OPSWAT.
Protecting the World's Critical Infrastructure

MetaDefender для Email Exchange Server

Покращений захист електронної пошти від загроз, які обходять вбудовані засоби безпеки

Електронна пошта, як і раніше, залишається головним вектором загроз кібербезпеці. Відповідно до звіту CISA Analysis, 87% фішингових атак обходять звичайний захист пошти.

Щоб протистояти цим загрозам, OPSWAT створив MetaDefender для Email Exchange Server. Він надає унікальний функціонал боротьби з сучасними загрозами.

Завдяки інтеграції мультисканування, глибокого знешкодження та реконструкції контенту (CDR), а також антифішингу в режимі реального часу, MetaDefender максимально точно виявляє невідомі загрози нульового дня, шкідливі програми, фішинг та експлойти.

Адаптивна пісочниця в режимі реального часу нейтралізує загрози до того, як вони потраплять до користувача, а проактивне запобігання втраті даних доповнює основні технології захисту та гарантує безпеку конфіденційних даних.

Виклики

Вектор загроз кібербезпеці №1 — електронна пошта, по ній поширюється 92% шкідливих програм.

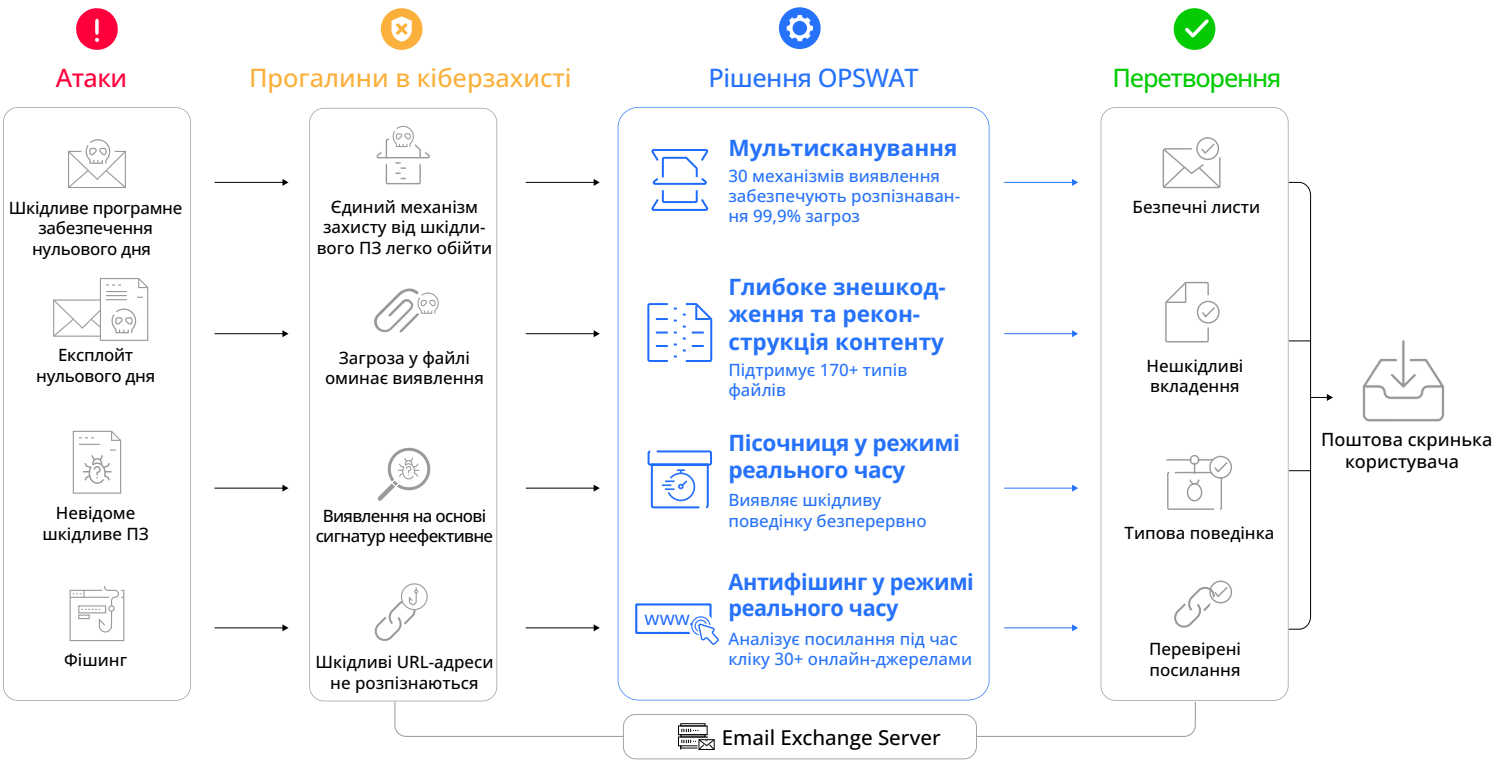
Виявлення невідомих шкідливих програм займає в середньому 49 днів, що збільшує термін дії загрози

