Security Operating Platform

paloalto® NETWORKS

Palo Alto Networks: Единая платформа кибербезопасности

Комплексная защита в эпоху цифровой трансформации

Современные цифровые технологии позволяют значительно повысить эффективность и производительность предприятий, а также качество нашейповседневной жизни. В то же время, цифровая трансформация приводит квозникновению новых рисков, в результате чего неуклонно растет ежегодноеколичество жертв кибератак. Появление новых угроз, ужесточение требований регуляторов (PCI DSS, СТО БР ИББС) и внутренних политик делают обеспечение кибербезопасности все более трудной задачей. Необходим новый подход, который обеспечит снижение рисков и позволит идти в ногу с технологиями.

Технологии ИБ должны быть гибкими, совместимыми и легкими в использовании

Современные компании ориентированы на качество и непрерывность предоставления услуг. Это приводит к все большему усложнению ИТ- инфраструктур: набирают популярность облачные технологии, внедряются системы Big Data и Machine Learning и т.д. Это требует построение автоматизированных систем защиты, включающих в себя сразу несколько технологий противодействия кибератакам. Именно на этом принципе Palo Alto Networks разработала свою единую платформу кибербезопасности.

Единая платформа кибербезопасности

Единая платформа кибербезопасности Palo Alto Networks является очередной ступенью развития средств сетевой защиты, защиты конечных точек и облачных сервисов. Ее возможности расширены дополнительными сервисами:

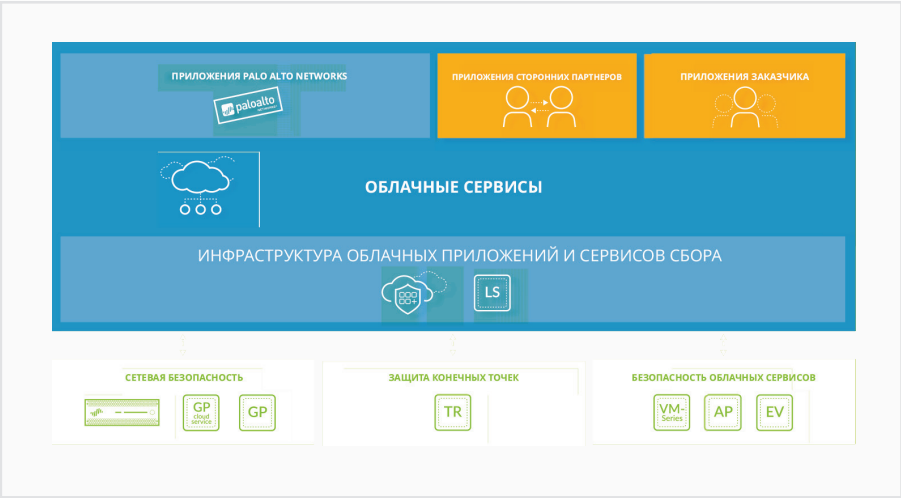
- **Threat Prevention** блокирует известное вредоносное ПО, инструменты эксплуатации уязвимостей и получения контроля над элементами сети.
- **URL Filtering** обеспечивает безопасный доступ к сети, включая предупреждение пользователей о вредоносных и фишинговых сайтах.
- **WildFire** автоматически обнаруживает и предотвращает неизвестные угрозы
- **AutoFocus** обеспечивает накопление и обмен информацией о новых угрозах
- **MineMeld** позволяет осуществлять обмен информацией об угрозах состоронними организациями, а также обеспечивает автоматическоепредотвращение атак в случае обнаружения индикаторов компрометации.

Платформа является открытой и может быть дополнена новыми функциями. Для этого применяется библиотека Application Framework и служба сбора логов Logging Service, на которых размещаются приложения Palo Alto Networks, а так же приложения сторонних организаций или клиентов.

- **Application Framework** позволяет интегрировать приложения с единой платформой кибербезопасности.
- **Logging Service** позволяет хранить логи в облаке.
- **Magnifier** обнаруживает активных злоумышленников в организации и осуществляет сбор аналитических данных на основе поведенческого анализа.

Единая платформа кибербезопасности на основе подхода Zero Trust

Единая платформа кибербезопасности Palo Alto Networks основана на подходеZero Trust, и это означает, что в центре внимания находится бизнес заказчика. В первую очередь мы фокусируемся на активах и данных, которые больше всег о нуждаются в защите. При использовании подхода Zero Trust необходимо определить, кто и куда должен иметь доступ, при этом анализироваться должен весь трафик.



СЕТЕВАЯ БЕЗОПАСНОСТЬ

NEXT-GENERATION FIREWALL

Next-Generation Firewall (NGFW) - первый в своем виде - является основой единой платформы кибербезопасности. Он дает полную визуализацию и контроль над всеми приложениями в сети, в том числе теми, которые пытаются выдать себя легитимными за счет работы по нестандартным портам и/или используя шифрование данных (например, TLS/SSL или SSH).

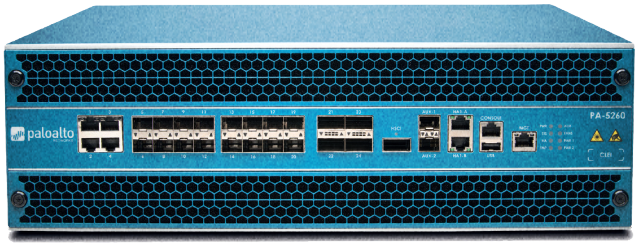
Palo Alto Networks NGFW:

- Проверяет и контролирует данные, передаваемые по сети, для обнаружения и блокировки известных и неизвестных угроз, и все это за одно сканирование.
- Увеличивает производительность за счет применения архитектуры однократного прохода, что обеспечивает сканирование трафика только один раз вне зависимости от включенных функций.
- Эффективно идентифицирует и блокирует неизвестное, новое или специализированное вредоносное ПО, и эксплойты.
- NGFW использует архитектуру с алгоритмом однократного прохода и параллельной обработки данных, которая применяет технологии App-ID, User-ID и Content-ID для идентификации приложений, пользователей и анализа контента соответственно, что обеспечивает NGFW непревзойденные возможности функций кибербезопасности.

PA-220

PA-800 Series

PA-5200 Series



STRATA™
BY PALO ALTO NETWORKS

App-ID - идентификация приложений

Система идентификации приложений App-ID™ безошибочно распознает приложения в потоке данных, проходящих через NGFW. App-ID может:

- Идентифицировать приложения, используя различные методы идентификации, в отличие от классических межсетевых экранов, которые используют IP-адрес, порт или протокол.
- Идентифицировать приложения, маскирующиеся под видом разрешенного трафика, используя динамические порты, или попытки пройти через межсетевой экран через зашифрованный SSL туннель.
- Применять специальные политики (Decryption Policy), чтобы дешифровывать и проверять входящий и исходящий SSL-трафик.
- Контролировать трафик через SSH-туннели.

User-ID - идентификация пользователей

Визуализация приложений по пользователю, а не по IP адресу, позволяет вам более эффективно контролировать приложения в вашей сети. Вы можете настроить порядок использования приложений в соответствии с требованиями вашего бизнеса и, при необходимости, информировать пользователей о нарушениях политики или даже блокировать их приложения.

При помощи User-ID можно:

- Создавать политики для безопасного использования приложений пользователями или группами пользователей, во входящем или исходящем направлении. Например, может быть предоставлен доступ для использования таких инструментов, как SSH, telnet и FTP на стандартных портах только сотрудниками IT-отдела.
- Контролировать как локальных, так и удаленных пользователей, независимо от типа используемых устройств и места их нахождения.
- Формировать отчеты с данными о действиях пользователей. Может быть создана собственная форма отчета или использованы типовые шаблоны.

Content-ID - идентификация данных

Технология идентификации данных Content-ID дает возможность проводить полный анализ всего трафика с целью предотвращения угроз.

Content-ID позволяет:

- Блокировать уязвимости в системе, предотвращать переполнение буфера и сканирование портов; защищать систему от вторжений и различных методов маскировки, используемых злоумышленниками; блокировать внешние соединения вредоносного ПО; блокировать доступ к вредоносным и фишинговым сайтам; снижать риски, связанные с несанкционированной передачей файлов и данных.
- Использовать подход на основе единого потока, упрощающий процесс управления, позволяющий модернизировать процесс обработки данных и значительно повышающий производительность системы.

