OPSWAT. | bako tech®

SOLUTION BRIEF

MetaDefender® ICAP Server and F5 NGINX

Защитите современные приложения от загрузки вредоносных файлов

MetaDefender ICAP Server легко интегрируется с NGINX с помощью сертифицированного динамического модуля. Совместное решение защищает корпоративные сети от вредоносного ПО, проверяя все загружаемые входящие файлы на наличие потенциальных угроз.

Риски и вызовы

Современные облачные и гибридные среды позволяют организациям разворачивать высокопроизводительные и многофункциональные приложения в большом объеме. Преимущества этих технологий неоспоримы, но с ними связаны и возрастающие риски безопасности, с которыми сталкиваются организации.

Контейнеризированные облачные системы, позволяющие передавать файлы, подвержены загрузке вредоносных документов, вымогательству, утечке данных и атакам на цепочки поставок, что наносит репутационный ущерб и приводит к потере доходов.

- Современные приложения, развернутые в контейнерных средах, могут быть уязвимы к кибератакам, таким как вредоносное ПО, DDoS или утечка данных.
- Уязвимости файлов — распространенный вектор атак на веб-приложения.
- Без очистки данных вредоносные файлы могут проскользнуть через сетевой периметр организации в ее среду.
- Чувствительные и конфиденциальные данные могут быть украдены или непреднамеренно переданы за пределы организации, что приводит к их утечке и нарушению нормативных требований.

Усильте кибербезопасность за счет разделения ответственности

Организации, использующие NGINX Plus или NGINX Open Source, могут внедрить MetaDefender ICAP Server, чтобы добавить дополнительный уровень защиты от угроз поверх существующей инфраструктуры.

F5 NGINX представляет собой облачный обратный прокси, балансировщик нагрузки, веб-сервер и платформу шлюза API для быстрой доставки приложений.

OPSWAT MetaDefender ICAP Server легко интегрируется с NGINX для защиты контейнерных приложений от переносимых через файлы вредоносных программ, известных и неизвестных угроз, утечек конфиденциальных данных и уязвимостей файлов приложений.

ОРГАНИЗАЦИЯ/КЛИЕНТ

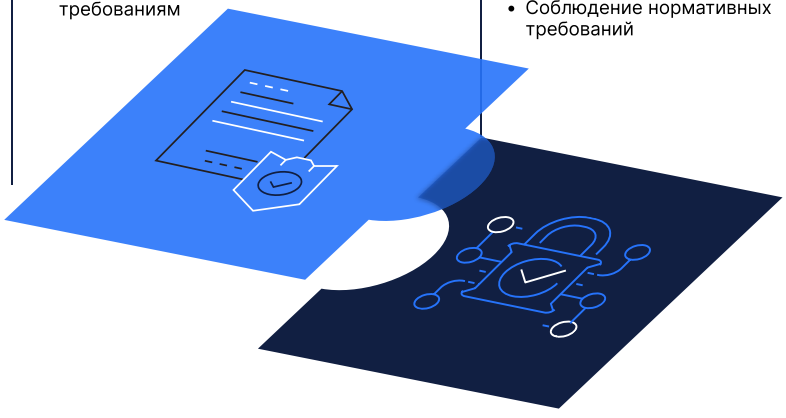
Отвечает за безопасность контента

- Сканирование контента на наличие вредоносного ПО
- Защита данных клиента
- Безопасность хранимых файлов
- Безопасность загрузки файлов
- Соответствие нормативным требованиям

ВЕНДОР

Ответственный за безопасность сети

- Управление доступом к сети
- Управление политиками безопасности
- Безопасность хранения данных
- Безопасность контейнеров
- Соблюдение нормативных требований



OPSWAT.

