Trellix Защита от утечки данных

TRELLIX DATA LOSS PREVENTION

это набор решений для защиты от утечки данных в сеть и за ее пределы. Политики Trellix DLP помогают понять типы данных в вашей сети, способ получения и передачи этих данных и наличие конфиденциальной информации.

ОСНОВНЫЕ ВОЗМОЖНОСТИ:

Trellix DLP предоставляет комплексную защиту от всех потенциальных каналов утечки, включая внешние накопители, облачные сервисы, электронную почту, мгновенные сообщения, веб-сайты, печать, буфер обмена, снимки экрана и приложения для обмена файлами.

Выполнение требований соответствия — обеспечение compliance путем реагирования на повседневные действия пользователей, такие как отправка электронной почты, публикация в облачные сервисы и загрузка на внешние накопители.

Ведущая защита — применение меток, классификации и маркировки файлов для защиты конфиденциальных, неструктурированных данных, таких как интеллектуальная собственность и коммерческие тайны.

Обучение пользователей — предоставление обратной связи в режиме реального времени через всплывающие образовательные сообщения, чтобы помочь формировать сознание о корпоративной безопасности и культуре.

Централизованное управление — интеграция с программным обеспечением Trellix ePO для оптимизации управления политиками и инцидентами.

Сканирование и обнаружение — сканирование файлов и баз данных, хранящихся на локальных конечных точках, общих хранилищах или облаках, для обнаружения конфиденциальных данных.

Продукты Trellix DLP:

TRELLIX DEVICE CONTROL

Контроль использования съемных носителей на конечных точках. Trellix Device Control содержит выборку правил защиты в Trellix DLP Endpoint для Windows и Mac.

ОСНОВНЫЕ ВОЗМОЖНОСТИ:

- Контролирует то, какие данные могут быть скопированы на съемные устройства, или контролирует сами устройства. Он может полностью блокировать их или делать доступными только для чтения.
- Обеспечивает защиту USB-накопителей, смартфонов, устройств Bluetooth и других съемных носителей.
- Предупреждает утечку исполняемых файлов на съемных носителях. Возможны исключения для обязательных исполняемых файлов, таких как защита от вирусов.

TRELLIX DLP ENDPOINT

Агентское решение, которое проверяет действия пользователей. Оно сканирует данные, используемые на конечных точках, и блокирует или шифрует несанкционированный перенос данных, определенных как конфиденциальные. Функция Endpoint Discovery сканирует локальную файловую систему, файлы хранения электронной почты и применяет правила защиты конфиденциального содержимого.

ОСНОВНЫЕ ВОЗМОЖНОСТИ:

- Trellix DLP Endpoint содержит все функции Trellix Device Control.
- Механизм классификации применяет определение и критерии классификации, которые обнаруживают контент, который нужно защитить, а также то, когда и где следует принять меры.
- Правила защиты применяют критерии классификации и другие определения защиты конфиденциального контента.
- Защита от потери данных из буфера обмена, облачных приложений, электронной почты, сетевых ресурсов, принтеров, снимков экрана, доступа к файлам для приложений, веб-публикаций, съемных носителей данных, файлов локальной файловой системы.
- Работает локально в конечной точке, ищет файлы локальной файловой системы и файлы хранения электронной почты и применяет политики для защиты конфиденциальных данных.

TRELLIX DLP PREVENT

Работает с вашим прокси-сервером или MTA сервером, чтобы защитить веб-трафик и электронную почту.

ОСНОВНЫЕ ВОЗМОЖНОСТИ:

- Trellix DLP Prevent взаимодействует с вашей электронной почтой и веб-трафиком, генерирует инциденты и сохраняет их для просмотра отдельных случаев.
- Проактивно применяет политики для всех типов информации, посылаемой по электронной почте или через Интернет.
- Применяет политики для известной и неизвестной конфиденциальной информации.
- Фильтрует и контролирует конфиденциальную информацию для защиты от известных и неизвестных рисков.
- Предоставляет широкий спектр встроенных политик и правил для общих требований, включая требования регулирования, интеллектуальной собственности и приемлемого использования.
- Поддерживает оптическое распознавание символов (OCR) для сканирования изображений, например добавленных в электронные письма.

