PALO ALTO NETWORKS
Система безопасности облаков APERTURE

Безопасность ваших приложений SaaS

Использование приложений SaaS увеличивает риски безопасности, включая распространение вирусных угроз, утечки данных, а также нарушения нормативных требований.

Задача

Достижение безопасности и контроля за использованием приложений SaaS с целью предотвращения вирусных угроз и утечки данных

Решение

Компания Palo Alto Networks имеет богатый опыт безопасного разрешения приложений посредством контроля за несанкционированными приложениями и управлением доступом к разрешенным приложениям.

Система защиты SaaS под названием Aperture™ дополняет платформу безопасности нового поколения Palo Alto Networks, обеспечи вая уникальный подход к безопасности разрешенных в компании приложений SaaS. Aperture привносит полную визуализацию по всем пользователям, папкам и файловой активности в рамках приложения SaaS, а также предоставляет детальный анализ и аналитику использования приложения для предотвращения рисков, связанных с данными, и нарушения нормативных требований. Кроме того, она реализует детальный контекстно-зависимый контроль за приложениями SaaS для наблюдения за пользователями и автоматического изолирования конфиденциальных данных при возникновении любых опасных ситуаций.

Внедрение системы безопасности Aperture совместно с облачным сервисом анализа угроз Palo Alto Networks WildFire™ предотвращает известные и неизвестные угрозы, распространяющиеся через санкционирование приложения SaaS, предотвращая тем самым проникновение вредоносных программ.

Концепция местонахождения данных лишь в едином централизованном месте уже не применяется в современных информационных сетях. Сейчас данные организаций расположены сразу в нескольких точках по миру, причем многие из этих точек, не контролируются данными организациями. Несмотря на местонахождение данных, ИТ-отдел все еще несет ответственность за безопасность их при хранении, обработке и передаче. Данная задача более сложна при использовании приложений SaaS. Использование таких приложений вызывает трудности контроля или визуализации процесса перемещения данных за периметр корпоративной сети. Это представляет собой проблему, поскольку конечные пользователи теперь играют роль своих собственных ИТ отделов, которые контролируют приложения, которые они используют и то, как именно они их используют, но без необходимой экспертизы по защите данных или оценке и предотвращению рисков и угроз. Без надлежащих инструментов, обеспечивающих визуализацию уязвимостей для данных компании и проникающих угроз, даже опытные пользователи с опытом в сфере безопасности, могут столкнуться с проблемами в рамках приложений SaaS.

PALO ALTO NETWORKS
Система безопасности облаков APERTURE

Для получения контроля над использованием приложений SaaS, вам необходимо начать с определения списка приложений SaaS, которые подлежат контролю и использованию в компании, и какие поведенческие действия допустимы в рамках выбранных приложений. Это требует четкого определения какие именно приложения считаются «санкционированными» или допустимыми и предусмотренными отделом ИТ; какие считаются «нейтральными» или не предусмотренными отделом ИТ, но допустимыми в рамках ограничений в условиях потребностей вашего бизнеса; и какие именно считаются «несанкционированными» или не допустимыми. Затем, применяются решения для обеспечения контроля за использованием данных приложений.

Привнесение индивидуальных рисков при использовании санкционированных приложений SaaS
Как только любое из приложений SaaS определяется как санкционированное, и данные помещаются в то облако, где находится данное приложение, возникают новые трудности. Данные уже не находятся под контролем организации и часто их становится невозможно отслеживать. Специалисты SaaS делают все возможное для защиты этих данных в приложениях, но, в конечном счете, они не несут за них ответственность. Как и за любую часть информационной сети, за таковые данные несут ответственность специалисты отдела ИТ, с целью их защиты и контроля, не смотря на их местоположение.

Злоумышленники извне
Постоянные атаки на сети приводят к значительной обеспокоенности безопасностью приложений SaaS. Приложение SaaS становится новой отправной и распределительной точкой для вредоносных программ, используемой злоумышленниками извне. Некоторые вредоносные программы даже специально нацелены на приложения SaaS, используя их для распространения вредоносного кода, и, таким образом, осуществлению атак на других сотрудников.