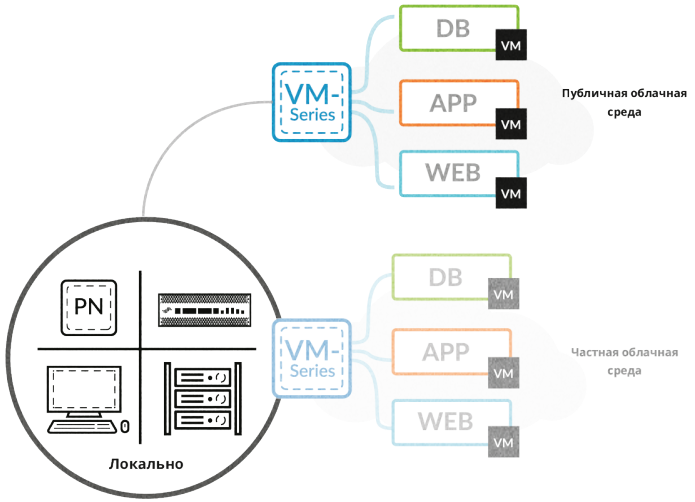
ВИРТУАЛЬНЫЕ NGFW
VM-SERIES

Для многих заказчиков переход в облачные среды является единственно верным для развития их бизнеса. Это дает отличную масштабируемость, увеличение производительности, быстрый доступ к новым технологиям, все то что дает возможность бизнесу оставаться конкурентноспособным.

В результате, приложения и данные начинают храниться и обрабатываться в различных облачных средах (частные облака, публичные облака, SAAS сервисы). Такой переход в облачные вычисления требует постоянной автоматической защиты, что предотвратит утечку данных и нарушение непрерывности бизнеса. Решения Palo Alto Networks создаются с учетом этих требований, в результате наши облачные сервисы поддерживают различных облачных провайдеров, постоянно расширяются и интегрируются со следующими облачными платформами:

- Частные облака: виртуальные NGFW VM-Series
- Публичные облака: виртуальные NGFW VM-Series, Evident и Traps
- Prisma SaaS

Виртуализированный NGFW VM-Series - может быть развернут в большинстве существующих частных и публичных виртуальных сред. VM-Series защищает публичную и частную облачную инфраструктуру контролируя приложения и предотвращая угрозы. Трафик классифицируется по приложению, а не по порту, давая полную визуализацию происходящего в сети. Использование политик, основанных на приложениях, предотвращает возможные риски и утечку данных.



PRISMA
BY PALO ALTO NETWORKS

Защита виртуальных ЦОДов и частных облаков

Виртуализированные ЦОДы это в первую очередь частные облака и вы ответственны за все аспекты виртуализации, включая аппаратное обеспечение, сетевые функции и безопасность. VM-Series защищает вашу частную облачную инфраструктуру используя политики, безопасно контролирующие приложения и предотвращая известные и неизвестные угрозы. Поддерживаемые среды виртуализации: VMware® ESXi™, NSX®, Cisco® ACI™, Citrix®, NetScaler®, SDX™, Microsoft®, Hyper-V® и KVM/OpenStack®.

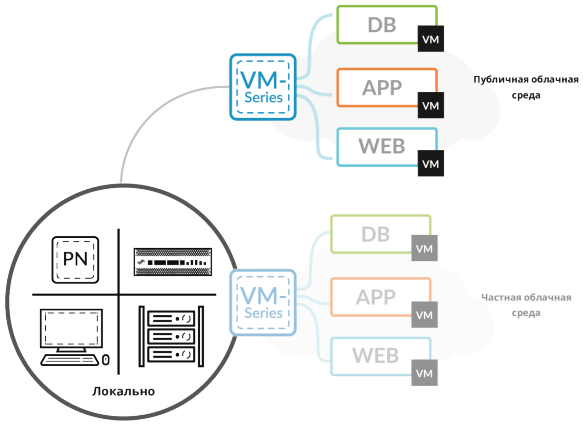
Защита данных, хранящихся в общедоступных облачных средах

Общедоступные облачные сервисы, такие как AWS, Microsoft Azure или облачная платформа Google, демонстрируют отличную динамичность, масштабируемость и единообразие инфраструктуры по сравнению с традиционными ЦОДами. Но риск утери данных по-прежнему существует. Внедрение VM-Series в жизненный цикл разработки приложения с целью дополнить существующие службы безопасности поможет предотвратить вредоносную активность.

Поддерживаемые общедоступные облачные среды: AWS®, Облачная платформа Google®, Microsoft®, Azure®, and VMware®, vCloud® Air™.

Автоматизация для поддержки вашего Бизнеса

Функции автоматизации VM-series упрощают процесс развертывания и обеспечения безопасности в частных и публичных облачных средах. Например, автоматически может быть создан виртуализированный NGFW VM-Series с рабочей конфигурацией, лицензией и подписками, а затем автоматически зарегистрирован на сервере централизованного управления и мониторинга Panorama. Процесс внесения изменений в конфигурацию VM--Series также может быть автоматизирован для динамического управления политиками безопасности используя штатные облачные сервисы и темплейты сторонних разработчиков, таких как Terraform® and Ansible®.



VM-Series

VM-Series состоит из пяти моделей, обеспечивающих производительность в режиме App-ID на скоростях от 200Mbps для VM-50 до 16Gbps для VM-700. Чтобы узнать больше о характеристиках VMSeries обратитесь по ссылке:

https://www.paloaltonetworks.com/products/product-selection

VM-
Series

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ И МОНИТОРИНГ

PANORAMA

Panorama™ предоставляет собой единый центр управления решениями Palo Alto Networks. Решение предоставляет статические правила и динамические обновления систем. Panorama значительно снижает рабочую нагрузку на офицеров ИБ за счет оптимизации управления сетевой защитой, предотвращения угроз, URL-фильтрации, идентификации приложений и пользователей, блокировки файлов и фильтрации данных. Из единой консоли управления можно проводить мониторинг трафика NGFW, конфигурировать устройства и назначать политики безопасности, получать развернутые отчеты.

Интегрированная платформа управления

Просмотр и управление трафиком NGFW, настройками конфигурации, глобальными политиками и отчетами по трафику и инцидентам ИБ, и все это с единой консоли. Panorama доступа в виде аппаратного или виртуального устройства.

Panorama обеспечивает:

- централизованное управление политиками NGFW
- упрощение рутинных операций
- визуализацию сетевого трафика и угроз
- полный сбор и хранение логов, включая логи от всех ваших NGFW и Traps

Логи NGFW, управляемых при помощи Panorama, группируются и хранятся вместе, обеспечивая

Общую визуализацию: Перечень приложений, URL, файлов и угроз со всех управляемых NGFW, отображаются вместе в единой графической консоли.

Гибкое управление политиками: поддержка глобального и локального управления политиками безопасности обеспечивает гибкость в управлении.

Гибкость в развертывании: Panorama доступна в виде физического устройства (M200 или M600), виртуальной машины для VMware® ESXi™ или в публичных облачных средах, таких как Amazon® Web Services и Microsoft® Azure®.

Panorama может быть развернута в трех разных режимах:

- **Panorama:** контроль политик и управление логами.
- **Management Only:** Только управление конфигурациями устройств, логи не собираются.
- **Log Collector:** только сбор и управление логами. Подразумевается, что еще развернута Panorama в режиме управления.

Разделение функций управления и сбора логов позволяет удовлетворять требованиям по расширяемости или разнесению устройств по географическому или организационному признаку. Выбор формы - фактора и режима развертывания дает максимальную гибкость по управлению NGFW Palo Alto Networks в распределенных сетях.

M-600

M-200

Panorama Specifications
Number of Devices Supported
· Up to 1.000
High Availability
· Active/Passive
Administrator Authentication
· Local database · RADIUS · SAML · LDAP · TACACS+
Administrator Authentication
· Gra · RADIUS · SAML

Public Clouds Supported
Amazon AWS
Microsoft Azure

Private Hypervisor Specifications			
	Management Only Mode	Panorama Mode	Log Collector Mode
Cores Supported	4 CPUs	8 CPUs	16 CPUs
Memory (minimum)	8 GB	32 GB	32 GB
Disk Drive	81 GB system disk	2 TB 24 TB log storage	2 TB to 24 TB log storage

Public Cloud Instance Types (BYOL License)			
	Management Only Mode	Panorama Mode	Log Collector Mode
Amazon AWS	t2.xlarge m4.2xlarge	m4.2xlarge m4.4xlarge	m4.4xlarge c4.8xlarge
Microsoft Azure	D4_V3 Standard D4S_V3 Standard	D16_V3 Standard	D16_V3 Standard D32_V3 Standard

СЕРВИСЫ БЕЗОПАСНОСТИ
WILDFIRE

Облачный сервис анализа вредоносного кода WildFire автоматически выявляет и останавливает неизвестные атаки. В отличие от классических замкнутых программных сред – «песочниц», для идентификации угроз используется расширенный функционал. WildFire способна в течение пяти минут определить наличие вредоносного кода в файле и автоматически запустить механизмы защиты в сети, на мобильных устройствах и в облаке. Самый большой в мире облачный сервис анализа вредоносного кода WildFire:

- Использует Data Science и машинное обучение, а также другие продвинутые методы анализа угроз, в том числе статический и динамический анализ, а также уникальный метод анализа в физических средах (без использования виртуализации).
- Автоматически создает и распространяет защиту от обнаруженного вредоносного ПО в течение 5 минут с момента обнаружения.
- Более 24 000 клиентов по всему миру подключены к сервису WildFire.