TRELLIX DLP DISCOVER

Сканирование сетевых файлов, Box, SharePoint и баз данных, чтобы идентифицировать и защитить конфиденциальные данные путем копирования или перемещения файлов, а также применения политики RM. Регистрационные сканы извлекают информацию о метках из файловых хранилищ для классификации файлов и сохраняют подписи в базе данных зарегистрированных документов.

ОСНОВНЫЕ ВОЗМОЖНОСТИ:

- Выявление и классификация чувствительного контента.
- Создание базы данных с подписями зарегистрированных документов.
- Перемещение или копирование чувствительных файлов.
- Интеграция с Microsoft Rights Management Service для защиты файлов.
- Автоматизация задач IT, таких как поиск пустых файлов, определение разрешений и список файлов, изменившихся в течение определенного временного диапазона.
- Поддержка оптического распознавания символов (OCR) для классификации, устранения недостатков и регистрации результатов сканирования файловых хранилищ.

TRELLIX DLP MONITOR

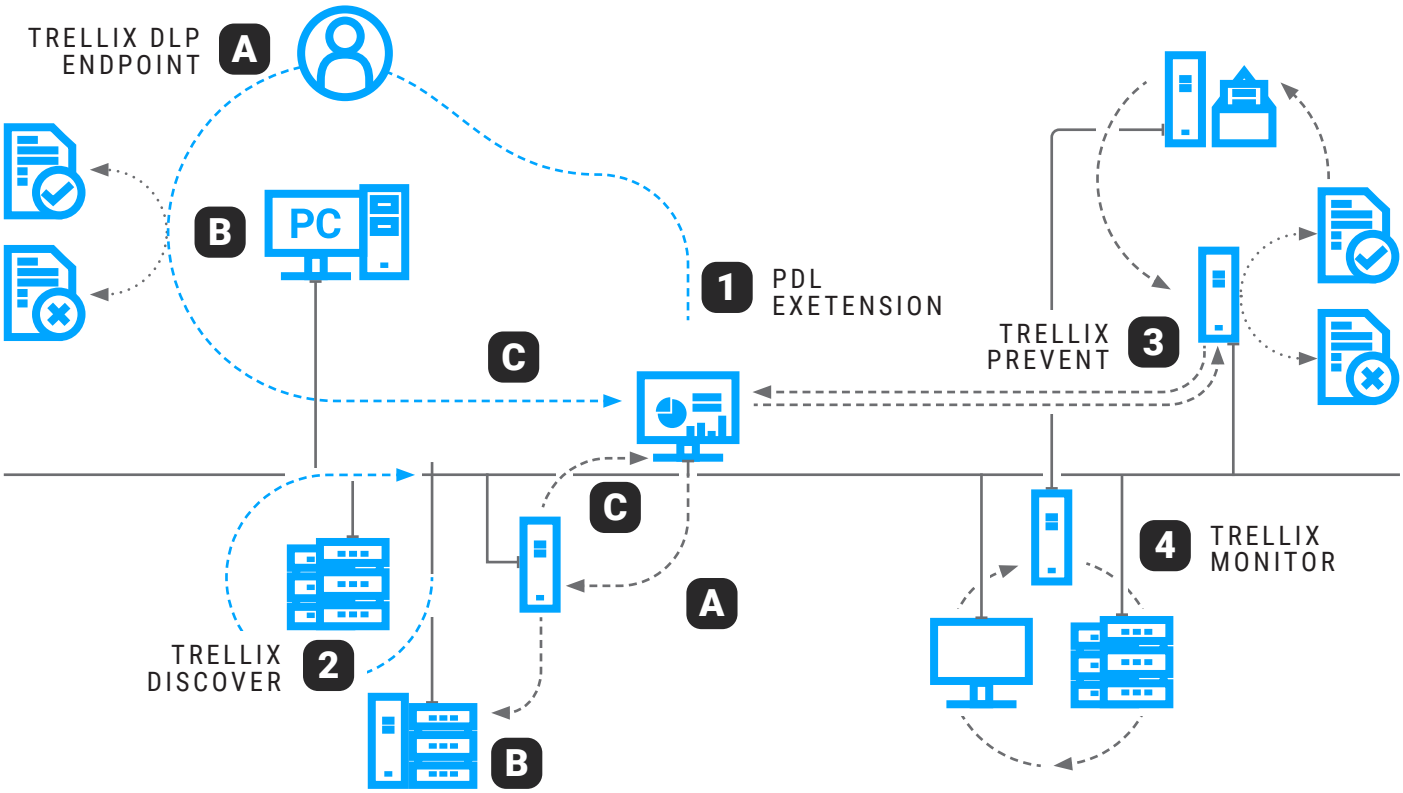
Пассивно сканирует незашифрованный сетевой трафик на предмет возможных случаев утечки данных.

