Forcepoint Web Security

ЛОКАЛЬНАЯ И ОБЛАЧНАЯ ВЕБ-БЕЗОПАСНОСТЬ ОТ КОМПАНИИ FORCEPOINT

FORCEPOINT
POWERED BY Raytheon

Forcepoint Web Security

ЛОКАЛЬНАЯ И ОБЛАЧНАЯ ВЕБ-БЕЗОПАСНОСТЬ ОТ КОМПАНИИ FORCEPOINT

Вашу компанию и ее данные постоянно атакуют. Традиционные решения безопасности больше не обеспечивают достаточной защиты. Фактически, они могут подвергнуть компанию риску потери данных и судебных разбирательств. Защита сети и данных от продвинутых угроз, вымогателей-шифровальщиков и пакетов эксплоитов имеет решающее значение для выживания компании в условиях все более рискованного мобильного и облачного цифрового мира.

Возможность настройки и расширения

Компании нуждаются в настраиваемых решениях, которые взаимодействуют друг с другом для защиты от таких типов угроз по мере их возникновения. ПО Forcepoint Web Security предлагает защиту в режиме реального времени от продвинутых угроз и краж данных посредством нескольких вариантов внедрения и вспомогательных модулей для настройки пакета веб-защиты в соответствии с потребностями компании.

ПО Forcepoint Web Security обеспечивает надежную защиту на основе контента, а также поиска и мониторинга облачных приложений. Это снижает риски связанные с конфиденциальными данными локальных и мобильных пользователей.

Самое главное, что ПО Forcepoint Web Security легко интегрируется с другими решениями компании Forcepoint, обеспечивая единообразные средства контроля безопасности, которые могут защитить от входящих и исходящих угроз даже при малом числе сотрудников отдела безопасности.

Цели веб-безопасности

Большинство современных решений безопасности не могут справиться с продвинутыми угрозами по мере их возникновения. ПО Forcepoint Web Security является передовым средством защиты от угроз в реальном времени.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КАЖДОГО ПОЛЬЗОВАТЕЛЯ, ГДЕ БЫ ОН НЕ НАХОДИЛСЯ, ОТ ПРОДВИНУТЫХ УГРОЗ

Незаметное для пользователя распространение защиты как на локальные рабочие места, так и на удаленные рабочие места, где бы они ни находились в сети.

ОПРЕДЕЛЕНИЕ И УПРАВЛЕНИЕ РИСКАМИ ОТ ПРИЛОЖЕНИЙ ТЕНЕВОГО ИТ И ОБЛАЧНЫХ СЛУЖБ

Поиск облачных приложений, используемых в компании. Мониторинг использования этих приложений для определения и блокирования тех из них, которые представляют наибольший риск.

УМЕНЬШЕНИЕ ЗАТРАТ НА БЕЗОПАСНОСТЬ ПРИ ОДНОВРЕМЕННОМ УЛУЧШЕНИИ ПРОИЗВОДИТЕЛЬНОСТИ ТРУДА

Консолидация не связанных продуктов безопасности на единой платформе с единообразными средствами контроля безопасности веб-приложений, данных и облачных приложений. Легкое расширение безопасности путем дополнительного использования облачных «песочниц», DLP, аналитических данных по угрозам и мобильной безопасности.

«Компания Forcepoint разрешает думать по-иному, архитектурно, и использовать больше облачных приложений для улучшения результатов деловой активности».

—Крис Андерсон (Chris Anderson), руководитель отдела инфраструктурных служб банка «Бендиго и Аделаида» (Bendigo and Adelaide Bank)

ПО Forcepoint Web Security

АНАЛИЗ В РЕАЛЬНОМ ВРЕМЕНИ ДЛЯ РАСШИРЕННОЙ ЗАЩИТЫ ОТ УГРОЗ

ПО Forcepoint Web Security превосходит антивирусную защиту посредством восьми областей оценки защиты. При этом используется сложный алгоритм оценивания, основанный на прогностическом анализе системы Forcepoint ACE. Несколько систем анализа контента в режиме реального времени анализируют весь контент веб-страниц, активные скрипты, веб-ссылки, контекстные профили, файлы и исполняемые модули.