Уникальный подход для идентификации неизвестного вредоносного ПО

WildFire использует не только статичный анализ характеристик файлов, но и динамический анализ поведения файла для обнаружения неизвестных угроз. Кроме того, WildFire использует машинное обучение, а также bare metal analysis - анализ файлов в аппаратной инфраструктуре для поиска вредоносного кода, который скрывает себя при обнаружении виртуальной песочницы.

Благодаря тому, что сервис WildFire является облачным, он постоянно добавляется новыми технологиями, например динамической распаковкой или профилированием сетевого трафика.

Файлы распаковываются и запускаются в различных операционных системах, в том числе на мобильных устройствах:

- Различные файлы: Windows PE (EXE and DLL), PDF, Microsoft Office, Java, Android APK. Поддерживаются Linux ELF, ZIP, 7ZIP, RAR и Adobe Flash (6.1 или более поздняя версия).

- Ссылки в электронных письмах анализируются, чтобы оценить, содержат ли данные сайты какие- либо потенциальные угрозы.

Защита в течение пяти минут

Когда WildFire обнаруживает новое вредоносное ПО, автоматически создается новая сигнатура и идентификаторы компрометации, которые распространяются по всем клиентам WildFire по всему миру в течение нескольких минут.

- Помимо сигнатур вредоносного ПО, также создаются и распространяются сигнатуры C&C, DNS сигнатуры и данные о вредоносных URL.

- В среднем, каждый день сообщается о 230 000 случаях успешной защиты от угроз благодаря сервису WildFire.

Возможность локального развертывания

Сервис WildFire, запущенный в облачной среде, обеспечивает масштабируемость и высокую наращиваемость среды «песочницы». В то же время, для клиентов, не желающих передавать данные в облако, имеется специальная аппаратная версия устройства WF- 500, которая также поддерживает различные типы анализа вредоносного ПО.

Отчеты

Чтобы понять, как вредоносное ПО себя ведет и воздействует на систему, офицеры ИБ могут получить доступ к отчетам о проведенном анализе WildFire. Это можно делать через GUI или портал, а также через панель управления AutoFocus. Сервис WildFire направляет отчеты об инцидентах службе ИБ для быстрого реагирования на новые угрозы, а также для разработки профилактических контрмер.

CORTEX XDR

Вовремя распознайте и остановите скрытые атаки, объединив информацию из сети, конечных устройств и облачных данных

Преимущества для бизнеса

- Автоматическое обнаружение скрытых атак: постоянное обнаружение угроз с помощью искусственного интеллекта, анализа поведения и настраиваемых пользователем правил и политик обнаружения.
- Снижение нагрузки на персонал: мгновенное отсеивание ложных срабатываний, повышение производительности аналитиков.
- Сокращение среднего времени обнаружения угрозы (MTTI): сочетание точного определения атак с быстрой расстановкой приоритетов относительно уведомлений об опасности существенно сокращает временные затраты.
- Сокращение среднего времени на сдерживание угроз (MTTC): быстрое обнаружение и безошибочная реакция на внешние атаки и внутренние угрозы без многолетнего опыта.
- Быстрый возврат инвестиций: решение всех вопросов безопасности посредством экосистемы надежных приложений при использовании существующей инфраструктуры в качестве средств и точек контроля доступа.

Уберите препятствия и упростите расследование

Довольно часто службе безопасности не хватает наглядности и автоматизации для предотвращения атак. Отдельные продукты, например, система защиты конечных точек от сложных угроз (EDR), а также система анализа сетевого трафика (NTA) агрегируют большие объемы информации. Они вынуждают аналитика использовать множество консолей для обнаружения угроз, что повышает сложность и замедляет расследование. Сталкиваясь с отсутствием специалистов по кибербезопасности, команды вынуждены упрощать операции или прилагать огромные усилия для проведения расследования и сдерживания атак.

Уберите препятствия и упростите расследование

Быстрый способ обнаружения, расследования и реакции на угрозы Cortex XDRTM – это первое в мире приложение, в которое изначально интегрированы данные о сети, конечных устройствах и облаке для предотвращения сложных атак. Эффективно используя поведенческую аналитику, приложение определяет неизвестные и труднообнаружимые угрозы сети. Машинное обучение и модели искусственного интеллекта определяют угрозы, исходящие из любых источников, включая управляемые и неуправляемые устройства.
Cortex XDR ускоряет расстановку приоритетов относительно угроз и скорость реагирования на инциденты, предоставляя полную картину по каждой угрозе и автоматически определяя основную причину такой угрозы. Объединяя различные типы данных и упрощая анализ, Cortex XDR снижает время реагирования на угрозу, а также требования к знаниям и опыту, необходимому для осуществления операций по сортировке и поиску угроз. Тесная интеграция с точками контроля доступа позволяет быстро реагировать на угрозы, а также применять знания, полученные в результате расследования, для обнаружения схожих атак в будущем.

Защита от известных и неизвестных угроз с помощью TrapsTM

Безопасность начинается с надежного предотвращения угроз. Приложение TrapsTM для защиты конечных устройств, интегрированное в решение Cortex XDR, использует комплексные методы предотвращения атак для защиты конечных точек от вредоносных программ и средств эксплуатации уязвимостей. Traps и Cortex XDR позволяют последовательно предотвращать, обнаруживать, отвечать на угрозы, которым могут подвергаться цифровые активы. Встроенная интеграция с облачным анализом угроз позволяет скоординировано предотвращать сетевые угрозы, на конечных устройствах и облачных ресурсах.

Основные возможности

Наглядность

Соотносит данные о сети, конечных устройствах и облачных данных, чтобы упростить обнаружение и реакцию на угрозы.

Cortex XDR позволяет сэкономить время, затрачиваемое на анализ данных вручную, путем автоматического объединения и сопоставления данных, собранных из сети, конечных устройств и облачных ресурсов. Система объединяет разрозненные типы данных с помощью Cortex Data Lake, которое представляет собой масштабируемое и эффективное облачное хранилище данных, используемое в целях точного определения атак и упрощения расследования инцидентов ИБ.

Автоматическое обнаружение атак с помощью искусственного Интеллекта

Обнаружение скрытых угроз с помощью поведенческой аналитики

Cortex XDR автоматически определяет активные атаки, позволяя службе безопасности правильно расставлять приоритеты и отражать угрозы, прежде чем будет нанесен ущерб. Используя машинное обучение, Cortex XDR постоянно анализирует профили пользователей и поведение устройств для выявления аномальной активности, свидетельствующей об атаках. Анализируя большой массив данных, Cortex XDR может определять такие атаки, как кража идентификационных данных, угрозы DNS- туннелирования, которые практически невозможно определить при чтении стандартных логов или при анализе сетевого трафика верхнего уровня приложений. Автоматизированное обнаружение угроз работает бесперебойно каждый день.

Обнаружение угроз с помощью мощных поисковых инструментов

Обнаружение скрытого вредоносного ПО, целенаправленных атак, внутренних атак.

Служба безопасности может осуществлять поиск, планирование и сохранение запросов для определения трудно обнаружимых угроз. Гибкие возможности поиска позволяют аналитикам отслеживать угрозы и осуществлять поиск индикаторов компрометации (IoCs), не прибегая к изучению нового языка запросов. Используя встроенный анализ угроз в рамках сети, конечных устройств и облачных данных, службы безопасности смогут обнаруживать вредоносное программное обеспечение, внешние угрозы и внутренние атаки, которые осуществляются в текущий момент времени или осуществлялись ранее.

