Trellix Email Security

Зупиніть програми-вимагачі, компрометацію корпоративної електронної пошти, цільовий фішинг та імітацію авторитетного відправника

Електронна пошта залишається найбільш успішним вектором атаки, і понад 90% кібератак починаються саме з фішингу. Кіберзлочинці використовують цілеспрямовану соціальну інженерію, щоб змусити користувачів натискати на шкідливі URL-адреси та відкривати шкідливі вкладення.

Trellix Email Security - це:

- **Захист від невидимих загроз**
  Багаторівневе виявлення на основі машинного навчання, штучного інтелекту та аналітики безпеки забезпечує безпрецедентний захист від багатоетапних кампаній
- **Комплексне розслідування та реагування**
  Автоматичне вилучення електронних листів після доставки, насичені метадані для інформування про реагування на інциденти та передача їх у Trellix DR для кореляції алертів із Email Security з наявними засобами контролю безпеки
- **Гнучкі варіанти розгортання**
  Розгорнутий безпечний шлюз електронної пошти (SEG) або інтегроване рішення для захисту електронної пошти у хмарі (ICES) забезпечують швидку та безперешкодну інтеграцію API з Microsoft 365 та Google Workspace
- **Надійний та відмовостійкий захист електронної пошти**
  Доступність сервісу на рівні 99,995%, активне розгортання AWS та сертифікація FedRAMP Moderate

trellix@bakotech.com // trellix.bakotech.com

Email Security Server Edition

Найбільш комплексне у галузі рішення для забезпечення безпеки корпоративного зв'язку та спільної роботи.

Сервер Trellix Email Security – Server, розгорнутий за основним шлюзом електронної пошти в режимі “in-line” або в режимі аналізу копій повідомлень, також підтримує розгортання в AWS і мінімізує ризик злому з великими збитками.

Trellix Email Security – Server:

- Забезпечує ефективне виявлення, ізоляцію та негайну зупинку програм-вимагачів, компрометації корпоративної електронної пошти, цільового фішингу, збір облікових даних та атак на основі вкладень до того, як вони потраплять у ваше середовище
- Виявляє, ізолює та блокує новітні URL-атаки та надає контекстну інформацію для визначення пріоритетів та прискорення реагування

Ключові особливості

- Поліпшене виявлення загроз
- Розширений захист URL-адрес
- Захист від шкідливих програм
- Швидка адаптація до мінливого ландшафту загроз
- Комплексне виявлення, розслідування та реагування
- Комплексний та відмовостійкий захист від загроз з електронної пошти

Основні можливості

- Підтримка аналізу на образах операційних систем Microsoft Windows та Apple macOS x
- Перевірка електронної пошти на наявність загроз, прихованих у захищених паролем файлах, зашифрованих вкладеннях та URL-адресах
- Розгортання локально з інтегрованою чи розподіленою службою IVX
- Потокова передача метаданих у сторонні рішення SIEM
- Підтримка налаштовуваних правил YARA для підвищення ефективності виявлення загроз

trellix@bakotech.com // trellix.bakotech.com

Email Security Cloud Edition

Trellix Email Security – Cloud – це найкращі в галузі засоби виявлення, що дозволяють виявляти, ізолювати та негайно зупиняти:

- програми-вимагачі
- компрометацію корпоративної електронної пошти
- цільовий фішинг
- видавання себе за іншу особу
- атаки на основі вкладень до проникнення у ваше середовище

