OPSWAT. | bako tech®

MetaDefender® ICAP Server

Plug-and-Play захист від шкідливого ПЗ для платформ F5 BIG-IP і F5 Distributed Cloud (XC)

Хмарна трансформація стимулює впровадження вебзастосунків, які використовують завантаження файлів для широкого спектра завдань: передавання файлів B2B, обробка особистих даних клієнтів та інші функції, необхідні для підтримки безперервності бізнесу.

Однак ця функціональність також відкриває новий вектор загроз для програм-вимагачів та іншого шкідливого контенту у вашій організації.

OPSWAT та F5 об'єднали свої зусилля, щоб забезпечити потужні можливості захисту від шкідливого ПЗ для компаній по всьому світу. Аналізуйте, виявляйте та блокуйте шкідливі файли, перш ніж вони потраплять до вебдодатків. У такий спосіб ваша організація зможе зменшити кількість атак та захистити мережу. Співпраця F5 та OPSWAT спрямована на створення більш безпечного цифрового простору, де клієнти можуть бути впевненими у захищеності своїх даних.

Проблема

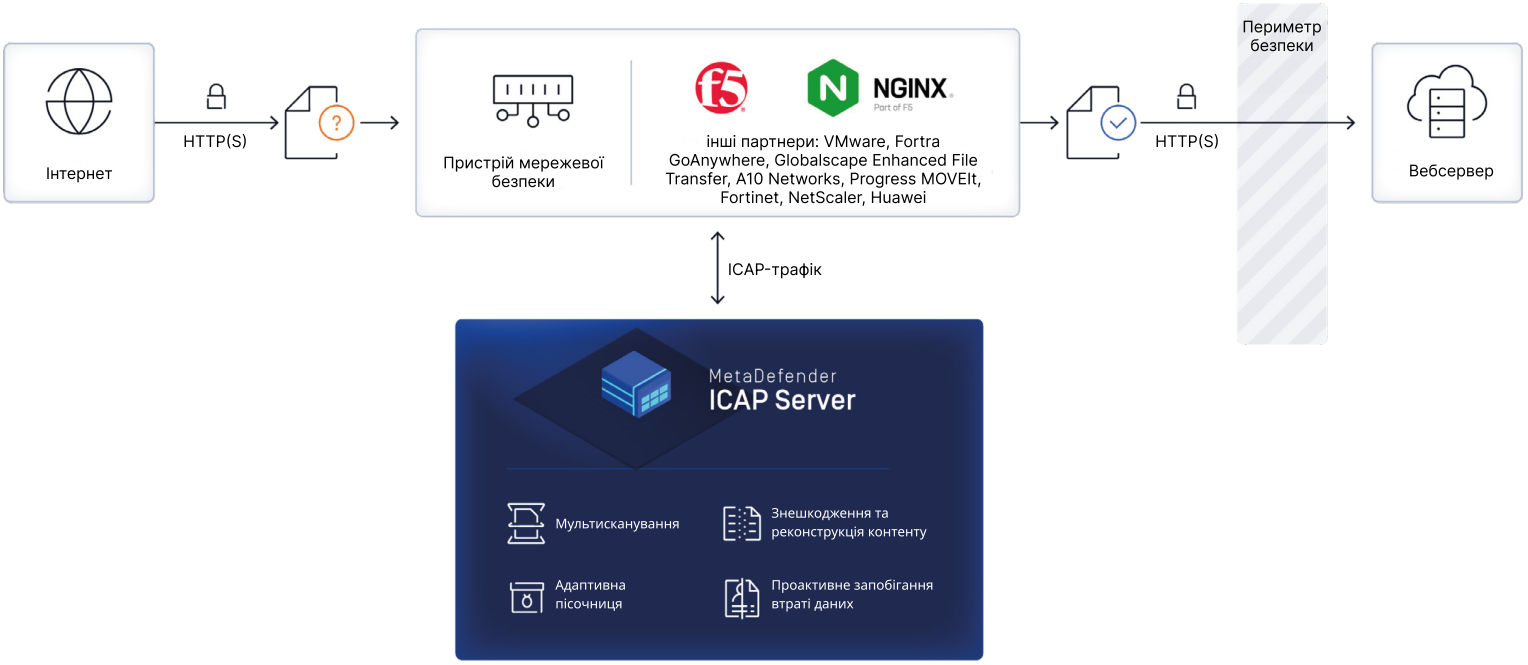
- Потреба в захисті файлів, які надходять у мережу, від шкідливого ПЗ, атак нульового дня, файлових вразливостей і витоку даних.
- Пристрої мережевої безпеки ефективно захищають середовище від мережевих атак. Однак вони не перевіряють вміст файлів, що передається через мережевий трафік.
- Середовища, що обробляють конфіденційні дані, потребують комплексного рішення для захисту вебзастосунків та хмарних сховищ від завантаження шкідливих файлів.
- Складна інтеграція, високі витрати на впровадження.

Рішення OPSWAT

Аналізуйте всі файли, що завантажуються, перш ніж вони потраплять у вашу мережу.

- **Мультисканування:** Збільште рівень виявлення загроз майже до 100% за допомогою 30+ антивірусних механізмів.
- **Deep CDR (знешкодження та реконструкція контенту):** Запобігайте атакам «нульового дня» та складним цільовим атакам.
- **Проактивна DLP (запобігання втраті даних):** Запобігайте витоку даних та дотримуйтесь нормативних вимог.
- **Пісочниця:** Технологія адаптивного аналізу загроз дозволяє виявляти шкідливе програмне забезпечення нульового дня і вилучати індикатори компрометації (IOC).
- **SBOM (Специфікація програмного забезпечення):** Виявляйте відомі вразливості, перевіряйте ліцензії та створюйте інвентаризацію компонентів для програмного забезпечення з відкритим вихідним кодом (OSS), сторонніх залежностей та контейнерів.
- **Оцінка вразливості:** Виявляйте вразливості додатків та файлів до їхнього встановлення.
- **Готове до використання:** Інтеграція в наявну інфраструктуру через ICAP займає менше п’яти хвилин без будь-яких змін архітектури.

OPSWAT. | bako tech®



Мережеві пристрої, що підтримуються

Безшовна інтеграція у наявну інфраструктуру

Зворотні та прямі проксі	Фаєрвол вебзастосунків (WAF)	Фаєрвол нового покоління (NGFW)
Балансувальник навантаження	Безпечний вебшлюз (SWG)	Контролер доставлення додатків (ADC)
Кероване передавання файлів (MFT)	Контролер входу	Корпоративне сховище

«Ми використовували технологію OPSWAT протягом кількох років у численних інтеграціях та різних продуктах, [і] їх репутація в галузі за цей час злетіла до небес. Я пропрацював у сфері 30 років, і OPSWAT — це компанія, якій я завжди довіряв і з якою продуктивно співпрацював».

Джо Пек
Старший директор
з управління продуктами F5®

opswat@bakotech.com