Trellix Захист від витоку даних

TRELLIX DATA LOSS PREVENTION

це набір рішень для захисту від витоку даних в мережу та за її межі. Політики Trellix DLP допомагають зрозуміти типи даних у вашій мережі, спосіб їх отримання й передачі та наявність конфіденційної інформації.

ОСНОВНІ МОЖЛИВОСТІ:

Trellix DLP надає комплексний захист від усіх потенційних каналів витоку, включно з зовнішніми накопичувачами, хмарними сервісами, електроною поштою, миттєвими повідомленнями, вебсайтами, друком, буфером обміну, знімками екрана та додатками для обміну файлами.

Виконання вимог відповідності — забезпечення compliance шляхом реагування на повсякденні дії користувачів, такі як відправлення електронної пошти, публікація в хмарні сервіси та завантаження на зовнішні накопичувачі.

Провідний захист — застосування міток, класифікації та маркування файлів для захисту конфіденційних, неструктурованих даних, таких як інтелектуальна власність та комерційні таємниці.

Навчання користувачів — надання зворотного зв'язку в режимі реального часу через навчальні спливаючі повідомлення, щоб допомогти формувати усвідомлене ставлення до корпоративної безпеки та культури.

Централізоване управління — інтеграція з програмним забезпеченням Trellix ePO для оптимізації управління політиками та інцидентами.

Сканування та виявлення — сканування файлів та баз даних, що зберігаються на локальних кінцевих точках, спільнихсховищах або в хмарі, для виявлення конфіденційних даних.

Продукти Trellix DLP:

TRELLIX DEVICE CONTROL

Контролює використання знімних носіїв на кінцевих точках. Trellix Device Control містить вибірку правил захисту в Trellix DLP Endpoint для Windows та Mac.

ОСНОВНІ МОЖЛИВОСТІ:

- Контролює те, які дані можуть бути скопійовані на знімні пристрої, або контролює самі пристрої. Він може повністю блокувати їх або робити доступними тільки для читання.
- Забезпечує захист для USB-накопичувачів, смартфонів, пристроїв Bluetooth та інших знімних носіїв.
- Запобігає витоку виконуваних файлів на знімних носіях. Можливі винятки для обов'язкових виконуваних файлів, таких як захист від вірусів.

TRELLIX DLP ENDPOINT

Агентське рішення, яке перевіряє дії користувачів. Воно сканує дані, що використовуються на кінцевих точках, та блокує або шифрує несанкціоноване перенесення даних, визначених як конфіденційні. Функція Endpoint Discovery сканує локальну файлову систему, файли зберігання електронної пошти та застосовує правила для захисту конфіденційного вмісту.

ОСНОВНІ МОЖЛИВОСТІ:

- Trellix DLP Endpoint містить всі функції Trellix Device Control.
- Механізм класифікації застосовує визначення та критерії класифікації, які визначають контент, який потрібно захистити, а також те, коли і де слід вжити заходів.
- Правила захисту застосовують критерії класифікації та інші визначення для захисту конфіденційного контенту.
- Захист від втрати даних з: буфера обміну, хмарних застосунків, електронної пошти, мережевих ресурсів, принтерів, знімків екрана, доступу до файлів для додатків, вебпублікацій, знімних носіїв даних, файлів локальної файлової системи.
- Працює локально на кінцевій точці, шукає файли локальної файлової системи та файли зберігання електронної пошти і застосовує політики для захисту конфіденційних даних.

TRELLIX DLP PREVENT

Працює з вашим вебпроксі або MTA сервером, щоб захистити вебтрафік та електронну пошту.

ОСНОВНІ МОЖЛИВОСТІ:

- Trellix DLP Prevent взаємодіє з вашою електронною поштою та вебтрафіком, генерує інциденти та зберігає їх для подальшого перегляду окремих випадків.
- Проактивно застосовує політики для всіх типів інформації, яка надсилається електронною поштою або через інтернет.
- Застосовує політики для відомої та невідомої вам конфіденційної інформації.
- Фільтрує та контролює конфіденційну інформацію, щоб захиститися від відомих та невідомих ризиків.
- Надає широкий спектр вбудованих політик та правил для загальних вимог, включно з вимогами регулювання, інтелектуальної власності та прийнятного використання.
- Підтримує оптичне розпізнавання символів (OCR) для сканування зображень, наприклад, доданих до електронних листів.