З'являється 109 млн нових шкідливих програм на рік

Найпопулярніші вкладення, що містять загрози, є звичайними документами Office

Середня вартість одного витоку даних у 2023 році склала $4,45M (IBM Research)

У 2023 році було виявлено 26 447 уразливостей



Прогалини Email Exchange Server	OPSWAT. MetaDefender для Email Exchange Server	
Шкідливі програми нульового дня Проблема атак шкідливого ПЗ нульового дня пов'язана з обмеженнями окремих антивірусних систем, розрізненим часом відгуку різних вендорів та виникненням хибних спрацьовувань.	Мультисканування виявляє **99.20 %** із 10 000 найнебезпечніших загроз	Мультисканування поєднує до 30 механізмів виявлення, посилених евристикою та машинним навчанням. Такий підхід значно підвищує ефективність виявлення загроз.
Експлойти нульового дня Невідомі експлойти та експлойти нульового дня є значним ризиком, оскільки вони можуть обійти вбудовані заходи безпеки, які не виявляють загрози у вкладеннях.	Deep CDR виявляє, знешкоджує та нейтралізує загрози у **170+** типах файлів	Глибоке знешкодження та реконструкція контенту (Deep CDR) дозволяє знайти та нейтралізувати складні для виявлення загрози, відновити весь вміст файлів, провести глибоке очищення зображень та запобігти шифруванню.
Невідоме шкідливе ПЗ Невідомі шкідливі програми обходять сигнатурне виявлення та залишаються загрозою під час автономного аналізу традиційними пісочницями.	Пісочниця виявляє шкідливі об'єкти у 10 разів швидше **у режимі реального часу**	Адаптивна пісочниця в режимі реального часу динамічно виявляє шкідливу поведінку, забезпечує швидкий та глибокий аналіз загроз і фокусується на виявленні цільових атак та вилученні IOC. Захист здійснюється до того, як електронний лист буде отримано користувачем.
Фішинг та збір облікових даних Соціальна інженерія та фішингові атаки часто вислизають від традиційних засобів захисту, використовуючи тактику приховування URL-адрес та таємного збору облікових даних.	Антифішинг в режимі реального часу аналізує посилання під час кліку за допомогою **30+** онлайн-джерел	Численні механізми виявлення та технологія контент-фільтрації забезпечують виявлення спаму та фішингових атак на рівні 99,98%. URL-адреси проходять перевірку репутації в момент натискання кнопки миші через 30 джерел, що дозволяє протистояти складній соціальній інженерії. Для посилення захисту також передбачені функції сканування та перезапису QR-кодів.
Витік даних Витік даних може призвести до ненавмисного розкриття особистої та захищеної корпоративної інформації.	Проактивне запобігання втраті даних зупиняє витік та підтримує **110+** типів файлів	Проактивний DLP захищає дані PHI та PII, виявляє неприйнятний контент та лексику, а також використовує OCR для автоматичного редагування конфіденційної інформації. Цей проактивний захід вкрай важливий для комплаєнсу та захисту від витоків даних.

Переваги:

MetaDefender для сервера електронної пошти Exchange

Зменште кількість людських помилок, виявляючи потенційні фішингові атаки на різних етапах.

Ефективно усувайте цілеспрямовані атаки нульового дня завдяки профілактиці, а не виявленню.

Скоротіть вікно вразливості (Window of Vulnerability, WoV) для шкідливих програм, ефективно запобігайте поширенню шкідливого ПЗ.

Захистіть робочі файли, видаливши з вкладення загрози на основі документів.

Підвищте ефективність виявлення шкідливих програм для забезпечення розширеного захисту електронної пошти від внутрішніх та зовнішніх загроз.

Виявляйте шкідливий вміст та невідомі загрози у вкладеннях у режимі реального часу.

Захистіть користувачів від атак соціальної інженерії, завдяки чому IT-відділ буде менше турбуватися через людський фактор.

Забезпечте відповідність вимогам PCI, іншим нормативним документам щодо електронної пошти, а також захист даних PII у компаніях.

Підвищте відсоток виявлення невідомих загроз завдяки унікальній технології динамічного аналізу

Зробіть наступний крок, щоб максимально підвищити безпеку Email Exchange Server

Підвищити безпеку

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT захищає критично важливу інфраструктуру (CIP). Наша мета — усунути шкідливе ПЗ та атаки нульового дня. Ми вважаємо, що кожен файл та кожен пристрій несуть загрозу. Загрози повинні бути усунені на всіх об'єктах у будь-який час — на вході, виході та в стані спокою. Наші продукти спрямовані на запобігання загрозам та створення процесів для безпечного передавання даних та захищеного доступу до пристроїв. У результаті ми створюємо продуктивні системи, що зводять до мінімуму ризик компрометації. Саме тому 98 % об'єктів атомної енергетики США довіряють OPSWAT забезпечення кібербезпеки та дотримання нормативних вимог

opswat.bakotech.com

opswat@bakotech.com