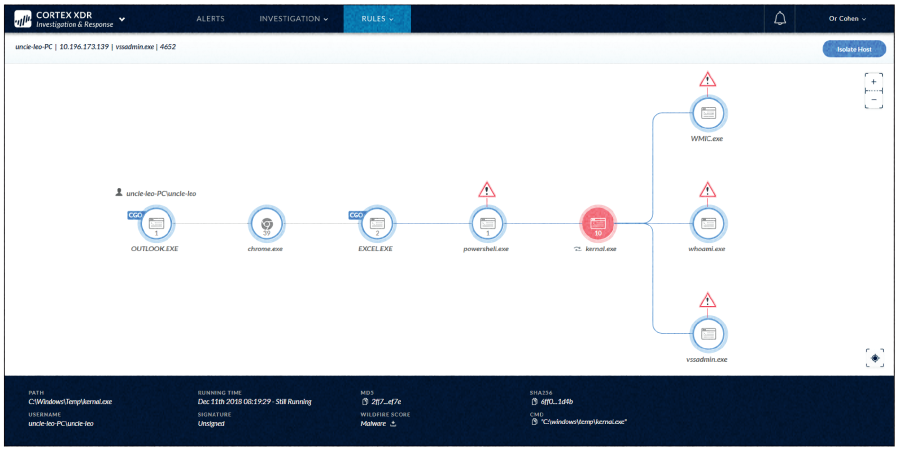


Рис. 1 Расстановка приоритетов и расследование угроз с помощью Cortex XDR

Мгновенное расследование событий

Автоматическое определение источника каждого уведомления безопасности

С помощью Cortex XDR аналитики могут в один клик анализировать предупреждения о нарушении безопасности из любого источника. Cortex XDR автоматические обнаруживает первопричину проблемы, выявляет историю и последовательность событий, связанных с каждым предупреждением, что снижает требования к опыту, необходимому для точного подтверждения проблемы. При расследовании, график всех атак предоставляет детальную информацию для изучения инцидента, позволяя аналитикам мгновенно определять объем и масштаб ущерба, а также последующие действия.

Скоординированный ответ с использованием точек контроля доступа

Быстрое и надежное отражение угроз

Cortex XDR позволяет службе безопасности оперативно отражать угрозы сети, конечных точек и облачных ресурсов из единой консоли. Аналитик может быстро остановить распространение вредоносного ПО, ограничить активности сети определенными устройствами, обновить список источников угроз, например, список неблагонадежных доменов посредством тесной интеграции с точками контроля доступа. С помощью Cortex XDR можно оперативно останавливать сложные атаки, что позволяет быстро вернуть инвестиции, вложенные в ИБ.

Адаптивная защита для остановки потенциальных атак

Определение тактики, методов, процедур и правил поведения атакующих

С Cortex XDR служба безопасности сможет получать новые знания из каждого расследования и применять их для сокращения масштабов поражения и ускорения последующего расследования, изменив тип защиты с реактивного на проактивный. Аналитики могут создавать детализированные правила поведения, которые позволят определять вредоносную активность, свойственную конкретной сети. Информативные оповещения позволятускорить анализ быстро идентифицируя подозрительное поведения, а также упрощает понимание сложных событий.

Защищайте конечные устройства с помощью лучшего отраслевого Решения

Использование единого агента для отражения угроз и предотвращения сбора данных на конечных устройствах

В подписку Cortex XDR включены агенты Traps, которые обеспечивают лучшую на сегодняшний день защиту конечных устройств. Traps позволяет останавливать известные и неизвестные вредоносные программы, средства эксплуатации уязвимостей, программы--вымогатели путем блокирования случаев подозрительного поведения и проникновения. Облачная система анализа вредоносного ПО с интегрированной службой защиты - Palo Alto Networks WildFire®- улучшает точность обнаружения и зону покрытия. Агент Traps записывает всю активность конечного устройства и пересылает данные в Cortex Data Lake для последующего анализа и позволяет выбрать правильную реакцию.

Простота развертывания и облачная поставка

Развертывание системы за считанные секунды

Облачное приложение Cortex XDR позволяет быстро и без затрат организовать развертывание системы защиты, устраняя потребность в установке новых локальных служб сбора данных и средств контроля. В качестве средств и точек контроля система использует существующие продукты Palo Alto Networks, тем самым, сокращая число продуктов, которыми вам нужно управлять. Новым клиентам достаточно развернуть одно средство контроля, например, Next--Generation Firewall или Traps, для обнаружения и предотвращения угроз с помощью Cortex XDR. Cortex XDR создано на единственной в отрасли SOC-платформе Cortex на базе искусственного интеллекта. Оно существенно упрощает защиту систем и позволяет добиваться лучших результатов применяя автоматизацию процессов.

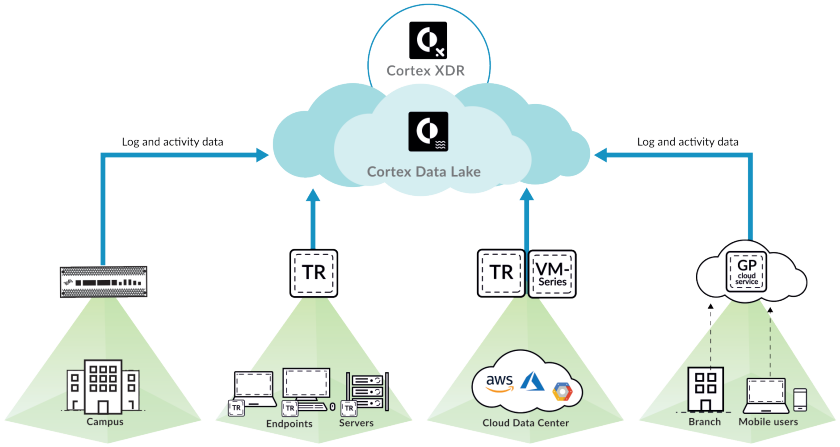


Рис. 2 Анализ данных из любого источника для предотвращения и реагирования на угрозы

Технологический эффект

Визуализация сети, конечных точек и облачных данных:
сбор и корреляция большого объема данных сети, конечных устройств и облачных данных для обнаружения, расстановки приоритетов для реагирования и предотвращения угроз.

Автоматическое обнаружение сложных и скрытых атак в режиме 24/7:
Постоянное использование функции машинного обучения и создания индивидуальных правил для обнаружения целевых кибератак и прочих хитросплетений злоумышленников.

Обработка оповещений без задержек:
Упрощает расследование угроз, в том числе анализ корневых проблем и позволяет создавать хронологию событий, тем самым, снижая требования к навыкам сотрудников, которые необходимы для оценки и анализа оповещений.

Значительное сокращение количества ложноположительных оповещений безопасности:
Применяет знания, полученные в ходе каждого расследования, для постоянного обновления правил определения поведенческих особенностей и уменьшает количество времени, затрачиваемого на проведение анализа в будущем, снижая уровень риска.

Повышает производительность SOC:
Собирает рабочие процессы в единую консоль, объединяя функции расстановки приоритетов в отношении оповещений, расследования, ответа на угрозы в рамках всей сети, конечных устройств и облачной среды.

Восстанавливает систему без последствий для бизнеса:
Предотвращает атаки с высокой точностью, не допуская перебоев в работе системы и пользователей.

Позволяет избегать целенаправленных кибератак:
Защищает сети от внутренних злоумышленников, нарушителей правил, внешних угроз, безфайловых атак и атак на оперативную память, атак 0-дня.

Разгружает службу безопасности:
купирует атаки, обнаруживая нарушения нормального функционирования системы безопасности, аномальное поведение, вредоносный характер активности.

Особенности Cortex XDR	
Автоматическое расследование предупреждений	Определение угроз, исходя из индивидуального характера поведения
Поиск источника возникновения угроз	Машинное обучение
Реагирование на инцидент	Определение вредоносных и безфайловых атак
Предотвращение инцидента и восстановление	Определение целевых кибератак
Анализ последствий после инцидента	Обнаружение внутренних угроз
Поиск угроз	Поведенческая аналитика
Индикаторы компрометации и аналитика угроз	Предотвращение атак с помощью вредоносного, хакерского ПО и использование уязвимостей посредством Traps

Технические характеристики	
Модель поставки	Облачная поставка
Хранение данных	30 дневное неограниченное хранение данных

Поддержка ОС
Traps поддерживает работу с оконечными устройствами на Windows®, macOS® и Linux ОС. Полный перечень системных требований и поддерживаемых ОС вы найдете в таблице совместимости Traps.
Минимальные требования Cortex XDR Pathfinder: 2-х ядерный процессор, 8 Гб оперативной памяти, устройство хранения данных на 128 Гб с тонкой резервацией памяти, VMware ESXiTM версия 5.1 или позже, или Microsoft Hyper ® версии 6.3.96 или более поздняя версия гипервизора.
Лицензия Cortex XDR включает право пользования:

- Cortex XDR – приложение для анализа
- Cortex XDR – приложение для расследования и реагирования на угрозы
- Агент Traps для защиты конечных точек и отражения атак
- Cortex XDR – Pathfinder служба анализа в конечных точках (альтернатива Traps без использования агента)

