TRELLIX ENDPOINT SECURITY SUITE (TRXE1)

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК, ВЫЯВЛЕНИЕ, РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ПРОДВИНУТЫЕ УГРОЗЫ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Комплекс безопасности объединяет ряд передовых технологий, обеспечивающих надежную защиту конечных точек от продвинутых угроз. Адаптивная архитектура безопасности, проактивная защита и непрерывный мониторинг систем позволяют существенно уменьшить последствия кибератак и как можно скорее восстановить бизнес–процессы.

ПРЕИМУЩЕСТВА:

- Поиск и расследование известных и неизвестных угроз на десятках тысяч конечных точек за считанные минуты
- Сокращение времени на обнаружение угроз и реагирование на них для минимизации потенциальных сбоев
- Реагирование и управление жизненным циклом защиты от угроз для поддержания производительности пользователей и администраторов
- Обнаружение и предотвращение новых вредоносных программ благодаря машинному обучению
- Автоматизация и упрощение сложных рабочих процессов
- Повышение производительности ИТ отдела благодаря управлению комплексом с единой консоли
- Уменьшение потребности в дополнительных ресурсах SOC благодаря управляемому расследованию

КОМПОНЕНТЫ:

ePolicy Orchestrator (ePO) – центральный сервер управления конечными точками, который может быть развернут как on-prem, так и в облаке, в том числе SaaS

- Ручное/автоматическое развертывание и обновление средств защиты
- Настройка политик безопасности
- для защиты от угроз, утечки информации, а также управление встроенным ОС шифрованием
- Запросы и отчеты о состоянии инфраструктуры
- Соответствие инфраструктуры стандартам безопасности
- Автоматизация процессов администрирования и реагирования на любые угрозы
- Интеграция с решениями других производителей
- Возможность управления инфраструктурой отовсюду.

Endpoint Security (ENS) – next-gen защита для Windows, macOS и Linux

- Поведенческий и сигнатурный анализ на основе репутации
- Контейнеризация – динамическое сдерживание приложений
- Защита от бестелесных (скриптовых) атак
- Изоляция систем с подозрительной активностью
- Автоматическое восстановление после устранения угроз

Trellix Endpoint – апгрейд Windows Defender функциями Endpoint Security

- Централизованное управление Windows Defender, Firewall и Exploit Guard
- Дополнение Windows Defender next–gen технологиями
- Оптимальное решение для защиты систем с минимальными ресурсами
- Использование минимума ресурсов

Trellix Insights – информационная база кибератак, инструмент аудита политик безопасности

- Практические рекомендации для улучшения защиты
- Источник индикаторов компрометации (IoC)
- Интеграция с Trellix EDR для поиска IoC по всей инфраструктуре
- Аудит политик безопасности

Trellix Endpoint Forensics (HX) – выполняет быстрые и точные криминалистические расследования на тысячах конечных точек

- Блокировка вредоносных приложений
- Защита от сетевых атак и фишинга
- Использование технологий искусственного интеллекта

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

- Фиксирование приложений и их версий в ОС
- Блокировка любых исполняемых файлов
- Без использования сигнатур
- Низкое использование системных ресурсов
- Поддержка Windows XP

Threat Intelligence Exchange (TIE) – центральная база репутаций исполняемых файлов

- Агрегация репутаций из решений безопасности (включая third–party)
- Обмен репутациями файлов между средствами защиты
- Ручное централизованное управление репутациями.

