Инновациии в безопасности XDR, HIP, SD-WAN, контейнеры и мгновенное обнаружение на основе Machine Learning

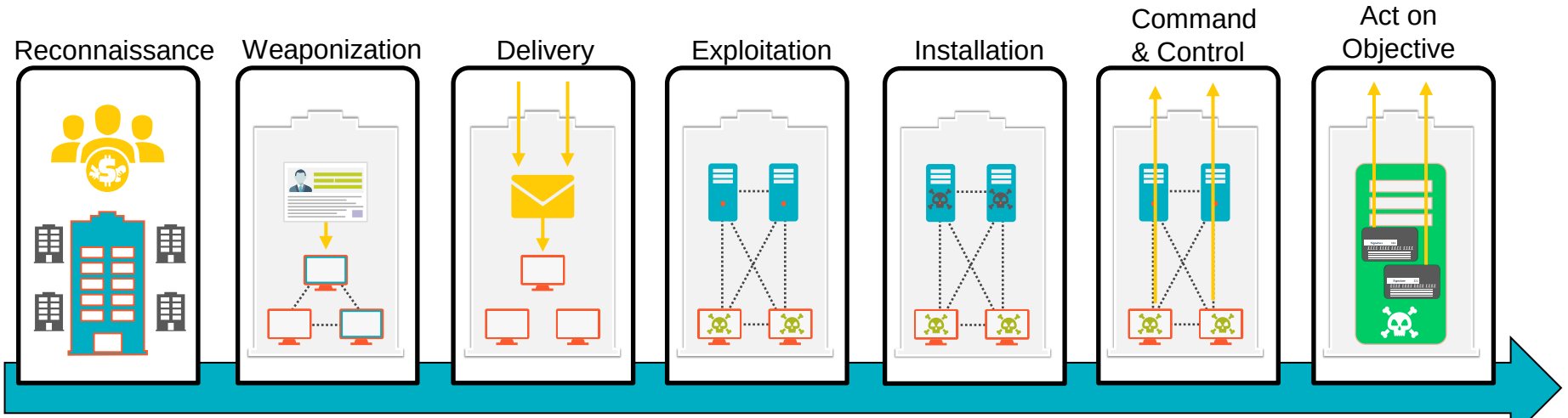
4 декабря 2020
profitday.kz/security

Денис Батранков, CISSP, PCNSE, GCIH
советник по информационной безопасности
denis@paloaltonetworks.com
russia@paloaltonetworks.com

Palo Alto Networks Россия и СНГ

канал на Youtube
tiny.cc/paloaltorussia

Как нас атакуют сегодня
Cyber-attack Lifecycle и Kill Chain



- Packet Sniffer
- Port Scan
- Shoulder Surf
- Wi-Fi Scan
- Social Networking

- .doc
- .exe
- .js
- .pdf
- .xls

- Email
- IM
- USB
- whatsapp
- www

- Нажми **СЮДА**
- Открой вложение

- Escalate Priv
- Root Kits
- Shell Access

- Dynamic DNS
- IRC
- Port Evasion
- Proxies
- SSL

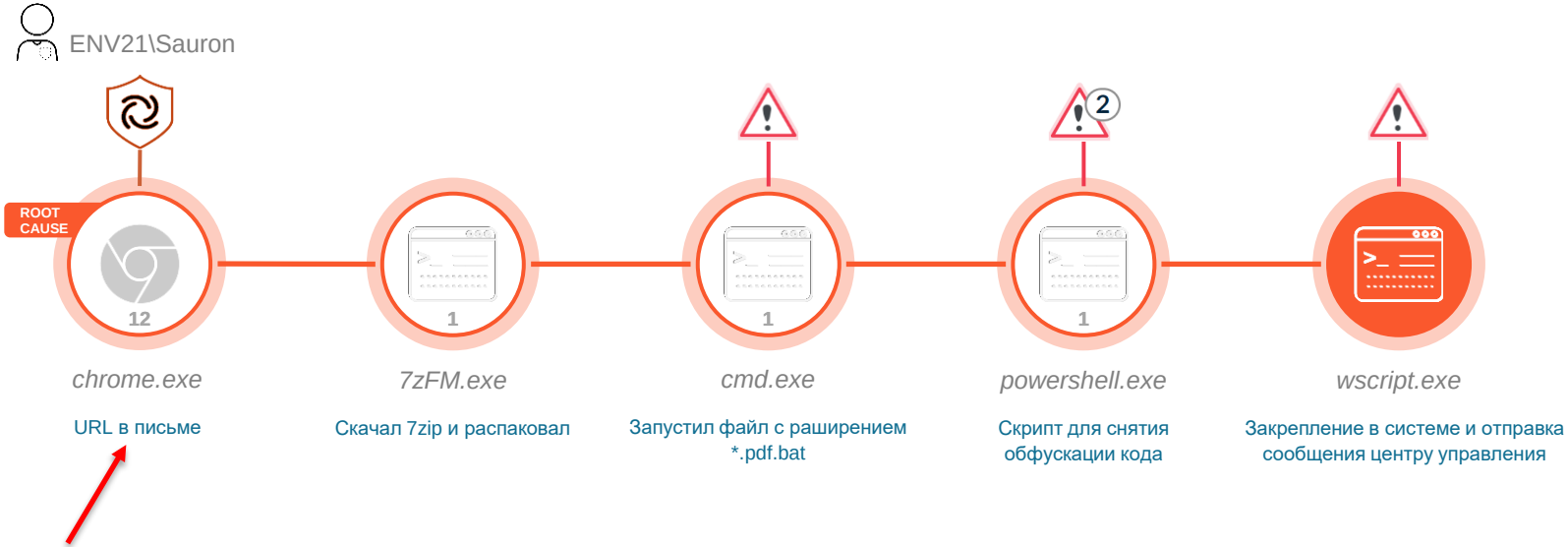
- Attack Other Target
- Data Theft
- DoS
- System Control

paloalto NETWORKS

Хакеры не атакуют вредоносным кодом

И как их остановить?

