Решения Palo Alto Networks для защиты сети предприятия

Russia@paloaltonetworks.com

tiny.cc/paloaltorussia – канал на Youtube
tiny.cc/panfb – группа Facebook

Подход и преимущества Palo Alto Networks

Лидирующая компания в мире в области кибербезопасности

95

из Fortune 100

используют Palo Alto Networks

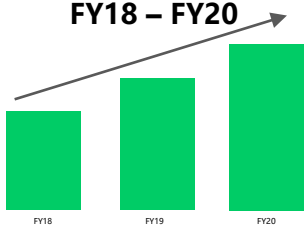
71% крупнейших 2К

заказчики Palo Alto Networks

#1

в Корпоративной безопасности

Рост выручки 22% CAGR FY18 – FY20



18% Год-к-Году

рост выручки

77 000

заказчиков

в 150+ странах

9/10

средняя оценка CSAT

Компания основана в 2005 году, головной офис в Санта-Кларе, США, Калифорния.
По состоянию на январь 2021 - **8000+ сотрудников**
Первый продукт – NGFW PA-серии выпущен в 2007 году,
Начиная с 2011 является лидером в сегменте NGFW согласно Gartner MQ. Множество наград и побед в различных тестах,
Активное развитие портфолио. **На текущий момент более 14 продуктов по безопасности,**
Капитализация на январь 2021 свыше **$34,8 млрд**.

Источник: Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19, 20 March 2020

Цифровая трансформация организаций повсюду фундаментально меняет то как они функционируют, внедряют новшества и коммуницируют с людьми для которых работают

Три силы, способствующие этой трансформации

Связность

От сетей электроснабжения до здравоохранения и торговли – большинство взаимодействия сейчас происходит через сеть

41.6 миллиард

Устройств будет подключено к Интернету к 2025 году

Облака

Мы можем все делать быстрее, эффективнее, автоматизированнее и более гибко

75%

всех баз данных будет развернуто или перенесено на облачные платформы к 2022 году

Данные & ИИ

Огромные массивы данных позволяют развивать и использовать продвинуты алгоритмы Машинного обучения и Искусственного Интеллекта

5-ти кратный

рост использования ИИ, развернутых на облачных платформах, с 2019 до 2023 года, превращает ИИ в один из самых используемых облачных сервисов

Источник: IDC, Gartner, Gartner

Для эффективной работы руководству необходимы

Прозрачность

Полная картина происходящего в сети и контроль над всей сложной архитектурой безопасности предприятия

40%

профессионалов ИБ сказали они хотели бы улучшить свои возможности обнаруживать, приоритезировать и устранять уязвимости в ПО

Доверенные источники данных Intelligence, автоматизация

и процессы с обратной связью, чтобы противостоять атакам, экономить время и масштабировать возможности по защите

95%

брешей облачных сервисов были из-за ошибок человека, например, из-за неправильной настройки

Простота & Гибкость

для безопасного функционирования сети всей компании, облака или смешанных сред

55%

организаций используют более 25 продуктов по безопасности

Источник: ESG Global, Gartner, ESG Global

Наш комплексный подход - это

Интегрированная платформа

Лучшие в индустрии возможности интегрированные между собой для превосходной прозрачности, контроля и эффективности

\+

Автоматизация

Быстрое реагирование, масштабирование для снижения количества рутинных операций, повышения эффективности и блокировки угроз

\+

Простота

Освобождает Вас для более важных и нужных задач, снижает стоимость эксплуатации, упрощает цифровую трансформацию

для обеспечения Вас платформой, которая находится на шаг впереди атакующего и предотвращает, а не только реагирует на уже состоявшуюся атаку

Портфолио Palo Alto Networks

Strata PA-серии

NGFW, использующие Машинное обучение

App-ID | User-ID | Content-ID | Device-ID

VM-серия

Виртуальные Next-Generation Firewall

App-ID | User-ID | Content-ID | Device-ID

CN-серия

Контейнерные Next-Generation Firewall

App-ID | User-ID | Content-ID | Device-ID

Panorama

Централизованное управление межсетевыми экранами и не только

Prisma Access

Secure Access Service Edge

FWaaS | Secure Web Gateway | Zero Trust Network Access

Prisma Cloud Enterprise & Compute

Cloud Native Security Platform

Cloud Security Posture Management (CSPM)
Cloud Workload Protection (CWPP)
Cloud Network Security (CNSP)
Cloud Infrastructure Entitlement Management (CIEM)

Prisma SaaS (CASB)

Анализ и защита SaaS приложений

SD-WAN

CloudGenix Next-Generation SD-WAN

Secure SD-WAN

Cortex XDR

Extended Detection & Response

Endpoint Threat Prevention
Endpoint Controls
Endpoint Detection & Response
Extended Detection & Response
Managed Detection & Response

Cortex XSOAR

Extended Security Orchestration, Automation and Response

Security Orchestration, Automation & Response | Threat Intelligence Management

AutoFocus

Платформа Threat Intelligence (TIP)

Сервисы безопасности

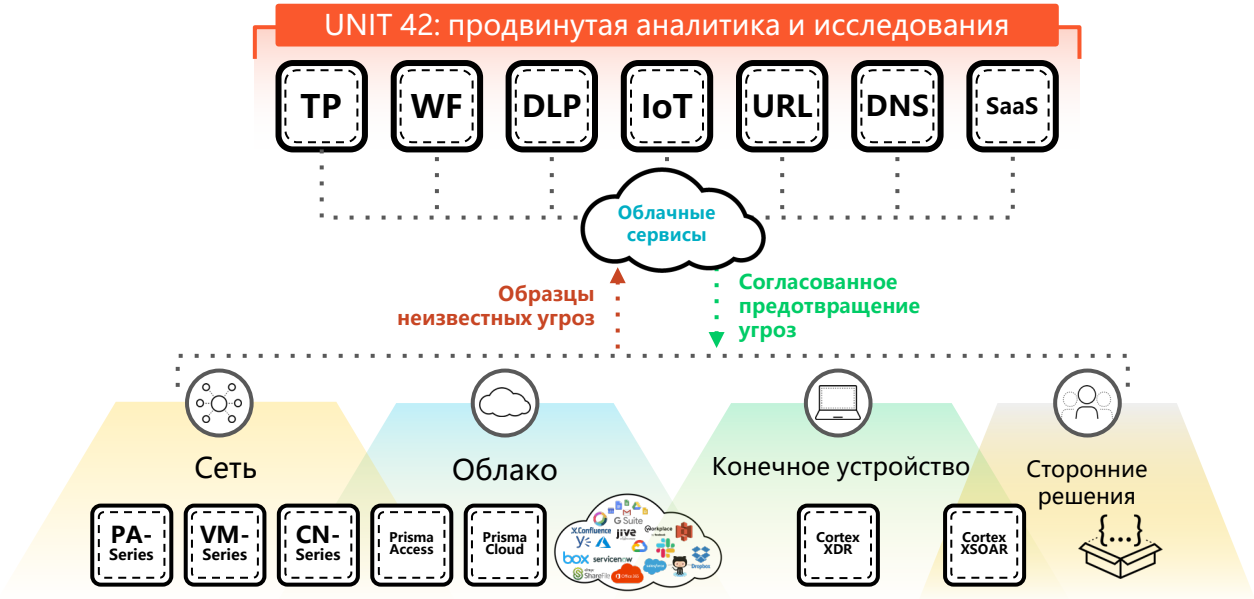
DNS Security	Защита от угроз	URL-фильтрация	WildFire	IoT Security	GlobalProtect	Машинное обучение	Data Loss Prevention
Защита от атак через DNS (DGA, туннели и т.д.)	Защита от эксплоитов, вирусов, программ-шпионов, C&C	Блокировка доступа к вредоносным и фишинговым сайтам	Обнаружение и блокировка угроз нулевого дня	Безопасность IoT для предприятия	Безопасность мобильных пользователей	Алгоритмы ML на NGFW блокируют угрозы нулевого дня и фишинговые сайты в режиме реального времени	Data Protection & Compliance

paloalto NETWORKS

НАША ЦЕЛЬ

Защитить всех Ваших пользователей, приложения, данные, сети и устройства с пониманием полного контекста. Всегда и в любой точке Вашей сети

Сервисы безопасности: лучшие в своем классе на базе взаимоувязанной платформы



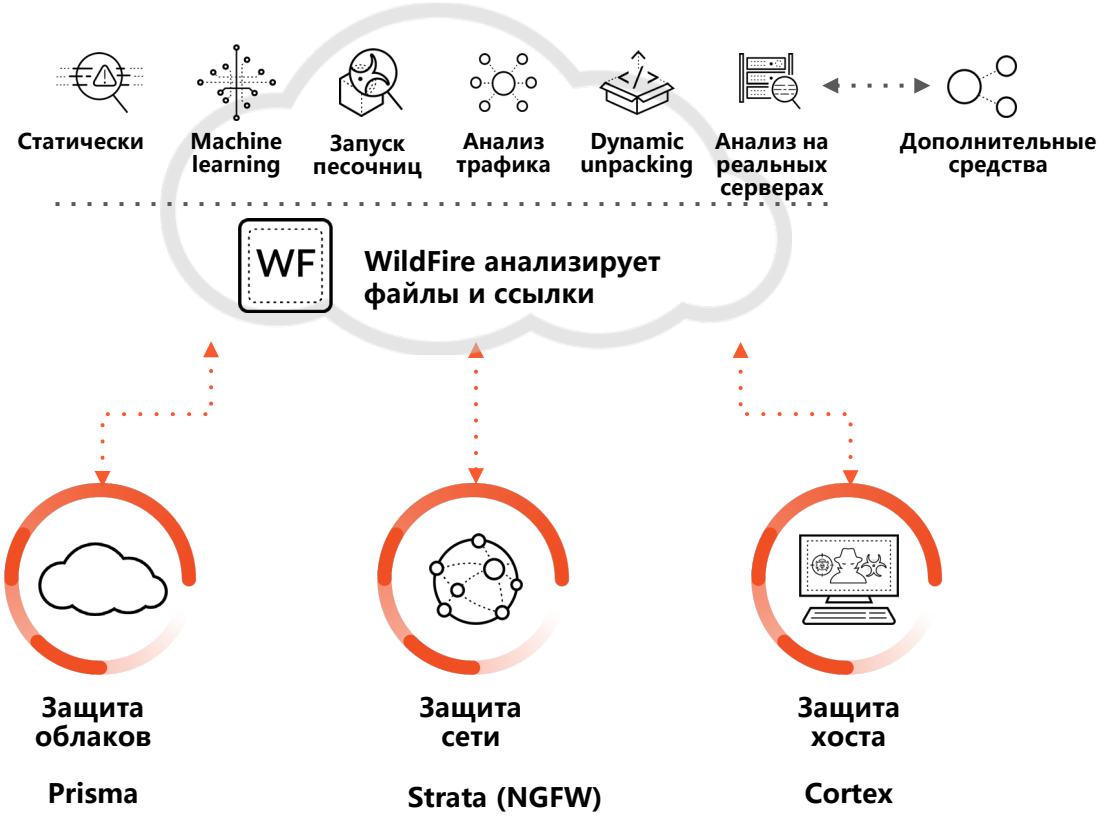
- Детектирование и предотвращение согласованное по всей компании без дополнительной инфраструктуры
- Сетевой кумулятивный эффект от 77000+ заказчиков с обновлениями в режиме реального времени
- Комбинация человеческого и искусственного интеллектов обеспечивают полное покрытие жизненного цикла атак
- Наивысшая эффективность и наилучший ROI по сравнению с конкурентами

Что такое платформа безопасности?
Автоматизация защиты и обмен данными встроены во все компоненты

1 NGFW, Prisma и Cortex отправляет подозрительные файлы и ссылки в WildFire

2 WildFire анализирует все неизвестное, обосновывает вердикт и оповещает через обновления

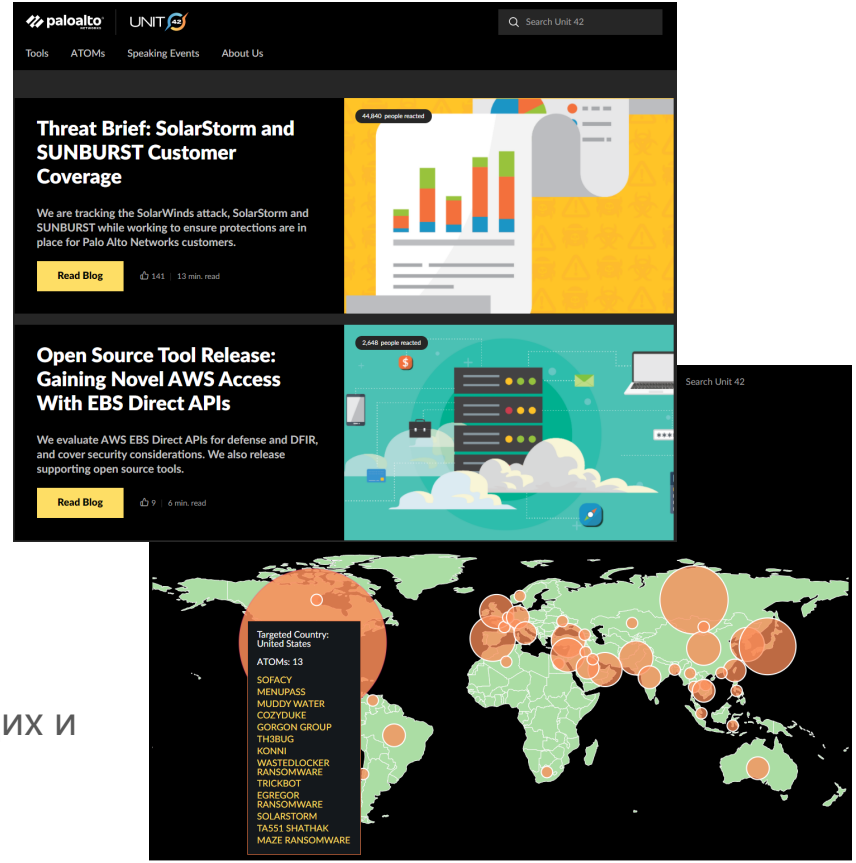
3 Автоматически настраивается защита от новой атаки на хосте, в облаке и в сети, базы сигнатур, ThreatIntel, URL пополняются



Кибербезопасность – это экспертиза

Исследовательская лаборатория **Unit42**

- **Unit 42** – команда исследователей и высококлассных специалистов по кибербезопасности Palo Alto Networks со всего мира.
- Мы занимаемся обнаружением новых угроз, threat hunting, поиском Zero-Day уязвимостей, reverse-engineering вредоносного ПО, анализом кода, анализом поведения хакерских группировок и их тактик, техник и процедур
- Результаты работы Unit42 используются для обновления баз угроз от Palo Alto Networks, совершенствования алгоритмов существующих и разработки новых продуктов и решений



https://unit42.paloaltonetworks.com/

Кибербезопасность – это экспертиза

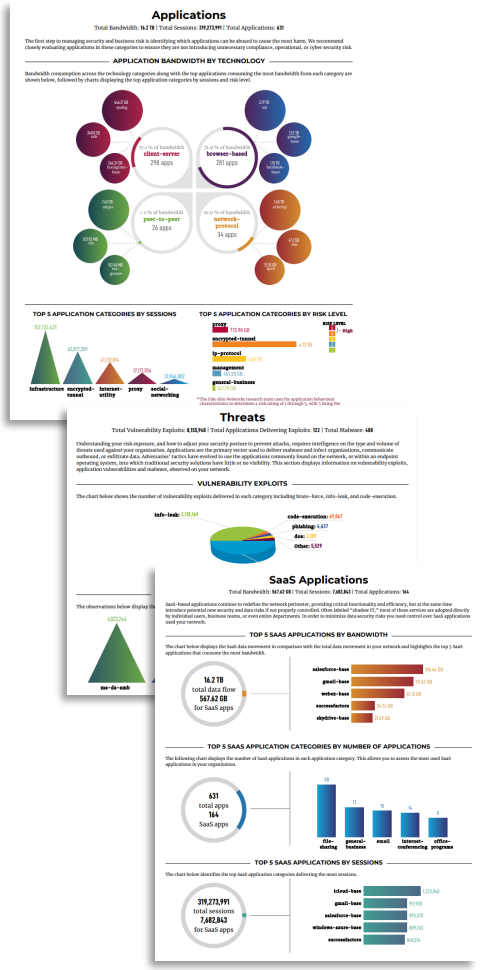
- **Crypsis** – команда экспертов Palo Alto Networks, предоставляющая заказчикам услуги по реагированию на инциденты, управлению рисками, форензике (расследованию)
- Мы используем экспертизу Crypsis, которую они получают работая с реальными инцидентами безопасности, для совершенствования наших технологий, алгоритмов и продуктов безопасности
- www.paloaltonetworks.com/resources/datasheets/crypsis-corporate-overview

- **Managed Detection & Response** – команда экспертов Palo Alto Networks, предоставляющая заказчикам услуги по обнаружению продвинутых угроз и реагированию на них используя продукты линейки Cortex
- Экспертиза используется для дальнейшего совершенствования наших продуктов, алгоритмов выявления атак, поведенческих правил, техник для выявления вредоносного когда нулевого дня
- www.paloaltonetworks.com/cortex/cortex-xdr/mdr

Кибербезопасность – это не только продукты

Широкий набор инструментов и лучших практик

- **Security Lifecycle Review** – визуализация происходящего в сети
- **Best Practice Assessment** – систематическая оценка соответствия конфигурации лучшим практикам
- **Prevention Posture Assessment** – оценка работы мер по предотвращению атак
- **Prevention Architecture Methodology** – методология внедрения Zero Trust
- **Expedition** – миграция конфигураций других производителей
- **Ultimate Test Drive** – бесплатные тренинги по продуктам
- **Бесплатное обучение** – академия и море документации
- **IronSkillet** – начальные настройки согласно лучшим практикам
- **PanHandler** – создание готовых конфигураций
- **Рекомендации и лучшие практики** по настройке



9-кратный лидер в Gartner Firewall MQ, NSS Labs Recommended

2020 Gartner Magic Quadrant for Network Firewalls

NSS Labs Recommended

Наивысшая эффективность защиты – проверено NSS Labs

Vendor	Palo Alto Networks	Check Point	Forcepoint	Huawei	Sophos	Fortinet	Vendor B	Vendor A
Blocked Exploits	1,783	1,779	1,784	1,721	1,680	1,781	Unknown	Unknow
Exploit Block Rate (1,784 Exploits)	99.94%	99.72%	100.00%	96.47%	94.17%	99.83%	88.40%	98.30%
Blocked Evasions	406	398	406	387	405	375	Unknown	Unknown
Evasion Block Rate (406 Evasions)	100%	99%	100%	98%	99%	94%	93%	79%
Security Effectiveness	97.90%	97.40%	96.20%	94.20%	93.30%	93.00%	82.20%	77.70%

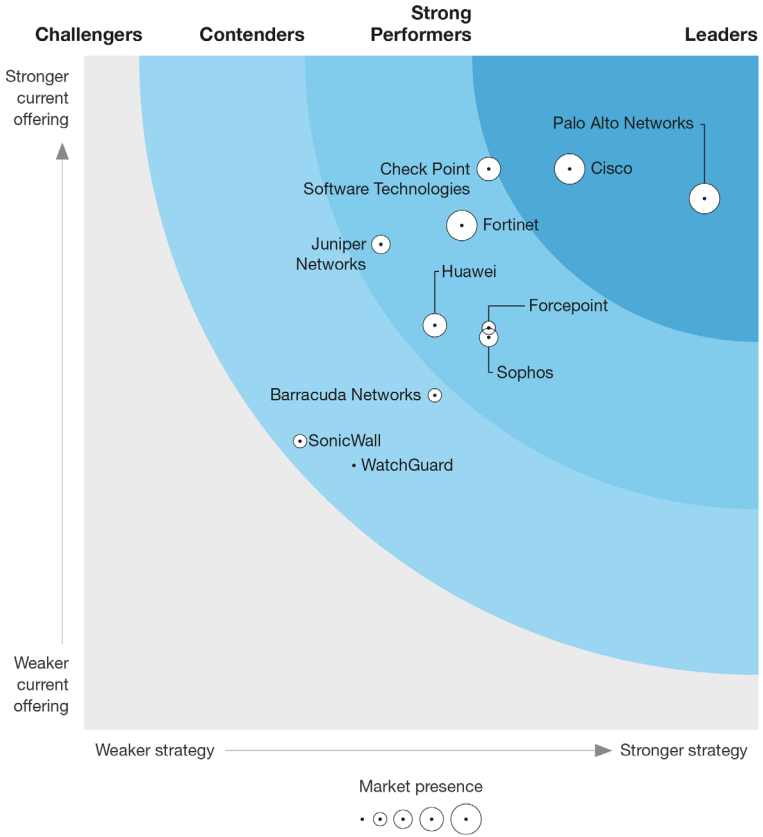
- Palo Alto Networks получило самую высокую оценку – 97.9% – заблокировав 1783 из 1784 эксплойтов и защитила от 406 техник обхода.
- Основная проблема современных IPS – техники обхода.

SOURCE: NSS LABS 2019 NGFW REPORT

THE FORRESTER WAVE™

Enterprise Firewalls

Q3 2020



Palo Alto Networks – лидер с самой сильной стратегией согласно отчету **The Forrester Wave™: Enterprise Firewalls, Q3 2020**

@Forrester Wave:

«With its combination of NGFWs, Cortex, Strata, and Prisma Access platforms, Palo Alto Networks is aiming to own not just the enterprise firewall market, but the cloud-security stack market of the future»

paloalto NETWORKS

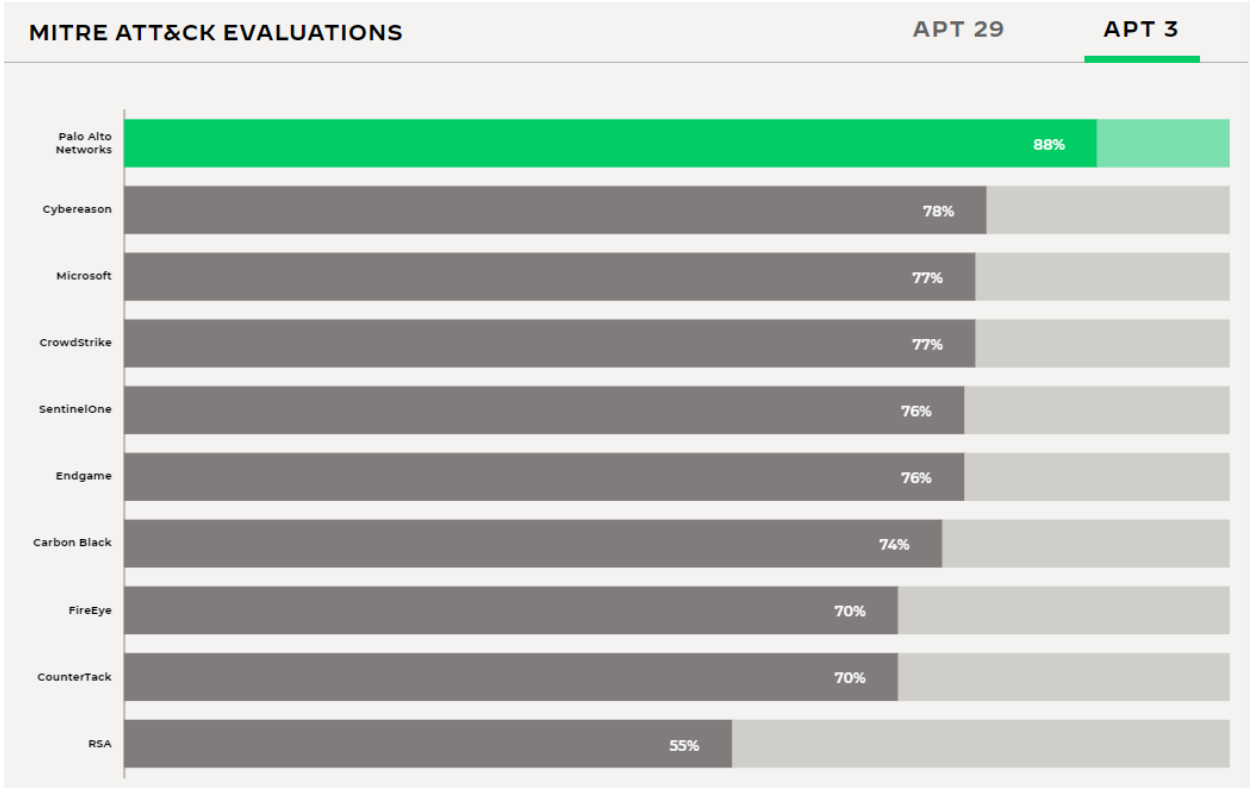
Мы лидируем предлагая решения для реализации модели Zero Trust

Оценки Forrester Wave Zero Trust eXtended (ZTX) помогает Вам двигаться к практической реализации модели Zero Trust

Мы убеждены наше позиционирование подтверждает, что интегрированная платформа Security Operating Platform может быть использована для реализации модели Zero Trust для предотвращения кибератак

Cortex XDR проверен MITRE ATT&CK

MITRE | ATT&CK™



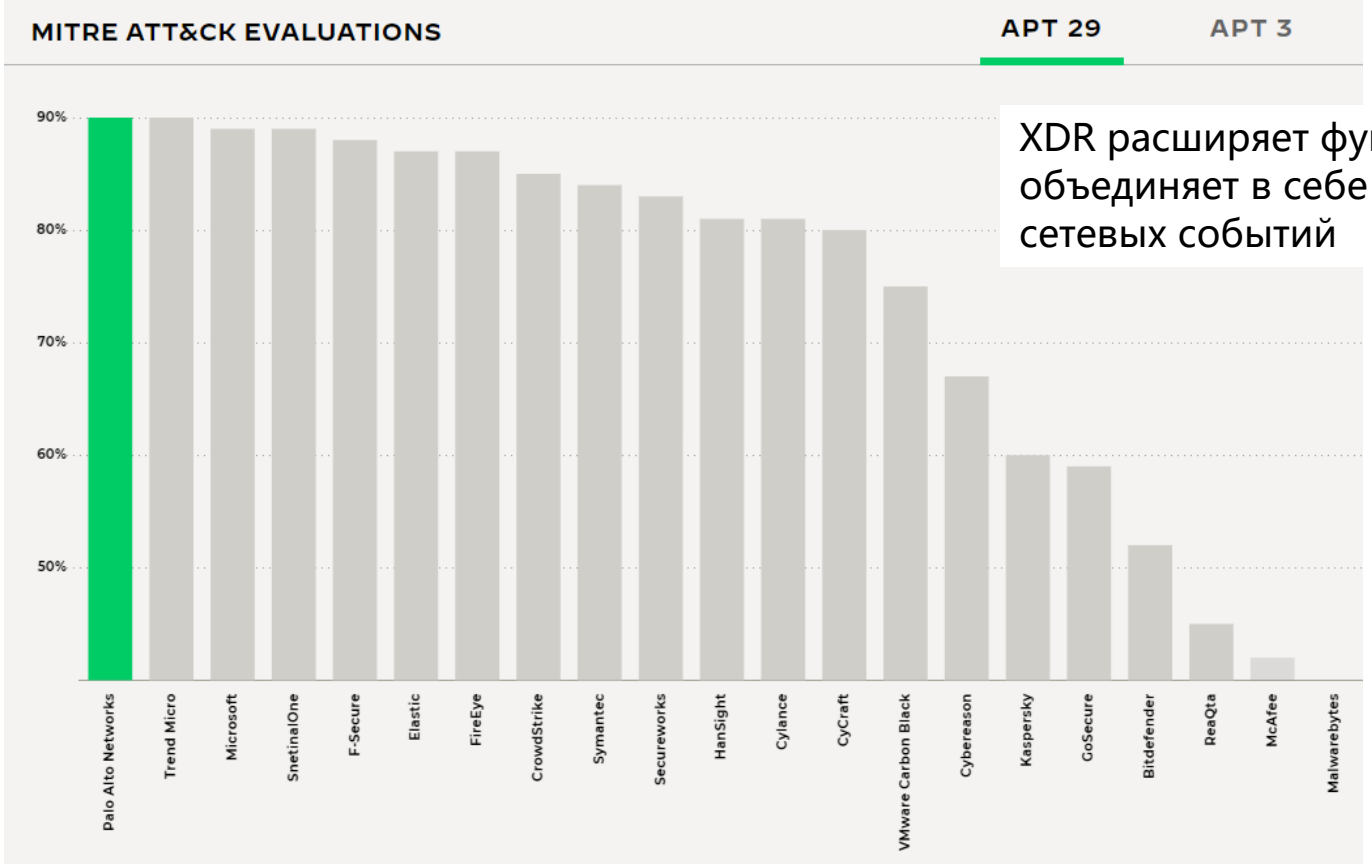
Больше всего баллов и на 93% меньше пропусков, чем у конкурентов

Покрытие техник атак

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

paloalto NETWORKS

Cortex XDR проверен MITRE и является лидером рынка EDR

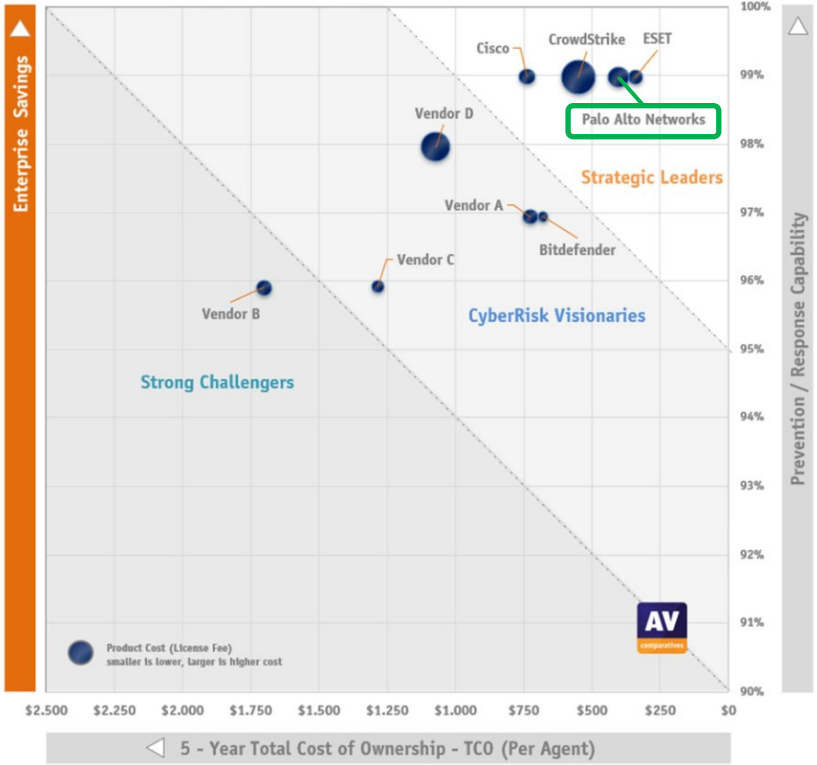


XDR расширяет функции EDR и также объединяет в себе функции анализа сетевых событий

blog.paloaltonetworks.com/2020/04/cortex-mitre/

Cortex XDR – стратегический лидер среди ERP

Наивысший процент обнаружения malware и невысокая стоимость владения



Product	5-Year Product Cost (Per Agent)	Active Response	Passive Response	Combined Prevention/Response Capabilities Y-Axis	5-Year TCO (Per Agent) X-Axis
Bitdefender	$100	93.9%	100%	96.9%	$679
Cisco	$158	98.0%	100%	99.0%	$737
CrowdStrike	$357	98.0%	100%	99.0%	$550
ESET	$149	98.0%	100%	99.0%	$342
Palo Alto Networks	$210	98.0%	100%	99.0%	$403
Vendor A	$146	93.9%	100%	96.9%	$725
Vendor B	$158	93.9%	98.0%	95.9%	$1,702
Vendor C	$125	93.9%	98.0%	95.9%	$1,283
Vendor D	$300	98.0%	98.0%	98.0%	$1,072

Description	Details
Enterprise Product Savings: **Palo Alto Networks** prevents most attacks and offers effective passive	High (>95%)
Overall **Active Response** Rate (Prevention Rate):	98.0%
Overall **Passive Response** Rate (Response Rate):	100%

blog.paloaltonetworks.com/2020/12/cortex-av-comparatives-epr-evaluation

Преимущества

В чем преимущества для бизнеса

- Легко использовать – походит для работы любых приложений
- Постоянство производительности – даже если появились новые функции
- Глубже настройки по тому что и как защищать – больше критериев проверки, наличие динамических групп и возможность включить все проверки одновременно
- Обучение и утилиты для помощи в настройке – Best Practice Assessment, Policy Optimizer, IronSkillet, Beacon и многое другое
- Счастливые заказчики – не существует заказчика, который видит смысл менять Palo Alto Networks на что-то другое
- Исследования в области новых атак и техник для лучшей защиты – знания и исследования лаборатории UNIT42

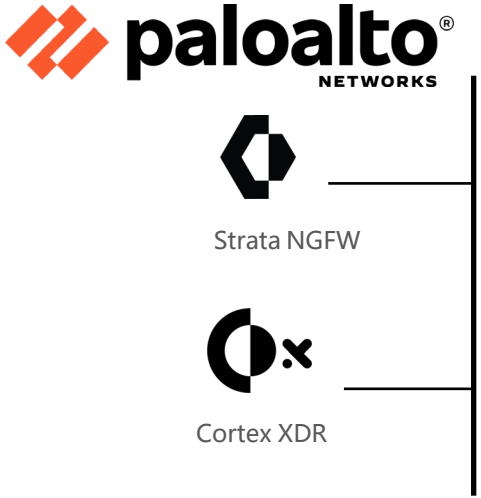
Почему с Palo Alto Networks выгоднее

Использование Palo Alto Networks NGFW выгодно

Palo Alto Networks NGFW выгоды	Почему это важно?
Нужно меньше оборудования и ПО для решения задач	Снижает CAPEX и OPEX
Предсказуемое время жизни оборудования из-за возможности перепрограммировать	Снижает CAPEX и OPEX
Гарантированная производительность без необходимости сложного тюнинга	Не нужно выключать безопасность для гарантии работоспособности сервисов
Panorama для связки всех NGFW	Снижение сложности и OPEX
Утилиты для снижения риска и расходов	Низкая вероятность неверной конфигурации, приводящей к взломам

