Barracuda
Your journey, secured.

Barracuda Email Protection

Полная безопасность для Microsoft Office 365

Barracuda Email Protection – это комплексное, простое в использовании решение для организаций, желающих защитить свой бизнес, бренд и сотрудников от самых продвинутых угроз, связанных с электронной почтой. Это решение обеспечивает защиту шлюза, защиту входящей почты на основе API, реагирование на инциденты, защиту данных и возможности по соблюдению нормативных требований.

Блокируйте спам, вредоносные программы и угрозы нулевого дня

В решении Barracuda используются продвинутые технологии для обнаружения известных разновидностей спама и вредоносных программ. Кроме того, оно обеспечивает бесперебойную работу электронной почты наряду с фильтрацией и шифрованием исходящего трафика, тем самым предотвращая потерю данных. Механизм встроенной защиты от сложных угроз обнаруживает вредоносные программы нулевого дня с помощью анализа полезной нагрузки и «работы в песочнице». Защита ссылок обеспечивает переадресацию подозрительных и поддельных URL-адресов, а механизм фильтрации по DNS блокирует доступ к вредоносным веб-доменам, не позволяя получателям почты случайно загрузить вредоносную программу.

Защититесь от целевого фишинга в реальном времени

Система Barracuda имеет уникальную архитектуру, построенную на основе API, благодаря которой ее движок искусственного интеллекта способен изучать электронную почту за прошлые периоды и запоминать уникальные шаблоны общения пользователей. Это позволяет ему обнаруживать аномалии в метаданных и содержимом сообщений, а также находить и блокировать в реальном времени атаки, построенные на основе социальной инженерии.

Защитите свою организацию от угона учетных записей.

Система Barracuda останавливает фишинговые атаки, используемые хакерами с целью сбора идентификационных данных, которые затем применяются для угона учетных записей. Она обнаруживает аномальное поведение электронной почты и оповещает лиц, ответственных за информационные технологии, после чего находит и удаляет все мошеннические электронные письма, отправленные из скомпрометированных учетных записей.

Реагируйте на угрозы, связанные с электронной почтой, уже после ввода продукта в эксплуатацию.

Система позволяет обнаруживать потенциальные угрозы уже после ввода продукта в эксплуатацию на основе выводов, полученных в результате анализа ранее доставленной электронной посты, и данных разведки угроз, предоставляемых сообществом. Экономьте ИТ-ресурсы благодаря автоматическому удалению вредоносных сообщений и автоматическим сценариям реагирования. Опередите киберпреступников и блокируйте предстоящие атаки путем непрерывного устранения уязвимостей.

Научите пользователей обнаруживать новейшие угрозы

Научите своих пользователей распознавать новейшие технологии фишинга и препятствовать распространению атак по вашей организации. Вы получите доступ к увлекательным обучающим материалам и имитациям фишинговых атак, созданным на основе реальных угроз.

Защитите свои данные и обеспечьте соответствие требованиям.

Резервируйте в облаке данные Microsoft Office 365, включая почтовые ящики Exchange Online, SharePoint Online, OneDrive for Business и Teams. В случае случайного или злонамеренного удаления данных вы сможете быстро выполнить их восстановление на определенный момент времени (восстановление типа point-in-time). Механизм архивирования в облаке поможет вам соблюсти требования по соответствию с помощью возможностей предоставления электронных документов, детально конфигурируемых политик хранения данных и хранилища данных, объем которого не ограничен.

Защитите себя от латеральных атак.

Цифровая трансформация в облако, особенно в Microsoft 365, ускорилась за последние несколько лет. Это связано с ростом числа удаленных сотрудников, удаленных подрядчиков и политик BYOD. В результате возникает новая поверхность атаки, когда скомпрометированная учетная запись подвергает весь набор средств совместной работы угрозе латеральных атак. Barracuda объединяет защиту электронной почты с Zero Trust Access, что позволяет постоянно проверять личность и доверие к сотрудникам и устройствам.