На экране цепочка событий связанных с заблокированной атакой



Причинно-следственная цепочка идет слева направо по времени
Все инициировал процесс chrome.exe на рабочей станции

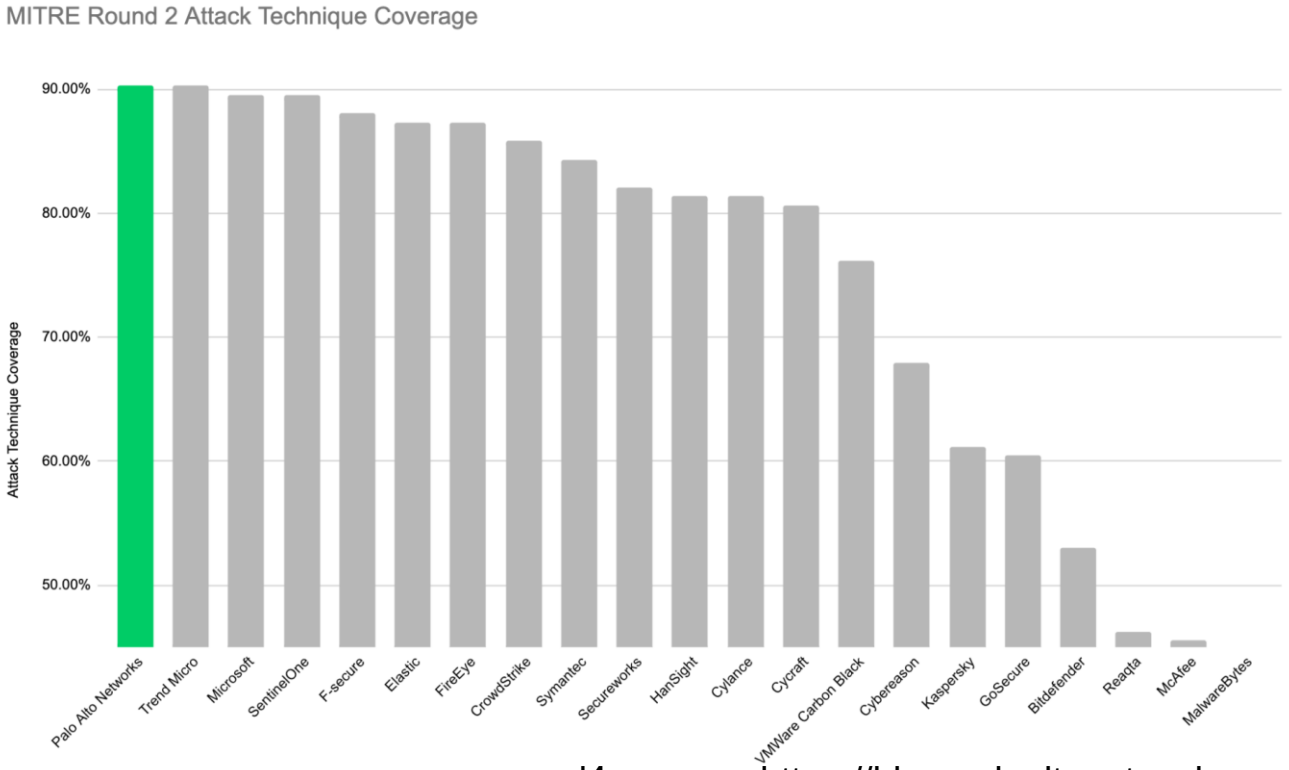
Сегодня мы защищаем хост + сеть + облака
eXtended Detection and Response (EDR стал XDR)

- **EDR/XDR – это защита от угроз, которые несут легитимные продукты и утилиты**
- EDR/XDR – это концентрация знаний и опыта людей (которые 20 лет расследуют инциденты) в виде поведенческих правил BIOC (IoA)
- EDR/XDR - это приобщение ваших аналитиков к очень дорогой глобальной экспертизе
- EDR/XDR – это возможность расследовать пройденный путь от заражения до блокировки мгновенно
- EDR/XDR- это графическое отображение вектора (графа) атаки
- EDR/XDR – это про имеющиеся блокировки и создание новых правил блокировки
- EDR/XDR – это про совместимость с другими продуктами и про нагрузку на станцию
- EDR/XDR – это про защиту мобильных устройств, Linux, Windows, VDI, Citrix, VmWare
- XDR – это про сбор подробных событий и блокировки на хостах, сети и в облаке
- XDR – это путь к сервису Managed Detection and Response (MDR)

Cortex XDR:
youtu.be/-PFWz3ceh4w

Как выбирать – EDR/XDR?

- Смотреть сколько техник атак по MITRE ATT&CK продукт видит и блокирует



Источник: https://blog.paloaltonetworks.com/2020/04/cortex-mitre/

paloalto NETWORKS

Сотрудники теперь «облачные»

И как их защитить?

Что требуется для безопасности удаленного рабочего места

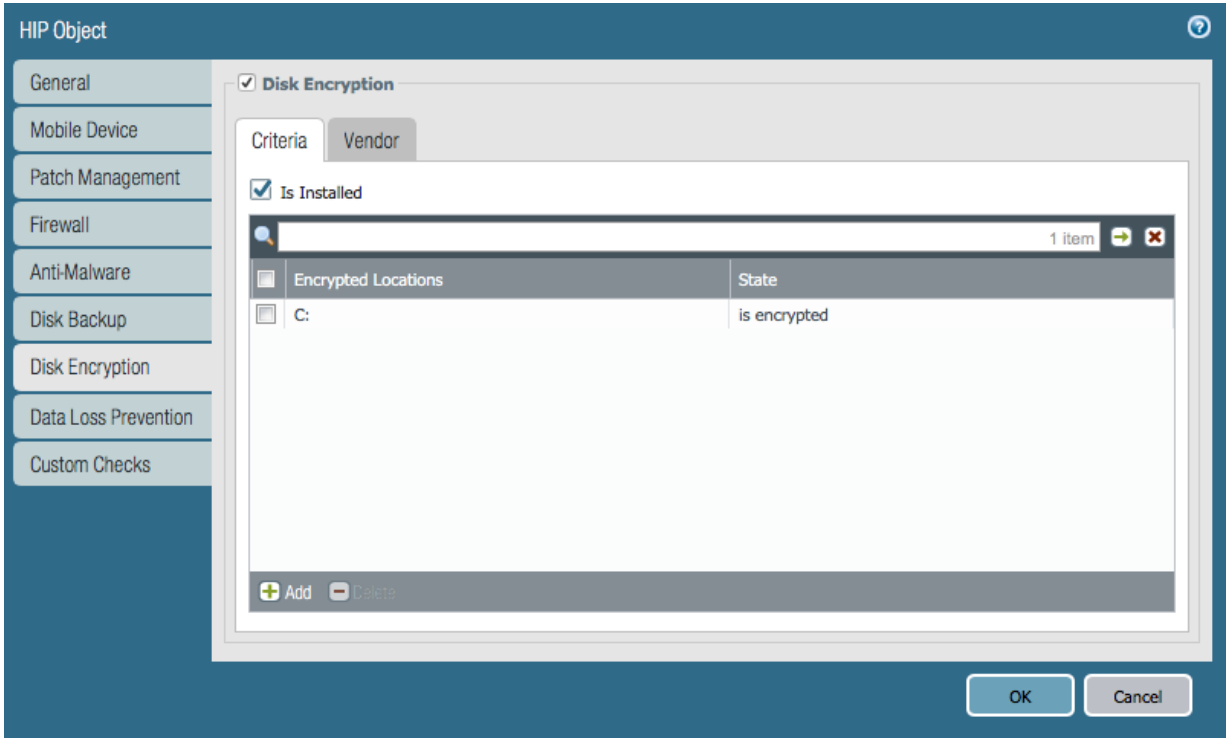
- Обновить операционную систему, приложения и плагины к ним
- Запустить активную хостовую защиту, например, Cortex XDR
- Зашифровать диски для защиты от хищения, например, встроенными средствами ОС
- Подключаться к компании по IPSEC или SSL VPN каналу, например, GlobalProtect
- Авторизоваться используя два фактора, например пароль и OKTA
- Использовать персональный firewall, например, встроенный в Windows
- Делать бекапы
- Проверять, что сотрудник ничего не выключил

