Подробнее о SASE, CASB, ZeroTrust и как хакеры видят вашу организацию

Вебинары: panacademia.ru/webinars/

Денис Батранков
консультант по
новым стратегиям безопасности
Palo Alto Networks Russia/CIS

Вопросы и предложения
Russia@paloaltonetworks.com

Цифровая трансформация

Технологии нового поколения для защиты

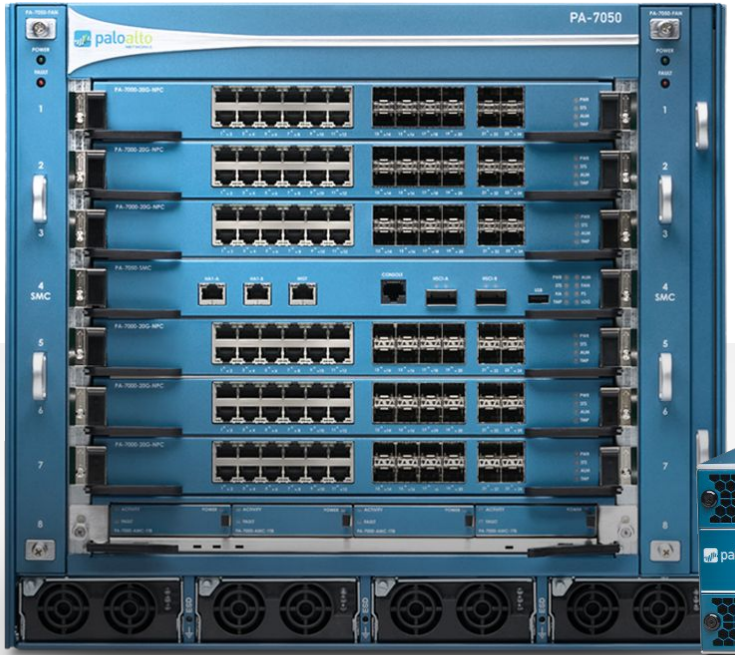
Palo Alto Networks исследует новые технологии и реализует их для защиты компаний

NEXT-GENERATION FIREWALL

Docker и Kubernetes

VM-Series

PA-7000 SERIES



ЗАЩИТА

СКОРОСТЬ

УДОБСТВО

PA-5200 SERIES

PA-800 SERIES

PA-220

PA-3200 SERIES

Каналы связи

Приложения

Люди

Каналы связи

STRATA™
BY PALO ALTO NETWORKS

Products

- Next-Generation Firewall
- Threat Prevention
- DNS Security
- Wildfire
- URL Filtering
- GlobalProtect
- Panorama
- 5G & IoT
- Zero Trust
- SD-WAN

Приложения

PRISMA™
BY PALO ALTO NETWORKS

Products

- Prisma Access
- Prisma SaaS
- Prisma Cloud
- VM-Series
- VM-Series on AWS
- VM-Series on Azure
- VM-Series on Alibaba Cloud
- VM-Series on Oracle Cloud
- VM-Series on Google Cloud
- VM-Series on VMware ESXi/vCloud Air
- VM-Series on VMware NSX

Люди

CORTEX™
BY PALO ALTO NETWORKS

Products

- Cortex XDR
- Cortex Data Lake
- Traps
- Autofocus
- Demisto

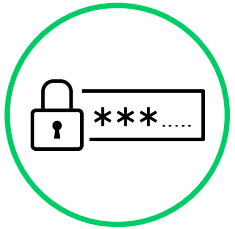
Блокировка украденных паролей

Конфиденциальные данные в компании

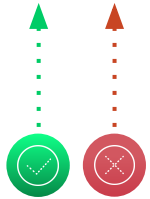
Платформа

Ping ID RSA okta SafeNet DUO Entrust

Multi-Factor Authentication



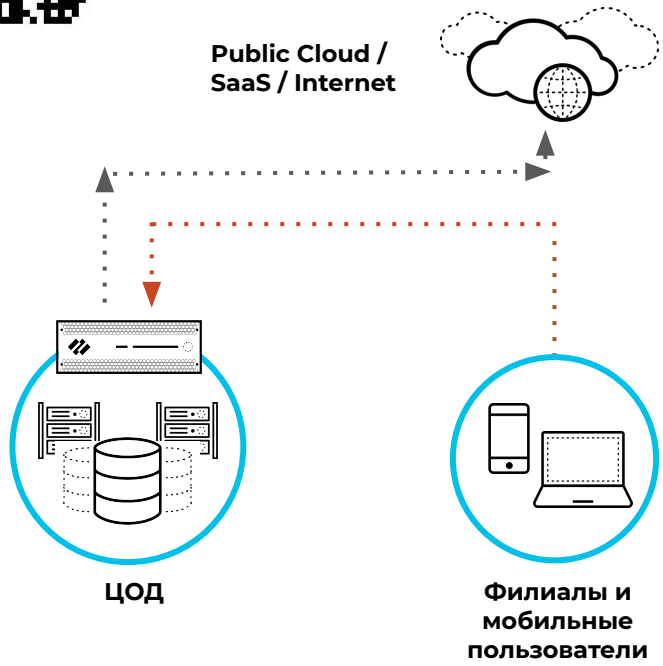
Пароль сотрудника



Украденный пароль

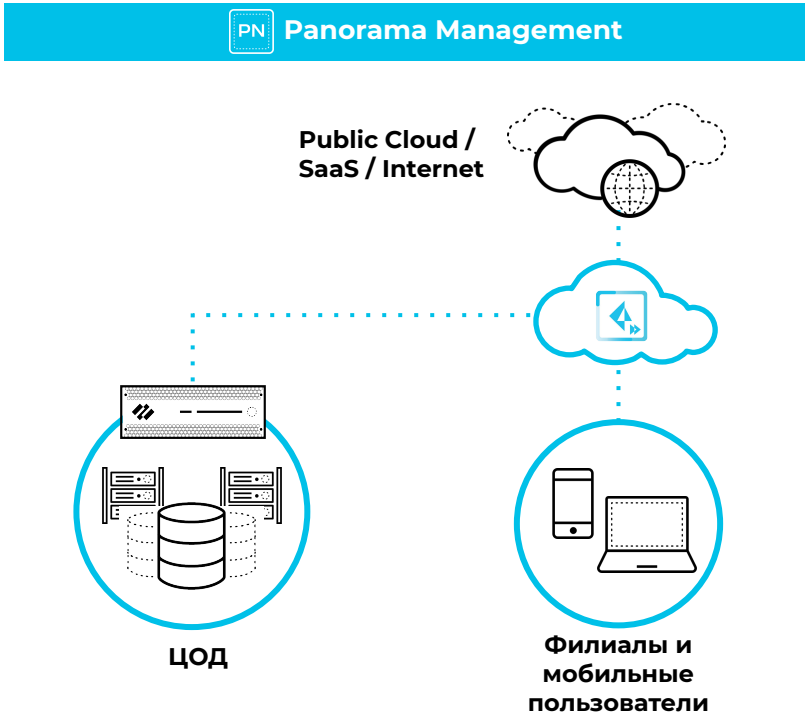
Новая архитектура применения защиты SASE – Secure Access Service Edge

Recommended Subscriptions: TP UF WF DNS GP



Старая

VPN трафик идет всегда через ЦОД



Новая

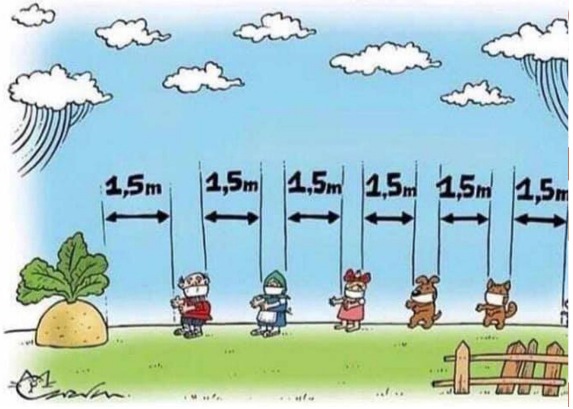
VPN идет через Prisma Access SASE и распределяется в ЦОД, в облака и общедоступный Интернет

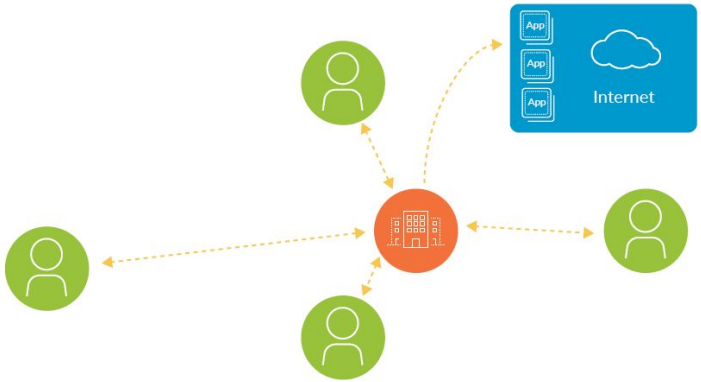
Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
ms-rdp	4	196.2G	11.2k	0	0	0	240
ssl	4	259.5G	925.0k	7.4k	0	742.1k	238
web-browsing	4	8.2G	109.2k	383	230	316.7k	225
mail.ru-base	4	1.8G	62.9k	0	0	1.5k	145
facebook-base	4	1.0G	8.5k	0	0	0	141
google-cloud-storage-download	2	49.3M	438	2	0	0	120
youtube-base	4	1.5G	8.7k	0	0	8.7k	114
yandex-maps	1	846.6M	5.9k	0	0	1	95
google-play	3	169.8M	10.9k	0	0	10.9k	88
ms-teams	2	40.3M	869	0	0	868	81
windows-azure-base	1	66.0M	1.9k	0	0	144	78
twitter-base	3	26.5M	717	0	0	0	74
vkontakte-base	4	286.7M	8.0k	0	0	0	61
outlook-web-online	3	186.6M	4.4k	0	0	2.3k	52
instagram-base	2	239.9M	2.8k	0	0	0	48
ms-onedrive-base	4	25.6M	1.2k	0	0	876	46
pinterest-base	2	38.3M	374	0	0	0	39
ms-office365-base	2	16.0M	400	0	0	399	37
itunes-base	3	58.0M	1.4k	0	0	1.2k	37
gmail-base	4	279.2M	2.2k	0	0	2.2k	34
teamviewer-base	3	303.5M	687	0	0	18	31
google-drive-web	5	115.1M	255	0	0	264	27
google-docs-base	3	209.9M	673	0	0	674	26

SASE или Prisma Access

Проблема – скорость настройки защиты для всех офисов

Обычно VPN делают для доступа к внутренним ресурсам.





Типовая схема

- А что если много ЦОД?
- А что если узкий канал в офис?
- А что если внезапно много людей?
- А как увидеть кто что делает?
- А что с безопасностью?

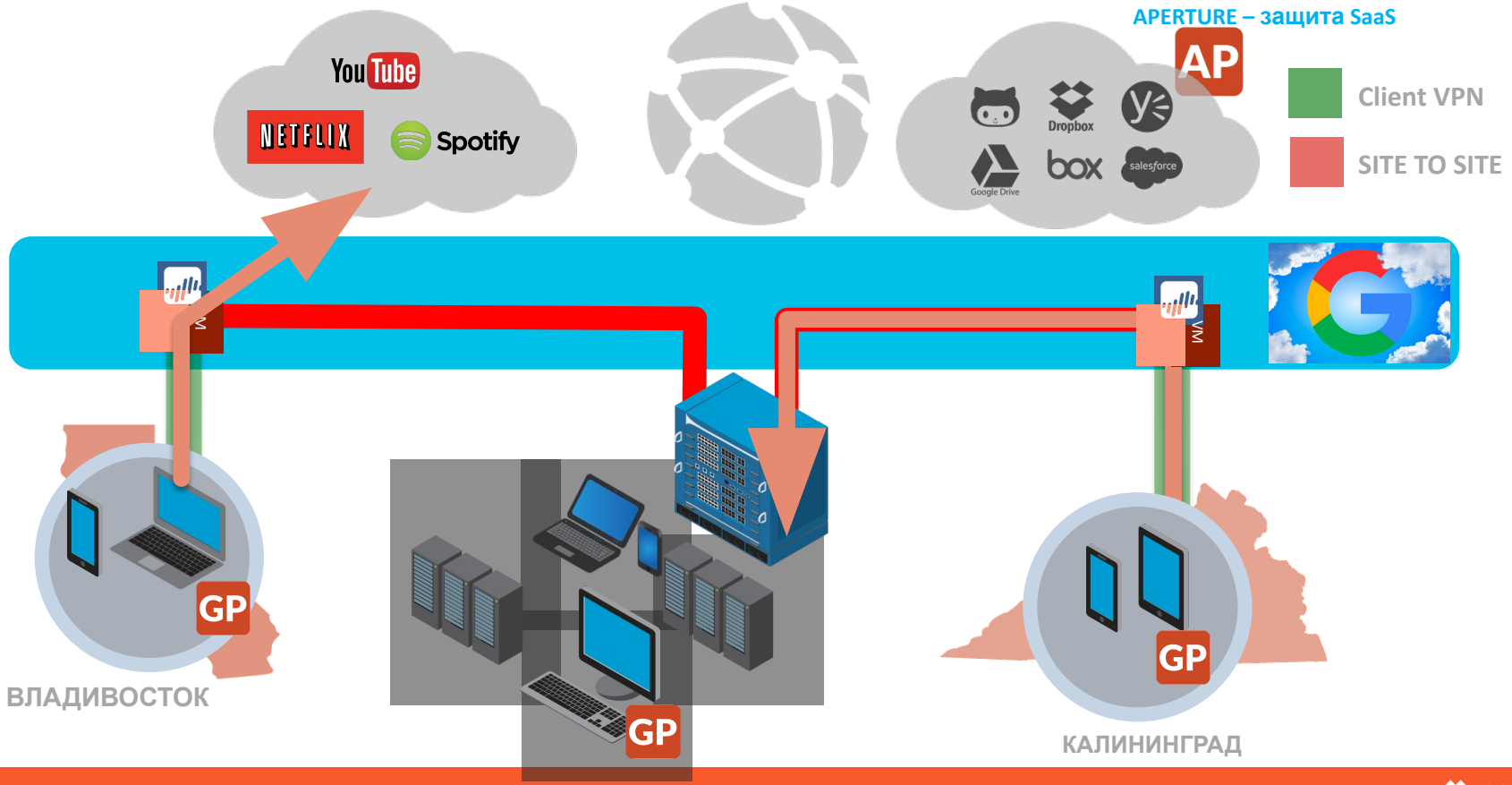
В чем риск создания VPN канала с домашнего компьютера в сеть компании

- Его сразу можно рассматривать как взломанный. Это значит, что есть риск что
  - Вместе с сотрудником по VPN зайдет и хакер
  - Хакер может получить логин/пароль для доступа и другие пароли сотрудника: почта, банки
  - Хакер может перехватывать нажатия клавиш, изображение экрана и звук рядом с компьютером
  - Хакер может производить соединения в сеть компании с домашнего компьютера, пока сотрудник зашел по VPN
  - Хакер может атаковать других сотрудников через локальную почту от имени этого сотрудника
  - Хакер может атаковать других сотрудников по открытым портам в сети: сеть Микрософт, веб-порталы и др.
  - Смартфон или компьютер могут украсть и получить доступ к данным локально

