Преимущества для бизнеса

- **Контроль над неуправляемыми устройствами**. Вы сможете идентифицировать все неизвестные IoT-устройства и устранить до 30% рисков.
- **Меньше проблем с защитой периметра**. Встроенный механизм предотвращения блокирует угрозы уже на периметре, избавляя ИБ-специалистов от малозначимых алертов.
- **Использование имеющихся ресурсов**. Дайте вашим специалистам по сети, безопасности и эксплуатации мощный инструмент для защиты IoT-среды без изменения процедур или политик.
- **Предсказуемое и упрощенное лицензирование**. Никаких утомительных сверок количества устройств: подписка IoT Security лицензируется просто по покрытию сети.
- **Легкое развертывание и максимальная отдача от инвестиций**. Добавьте поддержку IoT к имеющемуся у вас межсетевому экрану нового поколения Palo Alto Networks на базе машинного обучения, не выстраивая дополнительную инфраструктуру.
- **Без точечных сенсоров**. Всем решениям требуются сенсоры, но с IoT Security заказчики получают ещё и возможности для предотвращения угроз, сегментирования и применения политик.
- **Защита корпоративного класса**. Решение подходит для финансовых, транспортных, образовательных и страховых организаций, ритейла, промышленных и горнодобывающих предприятий, учреждений здравоохранения, умного города, коммунальных служб, региональных и местных органов власти и т.д.

Подписка IoT Security

IoT-устройства выходят из-под контроля безопасности

Неуправляемые устройства интернета вещей (IoT) и операционных технологий (OT) составляют более 30% от всех устройств в корпоративных сетях[1]. Хотя от IoT-устройств зависит функционирование всего бизнеса, организации не могут им доверять: в основном нерегулируемые, зачастую полные уязвимостей и имеющие неограниченный доступ к сети, эти IoT-устройства несут в себе колоссальные риски информационной безопасности. ИБ-специалистов редко привлекают к участию в закупках, и в результате из-за необъятного многообразия сборок, длинных жизненных циклов, а также недостаточной функциональности традиционных средств безопасности, купленные устройства чрезвычайно сложно защитить.

1. «Отчет исследовательской группы Unit 42 об угрозах в IoT-среде за 2020 год», компания Palo Alto Networks, 10 марта 2020 г., https://unit42.paloaltonetworks.com/iot-threat-report-2020.

Существующим решениям для защиты IoT-среды видны только известные устройства и нужны отдельные сенсоры, при этом они не в состоянии отражать атаки самостоятельно, а для применения политик в режим блокировки им требуется внешние интеграции. Поэтому ИБ-специалисты оказываются в весьма затруднительном положении, когда они не в состоянии масштабировать свою работу, расставлять задачам приоритеты и минимизировать риски.

Доверяйте каждому устройству в вашей сети

Компания Palo Alto Networks предлагает первое в отрасли решение для безопасности IoT-среды «под ключ», с которым вы сможете управлять IoT- и OT-устройствами в вашей сети и держать сопутствующие риски под контролем.

Используя машинное обучение для точного определения и классификации любых, даже ранее неизвестных, неуправляемых IoT-устройств, облачный сервис IoT Security, предоставляемый по подписке, анализирует данные из всех доступных источников, чтобы выявлять аномальную активность, непрерывно оценивать риски и предлагать рекомендации для политик и усиления общей безопасности. В сочетании с нашей лучшей в отрасли платформой NGFW на базе машинного обучения, IoT Security может автоматически применять политики, сокращая тем самым нагрузку на сотрудников, и предотвращать все угрозы, обеспечивая защиту устройств. Кроме того, решение просто в развертывании и не требует дополнительных затрат на инфраструктуру.

