FORCEPOINT
POWERED BY Raytheon

Спецификация

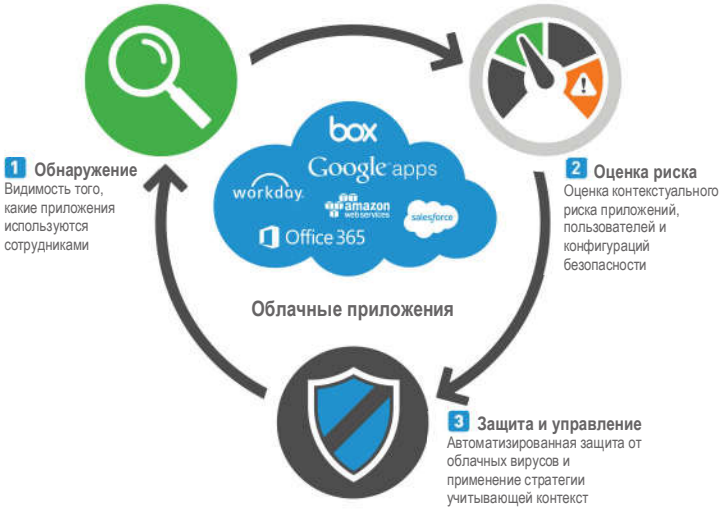
Брокер безопасности контроля доступа к облаку компании Forcepoint (Cloud Access Security Broker, CASB) автоматически ищет используемые облачные приложения, анализирует риски и обеспечивает выполнение подходящих элементов управления для программного обеспечения как услуги и прикладного программного обеспечения. Используя брокер Forcepoint CASB, пользователи работают с нужными им приложениями, а сотрудники ИТ-отдела получают необходимый им контроль за использованием приложений.

ПРЕДОСТАВЛЕНИЕ ВИДИМОСТИ И КОНТРОЛЯ ЗА ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

Облачные приложения позволяют организациям сокращать затраты и гибко распределять ресурсы, но также создают риски для безопасности и соответствия нормативным требованиям. Ускорение внедрения использования облачных приложений на рабочем месте наряду с распространением политики «принеси свое собственное устройство» (BYOD), создало потребность в обеспечении безопасности для использования расположенных в облаке одобренных приложений, таких как Office 365, Dropbox и Salesforce. Предотвращение утечек данных и обеспечение использования детальных элементов управления доступом оправданно являются приоритетным для ИТ-отдела.

Сотрудники могут быть одним из основных источников рисков для безопасности, так как злонамеренные штатные работники стремятся использовать неограниченный доступ к облачным приложениям организации для скрытого выведения данных.

Компания Forcepoint обеспечивает безопасное и продуктивное использование облачных приложений для всех пользователей и конечных устройств.



Для обеспечения видимости и контроля необходим брокер безопасности доступа к облаку, который поддерживает обнаружение приложений, управление рисками, контроль доступа и защиту данных как от санкционированных, так и несанкционированных приложений.

СНИЖЕНИЕ РИСКОВ ОБЛАЧНОГО ПРИЛОЖЕНИЯ

Как правило, организациям требуется видимость структуры доступа к облаку перед внедрением политик устранения или ограничения рисков. Вот почему важно иметь набор автономных функций, которые помогут определить и оценить уровень риска. После того, как набор угроз изучен и создана необходимая политика для устранения угроз безопасности, можно превратить такие автономные функции в облачные внутренние решения для реального применения таких политик. Компания Gartner рекомендует решения, которые предлагают «лучшее из обоих миров» (то есть сочетание прокси и API), что позволяет охватить все случаи использования облачной безопасности современными организациями.

Сотрудники корпорации, мобильные пользователи и хакеры

Поддерживаются облачные встроенные и автономные внедрения

Облачные приложения

Брокер безопасности контроля доступа к облаку компании Forcepoint обеспечивает видимость и управление санкционированными и несанкционированными облачными приложениями.

СВОЙСТВА И ПРЕИМУЩЕСТВА

- Часть семейства программных продуктов облачной безопасности компании Forcepoint для локальной и облачной сред.
- Всеобъемлющее решение, объединяющее в себе поиск приложений, контроль, аналитику и защиту.
- Параметры внедрения для автономного (режим API) и / или облачного встроенного (режима прокси) режимов работы.
- Детальная политика для мобильных и конечных устройств позволяет управлять доступом и защитой данных для управляемых и неуправляемых мобильных телефонов, планшетов и ноутбуков.
- Встроенный интегрированный доступ к корпоративным директориям, системе управления информацией о безопасности и событиями безопасности, а также системе управления мобильными устройствами.
- Полная поддержка систем Office 365, AWS, Salesforce, Google Apps, Box, Dropbox, NetSuite, Workday, Microsoft Azure и других.
- Сертифицированная функциональная совместимость с партнерами, обеспечивающими идентификационную безопасность как услугу: Centrify, Ping, Okta, OneLogin, SecureAuth и Microsoft.
- Расширяет на облачные вычисления возможности организации по выявлению аномального поведения и угроз.
- Репутационные данные IP адреса позволяют создавать и применять более точную стратегию снижения рисков.