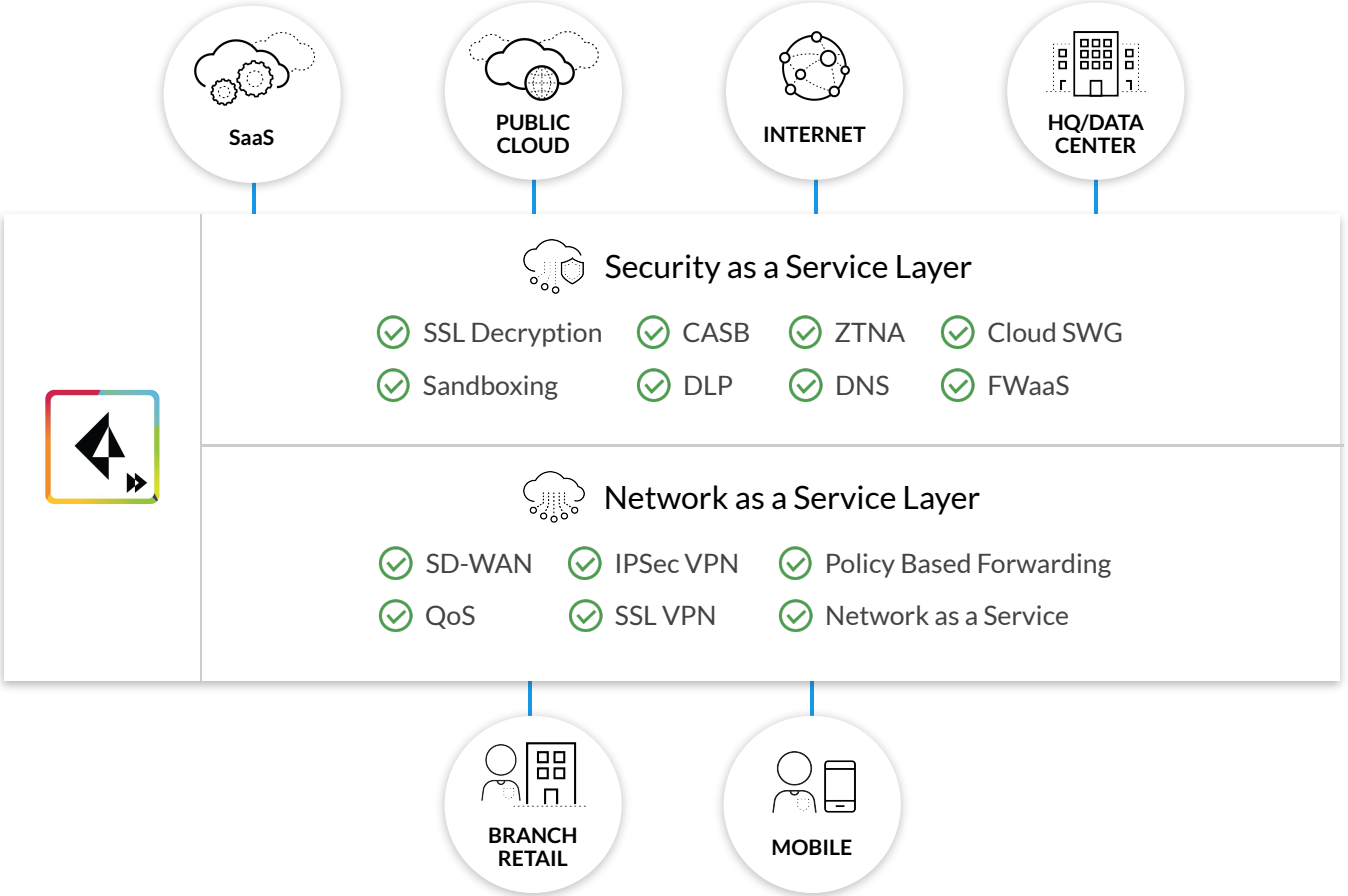
- Zero Trust: нулевое доверие каждому удаленному сотруднику, в том числе себе
  - Взять под контроль весь софт на рабочей станции или смартфоне

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

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



Prisma Access – набор всех необходимых сервисов

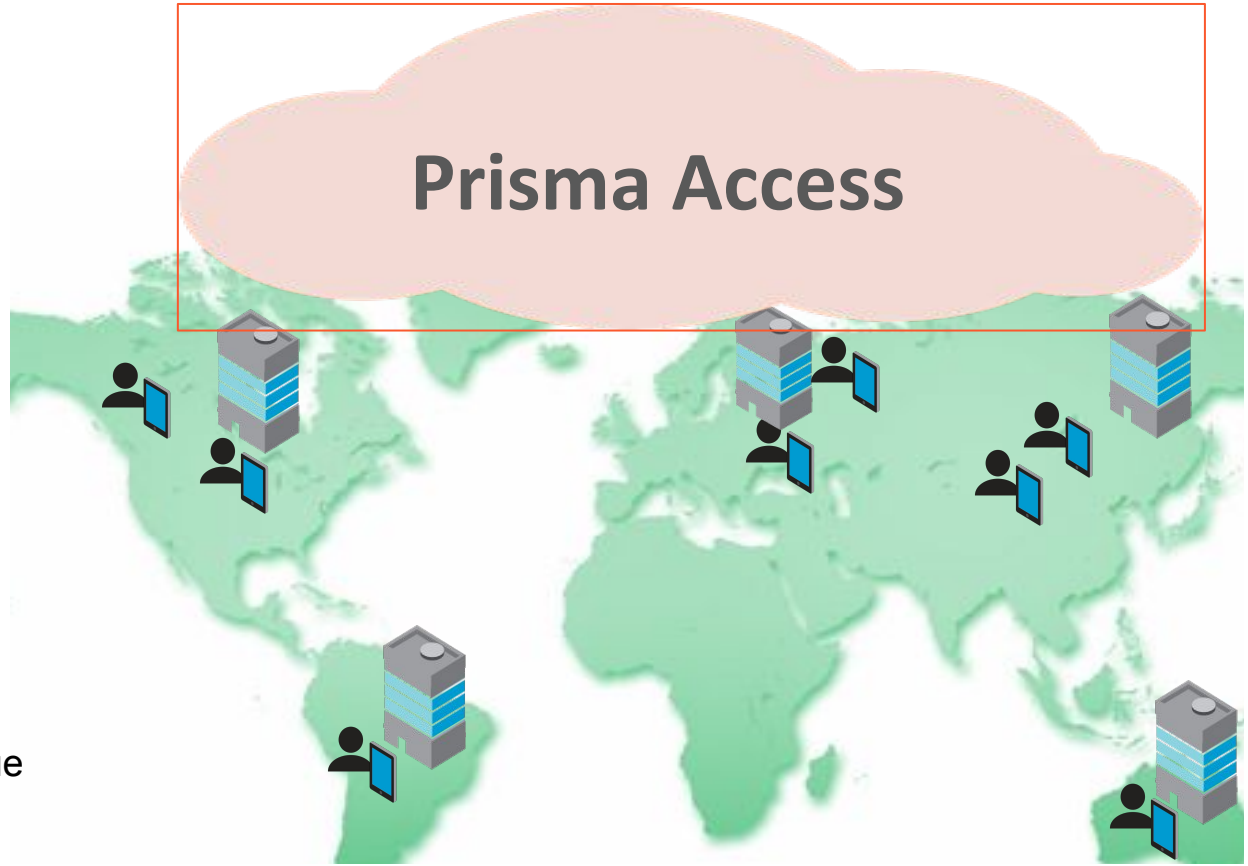


Prisma Access – облачный сервис где, удобно получать нужное число сервисов безопасности, например, VPN

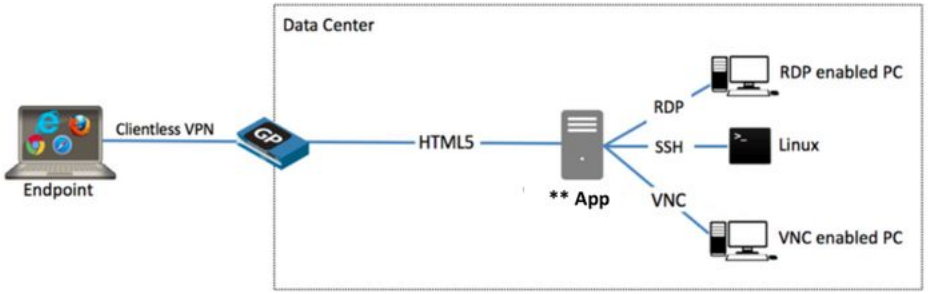
ЦОД Google находится также в России, поэтому шлюзы в России и их может быть сколько угодно с ростом компании

Prisma Access - сервис защищенного доступа

- Содержит уже готовую инфраструктуру
- Все функции безопасности из облака
- Все континенты
- Доступ к любым ресурсам компании
- Централизованное управление через Panorama
- Оплата за скорость канала
- Основана на Google Cloud



Доступ к внутренним приложениям без клиентов: Clientless VPN

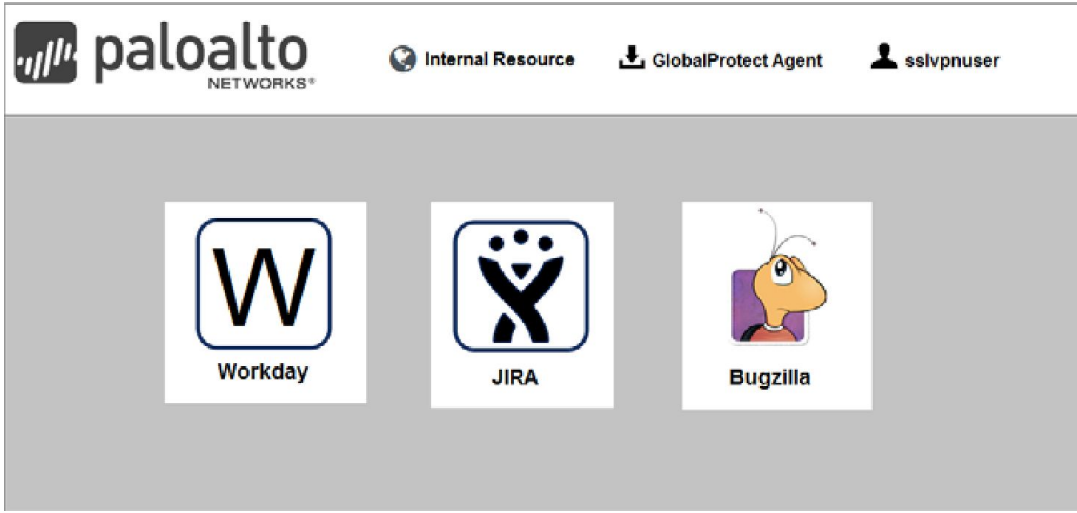


**App – Any VDI you have already deployed in your environment – Citrix VDI, VMware vSphere, vCenter etc. enabled with HTML5 access

Приложения публикуются как URL к соответствующему приложению

Доступен VDI, RDP, SSH и т.д.

Подробнее:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRaCAK

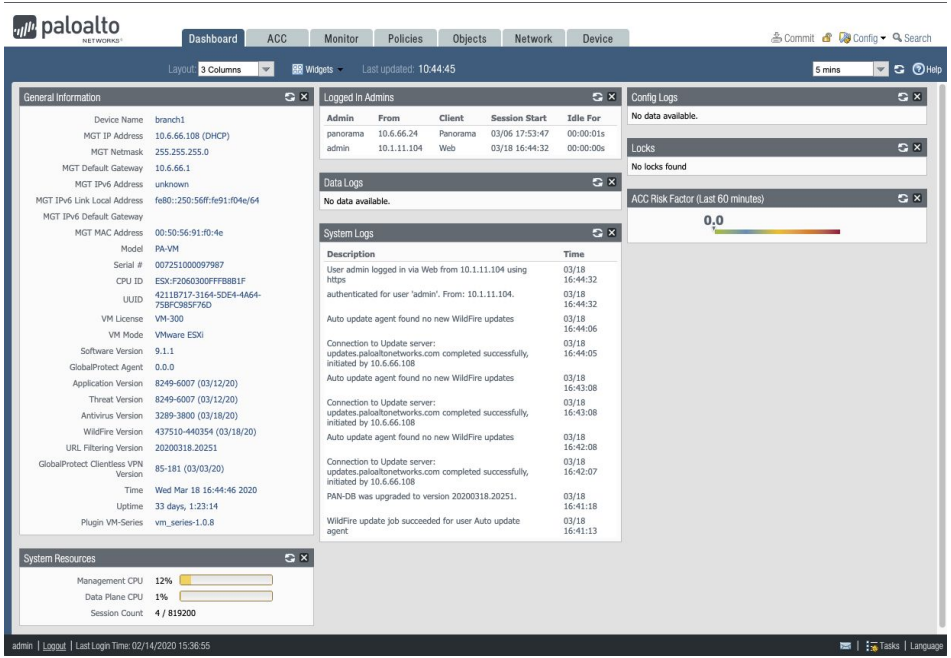


В чем преимущества Palo Alto Networks для бизнеса

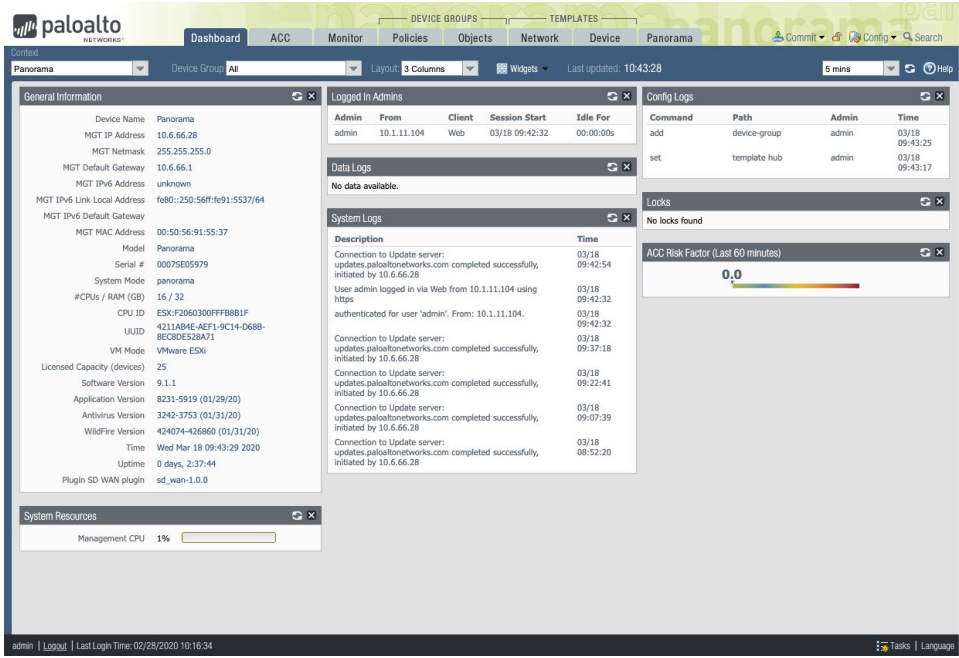
- Легко использовать – подходит для работы любых приложений
- Постоянство производительности – даже если появились новые функции
- Глубже настройки по тому что и как защищать – больше критериев проверки, наличие динамических групп и возможность включить все проверки одновременно
- Обучение и утилиты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

Встроенная система управления NGFW и Panorama выглядят одинаково

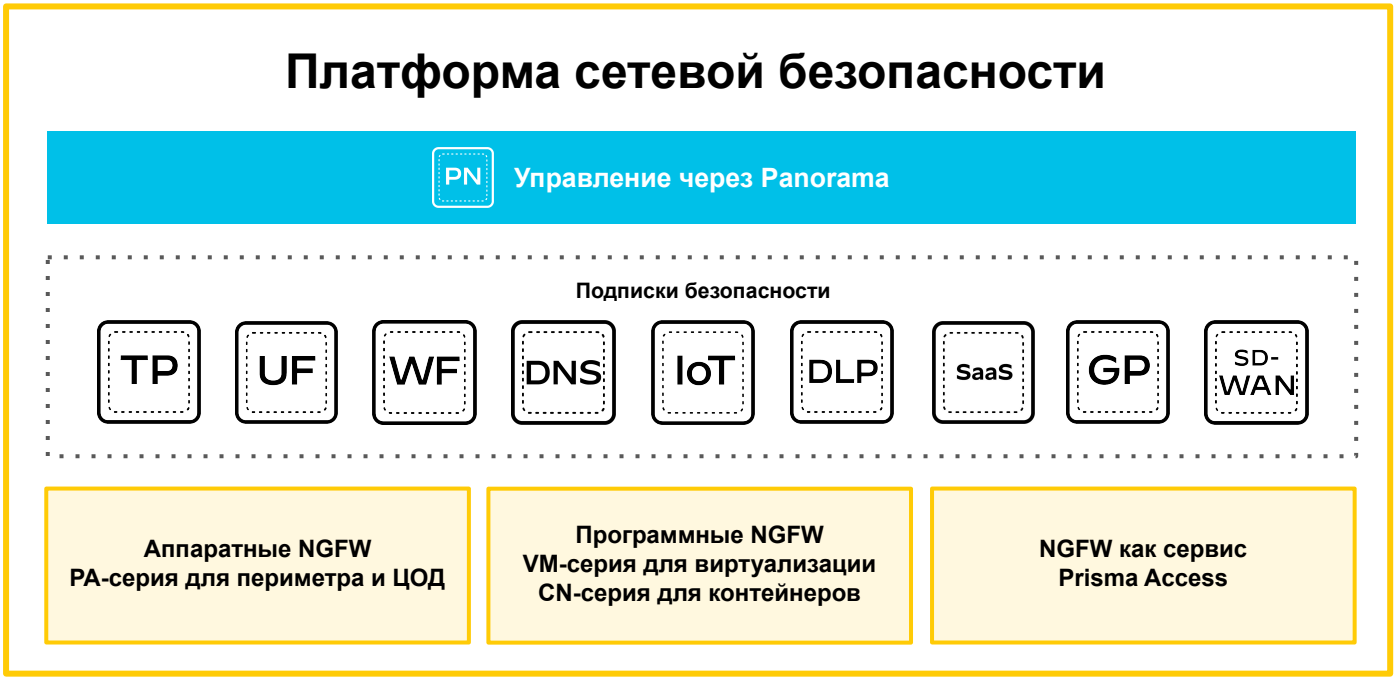
NGFW



Panorama



Все функции безопасности в единой платформе



Использовать разное или одну платформу?