Пригласите лучше меня на встречу и мы обсудим: denis@paloaltonetworks.com

Как выбирать VPN на примере GlobalProtect

- VPN должен терминироваться на вашем текущем аппаратном или виртуальном NGFW
- Установление защищенного туннеля IPSEC или SSL VPN и обеспечение конфиденциальности передаваемых данных и доступа к внутренним приложениям компании
- Авторизация пользователя в домене компании по паролю и второму фактору (сертификат по SCEP, смс, звонок, OKTA, DUO, UbiKey, RSA и т.д.) и обеспечение минимизации риска кражи пароля
- Защита от ввода паролей и логинов домена на фишинговых сайтах
- **Активная проверка, что на хосте установлены последние патчи, запущен и обновлен антивирус, стоит персональный firewall и зашифрованы диски и отправка рекомендаций что нужно делать, чтобы исправить ошибки (HIP Notification)**
- Интеграция с NGFW: антивирус, IPS, URL фильтрация, Threat Intelligence, защита DNS и других приложений, контроля страны подключения по VPN, Machine Learning
- Разграничение доступа пользователей к только нужным им приложениям: бухгалтеру к 1С, администраторам к SSH, программистам к docker и Kubernetes, контроль доступа к файлообменниками и веб-почте и другим ресурсам SaaS

Host Information Profile - информация о настройках на хосте (смартфоне, ноутбуке, виртуальной машине в VDI)



Как защитить домашний компьютер сотрудника, используя GlobalProtect
https://safebdv.blogspot.com/2020/03/globalportal-vpn.html

70+ новых возможностей в NGFW версии 10.0

Они есть только у клиентов
Palo Alto Networks

70+ новых возможностей в NGFW версии 10.0
Инновации в атаках порождают инновации в защите

Безопасность IoT
- Визуализация картины по IoT-устройствам
- Обнаружение аномалий в поведении
- Рекомендации по политикам на основе анализа риска
- Единая точка реализации политик

Защита «нулевого пациента»
- Машинное обучение для защиты реального времени
- WildFire и URL-фильтрация блокируют вредоносные файлы, кражу учетных данных, нехорошие скрипты
- Запатентованная бессигнатурная технология

CN-серия
- NGFW в форм-факторе контейнера
- Развертывание в среде Kubernetes
- Централизованное управление из Panorama

Анализ зашифрованного трафика
- Поддержка TLS 1.3
- Улучшенный сбор данных
- Улучшенная диагностика

Сеть
- Улучшения для кластеров HA
- Дополнительные path monitoring groups
- Защита Ethernet SGT

GlobalProtect
- Идентификация и карантин скомпрометированных узлов

SD-WAN
- Мониторинг доступности SaaS-приложений
- Forward error correction
- Дублирование пакетов

WildFire
- Мульти-векторный рекурсивный анализ для блокировки много-шаговых атак
- Улучшения модели статического анализа для вынесения молниеносного вердикта относительно более 90% образцов вредоносных PE-файлов

Улучшения поддержки Snort
- Поддержка сигнатур SNORT и Suricata в UI и API
- Автоматическая конвертация, верификация, загрузка и управление сигнатурами

Железо: Data Processing Card
- Новые карты для PA-7000-серии: новые data processing card мощнее на 33%

Функции политик безопасности
- Поддержка заголовков X-Forwarded-For HTTP в политиках

Безопасность 5G
- Безопасность 5G network slice
- 5G и 4G equipment ID security
- 5G и 4G subscriber ID security

https://youtu.be/YnF1Z4UAI4U

70+ новых возможностей в NGFW версии 10.0

Безопасность IoT
- Визуализация картины по IoT-устройствам
- Обнаружение аномалий в поведении
- Рекомендации по политикам на основе анализа риска
- Единая точка реализации политик

Защита «нулевого пациента»
- Машинное обучение для защиты реального времени
- WildFire и URL-фильтрация блокируют вредоносные файлы, кражу учетных данных, нехорошие скрипты
- Запатентованная бессигнатурная технология

CN-серия
- NGFW в форм-факторе контейнера
- Развертывание в среде Kubernetes
- Централизованное управление из Panorama

Анализ зашифрованного трафика
- Поддержка TLS 1.3
- Улучшенный сбор данных
- Улучшенная диагностика

Сеть
- Улучшения для кластеров HA
- Дополнительные path monitoring groups
- Защита Ethernet SGT

GlobalProtect
- Идентификация и карантин скомпрометированных узлов

SD-WAN
- Мониторинг доступности SaaS-приложений
- Forward error correction
- Дублирование пакетов

WildFire
- Мульти-векторный рекурсивный анализ для блокировки много-шаговых атак
- Улучшения модели статического анализа для вынесения молниеносного вердикта относительно более 90% образцов вредоносных PE-файлов

Улучшения поддержки Snort
- Поддержка сигнатур SNORT и Suricata в UI и API
- Автоматическая конвертация, верификация, загрузка и управление сигнатурами

