TRELLIX ENDPOINT SECURITY SUITE (TRXE1)

ЗАХИСТ КІНЦЕВИХ ТОЧОК, ВИЯВЛЕННЯ, РОЗСЛІДУВАННЯ ТА РЕАГУВАННЯ НА ПРОСУНУТІ ЗАГРОЗИ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Комплекс безпеки, що розширює бандл Trellix Protect Plus EDR for Endpoint функціями розслідувань та аналізу кінцевих точок. Посилене форензикою рішення з можливістю наземного розгортання, що допомагає у збиранні криміналістичних даних та пошуках ознак компрометації, а також дозволяє віддалено підключитися до робочої станції для збирання додаткових даних та усунення загроз.

ПЕРЕВАГИ:

- Пошук та розслідування відомих та невідомих загроз на десятках тисяч кінцевих точок за лічені хвилини
- Скорочення часу на виявлення загроз та реагування на них для мінімізації потенційних збоїв
- Реагування і керування життєвим циклом захисту від загроз для підтримки продуктивності користувачів і адміністраторів
- Виявлення та запобігання новим шкідливим програмам завдяки машинному навчанню
- Автоматизація та спрощення складних робочих процесів
- Підвищення продуктивності IT відділу завдяки управлінню комплексом з єдиної консолі
- Зменшення потреби в додаткових ресурсах SOC завдяки керованому розслідуванню

КОМПОНЕНТИ:

ePolicy Orchestrator (ePO) – центральний сервер керування кінцевими точками, що може бути розгорнутий як on-prem, так і в хмарі, в тому числі SaaS

- Ручне/автоматичне розгортання
- та оновлення засобів захисту
- Налаштування політик безпеки для захисту від загроз, витоку інформації, а також керування вбудованим в ОС шифруванням
- Запити та звіти про стан інфраструктури
- Відповідність інфраструктури стандартам безпеки
- Автоматизація процесів адміністрування та реагування на будь–які загрози
- Інтеграція з рішеннями інших виробників
- Можливість управління інфраструктурою звідусіль

Endpoint Security (ENS) – next-gen захист для Windows, macOS та Linux

- Безсигнатурний та сигнатурний аналіз на основі репутації
- Контейнеризація – динамічне стримування застосунків
- Захист від безтілесних (скриптових) атак
- Ізоляція систем з підозрілою активністю
- Автоматичне відновлення після усунення загроз

Trellix Endpoint – апгрейд Windows Defender функціями Endpoint Security

- Централізоване керування Windows Defender, Firewall та Exploit Guard
- Доповнення Windows Defender next–gen технологіями
- Оптимальне рішення для захисту систем з мінімальними ресурсами
- Використання мінімуму ресурсів

Trellix Insights – інформаційна база кібератак, інструмент аудиту політик безпеки

- Практичні рекомендації для покращення захисту
- Джерело індикаторів компрометації (IoC)
- Інтеграція з Trellix EDR для пошуку IoC по всій інфраструктурі
- Аудит політик безпеки
- Використання мінімуму ресурсів

Trellix Endpoint Forensics (HX) – виконує швидкі та точні криміналістичні розслідування на тисячах кінцевих точках

- Запобігання кібератакам на кінцеві точки
- Виявлення шкідливих програм та інших ознак компрометації на робочих станціях у масштабах підприємства
- Оперативне реагування на інциденти, пов'язані з безпекою кінцевих точок.

Application Control for PCs – модуль контролю запуску застосунків на основі black/white lists

- Фіксування застосунків та їх версій в ОС
- Блокування будь–яких виконуваних файлів
- Без використання сигнатур
- Низьке використання системних ресурсів
- Підтримка Windows XP

Threat Intelligence Exchange (TIE) – центральна база репутацій виконуваних файлів

- Агрегація репутацій з рішень безпеки (включаючи third–party)
- Обмін репутаціями файлів між засобами захисту
- Ручне централізоване управління репутаціями

Data Exchange Layer (DXL) – технология для хранения и обмена системной информацией, телеметрией и репутациями

- Практически мгновенный обмен информацией и координирование задач в режиме реального времени
- Сокращение задержек, облегчение и упрощение интеграции решений различных производителей