Функционал (примеры)	Разное	Платформа
Firewall	Check Point	
Intrusion Detection	TREND MICRO	
URL Filtering	Symantec	
Sandbox Detection	FIREEYE	
Remote Access for Users	CISCO	paloalto NETWORKS
Endpoint + EDR Security	McAfee	
Public Cloud Security / Compliance	netskope	
Secure Web Gateway	zscaler	
SaaS Security / SaaS Compliance	Dome9 SECURITY	
SD-WAN	velocloud	

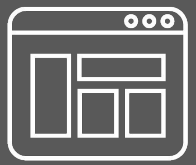
А как проверить ошибки настройки?

БЕСПЛАТНЫЕ УТИЛИТЫ ДЛЯ ПОМОЩИ В НАСТРОЙКЕ БЕЗОПАСНОСТИ

Security Lifecycle Review
Визуализирует что творится в сети

Expedition Migration Tool
Помогает конвертировать конфигурации и помогает писать правила на основе анализа трафика

Best Practice Assessment
Сравнивает конфигурацию с лучшими конфигурациями



Prevention Posture Assessment
Оценивает как работает предотвращение

Heatmap: насколько верно реализованы правила

Утилита показывает процент правил, где включены функции безопасности

paloalto NETWORKS | Trending | Device Group | Serial Number & Vsys | Zones | Zone Type | Area of Architecture | Tags | Rule Detail | Go to Best Practice Assessment | Security Policy Capability Adoption Heatmaps

Documentation / Help

Column Filters

				WildFire	Threat Prevention (IPS)				URL-Filtering						
Device Group	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
DC1	250	250	0	74.4	74.4	0.0	74.4	74.4	0.0	74.4	0.0	12.8	0.0	0.0	100.0
DC2	32	32	0	87.5	87.5	0.0	87.5	87.5	0.0	87.5	0.0	100.0	0.0	0.0	100.0
DC3	32	32	0	87.5	87.5	0.0	87.5	87.5	0.0	87.5	0.0	100.0	0.0	0.0	100.0
Perimeter	11	8	3	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	100.0	90.9	100.0	100.0
East-West	5	4	1	50.0	50.0	0.0	50.0	100.0	0.0	50.0	0.0	0.0	80.0	100.0	100.0
HQ	5	5	0	60.0	40.0	0.0	80.0	80.0	0.0	20.0	0.0	20.0	100.0	100.0	100.0
Branch Offices	3	2	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Internal Core	3	2	1	100.0	100.0	100.0	100.0	100.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0
North-South	3	3	0	0.0	0.0	0.0	66.7	100.0	0.0	66.7	0.0	100.0	100.0	100.0	100.0
shared	3	2	1	0.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0
Cloud	2	2	0	50.0	0.0	0.0	50.0	100.0	0.0	50.0	0.0	0.0	100.0	100.0	100.0
Grand Total:	349	342	7	75.4	75.4	0.6	76.3	78.1	2.3	75.4	0.0	31.8	7.7	100.0	100.0

PRISMA
BY PALO ALTO NETWORKS

Prisma Access Zero Trust Network Access (ZTNA)

Денис Батранков

ваш помощник по новым стратегиям безопасности

ISC Certified Information Systems Security Professional, GIAC Certified Incident Handler, PAN Certified Network Security Engineer

Блог safebdv.blogspot.com

Twitter @Batrankov

Youtube bit.ly/bdv-video

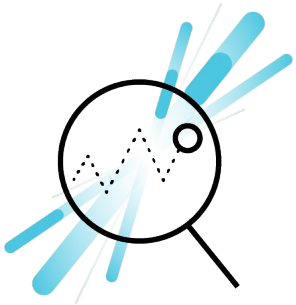
paloalto NETWORKS

Zero Trust Network Access ≠ Zero Trust

Zero Trust *– стратегическая инициатива для появления явного контроля за каждым потоком данных в организации.*

Zero Trust Network Access (ZTNA) *– набор технологий для обеспечения безопасного удаленного доступа к приложениям организации и Интернет согласно принципу минимизации привилегий и контроля безопасности.*

What is ZTNA? Understanding the Challenges

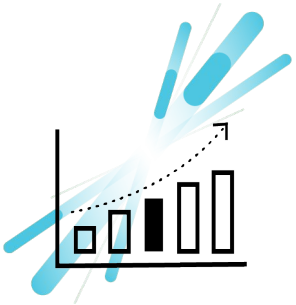


Exposed Services

Services in your datacenters and clouds can be accessed externally by attackers and seen by all users on the network.

Inconsistent Policies

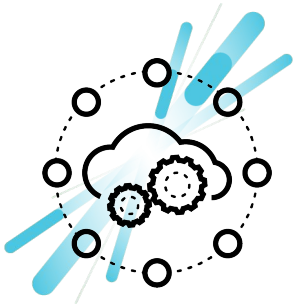
Controlling what remote users can access is inconsistently enforced, difficult to manage, and often differs by location.



Unscalable Remote Access

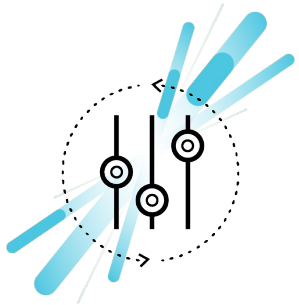
Adding VPN capacity requires hardware deployments and complicated IP management as users and apps change.

Why ZTNA



Scalable Remote Access

On demand, secure remote access that scales as capacity needs change and works with your existing infrastructure.



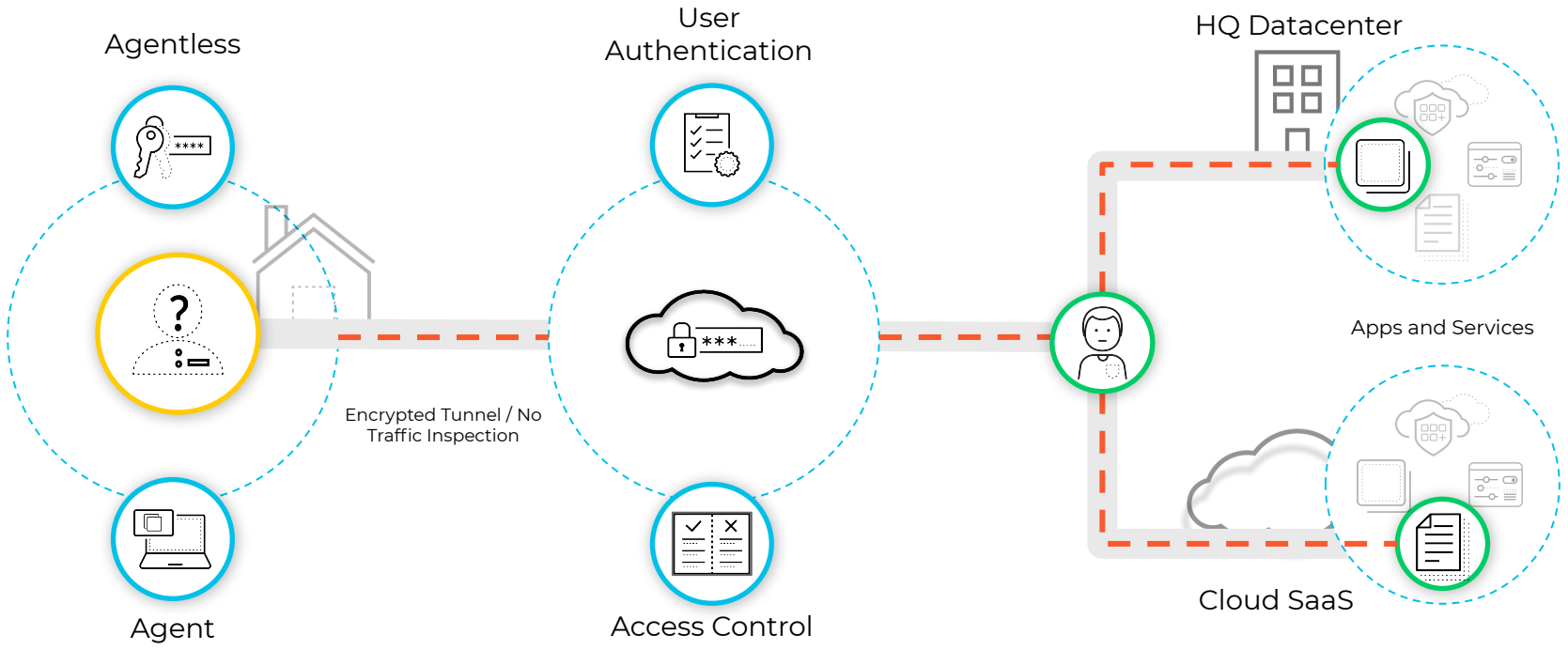
Simplified Management

Centralized policy management and enforcement across your entire enterprise; Monitor and prioritize connections.

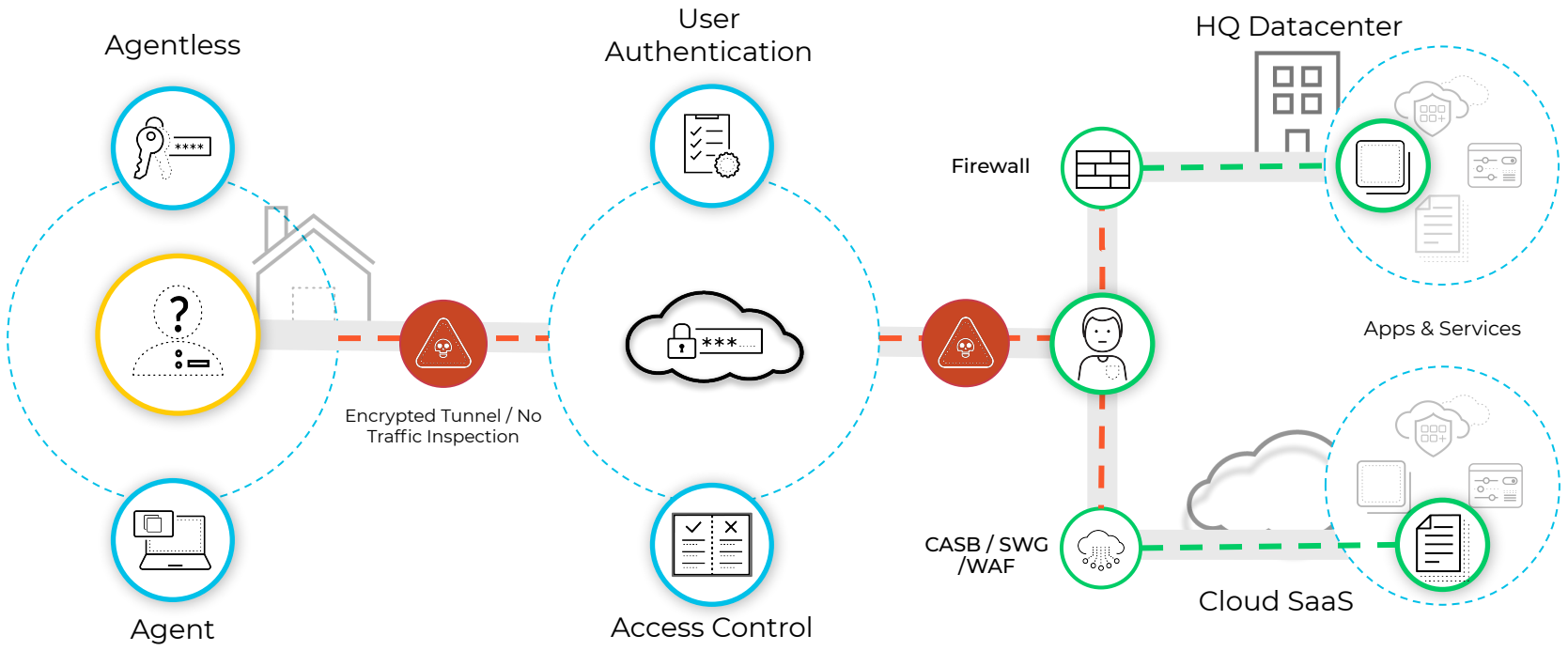
Granular Access Controls

Grant users access to specific applications and services based on their identity, role, location, and device posture.

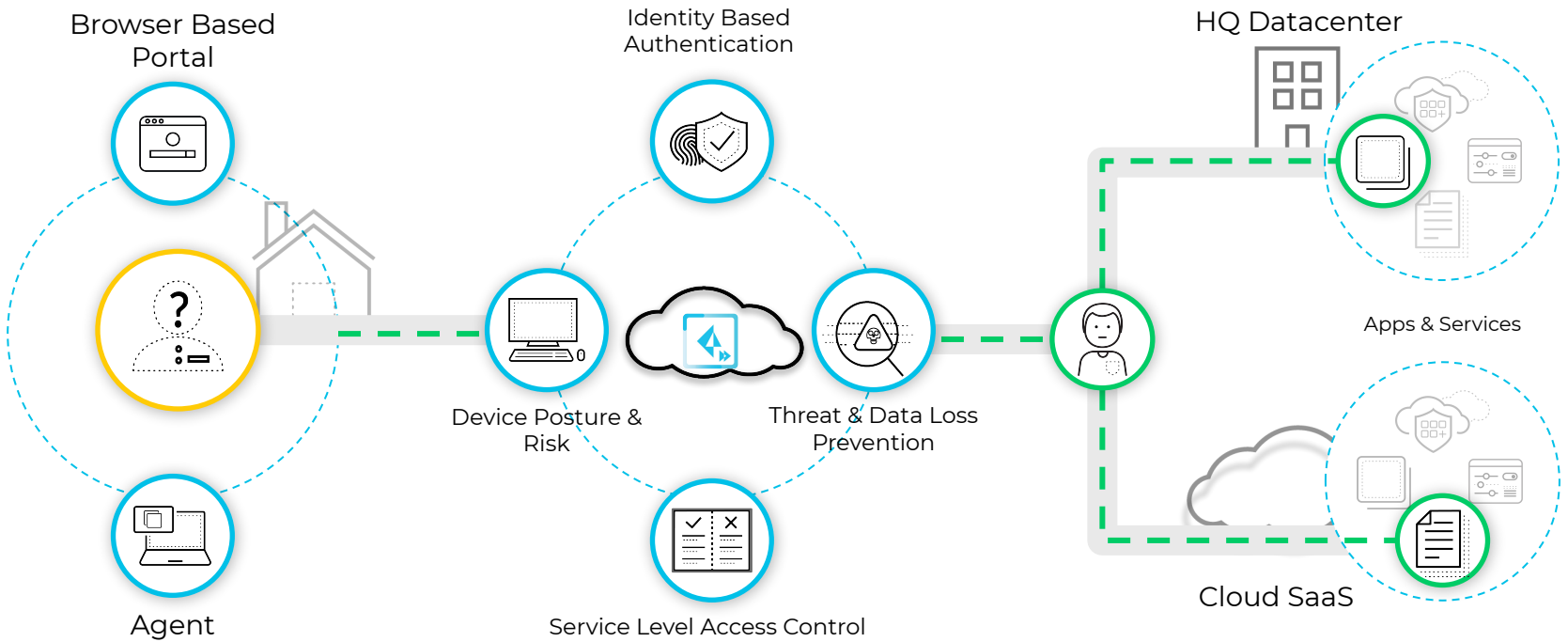
How Traditional ZTNA Works



Traditional ZTNA - Not True Zero Trust



Prisma Access ZTNA: Remote Access & Context Based Policy



 |

GP агент собирает и присылает в Host Information Profile

Log Details

Report Generated	04/18/2018 11:03:17	
User Information	User: mdensley	IP Address: 192.168.77.30
Host Information	Machine Name: SJCWIN65NM662	Domain: paloaltonetworks.local
OS	Microsoft Windows 10 Enterprise , 64-bit	Host ID: af0bbd00-2964-4f50-8ad3-7316a073f3f6
Client Version	4.1.0-98	

Network Information

Interface	MAC Address	IP Address
PANGP Virtual Ethernet Adapter #2	02-50-41-00-00-01	169.254.169.188 192.168.254.3 fe80::55d:e88f:6473:a9bc
Intel(R) Ethernet Connection I217-LM	F8-CA-B8-1C-57-FD	192.168.77.30
Dell GigabitEthernet	9C-EB-E8-2E-23-56	169.254.251.202 fe80::5cd:2d55:c721:fbca
Intel(R) Dual Band Wireless-AC 7260	7C-5C-F8-32-8F-3E	169.254.174.102 fe80::3983:c9ee:6540:ae66
Microsoft Wi-Fi Direct Virtual Adapter	7C-5C-F8-32-8F-3F	169.254.99.238 fe80::2047:93c0:eaee:63ee
VMware Virtual Ethernet Adapter for VMnet4	00-50-56-C0-00-04	192.168.1.40
VMware Virtual Ethernet Adapter for VMnet8	00-50-56-C0-00-08	192.168.202.1
Software Loopback Interface 1		127.0.0.1 ::1
Microsoft Teredo Tunneling Adapter	00-00-00-00-00-00	fe80::100:7f:fffe