Железо: Data Processing Card
- Новые карты для PA-7000-серии: новые data processing card мощнее на 33%

Функции политик безопасности
- Поддержка заголовков X-Forwarded-For HTTP в политиках

Безопасность 5G
- Безопасность 5G network slice
- 5G и 4G equipment ID security
- 5G и 4G subscriber ID security

https://youtu.be/YnF1Z4UAI4U

Inline Prevention на основе ML

Каждая секунда имеет значение

Представляем первый в индустрии NGFW с машинным обучением

paloalto NETWORKS

Существующим решениям трудно быстро блокировать атаки 0-дня

Обособленные решения

Не поспевает за масштабами и множеством вариаций современных атак

Требуется компромисс

Нужна нулевая жертва для последующего детектирования

Остановка бизнеса

Существующий подход Задержать-Проверить-Отпустить влияют на пользователей и бизнес-процессы

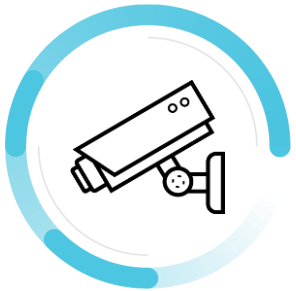
Множество беспрецедентных инноваций в одной платформе

Мгновенная защита от угроз используя машинное обучение

До 95% НЕИЗВЕСТНЫХ файловых и веб-угроз предотвращаются в режиме реального времени, inline

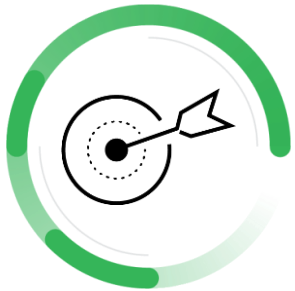
Защита практически реального времени с сигнатурами

Новые сигнатуры менее, чем через 10 секунд обеспечивают снижение затрагиваемых угрозой систем на 99.5%



Полная, интегрированная защита IoT

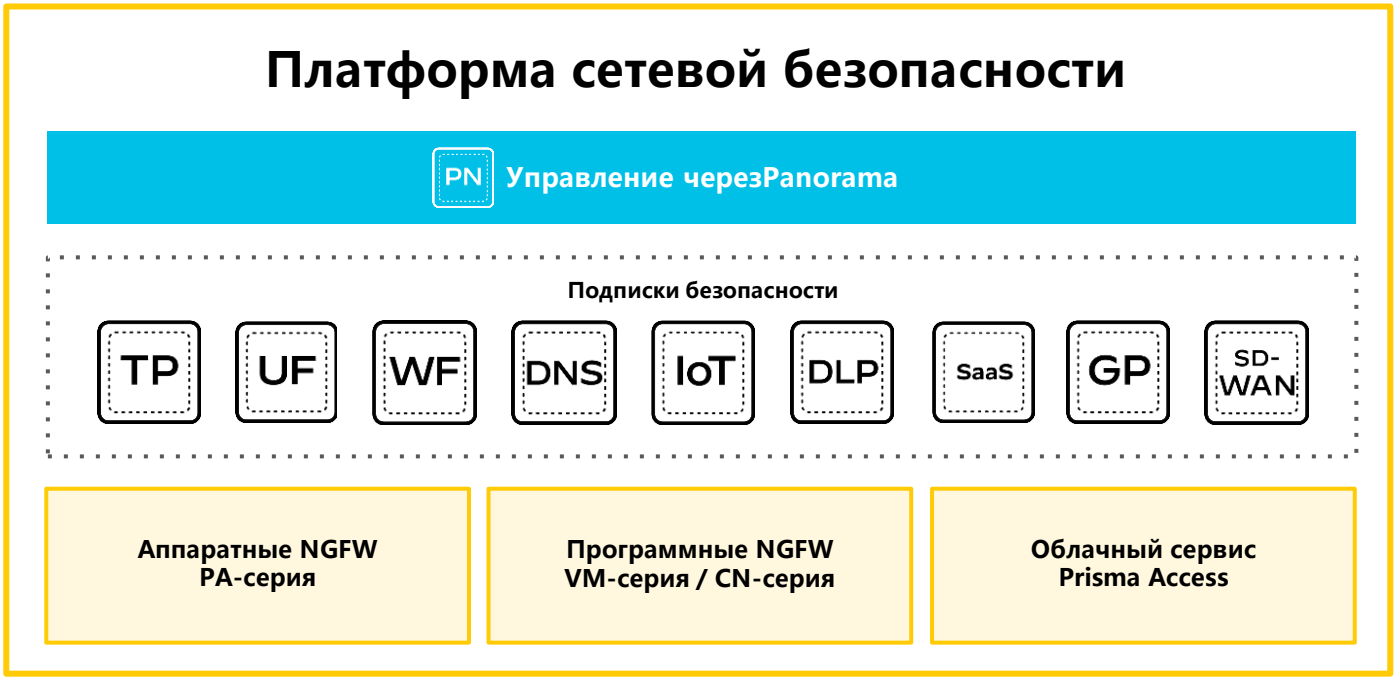
Детектирование в 3 раза больше IoT-устройств, чем конкуренты



Автоматические рекомендации по политикам

99% брешей вызваны неправильной конфигурацией (Gartner Inc.)

Поставляется как часть Единой платформы



Блокируем угрозы 0-дня сегодня

Бесконечное масштабирование | Анализ триллионов образцов | Моментальные обновления

Защита от неизвестных угроз в течение минут и быстрее с подписками на сервисы безопасности, лидирующими в индустрии

Масштабирование возможностей защиты на базе облачного сервиса безопасности

Защита становится доступной **сразу всем** пользователям сервиса

- Анализ файлов: **5 минут**
- Фильтрация URL: **1 минута**
- Защита DNS: **Мгновенно**

Блокируем угрозы 0-дня сегодня

Бесконечное масштабирование | Анализ триллионов образцов | Моментальные обновления