ОБНАРУЖЕНИЕ И УПРАВЛЕНИЕ В ОБЛАКЕ

Брокер Forcepoint CASB расширяет традиционные данные об обнаруженных облачных приложениях, предоставляя сведения о факторах риска, которые являются уникальными и специфичными для организации. Например, брокер Forcepoint CASB обеспечивает видимость спящих (то есть неактивных) учетных записей, потерянных учетных записей (например, бывших сотрудников) и внешних учетных записей (например, контрагентов), которые представляют различные риски безопасности.

Кроме того, компания Forcepoint сравнивает конфигурации безопасности облачных приложений организации с лучшими в отрасли методами и нормативными требованиями, что позволяет более точно определить бреши в безопасности и соблюдении нормативов и предпринять действия для их исправления.

Все функции облачного обнаружения и управления доступны через интерфейсы API поставщика облачных приложений, процессы являются автономными, неинтрузивными, не требующими наблюдения. Изменения в приложениях или журналах отправляются в компанию Forcepoint.

ОБЛАЧНЫЙ АУДИТ И ЗАЩИТА

Средства облачного аудита и защиты брокера Forcepoint CASB предоставляют оперативную информацию и инструменты, необходимые для защиты данных в облаке и обеспечивают всеобъемлющий контроль доступа пользователей. Компания Forcepoint предоставляет важные аналитические обзоры в следующих областях:

- **Предотвращение утечки данных для хранящихся данных и передающихся данных:** средства контроля конфиденциальными и регулируемыми данными в облаке,
- **Мониторинг пользователей:** мониторинг активности в реальном времени и отчетность конечных пользователей и администраторов,
- **Предотвращение кибер-угроз**: принудительное применение стратегии предупреждения, блокировки или требующих проверки контроля подлинности для любых подозрительных действий.

Брокер Forcepoint CASB производит мониторинг и контролирует выгрузку, загрузку и совместное использование конфиденциальных данных на основе различных критериев, таких как назначение данных, пользовательское или облачное приложение. Кроме того, он сканирует корпоративные данные, хранящиеся в службах синхронизации файлов, таких как OneDrive и Box, выделяя те файлы, которые содержат конфиденциальные или регулируемые данные, чтобы можно было применить соответствующую стратегию (например, отправить оповещение) для снижения риска.

Брокер Forcepoint CASB проверяет файлы и их содержимое в режиме реального времени, чтобы обеспечить защиту личных данных, документов индустрии платежных карт, закон по обеспечению доступности и подотчётности в медицинском страховании HIPAA и другой конфиденциальной информации. Администраторы могут выбрать карантин файлов, удалить конфиденциальные файлы из облачного хранилища и уведомить конечных пользователей. Копия файла также может быть добавлена в доверенную папку для дальнейшего просмотра. Брокер Forcepoint CASB предлагает встроенную защиту от утечки данных (DLP) или стандартную ICAP-интеграцию с ведущими DLP-решениями, что позволяет использовать имеющуюся стратегию защиты данных.

Брокер CASB компании Forcepoint автоматически обнаруживает и блокирует угрозы для облачных приложений и проводит политику снижения рисков. Благодаря уникальным методам дактилоскопии, брокер Forcepoint CASB быстро устанавливает подробные профили поведения, основанные на обычных шаблонах использования для каждого пользователя, отдела и устройства. Любой доступ, который не прошел тест на отпечатки пальцев, может быть настроен на немедленное оповещение, блокировку или иметь двухступенчатую аутентификацию в режиме реального времени. Можно также быстро создавать настраиваемую стратегию и применять ее в выбранных облачных приложениях.

Брокер Forcepoint CASB позволяет блокировать или ограничивать доступ к облачным приложениям из неуправляемых конечных устройств (например, для устройств BYOD или персональных устройств), что является экономичной альтернативой маршрутизации всего удаленного доступа через VPN. Кроме того, брокер Forcepoint CASB имеет встроенные адаптеры, которые упрощают интеграцию с корпоративными каталогами и ведущими на рынке решениями системы управления информацией о безопасности и событиями безопасности (SIEM).