Anti-Malware

Software	Vendor	Version	Engine Version	Definition Version	Date	Real Time Protection	Last scanned
Traps	Palo Alto Networks, Inc.	4.1.3.33176	4.1.3.33176	2018.04.18	4/18/2018 ✓		n/a
Windows Defender	Microsoft Corporation	4.12.16299.15	1.1.13000.0	1.227.2644.0	9/19/2016	n/a	09/19/2016 08:26:54

Disk Backup

Software	Vendor	Version	Last Backup
CrashPlan	Code42 Software	4.6.0.403	n/a
Dropbox	Dropbox, Inc.	47.4.74	n/a
Box Sync	Box, Inc.	4.0.7900.0	n/a
Windows Backup and Restore	Microsoft Corporation	10.0.16299.15	n/a
Windows File History	Microsoft Corporation	10.0.16299.15	n/a

Disk Encryption

Software	Vendor	Version
BitLocker Drive Encryption	Microsoft Corporation	10.0.16299.15

Drive	State
C:\	encrypted
E:\	unencrypted

Проверка наличия установки TRAPS на хосте

HIP Object

- General
- Mobile Device
- Patch Management
- Firewall
- Anti-Malware
- Disk Backup
- Disk Encryption
- Data Loss Prevention
- Custom Checks

Anti-Malware

Is Installed — Real Time Protection: yes

Virus Definition Version: Within — Days: 7

Product Version: None

Last Scan Time: Within — Days: 7

1 item

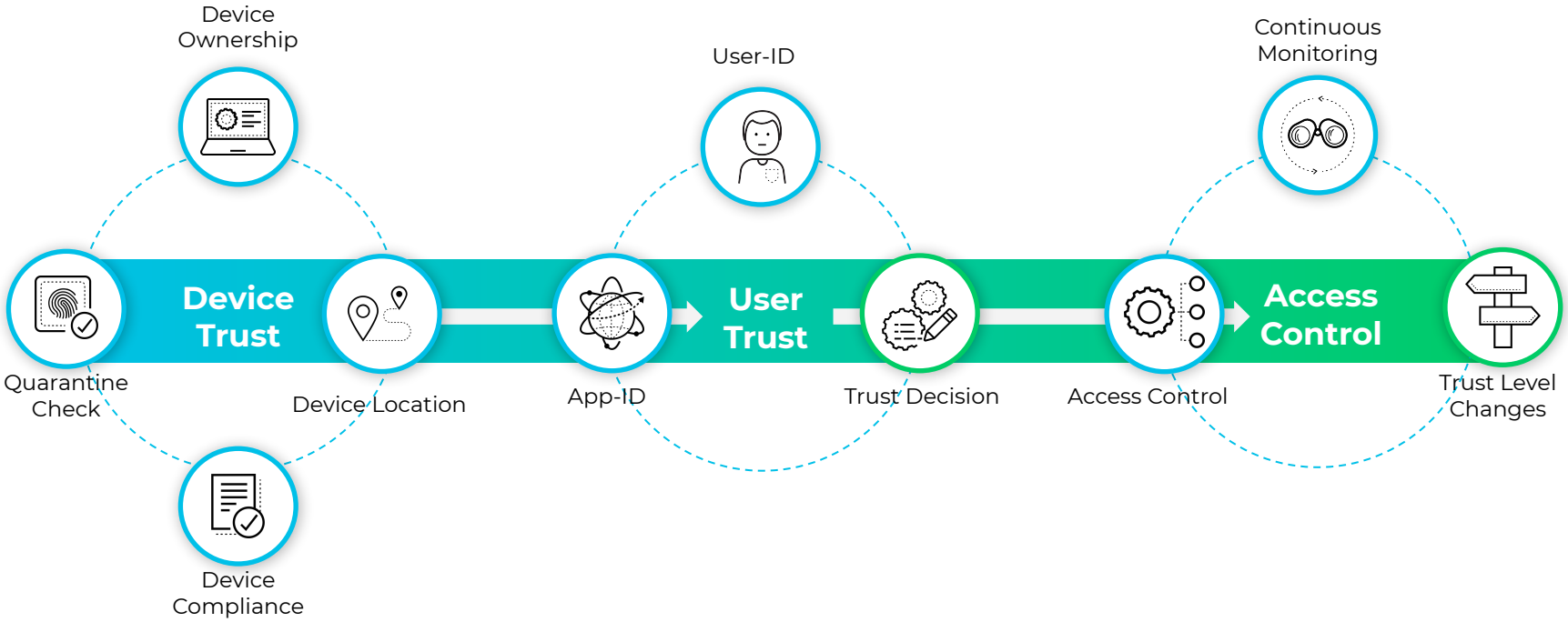
Vendor	Product
Palo Alto Networks, Inc.	Traps

Add Delete

Exclude Vendor

OK Cancel

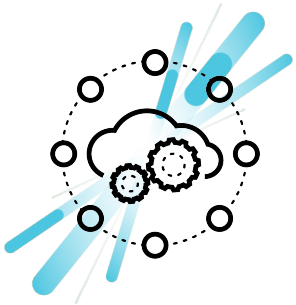
How Prisma Access Performs Trust Assessment



Prisma Access, ZTNA, and VPN Comparison

	Prisma Access ZTNA	ZTNA	Traditional VPN
DLP	✓		
Malware & Exploit Detection	✓		
Credential Theft & Device Risk Assessment	✓		
App & Service Level Access Control	✓	✓	
Centralized Management	✓	✓	
App & Service Cloaking	✓	✓	
Cloud Delivered	✓	✓	
Secure Remote Access	✓	✓	✓
Encrypted Connection	✓	✓	✓

The Value of Prisma Access for ZTNA

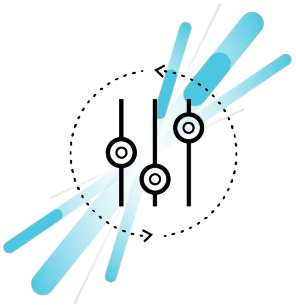


Scalable Remote Access

On demand, secure remote access that scales as capacity needs change and works with your existing infrastructure. Monitor and prioritize connections.

Granular Access Controls & Simplified Management

Grant users access to specific applications and services based on their identity, role, location, and connecting device posture. Centralize policy management and enforcement.

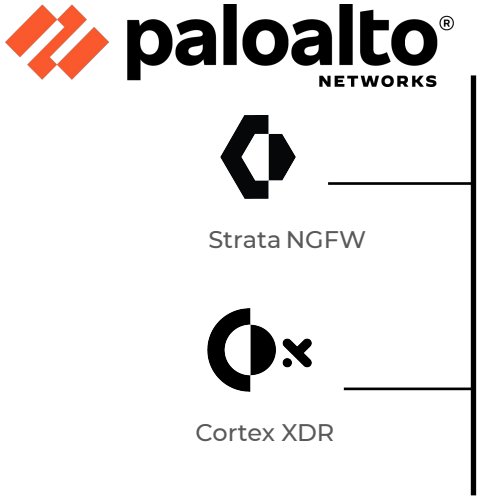


True Zero Trust Implementation

Prevent data theft from compromised user accounts by monitoring user behaviors after they authenticate and have been granted access to an application or service.

А что в комплексе:
многоэшелонированная защита на хосте и сети

Нет шансов для взлома



Cortex XDR предотвращает заражение операционных систем

Блокировка криптолокеров, эксплойтов и бесфайловых атак

Блокировка на основе данных threat intelligence Расследование инцидентов

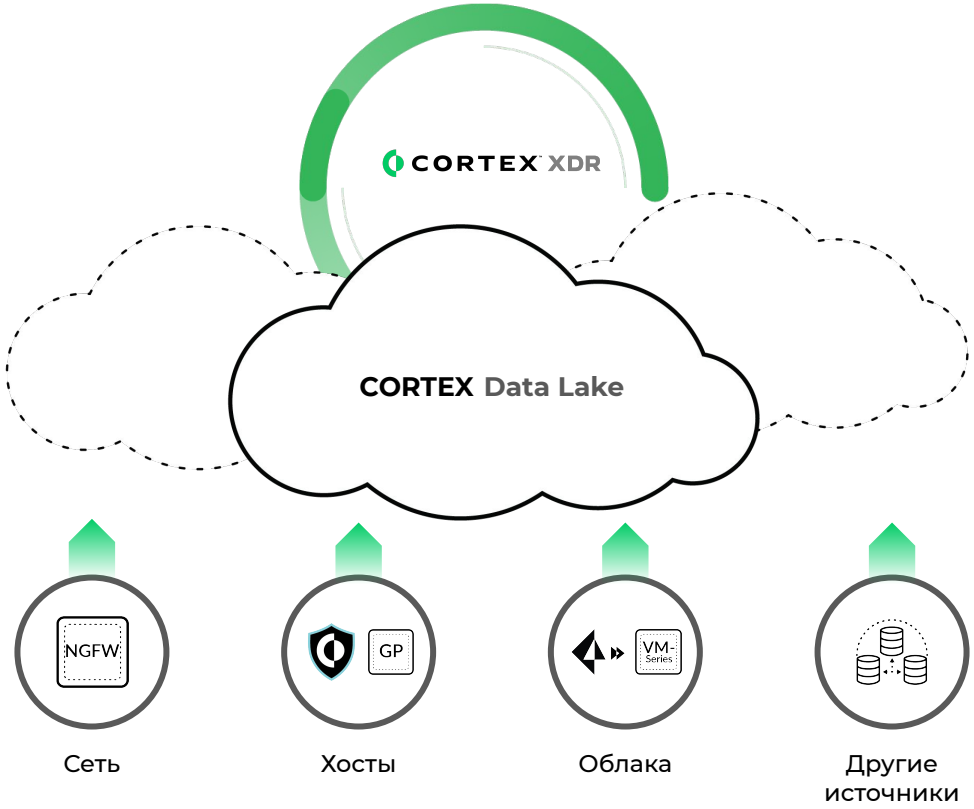
Обнаружение атак на основе machine learning

ADVANCED ENDPOINT PROTECTION

Traps предотвращает неизвестные атаки

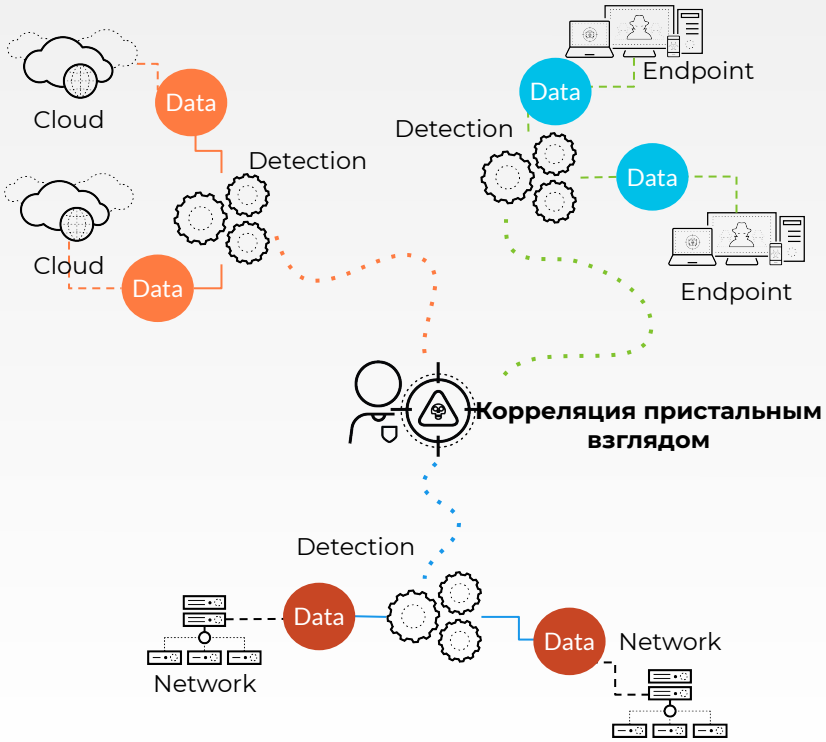
- Без сигнатур
- Без обновлений
- Без знаний об уязвимостях