А что в комплексе?
Глубокоэшелонированная защита на хосте и сети

Нет шансов для взлома

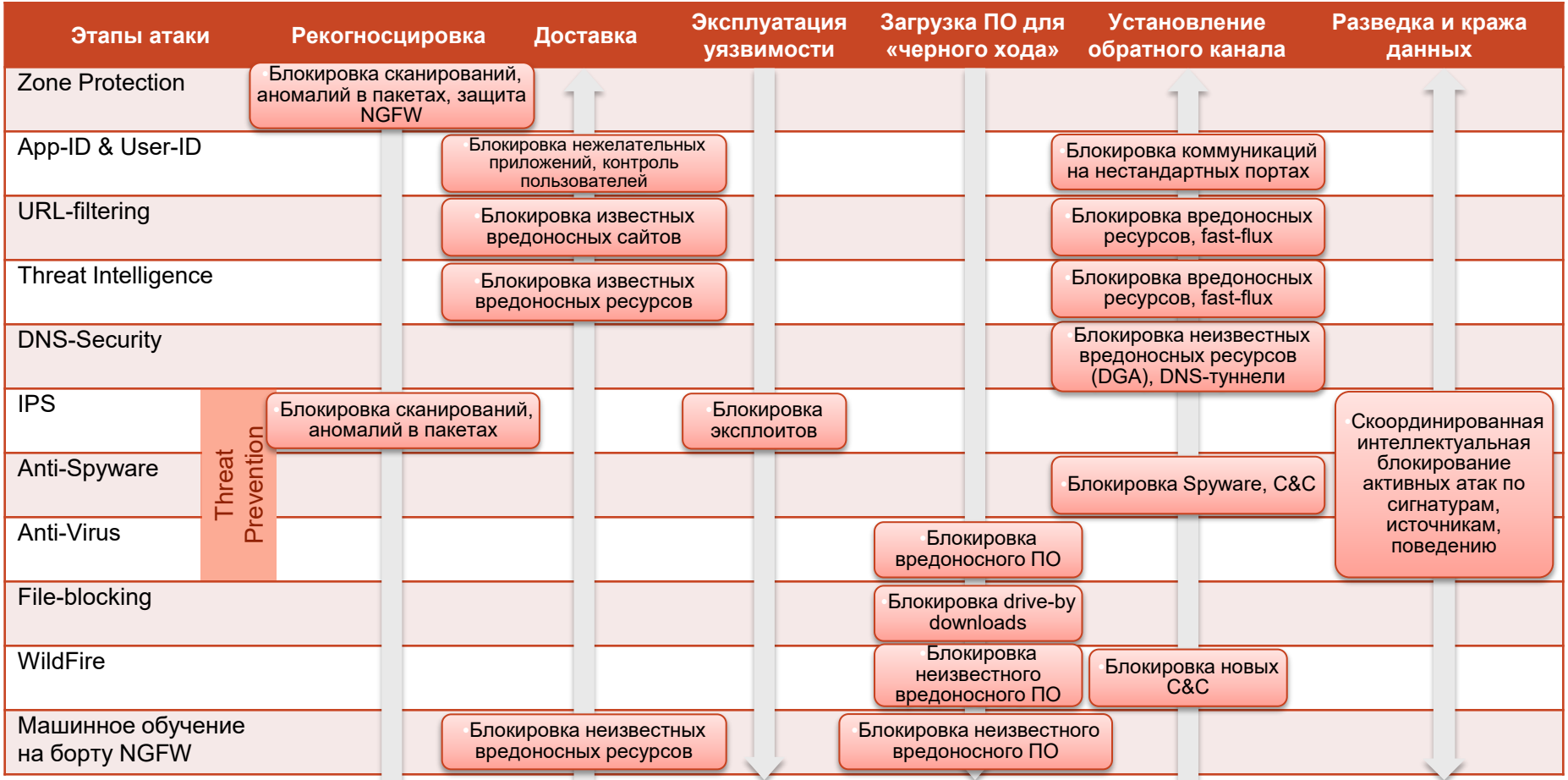


Next-Generation Firewall

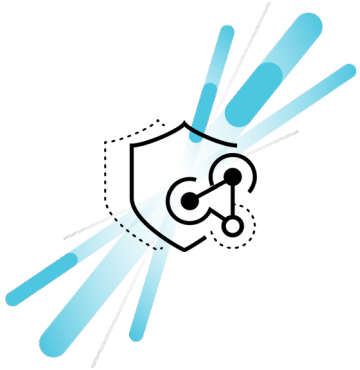
paloalto NETWORKS

Palo Alto Networks – это платформа защиты нового поколения

Глубокоэшелонированная защита



Межсетевой экран с Машинным обучением



Предотвратить то, что не встречалось раннее

Обнаруживает новые варианты угроз и новые устройства без сигнатур

Рекомендовать политики и изменения конфигурации

Анализирует поведение устройств и автоматически создает IoT-политики безопасности, использует изменения инфраструктуры для изменения конфигурации

Обнаружить используя анализ больших данных

Выполняет обучение на массивах данных масштабов облака постоянно анализируя огромное число данных об угрозах и телеметрию

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**

Как это работает: блокировка вредоносных файлов с помощью машинного обучения

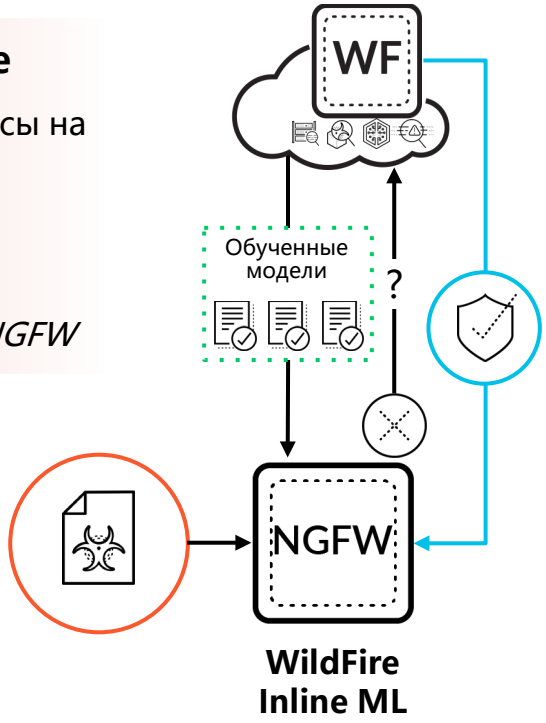
Продвинутый анализ в облаке

Бесконечные вычислительные ресурсы на страже против сложных угроз в поддерживаемых типах файлов

- *Генерирует сигнатуру за секунды*
- *Обучает и поставляет обновления моделей машинного обучения в NGFW*

Мгновенная защита на NGFW

- ⊘ Вредоносный код в Portable Executable/DLL
- ⊘ Атаки через PowerShell



9.6 миллиардов атак с использованием ВПО в год (2019)

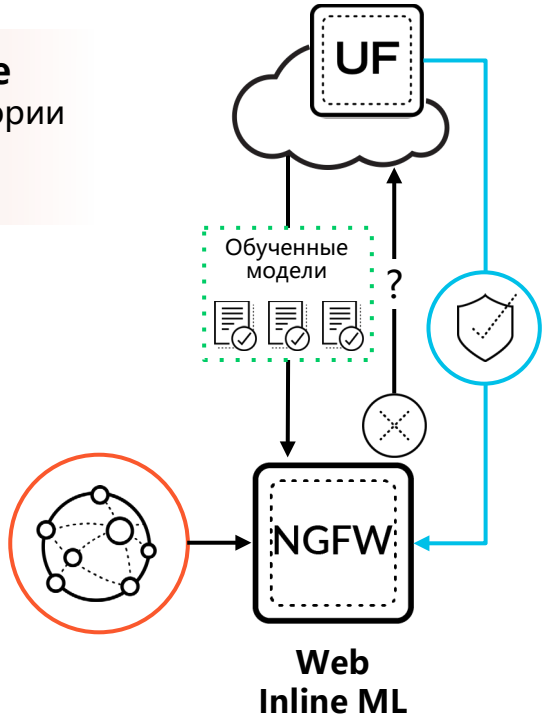
38 000 вариаций вредоноса Emotet (первая половина 2019)

Как это работает: блокировка веб-атак с помощью машинного обучения

Продвинутый анализ в облаке

Вредоносные или безвредные категории

- Категоризация в течение минут
- Действия на основе политик



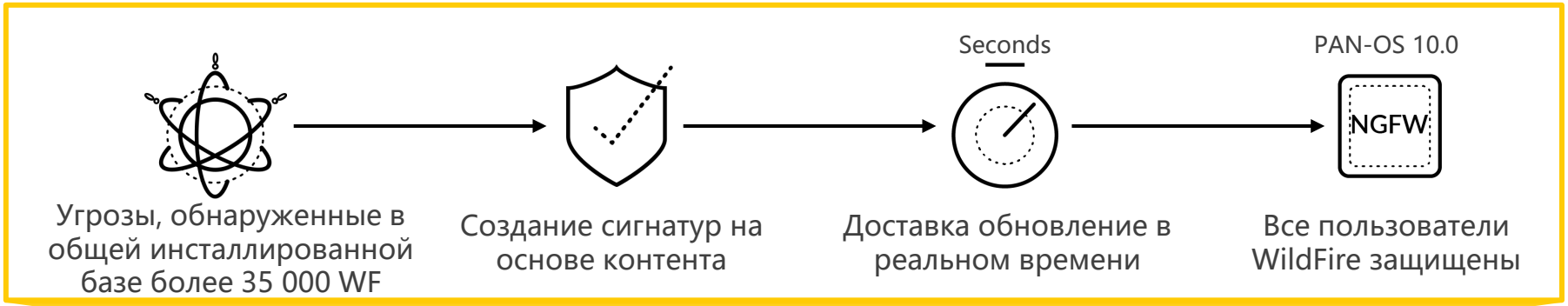
Мгновенная защита на NGFW

- ⊘ Фишинговые атаки
- ⊘ JavaScript атаки

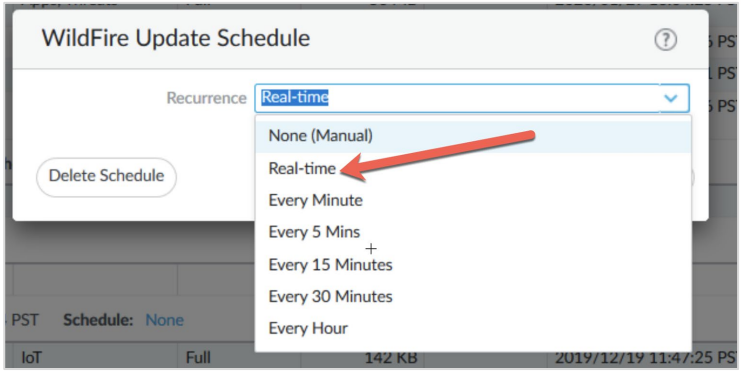
Тысячи совершенно новых фишинговых атак происходят каждый день

Свыше **30%** фишинговых писем открываются в течение 60 секунд после отправления

Доставка обновлений защиты беспрецедентно быстро

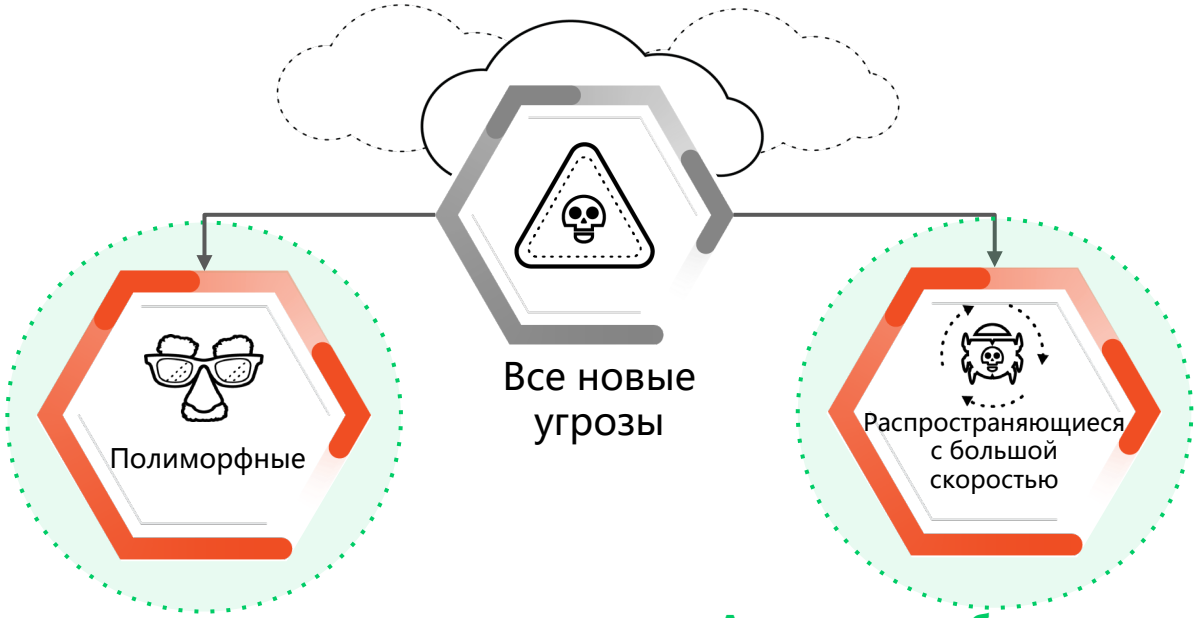


РАНЬШЕ
Лидирующее в индустрии время создания и доставки сигнатур за **5 минут**



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

Нивелируя преимущества атакующих



Машинное обучение

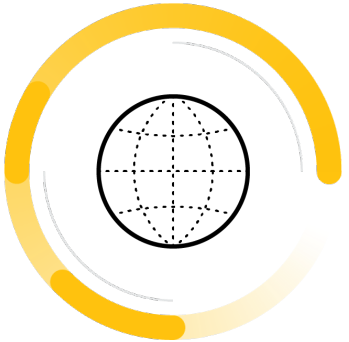
Анализ в глобальном сервисе с генерацией сигнатур в реальном времени

- **Обеспечивается масштабированием платформы**
- **Предотвращает начальное заражение**
- **Нет нарушений бизнес-процессов**

DNS Security

Блокировка известных «плохих» доменов

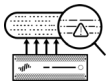
Использование машинного обучения и предиктивного анализа для блокировки вредоносного трафика, использующего DNS



Интеграция с NGFW означает, что защиту нельзя обойти

Данные

WildFire Analysis



Passive DNS

URL-фильтрация

Honeynets

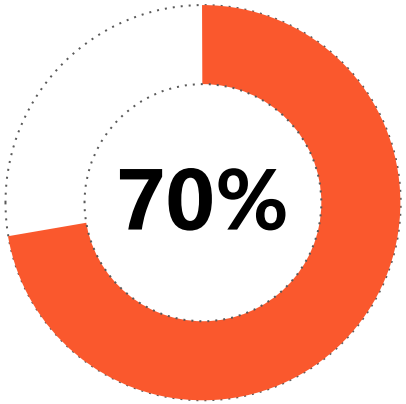
Unit 42

Whois

Зашифрованный трафик представляет большой риск

Сейчас почти весть Интернет трафик шифруется (HTTPS, SMTPS, IMAPS и т.д.)

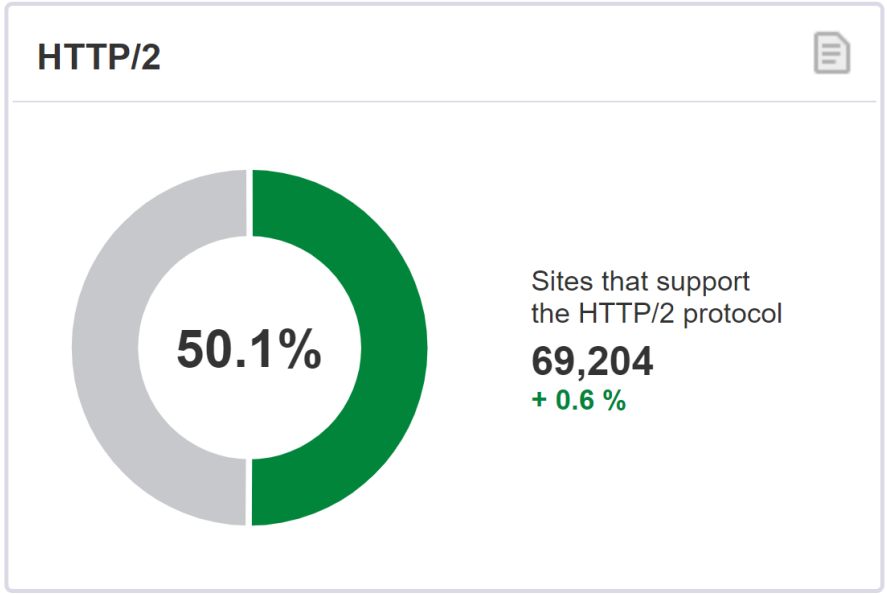
Атакующие пользуются этим

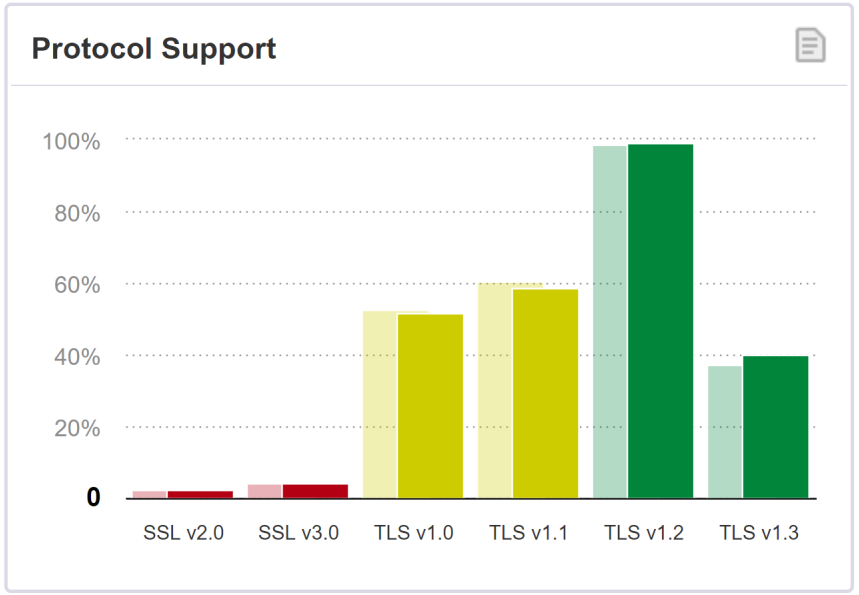


Более 70% вредоносных кампаний в 2020 будут использовать один из видов шифрования для скрытия вредоносной активности. Gartner

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

HTTP/2 + TLS 1.3 для защиты любых современных приложений



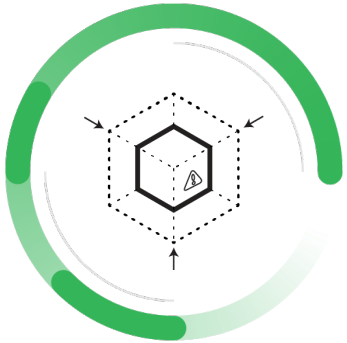


Поддержка HTTP/2 и TLS 1.3 ресурсами в сети Интернет

Уже сейчас HTTP/2 половина ресурсов в Интернете используют HTTP/2, а полгода назад было 40%.
Идет быстрый рост. Если Ваш фаервол не понимает HTTP/2 он не видит половины браузерного трафика

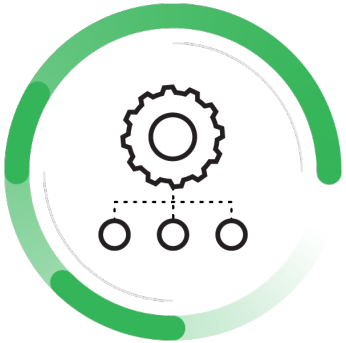
Источник: https://www.ssllabs.com/ssl-pulse/ по состоянию на Декабрь 2020г.

Инспекция TLS 1.3 и HTTP/2



Уменьшение рисков безопасности

Контролируйте использование устаревших версий SSL/TLS, небезопасных шифров и сертификатов с нарушениями



Упрощение внедрения

Разворачивайте и поддерживайте дешифрование легче используя предназначенные для этого средства диагностики и мониторинга

Инспекция трафика облачных приложений быстрее

Проверяйте и защищайте трафик HTTP/2 и TLS 1.3. Теперь с 2-х кратным увеличением производительности

Риски, связанные с DNS

80% вредоносного кода используют DNS

DNS используется для создания каналов управления (Command and Control) и кражи данных

Новые домены

Вредоносный код используют алгоритмы генерации доменных имен (Domain Generation Algorithms) для обхода детектирования

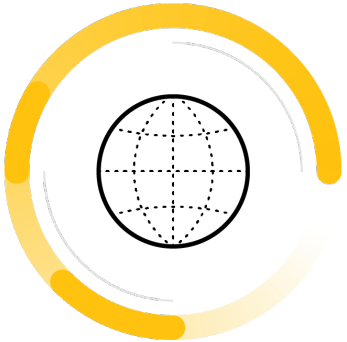
Утечка данных

Использование DNS-туннелирования для создания скрытых каналов

DNS Security

Блокировка известных «плохих» доменов

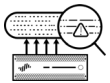
Использование машинного обучения и предиктивного анализа для блокировки вредоносного трафика DNS



Интеграция с NGFW означает, что защиту нельзя обойти

Данные

WildFire Analysis



Passive DNS

URL-фильтрация

Honeynets

Unit 42

Whois

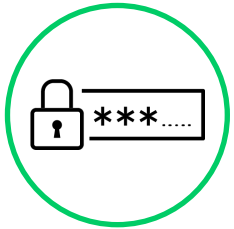
Блокировка краденных паролей

Конфиденциальные данные в компании

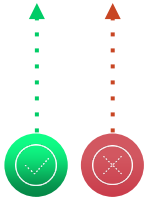
Платформа

Ping ID RSA okta SafeNet DUO Entrust

Multi-Factor Authentication



Пароль сотрудника



Украденный пароль

Статические и динамические группы безопасности

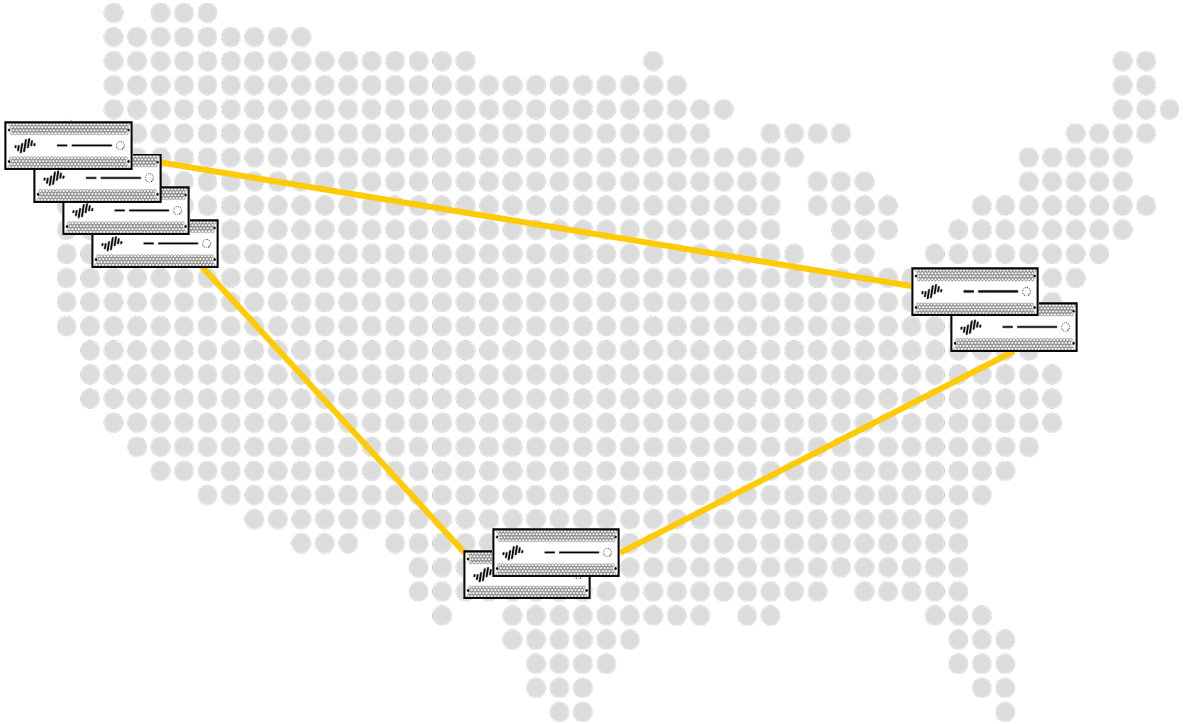
Статические группы

- Содержат набор объектов (vCenter Objects, NSX Objects, Network Objects, AD Objects)
- Некоторые типы объектов на самом деле динамические
- Примеры – VMs, vNICS, Logical Switches, IPSets, AD Groups

Динамические группы

- Используют выражение (шаблон, regex) для определения набора ВМ на основе метаданных
- Пример: ВМ из кластера Test с операционной системой Windows 2008 R2

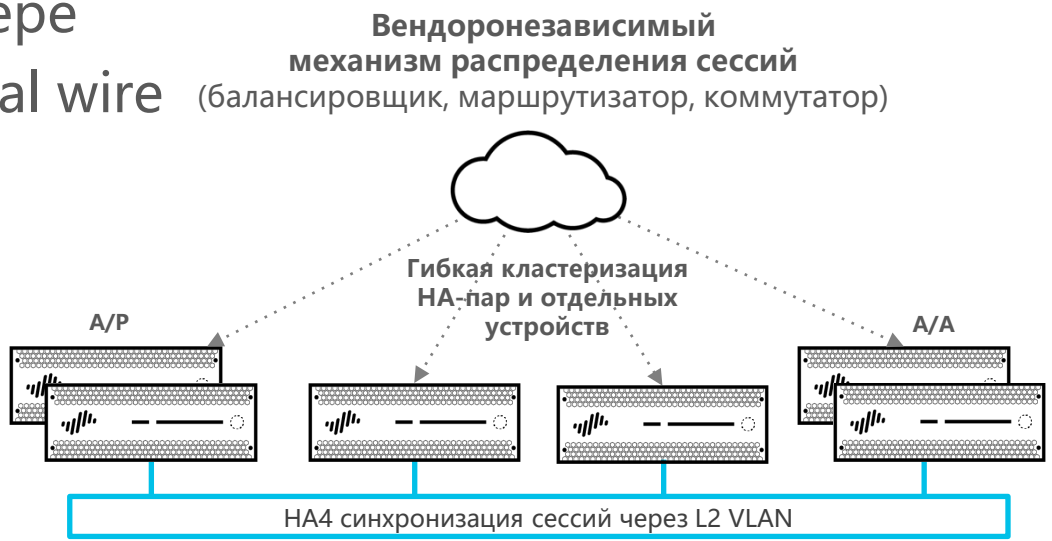
Простое масштабирование отказоустойчивых кластеров



- Добавляйте новые устройства для масштабирования производительности и емкости
- Высокая уровень отказоустойчивости для предотвращения нарушения бизнес-процессов
- Сервисы безопасности работают бесшовно и масштабируются вместе с Вашими приложениями

Обзор новых возможностей для кластеров высокой доступности

- До 16 устройств в кластере
- Поддержка Layer 3, virtual wire
- Работает на:
  - PA-3200-серии
  - PA-5200-серии
  - PA-7000-серии
    (применимо к XM и 100G NPC)
  - VM-300, 500, 700



VM-серия

Всесторонняя защита в различных средах виртуализации

Спецификации						
Модель	Сессий	Правил	Security Zones	Dynamic Address Objects	IPSec VPN Tunnels	SSL VPN Tunnels
VM-50	50 000	250	15	1000	250	250
VM-100 VM-200	250 000	1500	40	2500	1000	500
VM-300 VM-1000-HV	900 000	10 000	40	100000	2000	2000
VM-500	2 000 000	10 000	200	100000	4000	6000
VM-700	10 000 000	20 000	200	100000	8000	12000
минимум 2 ядра (2 или 8 ядер оптимально)						
Минимум 4GB RAM для VM-50 Lite mode						
Минимум 40GB HD (дополнительно 2 TB HD optional)						
До 10 интерфейсов – 1 управляющий и 9 для Data Plane – Tap, vWire, L2 & L3						
Поддержка High Availability (Active/Passive, Active/Active)						
Поддержка CPU oversubscription, поддержка Jumbo Frame						

Всесторонняя защита в различных средах виртуализации

Системные требования

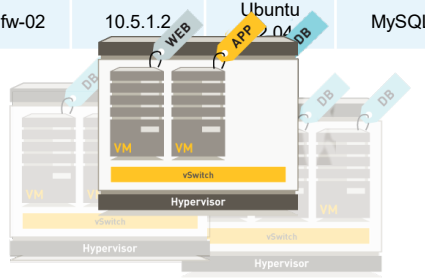
Модель	Гипервизор	vCPU	vRAM	Минимум жесткий диск
VM-50	ESXi, Hyper-V, KVM	2	5.5GB 4.5GB in Lite mode	32GB (60GB at boot)
VM-100 VM-200	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, NSX-V, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS NSX-T (VM-100)	2	6.5GB	60GB
VM-300 VM-1000-HV	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, NSX-V, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T (VM-300)	2, 4	9GB	60GB
VM-500	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, NSX-V, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	2, 4, 8	16GB	60GB
VM-700	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	2, 4, 8, 16	56GB	60GB

https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-models/vm-series-system-requirements.html

Динамические адресные группы (DAG) и мониторинг VM

VMware vCenter или ESXi

Name	IP	Guest OS	Container
web-sjc-01	10.1.1.2	Ubuntu 12.04	Web
sp-sjc-04	10.1.5.4	Win 2008 R2	SharePoint
web-sjc-02	10.1.1.3	Ubuntu 12.04	Web
exch-mia-03	10.4.2.2	Win 2008 R2	Exchange
exch-dfw-03	10.4.2.3	Win 2008 R2	Exchange
sp-mia-07	10.1.5.8	Win 2008 R2	SharePoint
db-mia-05	10.5.1.5	Ubuntu 12.04	MySQL
db-dfw-02	10.5.1.2	Ubuntu 12.04	MySQL
	10.5.1.9		



Dynamic Address Groups

Name	Tags	Addresses
SharePoint Servers	SharePoint Win 2008 R2 “sp”	10.1.5.4 10.1.5.8
MySQL Servers	MySQL Ubuntu 12.04 “db”	10.5.1.5 10.5.1.2 10.5.1.9
Miami DC	“mia”	10.4.2.2 10.1.5.8 10.5.1.5
San Jose Linux Web Servers	“sjc” “web” Ubuntu 12.04	10.1.1.2 10.1.1.3

Security Policy

Source	Destination	Action
San Jose Linux Web Servers	SharePoint Servers	✔
MySQL Servers	Miami DC	⊘

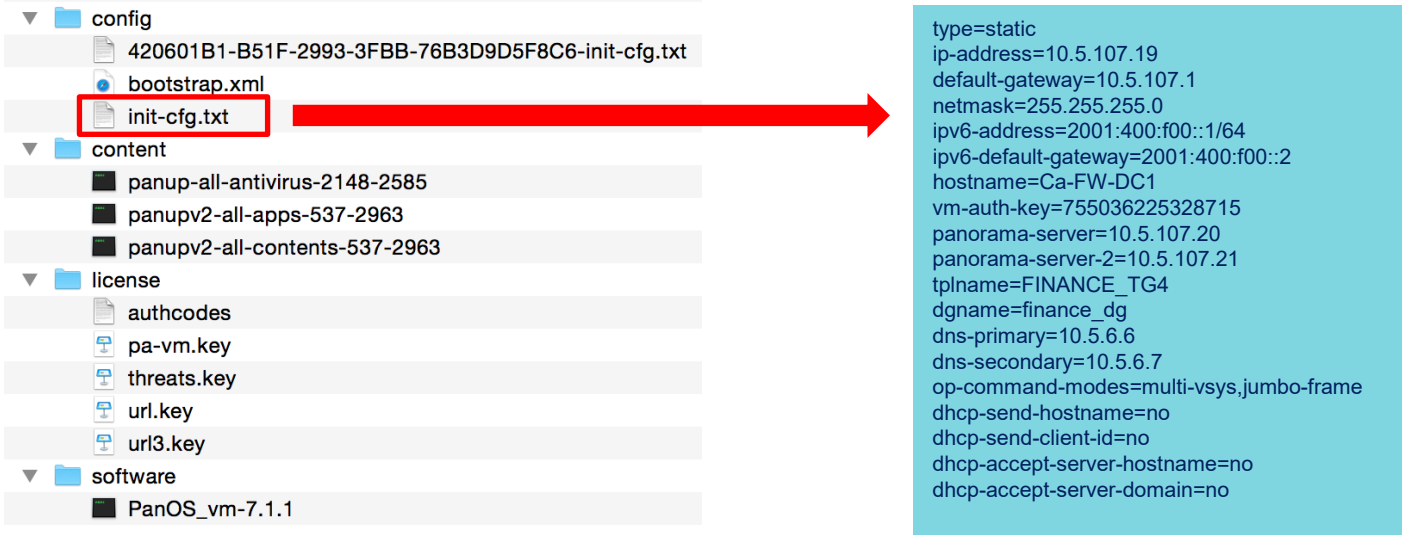
Политики безопасности внутри ЦОД

		Source	Destination			
Name	Location	Address	Address	Application	Action	Profile
To Domain Controller	NSX Device Group	MSSQLServers SharePointServers WebFrontEndServers	ActiveDirectoryServers	Domain Controller Applications	✓	
From Domain Controller	NSX Device Group	ActiveDirectoryServers	MSSQLServers SharePointServers WebFrontEndServers	AD Polling	✓	
WebFrontEnd to SharePoint	NSX Device Group	SharePointServers WebFrontEndServers	SharePointServers WebFrontEndServers	WFE - SP	✓	
To MS SQL	NSX Device Group	SharePointServers WebFrontEndServers	MSSQLServers	MSSQL	✓	
Management Traffic	NSX Device Group	ManagementServers	ActiveDirectoryServers MSSQLServers SharePointServers WebFrontEndServers	Management Traffic	✓	

- Только «белые списки»:
  - Известные приложения
  - «Самописные» неизвестные приложения
  - Динамические группы адресов VM

Интеграция с системами оркестрации

- Автоматизация развертывания, загрузки конфигурации и обновления
- Применение лицензий и взятие под управление в систему Panorama автоматически
- Автоматическая загрузка и применение InitConfig и Production config
- Работает при наличии доступа в Интернет у VM NGFW, при наличии доступа в Интернет через Panorama, а также без доступа в Интернет




```
type=static
ip-address=10.5.107.19
default-gateway=10.5.107.1
netmask=255.255.255.0
ipv6-address=2001:400:f00::1/64
ipv6-default-gateway=2001:400:f00::2
hostname=Ca-FW-DC1
vm-auth-key=755036225328715
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=no
dhcp-send-client-id=no
dhcp-accept-server-hostname=no
dhcp-accept-server-domain=no
```

https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/bootstrap-the-vm-series-firewall.html

Автоматизация

- Поддержка управления NGFW и EMS Panorama через REST API

Resource Method		Read the list of resources	Create a resource	Modify a resource	Delete a resource	Rename a resource	Move a policy rule(Policies only)
HTTP Method		**GET**	**POST**	**PUT**	**DELETE**	**POST**	**POST**
Query Parameters	name	optional	required	required	required	required	required
	location	required, valid values on the firewall: predefined , ,shared for Objects nly , vsys , or panorama-pushed	required, valid values on the firewall: ,shared for Objects nly , vsys valid values on Panorama: shared or device-group	required, valid values on the firewall: ,shared for Objects nly , vsys valid values on Panorama: shared or device-group	required, valid values on the firewall: ,shared for Objects nly , vsys valid values on Panorama: shared or device-group	required, valid values on the firewall: ,shared for Objects nly , vsys valid values on Panorama: shared or device-group	required, valid values on the firewall: shared , vsys valid values on
	vsys	required, if location is vsys or panorama-pushed	required, if location is vsys	required, if location is vsys	required, if location is vsys	required, if location is vsys	

Create an Address Object

Make a POST request to create an address object. In the request, the query parameters must include the name and the location on where you want to create the object. And in the request body include the same name, location and other properties to define the object. For example:

```
curl -X POST \
        'https://10.1.1.4/restapi/v10.0/objects/Addresses?location=shared&name=web-servers-production' \
        -H 'X-PAN-KEY: LUFRPTO=' \
        -d '{
        "entry": [
                {
                "@name": "web-servers-production",
                "@location": "shared",
                "fqdn": "docs.paloaltonetworks.com",
                "tag": {
                "member": [
                "blue"
        ]
        },
        "description": "what is this for?"
        }
        ]
        }'
```