БРОКЕР FORCEPOINT CASB — СРАВНЕНИЕ СВОЙСТВ ПРОДУКТА

ПРОДУКТЫ КОМПАНИИ FORCEPOINT

ГРУППА СВОЙСТВ	ОПИСАНИЕ СВОЙСТВ	УПРАВЛЕНИЕ ОБЛАКОМ	ОБЛАЧНЫЙ АУДИТ И ЗАЩИТА	КОМПЛЕКС ОБЛАЧНОЙ БЕЗОПАСНОСТИ
Видимость приложений и оценка рисков (доступно для автономного и API внедрений)	ПОИСК ОБЛАЧНЫХ ПРИЛОЖЕНИЙ — использование существующих журнальных файлов для автоматизации обнаружения и категоризации облачных приложений.	●		●
	ОЦЕНКА РИСКОВ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ — оценивание общего риска для каждого приложения в облаке на основе нормативных и отраслевых сертификатов и методических рекомендаций.	●		●
	СВОДКА ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ — включает количество пользователей, действия, объем трафика и обычную длительность промежутка времени использования для каждого облачного приложения.	●		●
	УСОВЕРШЕНСТВОВАННЫЕ РИСКОВЫЕ МЕТРИКИ — подробные сведения об уровне рисков для облачных приложений и информация по каждому приложению.	●		●
	НАСТРАИВАЕМЫЕ РИСКОВЫЕ МЕТРИКИ — Подробные показатели рисков облачных приложений с настраиваемыми весовыми коэффициентами.	●		●
	НЕПРЕРЫВНЫЙ ПОИСК — Создание расписания автоматизированного сканирования журнальных файлов и периодическое формирование поисковых отчетов.	●		●
	ОБЩАЯ ПОИСКОВАЯ ПАНЕЛЬ — Результаты агрегированного поиска, текущее использование в сравнении с предыдущим и тренды использования.	●		●
	ИНТЕГРАЦИЯ С СИСТЕМОЙ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ О БЕЗОПАСНОСТИ И СОБЫТИЯМИ БЕЗОПАСНОСТИ (SIEM) — Формирование поисковых данных в общем формате событий для интеграции с существующими системами SIEM.	●		●
	КАТАЛОГИ ПРИЛОЖЕНИЙ И ОБНОВЛЕНИЕ РИСКОВ — Автоматическое обновление каталога приложений облака и изменение свойств рисков по мере доступности такой информации.	●		●
	НАБОРЫ ЖУРНАЛОВ ДЕЯТЕЛЬНОСТИ — Сбор основных журналов деятельности пользователей и привилегированных пользователей посредством API облачных приложений.	●		●
УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ И ДАННЫМИ (доступно для автономного и API внедрения)	КЛАССИФИКАЦИЯ ДАННЫХ — Каталогизация и определение конфиденциальных или регулируемых данных, включая привилегии доступа для каждого файла, хранящегося в службах синхронизации файлов, для обеспечения соответствия нормам, таким как PCI, SOX и HIPAA.	●		●
	УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ — Определение спящих (то есть неактивных) учетных записей, потерянных учетных записей (например, бывших сотрудников) и внешних пользователей (например, контрагентов), чтобы сократить операционные расходы и минимизировать соответствующие угрозы безопасности.	●		●
	УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ — Проведение сравнительного анализа конфигураций безопасности для облачных приложений с набором методических рекомендаций и индустриальных нормативных требований (например, PCI DSS, NIST, HIPAA, CJIS, MAS, ISO) с целью выявления брешей в безопасности и соответствия требованиям.	●		●
	ИНТЕГРИРОВАННЫЙ РАБОЧИЙ ПРОЦЕСС ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ — Использование встроенного организационного рабочего процесса для назначения и выполнения задач по снижению рисков с помощью брокера Forcepoint CASB или интегрирования со сторонними системами отслеживания ошибок.	●		●
Мониторинг деятельности в реальном времени и аналитика (доступно для встроенных и прокси внедрений)	МОНИТОРИНГ ДЕЯТЕЛЬНОСТИ И АНАЛИТИКА — Мониторинг деятельности и аналитика в реальном времени для пользователя, группы, местоположения, устройства, действия приложения и т.д.		●	●
	МОНИТОРИНГ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ — Мониторинг деятельности и отчетность привилегированных пользователей и администраторов в реальном времени.		●	●
	ИНТЕГРИРОВАНИЕ С КОРПОРАТИВНОЙ СИСТЕМОЙ SIEM — Адаптеры для прямого чтения журналов деятельности ведущими решениями SIEM, включая ArcSight, Splunk и Q1 Labs.		●	●
	ИНТЕГРИРОВАНИЕ С КОРПОРАТИВНЫМИ ДИРЕКТОРИЯМИ — Использование существующей инфраструктуры каталогов AD или LDAP для пользовательских, групповых и организационных отчетов и политик.		●	●
	ОСНОВАННОЕ НА РОЛЯХ АДМИНИСТРИРОВАНИЕ — Определение прав администратора для редактирования активов, политик и системных настроек.		●	●
	КОРПОРАТИВНАЯ ОТЧЕТНОСТЬ — Гибкие варианты отчетности, в том числе предопределенные отчеты с возможностью редактирования и сохранения настроенных отчетов.		●	●

