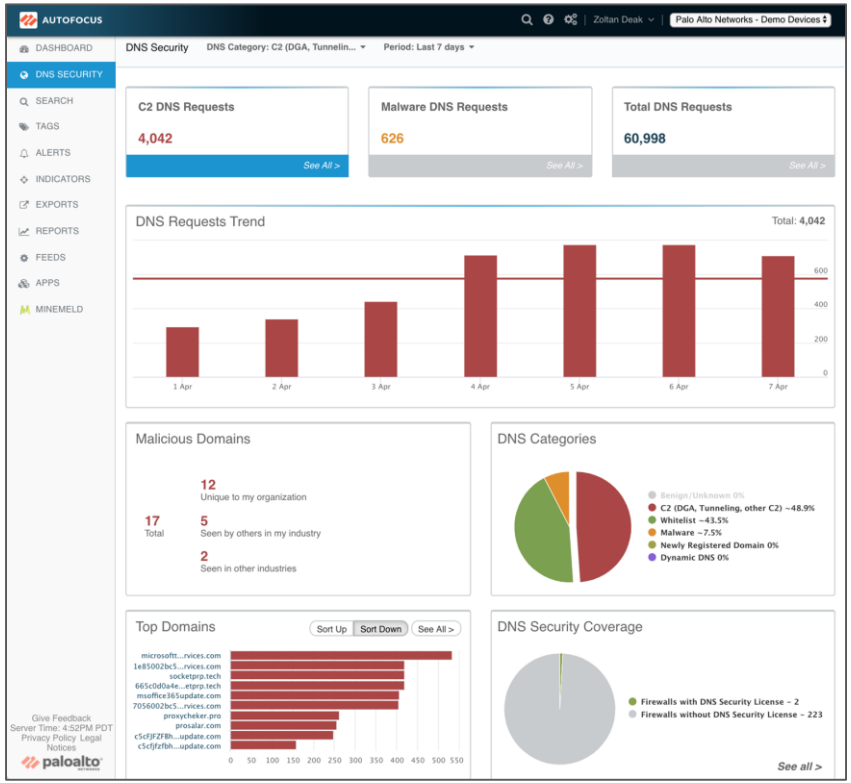
- Полное понимание всего DNS-трафика и угроз
- Фильтры по категориям DNS и датам
- Угрозы в DNS (вредоносы, C2, туннели, DGA)