3000 Tannery Way
Santa Clara, CA 95054
Основной телефон: +1.408.753.4000
Отдел продаж: +1.866.320.4788
Служба поддержки: +1.866.898.9087
www.paloaltonetworks.com

cortex-xdr-ds-053119

НЕ ИМЕЮЩАЯ АНАЛОГОВ ЗАЩИТА КОНЕЧНЫХ УСТРОЙСТВ

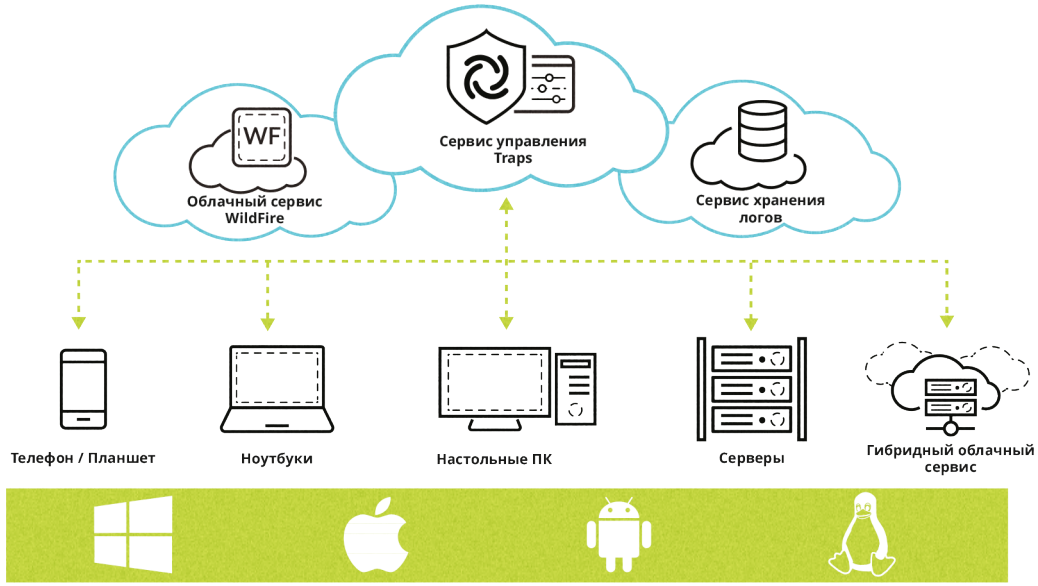
TRAPS

Решение по защите конечных устройств Traps™ от компании Palo Alto Networks предотвращает атаки на сервера, рабочие станции и мобильные устройства. Traps представляет собой легковесный, не требовательный к ресурсам агент, предотвращающий вредоносную активность за счет блокировки вредоносного ПО, эксплоитов и вирусов- вымогателей. Может использоваться для операционных систем Windows®, macOS®, Android® и Linux и может управляться как локально, так и из облака.

Различные методы защиты вредоносного ПО

Traps предотвращает исполнение вредоносного кода, защищая как от традиционных, так и от современных атак. Кроме этого, администратор может настроить периодическое сканирование для поиска угроз, соответствию требованиям регуляторов и ускорения расследования инцидентов.

Технологии Traps являются уникальными с точки зрения предотвращения вредоносной активности. Основное преимущество Traps по сравнению с другими решениями - нацеленность на техники, используемые инструментами эксплуатации уязвимостей. Это позволяет защищать приложения и ОС от угроз нулевого дня до выхода патчей.



CORTEX™
BY PALO ALTO NETWORKS

Технологии Traps:

- **Данные об угрозах:** Traps использует данные об угрозах, получаемые от десятков тысяч подписчиков облачного сервиса анализа вредоносного ПО WildFire для постоянного сбора данных об угрозах и обеспечению защиты на уровне рабочих станций, сети и облачных сервисов. Traps запрашивает WildFire и практически моментально получает ответ о том, является ли файл вредоносным или нет. Если файл неизвестен, Traps выполняет дополнительные методы проверки для определения, является ли это угрозой, которую необходимо предотвратить.

- **Локальный анализ с использованием машинного обучения:** если файл остается неизвестным после первоначальной проверки hash суммы или если он не был идентифицирован администраторами, Traps использует локальный анализ, основанный на машинном обучении для того, чтобы определить, можно ли запускать данный файл даже до получения отчета от WildFire.

- **Динамический анализ:** в дополнение к локальному анализу, Traps отправляет неизвестные файлы в WilFire для глубокого анализа и быстрой идентификации неизвестного вредоносного кода . WildFire использует собственные техники высокоточного анализа, исключающего возможности проникновения в систему.

  - **Статический анализ** с применением машинного обучения – более мощная версия облачного локального анализа, анализирующая характеристики файлов без необходимости его запуска.

  - **Динамический анализ** – специально построенное виртуальное окружение с защитой от техник обхода и идентификации, в котором запускаются ранее неизвестные экземпляры ПО для его анализа поведения.

- **Bare metal – анализ** – технология запуска неизвестных файлов в физической среде. Специально разработанная для анализа сложного вредоносного кода, который чрезвычайно трудно обнаружить, и который может распознать виртуальный анализ и запуск в виртуальной замкнутой программной среде («песочнице»).

В случае, если WildFire определяет, что файл является вредоносным, автоматически создается новый механизм предотвращения угрозы Traps и других компонентов платформы кибербезопасности Palo Alto Networks. В течение не более 5 минут новая информация распространяется по всем средствам защиты Palo Alto Networks для немедленной классификации и дальнейшего предотвращения данной угрозы.

Защита от вредоносного ПО – Traps по умолчанию, прямо «из коробки» защищает от атак, основанных на скриптах и не использующих файлы, за счет гранулированного контроля за запуском легитимных приложений, таких как скриптовые движки и командные шеллы.

Защита от вирусов-вымогателей – В дополнение к существующим методам предотвращения, включая защиту от эксплоитов, локальный анализ и WildFire, Traps мониторит поведение вирусов-вымогателей. В случае обнаружения такой активности, он моментально блокирует атаку и предотвращает дальнейшее шифрование данных пользователя.

Различные методы предотвращения эксплуатации уязвимостей

Уникальность Traps в его возможности предотвращать эксплуатацию уязвимостей за счет идентификации техник уязвимостей и защиты от применения таких техник. Traps защищает от техник, которые необходимо применить в случае любой атаки, основанной на эксплуатации уязвимости.

Различные методы предотвращения эксплуатации уязвимостей

Предотвращая эти техники, Traps может защитить непатченные системы, неподдерживаемые старые системы в том числе от ранее не встречавшихся эксплоитов, так называемых эксплоитов нулевого дня

Traps защищает от эксплоитов за счет различных методов, включая:

- **Предварительная защита (pre-exploit):** Traps предотвращает использование техник профилирования уязвимостей, которые используют т.н. эксплоит киты перед тем, как запустить атаку. Блокируя эти техники, Traps не дает возможность злоумышленнику получить доступ к уязвимой рабочей станции или приложению, таким образом предотвращая атаку еще до момента ее начала.
- **Защита от техник уязвимостей:** Traps защищает от известных, неизвестных и непатченных уязвимостей блокируя техники эксплуатации уязвимостей, которые используют злоумышленники для манипуляции приложениями.
- **Защита от уязвимостей ядра:** Traps защищает от эксплоитов, использующих уязвимости ядра операционной системы для создания процессов и повышения привилегий. Также Traps защищает от новых техник эксплуатации, которые использовались в последних атаках WannaCryb NotPetya.

Блокируя эти техники, Traps обеспечивает пользователю следующие преимущества:

1. Защита непатченных приложений и swadow IT
2. Минимизация рисков, связанных с задержками по обновлению систем
3. Защита от эксплоитов нулевого дня

Помимо предотвращения запуска вредоносного ПО и эксплуатации уязвимостей, Traps также выполняет следующие функции:

- **Сканирование:** администраторы могут сканировать конечные устройства и подключенные съемные носители на предмет наличия скрытого вредоносного ПО, а также использовать опцию автоматического помещения подозрительных файлов в карантин.
- **Политики замещения администратора:** Traps позволяет определять политики на основании хэша исполняемых файлов, контролируя, что можно, а что нельзя запускать.
- **Карантин для вредоносного ПО:** Traps может немедленно направить вредоносные исполняемые файлы, DLL и офисные файлы в карантин, чтобы предотвратить дальнейшее распространение вредоносного ПО и попытки запуска зараженных файлов.
- **Классификация условно вредоносного ПО:** Traps позволяет идентифицировать не вредоносное, но нежелательное ПО, такое как рекламное ПО, и не допускать его запуск.
- **Ограничение по выполнению программ:** технология Traps позволяет организациям определять политики по ограничению определенных сценариев выполнения программ.