ПРОСТАЯ ПАНЕЛЬ ДОСТУПА К КРИМИНАЛИСТИЧЕСКИМ ДАННЫМ

Панель расширенной защиты от угроз ПО Forcepoint Web Security обеспечивает доступ к криминалистической отчетности о том, кто был атакован, какими данными интересовались, конечном устройстве, для которого предназначались данные, и способе выполнения атаки. Инциденты в системе безопасности включают перехват краж данных, по возможности. Защита анализирует входящие и исходящие сообщения.

ИНТЕГРИРОВАННАЯ ЗАЩИТА ОТ КРАЖ ДАННЫХ

Лучшее в отрасли ИТ решение для защиты от краж данных (дополнительное) обнаруживает и перехватывает попытки краж данных и обеспечивает соблюдение нормативных требований для предотвращения утечки данных (DLP). Примеры таких возможностей включают обнаружение зашифрованных пользователем загрузок данных, кражу данных из файлов паролей, медленные утечки данных (Drip-DLP), оптическое распознавание символов (OCR) текста в изображениях и понимание геолокационной цели.

ИНТЕГРИРОВАННАЯ ПЕСОЧНИЦА

Позволяет узнать, как лучше защитить активы компании за счет автоматического анализа поведения вредоносных программ с помощью интегрированной службы песочницы.

ПОИСК ОБЛАЧНЫХ ПРИЛОЖЕНИЙ, МОНИТОРИНГ И КОНТРОЛЬ

Поиск облачных приложений, которые используются в организации, и защита пользователей от рисков, связанных с отправкой данных несанкционированным облачным приложениям и службам.

Модули расширенной защиты

ВНЕДРЕНИЕ В ГИБРИДНОМ ОБЛАКЕ	**Распространение веб-защиты и применение политик для удаленных пользователей.** Внедрение ПО Forcepoint Web Security в качестве физического или виртуального устройства для частного облака. Любое выбранное решение может быть расширено посредством глобальной облачной инфраструктуры компании Forcepoint для защиты удаленных пользователей.
DLP ДЛЯ ИНТЕРНЕТ	**Дополнительное использование мощного, контекстно-зависимой системы DLP для защиты исходящих данных от кражи.** Модуль Forcepoint Web DLP обеспечивает защиту от кражи данных и гарантирует соблюдение более 1700 заранее определенных политик и шаблонов. Модуль также включает лучшую в отрасли защиту, такую как защита Drip-DLP от медленных утечек данных, оптическое распознавание символов (OCR) от кражи данных из файлов изображений или обнаружение пользовательского шифрования для установления зашифрованных с умыслом файлов.
ОБЛАЧНАЯ ПЕСОЧНИЦА	**Интеграция поведенческой песочницы для автоматического и ручного анализа файлов вредоносных программ.** Анализ подозрительных файлов в виртуальной среде, значительно более глубокий в сравнении с простым выполнением файлов для обеспечения наивысшего уровня защиты от продвинутых вредоносных программ. При обнаружении вредоносных файлов автоматически формируется детальная криминалистическая отчетность.
МОБИЛЬНАЯ БЕЗОПАСНОСТЬ	**Расширение стратегии и защиты для пользователей ОС iOS и Android.** Распространение существующих стратегий безопасности на мобильные устройства для защиты их от продвинутых угроз, мобильных вредоносных программ, фишинговых атак, имитация соединений и т.д. Модуль Forcepoint Mobile Security может взаимодействовать с менеджером мобильных устройств (MDM) для обеспечения полной защиты мобильных устройств.

Дополнительные возможности

ЗАЩИТА УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ

Управление корпоративными, отраслевыми и удаленными пользователями с помощью одной консоли и политики посредством гибридного облачного внедрения.

ГИБКАЯ ПРОВЕРКА SSL

Детализованные возможности проверки протокола SSL позволяют отслеживать трафик протокола HTTPS при соблюдении конфиденциальности и нормативных требований.

ИНТЕРФЕЙС API АНАЛИТИКИ ПО УГРОЗАМ

Использование интерфейса получения данных Published API повышает интеллектуальность веб-безопасности компании за счет включения отраслевой или региональной аналитики по угрозам и автоматизации управления безопасностью.

УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ И ПРОТОКОЛАМИ

Сетевой агент администрирования обеспечивает детальный контроль над сотнями протоколов и приложений для повышения безопасности.