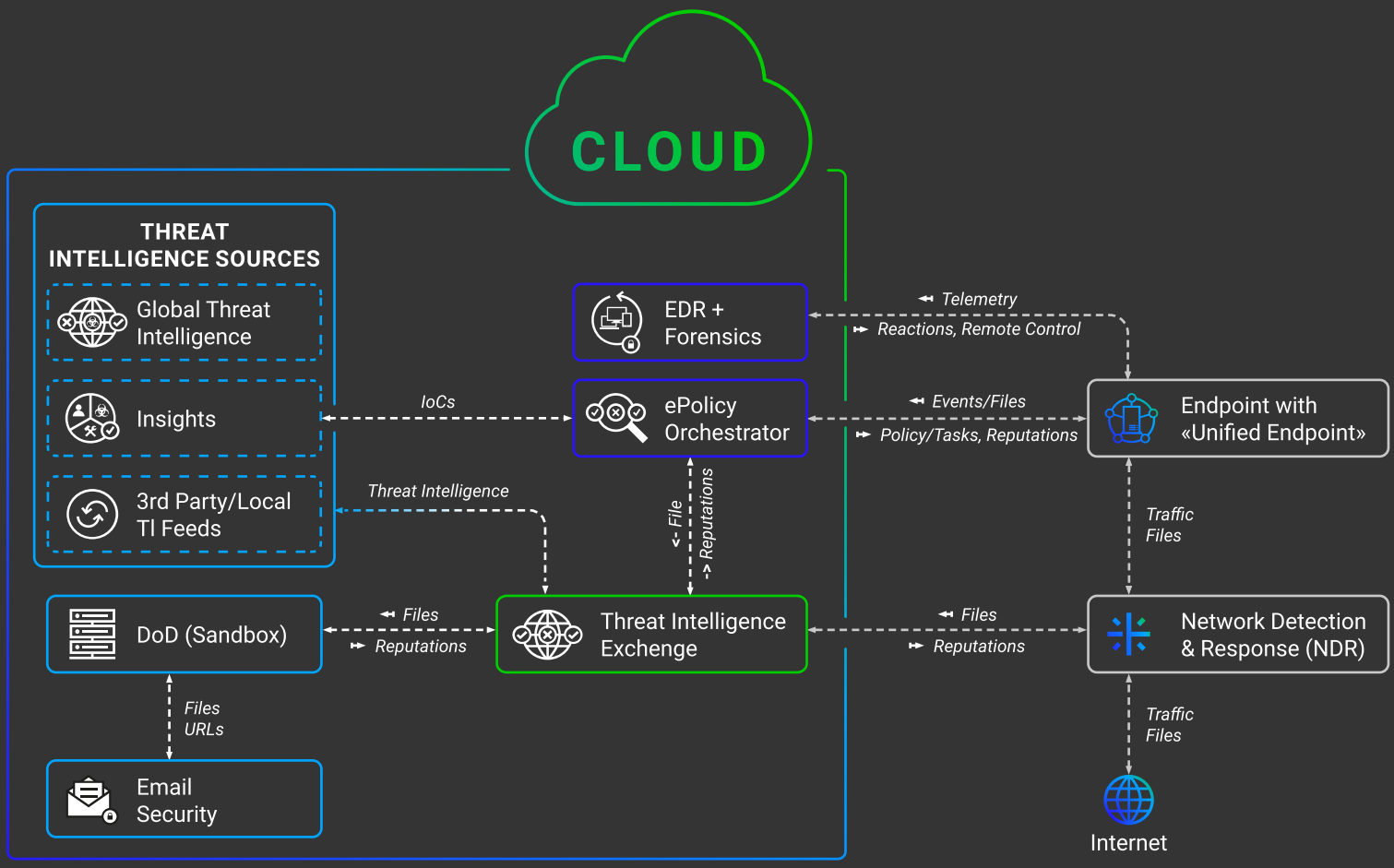
Trellix EDR – інструмент для виявлення та реагування на ускладнені загрози

- Постійний моніторинг кінцевих точок
- Проведення професійного розслідування за участі штучного інтелекту
- Пошук слідів на кінцевих точках у режимі реального часу
- Реагування на інциденти шляхом запуску скриптів (в тому числі власних)

Device Control – інструмент для контроля і управління будь–якими пристроями, підключеними до систем

- Чорні/білі списки пристроїв
- Заборона читання/запису на носії інформації
- Контроль підключення мобільних пристроїв
- Детальний звіт по кожному інциденту

АРХИТЕКТУРА :



Примітка: Email Security, DoD та NDR не входять до цього комплексу