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

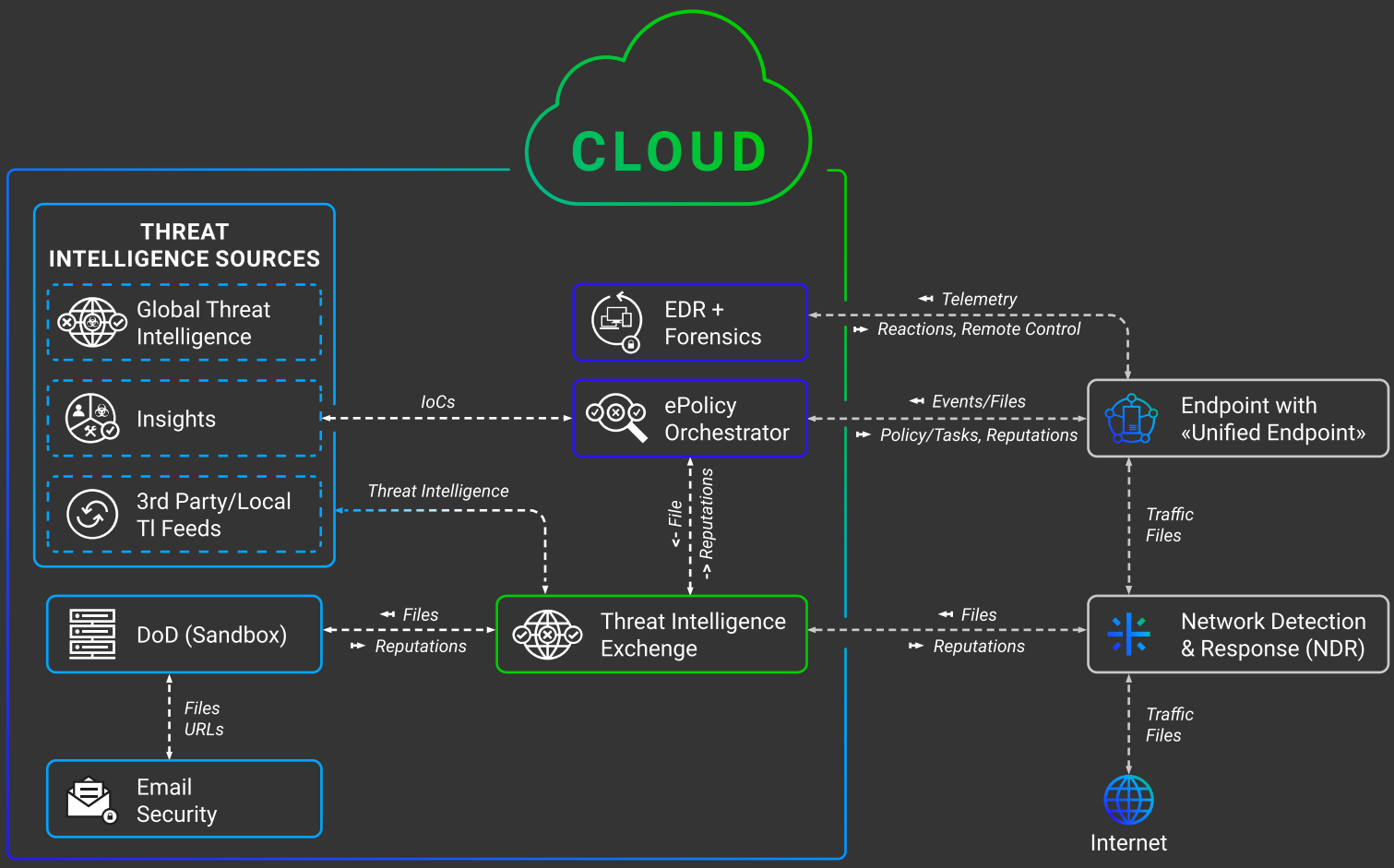
Trellix EDR – инструмент для обнаружения и реагирования на продвинутые угрозы

- Постоянный мониторинг конечных точек
- Проведение профессионального расследования с участием искусственного интеллекта
- Поиск следов на конечных точках в режиме реального времени
- Реагирование на инциденты путем запуска скриптов (в том числе собственных)

Device Control я инструмент для контроля и управления любыми устройствами, подключенными к системам

- Предотвращение кибератак на конечные точки
- Обнаружение вредоносных программ и других признаков компрометации на рабочих станциях в масштабах предприятия
- Оперативное реагирование на инциденты, связанные с безопасностью конечных точек

АРХИТЕКТУРА :



Примечание: Email Security, DoD, и NDR не входят в этот комплекс