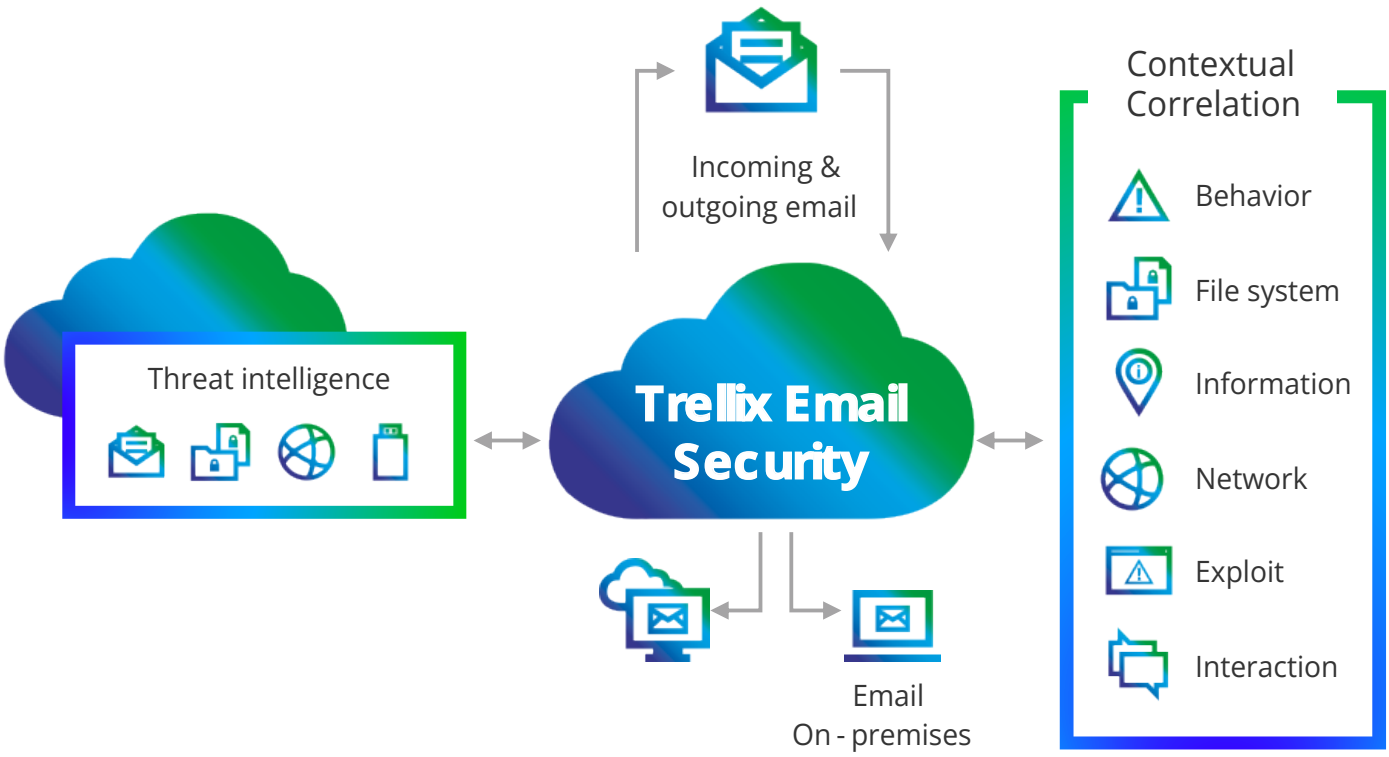
Email Security – Cloud можливості:

- Сканування вихідного поштового трафіку на наявність складних загроз, спаму та вірусів
- Комплексне розслідування та реагування допомагають узгодити операції із забезпечення безпеки у вашій організації
- Автоматичне виправлення для Microsoft 365 та Google Workspace вилучає електронні листи після доставки
- Більше 1000 зручних користувальницьких правил, що налаштовуються
- Перегляд сповіщень в режимі реального часу, створення інтелектуальних налаштовуваних правил і звітів на порталі Trellix

Містить ключові особливості Trellix Email Security Server, а також:

- Захист вихідної електронної пошти
- Просте розгортання та надійний захист
- Комплексний захист вхідної та вихідної електронної пошти
- Хмарна інтеграція з підтримкою API з Microsoft 365 та Google Workspace
- Автоматичне вилучення електронних листів після доставки
- Розгортання в режимі "in-line", з функціями антивірусу та антиспаму (ASAV) або в режимі аналізу копій повідомлень
- Потокова передача метаданих у сторонні рішення SIEM
- Доступність сервісу на рівні 99,995%
- Підтримка налаштовуваних правил YARA для підвищення ефективності виявлення загроз
- Відповідність вимогам безпеки FedRAMP та SOC2
- Можливість відстежувати черги електронної пошти та розширені параметри за допомогою трасування електронної пошти

Інфраструктура Trellix Email Security



КОНТАКТИ:

trellix@bakotech.com

trellix.bakotech.com

Trellix | bako tech®

WE BRING SECURITY TO LIFE