До 95% **угроз в распространенных типах файлов и веб блокируются in-line**

NGFW

WildFire Inline ML

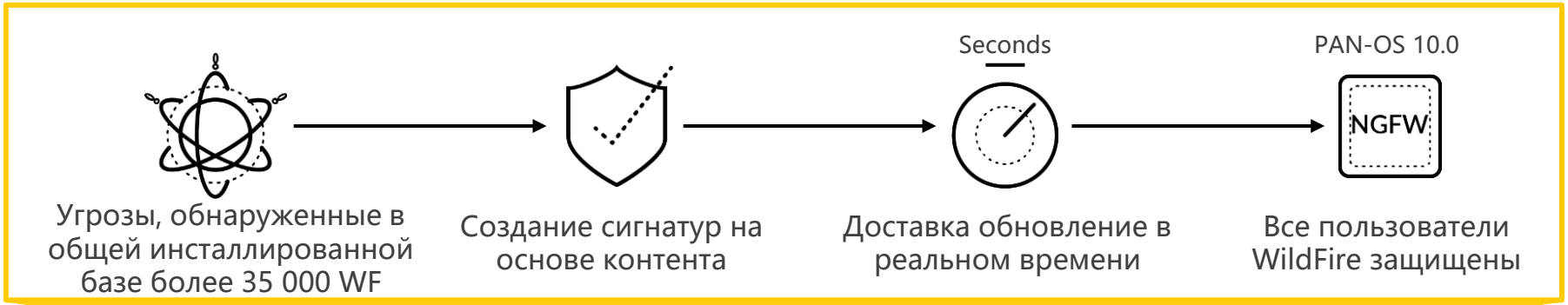
URL-фильтрация Inline ML

Масштабирование возможностей защиты на базе облачного сервиса безопасности

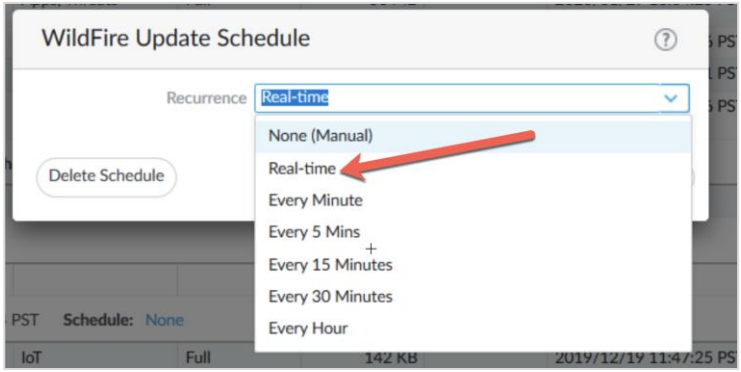
Защита становится доступной **сразу всем** пользователям сервиса

- Анализ файлов: **Мгновенно**
- Фильтрация URL: **Мгновенно**
- Защита DNS: **Мгновенно**

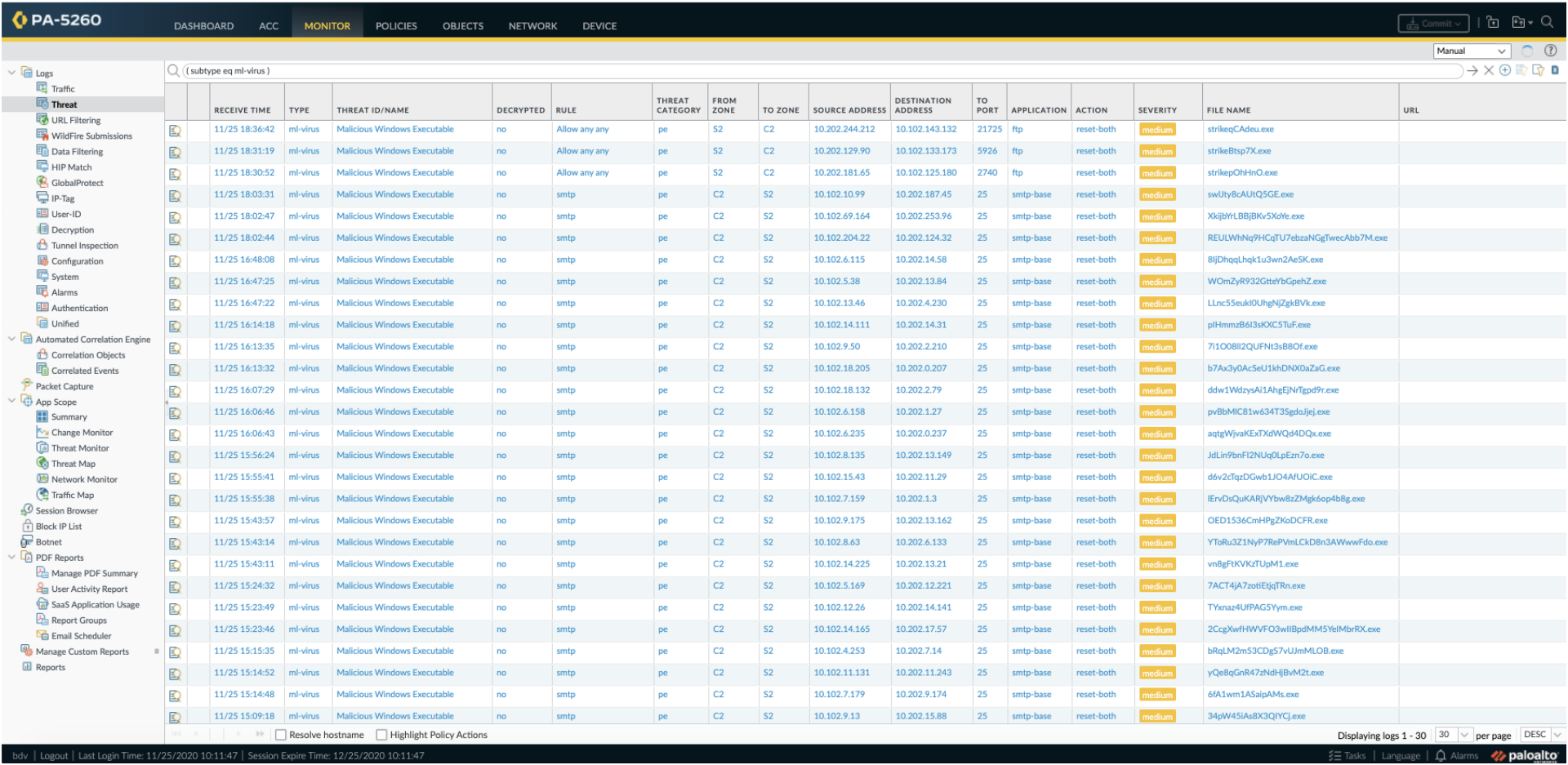
Доставка обновлений защиты беспрецедентно быстро