TRELLIX DLP DISCOVER

Сканує мережеві файли, Box, SharePoint та бази даних, щоб ідентифікувати та захистити конфіденційні дані шляхом копіювання або переміщення файлів чи застосування політики RM. Реєстраційні скани витягують інформацію про мітки з файлових сховищ для класифікації файлів та зберігають підписи в базі даних зареєстрованих документів.

ОСНОВНІ МОЖЛИВОСТІ:

- Виявляє та класифікує чутливий контент.
- Створює бази даних з підписами зареєстрованих документів.
- Переміщує або копіює чутливі файли.
- Інтегрується з Microsoft Rights Management Service для застосування захисту до файлів.
- Автоматизує завдання IT, такі як пошук порожніх файлів, визначення дозволів та перелік файлів, які змінилися протягом визначеного часового діапазону.
- Підтримує оптичне розпізнавання символів (OCR) для класифікації, усунення недоліків та реєстрації результатів сканування файлових сховищ

TRELLIX DLP MONITOR

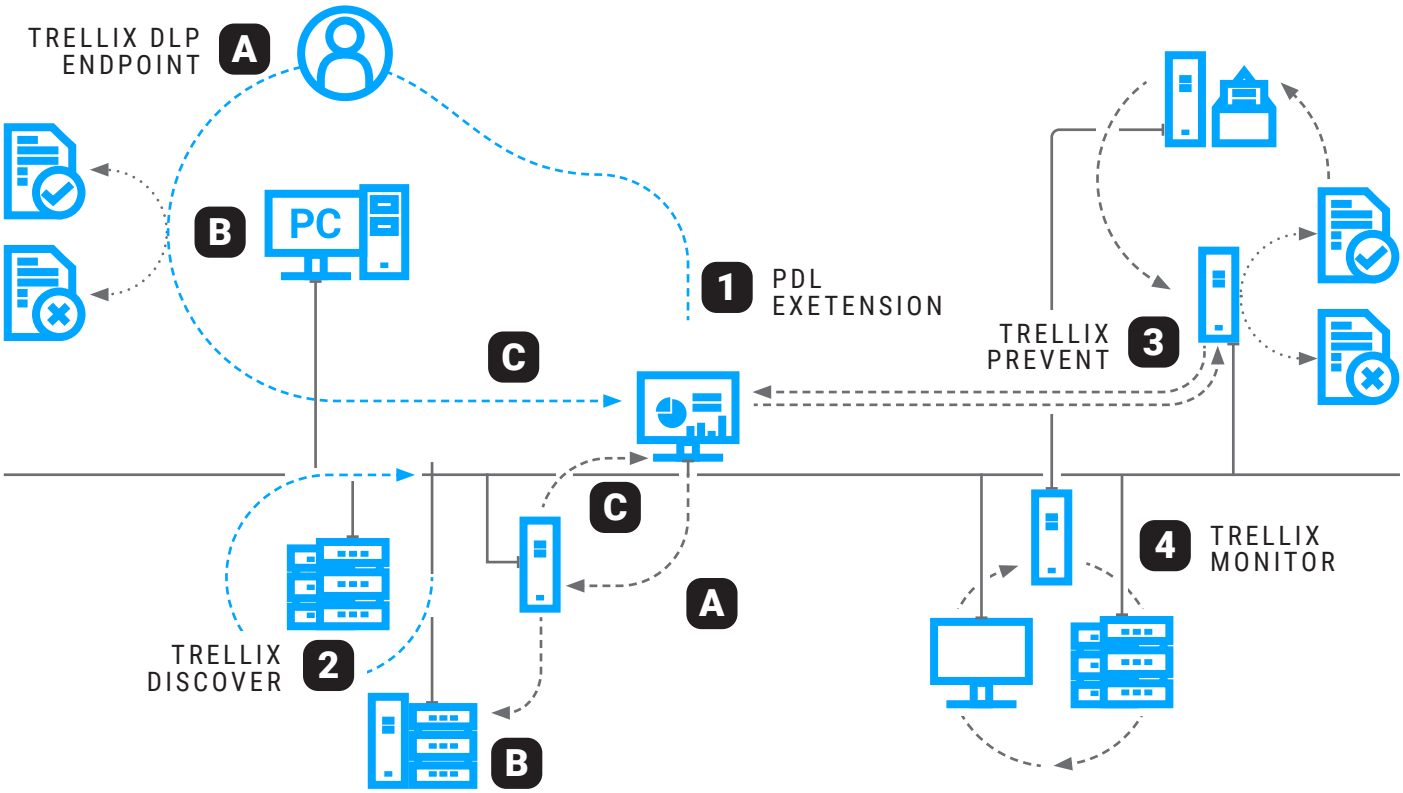
Пасивно сканує незашифрований мережевий трафік щодо потенційних випадків витоку даних.

