Система защиты от утечек данных (DLP) и решение для конечных устройств DLP Endpoint компании Forcepoint

УЛУЧШЕНИЕ ОСВЕДОМЛЕННОСТИ И КОНТРОЛЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

FORCEPOINT
POWERED BY Raytheon

Система защиты от утечек данных (DLP) и решение для конечных устройств DLP Endpoint компании Forcepoint

НЕПРЕВЗОЙДЕННАЯ ОСВЕДОМЛЕННОСТЬ И КОНТРОЛЬ НАД ВАЖНЫМИ ДАННЫМИ В ЛЮБОЕ ВРЕМЯ И В ЛЮБОМ МЕСТЕ — В ОФИСЕ, В ПУТИ ИЛИ В ОБЛАКЕ

Важные данные подвержены изменениям. Данные хранятся и доступны через облачные службы, такие как Office 365 и Box, что способствует совместной работе над ними. Forcepoint DLP — это лидирующее в отрасли решение DLP, которое обеспечивает осведомленность и контроль над данными для защиты данных вне зависимости от того, хранятся ли они или с ними выполняется работа через мобильные устройства, такие как ноутбуки Windows или Apple, или же данные распространяются через электронную почту и систему мгновенного обмена сообщениями (IM).

Защитите свои конфиденциальные данные, где бы они не находились — в облаке или локально посредством системы Forcepoint DLP.

Система DLP компании Forcepoint расширяет возможности корпорации.

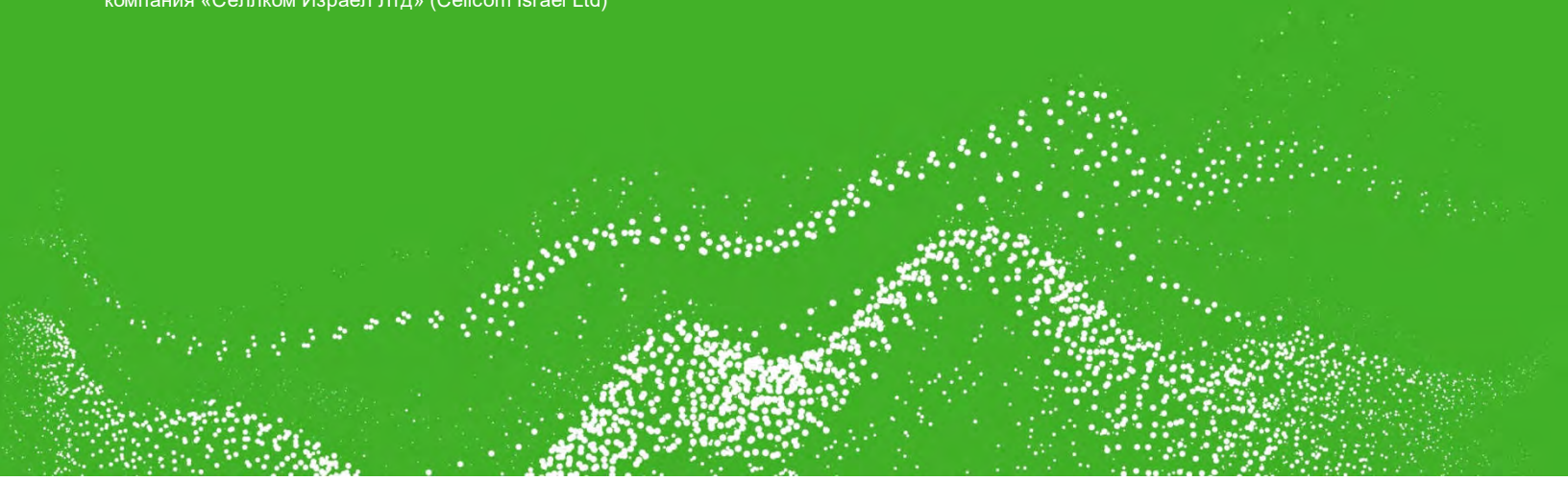
- Быстро приводит в соответствие глобальные и отраслевые нормативные требования с заранее определенными политиками, которые поддерживаются и обновляются специализированной исследовательской группой компании Forcepoint.
- Использует инструменты классификации данных для определения и защиты вашей интеллектуальной собственности, независимо от того, где она хранится.
- Поведенческие стратегии сочетают осведомленность о контенте и контексте для автоматического определения поведения пользователей с высоким риском, такого как пересылка электронной почты на персональные учетные записи или упаковывание данных с использованием шифрования с целью выведения данных с целью кражи.
- Простой поиск и защита файлов, которые хранятся на конечных устройствах Mac, Windows и Linux.
- Определение и предотвращение потери данных в облачных службах, таких как Office 365 и Box.
- Реализация эффективных элементов контроля доступа на основе ролей и всестороннего аудита для удовлетворения внутренних и внешних требований соответствия.
- Простое интегрирование со сторонними решениями по безопасности данных от компаний Microsoft, HP, Splunk, IBM, Titus, Boldon James и Citrix.
- Аналитика системы DLP, использующая моделирование данных и статистический анализ для автоматического определения поведения пользователя, представляющего наибольший риск потери или кражи данных, позволяет отделу обеспечения безопасности использовать опыт исследований компании Forcepoint.
- Архитектура TRITON компании Forcepoint позволяет унифицировать решения безопасности, координировать защитные стратегии, делиться информацией по нескольким направлениям и пользоваться централизованным управлением безопасности данных.