РАНЬШЕ
Лидирующее в индустрии время создания и доставки сигнатур за **5 минут**

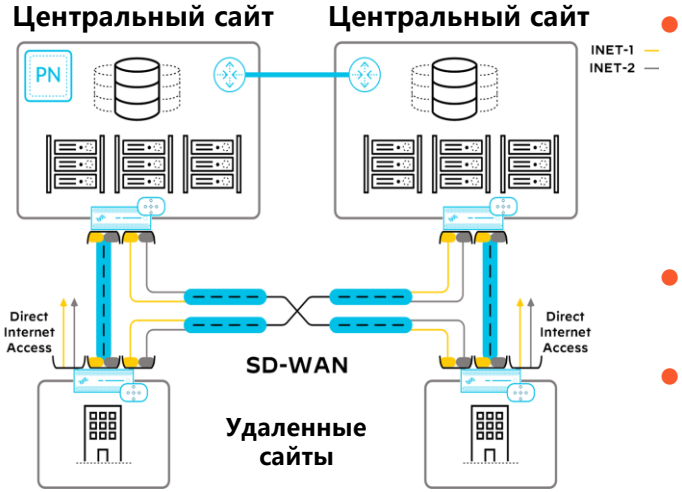


Начиная с версии 10.0
Обновления безопасности передаются на NGFW в потоковом режиме в течение **единиц секунд**

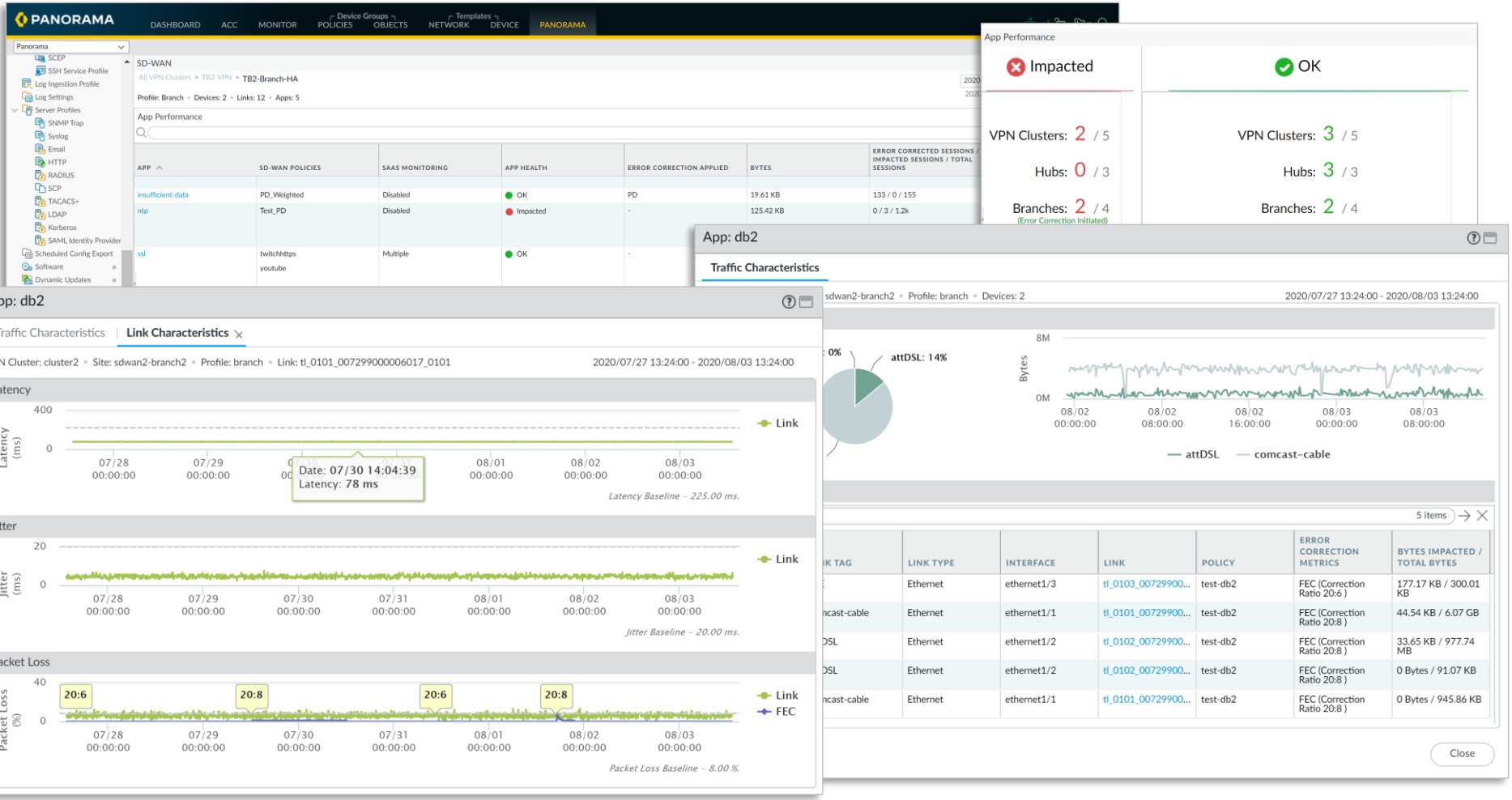


Secure SD-WAN, CloudGenix

Способы настройки устройств филиалов (CPE)