ОСНОВНІ МОЖЛИВОСТІ:

- Аналізує трафік відомих протоколів TCP, щоб ідентифікувати користувачів або пристрої, які надсилають великий обсяг невідомого трафіку, що може свідчити про порушення політики компанії.
- Аналізує точки втрати даних без впливу на вашу мережу, щоб допомогти вам спланувати свою стратегію запобігання витоку даних.
- Підтримує протоколи, які не обробляються проксі-серверами чи поштовими шлюзами.
- Моніторить мережевий трафік для пристроїв, на яких не встановлено Trellix DLP.
- Надає широкий спектр вбудованих політик та правил для загальних вимог, включно з вимогами регулювання, інтелектуальної власності та прийнятного використання.
- Підтримує оптичне розпізнавання символів (OCR) для сканування зображень, що надсилаються в інтернет, або зображень, знайдених в іншому мережевому трафіку.

ПРОДУКТИ TRELLIX DLP PREVENT ТА TRELLIX DLP MONITOR, ЯКІ МАЮТЬ ФУНКЦІЮ DLP CAPTURE, ТАКОЖ:

- Захоплюють вміст для подальшого аналізу ключових слів, діяльності користувачів або назв файлів, щоб виявити можливі випадки втрати даних, які були пропущені захистом електронної пошти, вебзахистом або правилами захисту мережевого зв'язку.
- Дозволяють повністю налаштовувати правила захисту електронної пошти, вебу або мережевого зв'язку для тестування за допомогою бази даних DLP Capture.



НА ДІАГРАМІ ПОКАЗАНО СПРОЩЕНУ МЕРЕЖУ, ДЕ РОЗГОРНУТІ ВСІ ПРОДУКТИ TRELLIX DLP ТА TRELLIX EPO.

1. **Адміністратори створюють політики в Trellix ePO та розгортають їх на клієнтах Trellix DLP Endpoint.**
   a. Користувачі створюють, зберігають та копіюють файли або електронні листи.
   b. Клієнт Trellix DLP Endpoint застосовує політики та блокує або дозволяє дії користувачів.
   c. Застосування політик створює випадки, які відправляються до DLP Incident Manager для звітності та аналізу.
2. **Trellix DLP Discover сканує файли з локальних або хмарних сховищ та локальних баз даних, збираючи метадані файлів.**
   a. Trellix DLP Discover отримує класифікації та політики від Trellix ePO для застосування під час класифікації або виправлення сканувань.
   b. Програмне забезпечення DLP Server створює бази даних зареєстрованих документів для використання в політиках для Trellix DLP Discover, Trellix DLP Prevent та Trellix DLP Monitor.
   c. Інциденти сканувань відправляються до DLP Incident Manager для звітності та аналізу.
3. **Trellix DLP Prevent отримує електронні листи від серверів MTA та вебтрафік від проксі-серверів.** Він аналізує повідомлення електронної пошти та вебтрафік, застосовує політики Trellix DLP та відправляє випадки і докази до DLP Incident Manager.
4. **Trellix DLP Monitor аналізує мережевий трафік, потім створює інциденти або зберігає докази для підтримуваних протоколів.** Він застосовує правила захисту для мережі, вебу або електронної пошти.