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-panorama-api/get-started-with-the-pan-os-rest-api/pan-os-rest-api.html

Гибкие возможности по лицензированию:

Bring your own license (BYOL), Pay as you go (PAYG), Enterprise License Agreement (VM-ELA)

- **PAYG** – это лицензирование на основе использования и доступно на marketplace поддерживаемых облачных платформ

- **BYOL**
  - Базовая лицензия, определяющая масштабируемость VM (VM-50/100/200 и т.д.). Может быть постоянной (perpetual) или как подписка (term-based)
  - Поддержка
  - Подписки на сервисы безопасности
  - Для удобства сгруппировано в наборы (бандлы)

- **Multi-model VM-Series ELA** включает большинство моделей VM-серии вместе с подписками на сервисы GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire и поддержку. Также Вы получаете неограниченное количество экземпляров системы управления Panorama virtual appliance с лицензией на управление 1000 NGFW на каждом. Срок действия 1 или 3 года

https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/license-the-vm-series-firewall/license-typesvm-series-firewalls.html

Подробнее про Multi-model VM-Series ELA

- **Multi-model VM-Series ELA** это единый контракт, заключаемый на 1 или 3 года, включающее различные модели VM-серии вместе с подписками на сервисы GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire
- Подписка и лицензия для системы управления Panorama также включены
- Вы приобретаете количество токенов в зависимости от Ваших потребностей
- Разные VM потребляют разное количество токенов
  - VM-50—10 токенов
  - VM-100—25 токенов
  - VM-300—50 токенов
  - VM-500—140 токенов
  - VM-700—300 токенов

https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/license-the-vm-series-firewall/license-typesvm-series-firewalls/vm-series-ela.html

Защита IoT

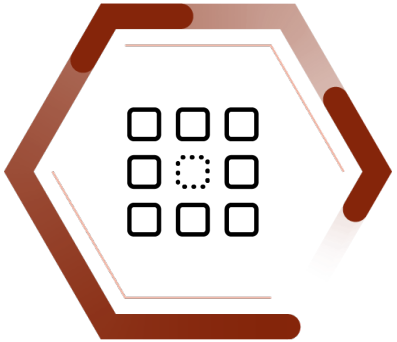
IoT необходимы для бизнеса, но использование рискованно

Взрывной рост подключенных IoT-устройств

30% всех устройств в корпоративной сети сегодня это IoT

Представляют большой риск для безопасности

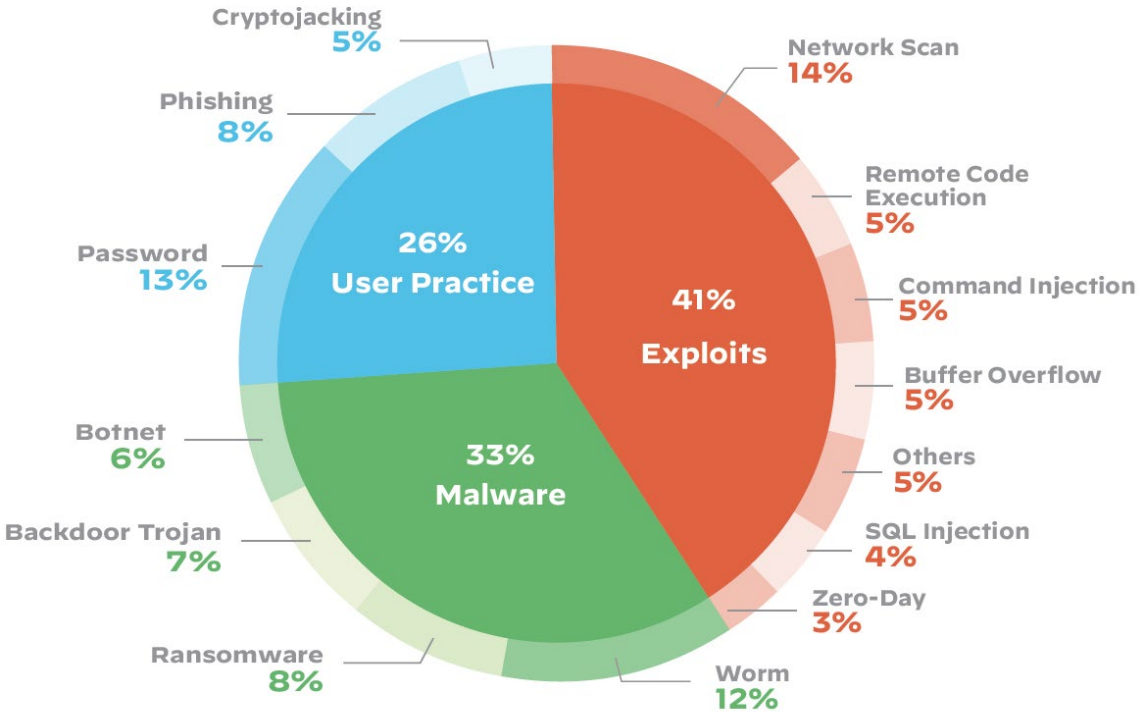
Поставляются с уязвимостями на борту, трудно или не возможно обновлять и часто имеют не ограниченный доступ к сети



Защита IoT сложная задача

Невероятное разнообразие устройств. Традиционные системы не подходят

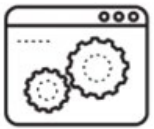
Unit 42 IoT Threat Report: актуальные угрозы для IoT-устройств



Почему IoT это идеальная точка входа?

Нет или минимальные встроенные механизмы безопасности

Уязвимости интерфейса браузера



Устаревшие ОС без обновлений

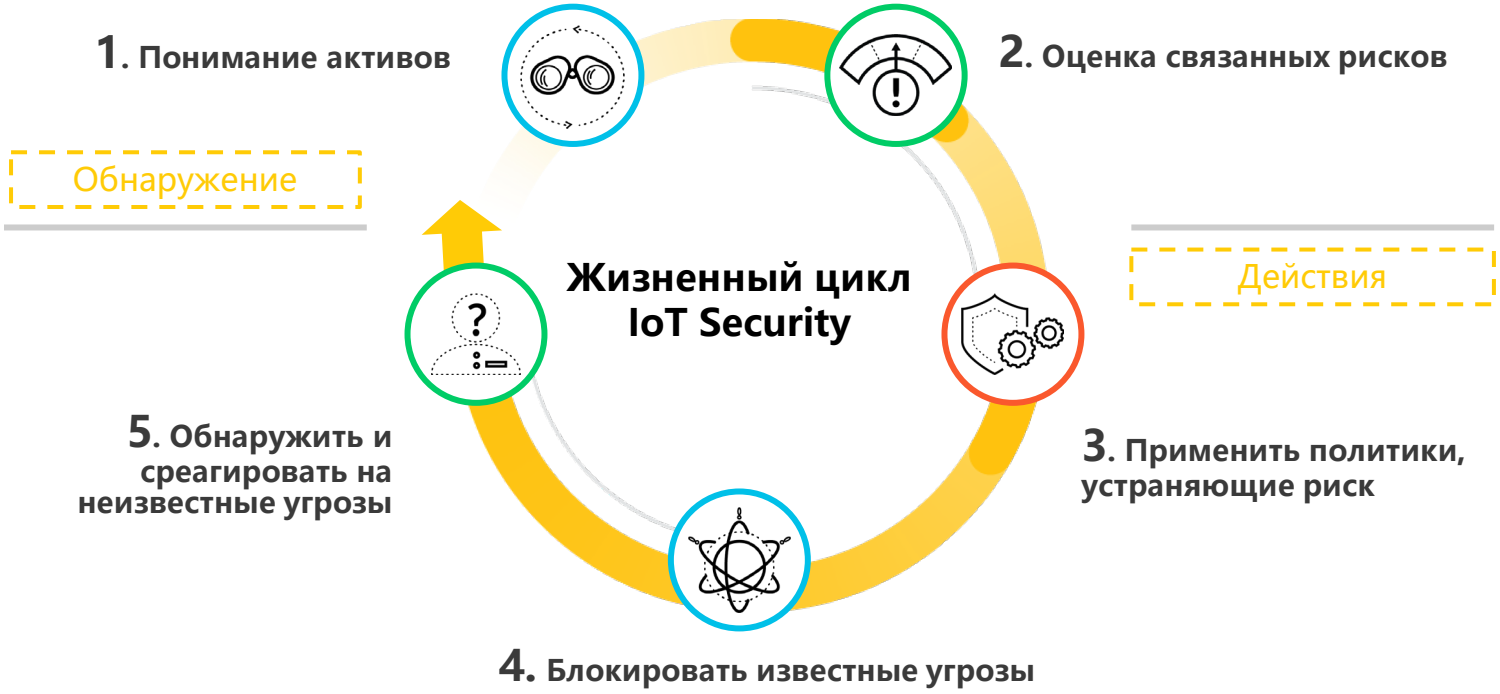
Проблемы с реализаций лучших практик

75% компаний говорят, что безопасность IoT имеет высокий приоритет для них, однако только 16% чувствуют себя подготовленными к этому

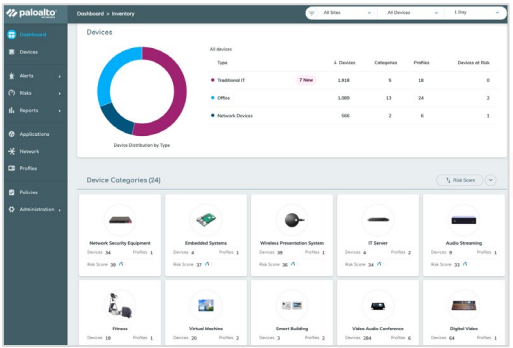
McKinsey

Источник: Digital McKinsey and Global Risk Practice, март 2019: Perspectives on transforming cybersecurity

Подход для защиты IoT-устройств или От IoT-устройств ☺

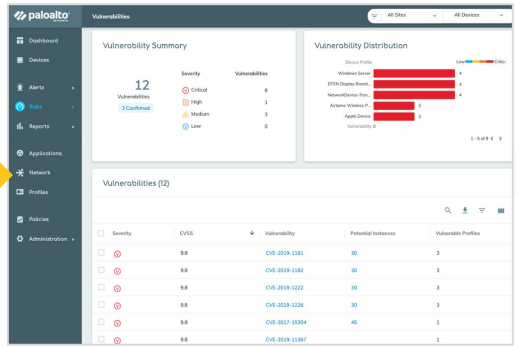


Представляем решение для защиты IoT



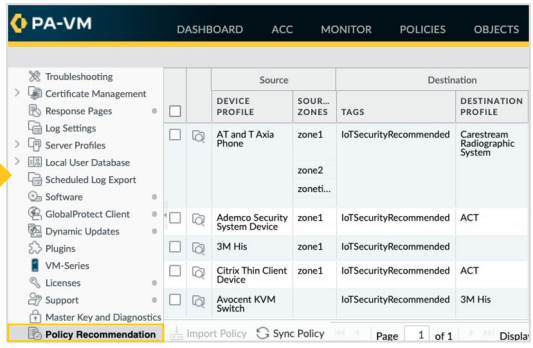
Исчерпывающая визуализация

Точная идентификация и классификация всех IoT-устройств используя алгоритмы машинного обучения включая те, которые Вы раньше не находили. Без сигнатур



Глубинный анализ рисков

Быстрое обнаружение аномалий, уязвимостей и степени риска для обдуманных решений



Интеграция с системами защиты

Автоматическое применение политик безопасности на NGFW используя новые конструкции Device-ID

Защита каждого устройства в Вашей сети

Используйте инфраструктуру

Развертывание за минуты без обособленных сенсоров или выделенного оборудования

Задействуйте обученный персонал

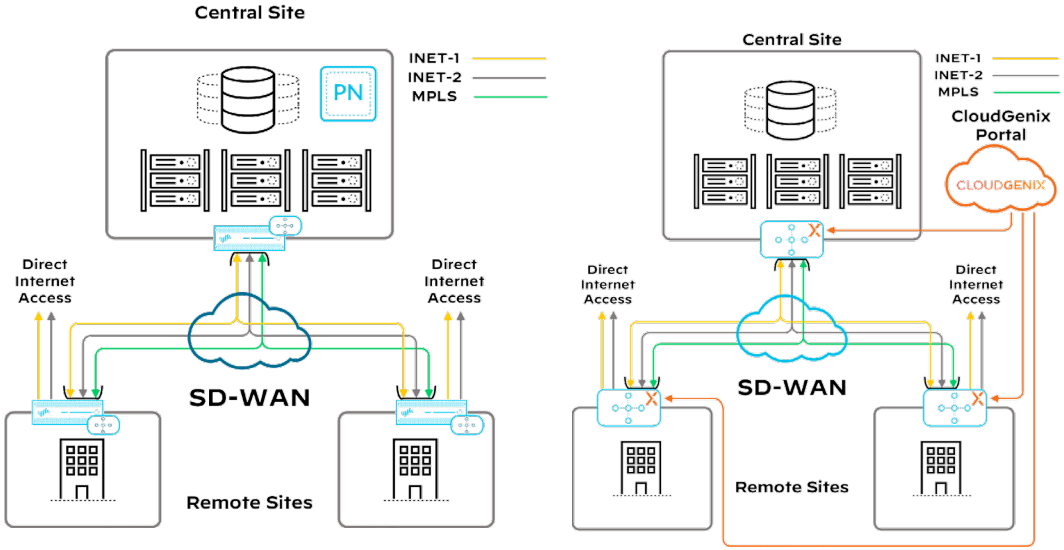
Продолжайте текущую эксплуатацию и задействуйте персонал уже обученный управлять NGFW для защиты IoT

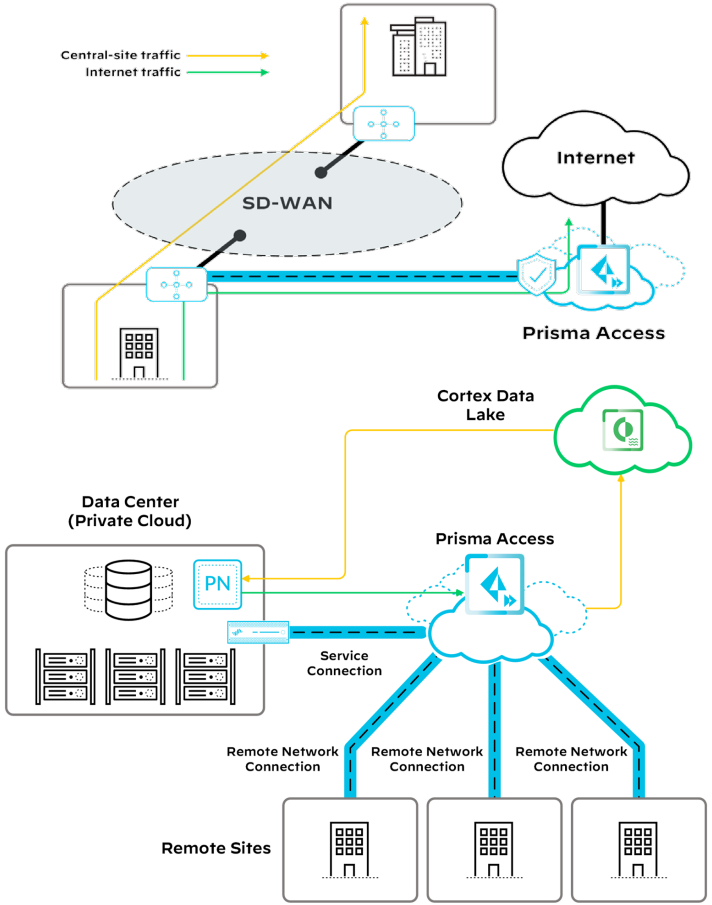
Всесторонняя защита IoT

Обнаружение, детектирование и предотвращение угроз к/от IoT-устройств в рамках единой платформы

SD-WAN

Дизайн под множество задач и сценариев

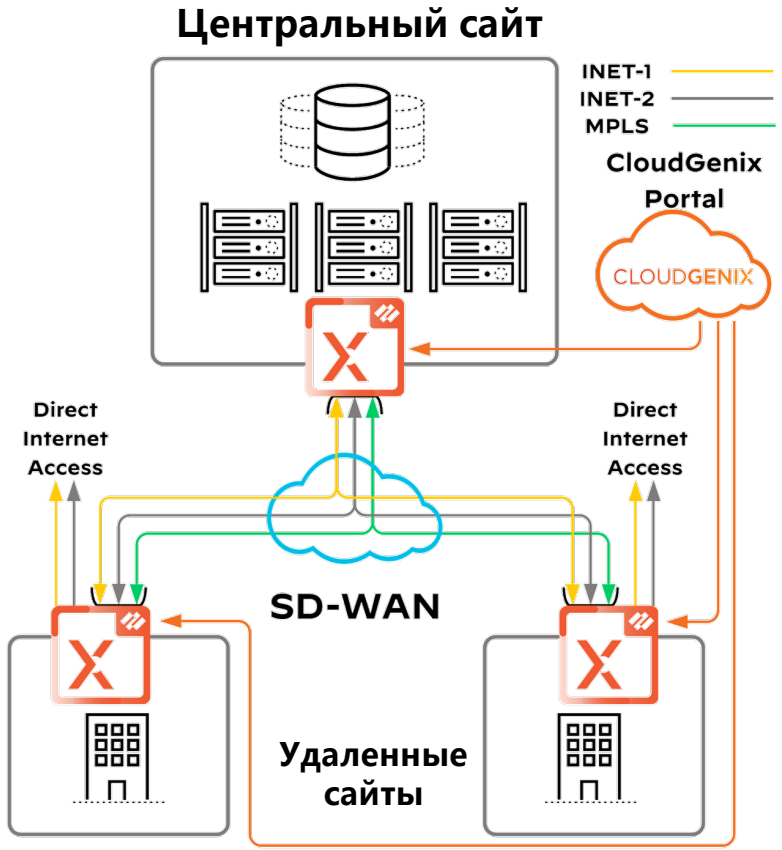




CLOUDGENIX NG SD-WAN

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

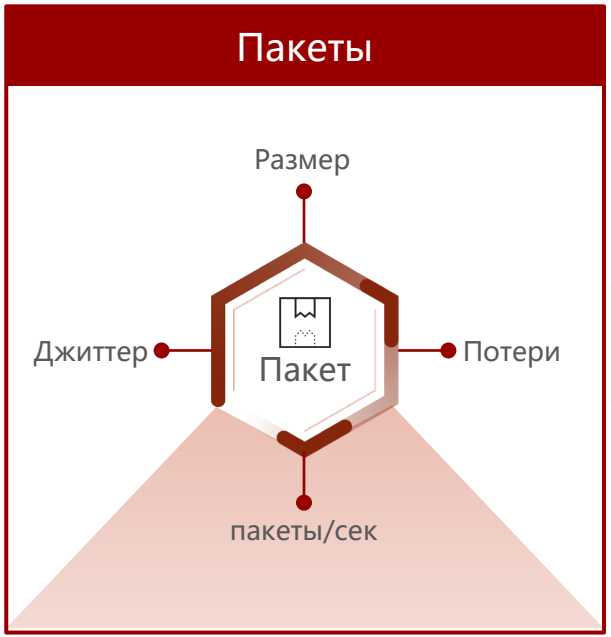
CLOUDGENIX

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

- The vendor has one of the highest customer experience ratings of any vendor in this research.
- Palo Alto Networks has one of the best visualization capabilities, compared with other vendors in this research.

paloalto NETWORKS

Реальный фокус на приложениях: сценарий для сети и безопасности

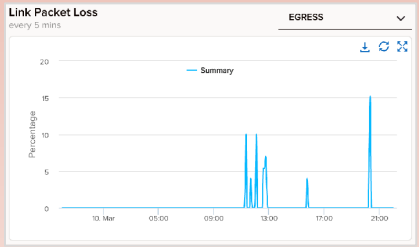


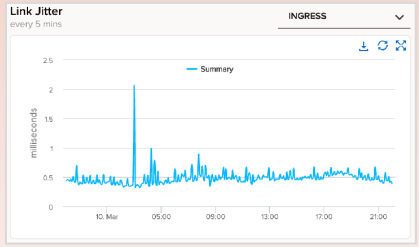
SD-WAN 1-го поколения: Packet-Based, Layer 3

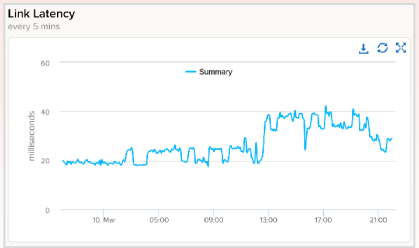
Next-Generation SD-WAN: App-Based, Layer 7

Подход L3-L7

Параметры сети: Потери, джиттер, задержка

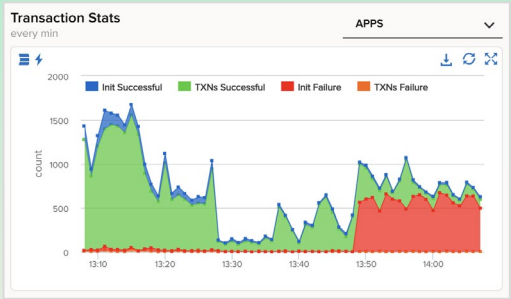




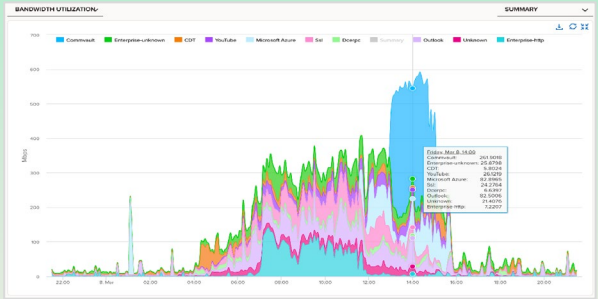


Next-Gen SD-WAN

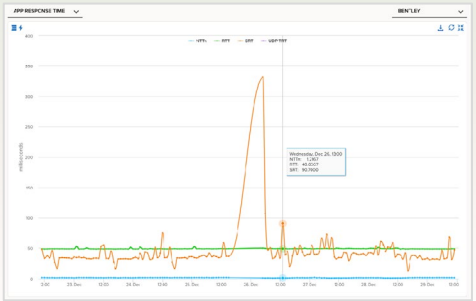
Детальная статистика по транзакциям

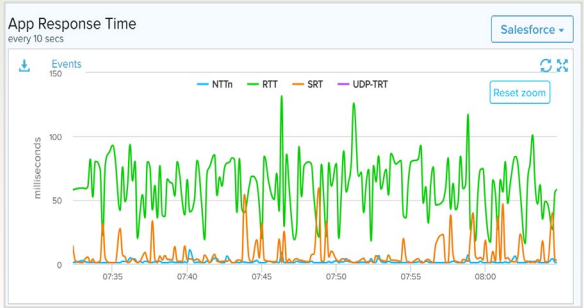


Загрузка по приложениям



Производительность и «самочувствие» приложений





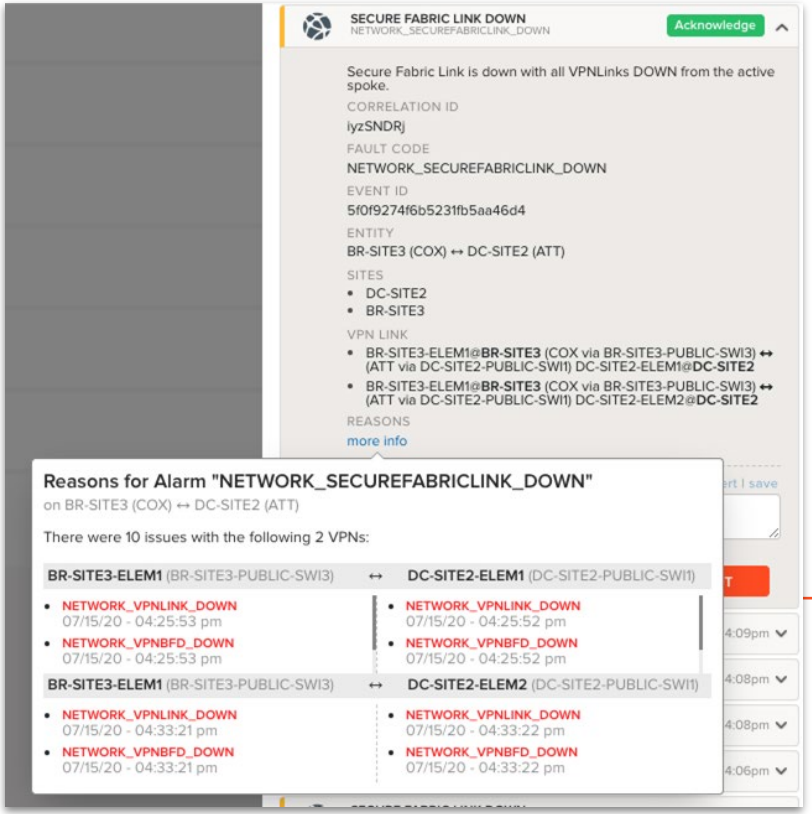
AutoNation

“Мы получили 10-ти кратный прирост производительности с CloudGenix SD-WAN за меньшие деньги, чем наше старое решение. Мы ожидаем сэкономить $3 млн. на оплате WAN в следующем году”

Adam Rasner
VP Technology Operations

paloalto NETWORKS

Автоматизируйте эксплуатацию используя корреляцию событий



Проблема
Админы вынуждены вручную коррелировать алерты для поиска корневой причины сбоя/проблемы

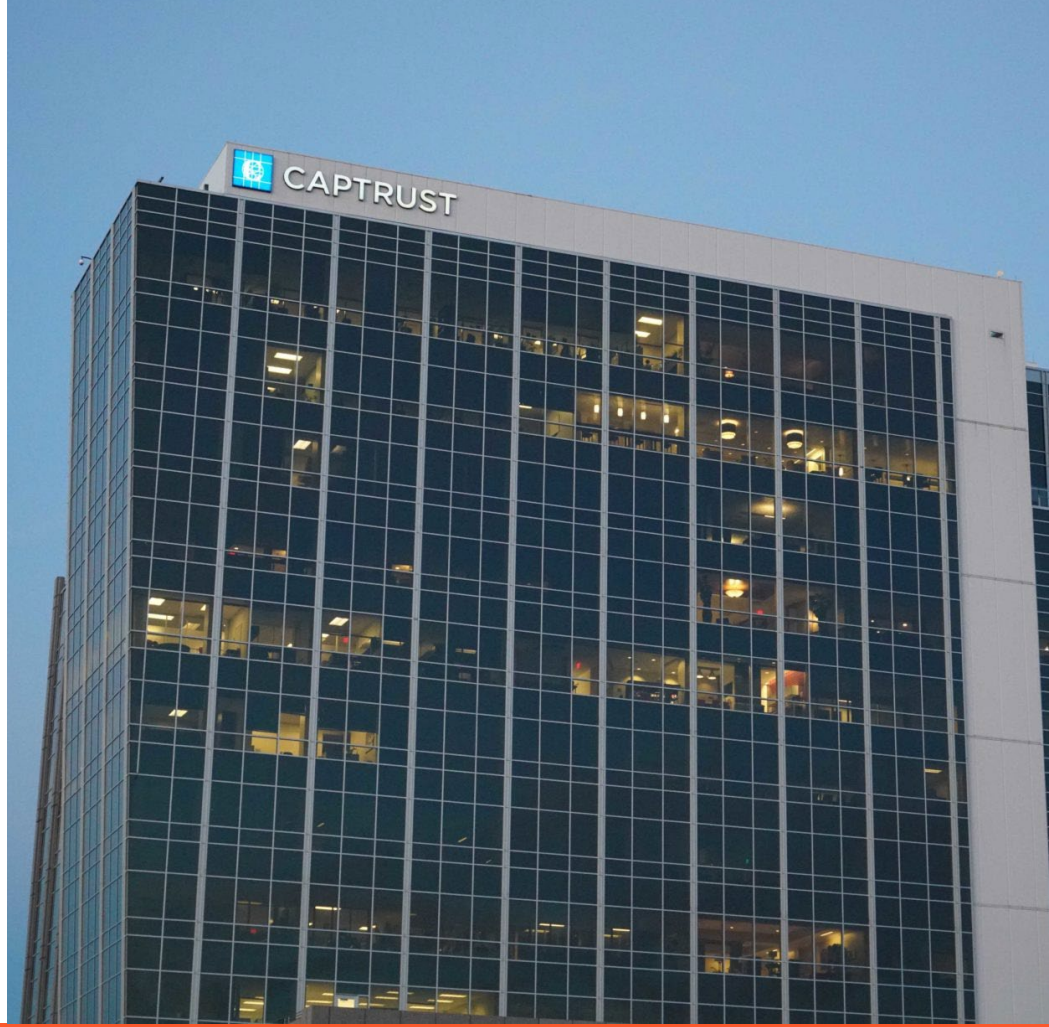
Автономный SD-WAN
Автоматизирует агрегацию событий, использует алгоритмы ML и определяет корневую причину проблемы

10 VPN сообщений скоррелированы в 1, указана корневая причина

CAPTRUST

“С CloudGenix SD-WAN мы снизили число заявок о проблемах на 99%”

John Meyer
Chief Technology Officer

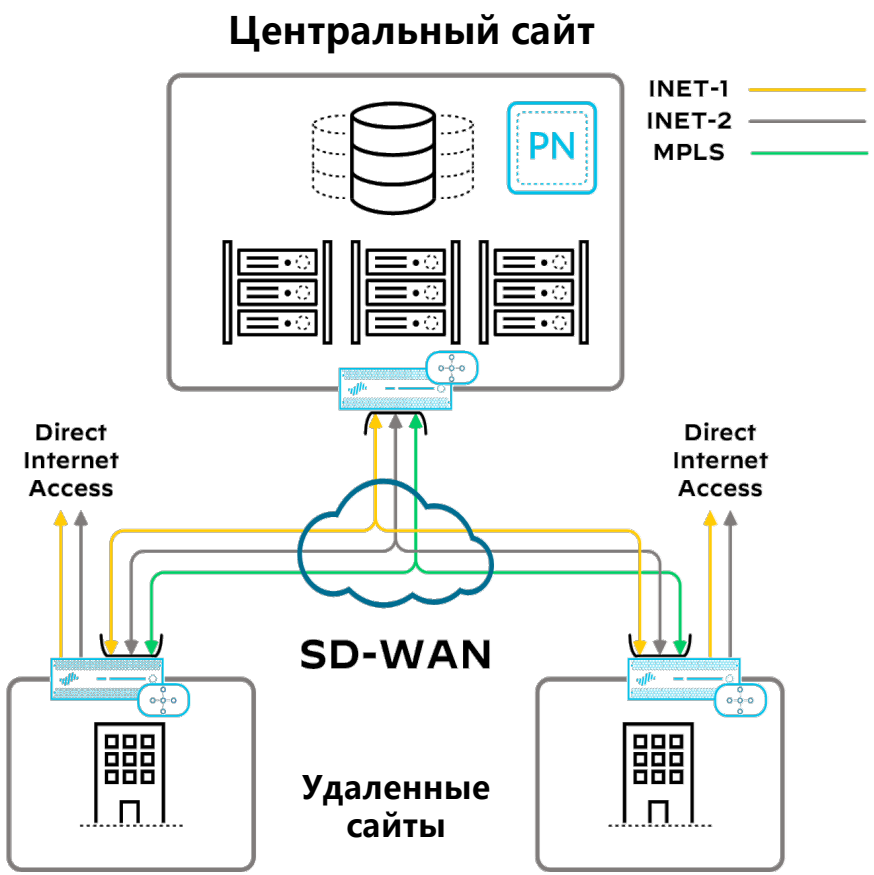


Palo Alto Networks OS Secure SD-WAN

Secure SD-WAN измеряет и отслеживает все WAN-каналы и динамически выбирает путь обеспечивая оптимальную загрузку каналов и наилучшую производительность приложений.

- Функционал появился в PAN-OS v.9.1
- Полностью интегрированные безопасность и SD-WAN
- Включается лицензией на аппаратных NGFW и VM-серии
- Централизованное управление из Panorama обеспечивает преимущества полного функционала NGFW Palo Alto Networks

tiny.cc/panw-sdwan – Вебинар о техн.подробностях



Обзор Palo Alto Networks Secure SD-WAN

Сервисы и качество безопасности от лидера рынка

- Функционал SD-WAN в зарекомендовавших себя NGFW
- Качество детекта приложений App-ID и сервисы безопасности не имеющие аналогов

Поддержка топологий и функции

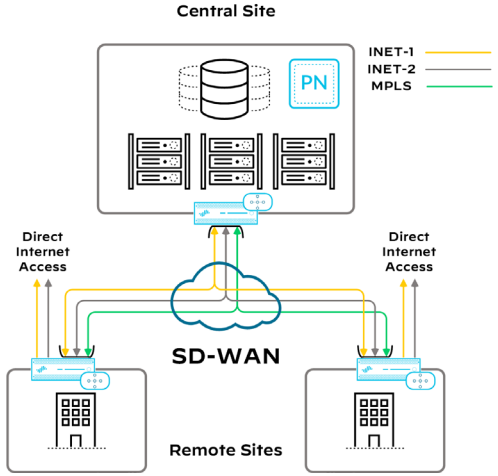
- Hub Spoke и Full Mesh (v.10.0.3)
- Динамическая маршрутизация с eBGP, опционально статическая маршрутизация (IPv4)
- QoS, Path SLA, алгоритмы распределения трафика, тегирование линков, Virtual Interface

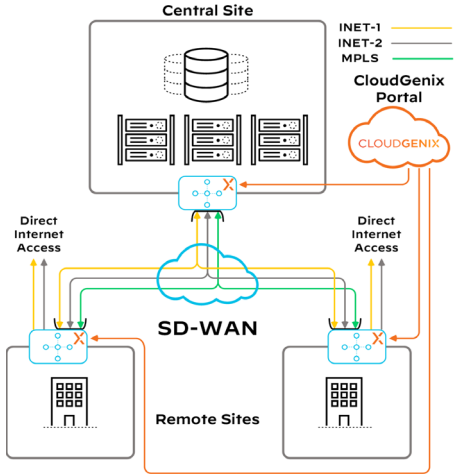
Система Panorama для централизованного развертывания, управления и мониторинга

- Поддержка ZTP
- Auto-VPN для быстрого построения топологий

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.