CORTEX™ BY PALO ALTO NETWORKS

Traps играет ключевую роль в платформе Кибербезопасности

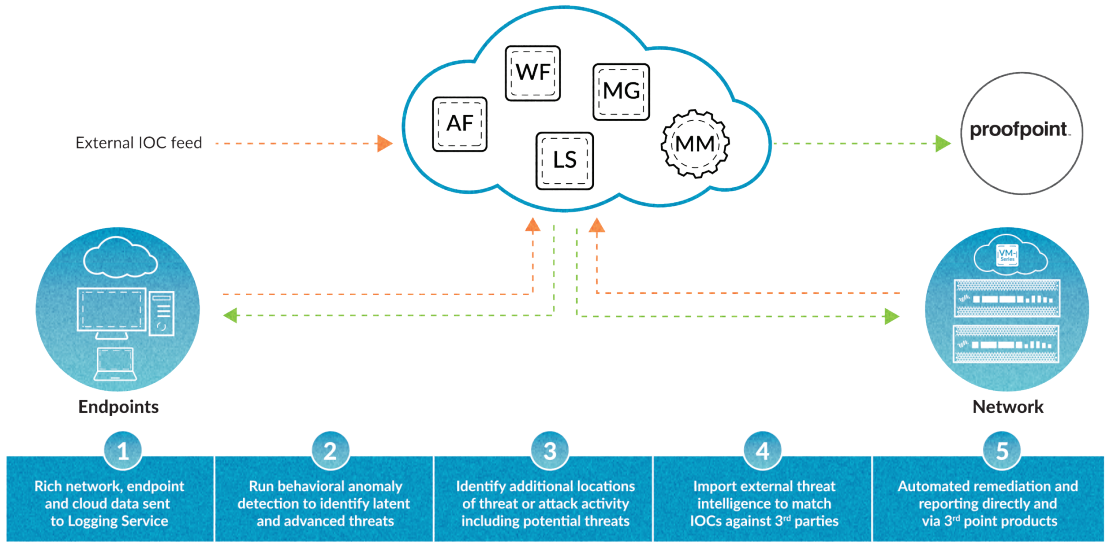
Traps передает данные о вредоносном ПО в облако WildFire, которое автоматически создает и отправляет новые методы предотвращения угроз для Traps и NGFW в течение 5 минут и без участия человека. Это значительно улучшает всю структуры системы безопасности, поскольку позволяет предотвращать случаи проникновения неизвестного вредоносного ПО через периметр.

Traps может отправлять свои логи в облачный сервис Logging Service

Это позволяет рассматривать логи безопасности вместе в одном контексте, обеспечивая корреляцию логов уровня сети и рабочих станций. Общая картина событий безопасности дает возможность обнаруживать угрозы, которые могли бы остаться незамеченными.

Traps объединяет все вместе

Как только Traps обнаруживает вредоносное ПО на конечном устройстве, оно добавляет это устройство в динамическую адресную группу политики, которая может изолировать зараженное устройство от всех остальных устройств сети. Кроме этого, автоматически может быть создан сервисный тикет для команды по расследованию инцидентов, То, что ранее делалось вручную, теперь может происходить без участия человека.



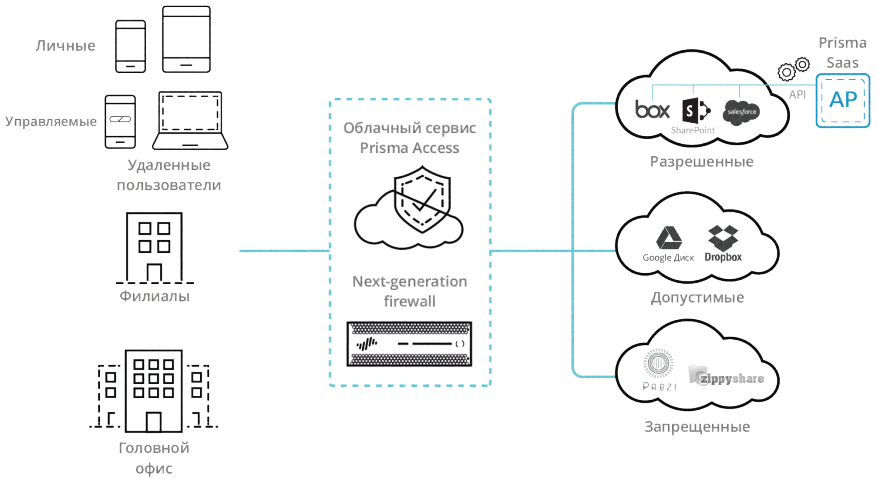
БЕЗОПАСНОСТЬ SAAS-ПРИЛОЖЕНИЙ

PRISMA SaaS

Использование облачных сервисов, таких как Office 365®, приложений Google, Salesforce® и т.д., значительно облегчает работу ИТ-служб и конечных пользователей. В то же время, такие приложения содержат скрытые угрозы: опасность утечки данных, возможность сложных атак на организацию, распространение вредоносного ПО и т.д.

Чтобы служба информационной безопасности имела полный контроль над используемыми SaaS-приложениями, должны быть четко определены допустимые приложения, а также действия пользователей, допустимые в данных приложениях.

Prisma SaaS обеспечивает снижение рисков компрометации сервисов SaaS. Prisma Saas напрямую подключается к облачному сервису, чтобы обеспечить классификацию данных, предотвращение утечек и обнаружение угроз, что дает возможность пользователям безопасно использовать разрешенные облачные приложения.



PRISMA
BY PALO ALTO NETWORKS

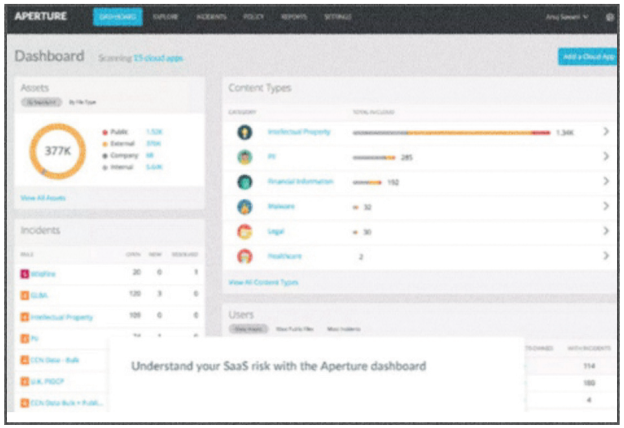
Функции CASB (брокер безопасного доступа к облачным сервисам)

При помощи сервиса Prisma Saas вы получаете полноценное решение класса CASB. Подключение к облачным приложениям происходит по специальным API и позволяет проверять весь трафик, а также устанавливать связь между трафиком и пользователем вне зависимости от его местоположения и типа устройства и настраивать политики безопасности. Сервис Prisma Saas обеспечивает полную визуализацию и отчетность, мгновенную классификацию пользователей и наблюдение за их активностью и действиями с файлами. Результаты анализа данных о каждодневном использовании сервиса позволяют быстро определять риски утечек данных или нарушений политик безопасности.

Сервис Prisma Saas позволяет тонко настраивать политики безопасности, в том числе, в случае заражения, отправлять в карантин файлы или временно изолировать пользователей. Таким образом, вы получаете возможность быстро и легко выполнить требования регуляторов, такие как PCI-DSS, сохраняя преимущества использования облачных приложений.

Защита от сложных атак

Благодаря интеграции с облачным сервисом WildFire, Prisma Saas это единственное решение класса CASB, которое может успешно бороться с угрозами нулевого дня. Вы можете предотвращать распространение вредоносного кода в разрешенных приложениях SaaS, не допуская появления новой уязвимой области для проникновения вредоносного ПО. Данные о новом вредоносном ПО, обнаруженном сервисами Prisma Saas и WIidFire, передаются на другие сервисы единой платформы кибербезопасности Palo Alto Networks, что значительно усиливает защиту вашей ИТ--инфраструктуры.



Преимущества Prisma Saas

Prisma Saas - облачный сервис, не требующий использования прокси или агентов. Он напрямую подключается к приложениям SaaS и анализирует данные, хранящиеся на любом источнике, вне зависимости от используемого устройства или местоположения. Так как Prisma Saas не устанавливается в разрыв, это никак не влияет на производительность приложений и не вносит никакие задержки, т.е. никак не отражается на работе конечного пользователя.