ПРОДУКТЫ КОМПАНИИ FORCEPOINT

ГРУППА СВОЙСТВ	ОПИСАНИЕ СВОЙСТВ	УПРАВЛЕНИЕ ОБЛАКОМ	ОБЛАЧНЫЙ АУДИТ И ЗАЩИТА	КОМПЛЕКС ОБЛАЧНОЙ БЕЗОПАСНОСТИ
УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ И ДАННЫМИ (доступно для автономного и API внедрений)	АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ АНОМАЛИЙ — Непрерывное отслеживание поведения и обнаружение аномальных действий, включая высокорисковые внутренние и внешние атаки.		●	●
	ПРЕДОТВРАЩЕНИЕ УГРОЗ В РЕАЛЬНОМ ВРЕМЕНИ — Корреляция аномалий деятельности с рискованными IP-адресами. Применение стратегии для предупреждения, блокировки, карантина или проверки подлинности для любого приложения или конкретного действия в приложении.		●	●
	ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ — Классификация хранящихся данных и проверка контента в реальном времени для более чем 100 типов файлов и сотен предопределенных типов данных, соответствующих требованиям ряда нормативных документов (например, PCI, PII, PHI, HIPAA, SOX).		●	●
	МУЛЬТИФАКТОРНАЯ АУТЕНТИФИКАЦИЯ — Проверка идентичности на основе рисков (например, одноразовый пароль, отправленный на мобильное устройство пользователя при обнаружении аномальных или высокорисковых действий.		●	●
	ЕДИНАЯ ТОЧКА ВХОДА — Использование встроенного решения SSO или стороннего решения для доступа к приложениям на основе SAML.		●	●
	ДИНАМИЧЕСКИЕ ПРЕДУПРЕЖДЕНИЯ — Получение оповещений в реальном времени о нарушении правил или пороговых значений деятельности с помощью SMS или электронной почты.		●	●
	УПРАВЛЕНИЕ ДОСТУПОМ К МОБИЛЬНЫМ УСТРОЙСТВАМ И КОНЕЧНЫМ УСТРОЙСТВАМ — Включение уникальной стратегии для управляемых и неуправляемых устройств, будь то из браузеров или мобильных приложений.		●	●
	УПРАВЛЕНИЕ ДОСТУПОМ НА ОСНОВЕ МЕСТОПОЛОЖЕНИЯ — Ограничение доступа на основе местоположения пользователя или местоположения облачной службы.		●	●
	ИНТЕГРИРОВАНИЕ С СИСТЕМОЙ УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ (MDM) — Использование существующих внедрений MDM для управления регистрацией конечных устройств и доступом к облачным системам.		●	●
	НАСТРАИВАЕМЫЕ ПОЛИТИКИ — Визуальный редактор политик разрешает простое конфигурирование настраиваемых политик на основе различных атрибутов.		●	●
Передовая облачная архитектура	ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ — Ускорение доступа к облачным приложениям благодаря функциям кэширования и оптимизации контента в сети доставки контента мирового класса с более чем 30-ю центрами обработки данных по всему миру.		●	●
	ОБЩАЯ АНАЛИТИКА УГРОЗ — Унифицированный просмотр аномалий и угроз для таблиц базы данных корпорации, файлов, хранящихся в общих папках и данных, хранящихся в облачных приложениях.		●	●

[1] Дополнительный продукт для базовой лицензии брокера Forcepoint CASB, приобретается отдельно.

КОНТАКТНАЯ ИНФОРМАЦИЯ

www.forcepoint.com/contact

О КОМПАНИИ FORCEPOINT

[DATASHEET_FORCEPOINT_CASB_EN]-100055.022217.