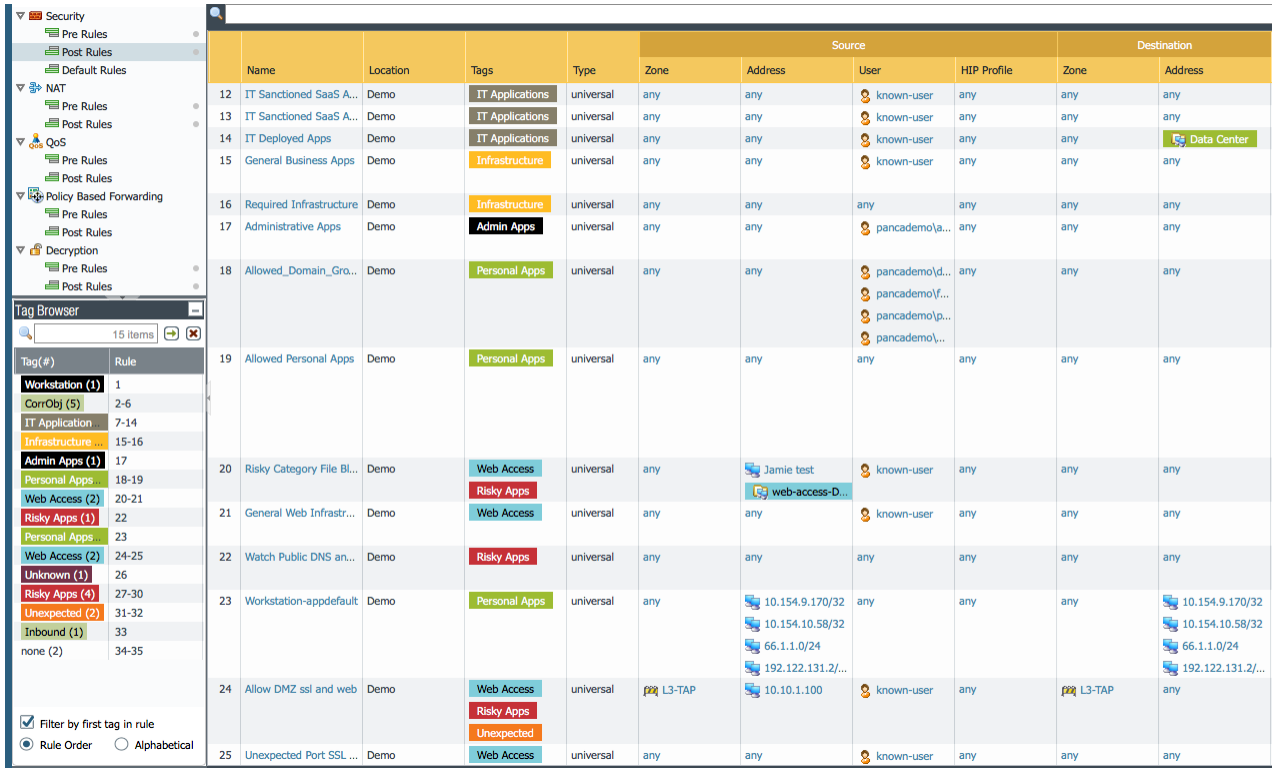




Также читайте:
https://blog.paloaltonetworks.com/2020/04/network-cloudgenix/

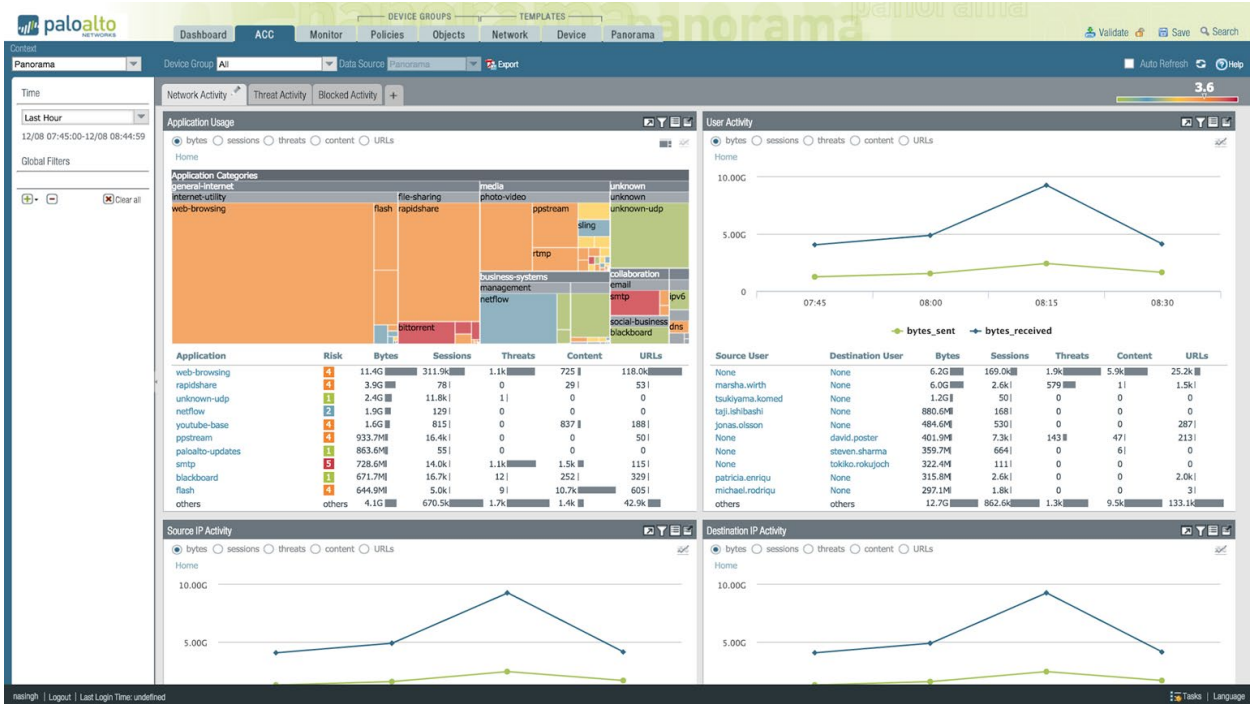
Централизованное управление с Panorama

Централизованное управление из Panorama



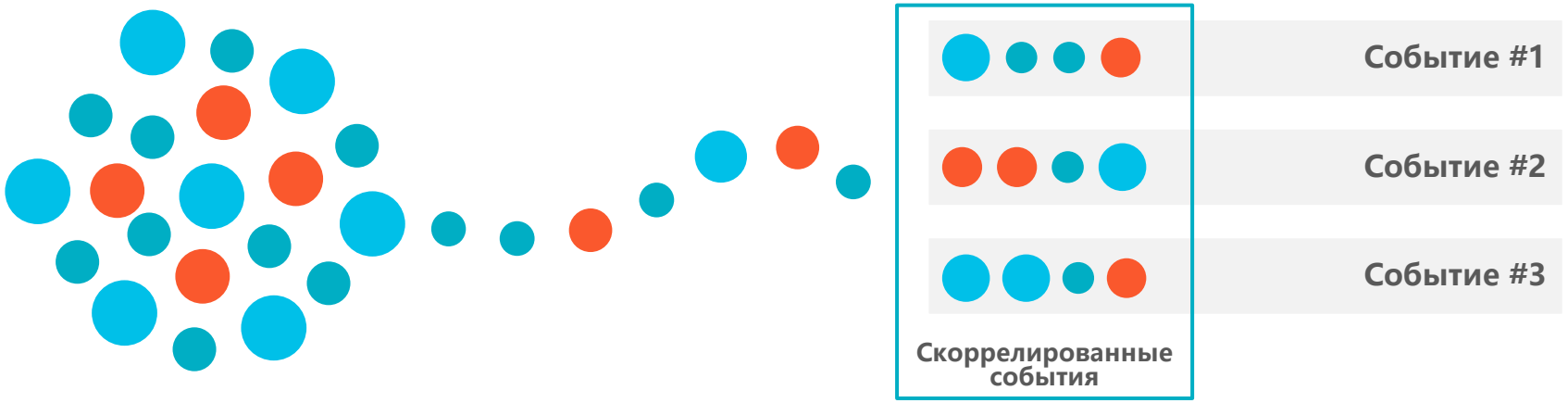
- Унифицированный интуитивный интерфейс
- Интерактивность и визуализация
- Простота

Подробные данные о происходящем в сети



- Визуализация
- Интерактивность
- Настройка под собственные нужды

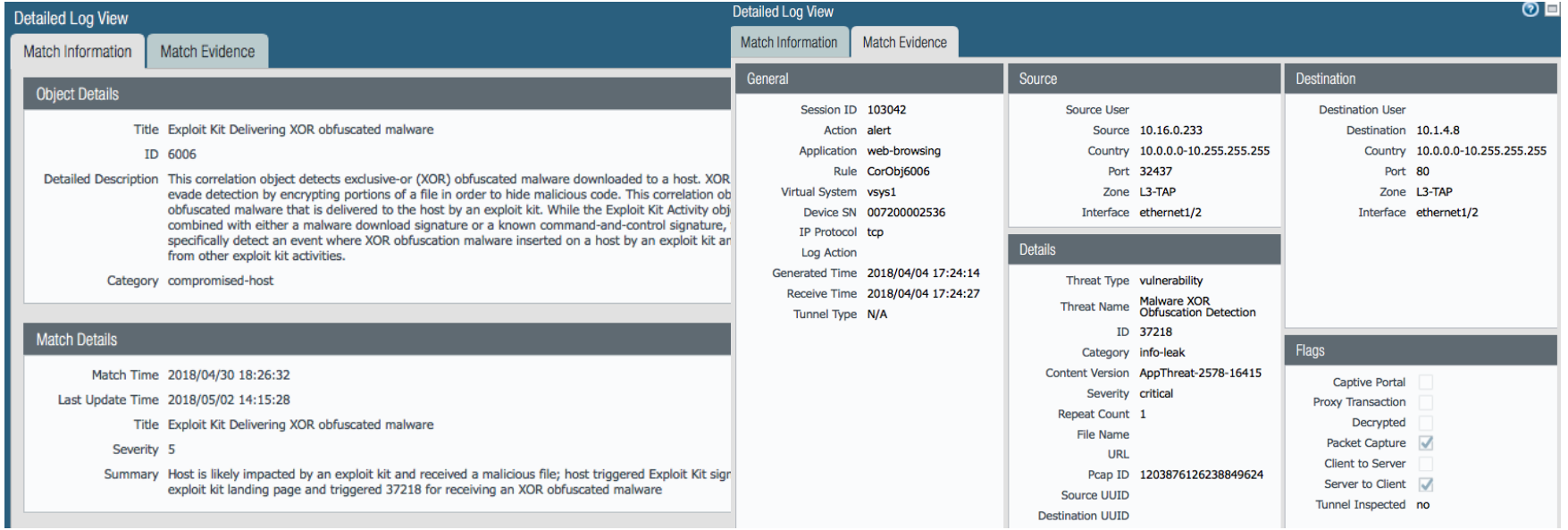
Корреляция событий для обнаружения угроз



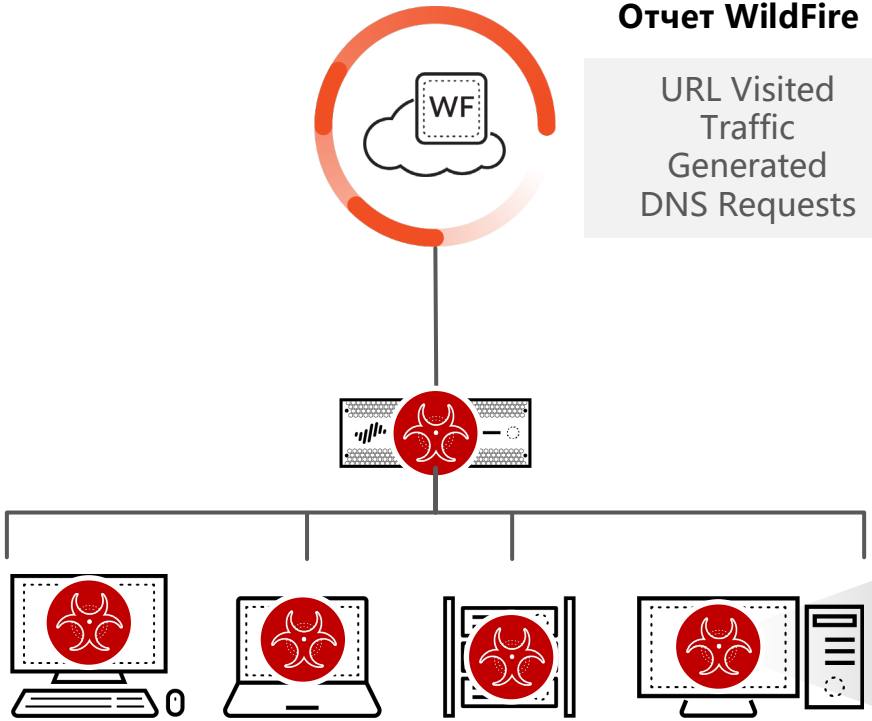
- Скоррелированные события позволяют находить сложные атаки
- Обнаружение скомпрометированных узлов через корреляцию индикаторов компрометации
- Требуется меньше ручной работы по сопоставлению данных

Пример корреляции объектов и событий

Title	Exploit Kit Delivering XOR obfuscated malware
Category	compromised-host
State	active
Description	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the



Обнаружение зараженных узлов



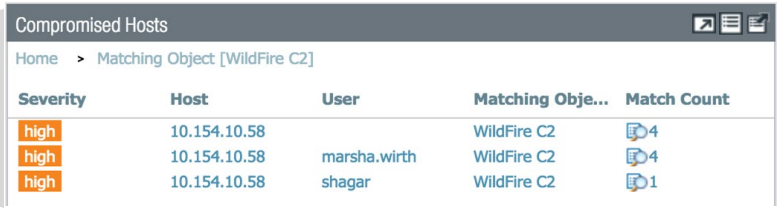
Отчет WildFire

URL Visited
Traffic
Generated
DNS Requests

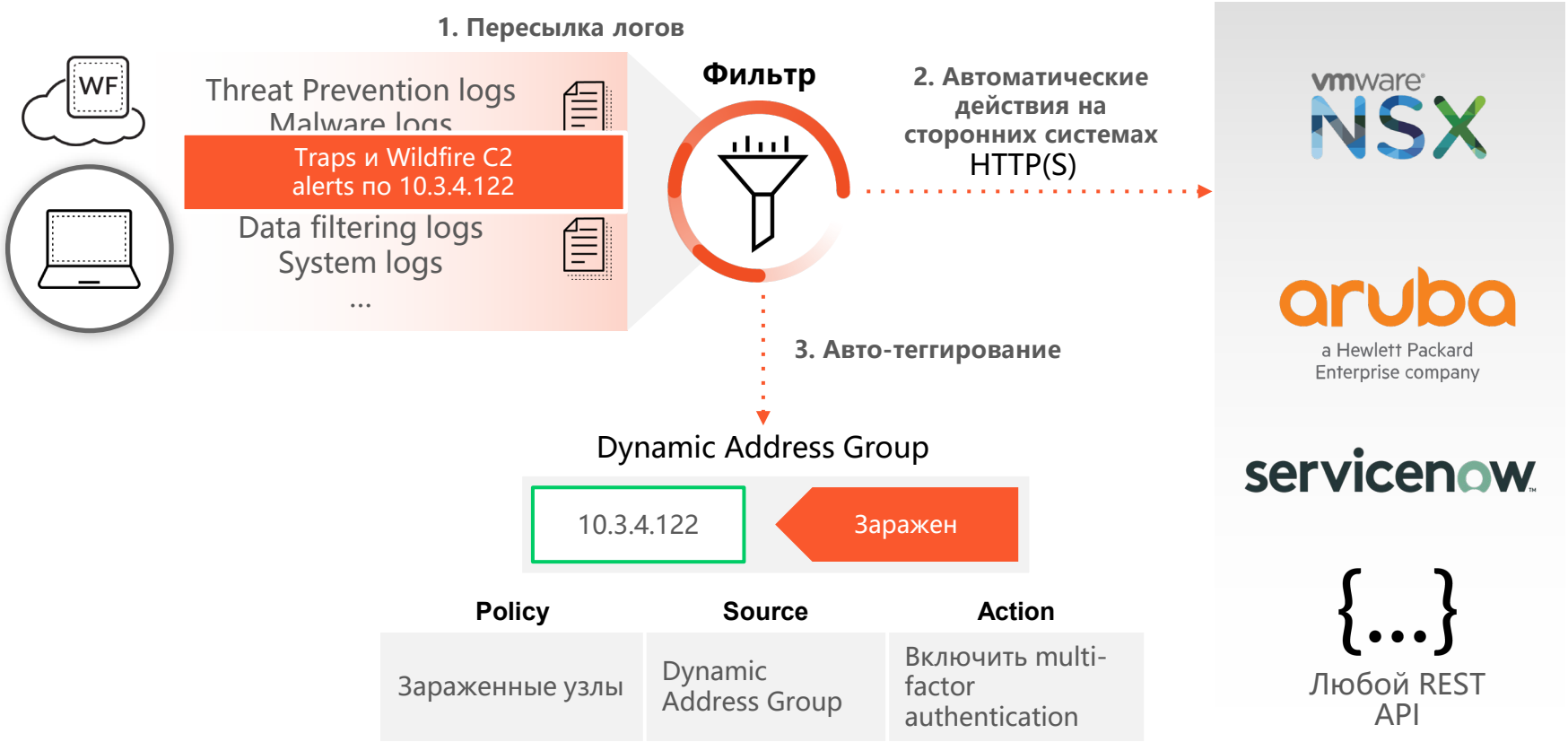
1. Пользователь загружает зараженный файл

2. Файл анализируется сервисом WildFire

3. WildFire возвращает отчет с деталями поведения кода

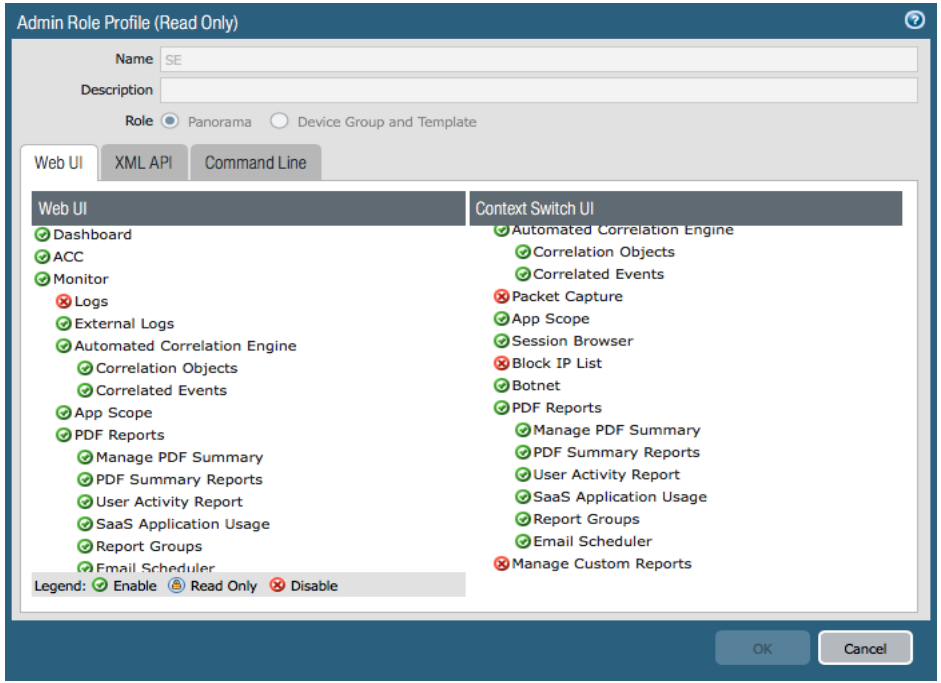


Автоматические действия



Policy	Source	Action
Зараженные узлы	Dynamic Address Group	Включить multi-factor authentication

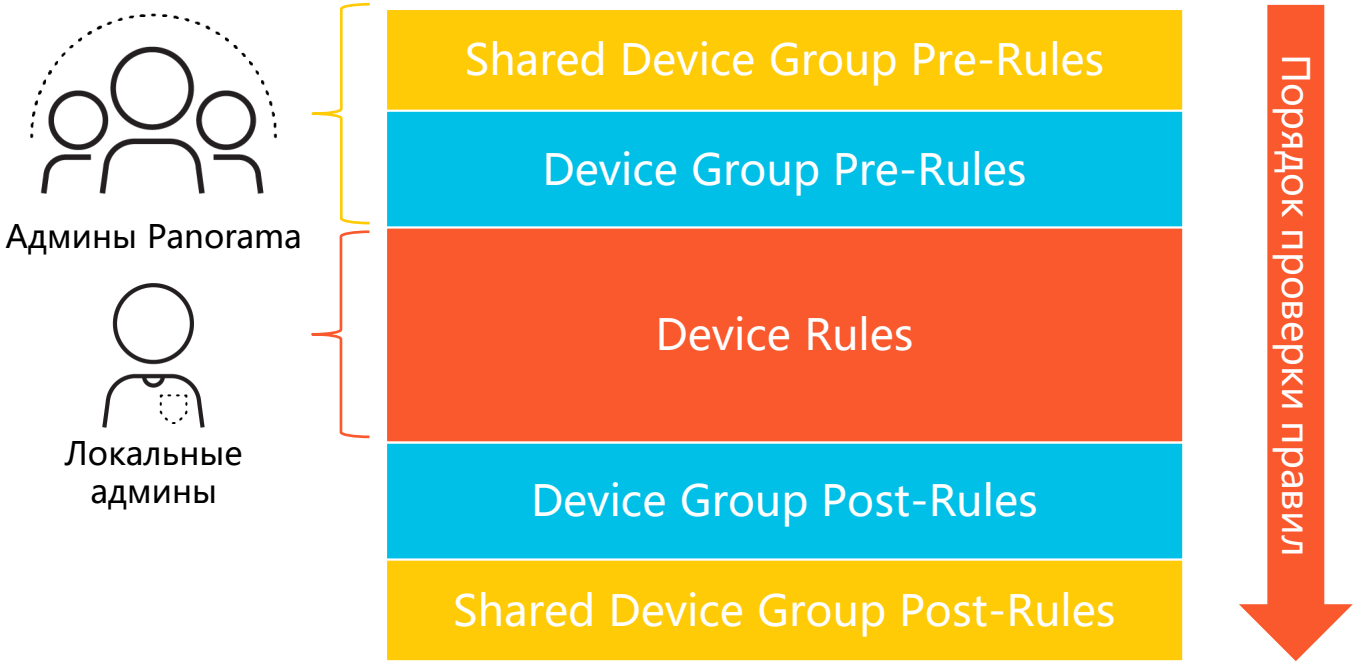
Гибкий Role-Based Access Control



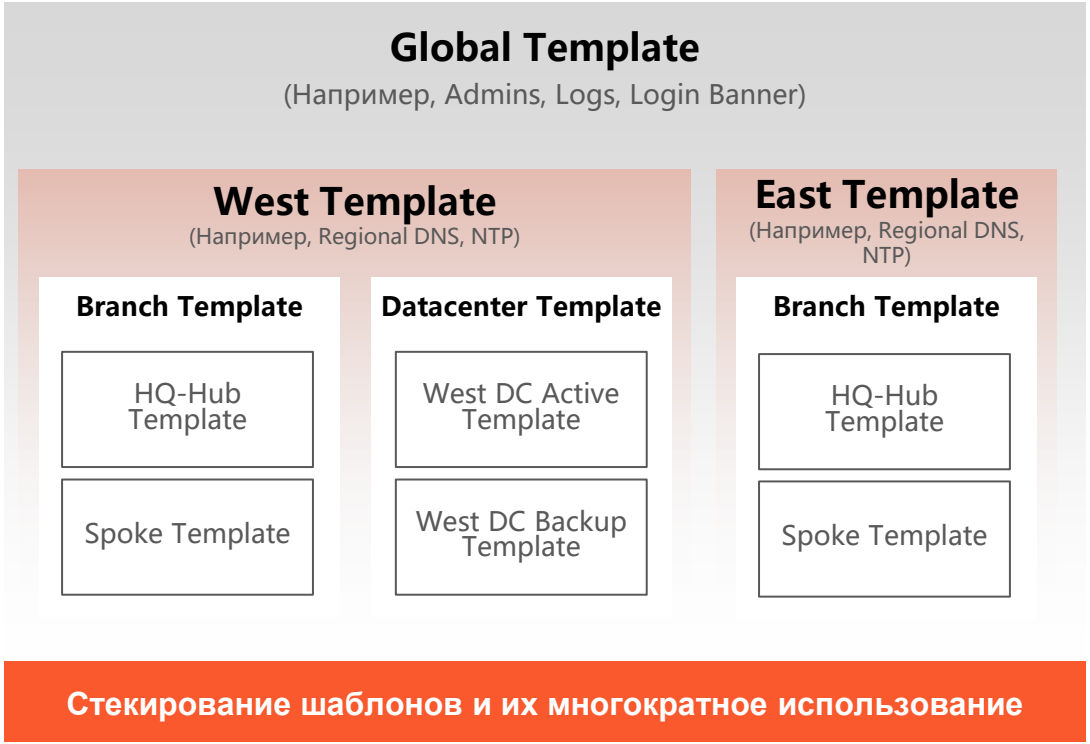
- Гибкая настройка каждой опции благодаря хорошей реализации RBAC
- Домены доступа для управления определенными устройствами
- Единообразный интерфейс NGFW и Panorama не требует переучивания персонала

Группировка правил: локальное и централизованное управление

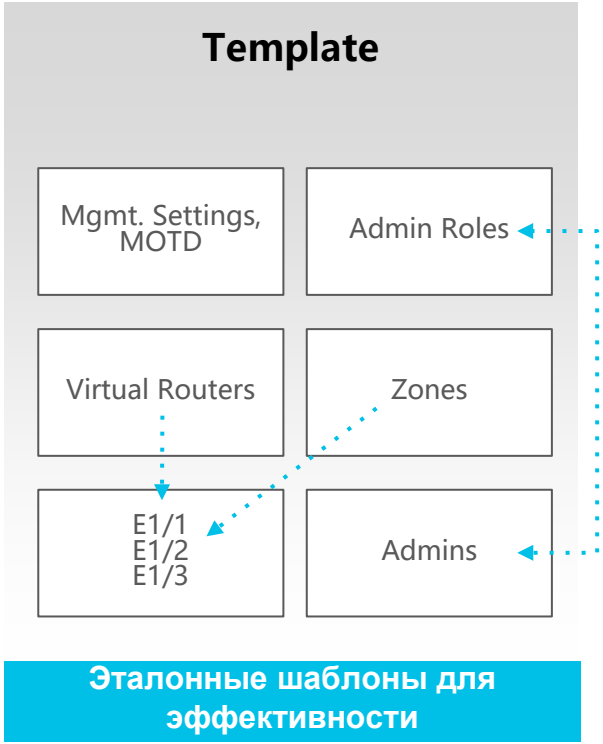
- Мощные возможности по группировке политик. Например, общая политика блокировки сервиса применяется на все NGFW, более специфичные только для групп NGFW. Это позволяет переиспользовать и иметь консистентные политики



Удобные инструменты для настройки множества NGFW



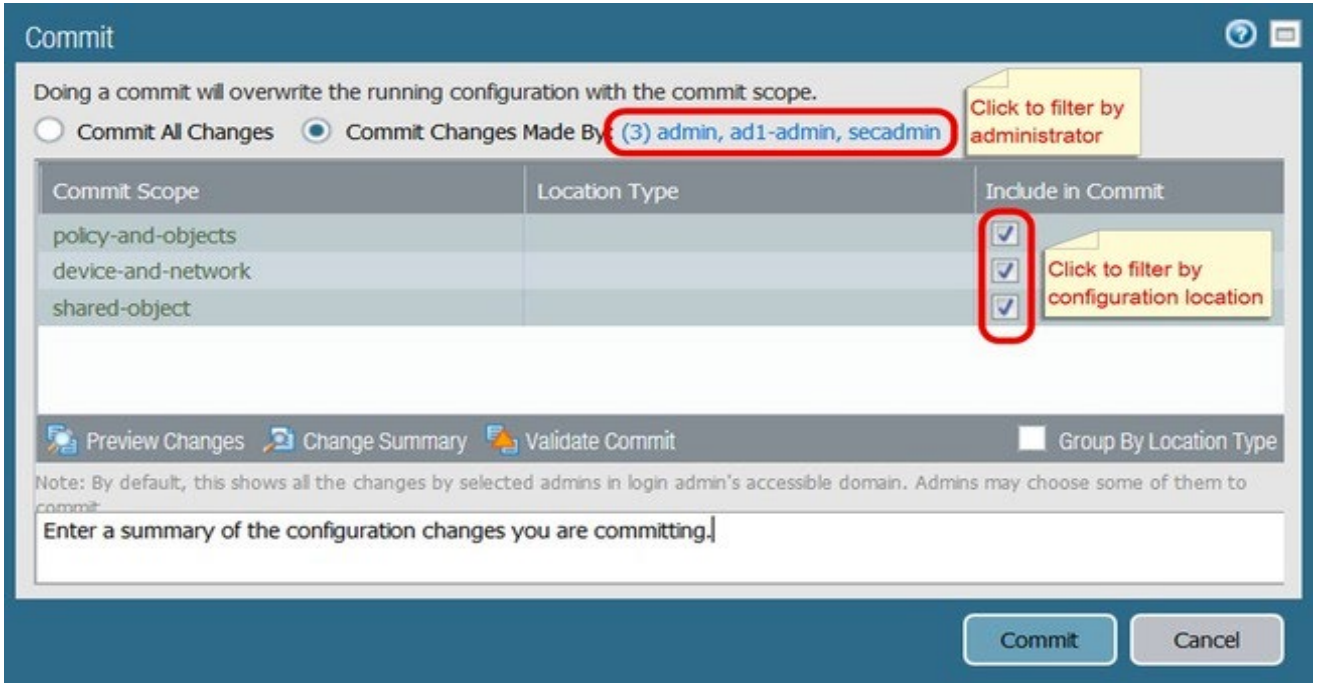
Стекирование шаблонов и их многократное использование



Эталонные шаблоны для эффективности

Commit только того, что требуется

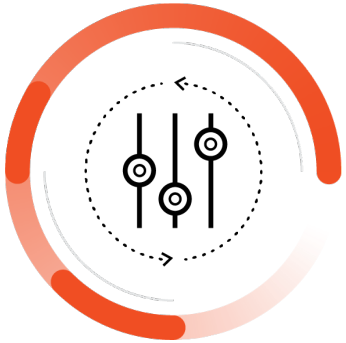
- Множество вариантов по применению разных политик к разным устройствам/группам



Различные режимы работы и форм-факторы

Panorama

Управляет NGFW и собирает логи, коррелирует данные, визуализирует



Только управление

Управляет NGFW

Log Collector

Сбор логов, корреляция данных, визуализация

Доступно в форм-факторах аппаратных и виртуальных комплексов

Prisma Cloud Compute Edition

защита контейнеров, хостов, бессерверных вычислений

paloalto NETWORKS

Prisma Cloud

Защищает большинство облачных рабочих нагрузок приложений

70%
списка Fortune 100
используют Prisma Cloud

1800+
заказчиков доверяют Prisma Cloud

1M+
рабочих нагрузок защищено

1.8млрд+
ресурсов отслеживается

5млрд+
логов аудита обрабатывается еженедельно

~200TB
логов о трафике обрабатывается еженедельно

Prisma Cloud

Заказчики по всему миру доверяют нам в защите их инфраструктур

ФИНАНСОВЫЙ СЕКТОР	PayPal, citi, TIAA, DISCOVER, USAA
ВЫСОКИЕ ТЕХНОЛОГИИ	cisco, aws, BROADCOM, DELL EMC, IBM
ЗДРАВООХРАНЕНИЕ	aetna, CENTENE Corporation, OPTUM, McKESSON, Anthem
МЕДИА И РИТЕЙЛ	Disney, Starbucks, Carnival, Red Bull, sky, Nike
ГОСУДАРСТВЕННЫЕ ОРГАНЫ	NASA, U.S. Department of Homeland Security, GSA, U.S. Army, U.S. Air Force, CDC, NIH
ПРОИЗВОДСТВО И ТЕЛЕКОМ	Charter, ExxonMobil, MAERSK, verizon, AT&T, Honeywell

Prisma Cloud

Oracle: кейсы
О чем думает бизнес
Интернет вещей
Умные города
Корпоративная мобильность
NetApp: новое в СХД
Безопасность
Цифровая трансформация
ИТ в госсекторе
ИТ в банках
ИТ в торговле
Телеком
Интернет
ИТ-бизнес

Росбанк повысил защиту инфраструктуры приложений с помощью Prisma Cloud

ИТ в банках

13.02.2020, Чт, 11:36, Мск , Текст: Владимир Бахур

Росбанк совместно с «Инфосистемы джет» реализовал первый в России проект по внедрению платформы Prisma Cloud для защиты инфраструктуры приложений. С помощью нее кредитная организация уже обеспечивает безопасность двух приложений дистанционного банковского обслуживания и планирует масштабировать решение на новые разработки.

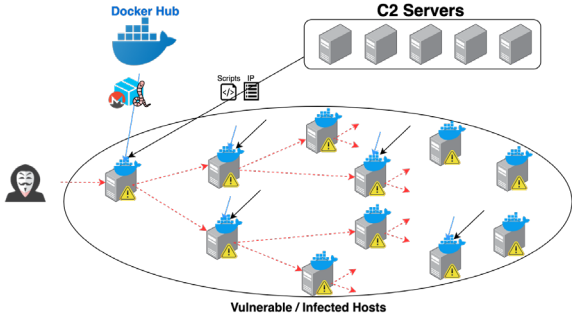
Автоматизация функций безопасности позволяет Росбанку повысить качество сервисов с минимальным влиянием на скорость их выпуска — time-to-market. Для сокращения этого параметра в кредитной организации применяется широкий набор средств, которые в совокупности позволяют ускорить процесс разработки и доставки ПО конечным пользователям. Например, программисты активно взаимодействуют со специалистами по ИТ-инфраструктуре и эксплуатации решений. При этом разные команды применяют единые подходы к созданию приложений и одинаковые средства автоматизации разработки и тестирования кода. Еще одной составляющей ускорения time-to-market в Росбанке стал поэтапный переход с монолитной архитектуры приложений на микросервисную: для этого кредитная организация использует контейнерные среды на базе платформы управления контейнерами OpenShift.

paloalto NETWORKS

Новые технологии – новые векторы атак

- В июне 2018 года 17 контейнеров с вредоносным кодом были удалены с портала Docker Hub, но до этого, в течение нескольких месяцев, их успели загрузить более миллиона раз
- В сентябре 2018 года на GitHub был опубликован пример атаки на установочные пакеты Python,в ходе которой файл setup.py модифицировался для запуска вредоносного кода при установке пакета. Поскольку, как правило, этот файл используется только для добавления модуля его содержимое мало кто проверяет
- CVE-2019-5736 от февраля 2019 года. Уязвимость позволяет вредоносному контейнеру (с минимальным взаимодействием с пользователем) переписать хостовый бинарник runc и таким образом получить возможность исполнения кода с правами root на хосте

Еще примеры угроз ИБ при использовании контейнеров



- **Graboid**. Октябрь 2019. Unit 42 заявил об обнаружении червя для криптоджекинга в образах контейнерах Docker Hub, который успел распространиться на более, чем 2000 хостов Docker

- CVE-2020-1983, CVE-2020-8608 и CVE-2020-7039. Slirp & Rootless Containers. Май 2020

Severity	Package	CVE	Fix Status	Risk Factors	Description
high	slirp4netns	CVE-2020-1983	open	5	Impacted versions: * Discovered: Less than an hour ago Published: 28 days ago

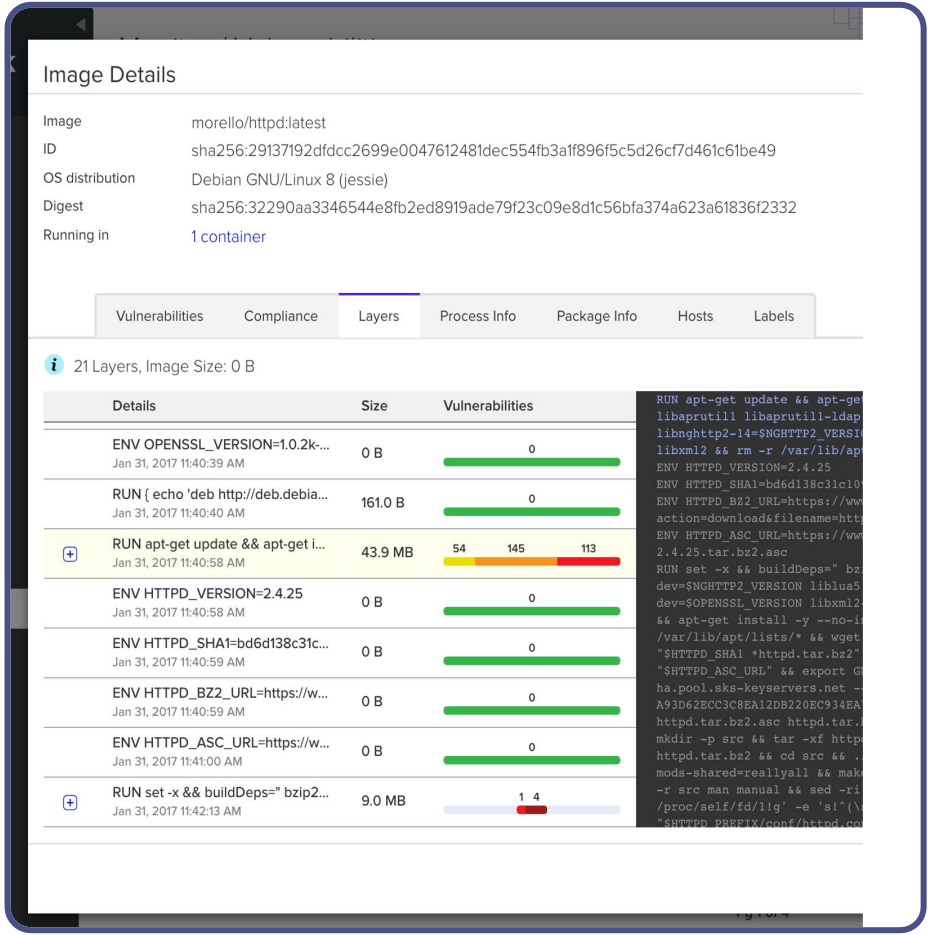
- Июнь 2020. В Docker Hub были найдены шесть вредоносных образов, содержавших скрытые майнеры криптовалюты Monero
- Декабрь 2020. CVE-2020-8554. Затрагивает все кластеры Multitenant Kubernetes. Архитектурная проблема k8s при которой атакующий перехватывает трафик чужих подов (MITM).

