OPSWAT.
Protecting the World's Critical Infrastructure

MetaDefender для Email Exchange Server

Улучшенная защита электронной почты от угроз, которые обходят встроенные средства безопасности

Электронная почта по-прежнему остается главным вектором угроз кибербезопасности. Согласно отчету CISA Analysis, 87% фишинговых атак обходят обычную защиту почты.

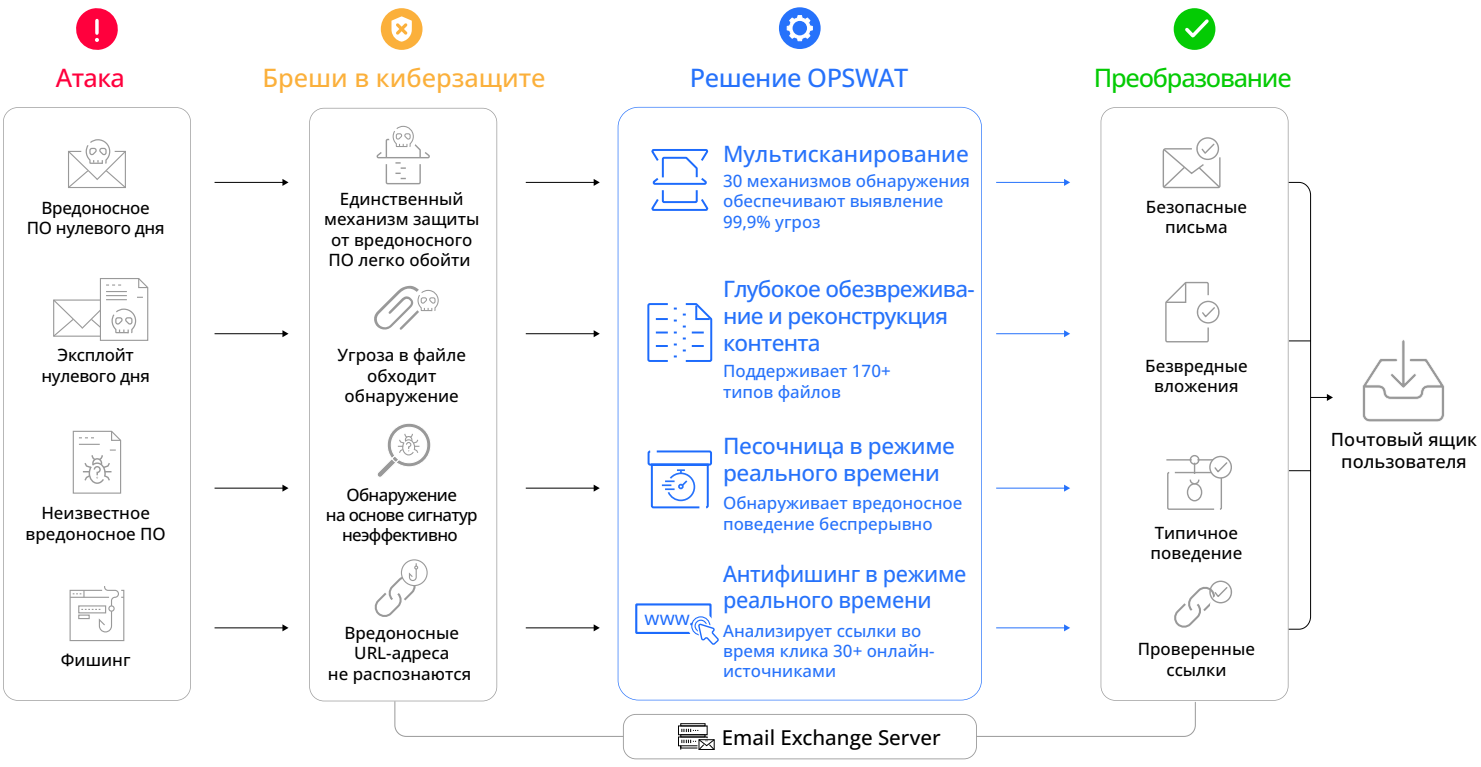
Чтобы противостоять этим угрозам, OPSWAT создал MetaDefender для Email Exchange Server. Он предоставляет уникальный функционал для борьбы с современными угрозами.

Благодаря интеграции мультисканирования, глубокого обезвреживания и реконструкции контента (CDR), а также антифишинга в режиме реального времени MetaDefender максимально точно обнаруживает неизвестные угрозы нулевого дня, вредоносные программы, фишинг и эксплойты.

Адаптивная песочница в режиме реального времени нейтрализует угрозы до того, как они попадут к пользователю, а проактивное предотвращение потери данных дополняет основные технологии защиты и обеспечивает безопасность конфиденциальных данных.