PRISMA™ CLOUD
BY PALO ALTO NETWORKS

Prisma Cloud Compute Edition

Проблемы безопасности в облачных средах

Традиционные инструменты и методологии безопасности не подходят для защиты облачных приложений, управляемых разработчиками и не привязанных к инфраструктуре:

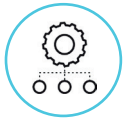
- Разработчики и команды DevOps играют жизненно важную роль в создании и развертывании облачных приложений, зачастую работая вне поля зрения традиционных технологий безопасности. Требуются решения по безопасности, которые интегрируются с инфраструктурой и инструментами разработчиков.
- Организации используют всё более разнородную инфраструктуру: физические сервера, частные облака, публичные облака или любые их комбинации.
- В облачных средах процесс изменений никогда не останавливается. От решений безопасности требуется автоматизация защиты растущего числа постоянно меняющихся микросервисов.

Комплексная защита хостов, контейнеров и функций

Prisma™ Cloud Compute Edition – это ведущая облачная платформа безопасности, обеспечивающая целостную защиту хостов, контейнеров и бессерверных вычислений на протяжении всего жизненного цикла приложений независимо от базовой вычислительной технологии или облака, в котором они работают.

Управление уязвимостями: Обнаруживает и блокирует уязвимости на уровне ОС, фреймворка приложений и отдельных сборок на протяжении всего жизненного цикла приложения (от процесса разработки до эксплуатации) .

Регуляторное соответствие: Обеспечивает регуляторное соответвствие на протяжении всего жизненного цикла приложения. Готовые шаблоны для HIPAA, PCI, GDPR и NIST SP 800-190, а также проверки для Docker, Kubernetes, Linux CIS Benchmarks, Istio®.



Интеграция с CI/CD : Полностью интегрируется в процесс разработки и доставки приложений. Автоматизированные и пользовательские политики могут блокировать сборку или публикацию на основании выявленных уязвимостей или несоответствий стандартам.

Runtime defense: Обеспечивает защиту инфраструктуры при помощи машинного обучения. Автоматически создаёт основанные на белых списках модели поведения приложений с минимально необходимыми привилегиями.

Cloud-native firewalls: Изучает топологию сетевого взаимодействия приложений и реализует необходимую изоляцию для каждого микросервиса, обеспечивая защиту на сетевом и прикладном уровне (WAF).

Контроль доступа: Позволяет управлять секретами, формировать и применять детализированные политики, регулирующие доступ пользователей к ресурсам Docker и Kubernetes с возможностью мониторинга их активностей.

PRISMA™ CLOUD
BY PALO ALTO NETWORKS

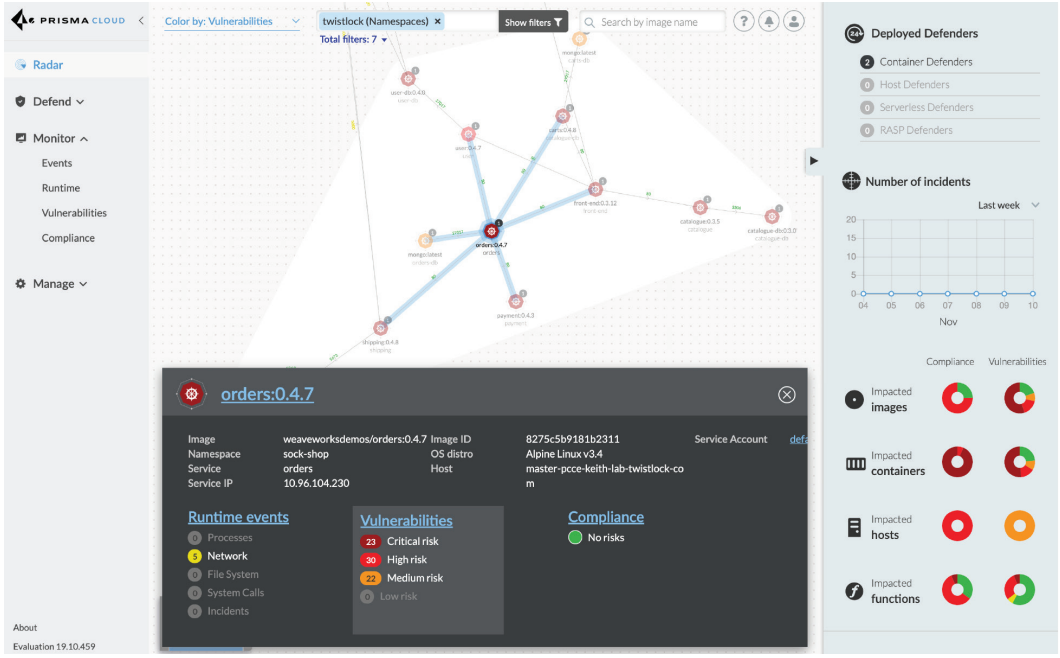
Архитектура

Prisma Cloud Compute Edition поставляется в виде образа контейнера и поддерживает множество вариантов развертывания: в публичных, частных (включая полностью изолированные) или гибридных облачных средах.

Defenders – это агенты, устанавливаемые внутри инфраструктуры, защищающие как виртуальные машины или физические хосты, так и контейнеры, кластеры Kubernetes, CaaS, PaaS и serverless приложения. Они изучают нормальное поведение приложений и предотвращают любые аномальные действия, а также обеспечивают комплексную защиту на основе технологий машинного обучения, комбинируя в моделях локальную активность и сетевое взаимодействие приложений.

Prisma Cloud Compute Edition позволяет управлять уязвимостями и регуляторным соответствием на протяжении полного жизненного цикла приложения путем интеграции с CI/CD процессом, реестром образов Docker, репозиторием кода и любой производственной средой, непрерывно оценивая факторы риска и приоритезируя события. Возможности разграничения доступа к системе и приложениям внутри нее по ролям позволяют безопасно и удобно управлять всей распределенной инфраструктурой, секретами, журналами Kubernetes, инструментами IAM.

Для получения дополнительной информации посетите www.paloaltonetworks.com.



Ключевые преимущества

- **Следуйте трендам и используйте любые облачные технологии.** Выберите подходящую архитектуру для своего приложения и будьте уверены, что Prisma Cloud обеспечит ее защиту.
- **Правильно приоритезируйте риски в облачных средах.** Используйте схемы взаимодействия и данные об угрозах для непрерывного анализа уязвимостей и определения приоритетов рисков во всей облачной инфраструктуре на протяжении всего жизненного цикла приложений.
- **Автоматизируйте безопасность на скорости DevOps.** Предоставьте командам разработчиков и DevOps возможность публикации приложений как можно быстрее, чтобы повысить эффективность бизнеса одновременно с повышением безопасности.

THREAT INTELLIGENCE
AUTOFOCUS

Сервис данных об угрозах AutoFocus™ позволяет экономить время и ресурсы для предотвращения угроз за счет ускоренного анализа и корреляции данных. Уникальным целевым атакам автоматическиприсваивается высокий приоритет с указанием полного контекста, что позволяет службе безопасности отвечать на критические атаки быстрее без использования дополнительных ресурсов IT-системы.

Помощь при определении приоритетов безопасности

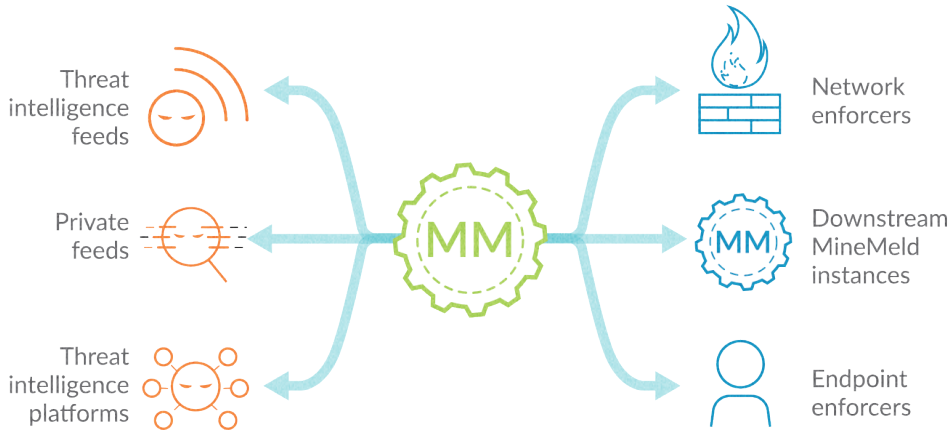
Сервис AutoFocus позволяет вам отличать наиболее важные угрозы от обычных повседневных типовых атак. Теперь вместо того, чтобы просто получать индикаторы атак, вам сразу же будут предоставлены все данные об атаке, такие как семейство вредоносного ПО, кампания или злоумышленник, который организовал атаку на вашу организацию и т.д. При идентификации угрозы Auto-Focus направляет службе безопасности предупреждение о событиях с высоким приоритетом, что позволит вам незамедлительно принять какие-либо действия и уменьшить потенциальное вредное воздействие.