ГИБКАЯ ОТЧЕТНОСТЬ

Четыре настраиваемые панели мониторинга, а также более 60 предопределенных и настраиваемых отчетов предоставляют легко читаемую деловую и техническую информацию, а также ценную информацию об уровнях угрозы и многое другое.

НЕСКОЛЬКО ВОЗМОЖНОСТЕЙ ВНЕДРЕНИЯ

Выбор варианта внедрения на основе гибридного облака или локального устройства (виртуального или физического).

ЗАЩИТА КОНЕЧНЫХ УСТРОЙСТВ БЕЗ ПРОКСИ

Наше решение защищает пользователей, работающих в любом месте и любой сети. Приложения продолжают работать в средах, которые обычно вызывают проблемы с облачными решениями на основе прокси.

РАНЖИРОВАНИЕ ИНЦИДЕНТОВ ПО РИСКАМ В ИНТЕГРИРОВАННОЙ DLP

Лидирующая в отрасли функциональность аналитики безопасности снижает затраты и повышает эффективность исследований DLP.

Возможности решений компании Forcepoint

СИСТЕМА КЛАССИФИКАЦИИ ACE (ADVANCED CLASSIFICATION ENGINE)

Система ACE компании Forcepoint обеспечивает облачную встроенную контекстуальную защиту в реальном времени для Интернета, электронной почты, данных и мобильных устройств, используя комбинированную систему оценки рисков и аналитику для обеспечения максимально эффективной защиты. Система также предоставляет сдерживание угроз путем анализа входящего и исходящего трафика, обеспечивая лидирующую в отрасли степень защиты данных от краж. Классификаторы для обеспечения безопасности в реальном времени, анализа данных и контента, которые были получены после многолетних исследований и разработок, позволяют системе ACE обнаруживать больше угроз, чем традиционные антивирусные системы (доказательство обновляется ежедневно по ссылке http://securitylabs.forcepoint.com). Система ACE является основной защитой всех решений компании Forcepoint, и поддерживается системой Forcepoint ThreatSeeker Intelligence.

ИНТЕГРИРОВАННЫЙ НАБОР ОЦЕНКИ ВОЗМОЖНОСТЕЙ ЗАЩИТЫ В ВОСЬМИ КЛЮЧЕВЫХ ОБЛАСТЯХ

- Доступны 10 000 аналитических функций для выполнения глубокого анализа,
- Предиктивная система безопасности предвидит несколько будущих событий,
- Встроенные средства защиты не только отслеживают, но **блокируют** угрозы.

Forcepoint ThreatSeeker Intelligence

ПО Forcepoint ThreatSeeker Intelligence, разработанное лабораторией Security Labs компании Forcepoint, предоставляет базовые общие аналитические возможности для всех продуктов безопасности компании Forcepoint. Оно объединяет более 900 миллионов конечных устройств, включая входные данные от Facebook, а с помощью системы ACE компании Forcepoint анализирует до 5 миллиардов запросов в день. Такая широкая осведомленность об угрозах безопасности позволяет Forcepoint ThreatSeeker Intelligence предлагать обновления безопасности в реальном времени, которые блокируют изощренные угрозы, вредоносные программы, фишинг-атаки, приманки и мошенничества. Кроме того, ПО также предоставляет последние веб-рейтинги. Forcepoint Intelligence ThreatSeeker не имеет себе равных по размеру и использованию системы ACE в режиме реального времени для анализа общих входных данных. (При обновлении до уровня Web Security, ПО Forcepoint ThreatSeeker Intelligence помогает снизить подверженность веб-угрозам и краже данных).

Архитектура TRITON

Обладая лучшей в своем классе безопасностью и унифицированной архитектурой, архитектура TRITON предлагает мгновенную защиту на основе встроенной защиты в реальном времени, обеспечиваемой системой Forcepoint ACE. Непревзойденная защита, обеспечиваемая в реальном времени системой ACE, поддерживается ПО Forcepoint ThreatSeeker Intelligence и опытом исследователей лаборатории Security Labs компании Forcepoint. В результате получена единая архитектура с одним унифицированным интерфейсом пользователя и единой системой сбора информации для обеспечения защиты.

КОНТАКТНАЯ ИНФОРМАЦИЯ
www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_WEB_SECURITY
_EN] 400002.021317

FORCEPOINT
POWERED BY Raytheon