ОСНОВНЫЕ ВОЗМОЖНОСТИ:

- Анализирует трафик известных протоколов TCP, чтобы идентифицировать пользователей или устройства, которые посылают большой объем неизвестного трафика, что может свидетельствовать о нарушении политики компании.
- Анализирует точки потери данных без влияния на вашу сеть, чтобы помочь вам спланировать свою стратегию предотвращения утечки данных.
- Поддерживает протоколы, не обрабатываемые прокси-серверами или почтовыми шлюзами.
- Мониторит сетевой трафик для устройств, на которых не установлен Trellix DLP.
- Предоставляет широкий спектр встроенных политик и правил для общих требований, включая требования регулирования, интеллектуальной собственности и приемлемого использования.
- Поддерживает оптическое распознавание символов (OCR) для сканирования изображений, передаваемых в интернет, или изображений, найденных в другом сетевом трафике.

ПРОДУКТЫ TRELLIX DLP PREVENT И TRELLIX DLP MONITOR, КОТОРЫЕ ИМЕЮТ ФУНКЦИЮ DLP CAPTURE, ТАКЖЕ:

- Захватывают содержимое для дальнейшего анализа ключевых слов, деятельности пользователей или названий файлов, чтобы обнаружить возможные случаи потери данных, пропущенных защитой электронной почты, веб-защитой или правилами защиты сетевой связи.
- Позволяют полностью настраивать правила защиты электронной почты, веб- или сетевой связи для тестирования с помощью базы данных DLP Capture.



НА ДИАГРАММЕ ПОКАЗАНА УПРОЩЕННАЯ СЕТЬ, ГДЕ РАЗВЕРНУТЫ ВСЕ ПРОДУКТЫ TRELLIX DLP И TRELLIX EPO.

1. **Администраторы создают политики в Trellix ePO** и развертывают их на клиентах Trellix DLP Endpoint.
   a. Пользователи создают, сохраняют и копируют файлы или электронные письма.
   b. Клиент Trellix DLP Endpoint применяет политики и блокирует или разрешает действия пользователей.
   c. Применение политик создает случаи, отправляемые в DLP Incident Manager для отчетности и анализа.
2. **Trellix DLP Discover сканирует файлы из локальных или облачных хранилищ** и локальных баз данных, собирая метаданные файлов.
   a. Trellix DLP Discover получает классификации и политики от Trellix ePO для применения во время классификации или исправления сканирования.
   b. Программное обеспечение DLP Server создает базы данных зарегистрированных документов для использования в политиках для Trellix DLP Discover, Trellix DLP Prevent и Trellix DLP Monitor.
   c. Инциденты сканирования отправляются в DLP Incident Manager для отчетности и анализа.
3. **Trellix DLP Prevent получает электронные письма от серверов MTA и веб-трафик от прокси-серверов.** Он анализирует сообщения электронной почты и веб-трафик, применяет политики Trellix DLP и отправляет случаи и доказательства DLP Incident Manager.
4. **Trellix DLP Monitor анализирует сетевой трафик, затем создает инциденты или сохраняет доказательства для поддерживаемых протоколов.** Он применяет правила защиты для сети, Интернета или электронной почты.