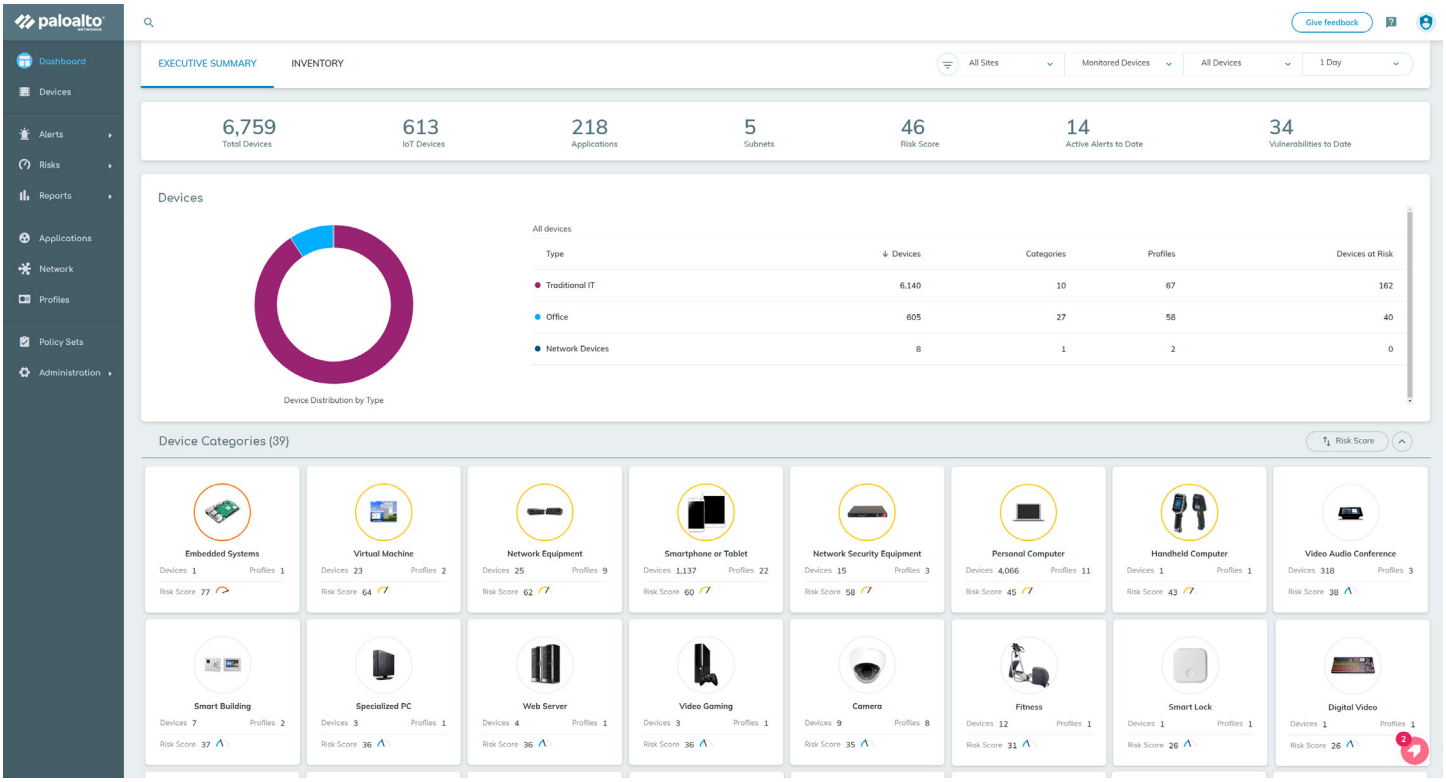

Рис. 1. Инвентаризация устройств в решении IoT Security

Основные возможности

Полная визуализация устройств благодаря машинному обучению

Вы сможете точно идентифицировать и классифицировать все IoT- и OT- устройства в вашей сети, даже те, что появились в ней впервые. Такая точность возможна за счет встроенной в IoT Security технологии App-ID™ от компании Palo Alto Networks, в то время как запатентованная модель трехуровневого машинного обучения ускоряет профилирование устройств. Профили позволяют классифицировать любые IoT-, OT- или IT-устройства и определить их тип, поставщика, модель, а также свыше 50 самых распространенных параметров, в том числе прошивку, ОС, серийный номер, MAC-адрес, физическое местонахождение, подсеть, точку доступа, используемые порты, приложения и многое другое. IoT Security обнаруживает новые устройства без каких-либо ограничений, обычно связанных с использованием сигнатур. Облачный масштаб даёт возможность сравнить использование устройств, исключить период тренировки (soak time), проверить правильность профилей и точно отстроить модели, чтобы ни одно устройство не осталось без контроля.