Важно: Аналитика по всем событиям в сети и облаке

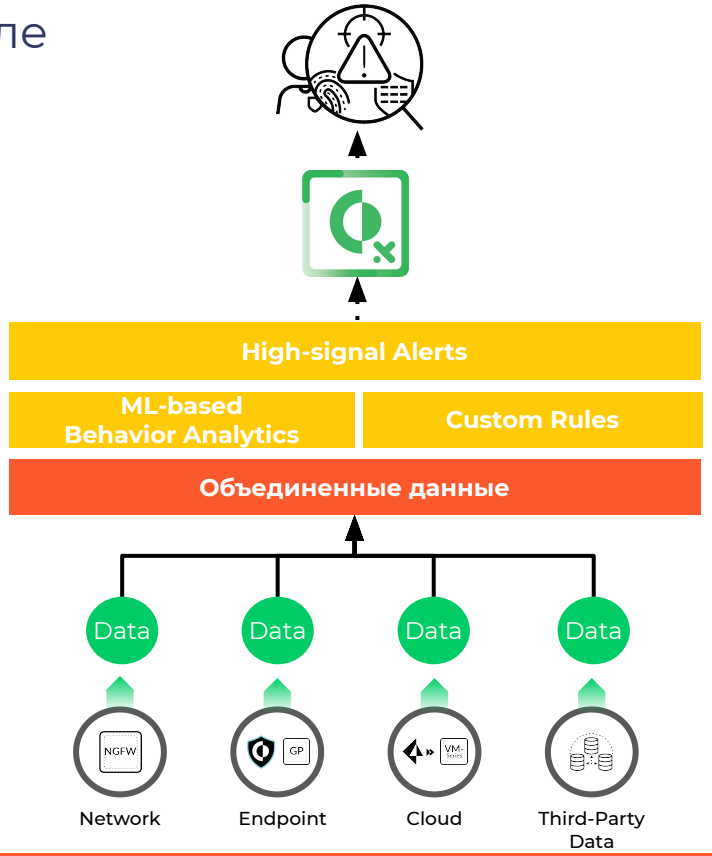


Наш подход: Machine Learning для анализа данных

До



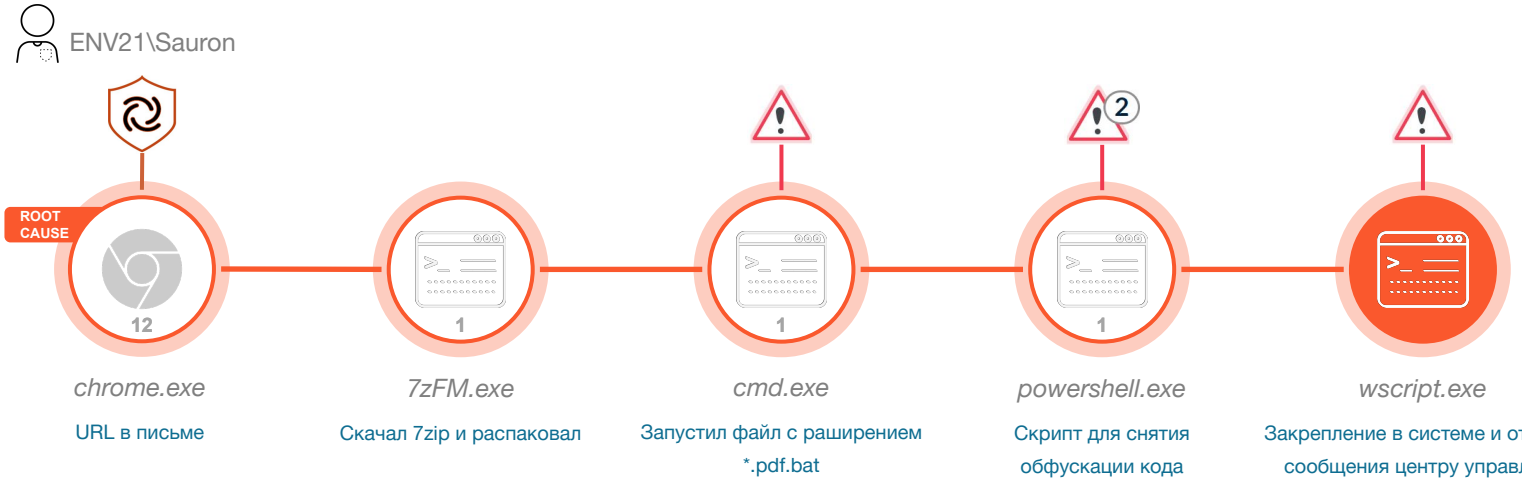
После



Cortex XDR = TRAPS + UEBA + Machine Learning

Предотвращение и расследование инцидентов

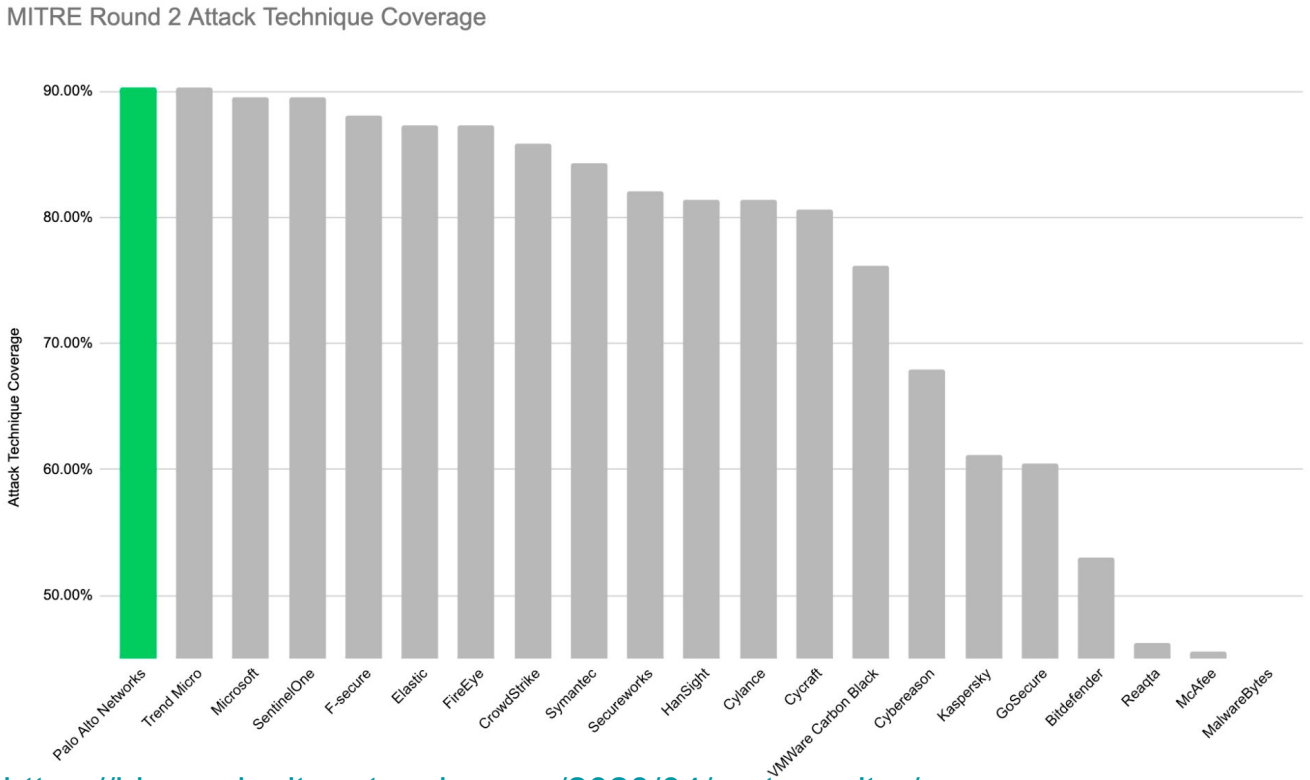
Итог: через XDR сразу видна первопричина события в одном окне



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

Cortex XDR проверен MITRE и является лидером рынка EDR

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



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

Наши партнеры предлагают сервис MDR

Чтобы достичь полного потенциала Cortex XDR нужны правильные настройки и люди

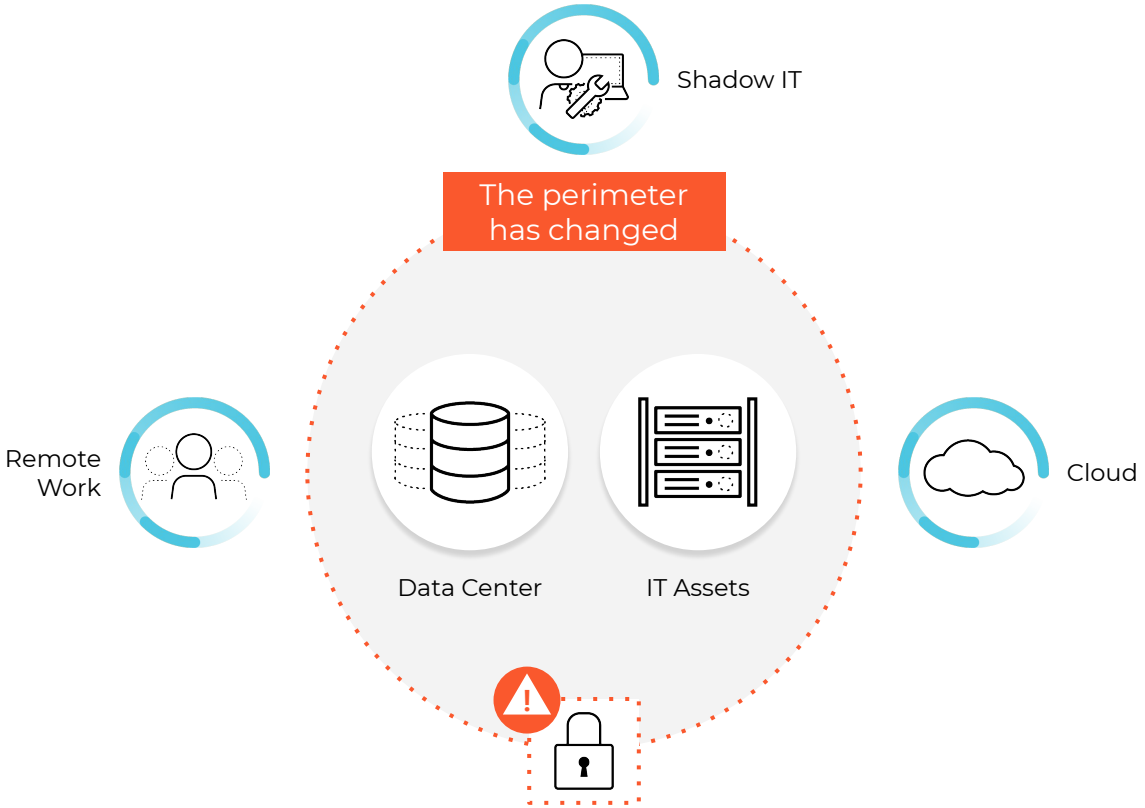
CORTEX
BY PALO ALTO NETWORKS

Управляйте площадью атаки EXPANSE

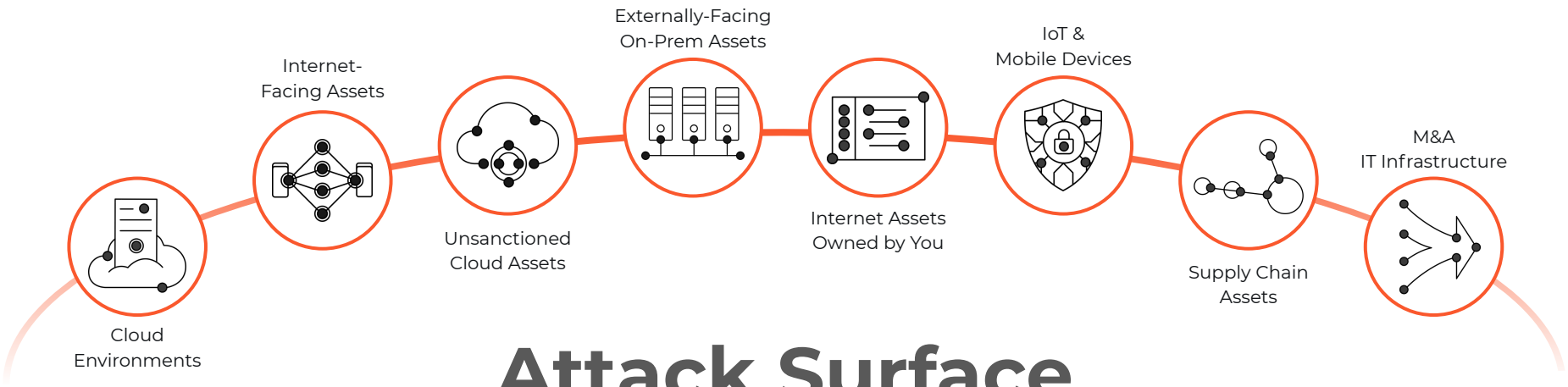
with EXPANSE
A PALO ALTO NETWORKS COMPANY

paloalto NETWORKS | EXPANSE
A PALO ALTO NETWORKS COMPANY

The Attack Surface used to be easily manageable



But now, your Attack Surface is made up of...



Attack Surface

Бизнесу требуется

Постоянное понимание поверхности атаки для обнаружения, оценки и предотвращения открытого доступа к сервисам подключенным к Интернет.

Managing your Attack Surface with Expanse

Discover

Continuously indexing the entire internet discovering all connected devices and exposed services.

Evaluate

Supervised ML engines power high-accuracy attribution and perpetual risk identification.

Mitigate

Automated policy-driven remediation leveraging existing processes and platforms.

Expanse Use Cases

Manage Attack Surface

Automatically inventory and discover risk across your Internet assets

Infrastructure Governance

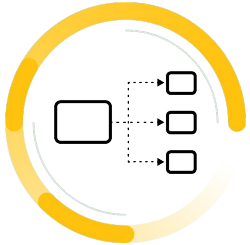
Monitor security across federated environments

Cloud Security

Eliminate cloud sprawl and enforce cloud policies centrally.

Compliance

Identify exposed assets against compliance requirements--NIST, PCI.



Third Party Due Diligence

Identify risk introduced from relationships with suppliers and M&A targets

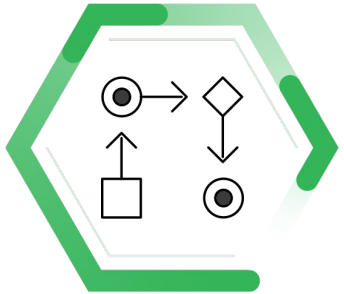
Expanse platform is made up of three products

Expander

Identifies and attributes all known and unknown internet-facing assets to map your attack surface

Behavior

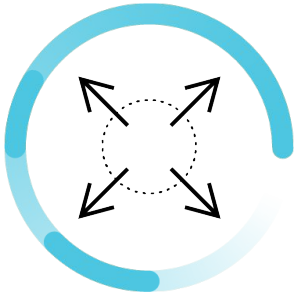
Uses global Internet flow data, surfacing risky communications between assets to detect and stop potential threats



Link

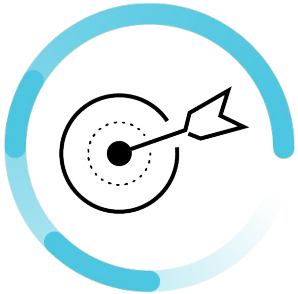
Continuously identifies risky services or misconfigurations in third parties to help secure a supply chain or identify risk for M&A due diligence

Expanse is superior at Attack Surface Management



Scalable Discovery

Internet-scale discovery method identifies **more assets** than anyone else with **higher accuracy**



Accurate Attribution

Patented technology that automatically identifies what assets **belong to your organization**

Complete Mitigation

White-glove **implementation** and wide range of integrations to optimize remediation workflow

Интеграция с другими продуктами

INVENTORY ASSETS	IDENTIFY ISSUES	ASSESS ISSUES	PRIORITIZE ISSUES	REMEDIATE & VALIDATE
Expander setup as source of truth.	Expanse scans coupled with VM scanners.	Understanding business context and associated risk.	Timely evaluation and alerting of misconfigurations and compliance issues.	Fix open Tickets and route to owner or automatically via SOARs. **Confirm success with Expanse!**
Enable with...	Enable with...	Enable with...	Enable with...	Enable with...
CMDB, IPAM, Asset Management	Vulnerability Management Scanners	CMDB, IPAM, Asset Management	SIEMs	ITSMs, SOARs
BLUECAT MarkMonitor ServiceNow	Qualys. RAPID7 tenable KENNA Security	BLUECAT MarkMonitor ServiceNow	splunk> LogRhythm IBM Radar FIREEYE	servicenow JIRA DEMISTO SWIMLANE

CASE STUDY #1

Asset discovery and remediation

Large SI

Challenges

- Up-to-date inventory of Internet connected assets (IPs, domains, and certificates)
- Remediate critical exposures, ensure proper configuration of perimeter devices, and address identified policy violations

40%
Increase
in IP network visibility

7,039
Connections
discovered at the start of the engagement

575
RDP servers
Addressed within two months of engagement

CASE STUDY #2

Cloud security and governance

Fortune 500 Insurance Firm

Challenges

- Manage cloud sprawl across multiple cloud providers
- Lacked visibility into different cloud providers, certificates and domains

11,372
Total
FQDNs monitored by Expanse

5,541
Certificates
managed by Expanse

64%
Increase
in asset visibility

CASE STUDY #3

Mergers and acquisitions / Third Party Risk

Fortune 500 Bank

Challenges

- Multiple acquisitions needed cyber due diligence.
- Lacked visibility into different cloud providers, certificates and domains.

3
Total
Acquisitions

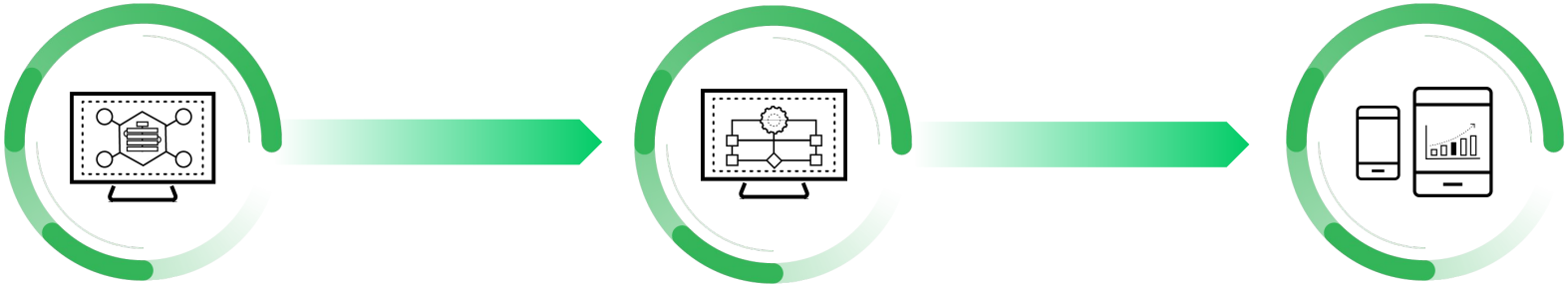
21,481
Assets
managed by Expanse

25
High priority
issues

paloalto NETWORKS

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

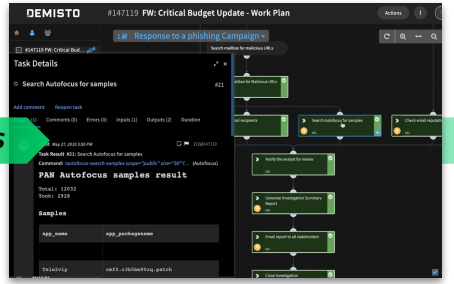
Case management

Аналитика и отчеты

Коммуникатор и совместная работа

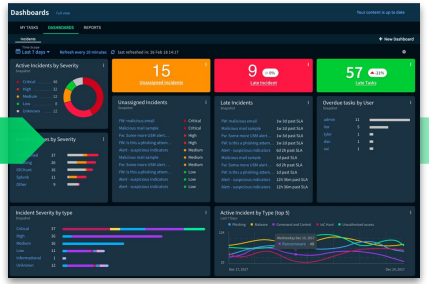
Реагировать и автоматизировать с Cortex XSOAR