Сценарии воздействия угроз в среде исполнения контейнеров

- Загрузка из открытого репозитория и запуск вредоносного контейнера
- Сборка контейнера, содержащего уязвимости
- Запуск контейнеров с небезопасной конфигурацией
- Взлом контейнеров в ходе исполнения и инжектирование внутрь вредоносного кода
- Загрузка из репозитория или взлом и запуск контейнера под контролем атакующего
- Взлом контейнера с последующим заражением других контейнеров сервиса
- Получение неавторизованного доступа к сервису извне
- Эксплуатация уязвимостей веб-сервиса на базе контейнеров

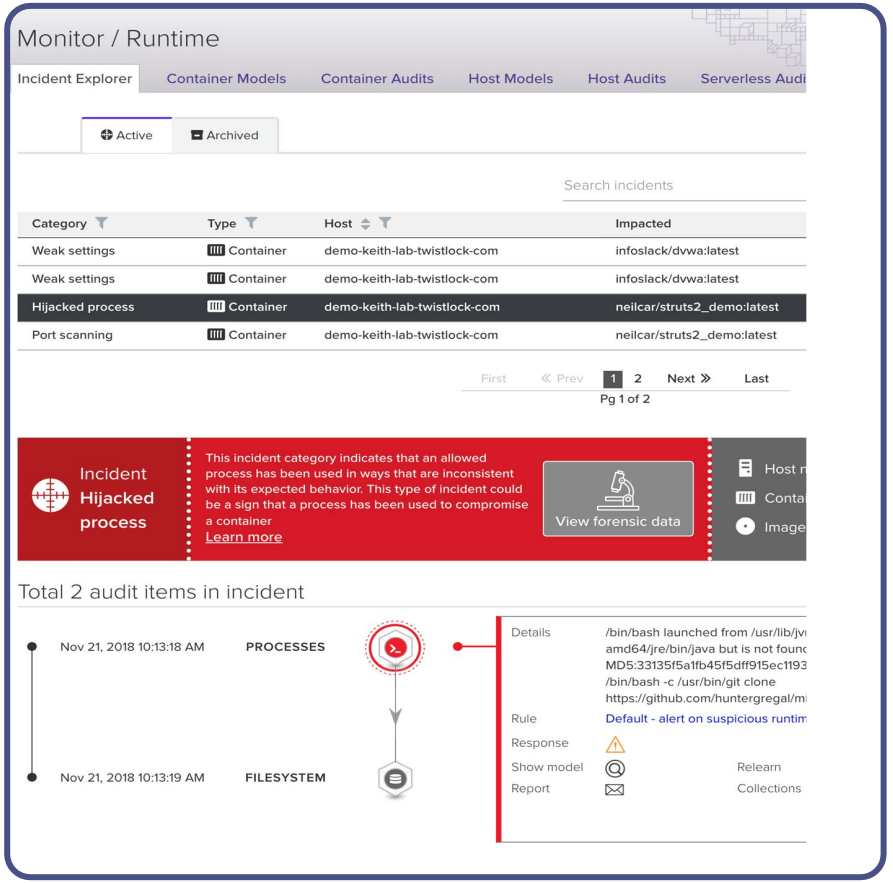
Что делает Prisma Cloud – Защита

- Проверка хостов, образов, контейнеров, бессерверных функций
- Приоритезация уязвимостей в зависимости от вашей инфраструктуры
- Запрет запуска уязвимого софта в Вашей среде
- Запрет запуска недоверенных образов
- Контроль исполнения команд



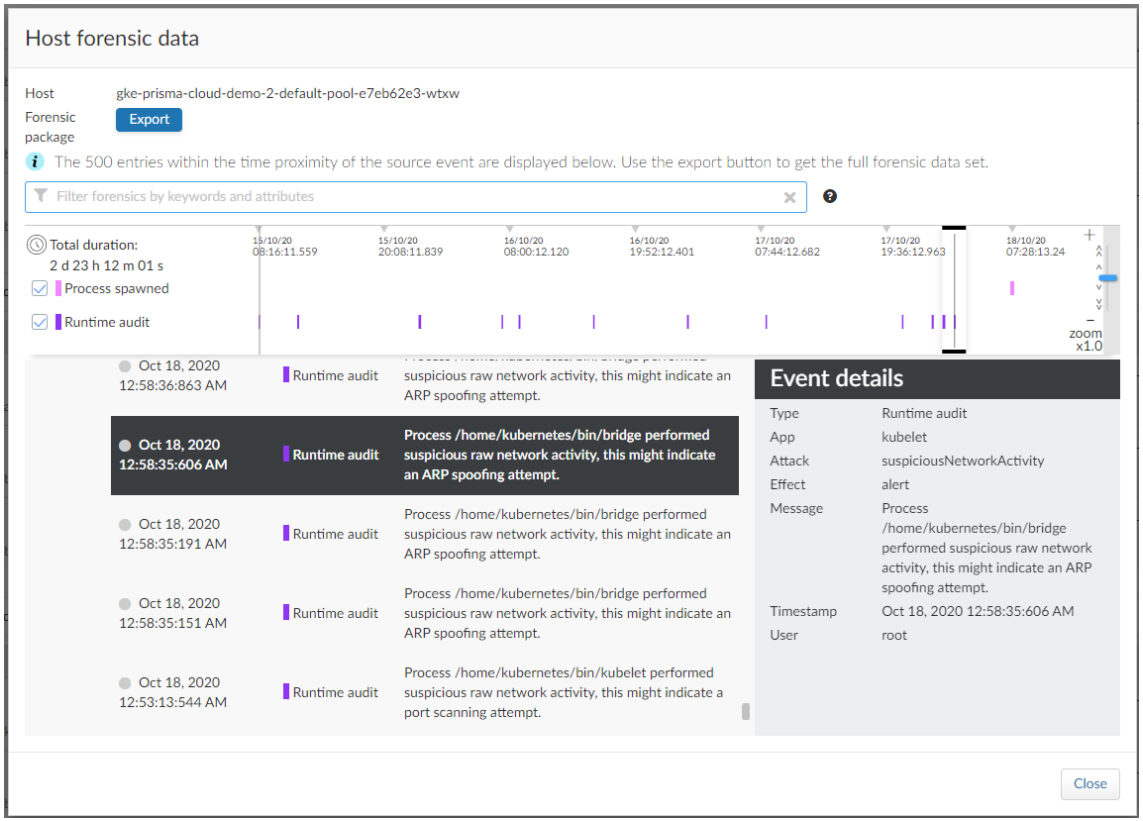
Автоматизация для защиты

- Автоматическое определение нормального поведения для каждого контейнера
- Анализ файлов конфигураций, образов, поведения и корреляция
- Автоматическое обнаружение и блокирование инцидента на базе построенной модели взаимодействия и поведения
- Сбор важной информации для разбора инцидентов на каждом хосте и контейнере



Расследование инцидентов

Подробный лог событий по каждому инциденту

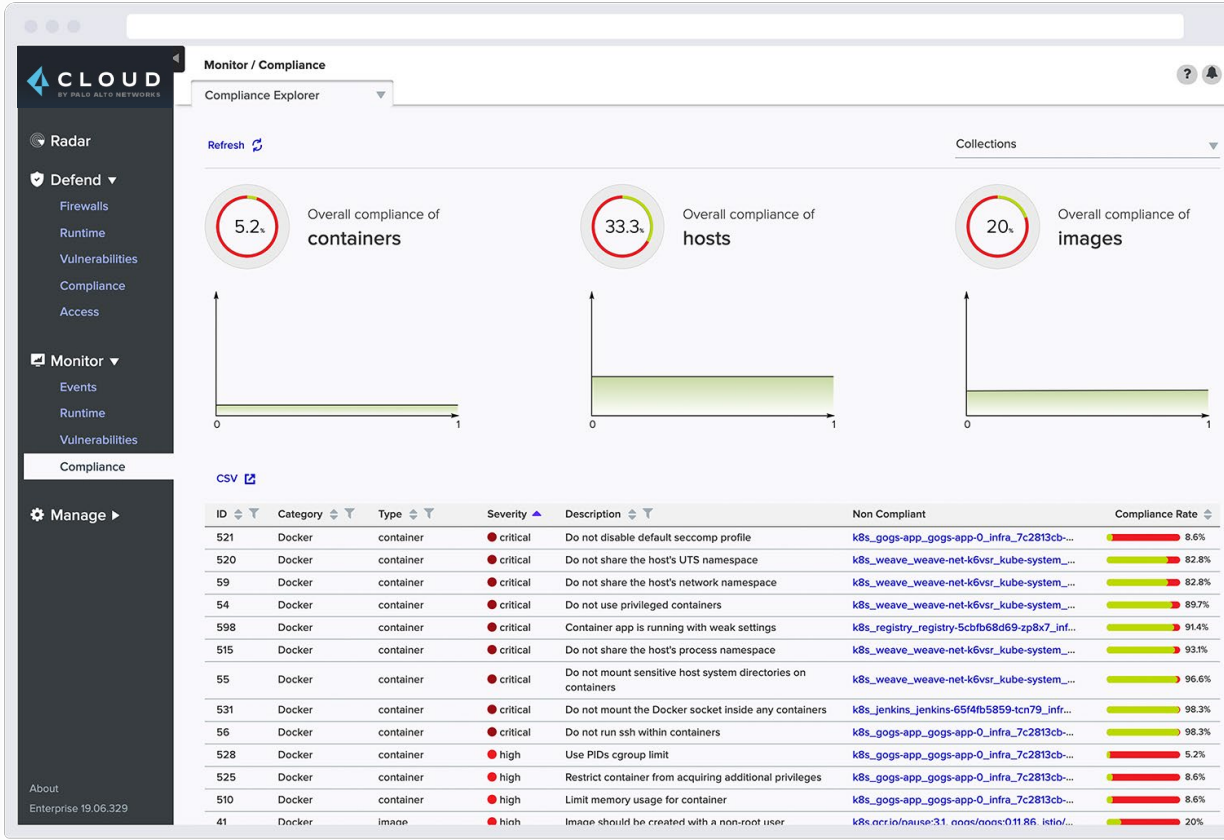


Проблемы в средах исполнения контейнеров

- Запуск контейнеров с небезопасной конфигурацией
- Большое количество сущностей – контейнеров – трудно за всем уследить
- Постоянно изменяющаяся среда
- Несколько разных сред исполнения: частные и публичные облака
- Необходимы стартовые безопасные конфигурации и лучшие практики, применение должно быть автоматическим

Что делает Prisma Cloud – Compliance Check

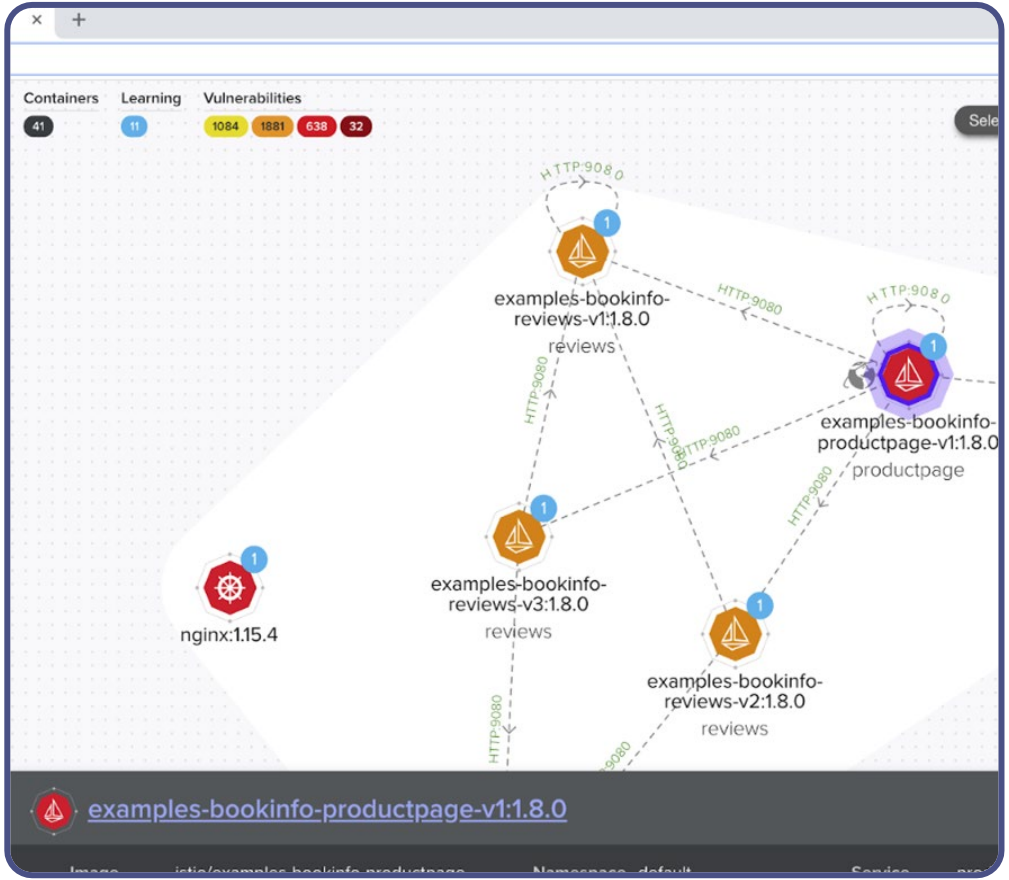
- Проверка на соответствие HIPAA, FISMA, PCI, GDPR
- Проверка на Best Practice Compliance для контейнеров
- CIS Benchmarks
- 400+ проверок из коробки
- Создание собственных проверок
- Пример: старт image с паролем по умолчанию, запуск как root и др.



https://blog.paloaltonetworks.com/2020/08/cloud-cis-controls/

Что делает Prisma Cloud – Визуализация

- Визуализация всех компонентов
- Автоматическое построение карты всех взаимодействий
- Встроенный Firewall L3-L7
- Автоматическое обнаружение сетевых взаимодействий и микросегментация



Два издания

ФУНКЦИИ	PRISMA CLOUD ENTERPRISE EDITION	PRISMA CLOUD COMPUTE EDITION
Интерфейс управления	Сервис в облаке Palo Alto Networks (SaaS)	Развертывания в Вашей инфраструктуре будь она локальная или облачная(self-hosted).
Модули	Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Data Security (DLP), Cloud Network Security (CNS) и Cloud Infrastructure Entitlement Management (CIEM)	Cloud Workload Protection Platform (CWPP)
Агенты	Вы развертываете и управляете	Вы развертываете и управляете
Административный доступ	Single sign-on в Prisma Cloud	Single sign-on в Prisma Cloud Compute Edition. Compute Console предоставляет доп.виды для Active Directory и интеграции с SAML
Multi-tenancy	Поддерживается в рамках Palo Alto Networks Hub	Поддерживается. Функция называется - Projects. Projects поддерживаются только в Compute Edition. Выключены в Enterprise Edition

https://www.paloaltonetworks.com/resources/guides/prisma-cloud-pricing-and-editions
https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/welcome/pcee_vs_pcce.html

CN-серия

первый полноценный NGFW для Kubernetes

paloalto NETWORKS

Проблемы при защите трафика контейнеров

- Динамичная среда, контейнеры постоянно запускаются и уничтожаются. Полагаться на IP-адреса нельзя – они динамичные и живут короткое время
- Трафик между контейнерами ходит внутри пода и снаружи не виден
- Трафик, выходящий за пределы пода имеет адрес кластера и не понятно кто его сгенерировал
- Необходима интеграция с Kubernetes, чтобы понимать какой трафик и между какими контейнерами ходит
- Необходима интеграция с Kubernetes, чтобы инспектировать трафик между контейнерами внутри пода, обнаруживать и блокировать угрозы

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

Представляем контейнерный NGFW CN-серии

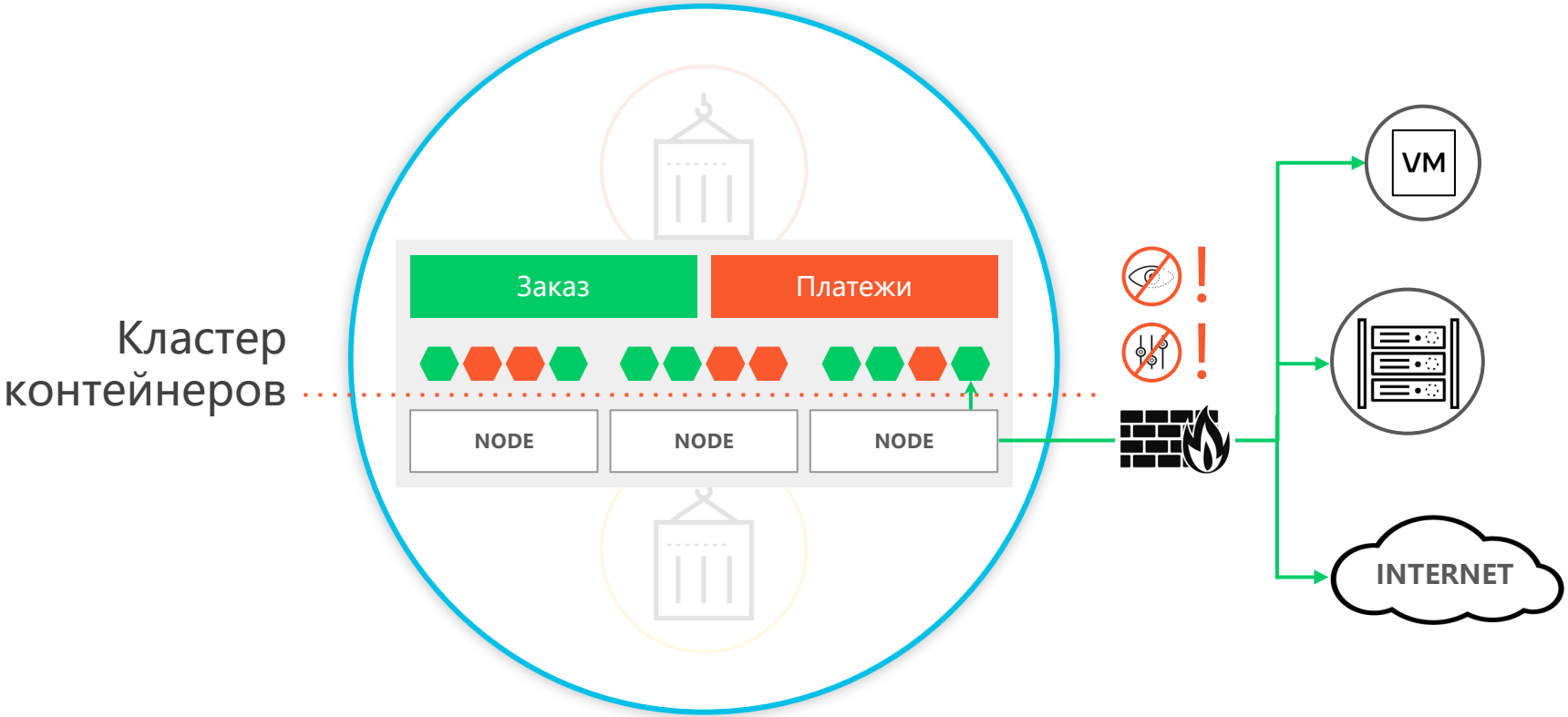
NGFW для среды Kubernetes

Возможности сервисов безопасности Palo Alto Networks в форма-факторе контейнера

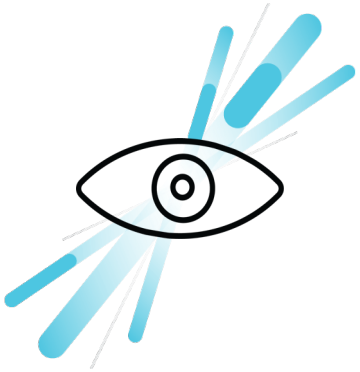
Защита сети на уровне L7 и предотвращение угроз

Интеграция с Kubernetes

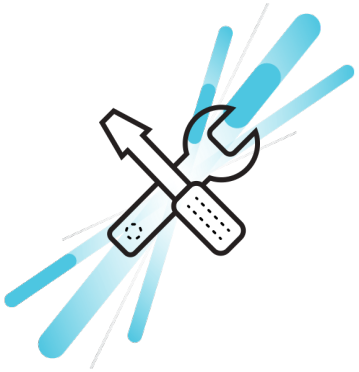
Классические форм-факторы МЭ не получают полной картины



Визуализация сетевых активов и защита от угроз в среде Kubernetes



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



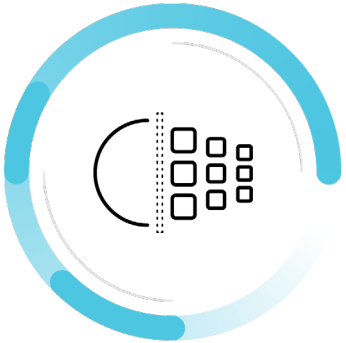
Централизованное управление политиками и NGFW из Panorama

Автоматизация и масштабирование благодаря интеграции с Kubernetes

Типовые сценарии использования CN-серии

Защита на L7 в направлении Восток-Запад

Реализация границ доверия между namespaces и другими типами рабочих нагрузок



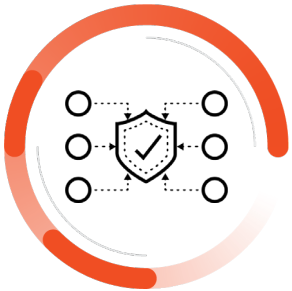
Инспекция исходящего трафика

URL-фильтрация проверка содержимого на L7

Инспекция входящего трафика

Блокировка известных и неизвестных угроз

Отличительные особенности CN-серии от Palo Alto Networks



Централизованное управление

DevOps оркестрация

Визуализация и понимание контекста Kubernetes

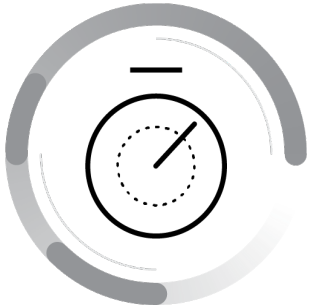
Лидер по уровню защиты

CORTEX XSOAR

Проблемы отделов безопасности

Количество уведомлений растет

Слишком много событий ИБ



Времени не хватает

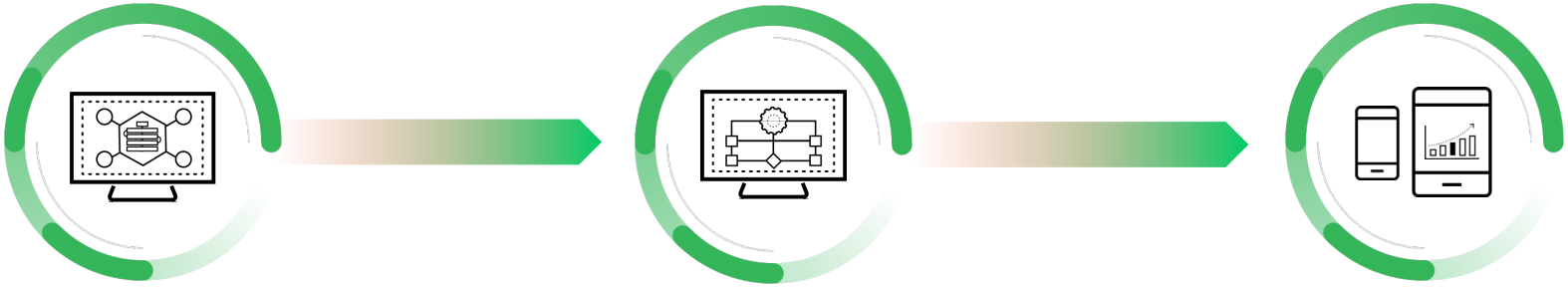
Много рутины (например, проверить все hash на VT и др.)

Ограниченный контекст

Мало информации по инцидентам, много времени на расследование

Что такое SOAR?

Security **O**rchestration, **A**utomation, and **R**esponse



Orchestration

Playbooks, runbooks, workflows

Логически выстроенная цепочка действий

Контроль за всеми несовместимыми продуктами из одной точки

Automation

Готовые скрипты автоматизации

Интеграция с другими продуктами

Запуск скриптов и получение результатов

Response

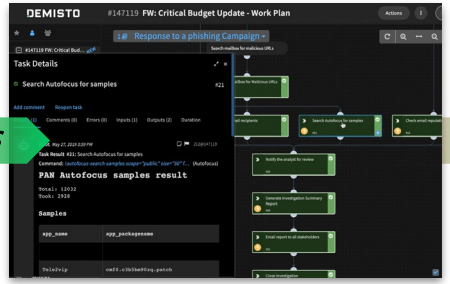
Case management

Аналитика и отчеты

Коммуникатор и совместная работа

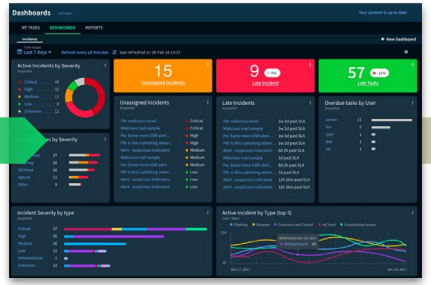
Реагировать и автоматизировать с Cortex XSOAR

ALERTS



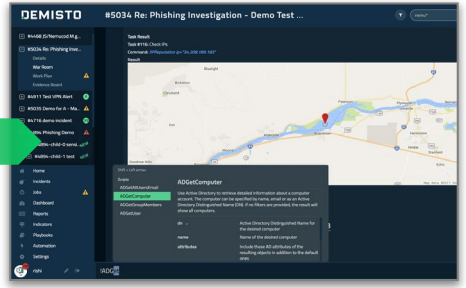
Автоматизация реагирования

Плейбуки на основе 350+ интеграций с другими вендорами



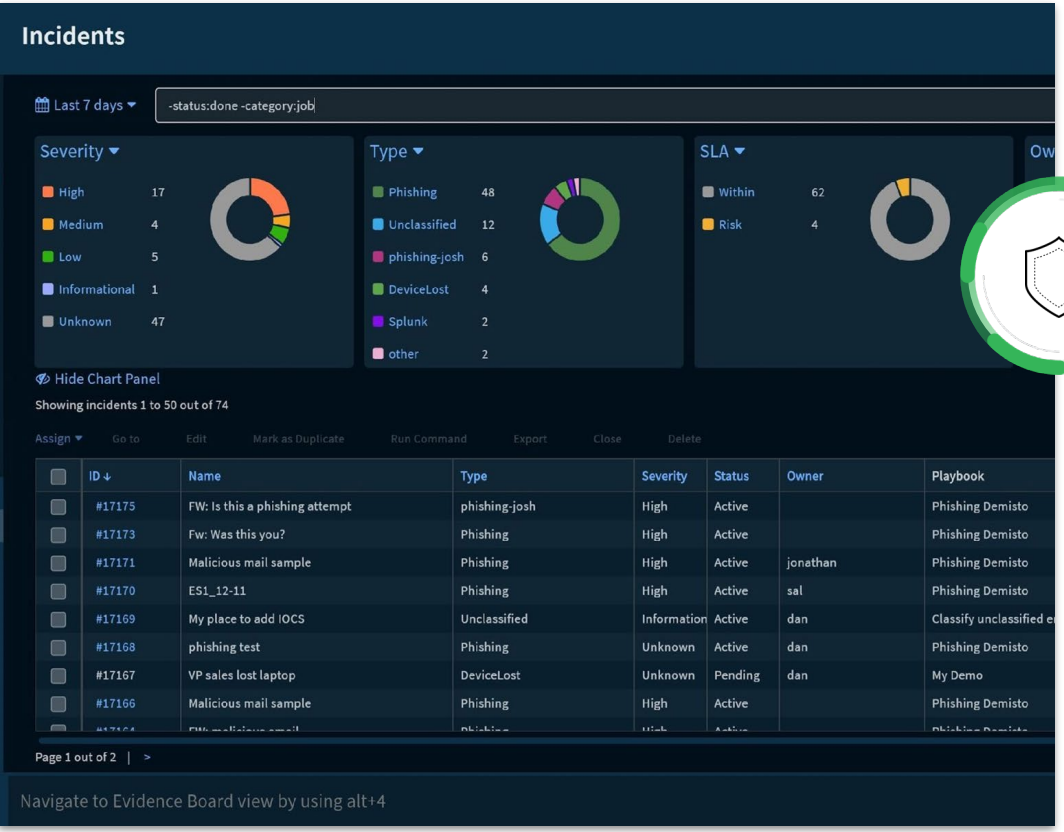
Управление инцидентами

Все инциденты в компании управляются из одной консоли



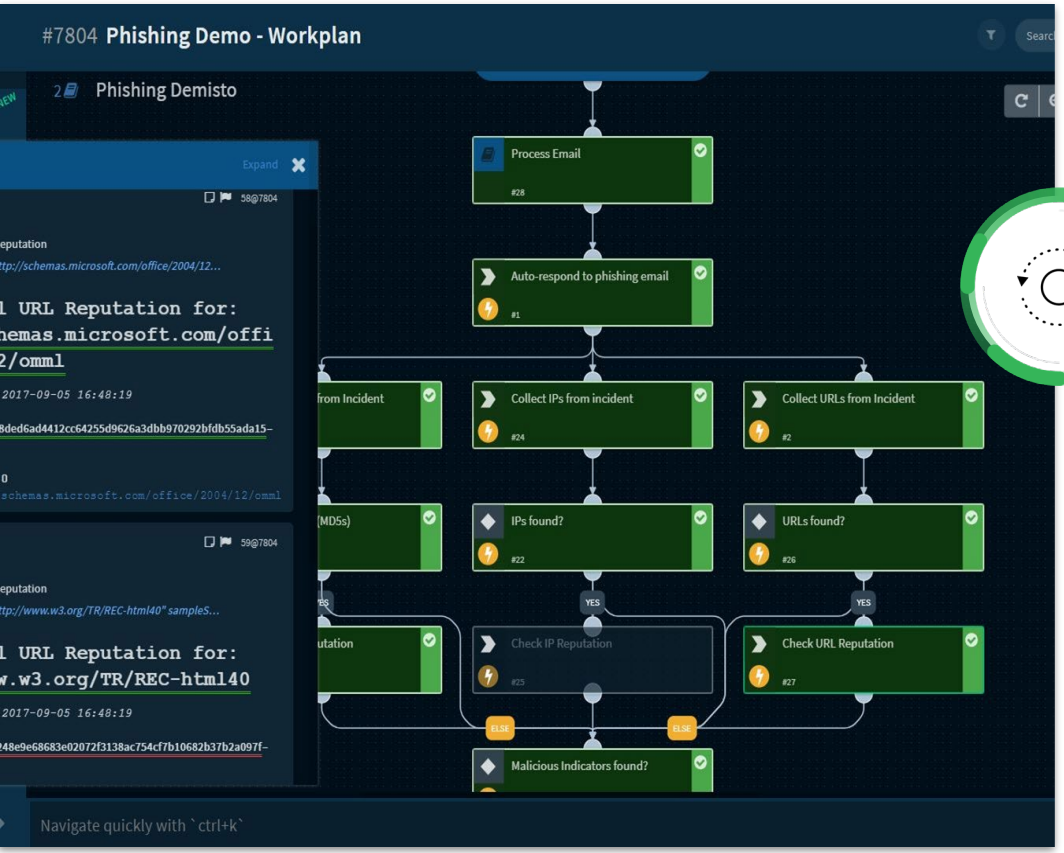
Совместная работа и обучение

Совместная работа и подсказки контекстные



Cortex XSOAR

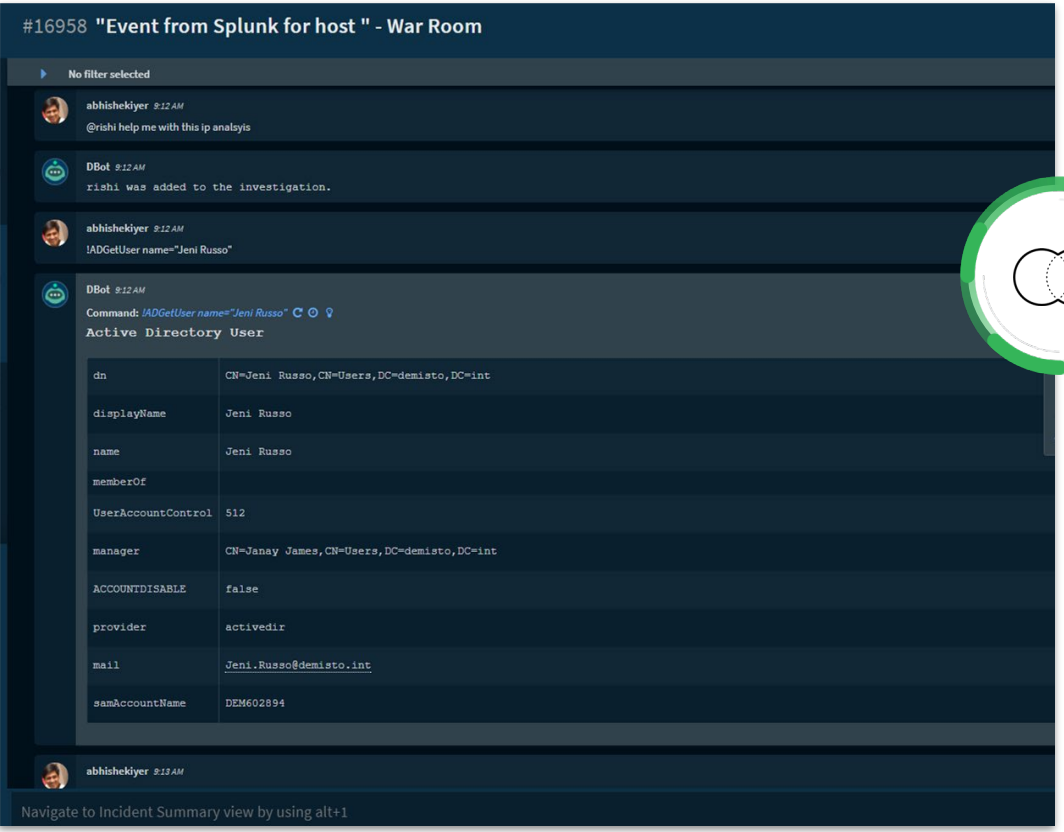
- **Система инцидентов**
- **Обогащение событий ИБ в реальном времени от разных источников**
- **Дашборды и отчетность**