Случайная незащищенность данных
Конечные пользователи зачастую сами являются одним из наиболее обычных рисков в рамках приложений SaaS. Действуя из лучших побуждений, они обычно не обучены и не знакомы с рисками, которые несут их действия. Так как используемые приложения SaaS разработаны для облегчения обмена данными, необходимо понимать, что эти данные могут стать непреднамеренно вредоносными. По большей части самими большими рисками в рамках приложений SaaS являются три типа случайной незащищенности данных конечным пользователем, которые на удивление являются довольно стандартными. Вот они:

• Случайный обмен данными: это когда обмен данными был предназначен для определенного лица, но случайно данные были переданы другому лицу или группе лиц или всему Интернету. Это стандартно случается при автозаполнении, либо в случае опечатки, что случайно ссылается на старый электронный адрес или неверное имя, группу или даже пользователя извне.

• Нелегитимный доступ к данным: это когда установлен легитимный обмен данными, но пользователь продолжает осуществлять данный обмен с другими лицами, которые не должны иметь доступ к этим данным. Это обычно заканчивается раскрытием содержимого данных для всех, так как данный процесс может зайти очень далеко.

• Обмен данными с уволенными сотрудниками: это когда работники и специалисты уже больше не работают в компании и больше уже не должны иметь доступ к данным, но до сих пор продолжают обмениваться данными. Без наличия надлежащих инструментов, обеспечивающих визуализацию и контроль за обменом данными, очень сложно отслеживать и регистрировать вышеуказанное, а также быть в курсе легитимности своей финансовой документации.

Злоумышленники внутри компании
Наименее стандартным из трех, в рамках приложений SaaS, является злоумышленник внутри компании, внутренний пользователь, который целенаправленно осуществляет обмен данными в целях кражи или мщения. Это может быть простой работник, покидающий компанию, установивший все папки на режим публичного доступа либо их получение через внешний электронный адрес с целью кражи данных с удаленного местоположения.

PALO ALTO NETWORKS
Система безопасности облаков APERTURE

Требования к безопасности приложений SaaS
Для получения контроля над использованием санкционированных приложений SaaS, необходимо соблюдать некоторые ключевые требования.

Защита от угроз
Защита от вредоносных программ является общей задачей обеспечения безопасности информационной сети, что не зависит от использования приложений SaaS. На самом деле, приложения SaaS привносят новые риски возникновения угроз, которые также нуждаются в понимании и контроле. Одним из наибольших рисков, является то, что многие из них автоматически синхронизируют файлы с пользователями. Помимо всего прочего, многие люди используют их для обмена данными с третьими лицами, которые не находятся под контролем компании. Комбинация этих двух типов использований приложений SaaS представляет собой новую возможность для проникновения вредоносных программ, которые могут не только проникнуть извне при обмене данных, но также и автоматически синхронизировать зараженные файлы всей организации без вмешательства пользователя.
Для надлежащей борьбы с новой опасностью угроз для SaaS, вам необходимо решение, которое поможет предотвратить размещение файлов в санкционированных приложениях SaaS, в независимости от того, является ли вредоносная программа известной или неизвестной, а также в независимости от источника файла. Необходимо остановить угрозу в источнике до того, как у нее появится возможность распространиться повсюду.

Визуализация и контроль уязвимости данных
При определении и контроле использования приложения SaaS посредством сконфигурированных политик, происходит перемещение данных в приложения, которые компания пометила как санкционированные. Как только данные достигнут облачного сервиса, они разместятся в рамках приложения SaaS и уже больше не будут визуализироваться в рамках периметра информационной сети организации. Это традиционно является «мертвой зоной видимости» для отдела ИТ. Изменения, такие так вредоносная программа третьих лиц и ненадлежащий обмен данных, также могут представлять опасность, как упомянуто ранее в разделе «Привнесение индивидуальных рисков при использовании санкционированных приложений SaaS, и компания необходимо защищать себя. Дополнительный набор элементов управления специально для уязвимых данных необходим для устранения рисков, являющихся индивидуальными для SaaS. Приоритетом должна быть защита данных в данной среде, т.е. глубокое понимание пользователей, данных, которые они передали и того как они были переданы.