ALERTS



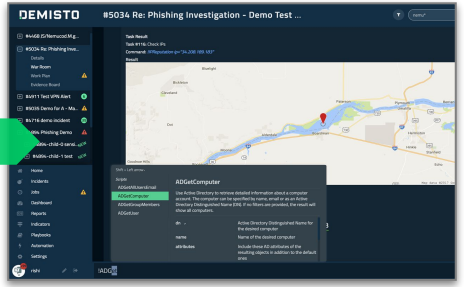
Respond and automate

Плейбуки на основе 350+ интеграций с другими вендорами



Manage incidents

Все инциденты в компании управляются из одной консоли

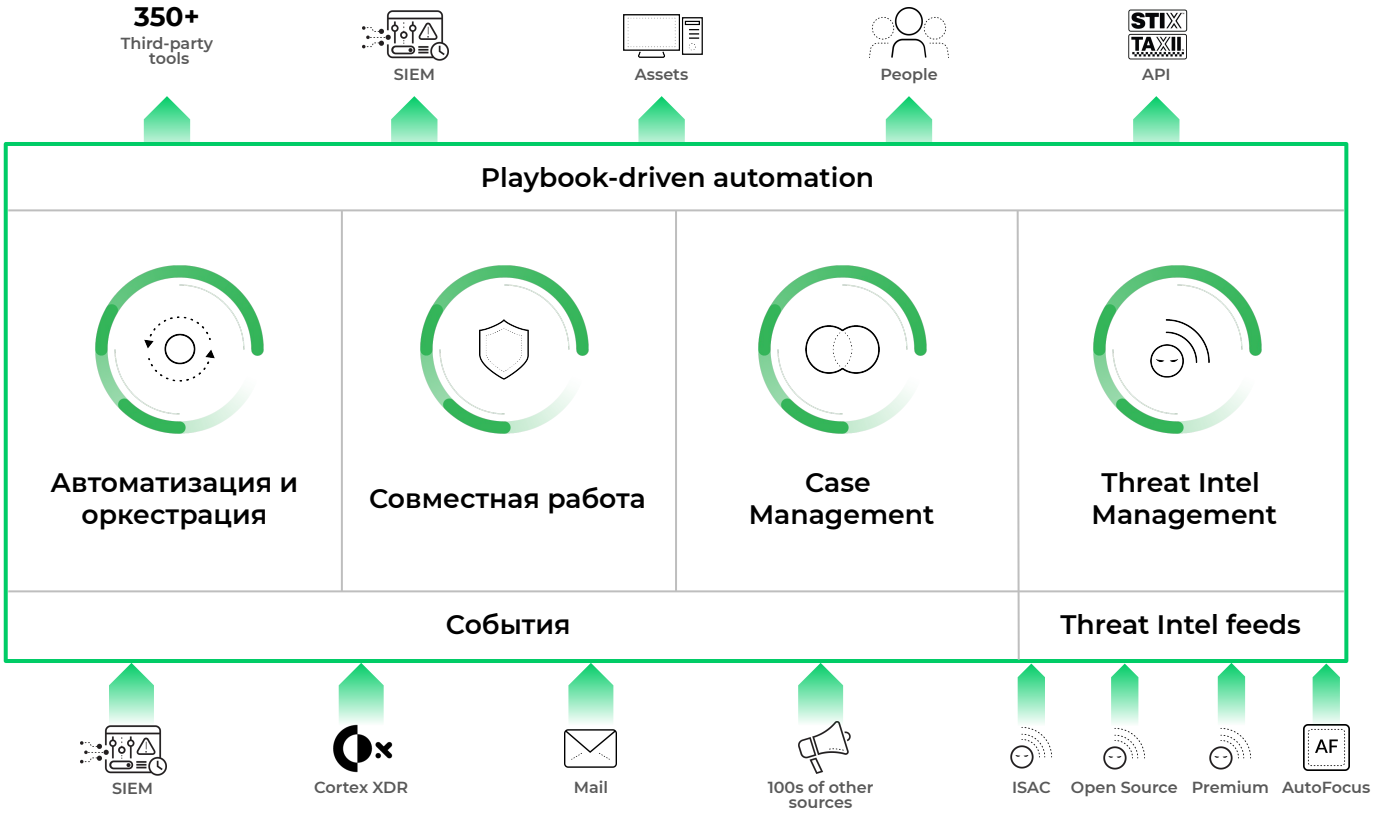


Collaborate and learn

Совместная работа и подсказки контекстные

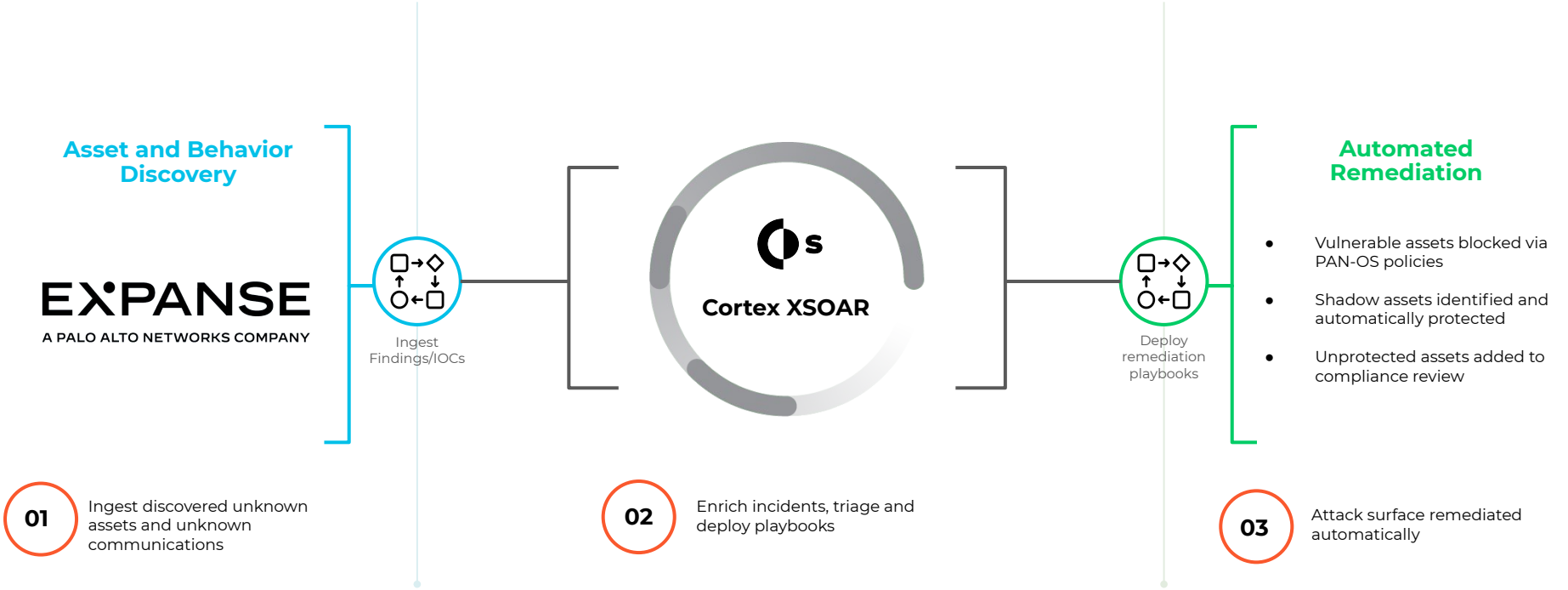
 |

CORTEX™ XSOAR
BY PALO ALTO NETWORKS



 |

Automate attack surface remediation with Expanse and XSOAR



 |

Why should I integrate Expanse with XSOAR ?

1. **Simplify and accelerate the implementation of ASM**
   Automating remediation of unknowns improves your security posture

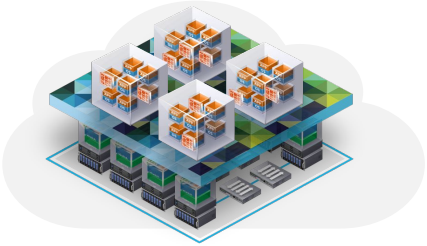
1. **Improve SOC productivity**
   Automated discovery and remediations drastically reduces MTTD and MTTR

1. **Make compliance easy**
   Fully automated asset discovery and remediation covering internal and external assets

Данные и приложения выходят в облака

Приложения как сервис (SaaS)

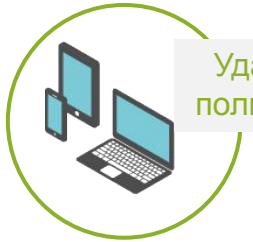
Публичное облако
(IaaS)



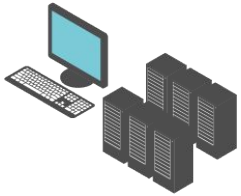
Приватное облако
NGFW для SDN и Spine-Leaf архитектуры
(NSX, OpenStack, ACI)

Как защитить ваше приложение и данные в облаке?

SAAS приложения не все одинаково полезны



Удаленные пользователи



Локальные пользователи

Разрешенные

box SharePoint salesforce

Допустимые

Google Drive Dropbox

Несанкционированные

Prezi zippyshare

РИСКИ **SAAS-***ПРИЛОЖЕНИЙ*

РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПО

СЛУЧАЙНАЯ ПУБЛИКАЦИЯ ДАННЫХ

ЗЛОУМЫШЛЕННАЯ УТЕЧКА ДАННЫХ

Примеры?

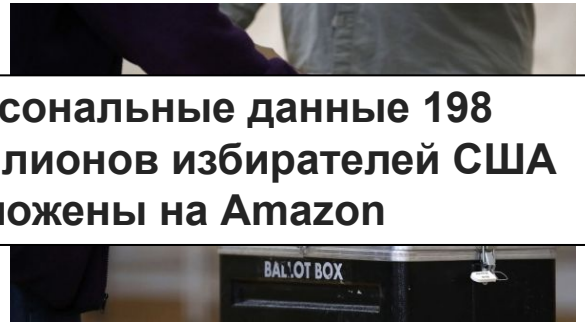
май 2017

Подрядчик выложил данные Пентагона на сервера Amazon без пароля

Почему?

- **Публичный доступ** Amazon S3 bucket
- Виноват подрядчик
- 60K файлов, 28GB данных, незашифрованные пароли

июнь 2017

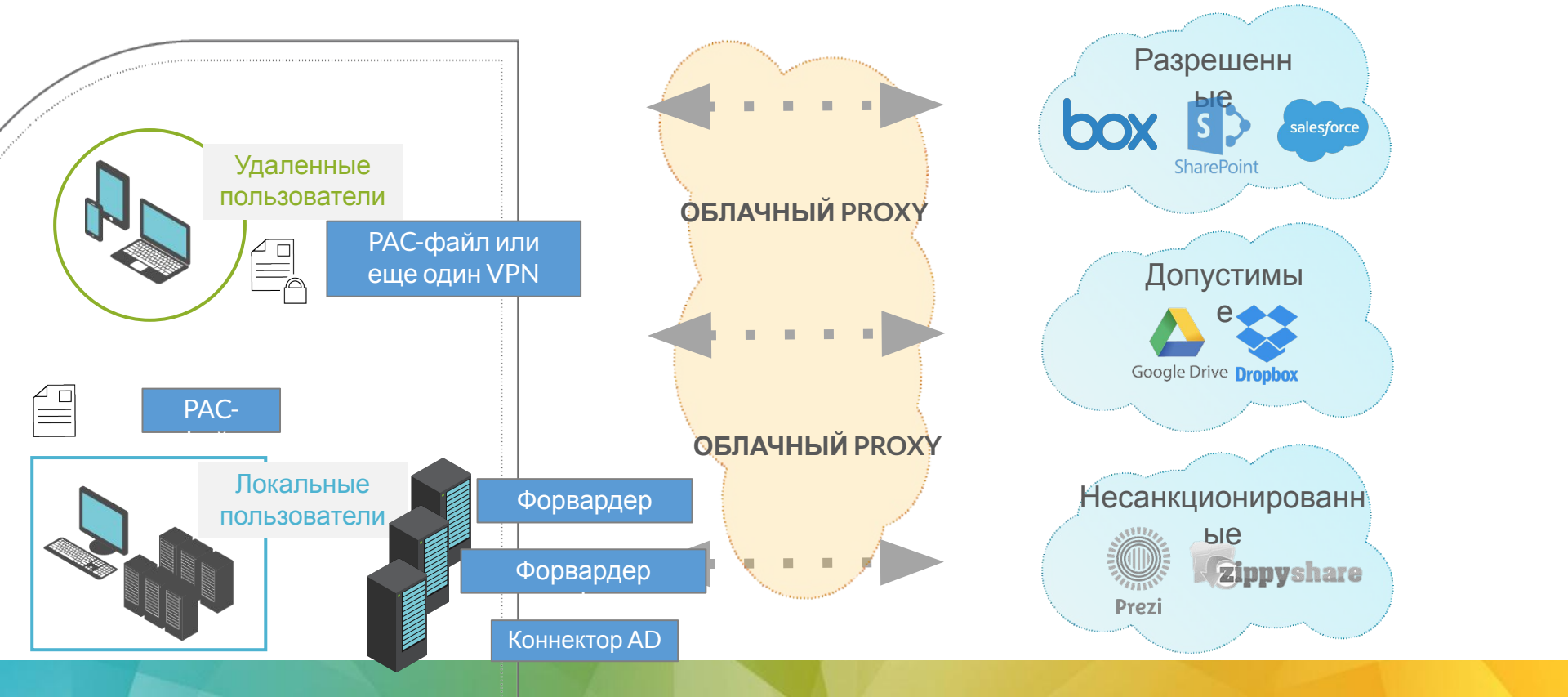


Персональные данные 198 миллионов избирателей США выложены на Amazon

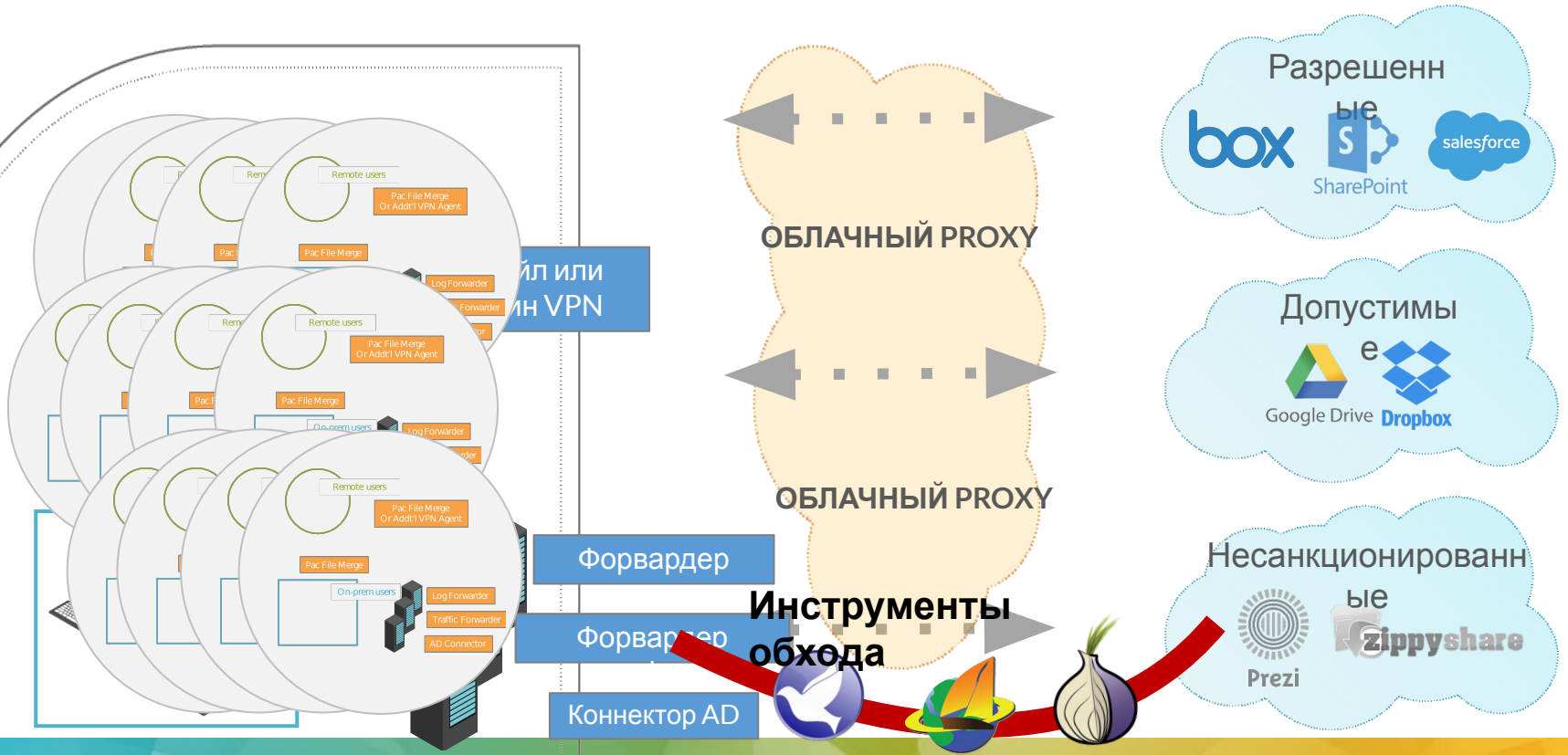
Почему?

- **Не защищали** Amazon S3 bucket
- 1.1 TB данных включая имена и адреса.