Основные возможности.

- **Ранжирование риска инцидентов** использует расширенную аналитику данных, чтобы предоставить отделу безопасности отчет о групповом ранжировании наиболее важных рисков для безопасности данных вашей компании.
- **Интегрированная система OCR** определяет конфиденциальные данные и IP-маркеры в изображениях, таких как чертежи САПР, сканированные документы, машинно-считываемая информация и копии экрана,
- **Система предотвращения медленных утечек данных (Drip DLP)** учитывает совокупную активность по передаче данных со временем для обнаружения небольшой утечки данных,
- **Основанные на поведении политики** объединяют осведомленность о контенте и контексте для автоматического определения момента, когда пользователи подвергают риску конфиденциальные данные.
- **Уникальная система работы с отпечатками пальцев PreciseID Fingerprinting** может обнаруживать частичный отпечаток пальца в структурированных (записи базы данных) или неструктурированных данных (документы) на конечных устройствах Mac и Windows вне зависимости от того, работает ли сотрудник в офисе или вне сети.
- **Автоматическое шифрование данных** применяется к съемным устройствам хранения для обеспечения безопасного обмена данными с партнерами.
- **Рабочий процесс обработки инцидентов через электронную почту** облегчает распространение инцидента для проверки и исправления владельцами данных и деловыми партнерами, не предоставляя им доступ к системе управления DLP.
- **Обнаружение и предотвращение** отправки закрытых данных из организации через электронную почту, выгрузку через Интернет, систему мгновенных сообщений и клиенты облачных служб, при этом дешифрование Native SSL выполняется как для сетевого трафика, так и на конечном устройстве.
- **Внедрение компонент системы DLP** в Microsoft с целью применения стратегий DLP в пакете Microsoft Office 365.

«Решение Forcepoint DLP было самым мощным из найденных нами для остановки и предотвращения утечек данных».

— Амир Шахар (Amir Shahar), менеджер по информационной безопасности, компания «Селлком Израел Лтд» (Cellcom Israel Ltd)



Функциональность системы Forcepoint DLP

СМЕЛО ОТНОСИТСЯ К НОВОВВЕДЕНИЯМ

Для удовлетворения потребностей клиентов и сохранения конкурентоспособности необходимы нововведения и возможность применения сотрудниками новых технологий. Система Forcepoint DLP, решение для защиты утечки данных компании Forcepoint, расширяет средства контроля за данными на корпоративные облачные приложения и конечные устройства. Это позволяет безопасно использовать мощные облачные сервисы, такие как Microsoft Office 365, Google for Work и SalesForce.com, а также защищать конфиденциальные данные и интеллектуальную собственность на портативных компьютерах Windows и Mac как в сети, так и вне ее.

Компания Forcepoint обеспечивает безопасный обмен и совместную работу над данными внутри организации и за ее пределами вместе с доверенными партнерами посредством стратегического шифрования конфиденциальных данных передаваемых на съемные устройства хранения, которые автоматически дешифруются на конечных устройствах, на которых запущена система Forcepoint DLP Endpoint.

УПРОЩЕНИЕ ПРОБЛЕМЫ РАЗВЕРТЫВАНИЯ И УПРАВЛЕНИЯ

Мы предлагаем самые точные и надежные политики корпоративной системы DLP на основе простейшей стратегии внедрения системы DLP любого поставщика. Готовая глобальная библиотека политик и простой модуль оперативной помощи использует региональные и отраслевые фильтры, чтобы рекомендовать набор политик DLP для быстрой защиты интеллектуальной собственности и регулируемых данных, и все это в одном шаблоне. Компания Forcepoint также является первым поставщиком DLP, который предоставляет политики на основе поведения, которые сочетают в себе осведомленность о контенте и контексте для автоматического определения момента, когда конфиденциальные данные подвергаются риску со стороны пользователей. Процесс обработки инцидентов через электронную почту упрощает распространение инцидента для проверки и исправления владельцами данных и деловыми партнерами без необходимости предоставления доступа к системе управления DLP. Система обеспечивает генерацию стандартизованных отчетов для аудиторов и позволяет их настраивать, при необходимости.