Cortex XSOAR

Быстрая реакция на инциденты

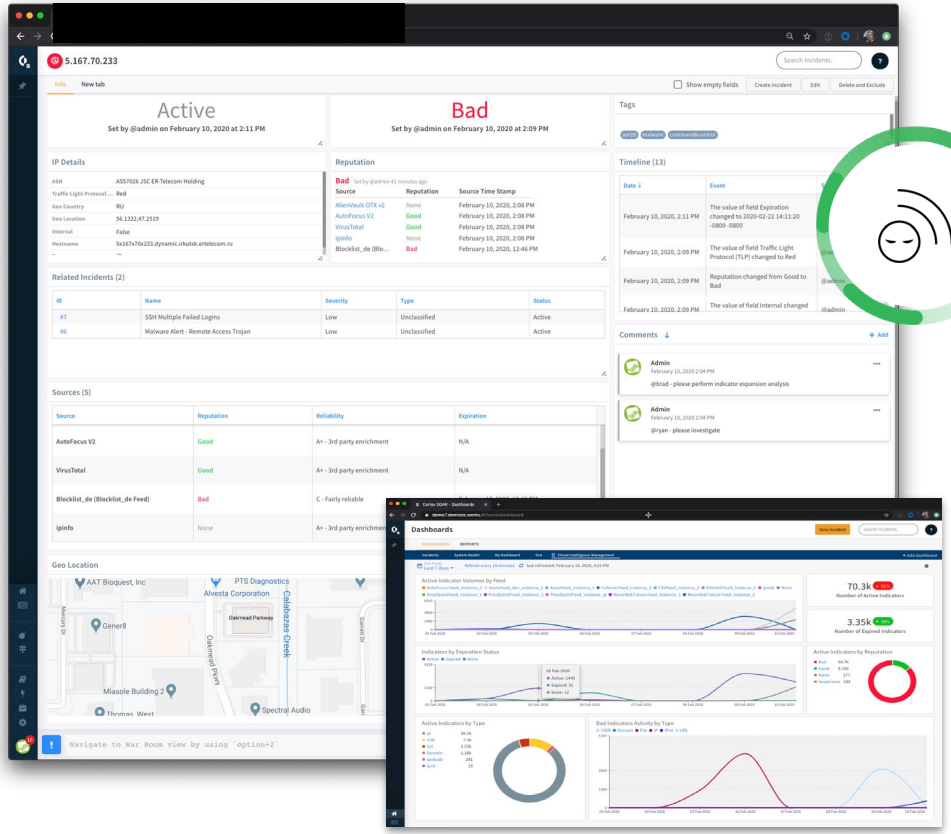
- **Интеграция с 450+ вендорами**
- **1000+ возможностей реакции**
- **Отработка по IoCs и не только**
- **Интуитивно понятный web-интерфейс**



Cortex XSOAR

Помогаем отделу ИБ работать как единая слаженная команда

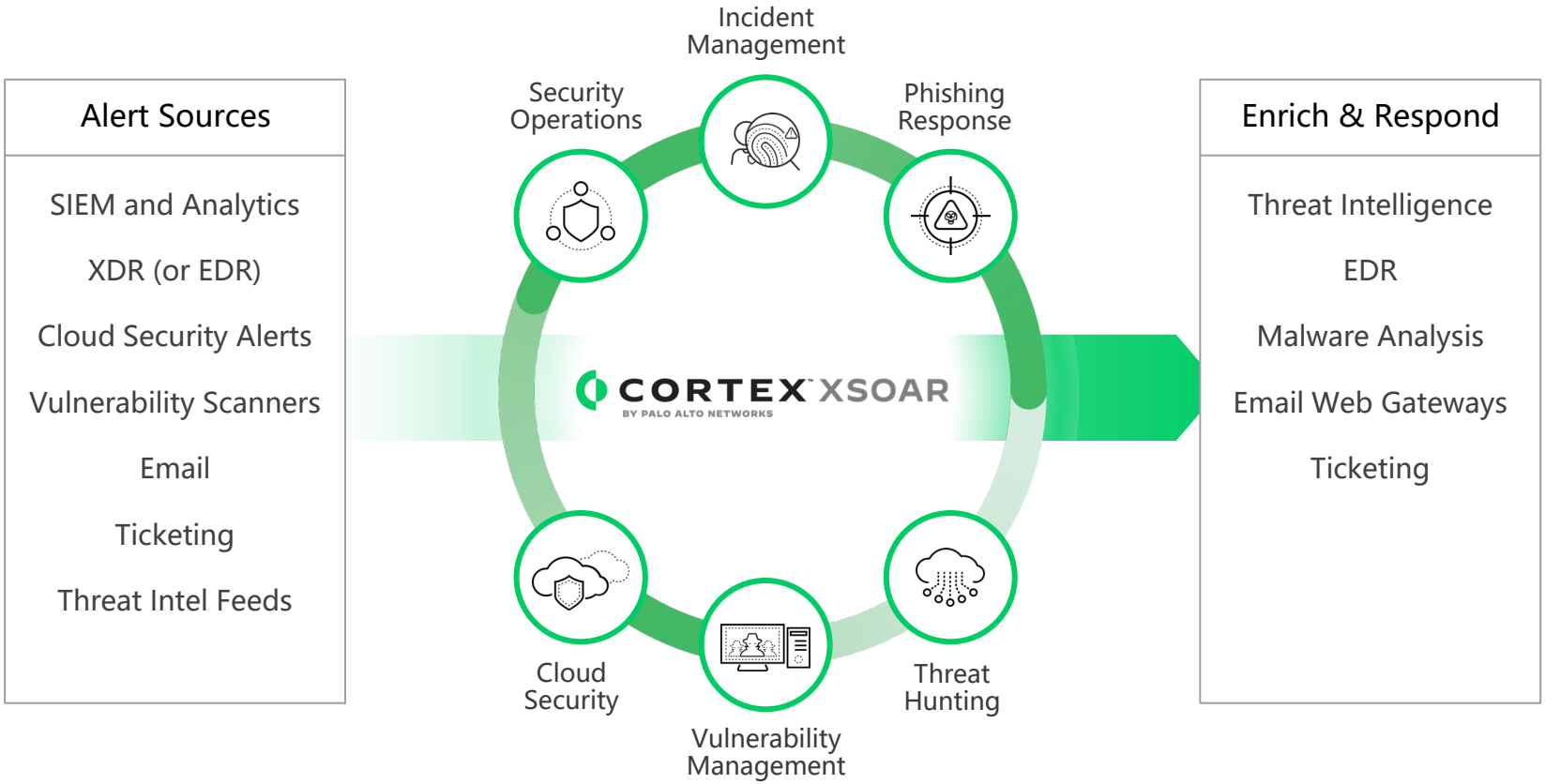
- **Virtual War Room**
- **ChatOps & real-time**
- **Автоматическое документирование и логирование**



Cortex XSOAR

- **Threat Intel Management (TIM)**
- **Автоматические наполнение информации из баз Threat Intelligence (Palo Alto Networks: Wildfire и Autofocus)**
- **Подключение любых внешних источников**
- **Повышение критичности IOC**

Множество различных сценариев применения Cortex XSOAR



Cortex XSOAR Ecosystem (более 450 интеграций)

Analytics and SIEM

CORTEX · DEVO · exabeam · FORTINET · JASK · LogRhythm · McAfee · MICRO FOCUS · Radar · splunk> · sumologic · Elastic SIEM

Threat Intelligence

paloalto · ALIEN VAULT · ANOMALI · COFENSE · CYMON · DOMAINTOOLS · FORSIGHT SECURITY · OpenPhish · Recorded Future · VirusTotal

Malware Analysis

paloalto · CISCO · cuckoo · FIREEYE · INTEZER · JoeSecurity · KOODOUS · REVERSING LABS · SNDBOX

Endpoint

CORTEX · Carbon Black. · CounterTack · CROWDSTRIKE · cybereason · CYLANCE · SentinelOne · Symantec. · TANIUM

Network Security

paloalto · Check Point · f5 · PROTECTWISE · Signal Sciences · zscaler · VECTRA · tufin

Authentication

CYBERARK · DUO · Active Directory · okta

Email Gateway

BitDam · mimecast · proofpoint. · Symantec.

Ticketing

cherwell · easyVISTA · freshdesk · Jira Software · salesforce · zendesk

Messaging

Exchange · pagerduty · slack · twilio · zoom

Cloud

CORTEX · PRISMA · aws · Google Cloud · Microsoft · netskope

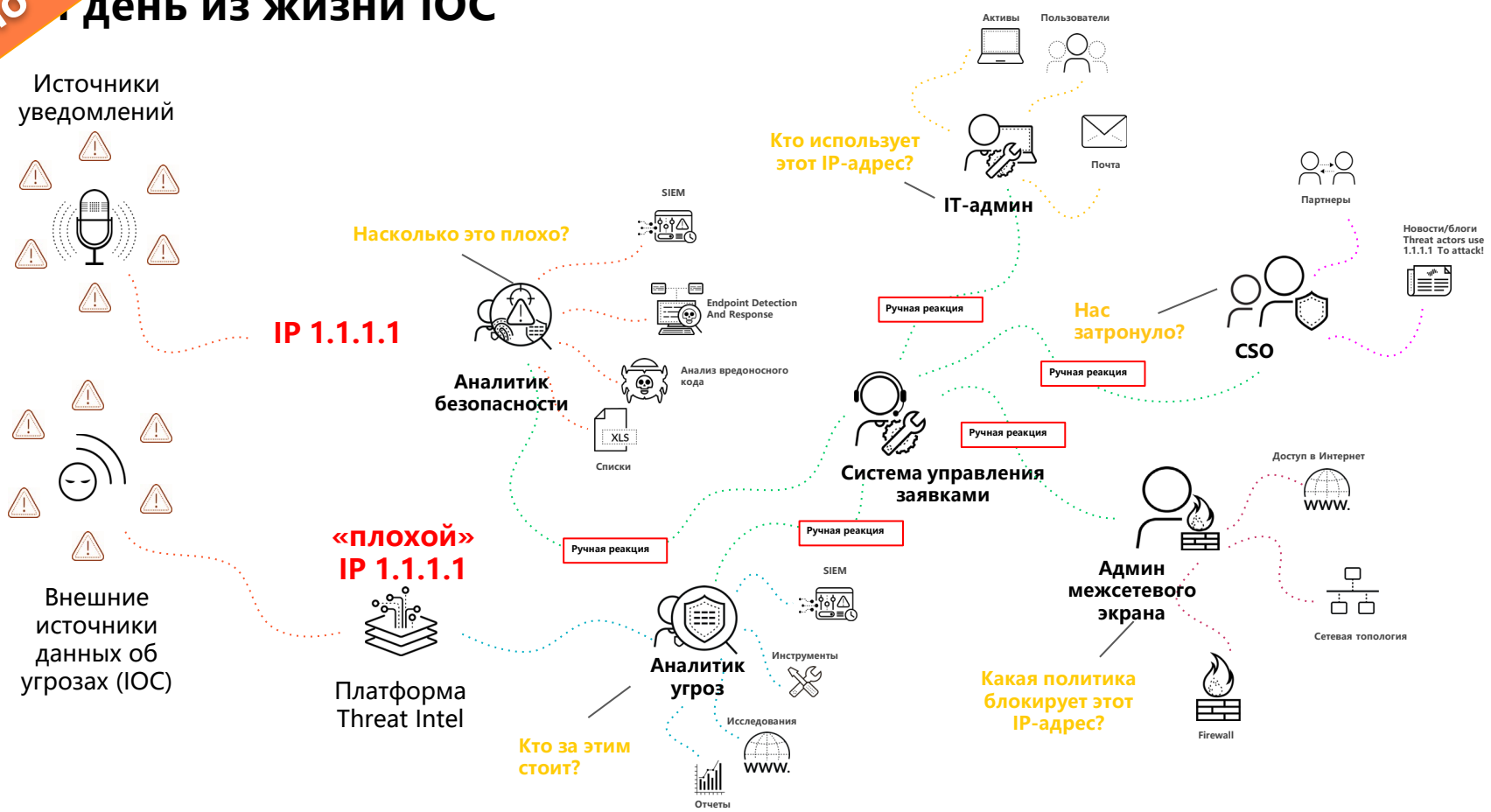
Пример сценария: **Реагирование на фишинг**

До

После

Было

…день из жизни IOC

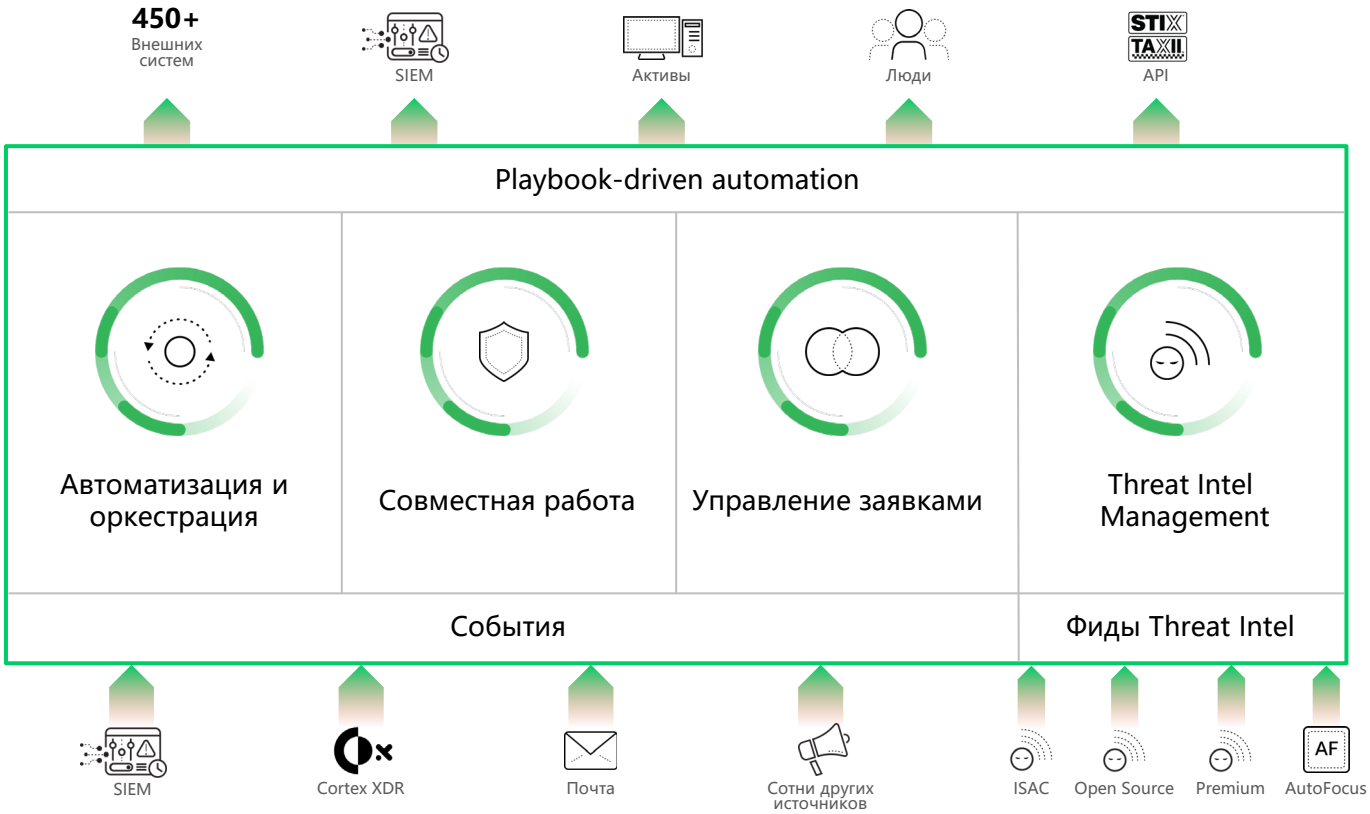


paloalto NETWORKS

Стало

…день из жизни IOC с Cortex XSOAR

CORTEX™ XSOAR
BY PALO ALTO NETWORKS



CORTEX XDR

paloalto NETWORKS

Cortex XDR предотвращает заражение операционных систем

Блокировка криптолокеров, эксплойтов и бесфайловых атак

Блокировка на основе данных threat intelligence Расследование инцидентов

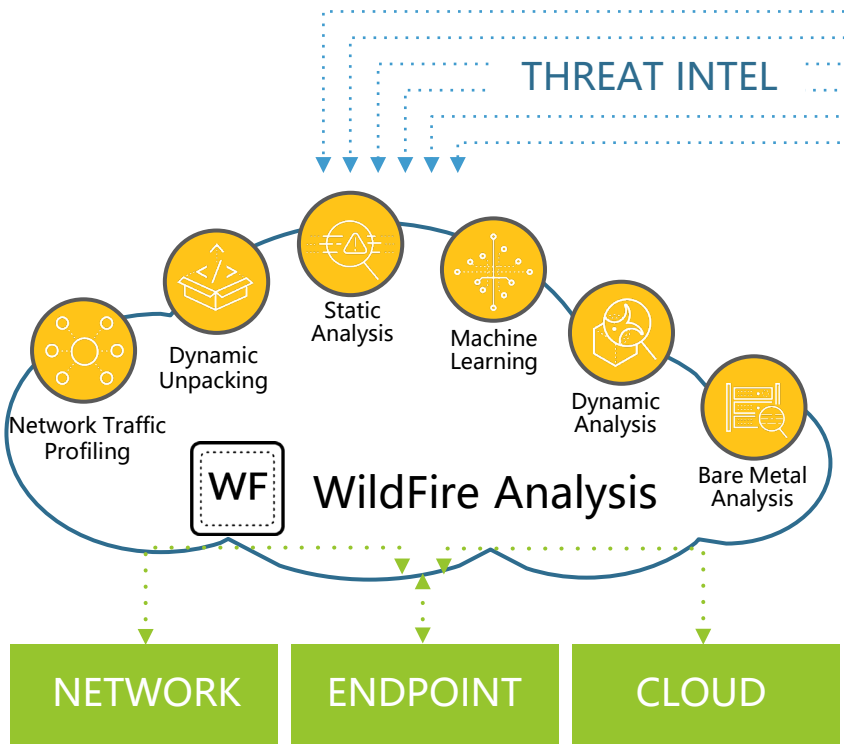
Обнаружение атак на основе machine learning

Продвинутая защита оконечных узлов

Предотвращает известные и неизвестные атаки:

- Без сигнатур
- Не требует постоянных обновлений
- Минимальная нагрузка на хост
- Знания о техниках реальных атак + Machine learning + анализ в WildFire

Cortex XDR использует песочницу WildFire

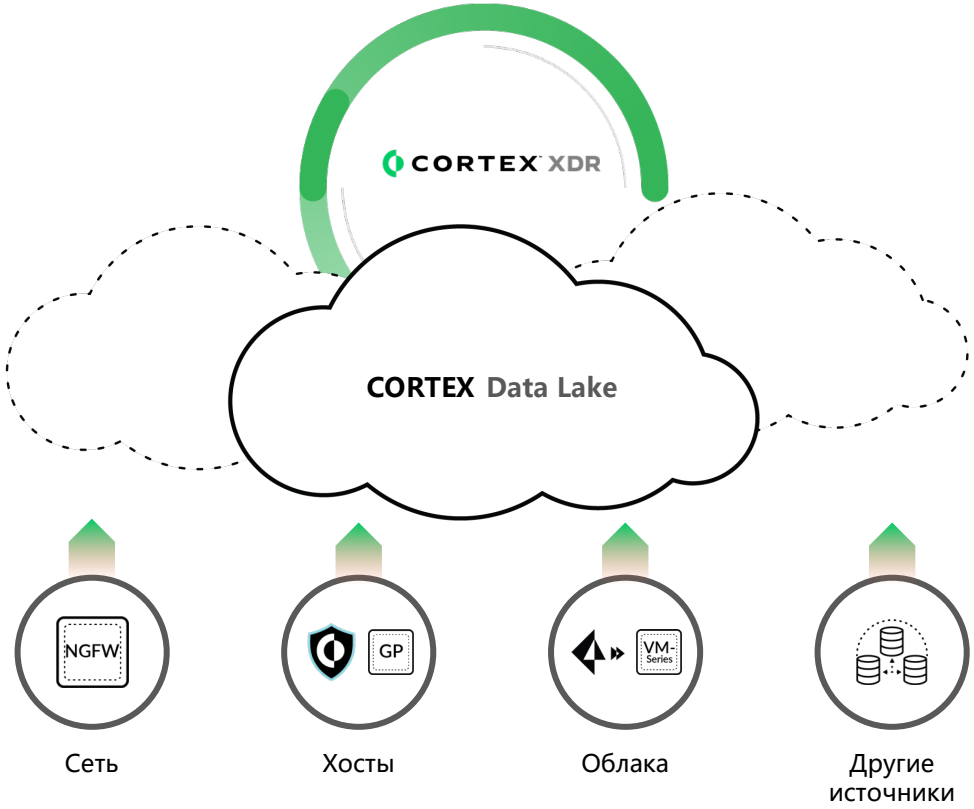


+150 Поставщики Threat Intelligence: 60000 заказчиков, Cyber Threat Alliance, VT....

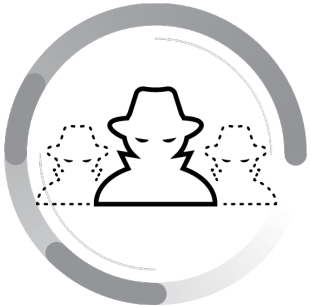
1000s **Не виртуальные, а реальные компьютеры - Bare-Metal Analysis**

300M новых вредоносных файлов WildFire **обнаруживает в месяц**

Важно: Аналитика по всем событиям в сети и облаке



Проблема: **Очень много False Positives и пропущенных атак**



Нельзя предотвратить атаку

Сложные атаки используют стандартные утилиты

Очень много ложных срабатываний

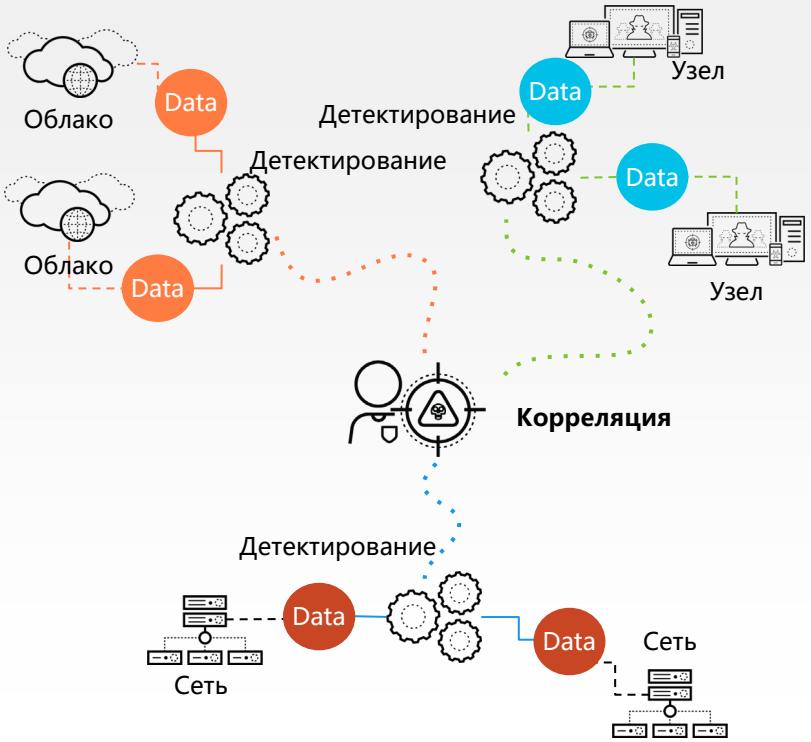
Трата времени на фильтрацию ложных срабатываний

Человеку невозможно заниматься обнаружением аномалий в таких объемах

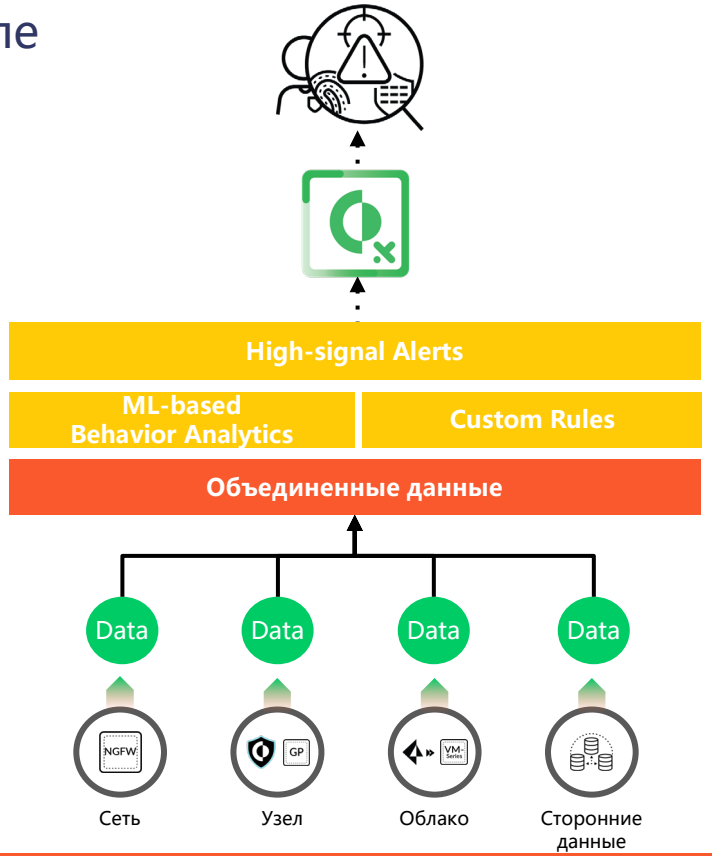
Чтобы обнаружить аномалии нужно обработать огромный объем данных

Наш подход: **Machine Learning для анализа данных**

До



После



Итог: через XDR сразу видна первопричина события в одном окне

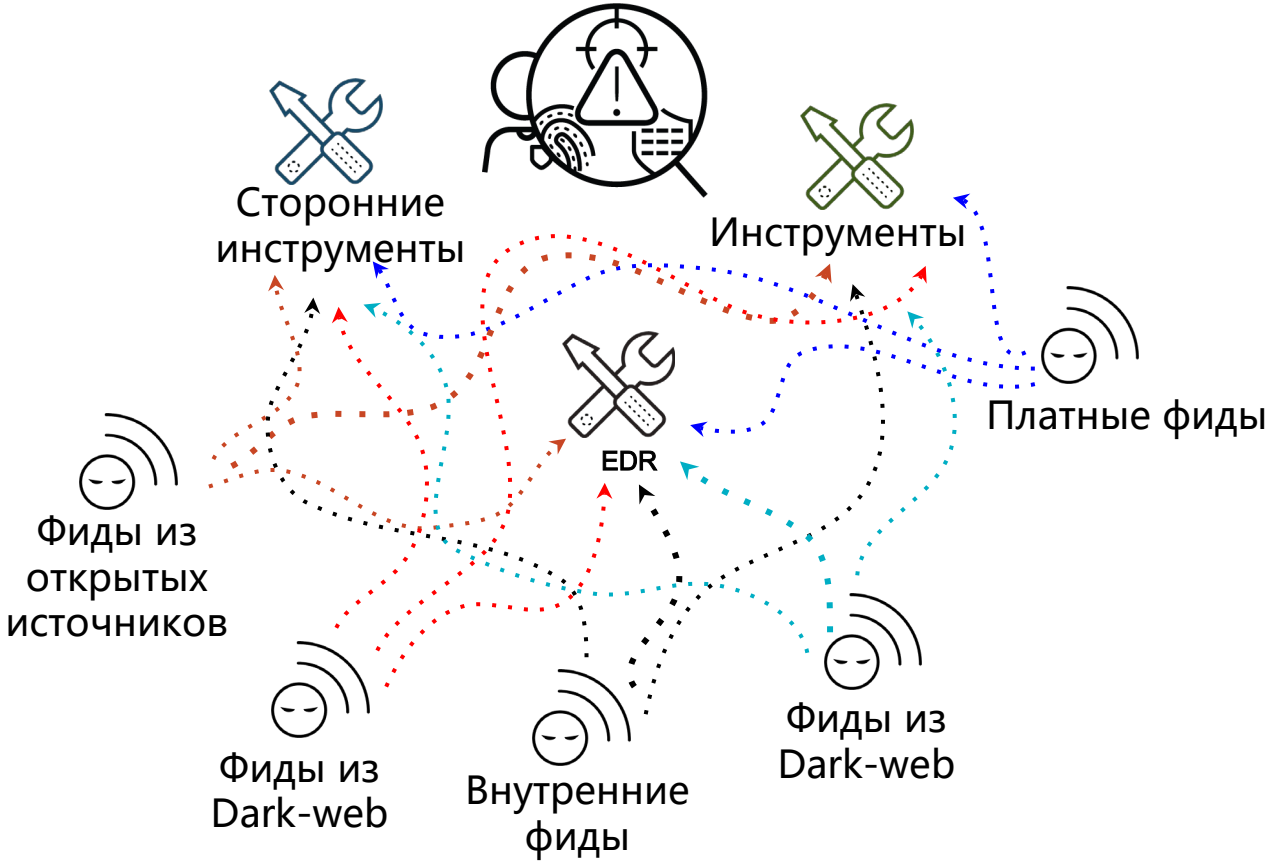
1. Расследование одним кликом
2. Цепочка событий в одном окне
3. Контекст, сигналы BIOC, threat intelligence, как шло во времени

AutoFocus

Платформа Threat Intelligence

paloalto NETWORKS

Проблемы с данными кибербразведки



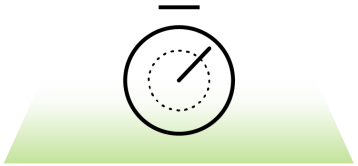
Проблемы с данными кибеpразведки

Невысокая ценность

Источников данных слишком много. Многие из них предоставляют данные низкого качества. Как выбрать адекватные?

