OPSWAT. | bako tech®

MetaDefender® ICAP Server

Plug-and-Play защита от вредоносного ПО для платформ F5 BIG-IP и F5 Distributed Cloud (XC)

Облачная трансформация стимулирует внедрение веб-приложений, которые используют загрузку файлов для широкого спектра задач: передача файлов B2B, обработка личных данных клиентов и другие функции, необходимые для поддержания непрерывности бизнеса.

Однако эта функциональность также открывает новый вектор угроз для программ-вымогателей и другого вредоносного контента в вашей организации.

OPSWAT и F5 объединили свои усилия, чтобы предоставить мощные возможности защиты от вредоносного ПО для компаний по всему миру. Анализируйте, обнаруживайте и блокируйте вредоносные файлы до того, как они попадут в веб-приложения. Таким образом ваша организация сможет сократить количество атак и защитить сеть. Сотрудничество F5 и OPSWAT направлено на создание более безопасного цифрового пространства, где клиенты могут быть уверены в защищенности своих данных.

Проблема

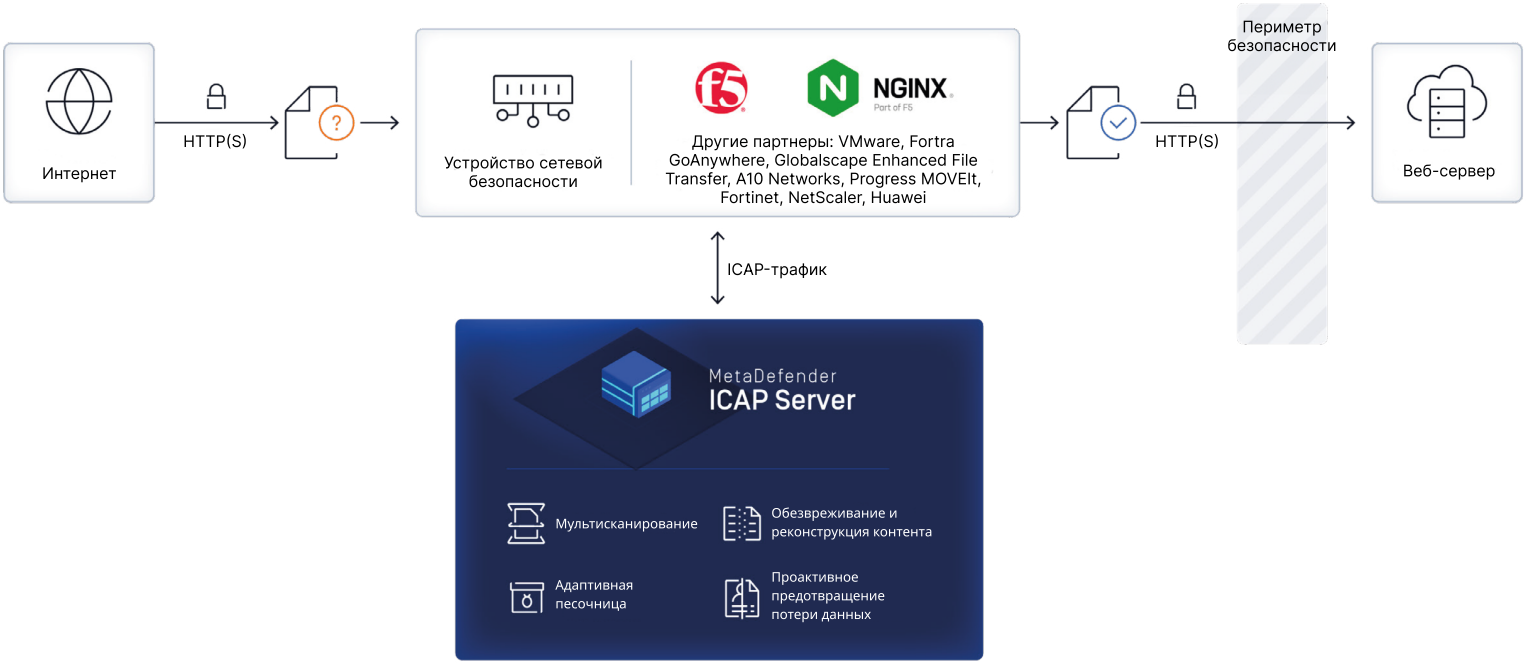
- Потребность в защите файлов, поступающих в сеть, от вредоносного ПО, атак нулевого дня, файловых уязвимостей и утечки данных.
- Устройства сетевой безопасности эффективно защищают среду от сетевых атак. Однако они не проверяют содержимое файлов, передаваемое через сетевой трафик.
- Средам, обрабатывающим конфиденциальные данные, требуется комплексное решение для защиты веб-приложений и облачных хранилищ от загрузки вредоносных файлов.
- Сложная интеграция, высокие затраты на внедрение.

Решение OPSWAT

Анализируйте все загружаемые файлы до того, как они попадут в вашу сеть.

- **Мультисканирование:** Увеличьте уровень обнаружения угроз почти до 100 % с помощью 30+ антивирусных механизмов.
- **Deep CDR (обезвреживание и реконструкция контента):** Предотвращайте атаки «нулевого дня» и сложные целевые атаки.
- **Проактивное DLP (предотвращение потери данных):** Предотвращайте утечку данных и соблюдайте нормативные требования.
- **Песочница:** Технология адаптивного анализа угроз позволяет обнаруживать вредоносное ПО нулевого дня и извлекать индикаторы компрометации (IOC).
- **SBOM (Спецификация программного обеспечения):** Выявляйте известные уязвимости, проверяйте лицензии и создавайте инвентаризацию компонентов для программного обеспечения с открытым исходным кодом (OSS), сторонних зависимостей и контейнеров.
- **Оценка уязвимости:** Обнаруживайте уязвимости приложений и файлов до их установки.
- **Готово к использованию:** Интеграция в существующую инфраструктуру через ICAP занимает менее пяти минут без каких-либо изменений архитектуры.

OPSWAT. | bako tech®



Поддерживаемые сетевые устройства

Бесшовная интеграция в существующую инфраструктуру

Обратные и прямые прокси	Файрвол веб-приложений (WAF)	Файрвол нового поколения (NGFW)
Балансировщик нагрузки	Безопасный веб-шлюз (SWG)	Контроллер доставки приложений (ADC)
Управляемая передача файлов (MFT)	Контроллер входа	Корпоративное хранилище

«Мы использовали технологию OPSWAT в течение нескольких лет в многочисленных интеграциях и в различных продуктах, [и] их репутация в отрасли за это время взлетела до небес. Я проработал в сфере 30 лет, и OPSWAT — это компания, которой я всегда доверял и с которой я продуктивно сотрудничал»

Джо Пек
Старший директор по управлению продуктами F5®

OPSWAT. | bako tech®

opswat@bakotech.com