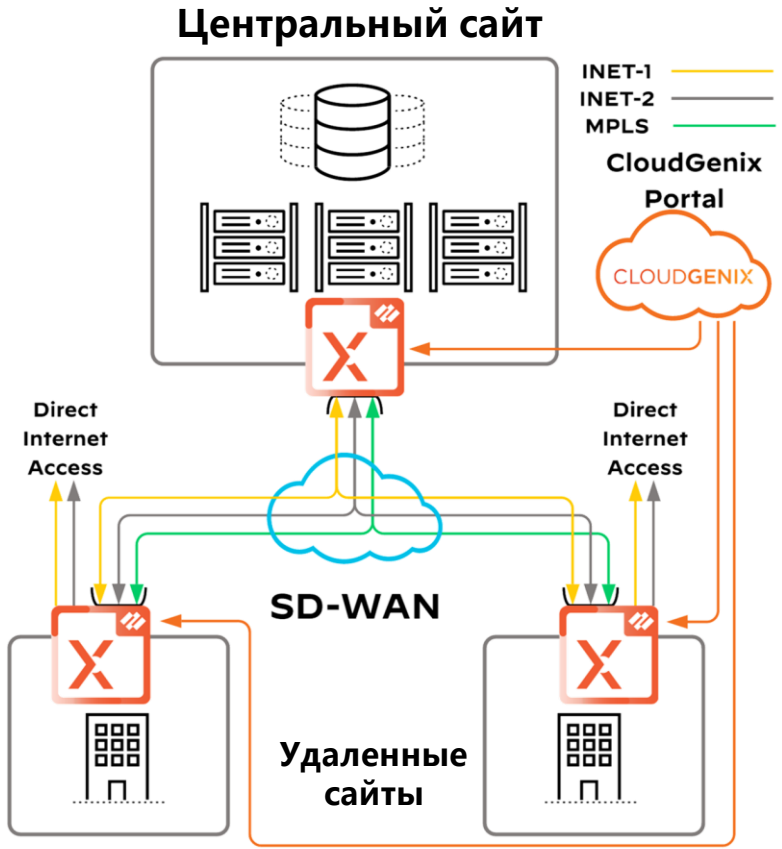
- Zero Touch Provisioning
- USB bootstrap – загрузка CPE с USB-флешки, содержащей нужную конфигурацию и (опционально) обновление версии ОС и контента,
- Централизованная преднастройка (staging)
- Настройка на объекте



CLOUDGENIX NG SD-WAN

CloudGenix SD-WAN позволяет создавать бизнес ориентированные политики с динамическим выбором пути следования трафика для обеспечения наивысшей производительности

- Управление через облачный портал CloudGenix
- Используются устройства CloudGenix Instant-On (ION) с поддержкой Zero-Touch-Provisioning
- Каналы Secure Fabric устанавливаются между всеми устройствами ION создавая VPN-канал поверх каждого WAN-канала
- Продвинутая визуализация, мощный набор инструментов для поиска причин неисправностей обеспечивают наилучшую производительность приложений



Прогресс в течение года

CLOUDGENIX

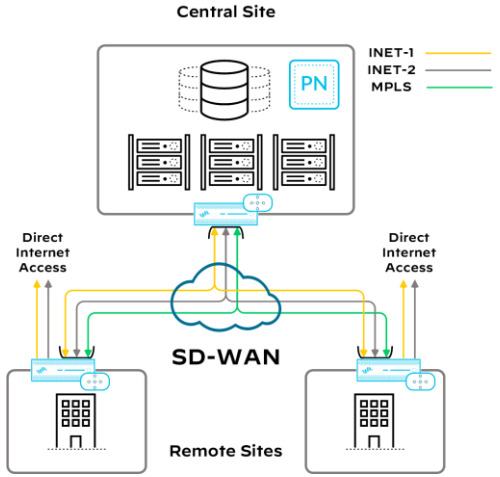
@Gartner WAN Edge Report 2020: Strengths (Сильные стороны)

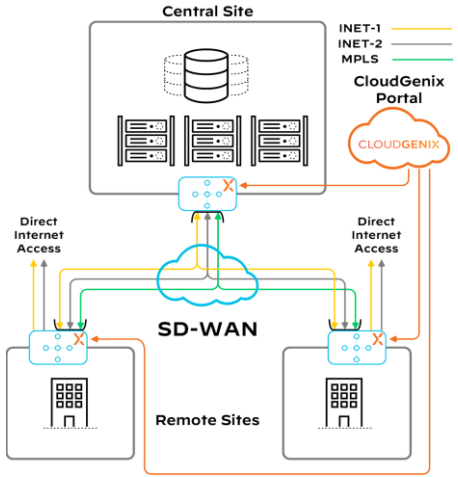
- Этот вендор получил самый высокий рейтинг среди заказчиков, которые пользуются SD-WAN.
- Palo Alto Networks одна из лучших функций визуализации среди других.

paloalto NETWORKS

Стратегия Palo Alto Networks SD-WAN

- Стратегия SD-WAN Palo Alto Networks позволяет Вам выбирать наилучшую архитектуру для Вашей организации.
- Мы продолжим совершенствовать обе технологии: CloudGenix SD-WAN и Palo Alto Networks OS Secure SD-WAN.
- Такая стратегия предоставляет Вам возможность выбора и гибкие возможности по реализации инфраструктуры SD-WAN используя как on-premises так и облачные решения в зависимости от Ваших потребностей.





Также смотрите вебинар:
https://youtu.be/dJUzel-5-FI

Полезные ресурсы

PaloAltoNetworks.com ➡ More ➡ Resources ➡ Content Library ➡ Фильтр “**By Type -** Guide”

- Architecture Guide - Palo Alto Networks SD-WAN
  https://www.paloaltonetworks.com/resources/guides/sd-wan-architecture-guide
- Deployment Guide - Palo Alto Networks PAN-OS Secure SD-WAN
  https://www.paloaltonetworks.com/resources/guides/pan-os-secure-sd-wan-deployment-guide
- Документация по SD-WAN
  https://docs.paloaltonetworks.com/sd-wan.html
- Документация по ZTP
  https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning.html
- Документация по USB bootstrapping
  https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/firewall-administration/bootstrap-the-firewall.html

Защита Docker, Kubernetes

Prisma, Aporeto, NGFW CN-серия

первый полноценный NGFW для Kubernetes

paloalto NETWORKS

Контейнеры получают все большее распространение в IT

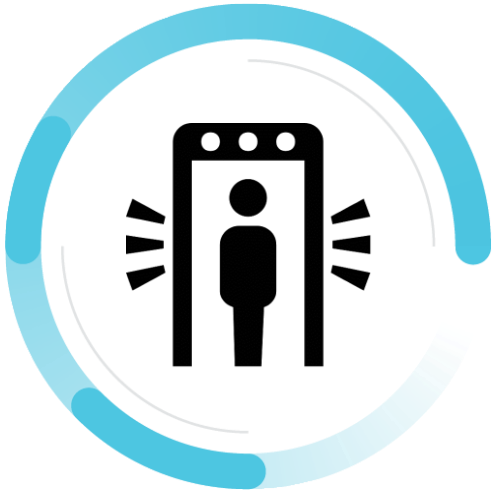
К 2023 году более 70% организаций будут использовать в продуктивной среде три и более приложений, работающий в контейнерах