Вызовы

- Вектор угроз кибербезопасности №1 — электронная почта, по ней распространяется 92 % вредоносных программ
- Обнаружение неизвестных вредоносных программ занимает в среднем 49 дней, что увеличивает срок действия угрозы
- Появляется 109 млн новых вредоносных программ в год
- Самые популярные вложения, содержащие угрозы, — обычные документы Office
- Средняя стоимость одной утечки данных в 2023 году составила $4,45M (IBM Research)
- В 2023 году было обнаружено 26 447 уязвимостей



Бреши Email Exchange Server	OPSWAT. MetaDefender для Email Exchange Server	
Вредоносные программы нулевого дня Проблема атак вредоносного ПО нулевого дня связана с ограничениями отдельных антивирусных систем, разрозненным временем отклика разных вендоров и возникновением ложных срабатываний.	Мультисканирование обнаруживает **99.20 %** из 10 000 самых опасных угроз	Мультисканирование объединяет до 30 механизмов обнаружения, усиленных эвристикой и машинным обучением. Такой подход значительно повышает эффективность обнаружения угроз.
Эксплойты нулевого дня Неизвестные эксплойты и эксплойты нулевого дня являются значительным риском, поскольку они могут обойти встроенные меры безопасности, которые не обнаруживают угрозы во вложениях.	Deep CDR выявляет, обезвреживает и нейтрализует угрозы в **170+** типах файлов	Глубокое обезвреживание и реконструкция контента (Deep CDR) позволяет обнаружить и нейтрализовать сложные для выявления угрозы, восстановить все содержимое файлов, провести глубокую очистку изображений и предотвратить шифрование.
Неизвестное вредоносное ПО Неизвестные вредоносные программы обходят сигнатурное обнаружение и остаются угрозой при автономном анализе традиционными песочницами.	Песочница обнаруживает вредоносные объекты в 10 раз быстрее **в режиме реального времени**	Адаптивная песочница в режиме реального времени динамически обнаруживает вредоносное поведение, обеспечивает быстрый и глубокий анализ угроз и фокусируется на обнаружении целевых атак и извлечении IOC. Защита осуществляется до того, как электронное письмо будет получено пользователем.
Фишинг и сбор учетных данных Социальная инженерия и фишинговые атаки часто ускользают от традиционных средств защиты, используя тактику скрытия URL-адресов и тайного сбора учетных данных.	Антифишинг в режиме реального времени анализирует ссылки во время клика с помощью **30+** онлайн-источников	Многочисленные механизмы обнаружения и технология контент-фильтрации обеспечивают обнаружение спама и фишинговых атак на уровне 99,98%. URL-адреса проходят проверку репутации в момент нажатия кнопки мыши через 30+ источников, что позволяет противостоять сложной социальной инженерии. Для усиления защиты также предусмотрены функции сканирования и перезаписи QR-кодов.
Утечка данных Утечка данных может привести к непреднамеренному раскрытию личной и защищенной корпоративной информации.	Проактивное предотвращение потери данных останавливает утечку и поддерживает **110+** типов файлов	Проактивный DLP защищает данные PHI и PII, обнаруживает неприемлемый контент и лексику, а также использует OCR для автоматического редактирования конфиденциальной информации. Эта проактивная мера крайне важна для комплаенса и защиты от утечек данных.

Преимущества:

MetaDefender для Email Exchange Server

Сократите количество человеческих ошибок, выявляя потенциальные фишинговые атаки на разных этапах.

Эффективно устраняйте целенаправленные атаки нулевого дня благодаря профилактике, а не обнаружению.

Сократите окно уязвимости (Window of Vulnerability, WoV) для вредоносных программ, эффективно предотвращайте распространение вредоносного ПО.

Защитите рабочие файлы, удалив из вложений угрозы на основе документов.

Повысьте эффективность обнаружения вредоносных программ для обеспечения расширенной защиты электронной почты от внутренних и внешних угроз.

Выявляйте вредоносное содержимое и неизвестные угрозы во вложениях в режиме реального времени.

Защитите пользователей от атак социальной инженерии, благодаря чему IT-отдел будет меньше переживать из-за человеческого фактора.

Обеспечьте соответствие требованиям PCI, другим нормативным документам касательно электронной почты, а также защиту данных PII в компаниях.

Повысьте процент обнаружения неизвестных угроз благодаря уникальной технологии динамического анализа.

Сделайте следующий шаг, чтобы максимально повысить безопасность Email Exchange Server

Повысить безопасность

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT защищает критически важную инфраструктуру (CIP). Наша цель — устранить вредоносное ПО и атаки нулевого дня. Мы считаем, что каждый файл и каждое устройство несут угрозу. Угрозы должны быть устранены на всех объектах в любое время — на входе, выходе и в состоянии покоя. Наши продукты направлены на предотвращение угроз и создание процессов для безопасной передачи данных и защищенного доступа к устройствам. В результате мы создаем продуктивные системы, которые сводят к минимуму риск компрометации. Именно поэтому 98% объектов атомной энергетики США доверяют OPSWAT обеспечение кибербезопасности и соблюдение нормативных требований

opswat.bakotech.com

opswat@bakotech.com