OPSWAT. | bako tech®

SOLUTION BRIEF

MetaDefender® ICAP Server and F5 NGINX

Захистіть сучасні програми від завантаження шкідливих файлів

MetaDefender ICAP Server легко інтегрується із NGINX за допомогою сертифікованого динамічного модуля. Спільне рішення захищає корпоративні мережі від шкідливого ПЗ, перевіряючи всі файли, що завантажуються, на наявність потенційних загроз.

Ризики та виклики

Сучасні хмарні та гібридні середовища дозволяють організаціям розгортати високопродуктивні та багатофункціональні програми у великому обсязі. Переваги цих технологій незаперечні, але з ними пов'язані й чимраз більші ризики безпеки, з якими стикаються організації.

Контейнеризовані хмарні системи, що дозволяють передавати файли, вразливі через завантаження шкідливих документів, вимагання, витоки даних та атаки на ланцюжки постачання, що завдає репутаційної шкоди й призводить до втрати доходів.

- Сучасні програми, розгорнуті в контейнерних середовищах, можуть бути вразливими до кібератак, таких як шкідливе ПЗ, DDoS або витік даних.
- Вразливість файлів — найпоширеніший вектор атак на вебзастосунки.
- Без очищення даних шкідливі файли можуть прослизнути через мережевий периметр організації у середовище.
- Чутливі та конфіденційні дані можуть бути вкрадені або ненавмисно передані за межі організації, що призводить до їх витоку та порушення нормативних вимог.

Зміцніть кібербезпеку шляхом розподілення відповідальності

Організації, що використовують NGINX Plus або NGINX Open Source, можуть впровадити MetaDefender ICAP Server, щоб додати ще один рівень захисту від загроз на додачу до наявної інфраструктури.

F5 NGINX — це хмарний зворотний проксі, балансувальник навантаження, вебсервер і платформа шлюзу API для швидкого доставлення застосунків.

OPSWAT MetaDefender ICAP Server легко інтегрується з NGINX для захисту контейнерних застосунків від шкідливих програм, що переносяться через файли, відомих і невідомих загроз, витоків конфіденційних даних і вразливостей файлів додатків.

ОРГАНІЗАЦІЯ/КЛІЄНТ

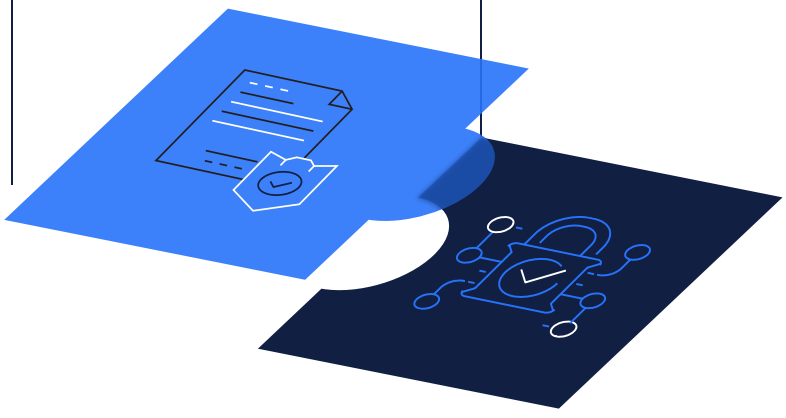
Відповідає за безпеку контенту

- Сканування контенту на наявність шкідливого ПЗ
- Захист даних клієнта
- Безпека збережених файлів
- Безпека завантаження файлів
- Відповідність нормативним вимогам

ВЕНДОР

Відповідальний за безпеку мережі

- Управління доступом до мережі
- Управління політиками безпеки
- Безпека зберігання даних
- Безпека контейнерів
- Дотримання нормативних вимог



OPSWAT.