ЗАВЕРШЕНИЕ ЗАЩИТЫ ДАННЫХ ПОСРЕДСТВОМ НАИБОЛЕЕ ПЕРЕДОВЫХ ТЕХНОЛОГИЙ В ИНДУСТРИИ

Вредоносный снимок экрана, представленный в виде файла, сканированного и сохраненного как изображение с расширением jpeg, файл с медицинским изображением, файл с банковским изображением, старые файлы, представляют собой «мертвые зоны» для традиционных решений DLP— но не для системы Forcepoint DLP.

С помощью оптического распознавания символов (OCR) компании Forcepoint можно надежно определить и защитить конфиденциальные данные внутри изображения. Такая уникальная возможность позволяет контролировать поток конфиденциальной информации на снимках экрана, страницах факса, смартфонах и настольных фотографиях, а также в документах, таких как чеки, квитанции и отсканированные старые файлы, защищая компанию от изощренных атак, внутренних угроз или кражи данных.

Улучшите осведомленности с целью лучшего понимания изощренных методов кражи данных, таких как настраиваемое шифрование для затруднения понимания данных или отправка данных малыми объемами, чтобы избежать обнаружения.

СОЕДИНЕНИЕ ПЕРЕМЕЩЕНИЯ ДАННЫХ С ПОВЕДЕНИЕМ ПОЛЬЗОВАТЕЛЕЙ С ЦЕЛЬЮ ПОЛНОЙ ЗАЩИТЫ ДАННЫХ

Компания Forcepoint является первым поставщиком, который интегрирует свое передовое решение DLP с инструментом поиска внутренних угроз Forcepoint Insider Threat для обеспечения контекста нарушений политики данных и документирования намерений пользователей. Такой ведущий в индустрии подход предоставляет контекст для попыток пользователя передать конфиденциальные данные. Съемка цифровой камерой «через плечо» пользователя и возможность воспроизведения записи обеспечивают необходимый контекст работы пользователя данных, выявляя ранние признаки взлома системы, кражи учетных данных или пользователя, выполняющего злонамеренные действия или просто совершающего ошибки.

Компоненты систем Forcepoint DLP и Forcepoint DLP Endpoint

Объединение системы Forcepoint DLP (Forcepoint DLP Discovery и Forcepoint DLP Network) с системой Forcepoint DLP Endpoint расширяет воздействие элементов управления системы Enterprise DLP компании Forcepoint на информационные каналы, представляющие наибольший риск для данных: Интернет, электронная почта, облачные приложения и конечные устройства. Компания Forcepoint является единственным поставщиком, предоставляющим стратегии и технологии корпоративного класса для защиты интегрированных информационных каналов (Интернет и электронная почта) и распространение данных стратегий и отчетов на решение Enterprise DLP. При этом обеспечивается передовая технология защиты важных данных. Система PreciseID Fingerprinting может обнаруживать даже фрагмент в структурированных или неструктурированных данных, находящихся как на локальном, так и на конечном устройстве Windows или Mac, в сети или вне сети.

ПО FORCEPOINT DLP ENDPOINT	ПО DLP Endpoint компании Forcepoint защищает важные данные на конечных устройствах Windows и Mac, внутри или вне корпоративной сети. ПО PreciseID Fingerprinting позволяет обнаруживать даже фрагмент структурированных или неструктурированных данных на конечном устройстве вне сети. ПО выполняет слежение за выгрузками через Интернет, в том числе, по протоколу HTTPS, а также выгрузками в облачные службы, такие как Office 365 и Box Enterprise. Обеспечивается полная интеграция системы с Outlook, Notes, клиентами электронной почты. При этом используется интерфейс пользователя идентичный интерфейсам решений Data, Web, Email и Endpoint компании Forcepoint.
ПО FORCEPOINT DLP DISCOVERY	ПО Forcepoint DLP Discovery определяет и защищает конфиденциальные данные в сети, а также данные, хранимые в облачных службах, таких как Office 365 и Box Enterprise. Посредством ПО Forcepoint DLP Endpoint возможности ПО Forcepoint DLP Discovery могут быть распространены на конечные устройства под управлением Mac OS X и Windows, внутри сети или вне ее. Использование передовых технологий работы с отпечатками пальцев гарантирует соблюдение конфиденциальности данных.
ПО FORCEPOINT DLP NETWORK	Крайне важно остановить кражу данных, которые передаются по каналам электронной почты и Интернет. ПО Forcepoint DLP Network помогает определять и предотвращать потерю данных по вине вредоносных программ или случайную потерю данных при внешних атаках или при увеличении числа внутренних угроз. Противодействие изощренным методикам уклонения угроз от обнаружения возможно благодаря использованию мощного модуля оптического распознавания символов OCR для распознавания данных в изображении. Используйте ПО Drip DLP для того, чтобы остановить кражу данных по одной записи за раз, а также производить мониторинг поведения для определения пользователей с высоким риском.
МОДУЛЬ АНАЛИЗА ИЗОБРАЖЕНИЙ	Для выполнения местных нормативных обязательств в различных странах или для того, чтобы просто гарантировать наличие среды, свободной от беспокоящих действий, используется дополнительный модуль анализа изображений (Image Analyses Module). Модуль определяет откровенные изображения, такие как порнография, которые хранятся в корпоративной сети или пересылаются по каналам электронной почты или Интернет. Перейдите по ссылке forcepoint.com/contact, чтобы запросить демонстрационный модуль.