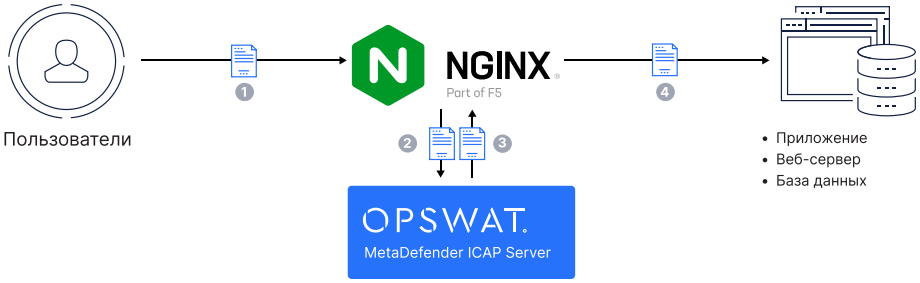
SOLUTION BRIEF

Ключевые преимущества

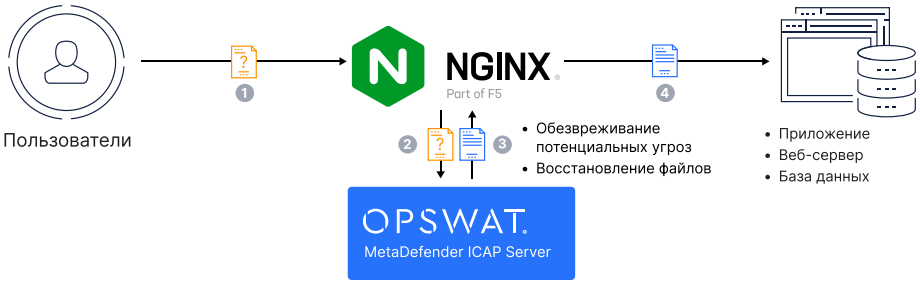
- Универсальный обратный прокси-сервер, балансировщик нагрузки, API-шлюз, веб-сервер и кэш контента
- Обнаружение вредоносного ПО с вероятностью почти 99% благодаря одновременному анализу с помощью 30+ антивирусных систем
- Устранение угроз «нулевого дня» путем обезвреживания всего потенциально вредоносного содержимого во вложенных архивах и других комплексных файлах.
- Обеспечение соответствия нормативным требованиям и конфиденциальности данных
- Сертифицированный NGINX динамический модуль, легко интегрирующийся в существующий стек развертывания

Принципы работы

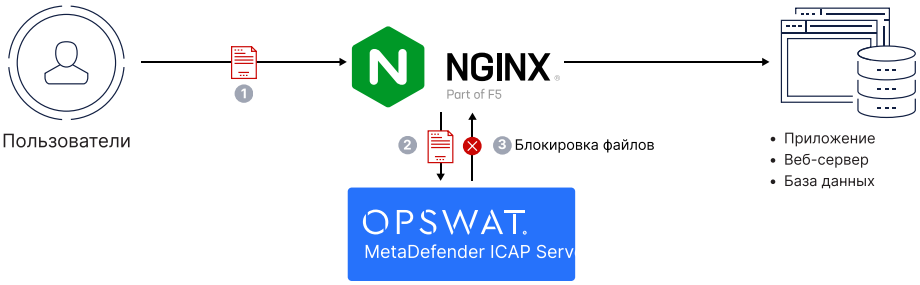
Позволяет очищать файлы



Очищает содержимое файлов



Блокирует вредоносные файлы



О MetaDefender ICAP Server

OPSWAT MetaDefender ICAP Server представляет собой многоуровневое и надежное решение для защиты корпоративных сетей от загрузки вредоносных файлов.

Решение можно легко интегрировать в любые сетевые устройства, поддерживающие ICAP-клиент:

- Обратный и прямой прокси
- Файрвол веб-приложений (WAF)
- Файрвол нового поколения (NGFW)
- Балансировщик нагрузки
- Безопасный веб-шлюз (SWG)
- Управляемая передача файлов (MFT)
- Контроллер доставки приложений (ADC)
- NGINX Ingress Controller **

** Нативная интеграция