ПРОКСИ-подходы неэффективны и не масштабируются



ПРОКСИ-подходы неэффективны и не масштабируются



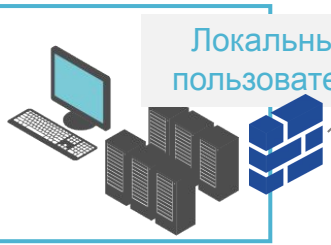
ПОДХОД PALO ALTO NETWORKS

Мониторинг и контроль активности в облаке с **Aperture**

Удаленные пользователи

GP

Полная видимость и контроль удаленных пользователей с **GlobalProtect**



Локальные пользователи

Полная видимость и контроль активности в локальной сети с **Next Generation Firewall**

AP

Разрешенные

box SharePoint salesforce

Допустимые

Google Drive Dropbox

Несанкционированные

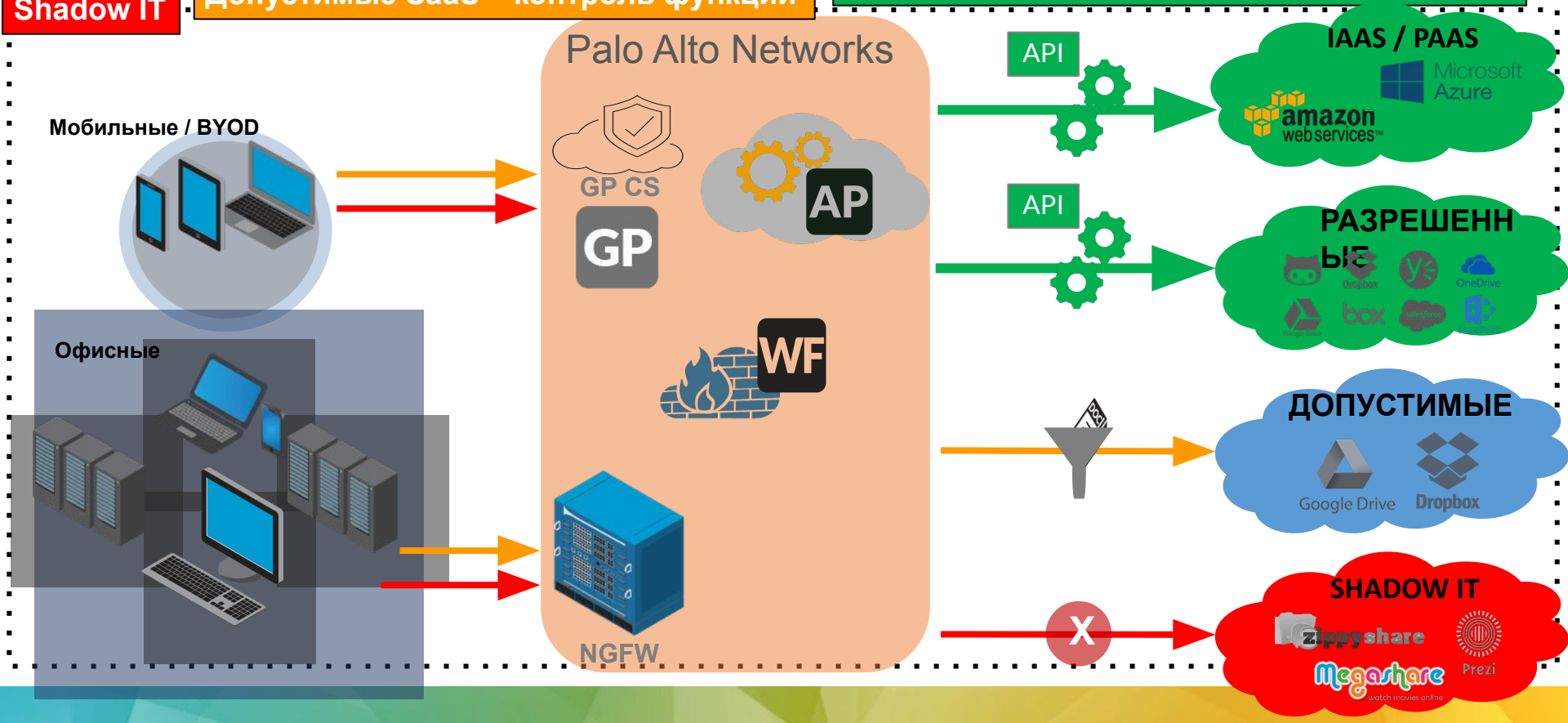
Prezi zippyshare

PALO ALTO NETWORKS – ПРОСТО И ЦЕНТРАЛИЗОВАННО

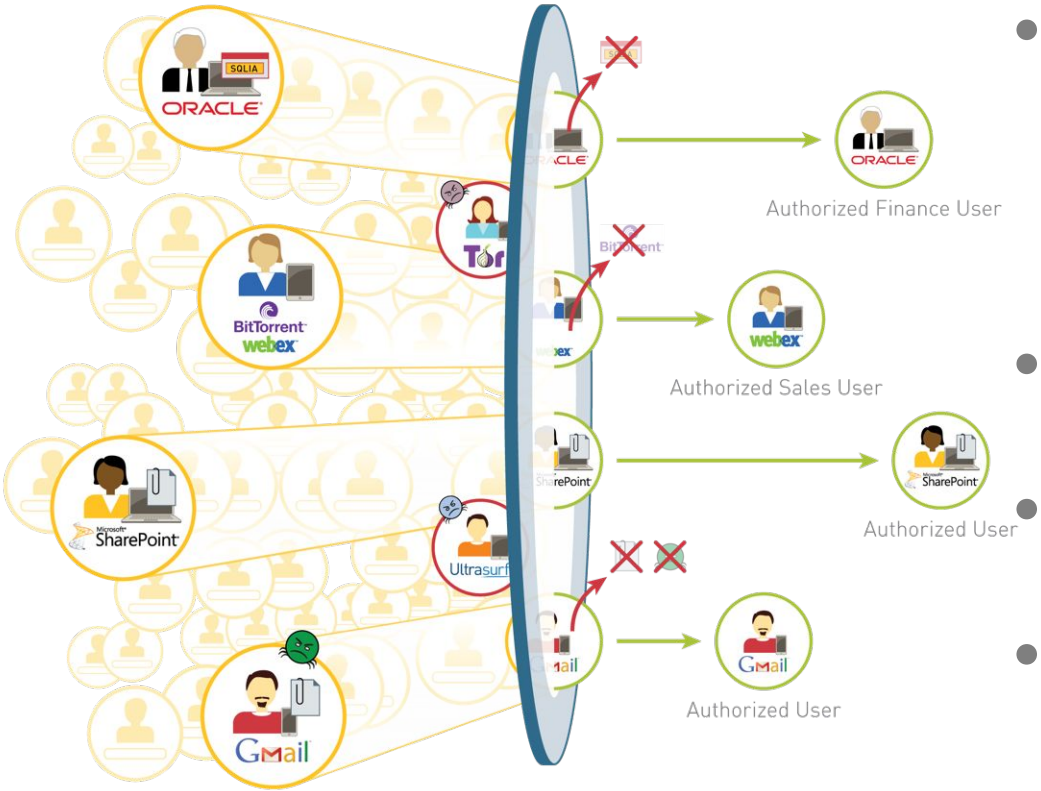
Shadow IT

Допустимые SaaS – контроль функций

Защищенный SaaS & IAAS/PAAS (через API)

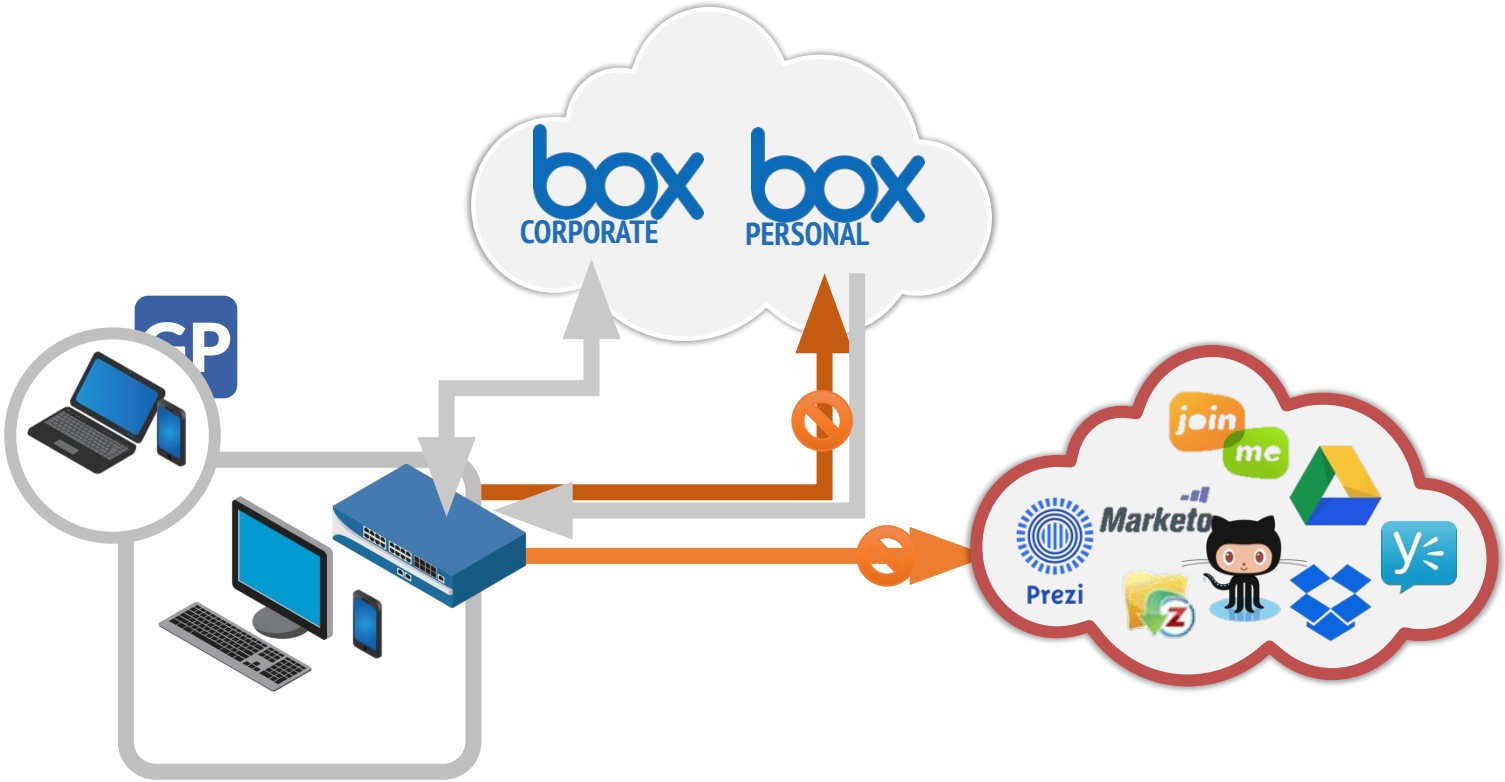


NGFW ВИДИТ SAAS ПРИЛОЖЕНИЯ

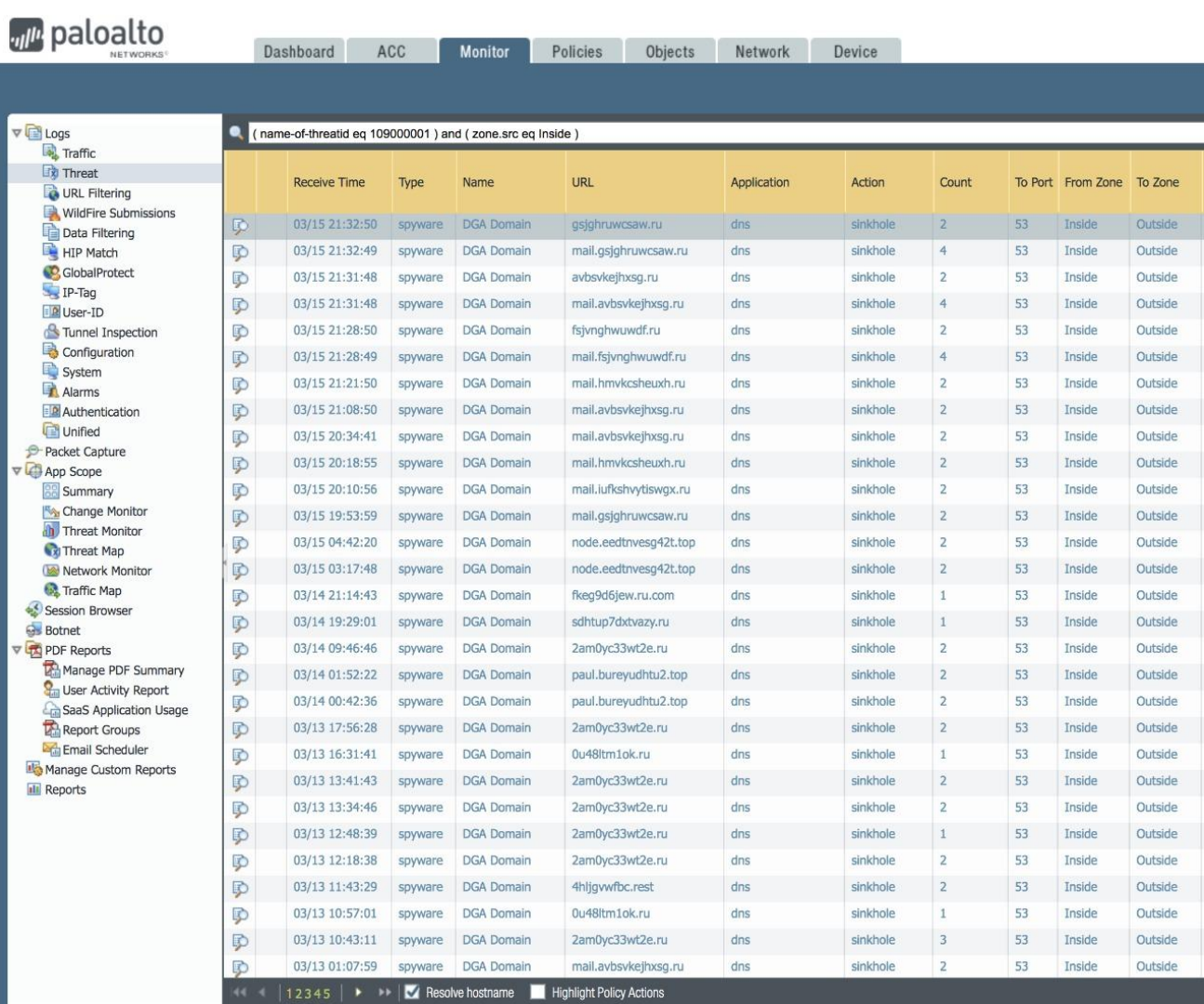


- **NGFW дает контекст и контроль**
  - Приложений и его функция
  - Пользователи и роли
  - Суть передаваемых данных
- **Это – ключевая функции PAN с момента ее создания**
- **Локальные пользователи контролируются политиками NGFW**
- **Трафик удаленный пользователей передается через GlobalProtect**