«Мне лучше спится, когда я знаю, что наши данные защищены компанией Forcepoint».

— Ахмет Таскезер (Ahmet Taskeser), топ менеджер SIMM, банк «Финансбанк» (Finansbank)

Возможности решений компании Forcepoint

Система классификации ACE (Advanced Classification Engine)

Система ACE компании Forcepoint обеспечивает облачную встроенную контекстуальную защиту в реальном времени для Интернет, 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

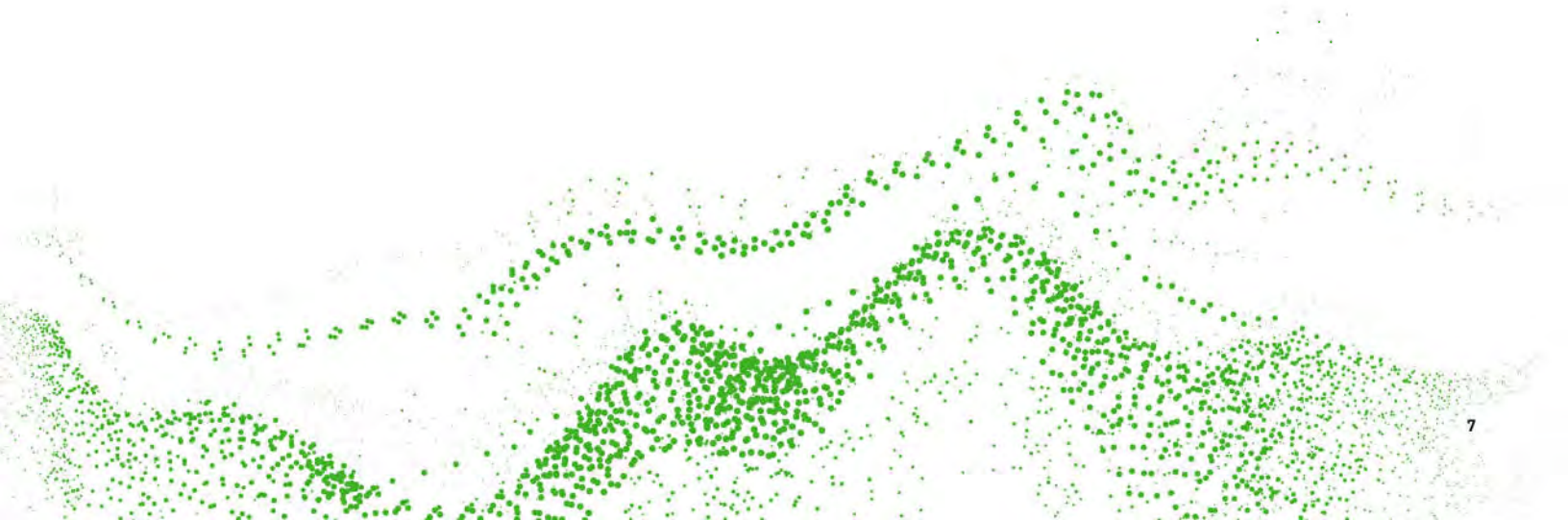
- Доступны 10 000 аналитических функций для выполнения глубокого анализа.
- Предиктивная система безопасности предвидит несколько будущих событий.
- Встроенные средства защиты не только отслеживают, но и блокируют угрозы.

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_DLP_EN] 400004. 021317

FORCEPOINT
POWERED BY Raytheon