Контекст по данным DNS

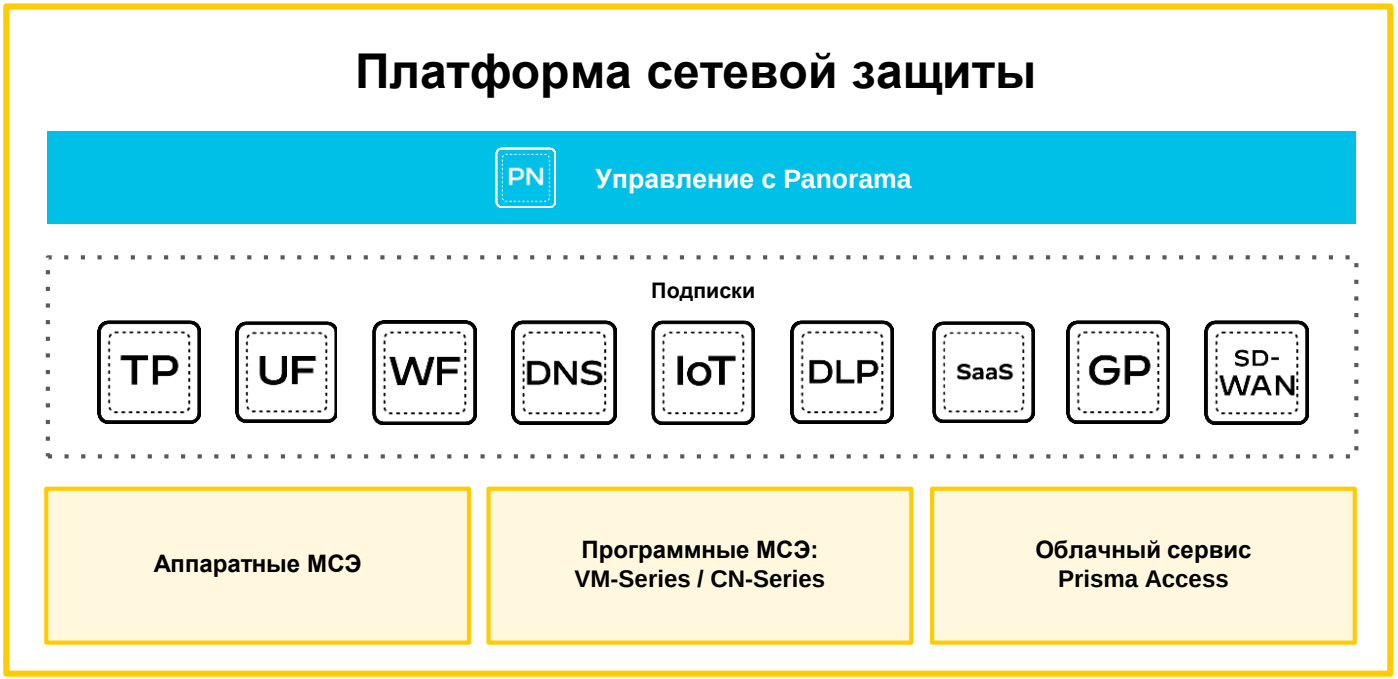
- Причина блокировки домена
- Доступ к связанной киберразведке
- Тэги AutoFocus
- Данные Whois и passive DNS

Гигиена DNS

- Информация о МСЭ, на которых активирована подписка DNS Security



Единая платформа сетевой защиты Palo Alto Networks



Более 70 новых возможностей в PAN-OS 10.0

Безопасность IoT
- Выявление и мониторинг IoT-устройств
- Выявление поведенческих аномалий
- Рекомендации по политикам на основе риска
- Встроенные контроли

Предотвращение первой жертвы
- Встроенное машинное обучение на сетевом уровне
- Предотвращение ВПО, фишинга УЗ и скриптов с WildFire и URL Filtering
- Патентнованный безсигнатурный подход

CN-Series
- NGFW в контейнере
- Нативное внедрение в Kubernetes
- Централизованное управление с Panorama

Расшифрование
- Поддержка TLS 1.3
- Улучшенный мониоринг
- Улучшенный траблшутинг

Сетевые функции
- Кластеры HA
- Дополнительные группы мониторинга пути в HA
- Защита Ethernet SGT

GlobalProtect
- Выявление и карантин зараженных устройств

SD-WAN
- Мониторинг пути для SaaS-приложений
- Прямая коррекция ошибок
- Дубликация пакетов

WildFire
- Мультивекторный рекурсивный анализ для предотвращения многостадийных многохостовых атак
- Улучшения моделей статического анализа дает вердикты из 90% вредоносных сэмплов

Поддержка Snort
- Поддержка сигнатур SNORT и Suricata в веб-интерфейсе и API
- Автоматическая конвертация, очистка, загрузка и управление сигнатурами IDPS

Карты DPC для шасси
- Новая карточка для PA-7000: пропускная способность на 33% выше

Политики безопасности
- Поддержка заголовка X-Forwarded-For HTTP в политиках

Защита 5G
- Защита 5G network slice
- Защита 5G и 4G equipment ID
- Защита 5G и 4G subscriber ID

Новая линейка оборудования PA 400
- PA-410
- PA-440
- Pa-450
- PA-460

Как узнать больше?

Как попробовать?

Пишите:

igor.Bondarev@muk.kz

Спасибо!

Пишите: igor.Bondarev@muk.kz

+7 (705) 229 00 29