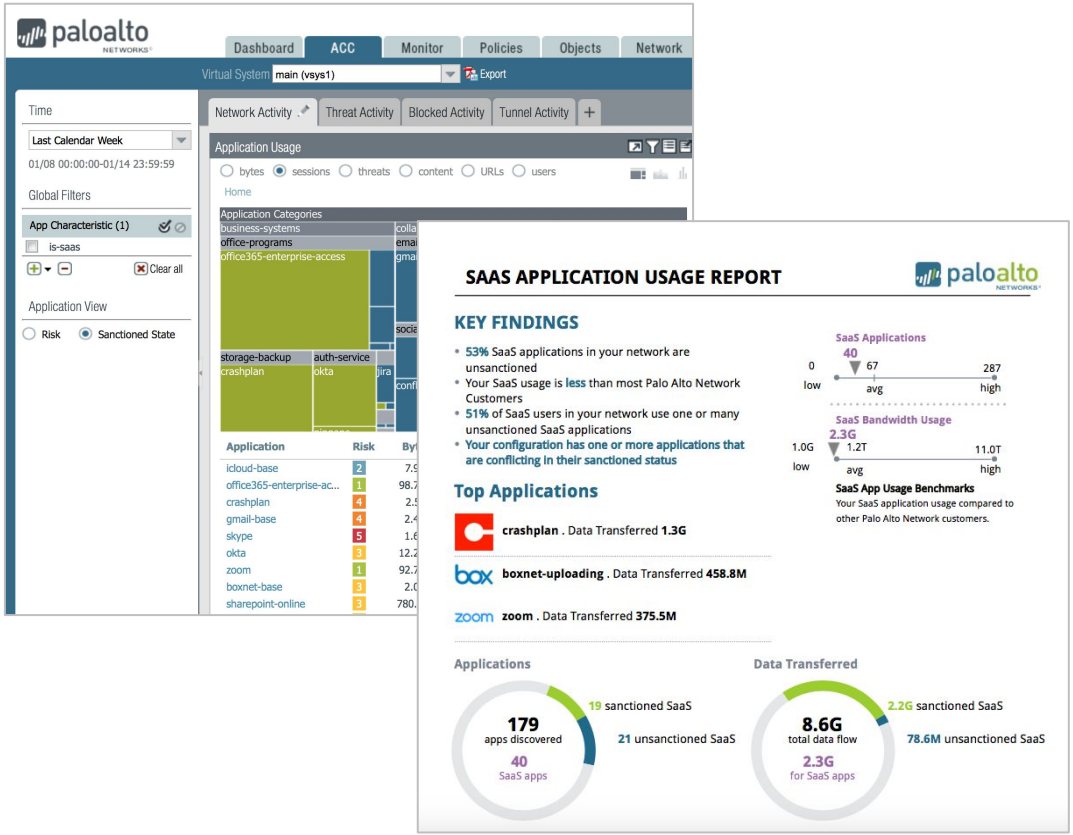
NGFW ДЛЯ SAAS НАХОДКА



DGA домены
Sinkholing
Видит NGFW



Аналитика и отчеты

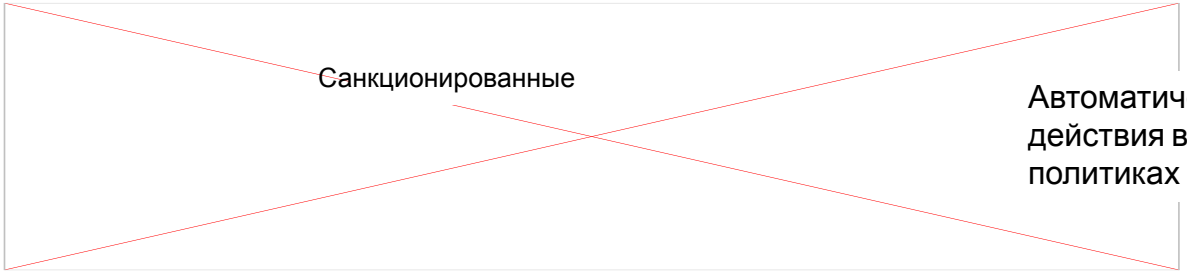


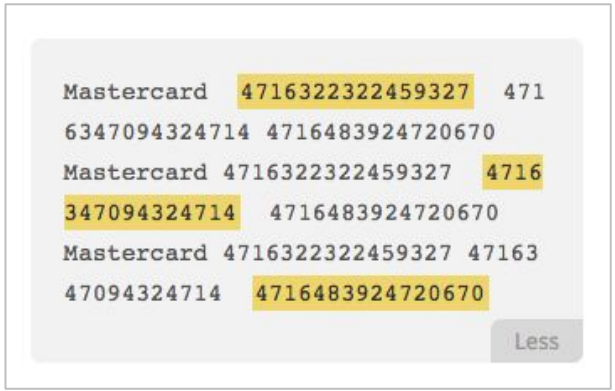
- Удобная навигационная панель SaaS
- Сортировка приложений по уровню риска или санкционированности
- Создание целевых отчетов на основе групп пользователей и зон
- Суммарный отчет использования приложений SaaS по группам
- Расширяет существующие функции SaaS-отчетности PAN-OS 7.1
- Полный функционал на базе Panorama без необходимости обновления PAN-OS

DLP	Песочница	Аномалии активности пользователей
Machine Learning	Контроль сторонних приложений (Google Apps)	Cloud Asset and Risk Discovery Amazon (S3, Key Rotation

МОМЕНТАЛЬНОЕ УСТРАНЕНИЕ РИСКОВ

Prisma SaaS

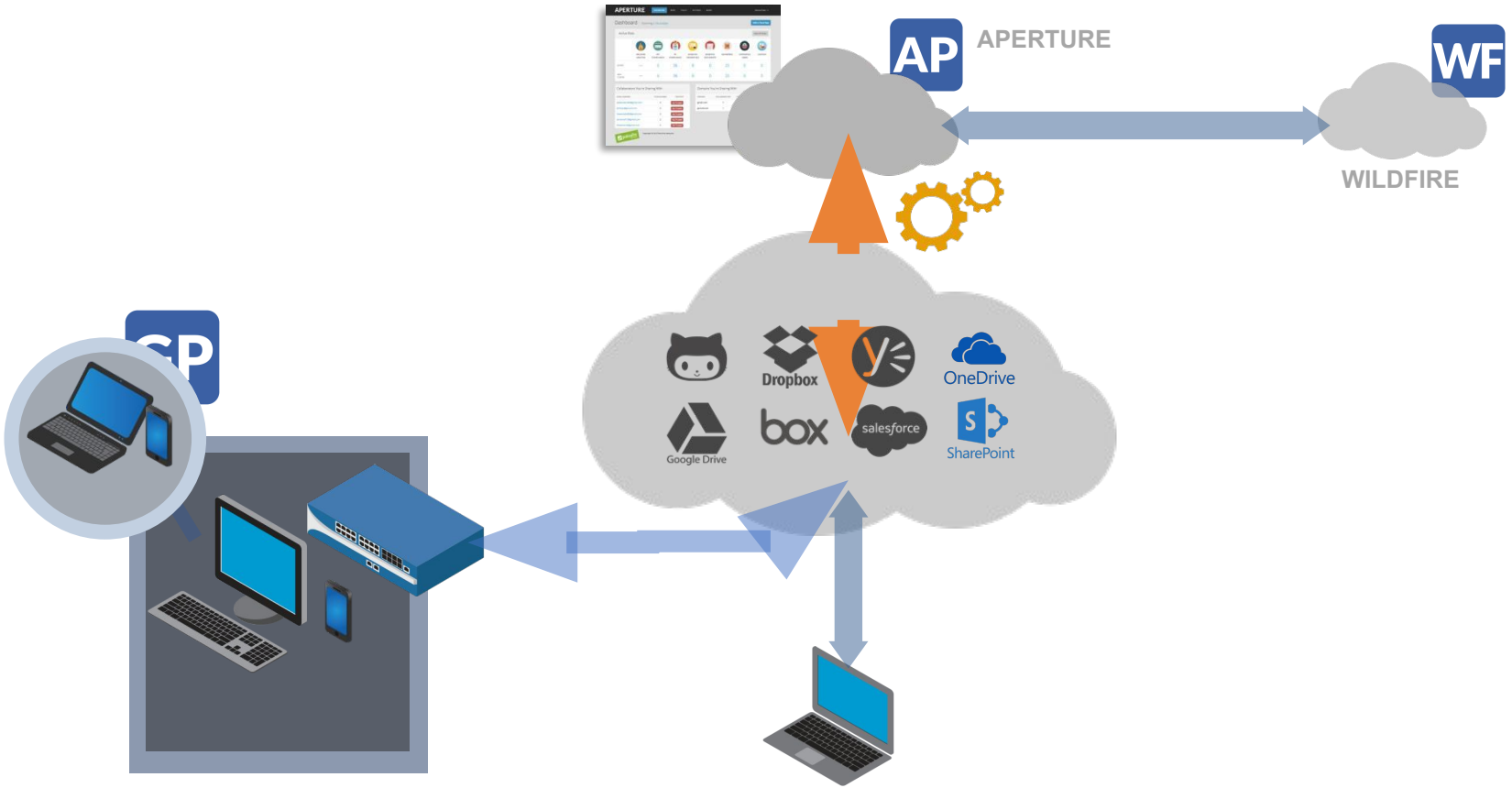




Полная безопасность данных в облаке с помощью API-интерфейсов SaaS-приложений

- Расширенная классификация данных
- Предотвращение кражи или утечки конфиденциальных данных
- Устранение вредоносного ПО благодаря интеграции с WildFire

ОБЛАЧНАЯ БЕЗОПАСНОСТЬ ИЗ ОБЛАКА



ЗАЩИТА САНКЦИОНИРОВАННЫХ SAAS-ПРИЛОЖЕНИЙ

ДЕТАЛЬНАЯ ИНСПЕКЦИЯ И АНАЛИТИКА ПО КОНТЕНТУ

КОНТЕКСТНЫЙ КОНТРОЛЬ РАСКРЫТИЯ ДАННЫХ

ПРОГРАММИРУЕМАЯ КЛАССИФИКАЦИЯ ДОКУМЕНТОВ

ОБНАРУЖЕНИЕ И УДАЛЕНИЕ ВРЕДОНОСНОГО ПО

УРОВНИ РАСКРЫТИЯ ДАННЫХ

Internal	Доступ не открыт явным образом
Company	Доступ явно разрешен сотрудникам внутри компании
External	Доступ явно разрешен контрагентам вне компании
Public	Доступно для всех в сети Интернет

ТИПЫ ПОЛИТИК

Какие правила вы хотите создать?


WildFire Analysis


PCI Compliance


PII Compliance


Sensitive Credentials


Source Code

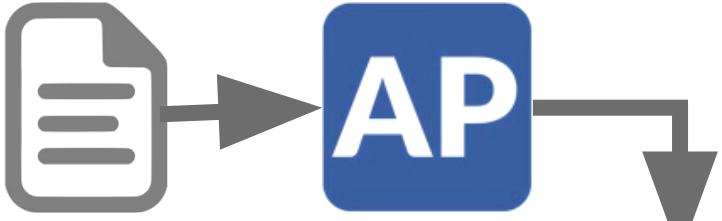

Untrusted Users


Sensitive Documents


Regular Expression

ОБУЧЕНИЕ APERTURE НА ТЕКСТАХ

СБОР И ВЗВЕШИВАНИЕ ТЕКСТОВ КЛАССИФИКАЦИЯ ДОКУМЕНТА



charles bailey was indicted for feloniously stealing on the 29th of december two dressed deer skins value 20 s the property of samuel savage and richard savage richard savage i am a leather seller 63 chiswell street my partner s name is samuel savage a few days previous to the 29th of december i looked out seventy skins for an order these skins being of a bad colour i directed them to be brimstoned to make them of equal colour pale on the 29th in the afternoon i saw them all smooth on a horse a few hours afterwards they appeared very much tumbled and one was thrown into the yard and dirtied i caused them to be brought in the warehouse and counted there was two gone our foreman went to worship street and brought armstrong and vickrey they searched and found this skin in the prisoner s breeches and the other skin was found in the workshop carter i am foreman to samuel and richard savage the seventy skins i was with mr savage looking them out i took them out of the stove and counted

МАТРИЦА ВЗВЕШАННЫХ ТЕКСТОВ

МАТРИЦА X

ФИНАНСОВЫЙ ДОКУМЕНТ

ЮРИДИЧЕСКИЙ ДОКУМЕНТ

МАТРИЦА Y

ПОДДЕРЖИВАЕМЫЕ ПРИЛОЖЕНИЯ

EXCHANGE ONLINE

SHAREPOINT ONLINE

ONEDRIVE FOR BUSINESS

YAMMER

BOX.COM

GOOGLE DRIVE

Gmail

G SUITE

EC2 / IAM

CONFLUENCE

AMAZON S3

APP-ID

GITHUB

SLACK

CITRIX SHAREFILE

JIVE

SERVICENOW

by facebook

SECURE DATA SPACE

SFDC

DROPBOX

2300+ приложений (SAAS И НЕ SAAS)

https://applipedia.paloaltonetworks.com

Глобальная доступность APERTURE

- Глобальное расширение Aperture с двумя новыми региональными ЦОДами в Европе и Азии
- Поддержка DLP и машинного обучения для родных региональных языков

ЛИЦЕНЗИРОВАНИЕ APERTURE

Лицензирование по пользователям в год

Тип лицензии: одно ИЛИ все приложения

Длительность подписок – 1 год, 3 года, 5 лет

WildFire и поддержка включены

СМЕЛО ИСПОЛЬЗУЙТЕ **SAAS**

PRISMA
BY PALO ALTO NETWORKS

panacademia.ru

Спасибо!
Thank you

Youtube bit.ly/bdv-video

paloaltonetworks.com

Денис Батранков, ваш помощник по новым стратегиям безопасности
ISC Certified Information Systems Security Professional, GIAC Certified Incident Handler, PAN Certified Network Security Engineer

Блог safebdv.blogspot.com

paloalto NETWORKS

Спасибо!

Академия Palo Alto Networks
https://panacademia.ru/

Подробная инструкция по настройке GlobalProtect на русском
http://tiny.cc/GLobalProtect

Денис Батранков
Palo Alto Networks Russia/CIS
Russia@paloaltonetworks.com

Вопросы и предложения
Russia@paloaltonetworks.com

Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
ms-rdp	4	196.9G	11.1k	0	0	0	240
ssl	4	256.4G	914.8k	7.1k	0	732.6k	238
web-browsing	4	8.0G	107.6k	383	233	315.2k	225
google-base	4	3.0G	96.5k	0	0	38.2k	218
ocsp	2	30.7M	9.5k	0	0	6	213
mail.ru-base	4	1.8G	62.6k	0	0	1.5k	145
google-analytics	2	144.9M	8.4k	0	0	7.2k	143
ntp	2	732.8k	4.0k	0	0	0	139
facebook-base	4	999.6M	8.3k	0	0	0	139
google-cloud-storage-download	2	50.3M	428	2	0	0	118
youtube-base	4	1.5G	8.7k	0	0	8.7k	113
yandex-maps	1	845.2M	5.9k	0	0	1	96
soap	2	35.2M	5.1k	0	0	9.2k	89
google-play	3	169.1M	10.8k	0	0	10.8k	88
ms-teams	2	39.7M	848	0	0	848	78
windows-azure-base	1	65.7M	1.8k	0	0	134	74
twitter-base	3	26.2M	694	0	0	0	73
mail.ru-mail	3	1.9G	40.7k	0	0	40.7k	73
insufficient-data	1	102.6M	80.9k	0	0	0	72
yahoo-web-analytics	1	8.1M	973	0	0	976	63
unknown-udp	1	463.1M	762	2.7k	0	0	63
vkontakte-base	4	284.3M	7.9k	0	0	0	61
outlook-web-online	3	184.1M	4.3k	0	0	2.3k	52

Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
ping	2	1.3M	9.6k	0	0	0	47
ms-onedrive-base	4	26.2M	1.2k	0	0	886	46
instagram-base	2	284.7M	3.4k	0	0	0	46
ms-store	1	6.9M	209	1	0	208	41
stun	2	27.9M	1.4k	0	0	0	41
new-relic	2	21.7M	2.1k	0	0	2.1k	41
pinterest-base	2	38.2M	362	0	0	0	39
unknown-tcp	1	792.2M	3.8k	0	0	0	38
ms-office365-base	2	16.0M	400	0	0	399	37
itunes-base	3	57.5M	1.4k	0	0	1.2k	37
gmail-base	4	281.0M	2.2k	0	0	2.2k	34
teamviewer-base	3	303.0M	684	0	0	18	31
google-drive-web	5	119.0M	265	0	0	265	28
dns	3	159.6k	1.1k	0	0	0	27
icloud-base	2	268.9M	11.0k	0	0	11.0k	25
google-docs-base	3	176.6M	659	0	0	662	25
ms-sms	3	1.2G	1.5M	0	0	1.5M	24
traceroute	2	91.6k	563	0	0	0	23
zoom-base	1	130.0M	1.2k	0	0	81	23
whatsapp-web	2	169.6M	2.4k	0	0	2.4k	22
skype	5	71.8M	4.4k	0	0	9.4k	22
hotmail	4	54.2M	486	0	0	486	19
linkedin-base	3	179.5k	31	0	0	16	19

Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
zendesk-base	3	3.4M	203	0	0	201	19
teamviewer-web	2	274.5k	29	0	0	28	17
google-maps	2	2.2M	46	0	0	44	17
whatsapp-base	1	133.4M	78	0	0	65	16
apple-maps	1	58.3M	3.0k	0	0	3.0k	16
whatsapp-file-transfer	3	378.1M	242	0	0	242	16
netbios-ns	2	84.2M	440.5k	0	0	0	16
zoom-meeting	2	11.7G	312	0	0	0	15
rtcp	1	4.1G	355	0	0	0	15
odnoklassniki-base	4	260.6k	42	0	0	0	15
disqus	2	1.7M	81	0	0	39	14
windows-push-notifications	1	3.8M	283	0	0	269	14
telegram	2	10.5M	1.5k	0	0	6	12
ldap	2	3.4M	7.0k	2	0	0	11
vimeo-base	4	13.0M	335	0	0	332	11
yandex-disk	3	1.4G	107	0	0	92	11
dropbox-base	4	29.9M	1.8k	0	0	1.8k	11
bing-maps	1	9.2M	126	0	0	123	11
facebook-video	4	479.3M	93	0	0	0	10
facebook-chat	3	12.3M	114	0	0	0	10
http-video	4	5.0G	706	0	9	3.3k	10
snapchat	2	698.3k	43	0	0	0	9
apple-siri	1	14.0M	864	0	0	864	9