paloalto NETWORKS

Технологии Traps:

Сервис AutoFocus обеспечивает беспрецедентную наглядность представления неизвестных угроз. Он получает и коррелирует данные от следующих сервисов:

- WildFire - самая крупномасштабная аналитическая среда для анализа вредоносного ПО
- PAN-DB сервис классификации и фильтрации URL
- MineMeld – агрегация/корреляция фидов от сторонних поставщиков в AutoFocus
- Traps – не имеющее аналогов средство защиты конечных устройств.
- Prisma Saas - сервис защиты SaaS-приложений
- Unit 42 – команда, отвечающая за сбор и анализ информации об угрозах
- Информацией об угрозах безопасности от технологических партнеров
- Глобальная пассивная DNS сеть Palo Alto Networks



Ускоренный анализ и упрощенные рабочие процессы

Ранее используемые подходы по обеспечению безопасности основывались на увеличении количества предупреждений об обнаружении угроз с последующим проведением сложного анализа событий в системе. Сервис AutoFocus позволяет упростить процесс обмена информацией об угрозах безопасности, что значительно сокращает время, необходимое для проведения анализа, криминалистики или операций по отслеживанию. Функция обмена информацией об угрозах безопасности доступны непосредственно из сервиса управления Panorama и портала AutoFocus.

Агрегация данных из разных источников

Организации используют разные источники данных по threat intelligence для более полной визуализации растущих угроз, но достаточно сложно агрегировать, коррелировать и проверять индикаторы от разных источников. Как часть AutoFocus, сервис MineMeld обеспечивает единый унифицированный источник данных различных поставщиков threat intelligence.

Защита на основе threat intelligence

Специалистам по безопасности требуется нечто больше, чем обычный источник threat intelligence – необходимы механизмы автоматического создания инструментов контроля для предотвращения будущих атак. AutoFocus упрощает процесс создания и применения новых механизмов контроля, от полностью автоматических до настраиваемых пользователем, внутри общей платформы кибербезопасности.

Поиск событий	Кто стоит	Реагирование
Статистический анализ позволяют выявлять критические события информационной безопасности	за атакой Идентификация исполнителя и техник атаки	на инцидент Блокировка соответствующих индикаторов

XSOAR

Операционная система управления ИБ

Полное управление инцидентами:

Отслеживание метрик SLA, сбор улик и журналирование, мобильное приложение, соответствие требованиям регуляторов.

Умная автоматизация и оркестрация:

Автоматические плейбуки, высокая доступность, кросс--корреляция.

Интерактивное расследование:

War Room на основе ChatOps, инструментарий для расследования, совместная работа в режиме реального времени.

Гибкое и масштабируемое развертывание:

Решение доступно для развертывания как в облаке, так и в локальной сети заказчика, поддержка мультиарендных сред с изоляцией данных и расширяемой архитектурой, возможность работы в прокси режиме для сегментированных сетевых сегментов, поддержка внешних чатботов (Slack mirroring).

A SOC's Challenges

Специалисты SOC в своей работе постоянно сталкиваются с огромным числом эволюционирующих сложных угроз.

Аналитики Tier-1 тонут в огромном количестве событий и задачах, для решения которых требуется большое количество времени: идентификация ложных срабатываний, выполнение повторяющихся ответов и анализе событий с большого числа различных средств ИБ.

Перед аналитиками Tier-3 всегда стоит проблема поиска реального инцидента среди цифрового шума, аналогично поиску иглы в стогу сена. Им достаточно сложно координировать работу многочисленных решений ИБ, которые находятся в их распоряжении, наиболее эффективным образом. Ввиду своей высокой загрузки, у них также не хватает времени, чтобы обучать начинающих аналитиков для помощи себе.

Для менеджеров SOC проблемой является попытка посчитать ROI, которое приносят решения ИБ для их SOC. Также перед ними стоит проблема постоянного давления SLA и неполных метрик контроля и документирования. Кроме того, угроза недостатка уровня знаний всегда висит у них над головой: в случае увольнения ведущего аналитика мы получаем значимые недостатки экспертизы и сразу же много шагов назад для SOC.

Это тот момент, когда появляется решение Demisto – SOAR (Security Orchestration, Automation, and Respons) платформа, объединяющая в себе управление инцидентами, процессы автоматизации и оркестрации, а также расследования инцидентов для помощи командам ИБ в их повседневной работе.

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Последовательные, прозрачные и документированные процессы

- Реагирование на основе плейбуков
- Автоматическое документирование всех запросов по поиску и расследованию
- Автоматическое детектирование дублированных Расследований
- Поиск между расследованиями, индикаторами и Уликами

Ускорение времени решения и лучшая эффективность SOC

- Портфолио настраиваемых плейбуков для автоматизации повторяющихся и резервных шагов
- Виртуальная “War Room” для совместных расследований в режиме реального времени
- Детализированное отслеживание инцидентов и метрик аналитиков
- Улучшение продуктивности аналитиков и совместное обучение команды
- Платформа для совместной работы позволяет аналитикам делится результатами расследования
- Обучение аналитиков по результатам прошлых расследований
- Подсказки на основе машинного обучения для выбора аналитика, ответных действий или аналогичного инцидента

Полный процесс управления инцидентами

Платформа Demisto помогает управлять всеми аспектами жизненного цикла инцидента:

- Открытая и расширяемая платформа с интеграцией со всеми необходимыми средствами, включая средства по обогащению данных, фиды Threat Intelligence, SIEM, NGFW, EDR, песочницы, системы анализа, почтовые системы и многое другое.
- Интуитивные плейбуки в режиме plug'n'play для автоматизации всех процессов SOC.
- Автоматическое документирование на всех этапах расследования инцидентов для контроля SLA.
- Хранилище индикаторов с возможностью контекстного поиска для хантинга.
- Мощный поиск с автоматическим детектированием дублированных расследований.
- Удобная панель управления с настраиваемым отчетами и архивированием результатов.
- Агенты для Windows/Mac/Linux OS для сбора данных с конечных узлов.
- Мобильное приложение с персонализируемыми настройками рабочего стола и задачами по расследованию инцидентов.

Умная автоматизация и оркестрация

Оркестрация Demisto как идеальная связь между людьми, процессами и технологиями:

- Портфолио плейбуков для автоматизации, включая более 100 интеграций и 1000 выполняемых задач ИБ.
- Динамические плейбуки, избавляющие аналитиков от рутинных задач, а конечных пользователей от постоянного ответа на электронную почту.
- Гибкость в создании новых функций/блоков и переноса их между плейбуками.
- Отказоустойчивость и высокая доступность плейбуков.Очень легко проверить работоспособность и начать действие с любой точки плейбука.
- Машинные подсказки при работе с инцидентами, повторяющиеся индикаторы в разных инцидентах

Интерактивное расследование

Интерактивное расследование Demisto помогает аналитикам в совместной работе и делает их умнее с каждым инцидентом:

- Виртуальная 'War Room', основанная на ChatOps, где аналитики могут совместно общаться в режиме реального времени и выполнять различные задачи.
- Инструментарий по расследованию инцидентов, обеспечивающий настраиваемую карту взаимосвязи инцидентов во времени.
- Специальный бот (In-house security bot (DBot)), помогающий выполнять команды, предлагать помощь других аналитиков и будущее направление действия.
- Механизм сбора улик и автоматического документирования с возможностью комментирования и сохранения заметок. инцидентами, повторяющиеся индикаторы в разных инцидентах

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ | ОРКЕСТРАЦИЯ | СОВМЕСТНАЯ РАБОТА

DBot – бот с искусственным интеллектом

В дополнение к решению текущих проблем SOC's, Demisto Enterprise использует силу искусственного интеллекта и машинного обучения в своем боте. Подсказки DBot доступны в системе тикетов, анализе задач, выборе аналитика и аналогичного инцидента. Машинное обучение используется во всех трех основных компонентах решения – управлении инцидентами, автоматизации и оркестрации и интерактивном расследовании. С каждым новым инцидентом аналитик и DBot становятся умнее, что снижает общее время на защиту от новых сложных угроз.

Palo Alto Networks

3000 Тэннери Уэй
г. Санта-Клара. шт. Калифорния 95054
Служба поддержки: +1.866.898.9087
www.paloaltonetworks.com