Непрерывный анализ уязвимостей для приоритизации рисков

Вы сможете найти всю необходимую информацию, чтобы быстро проанализировать уязвимые устройства и инициировать дальнейшие действия. IoT Security объединяет разнородные решения из традиционного ИБ-контура, поэтому специалистам по безопасности проще проводить анализ и оценку обстановки. Профили устройств составляются с помощью машинного обучения по пяти основным характеристикам: внутренние подключения, подключения к интернету, протоколы, приложения и полезная нагрузка. Затем каждый показатель отслеживается в динамике и сопоставляется с показателями аналогичных привлеченных устройств, информацией о патчах, выпущенной производителем устройства, аналитикой угроз от группы Unit 42 и общим перечнем уязвимостей и рисков (перечень CVE), что позволяет непрерывно анализировать риски. Исходя из степени риска, рассчитанной по Общей системе оценки уязвимостей (CVSS), можно легко и удобно ранжировать результаты, быстро выявляя поведенческие аномалии и предоставляя подробную информацию об угрозе, чтобы ИБ-специалисты могли реагировать и последовательно уменьшать поверхность атаки.

Быстрое внедрение политик и автоматические рекомендации на основе анализа рисков

Вы без труда сможете вносить изменения в политики, чтобы сократить риски, привносимые IoT-устройствами. IoT Security сравнивает метаданные миллионов IoT-устройств с найденными в вашей сети и с помощью профилей устройств может определить шаблоны нормального поведения. Затем для каждого IoT-устройства и категории устройств рекомендуется политика, позволяющая ограничить или разрешить доверенное поведение. Рекомендованные политики экономят несчетное количество часов, которые при создании политик вручную пришлось бы потратить на сбор данных об использовании приложений, соединениях, портах и протоколах по каждому устройству. Пересмотренные политики можно быстро импортировать в ваш NGFW на базе машинного обучения, и любые изменения будут добавлены автоматически, что минимизирует ваши расходы на администрирование.

Сегментирование устройств и снижение рисков за счет встроенного механизма применения политик

Вы сможете применять передовые ИБ-практики, используя сегментирование с учетом контекста и предотвращая латеральное движение между IoT- и IT-устройствами. IoT Security составляет рекомендации по политикам на основе анализа рисков, что позволяет контролировать передачу данных на IoT-устройствах. Для применения политик IoT Security в паре с NGFW на базе машинного обучения задействует новый элемент политики Device-ID™, благодаря которому можно распространять информацию о профиле устройств и гарантированно контролировать каждое отдельное устройство независимо от сетевого расположения. IoT Security может ещё больше сократить поверхность атаки, предоставив контекст для сегментирования IoT- и IT-устройств в разные VLAN-ы и применяя принцип нулевого доверия.

Предотвращение известных и неизвестных угроз благодаря подпискам на сервисы безопасности

Вы сможете отразить все атаки на ваши IoT-устройства с помощью лучшей отраслевой системы предотвращения вторжений (IPS), инструментов анализа вредоносного ПО, а также технологий предотвращения атак через веб и DNS. Для загруженной ИБ-команды каждое оповещение от средства защиты – это дополнительная задача, требующая расследования и принятия мер. Кроме целевых атак, на IoT-устройства обрушиваются устаревшие и забытые вирусы и черви, которые изначально предназначались IT-устройствам. Подписки на наши облачные сервисы безопасности, органично интегрируемые с решением IoT Security, позволяют координировать аналитические данные, чтобы предотвращать все угрозы для IoT- и IT-среды, не создавая дополнительной нагрузки на специалистов по безопасности. Время реагирования тоже сокращается, так как IoT-устройства с подтвержденными угрозами можно оперативно изолировать, как только угроза обнаружена вашим NGFW на базе машинного обучения. Так, ИБ-специалисты могут спокойно составить план по исправлению последствий атаки, не боясь дальнейшего распространения вируса с зараженного устройства. Для еще более надежной защиты решение IoT Security можно дополнить подписками на следующие сервисы безопасности:

- **Threat Prevention**: Решение для предотвращения угроз превосходит традиционные IPS-системы и автоматически отражает все известные атаки по всему трафику за один проход.
- **WildFire®**: Сервис противодействия вредоносному ПО гарантирует безопасность файлов, так как автоматически обнаруживает и отражает атаки неизвестного вредоносного ПО благодаря лучшим в отрасли облачным инструментам анализа.
- **URL Filtering**: URL-фильтрация обеспечивает безопасное использование интернета, блокируя доступ к известным и новым вредоносным веб-сайтам еще до того, как пользователи смогут на них зайти.
- **DNS Security**: Сервис безопасности DNS отражает атаки, проводимые через систему доменных имен и направленные на command-and-control и кражу данных, при этом не требуя изменений в инфраструктуре.
- **GlobalProtect™**: Сервис сетевой безопасности для хостов позволяет NGFW на базе машинного обучения распространить защиту на удаленных пользователей, обеспечивая целостную защиту всей вашей среды.

Легкое развертывание и использование из облака

Уникальное сочетание решения IoT Security от компании Palo Alto Networks и NGFW на базе машинного обучения – это первое в отрасли комплексное решение для визуализации, предотвращения атак, оценки рисков и применения политик, предлагаемое заказчикам Palo Alto Networks. Такая комбинация решений позволяет ИБ-специалистам незаметно для пользователей улучшить как работу выстроенной сети, так и защиту IoT-среды – и для применения политик не нужно больше никаких долгих интеграций со сторонними инструментами.

Текущие заказчики Palo Alto Networks

IoT Security доставляется по подписке как облачный сервис безопасности, который даст вашим ИБ-специалистам возможность взять под контроль неуправляемые IoT-устройства через несколько минут после активации. Достаточно активировать решение IoT Security для любого форм-фактора вашего NGFW (например, PA-Series, VM-Series или Prisma™ Access).

При подписке на облачные сервисы безопасности Threat Prevention, WildFire, URL Filtering и DNS Security они автоматически усилят ваши возможности по предотвращению угроз, чтобы обмениваться аналитикой и блокировать все известные и неизвестные угрозы, направленные на ваши IT- и IoT-устройства.

Потенциальные заказчики Palo Alto Networks

При подписке на IoT Security наш лучший в отрасли NGFW на базе машинного обучения будет работать и как сенсор, и как точка применения политики. Эта мощная комбинация решений позволяет обнаруживать неуправляемые устройства, предотвращать угрозы, оценивать риски и применять политики в таких местах сети, где редко развертывают обычные МСЭ. Вам больше не придётся закупать, интегрировать и обслуживать множество точечных продуктов, а также перестраивать операционные процессы, чтобы добиться целостной безопасности IoT-среды.

Ни одно решение по безопасности IoT не работает без сенсоров, но только в IoT Security от Palo Alto Networks такой датчик, помимо прочего, предотвращает угрозы и обеспечивает применение политик, а значит, повышает окупаемость инвестиций и сокращает операционные расходы.

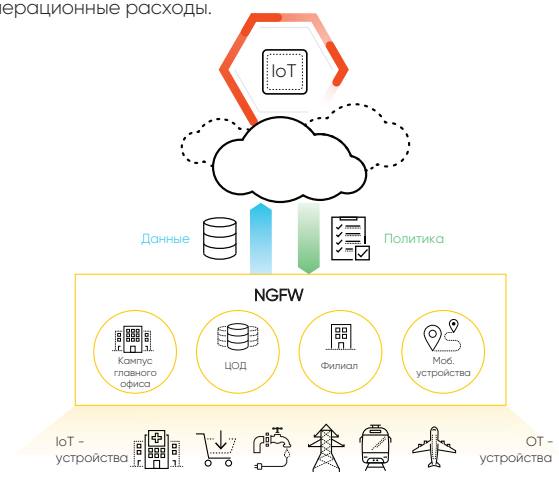

Рис. 2. Архитектура решения IoT Security с NGFW для визуализации, предотвращения угроз и применения политик

Эксплуатационные преимущества

Подписка на IoT Security позволит вам:

- **Ограничить операционные расходы и издержки на инфраструктуру**. Больше не нужно разворачивать и обслуживать разрозненные датчики, перестраивать процессы или создавать интеграционные схемы, ведь IoT Security обеспечит ИБ-специалистами полную визуализацию ваших устройств.
- **Сократить время развертывания решения на 90%**. Больше не придется ждать несколько месяцев, ведь IoT Security можно развернуть за считанные минуты, а затем идентифицировать и классифицировать каждое, даже неизвестное, IoT-устройство в течение 48 часов.
- **Быстро обнаруживать все устройства с помощью машинного обучения**. Воспользуйтесь преимуществами бессигнатурного подхода для идентификации и понимания быстро меняющихся IoT-устройств.
- **Понять весь контекст устройства**. Воспользуйтесь информацией об IoT-устройствах в вашем NGFW на базе машинного обучения для сегментирования, политик и реагирования на инциденты с учетом контекста.
- **Сэкономить значительную часть рабочего времени на оценке рисков, устранении неполадок и разработке политик**. Вы сможете легко защитить устройства с помощью автоматизированного анализа рисков, рекомендаций по политикам и составления профилей поведения.
- **Легко применять политики на основе принципа нулевого доверия**. Вы сможете разрешать только модели доверенного поведения IoT-устройств с помощью технологий App-ID™, User-ID™ и Device-ID™ на ваших NGFW на базе машинного обучения.
- **С легкостью разворачивать и обслуживать сервисы.** Активируйте подписки на облачные сервисы и централизованно управляйте безопасностью с помощью Panorama.
- **Воспользоваться единым предложением для получения всесторонней отраслевой аналитики**. Вы сможете обеспечить безопасность в системах здравоохранения, корпоративных ИТ, нефтегазовой отрасли, умных городах и средах АСУТП с поддержкой протоколов АСУТП и транзакций.
- **Полностью обезопасить IoT-среду**. Всего один продукт обеспечит вам полную визуализацию, предотвращение угроз и применение политик в отношении каждого IoT- и OT-устройства в сети.

Таблица 1. Функции и возможности решения IoT Security от компании Palo Alto Networks

Обнаружение и классификация IoT- и OT-устройств (тип, поставщик, модель и свыше 50 специфических параметров)	Предотвращение всех известных угроз
Составление профилей на IoT- и OT-устройства с помощью запатентованной модели трехуровневого машинного обучения	Оценка уязвимостей через интеграцию с общим перечнем уязвимостей и рисков (перечень CVE)
Обнаружение поведенческих аномалий	Расчет степени риска по Общей системе оценки уязвимостей (CVSS)
Рекомендации по политикам на основе анализа рисков	Автоматическое применение политик
Сертификация средств контроля обслуживающей организации SOC 2 (Тип II)	

Таблица 2. Краткие сведения о конфиденциальности и лицензировании

Конфиденциальность	
Надежность и конфиденциальность	Palo Alto Networks обеспечивает строгий контроль конфиденциальности и безопасности, чтобы предотвратить несанкционированный доступ к конфиденциальным или персональным данным. Мы следуем передовым отраслевым стандартам и практикам в сфере безопасности и конфиденциальности. С более подробной информацией вы можете ознакомиться в наших Технических описаниях обеспечения конфиденциальности.
Лицензирование и требования	
Требования	Межсетевые экраны нового поколения Palo Alto Networks с версией PAN-OS 8.1 или выше (в версии PAN-OS 10.0 есть встроенный механизм для автоматического применения политик благодаря новому элементу политики Device-ID).
Рекомендуемая среда	Межсетевые экраны нового поколения Palo Alto Networks разворачиваются в сегментах сети и на точках выхода в интернет везде, где есть IoT-устройства.
Лицензия IoT Security	Для работы IoT Security нужна отдельная лицензия, которая предоставляется как комплексная подписка на облачный сервис для межсетевых экранов нового поколения Palo Alto Networks.
Поддерживаемые МСЭ нового поколения	Все модели межсетевых экранов серий PA и VM, кроме PA-220, VM-50 и VM-200.

3000 Tannery Way Santa Clara, CA 95054

Основной номер: +1.408.753.4000
Отдел продаж: +1.866.320.4788
Служба поддержки: +1.866.898.9087

www.paloaltonetworks.com