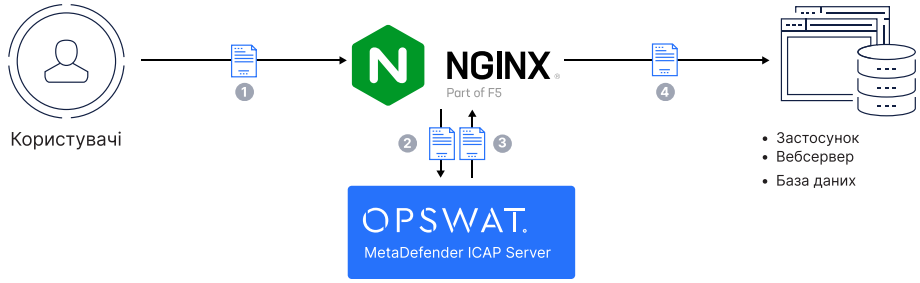
SOLUTION BRIEF

Ключові переваги

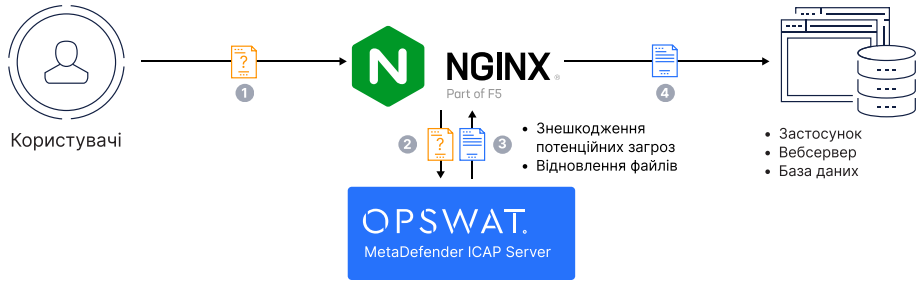
- Універсальний зворотний проксі-сервер, балансувальник навантаження, API-шлюз, вебсервер та кеш контенту
- Виявлення шкідливого ПЗ з ймовірністю майже 99% завдяки одночасному аналізу за допомогою 30+ антивірусних систем
- Усунення загроз «нульового дня» шляхом знешкодження всього потенційно шкідливого вмісту у вкладених архівах та інших комплексних файлах.
- Забезпечення відповідності нормативним вимогам та конфіденційності даних
- Сертифікований NGINX динамічний модуль, що легко інтегрується в наявний стек розгортання

Принципи роботи

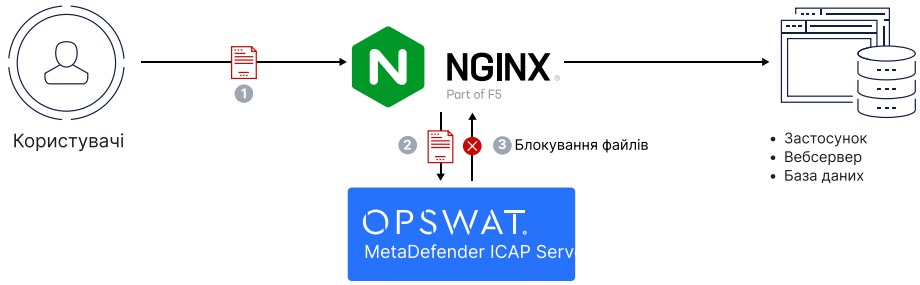
Дозволяє очищати файли



Очищує вміст файлів



Блокує шкідливі файли



Про MetaDefender ICAP Server and F5 NGINX

OPSWAT MetaDefender ICAP Server є багаторівневим і надійним рішенням для захисту корпоративних мереж від завантаження шкідливих файлів.

Рішення можна легко інтегрувати в будь-які мережеві пристрої, що підтримують ICAP-клієнт:

- Зворотний та прямий проксі
- Фаєрвол вебзастосунків (WAF)
- Фаєрвол нового покоління (NGFW)
- Балансувальник навантаження
- Безпечний вебшлюз (SWG)
- Кероване передавання файлів (MFT)
- Контролер доставки додатків (ADC)
- Контролер входу NGINX **

** Нативна інтеграція