Предотвращение рисков, просто не отвечайте
В отличие от традиционной межсетевой защиты, защита от угроз и уязвимости данных не должна быть встраиваемой функцией, направленной только на события в будущем. Вместо этого, она должна быть направлена в прошлое на все предыдущие данные и их обмен в приложениях, даже до того, как будет задействованы сконфигурированные политики. Таким образом, устанавливаются и разрешаются все ненадлежащие обмены данными, до того, как негативные, существующие в реальном времени триггеры событий потребуют ответа вручную.

Внедрение Aperture компанией Palo Alto Networks
Размещение данных в рамках приложений SaaS, авторизованных компанией, не визуабельно в рамках периметра информационной сети организации. Сервис Aperture позволяет подсоединиться напрямую к санкционированным приложениям SaaS для обеспечения классификации данных, визуализации обмена / санкционированности данных, а также обнаружение угроз в рамках приложения. Это способствует невероятной визуализации, позволяя организациям инспектировать контент на предмет риска нарушений данных и контроля доступа за обменом данных через контекстуальную политику.

Сервис Aperture построена на существующей визуальности SaaS и возможностях сконфигурированного контроля платформы безопасности нового поколения через технологию идентификации приложений App-ID™ с детальным отчетным контролем использования SaaS внутри SaaS. Сервис Aperture привносить визуальность и контроль в рамках приложений SaaS и обеспечивает полную непрерывную безопасность без необходимости в каком-либо дополнительном аппаратном обеспечении, программном обеспечении или изменениях сети.

PALO ALTO NETWORKS
Система безопасности облаков APERTURE

Предотвращение угроз в приложениях SaaS
Песочница WildFire, внедренная в систему защиты Aperture, обеспечивает продвинутую защиту от угроз, блокируя известные вредоносные программы и идентифицируя и блокируя неизвестные вредоносные программы. Данная функция использует интеграции песочницы WildFire с целью предотвращения распространения zero-day угроз по санкционированным приложениям SaaS, предотвращая тем самым новые проникновения вредоносных программ. Информация о новых вредоносных программах, обнаруженных сервисом Aperture, передается всей платформе защиты, даже, если она не находится в контуре приложений SaaS, но защищает другие системы.

Визуализация незащищенности данных
Сервис Aperture обеспечивает полную визуализацию по всем пользователям, папкам и файловой активности, предоставляя подробный анализ, что помогает вам визуально видеть, что происходит в любой момент в любой точке. При наличии возможности видеть глубокую аналитику в рамках ежедневного использования приложений, вы можете быстро определять наличие рисков в отношении данных или нарушений политики использования данных. Этот подробный анализ пользователя и активности данных обеспечивает возможность детального управления данными и проведения судебной экспертизы.
Так как сервис Aperture напрямую подключается к самим приложениям, она обеспечивает непрерывный, скрытый мониторинг рисков в рамках санкционированных приложений SaaS наряду с детальной визуализацией, что раньше было невозможно.

Контекстно-зависимый контроль незащищенных данных
Сервис Aperture позволяет вам устанавливать детальный, контекстно-зависимый контроль, который обеспечивает вас возможностью принуждения к соблюдению требований и изолирования пользователей и данных сразу же после возникновения любых нарушений. Это позволяет вам быстро и легко соблюдать требования о соответствии данных в отношении возможны рисков, такие как PCI и PII, в то же время пользуясь преимуществами облачных приложений.
Данные не обязательно должны быть основаны только на размещаемых файлах, а также не представлять собой «неструктурированные данные». Данные могут являться входными данными приложений – «структурированными данными» - такими, как входные данные Salesforce.com. В обоих случаях сервис Aperture защищает незащищенные данные, способствуя распространенной проблеме незащищенных размещенных файлов, а также самостоятельному размещению входных данных приложений.

Усовершенствованная классификация документов
Сервис Aperture осуществляет проверку документов на предмет наличия конфиденциальных данных, таких как номера кредитных карт, SSH-ключей и номеров социальной страховки, маркируя их в качестве потенциальных рисков, если обмен этими данными был выполнен ненадлежащим образом.