Ненадежные данные

Источники имеют небольшой охват или предоставляют IoC, которые берут друг у друга, данные без контекста



Потерянное время

Ваши аналитики тратят время собирая и обрабатывая разрозненные ценные данные вручную

AutoFocus платформа Threat Intelligence

Threat Intelligence высочайшего качества

Подробные данные об IoC и вредоносных образцах, собранные из крупнейшей сети источников, включающих сети, оконечные узлы и облака

UNIT 42

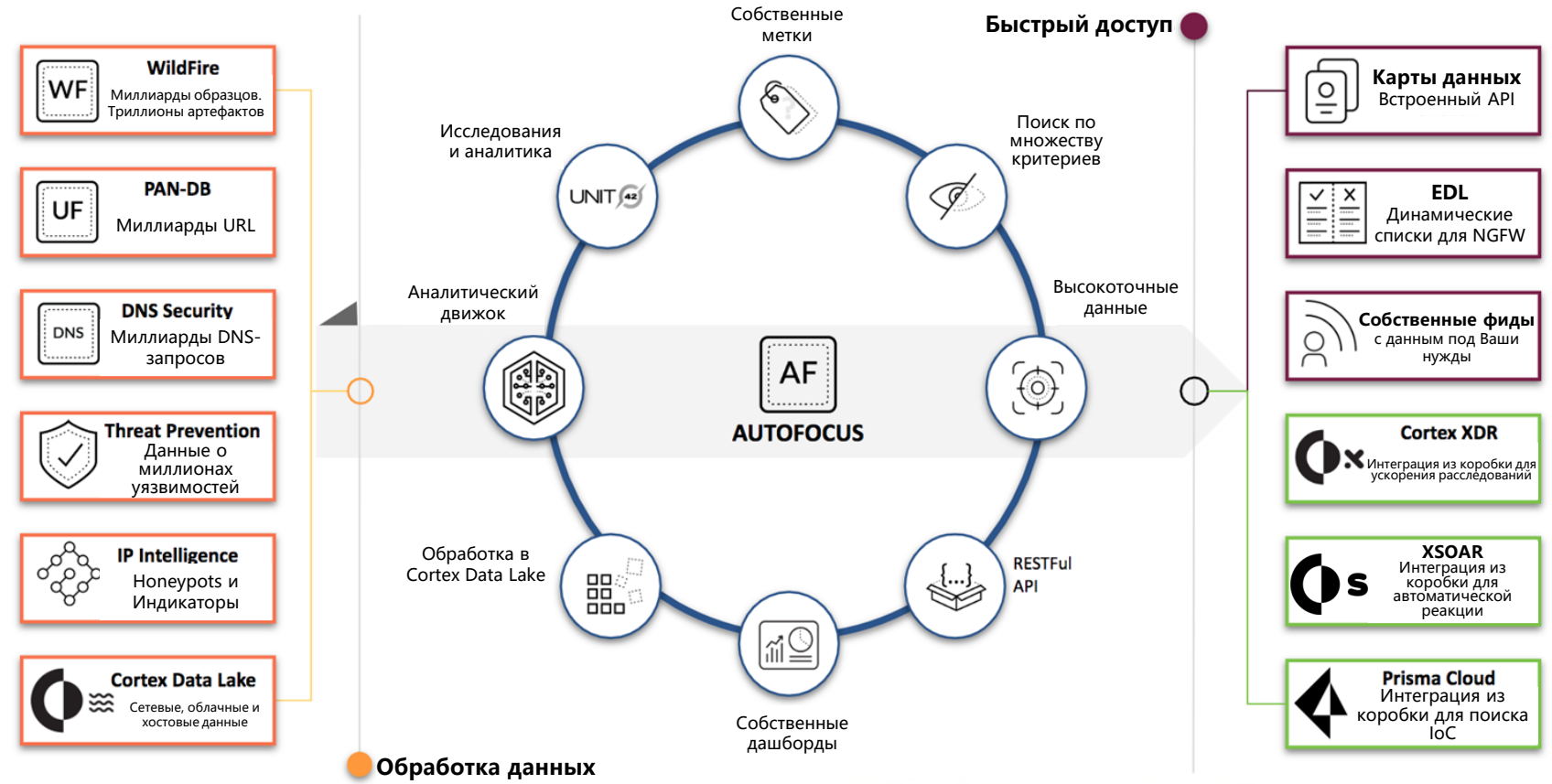
Подготовленные и проверенные данные

Данные обогащаются информацией из нашей лаборатории Unit42, команды исследователей и экспертов профессионалов

Мгновенный доступ

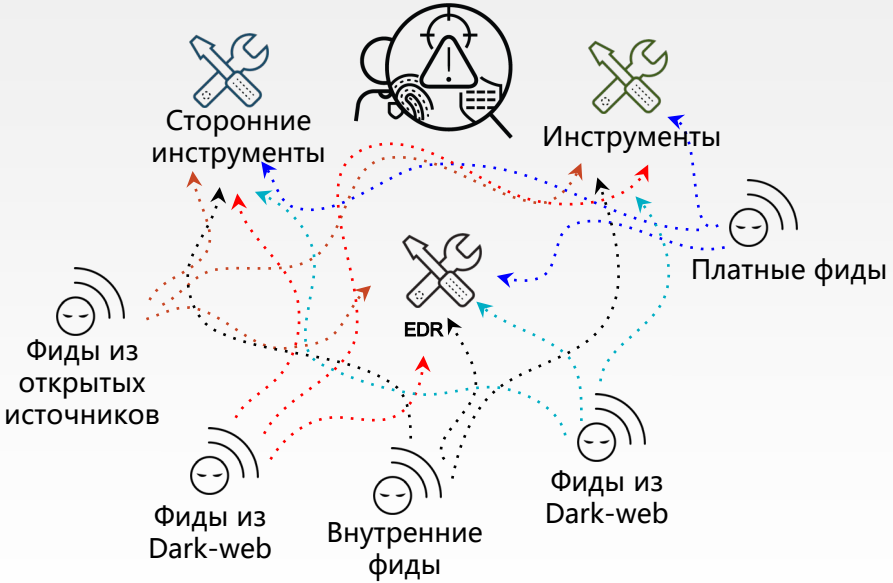
Экономия времени для аналитиков, т.к. данные встроены в продукты и инструменты используя собсвенные фиды и API

Архитектура AutoFocus

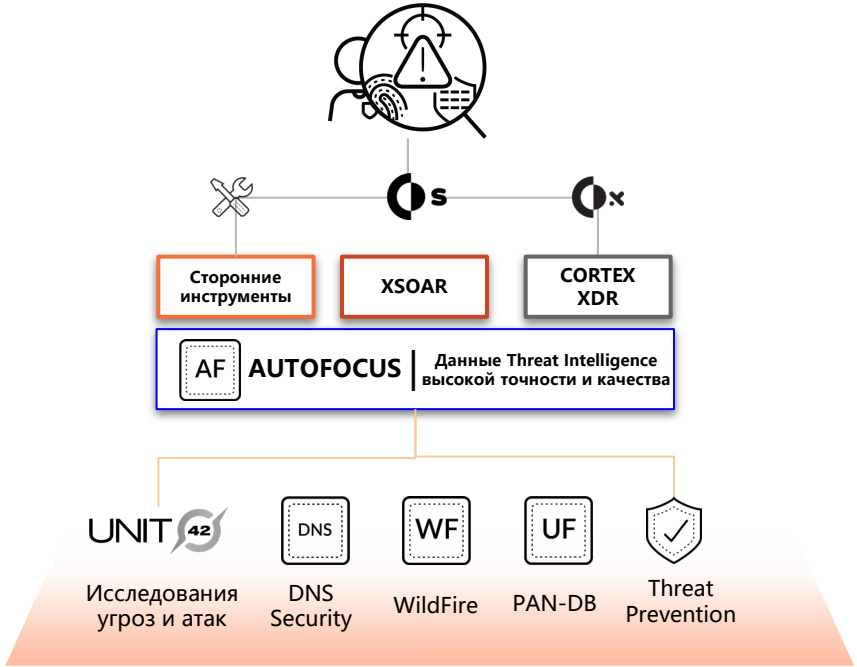


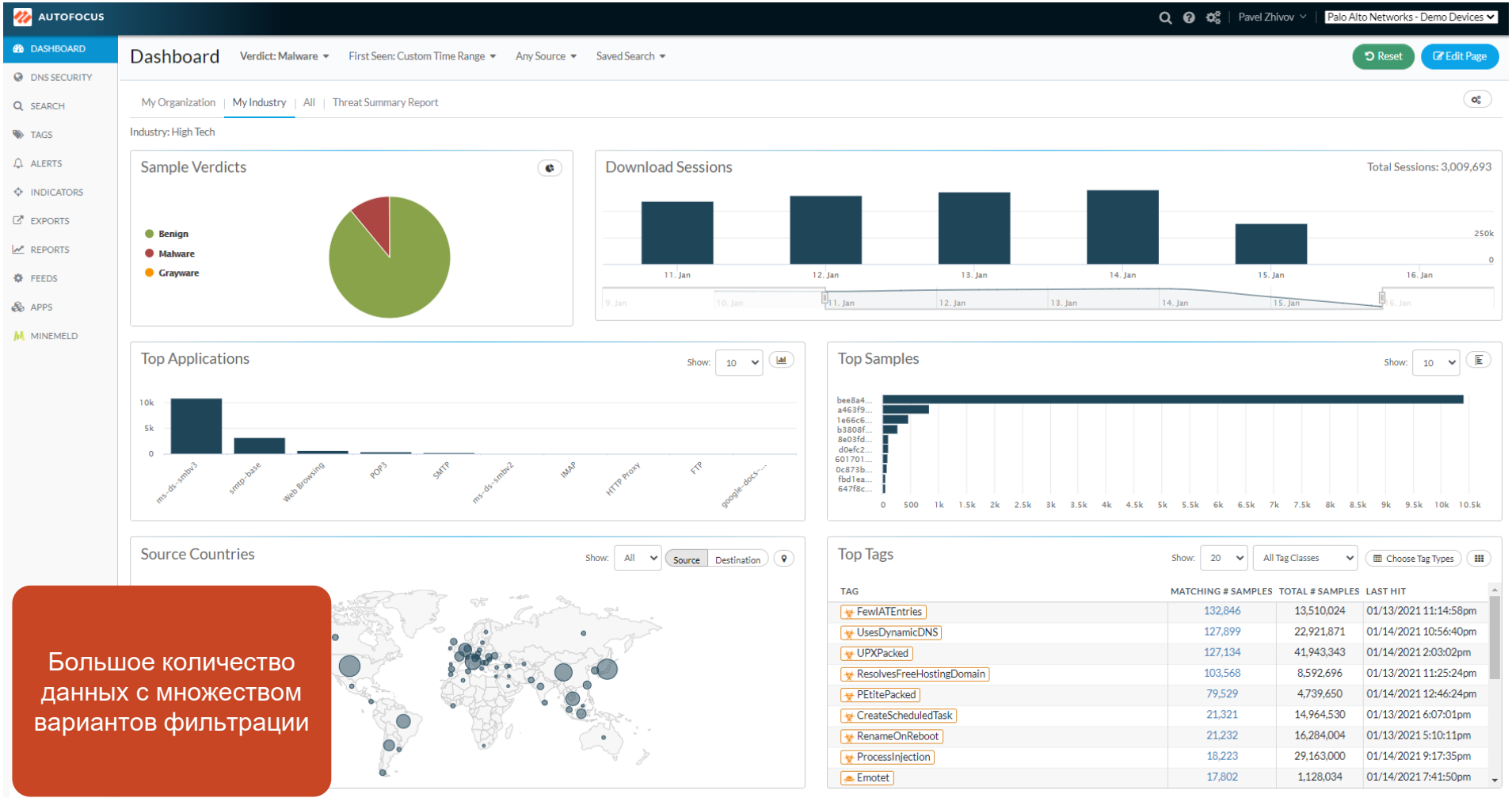
One-Stop-Shop Threat Intel

До

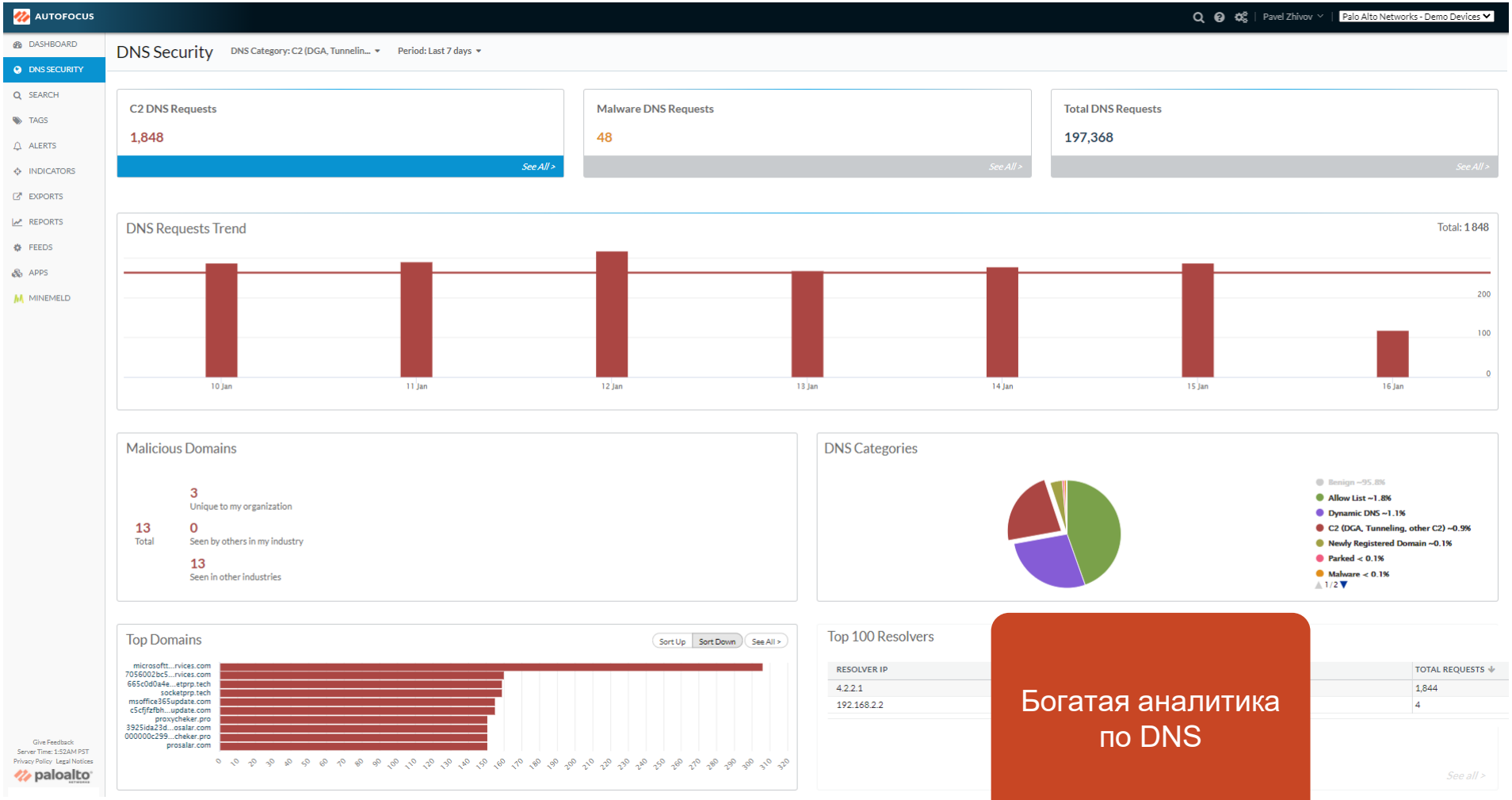


После



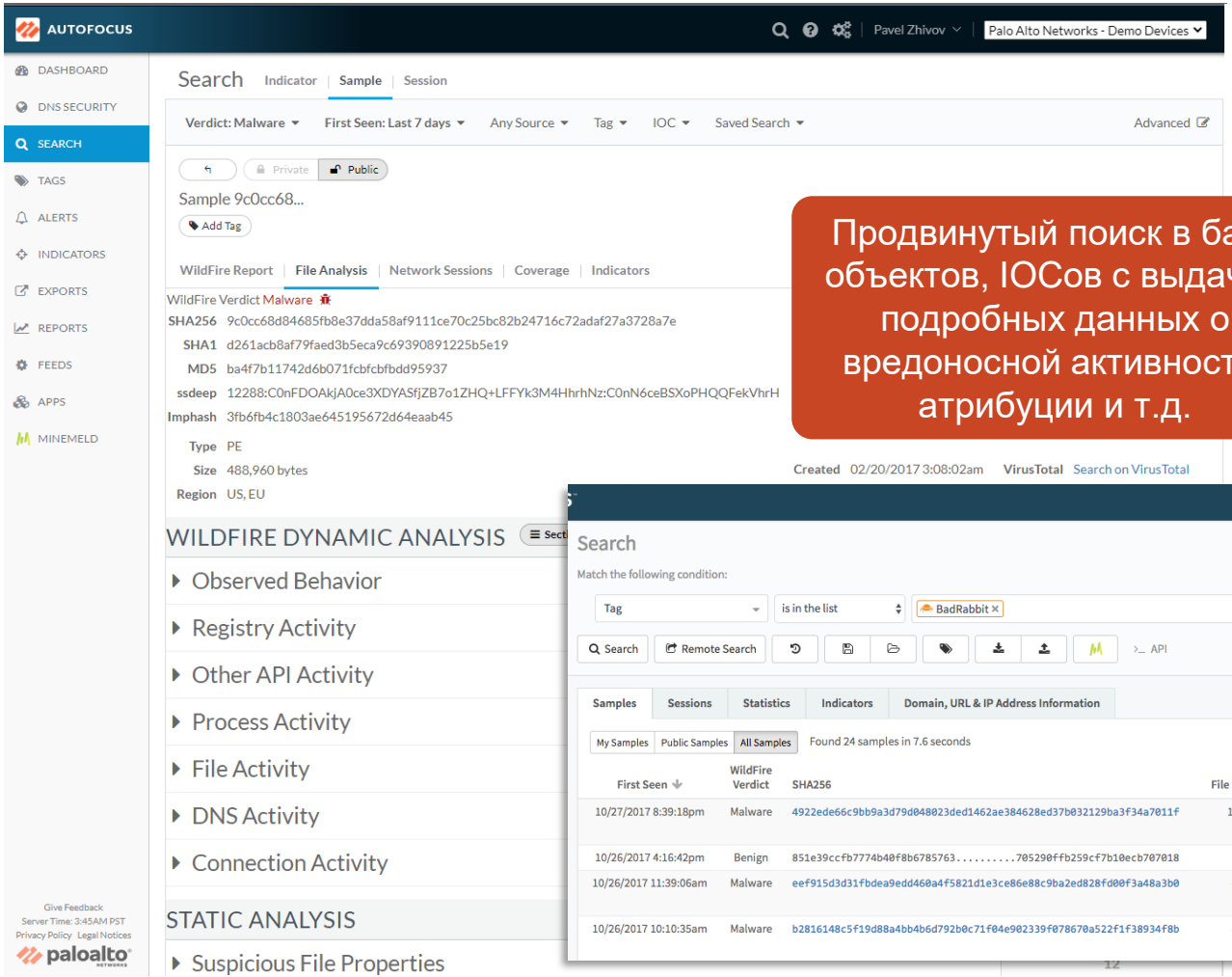


Большое количество данных с множеством вариантов фильтрации



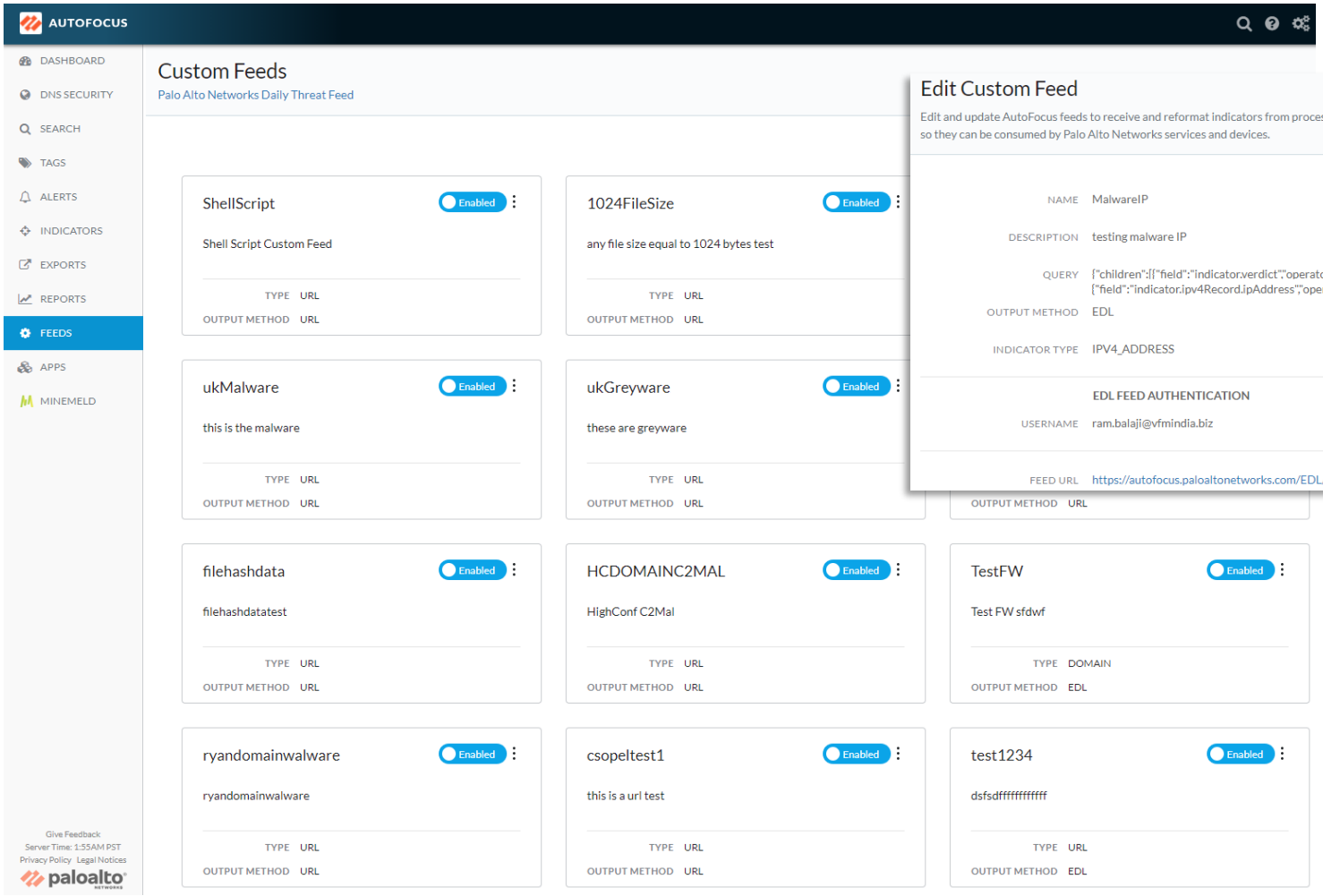
Богатая аналитика по DNS

paloalto NETWORKS



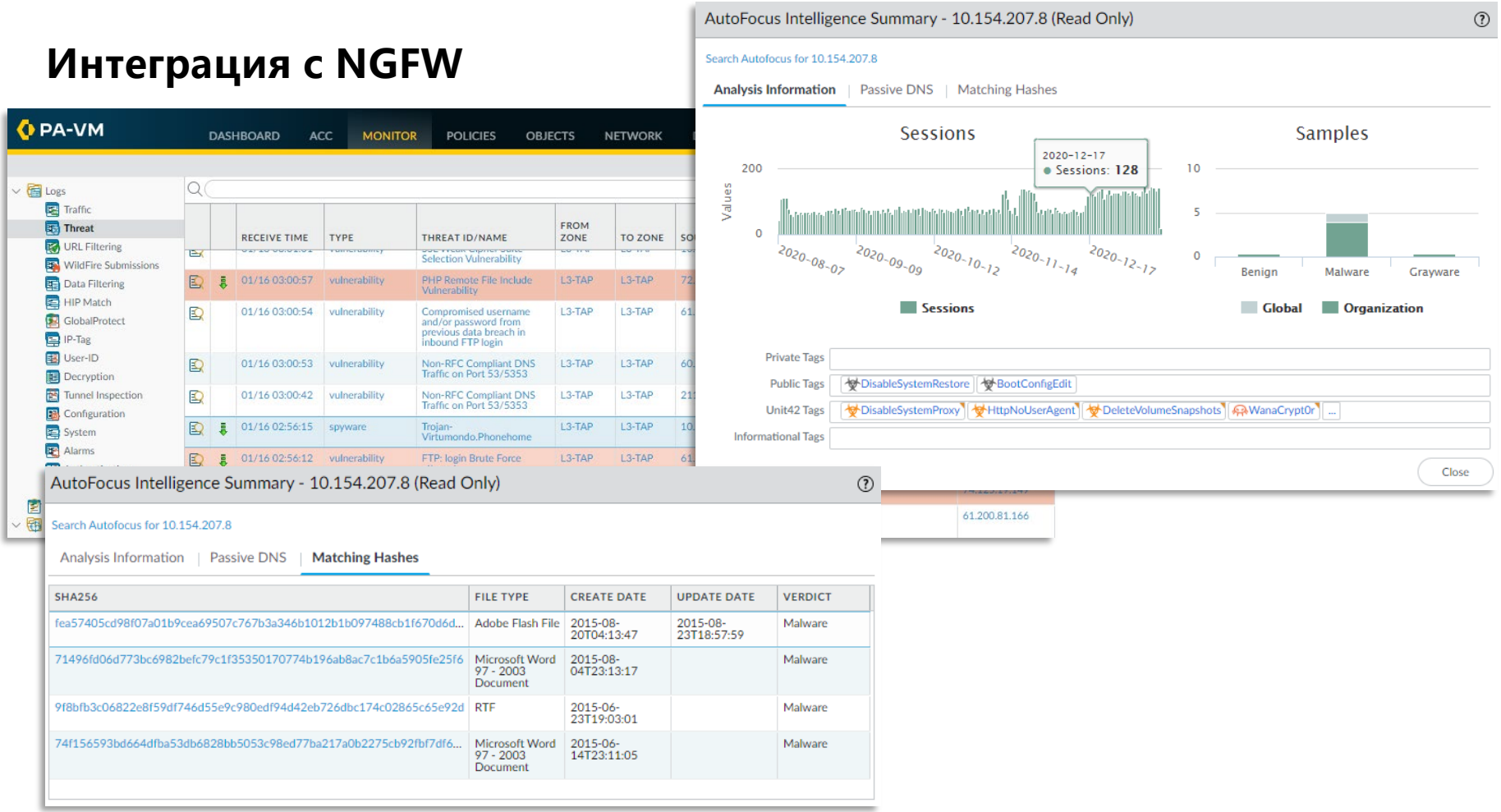
Продвинутый поиск в базе объектов, IOCов с выдачей подробных данных о вредоносной активности, атрибуции и т.д.

Огромный перечень критериев поиска



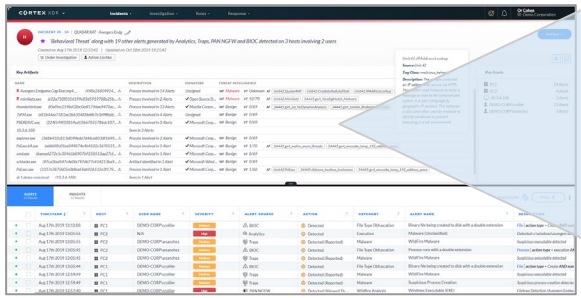
Создание собственных фидов с различными типами выходных данных и параметрами запросов

Интеграция с NGFW



Данные с тегами из AutoFocus в сводке по инциденту

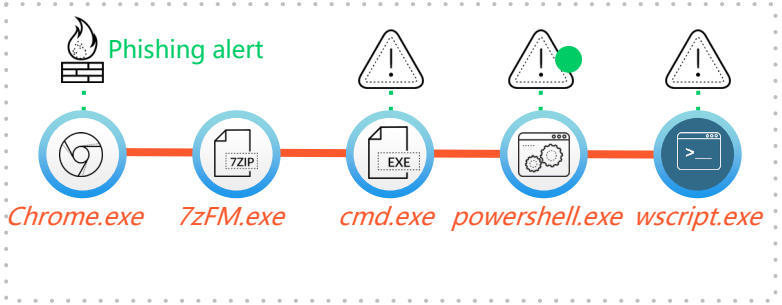
Инцидент



SIGNATURE	THREAT INTELLIGENCE			
Unsigned	WF Malware	VT Unknown	AF	Unit42.QuasarRAT, Unit42.CreateScheduledTask, Unit42.IPAddressLookup
✓ Open Source D...	WF Malware	VT 52/70	AF	Unit42.Mimikatz, 34445.gsrt_YaraSigMatch_Malware
✓ Mozilla Corpor...	WF Benign	VT 0/69	AF	34445.gsrt_jsa_NoDynamicAnalysis, 34445.gsrt_tomlan_BrokenImportTable
Unsigned	WF Benign	VT 0/69		
✓ Microsoft Corp...	WF Benign	VT 0/69		
✓ Microsoft Corp...	WF Benign	VT 0/69		
✓ Microsoft Corp...	WF Benign	VT 1/70	AF	34445.gsrt_malim_enum_threads, 34445.gsrt_amccabe_temp_192_address_space
✓ Microsoft Corp...	WF Benign	VT 0/69		
✓ Microsoft Wind...	WF Benign	VT 0/69		
✓ Microsoft Corp...	WF Benign	VT 1/68	AF	Unit42.PsExec, 34445.rfalcone_twoface_toolnames, 34445.gsrt_amccabe_temp_192_address_space

Description: The sam... an IP address info ser... This is often used mal... message or note to th... system in a user's lang... geographic IP locatior... is also used often used... identify sandboxes to ... executing in a lab env...

Тэги AutoFocus



AF +

Ускорение расследование и получение более полного контекста

AutoFocus и Cortex – упрощение расследования & реакция

WildFire
Миллиарды образцов. Триллионы артефактов

PAN-DB
Миллиарды URL

DNS Security
Миллиарды DNS-запросов

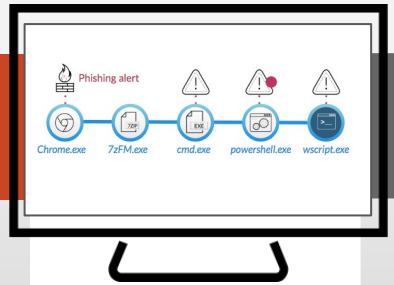
Threat Prevention
Данные о миллионах уязвимостей

IP Intelligence
Honeypots и Индикаторы

Cortex Data Lake
Сетевые, облачные и хостовые данные

Упрощение расследований и получение более детальной информации

AF



CORTEX XDR

Высокоточные данные

Расследование

Контекст инцидента
Обогащение дополнительной информацией

Повышение точности и ускорение работы

paloalto NETWORKS

AutoFocus и XSOAR – Автоматизация реакции на инцидент

WildFire
Миллиарды образцов.
Триллионы артефактов

PAN-DB
Миллиарды URL

DNS Security
Миллиарды
DNS-запросов

Threat Prevention
Данные о
миллионах
уязвимостей

IP Intelligence
Honeypots и
Индикаторы

Cortex Data Lake
Сетевые, облачные и
хостовые данные

Автоматизированная Кибербразведка

AF

Cortex
XSOAR

Высокоточные данные

Автоматизация

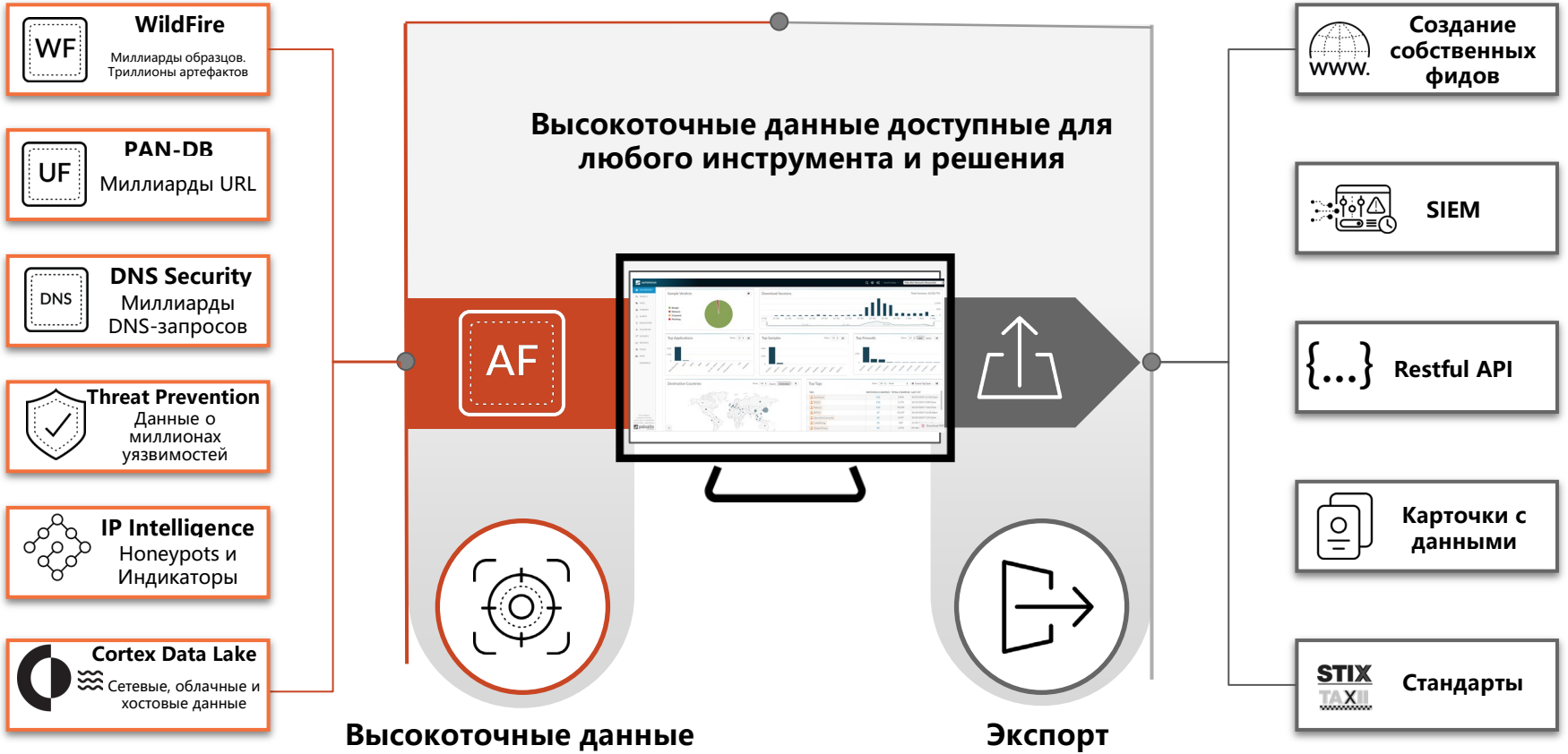
Унификация процессов

Управление кейсами

Обогащение плейбуков

Автоматизация реакции

Threat Intel для любых сторонних инструментов



Prisma Access
Платформа Secure Access Secure Edge

paloalto NETWORKS

Secure Access Service Edge

"Digital business and edge computing have inverted access requirements, with ***more users, devices, applications, services and data located outside of an enterprise*** *than inside."*

"Security and risk management ***leaders need a converged cloud-delivered secure access service edge*** *to address this shift."*

- Gartner, 2019

Gartner

The Future of Network Security Is in the Cloud

Published: 30 August 2019 **ID:** G00441737

Analyst(s): Neil MacDonald, Lawrence Orans, Joe Skorupa

Digital business transformation inverts network and security service design patterns, shifting the focal point to the identity of the user and/or device — not the data center. Security and risk management leaders need a converged cloud-delivered secure access service edge to address this shift.

Key Findings

- Network security architectures that place the enterprise data center at the center of connectivity requirements are an inhibitor to the dynamic access requirements of digital business.
- Digital business and edge computing have inverted access requirements, with more users, devices, applications, services and data located outside of an enterprise than inside.
- Complexity, latency and the need to decrypt and inspect encrypted traffic once will increase demand for consolidation of networking and security-as-a-service capabilities into a cloud-delivered secure access service edge (SASE, pronounced "sassy").
- Inspecting and understanding data context will be required for applying a SASE policy.
- To provide low-latency access to users, devices and cloud services anywhere, enterprises need SASE offerings with a worldwide fabric of points of presence (POPs) and peering relationships.

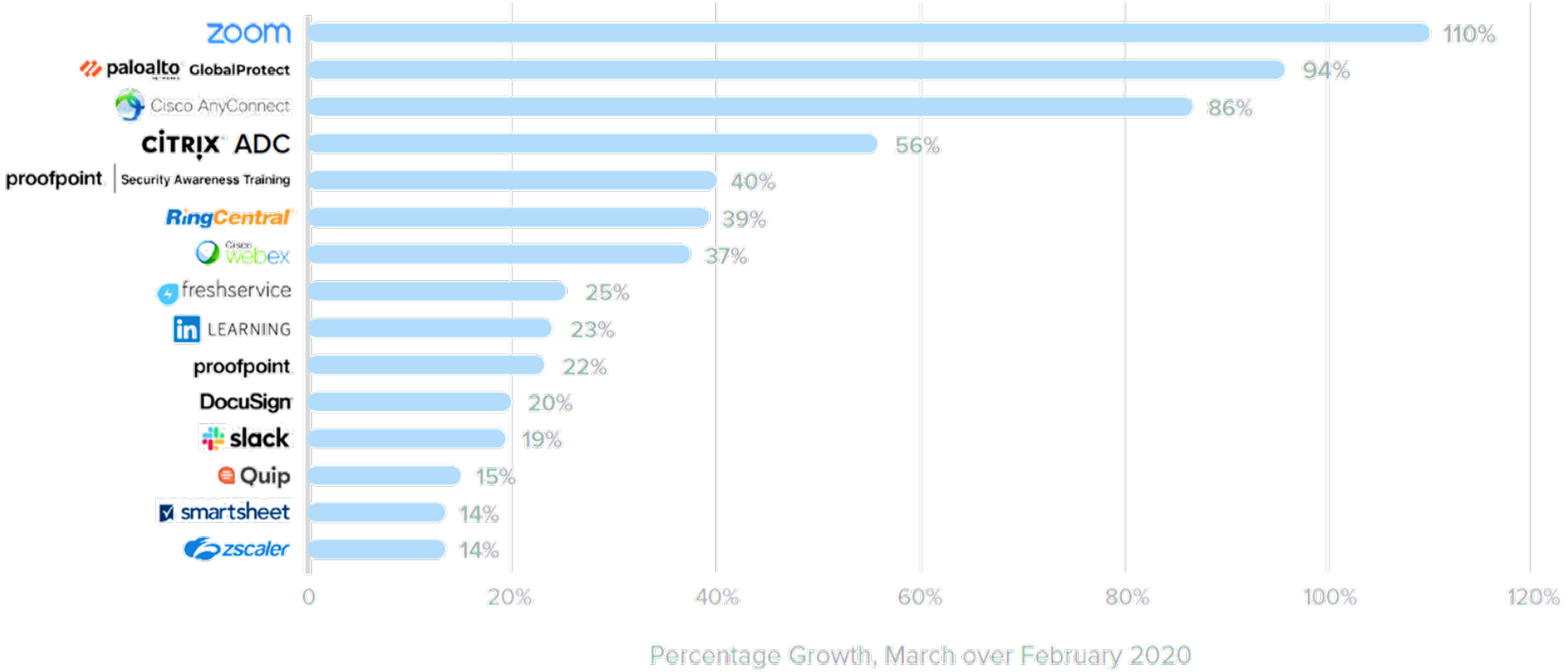
Recommendations

Security and risk management leaders responsible for security of networks and endpoints should:

- Position the adoption of SASE as a digital business enabler in the name of speed and agility.
- Architect to move inspection engines to the sessions, not to reroute the sessions to the engines.
- Shift security staff from managing security boxes to delivering policy-based security services.
- Engage with network architects now to plan for SASE capabilities. Use software-defined WAN and MPLS offload projects as a catalyst to evaluate integrated network security services.
- Reduce complexity now on the network security side by moving to ideally one vendor for secure web gateway (SWG), cloud access security broker (CASB), DNS, zero trust network access (ZTNA), and remote browser isolation capabilities.