Gartner, 2019

Многоэшелонированная защита для сред контейнеризации

Network Visibility

Microsegmentation



Layer 7 Threat Protection

Prisma

Aporeto

CN-Series

Strata

paloalto NETWORKS

Представляем контейнерный NGFW CN-серии

Подробнее про CN-series
https://youtu.be/IaJfdMs0qHg

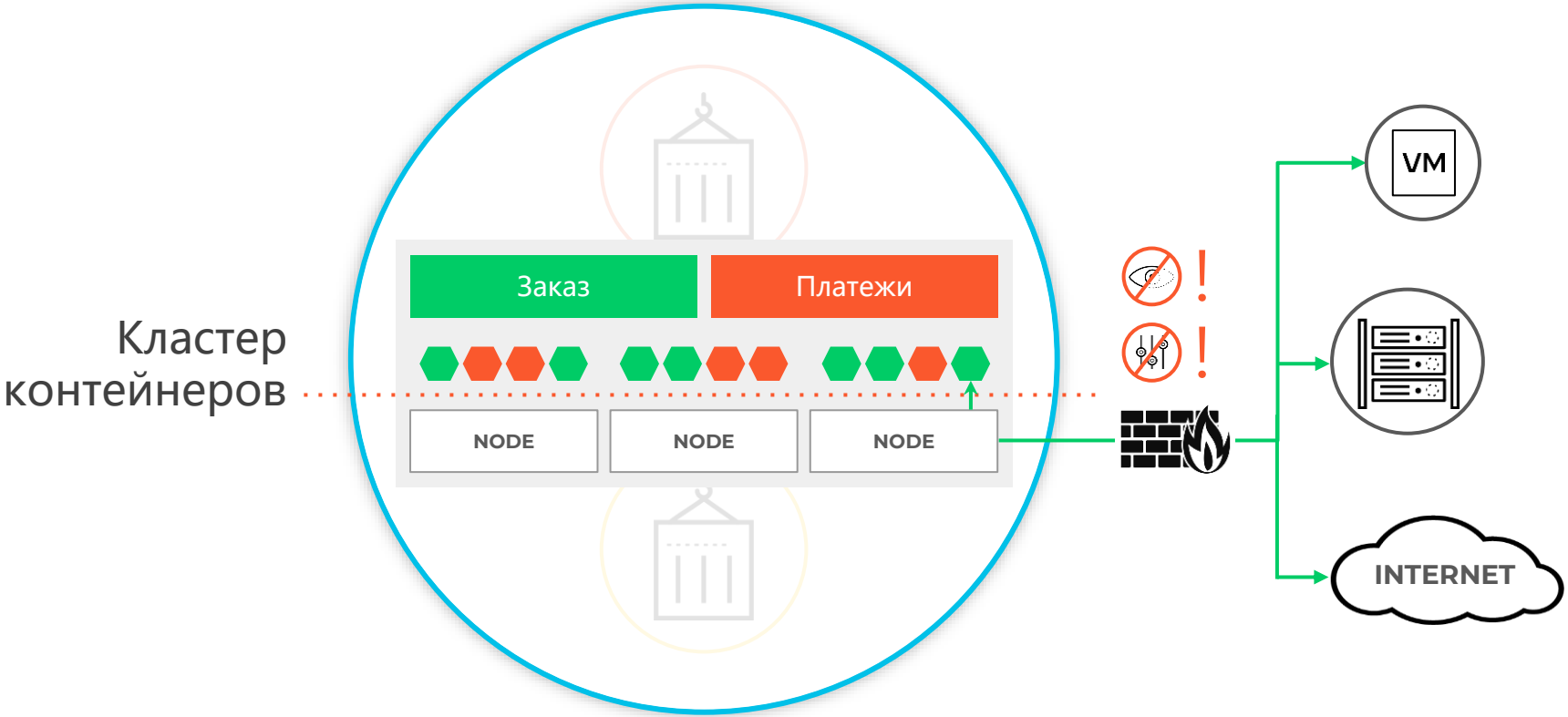
NGFW для среды Kubernetes

Возможности сервисов безопасности Palo Alto Networks в форма-факторе контейнера

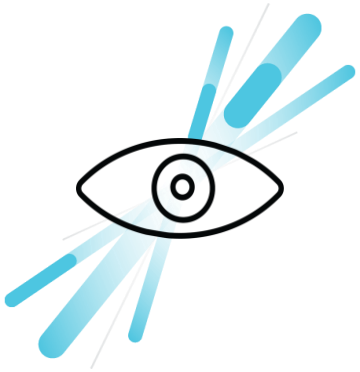
Защита сети на уровне L7 и предотвращение угроз

Интеграция с Kubernetes

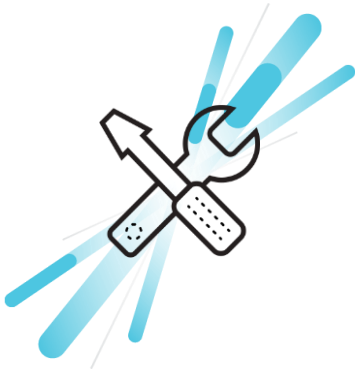
Классические форм-факторы МЭ не получают полной картины



Визуализация сетевых активов и защита от угроз в среде Kubernetes



Подробные данные о сущностях K8’s для контроля на базе контекста



Централизованное управление политиками и NGFW из Panorama

Автоматизация и масштабирование благодаря интеграции с Kubernetes

Поддержка контейнерных приложений on-premise и в облаке одновременно

Под Вашим управлением

На Ваших объектах

Публичные облака

Под управлением провайдера

Типовые сценарии использования CN-серии

Защита на L7 в направлении Восток-Запад

Реализация границ доверия между namespaces и другими типами рабочих нагрузок

Инспекция исходящего трафика

URL-фильтрация проверка содержимого на L7

Инспекция входящего трафика

Блокировка известных и неизвестных угроз

10.12.2020 | 11:00 MSK

ONLINE

Palo Alto Networks LIVE 2020

Зарегистрироваться

УЧАСТИЕ БЕСПЛАТНОЕ ПО ПРЕДВАРИТЕЛЬНОЙ РЕГИСТРАЦИИ

https://paloaltolive.tiger-optics.ru

Спасибо!

Денис Батранков

Russia@paloaltonetworks.com

paloaltonetworks.com

Palo Alto Networks Россия и СНГ
канал на Youtube
tiny.cc/paloaltorussia

https://paloaltolive.tiger-optics.ru