Спецификой сервиса Aperture является возможность идентификации документов по типу посредством усовершенствованной классификации документов, в независимости от данных, которые содержаться в самом документе. Сервис Aperture изначально разработана для автоматической идентификации конфиденциальных документов, таких как финансовые и юридические документы. Механизм классификации документов не только осуществляет заранее определенную классификацию типов документов, но также может поддерживать загрузку индивидуальных документов для последующей классификации, что, в свою очередь, способствует управлению рисками специфических данных.
Например, пустой заказ на закупку может быть загружен в Aperture для классификации документа, т.е. политика документа и его визуализация могут быть отрегулированы для каждого индивидуального документа. Если данная форма будет подлежать незащищенной передаче, это будет промаркировано, как потенциальный риск, в независимости от того, содержаться ли в данном документе конфиденциальные данные.

Ретроспективная политика

Сервис Aperture обладает уникальным подходом к политике, не зависимом от времени. Типичная политика безопасности корпоративной сети является эффективной только в отношении данных, статус которых определен уже после установления политики, так как она распознает только линейные данные и применяет политику исключительно начиная от данной точки и далее. Это не работает в отношении безопасности незащищенных данных SaaS, так как данные, передаваемые сегодня, могли быть изначально переданы и несколько лет назад. Вместе с тем, политики, созданные в Aperture, будут распространяться на всех пользователей и данные от начала создания учетной записи с целью идентификации любых нарушений. Нет необходимости в ожидании кого-то, кто сможет получить доступ к данным, и уже впоследствии решать эту проблему; это предусмотрительно касается всех данных, не смотря на то, насколько старыми являются эти данные или, когда они были переданы.

Политики являются контекстно-зависимыми, что способствует детальному определению рисков незащищенных данных. Это необходимо для возможности использования SaaS пользователями и одновременного предотвращения случайной незащищенной передачи данных. Политики учитывают несколько факторов при создании совокупного риска незащищенности данных. Один или два фактора не могут быть достаточными для установления потенциального риска для обмена теми или иными данными. Это срабатывает только после охвата полного контекста передаваемых данных, который может быть определен как совокупный риск незащищенности данных.

Риски рассчитываются по типу пользователя, типу документа, содержанию конфиденциальной информации, то, каким образом передаются данные и содержится ли в них вредоносная программа. Это обеспечивает возможность управления незащищенностью данных на детальном уровне, основанном на некотором количестве важных факторов.

Например, финансовый отдел имеет возможность обмениваться финансовой информацией с лицами, работающими внутри отдела – но не за его пределами. Даже, если разрешен обмен оригинальных данных, они не имеют права обмениваться данными, содержащими вредоносную программу.

Приложение	Контроль	Компонент
Поле	Поле – персональное	App-ID
	Поле – корпоративное	App-ID
	Контроль выгрузки	Блокировка файлов
	Контроль загрузки	Блокировка файлов
	Обнаружение вредоносных программ	WildFire и профиль защиты
	Контроль пользователей	User-ID

Примеры детального контроля, обеспечиваемые App-ID

Тем не менее, финансовый отдел может осуществлять обмен не конфиденциальными данными в пределах всей компании, или, в некоторых случаях, с внешними продавцами. При этом важным является возможность инспектирования такового обмена данными в контексте всех указанных факторов.
Самой основной необходимости в отношении безопасности приложений SaaS является обеспечение соблюдения стандартов PCI и II в рамках организации. Сервис Aperture учитывает это посредством предопределенных политик.

Влияния без участия пользователя или влияние на сеть
Сервис Aperture представляет собой полностью облачное решение, не имеющее необходимости в каких-либо прокси-серверах или агентах для его работы. Так как Aperture осуществляет коммуникацию напрямую с самими приложениями SaaS, оно выполняет проверку любых данных из любого источника, в независимости от устройства или места, откуда они поступили. Так как Aperture не является линейным сервисом, она не оказывает влияние на задержку передачи данных или полосу пропускания приложений, а также не влияет на взаимодействие конечных пользователей. Встроенные приложения на мобильных устройствах также не подвержены ее воздействию. Таким образом, ваши пользователи не ограничены использованием только доступа через интернет. При отсутствии необходимых изменений в информационной сети или установленных прокси-серверов, Aperture не оказывает влияния на конфигурации сети. Также Aperture не требует установки какого-либо нового программного или аппаратного обеспечения для ее использования. Она просто выполняет свою работу.