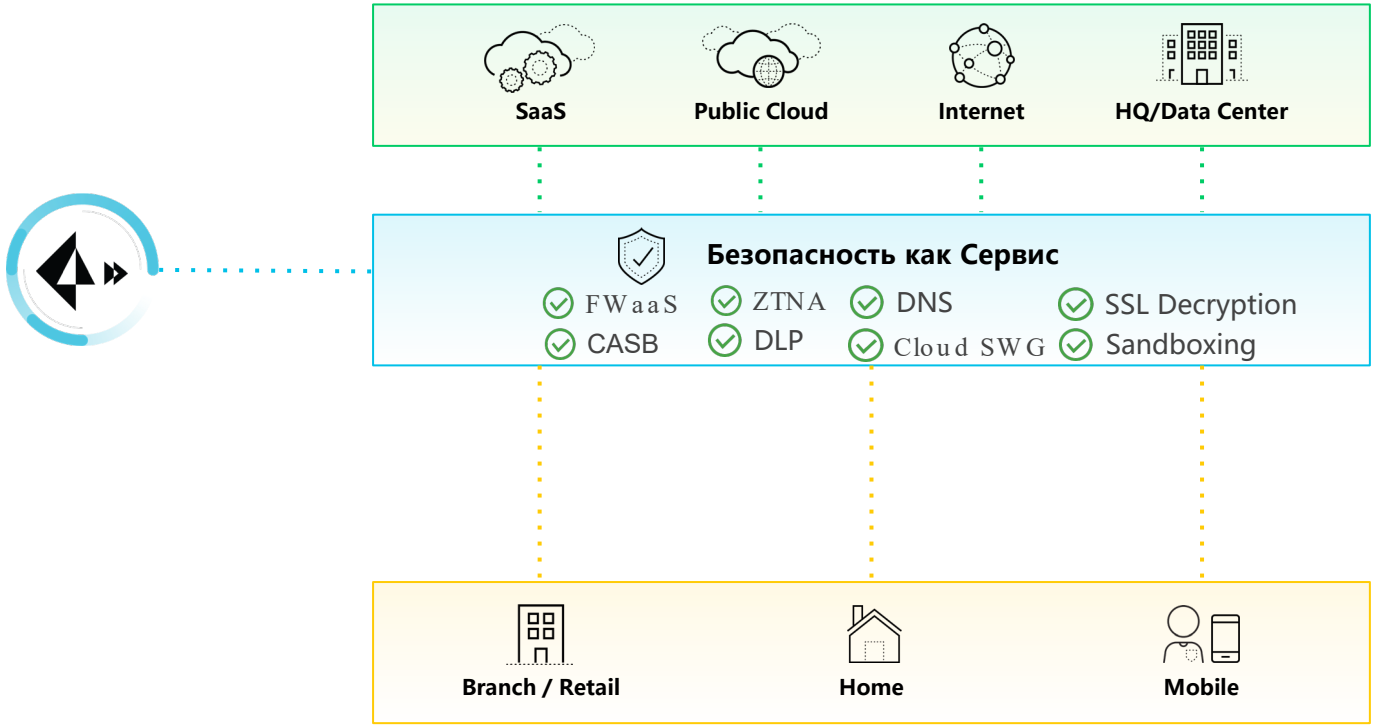
https://www.paloaltonetworks.com/cyberpedia/what-is-sase

Исследование Okta: ТОП приложений по росту количества уникальных пользователей

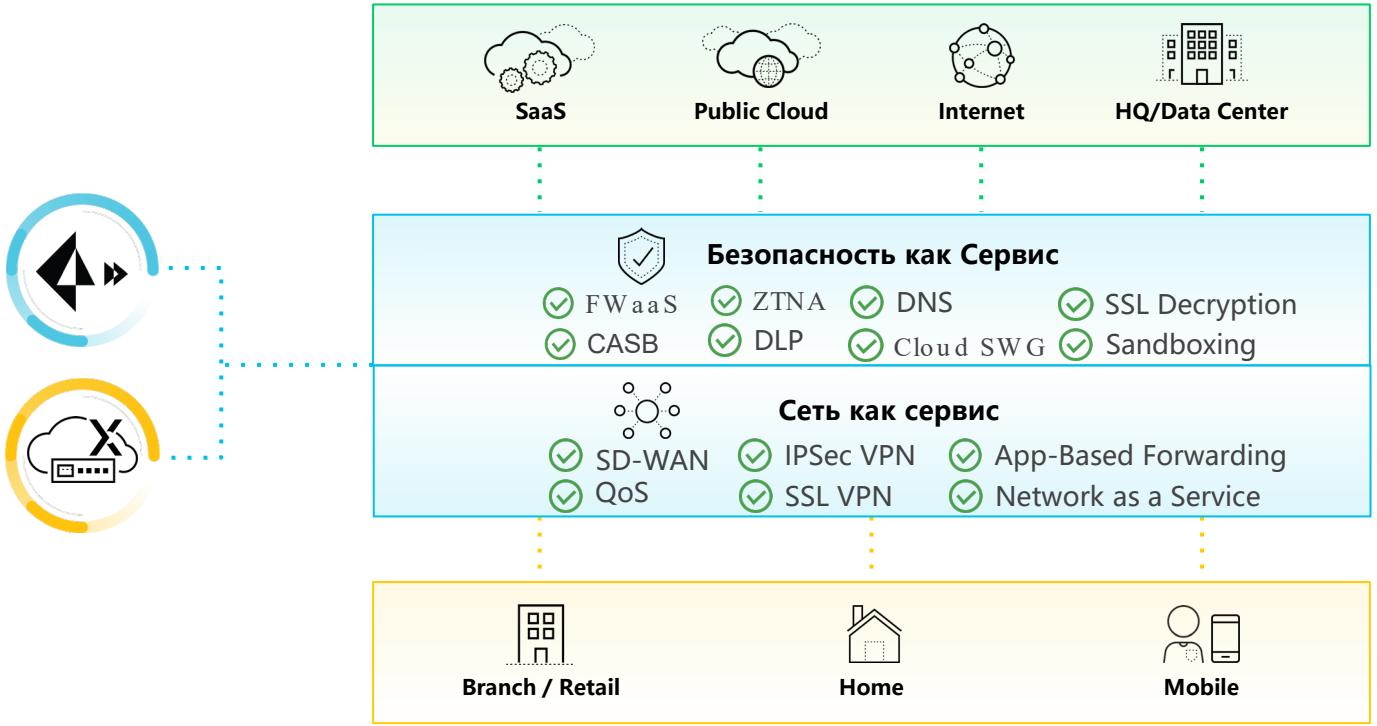


Источник: https://www.okta.com/businesses-at-work/2020/work-from-home/

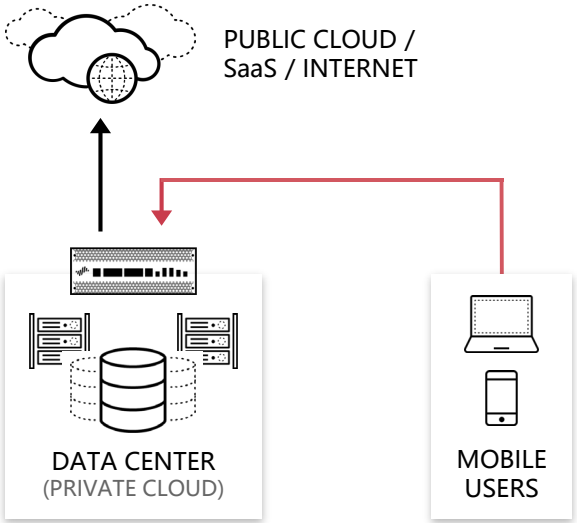
Prisma Access: Безопасность как сервис



Prisma Access: Безопасность + Сеть как сервис

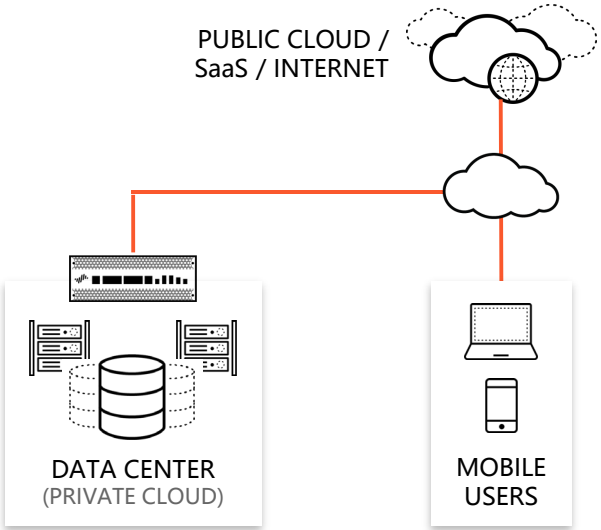


Два типа удаленного доступа



Собственный VPN внутри NGFW

Удаленный доступ по VPN в собственный ЦОД



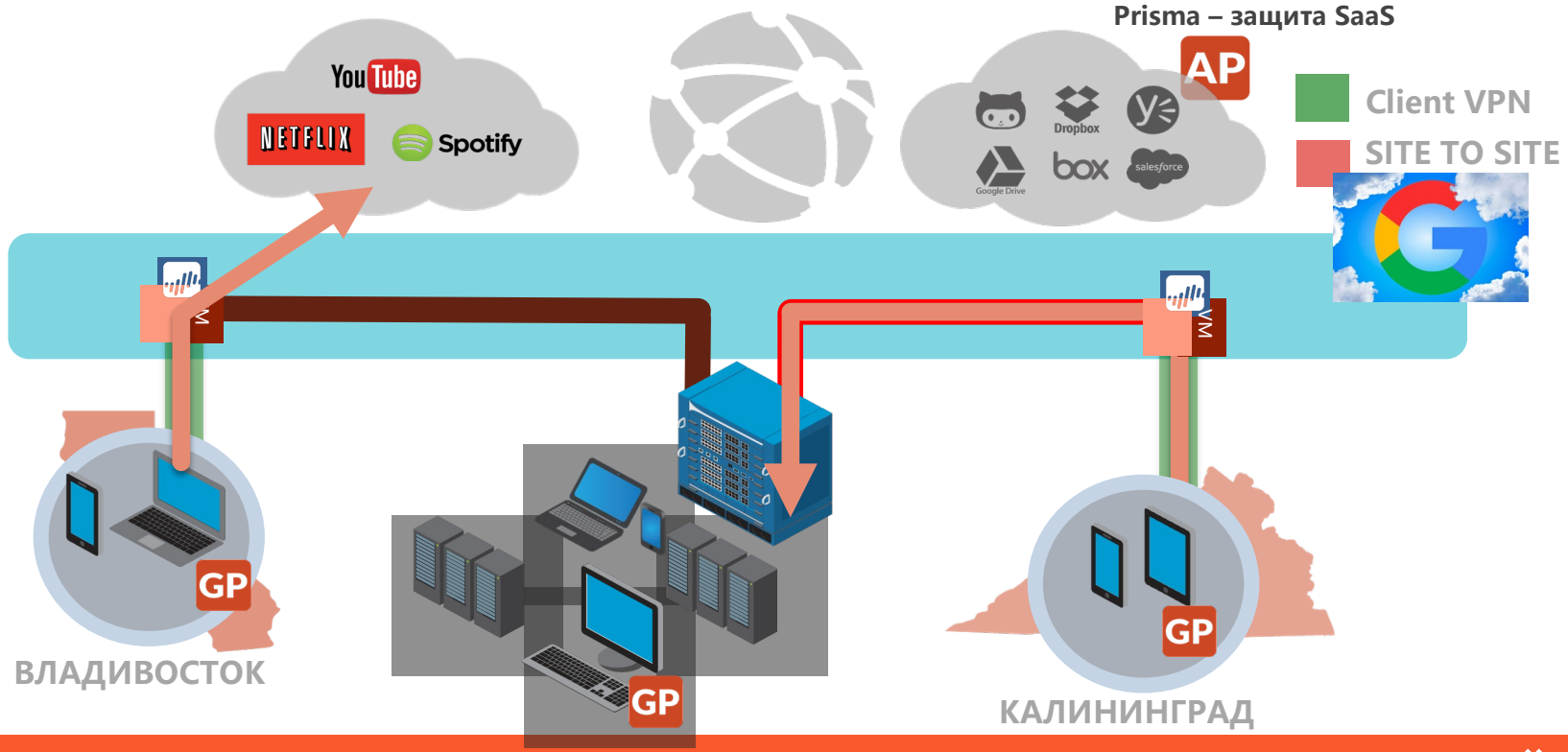
VPN и NGFW как сервис

Удаленный доступ по VPN : технология SASE

https://www.paloaltonetworks.com/resources/videos/cloud-enabled-mobile-workforce

Secure Access Service Edge (SASE) - сервисный слой защиты пользователей

Gartner: SASE комбинирует возможности SWG, CASB, FWaaS и Zero Trust Networks

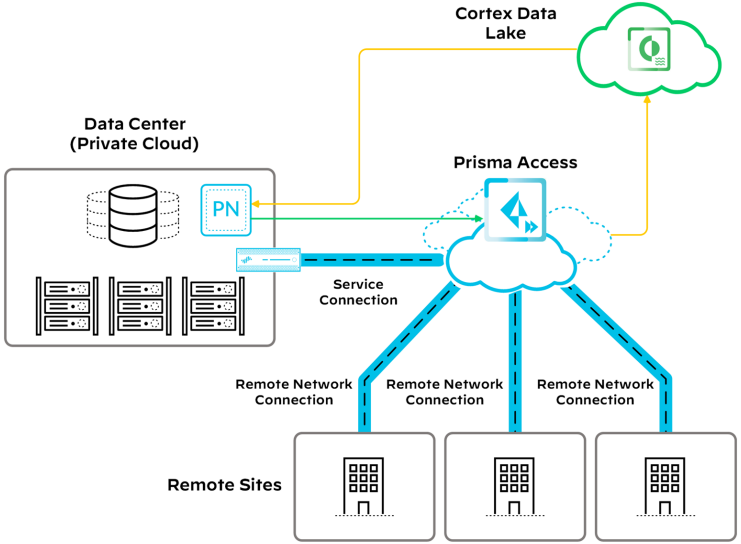


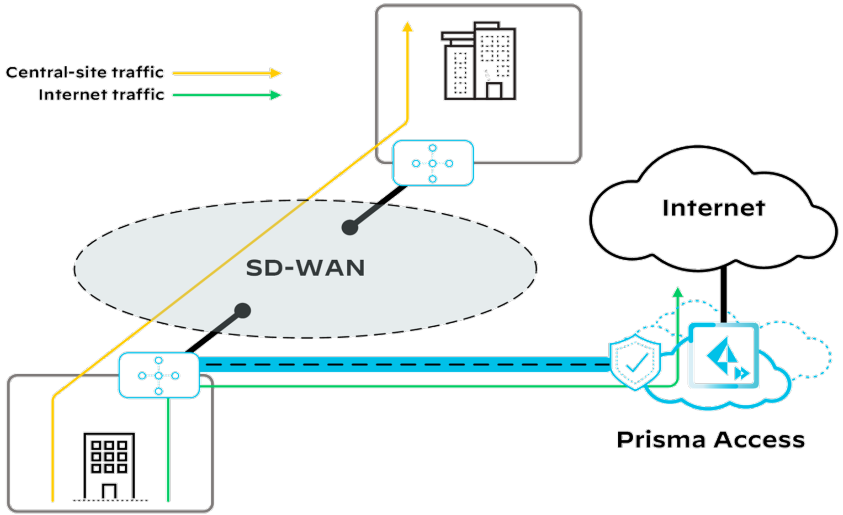
Prisma Access – облачный сервис где, удобно получать нужное число сервисов безопасности, например, VPN

ЦОД Google находится также в России, поэтому шлюзы в России и их может быть сколько угодно с ростом компании

Prisma Access + SD-WAN

- Не нужно заботиться о подборе «железа» для терминации всех туннелей SD-WAN – эластичное расширение в зависимости от нагрузки,
- В филиалах может быть ЛЮБОЕ оборудование, поддерживающее IPsec VPN – на уровне Prisma Access Вы получаете лидирующие в индустрии сервисы безопасности,
- Подключение центральных офисов, филиалов и любого ПК/телефона с клиентом GlobalProtect – единая защищенная сеть,
- Все, что Вам требуется – это иметь канал в Интернет



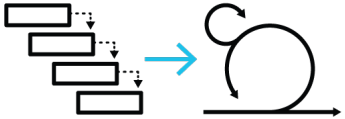


Prisma Cloud Enterprise Edition – Cloud Native Security Platform

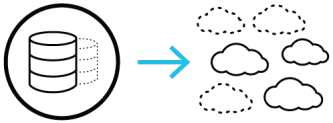
Защита полного жизненного цикла приложений в облаке.
Для любых облачных и виртуальных сред

paloalto NETWORKS

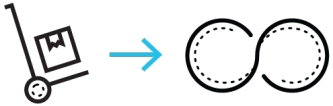
Облака модернизируют цикл разработки ПО



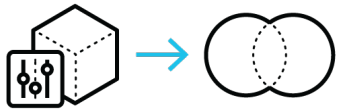
Переход от Waterfall- к Agile-модели



Монолитная архитектура к использованию микросервисов

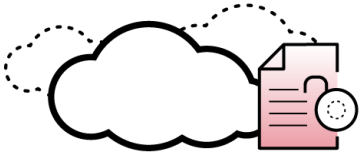


Выпуск пакетов к DevOps



Нишевое использование облаков к Общей Модели Эксплуатации

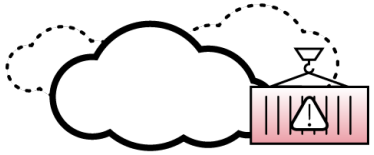
Вместе с инновациями приходят и новые проблемы



Небезопасные конфигурации

42%

шаблонов развертывания небезопасны



Уязвимые настройки по умолчанию

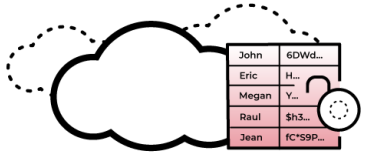
51%

доступных извне контейнеров Docker используют небезопасные значения по умолчанию

Уязвимости узлов и платформ

24%

доступных извне облачных узлов имеют известные уязвимости



Несоответствие требованиям

43%

облачных баз данных не используют шифрование

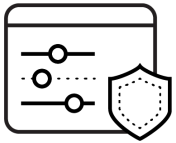
источник: Исследование лаборатории Palo Alto Networks Unit 42

Prisma Cloud

Платформа Cloud Native Security охватывающая весь жизненный цикл приложения

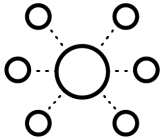
Cloud Security Posture Management

Мониторинг конфигураций, детектирование и реагирование на угрозы, аудит и реализация выполнения требований регуляторов



Cloud Workload Protection

Защита узлов, контейнеров и бессерверных вычислений на протяжении всего жизненного цикла приложения



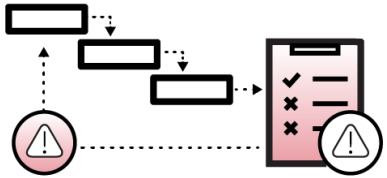
Cloud Network Security

Картина происходящего в сети, микросегментация, глубокая инспекция трафика и реализация зон безопасности

Cloud Infrastructure Entitlement Management

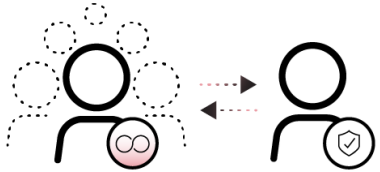
Реализация политик использования учетных записей в облачных и контейнерных средах

Необходим интегрированный и всеохватывающий подход



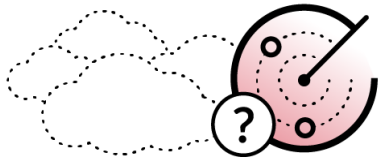
Контроль безопасности на протяжении всего жизненного цикла разработки

Безопасность должна быть интегрирована и автоматизирована, а не быть последующим дополнением



Сотрудничество команд DevOps & Security

Больше версий ПО не значит, что можно экономить на безопасности



Изменения – единственная константа

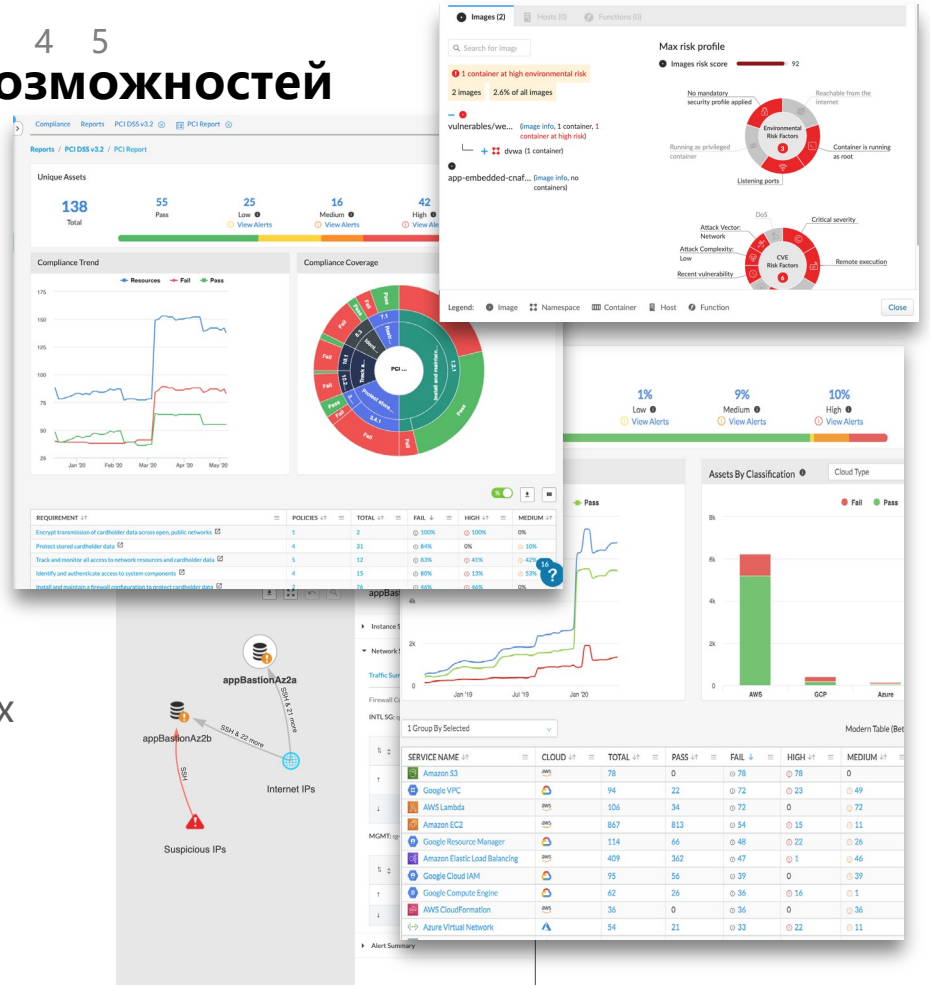
Облачные среды постоянно развиваются и являются изменчивыми

5 причин по которой заказчики выбирают Prisma Cloud Enterprise

1. Комплексный подход, функциональность и высокая интеграция
2. Работа с ПО на всем его жизненном цикле
3. Поддержка любых облачных платформ и сред
4. Зарекомендовавшая себя эксплуатационная методология
5. Единая ценовая модель

Интеграция лучших в индустрии возможностей

- Учет активов и инвентаризация
- Аудит и оценка конфигураций
- Оценка соответствия требованиям
- Сканирование инфраструктуры и образов на уязвимости
- Детектирование сетевых аномалий
- User Entity Behavior Analytics (UEBA)
- Классификация данных и DLP
- Обнаружение известного и неизвестного вредоносного кода
- Использование алгоритмов машинного обучения, динамического анализа, данных кибер разведки для обнаружения подозрительной активности и вредоносного кода
- Автоматическое исправление и реакция
- и много другое



Prisma Cloud – Полный жизненный цикл, полный стек, любые облачные платформы

Поддержка всех облачных сред и стеков

Интеграция с DevOps	Bitbucket, circleci, GitHub, GitLab, HashiCorp, Jenkins, VS Code
Вычислительные платформы	AWS Fargate, AWS Lambda, Azure Kubernetes Service (AKS), docker, Kubernetes, Google Kubernetes Engine, OPENSHIFT
Размещение данных (SaaS)	NAM, EU, CHINA, AU, Coming soon (SIN, CAN, ...)
Публичные облачные платформы	Alibaba Cloud, aws, Azure, Google Cloud
Варианты развертывания	SaaS, Self-managed (*Compute Edition), FedRAMP In process

Доказанная экспертиза при развертывании и эксплуатации

Структурированная методология & эксперты для помощи в развертывании и внедрении

Проверенный вместе с **1500+ заказчиков** процесс внедрения, чтобы помочь Вам быстрее вернуть инвестиции (return on investment, ROI)

Доступ к **100+** экспертам Customer Success (CS) experts для ускорения трансформации продукта в ценность для Вашей компании

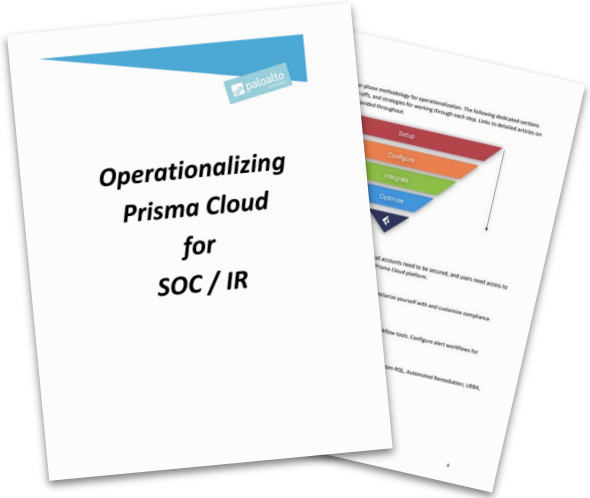
Обеспечение **лучших практик внедрения** при интеграции с Вашей существующей инфраструктурой безопасности

Команда Prisma CS **делится с Вами расширенной экспертизой** посредством ежегодных оценок состояния, планов по оптимизации

Установка → Настройка → Интеграция → Оптимизация

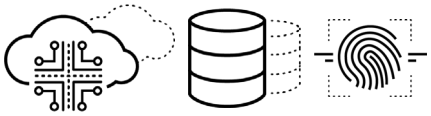
Ощутимый результат менее, чем за **60 дней**

Персонализированные руководства по эксплуатации, чтобы выстроить корректные процессы



Детектирование аномалий на базе Машинного обучения, данных Кибербразведки и учета контекста

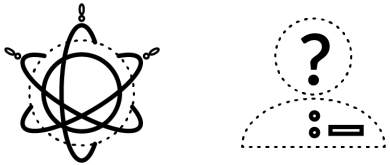
Мгновенное обнаружение критичных проблем с высоким уроном



Источники данных:
Логи IaaS/PaaS, логи о пользователях, логи хранилищ данных, логи сетевого трафика

Threat Intelligence/Кибербразведка:
Вредоносные/подозрительные IP-адреса, сигнатуры вредоносного кода, интеграция со сторонними инструментами

Продвинутых анализ:
Машинное обучение, статическое моделирование, анализ графов, обработка естественного языка



Обнаружение угроз:
Продвинутый анализ данных из различных источников и данные кибербразведки для **детектирования известных и неизвестных угроз**

Простая модель лицензирования

1 SKU = 100% гибкость

PRISMA CLOUD

CLOUD SECURITY POSTURE MANAGEMENT	CLOUD WORKLOAD PROTECTION	CLOUD NETWORK SECURITY	CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT

КОНТЕЙНЕРЫ	ВИРТУАЛЬНЫЕ МАШИНЫ	БЕССЕРВЕРНЫЕ ВЫЧИСЛЕНИЯ

192 | © 2020 Palo Alto Networks, Inc. All rights reserved.

Prisma Cloud

Защищает большинство облачных рабочих нагрузок приложений

70%
списка Fortune 100
используют Prisma Cloud

1800+
заказчиков доверяют Prisma Cloud

1M+
рабочих нагрузок защищено

1.8млрд+
ресурсов отслеживается

5млрд+
логов аудита обрабатывается еженедельно

~200TB
логов о трафике обрабатывается еженедельно

Prisma Cloud

Заказчики по всему миру доверяют нам в защите их инфраструктур

ФИНАНСОВЫЙ СЕКТОР	PayPal, citi, TIAA, DISCOVER, USAA
ВЫСОКИЕ ТЕХНОЛОГИИ	cisco, aws, BROADCOM, DELL EMC, IBM
ЗДРАВООХРАНЕНИЕ	aetna, CENTENE Corporation, OPTUM, McKESSON, Anthem
МЕДИА И РИТЕЙЛ	Disney, Starbucks, Carnival, Red Bull, sky, Nike
ГОСУДАРСТВЕННЫЕ ОРГАНЫ	NASA, U.S. Department of Homeland Security, GSA, U.S. Army, U.S. Air Force, CDC, NIH
ПРОИЗВОДСТВО И ТЕЛЕКОМ	Charter, ExxonMobil, MAERSK, verizon, AT&T, Honeywell

Prisma SaaS

Решение **Cloud Access Security Broker (CASB)** для управления доступом к Вашим облачным приложениям

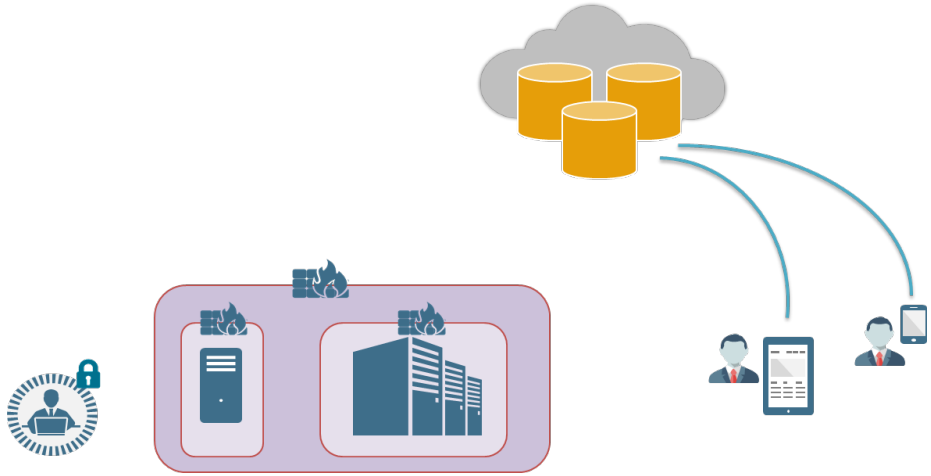
paloalto NETWORKS

Переворот в ЦОД

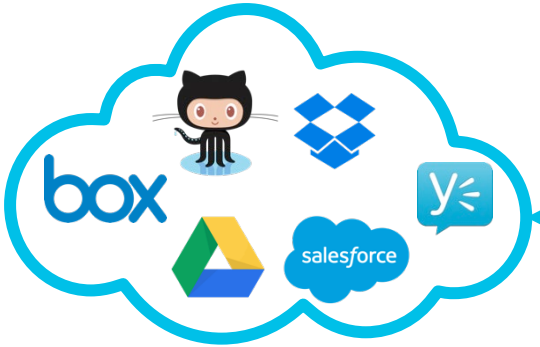
Традиционные границы смещаются

Новые вызовы

- Данные SaaS располагаются ВНЕ периметра компании
- IT-отдел теперь не контролирует кто и как получает к ним доступ
  - Теперь с SaaS контроль лежит в руках пользователя
- Традиционные меры контроля не позволяют видеть куда сохраняются данные и кто имеет к ним доступ
- SaaS приложения для хранения данных (Google Drive, Yandex Disk, Dropbox и т.д.) могут «работать» как отличные «системы распространения вредоносного кода»



Темная сторона SAAS



Санкционированные приложения

Быстрое развертывание с минимальными затратами

Бесконечное масштабирование

Несанкционированные приложения

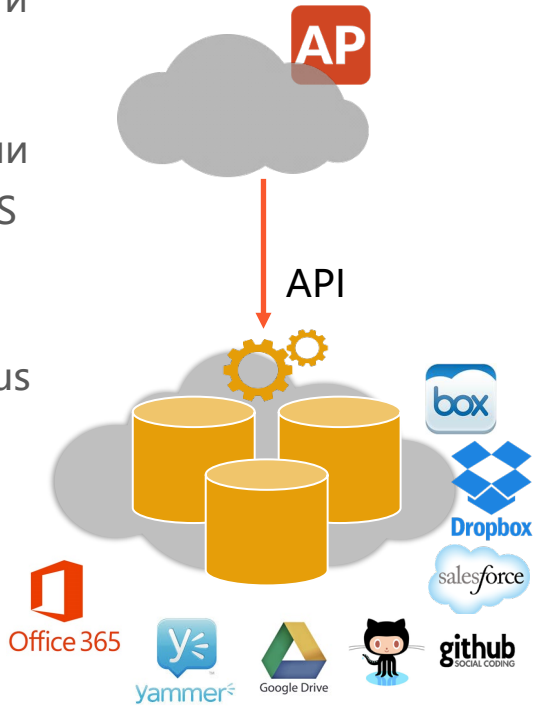
Нарушают требования и политики

Утечка корпоративных данных

Распространение вредоносного кода

Prisma SaaS для решения всех этих проблем

- Защищает данные в SaaS-приложениях от вредоносного кода и утечек, обнаруживает и блокирует несанкционированные приложения
- Анализирует пользовательскую активность, выявляет аномалии
- Не требует изменений в сети или на хостах – интеграция с SaaS через API
- Очень быстрое внедрение
- Дополнительных действий по интеграции с WildFire и Autofocus не требуется – работает из коробки
- Постоянный и ретроспективный мониторинг
- Поддержка Amazon S3, Box, Cisco Webex Teams, Citrix Sharefile, Confluence, Dropbox, GitHub, Gmail, Google Cloud Platform, Google Drive, G Suite Marketplace, Jive, Microsoft Azure Storage, Microsoft Exchange, Office365, Salesforce, Slack for Enterprise, ServiceNow, Workplace by Facebook, Yammer
- Список поддерживаемых приложений все время расширяется*



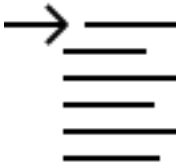
docs.paloaltonetworks.com/prisma/prisma-saas/prisma-saas-admin/secure-cloud-apps/supported-saas-applications.html

Что увидела Prisma SaaS?

Конфиденциальные данные доступны извне

Распространение вредоносного кода

Доступ к исходных кодам ПО



Терабайты пиратских копий фильмов

Что на счет Shadow-IT?

ПРОЗРАЧНОСТЬ

Приложения, пользователи, категории и статистика

АНАЛИЗ

Объемы и направление движения данных, вредоносного кода и угроз

ПРИМЕНЕНИЕ ПОЛИТИК

Детальные политики на основе функций

Полезные ссылки

- Детектируемые приложения – Applipedia
- База атак – Threat Vault
- Проверка категорий URL

Спасибо!

paloaltonetworks.com

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