За пределами санкционированных приложений SaaS
Aperture добавляет другое измерение уровня безопасности к платформе безопасности нового поколения Пало Альто Нетворкс, обеспечивая глубокое понимание уровня незащищенности данных и угроз в рамках приложений SaaS. При включении Aperture в расширенное решение межсетевой защиты нового поколения, возможности обеспечения безопасности значительно увеличиваются, реализуясь во всеобъемлющем решении для SaaS с реальной картиной визуализации по всем приложениям. Это касается как санкционированных, так и несанкционированных приложений SaaS, наряду с детальным контролем использования данных приложений (см. Рисунок 2).

Полная визуализация во всех приложениях
Технология межсетевой защиты нового поколения Palo Alto Networks была изначально разработана для обеспечения исключительной визуализации и контроля всех приложений, включая подробную информацию об использовании приложений в рамках всей информационной сети. SaaS является одной из многих категорий приложений, которая сегодня поддерживается посредством мощной библиотеки примеров App-ID, обеспечивающей немедленную классификацию и сверхдетальный контроль.

Детальный контроль всех приложений
Межсетевая защита нового поколения Пало Альто Нетворкс обеспечивает лидирующий в данной индустрии детальный контроль входов и выходов приложений SaaS. Это предоставляет возможность организациям контролировать доступ к приложениям SaaS на детальном уровне, определяя не только какие приложения являются санкционированными, но также и приемлемое поведение в рамках приложений. Сразу же после надлежащей классификации приложений SaaS, политики безопасности устанавливают контроль доступа и пользования в рамках информационной сети, устройства и уровней пользователя. Это не только обеспечивает возможность блокирования доступа несанкционированных приложений, но также обеспечивает детальный контроль допустимых приложений; что, в свою очередь, позволяет контролировать то как они используются с целью обеспечения безопасности бизнеса.

PALO ALTO NETWORKS
Система безопасности облаков APERTURE

Непрерывная безопасность всех пользователей
С помощью защиты информационной сети для конечных точек Пало Альто Нетворкс ГлобалПротект™, пользователи непрерывно подключаются к сети, исключая большое количество пользователей, выходящих за пределы информационной сети организации. Global Protect работает посредством подключения устройства пользователя к наиближайшей межсетевой защите нового поколения, таким образом, обеспечивая полную безопасность сети, не зависимо от физического местоположения пользователя. При наличии VM-series, используемой на публичных облачных сервисах, таких как Amazon® AWS®, самая ближайшая межсетевая защита нового поколения может находится очень близко к пользователю.

Повсеместное предотвращение угроз
WildFire разработана для идентификации известных и неизвестных вредоносных программ, размещаемых в рамках информационной сети, а затем обменивающихся этими данными с остальной платформой безопасности нового поколения. Aperture обеспечивает дополнительную визуализацию таких вредоносных программ напрямую в рамках приложений SaaS.

Полная безопасность данных независимо от их местоположения
Aperture является частью большого облачного решения, которое наряду с платформой безопасности нового поколения, обеспечивает защиту данных в независимости от их местоположения. Будь то локальное размещение данных; их виртуализация и необходимость в защите в частном облаке (NSX®, ACI™, Hyper-V®, KVM / OpenStack®); их расширение до публичного облака (AWS, Azure®, vCloud® Air™); или перемещение в приложение SaaS, Пало Альто поможет обеспечить их защиту.

Palo Alto Networks ®

4401 Грейт Америка Парквей
Санта Клара, Калифорния 95054

Общий отдел: +1.408.753.4000
Продажи: +1.866.320.4788
Поддержка: +1.866.898.9087

www.paloaltonetworks.com

Контакты офиса в Москве: russia@paloaltonetworks.com
Адрес: Москва, Пресненская набережная, дом 10, блок С, офис 424