Основные функциональные возможности

Защита от фишинга и маскировки под законного пользователя

- Возможность непосредственного подключения к Microsoft 365
- Быстрая, простая установка (менее чем за 5 минут)
- Блокирует целевые фишинговые атаки, компрометацию корпоративной электронной почты (BEC), вымогательство и другие атаки, построенные на основе социальной инженерии
- Искусственный интеллект для обнаружения и блокировки атак в реальном времени
- Обнаруживает попытки угона учетной записи и оповещает о них
- Уведомляет внешних пользователей и удаляет скомпрометированную электронную почту
- Блокирует доступ взломщиков к скомпрометированной учетной записи
- Делает видимыми изменения в правилах, которые применяются к входящей почте, и подозрительные входы в систему
- Аналитика и отчетность об угрожающей среде

Реагирование на инциденты

- Надстройка для Outlook и отчетность об угрозе одним нажатием кнопки
- Оповещения о нарушениях безопасности
- Данные географического анализа
- Данные об угрозах, предоставляемые сообществом
- Данные о получателе и поведении
- Удаляет электронные письма из почтовых ящиков пользователей
- Внедряет политики касательно входящей электронной почты
- Блокирует доступ к вредоносному веб-контенту
- Автоматическое устранение вредоносного контента
- Непрерывное устранение нарушений
- Автоматизированный построитель рабочих процессов
- Интеграция API для платформ SOAR/SIEM/XDR

Межоблачное резервирование

- Резервирование и восстановление для Microsoft 365: Exchange Online, SharePoint Online, OneDrive и Teams for Business.
- Выборочное планирование и восстановление
- Автоматизированное или ручное резервирование
- Восстановление с выбором нескольких элементов
- Выборочное восстановление элементов SharePoint
- Восстановление в системе Exchange Online или OneDrive for Business либо локальная загрузка файлов

Защита шлюза электронной почты

- Облачная защита от спама, вредоносных программ, вирусов, фишинга и других угроз, связанных с электронной почтой
- Продвинутая защита от угроз с использованием эмуляционной песочницы, охватывающей всю систему
- Шифрование электронной почты и предотвращение потери данных без использования агента
- Защита ссылок и защита от подделки адресов
- Непрерывность работы электронной почты с отказоустойчивостью при переходе на облачный почтовый сервис
- Аварийный почтовый ящик для отправки, получения, чтения и ответа на электронную почту

Архивирование в облаке

- Архивирование непосредственно из Microsoft 365 в облачный архив
- Управление файлом личных папок PST для старых версий почтового клиента
- Детально конфигурируемые политики хранения данных
- Полнотекстовый поиск с несколькими операторами

Обучение мерам безопасности

- Моделирование угроз для электронной почты, SMS, голоса и физических носителей
- Шаблоны реальных угроз
- Обучение на тему безопасности и обучающие микро-видео
- Тесты и упражнения по оценке рисков
- Более 16 000 собранных точек данных
- Подробный анализ тенденций
- Настраиваемые отчеты и панели инструментов

Защита домена от мошенничества

- Аутентификация, отчетность и анализ по технологии DMARC
- Предотвращение подделки домена и угона бренда

Безопасность в Интернете

- Защита от веб-угроз
- Фильтрация веб-контента
- Журналы фильтрации веб-сайтов по содержимому
- Административные отчеты
- Автоматические оповещения

Инспектор данных

- Сканирование OneDrive и SharePoint на наличие конфиденциальной информации и вредоносных файлов
- Идентификация вредоносных файлов
- Настройки классификации данных
- Автоматизированные уведомления по электронной почте для администраторов, специалистов по обеспечению соответствия требованиям и пользователей
- Контроль доступа на основе ролей
- Расширенные возможности шифрования

Доступ к сети с нулевым доверием

- Защита от фишинга и блокирование угроз на уровне устройств
- Механизм политики управления доступом на основе ролей и атрибутов
- Оптимизированная инициализация
- Реализация глобальной политики
- Соответствие требованиям

Защита электронной почты Barracuda Email Protection доступна в виде трех планов. Выберите план, который вам подходит.

ВОЗМОЖНОСТИ	ADVANCED	PREMIUM	PREMIUM PLUS
Защита от спама и вредоносных программ	✓	✓	✓
Защита вложений	✓	✓	✓
Защита ссылок	✓	✓	✓
Бесперебойная работа электронной почты	✓	✓	✓
Шифрование электронной почты	✓	✓	✓
Предотвращение утечки данных	✓	✓	✓
Защита от фишинга и маскировки под законного пользователя	✓	✓	✓
Защита от угона учетной записи	✓	✓	✓
Автоматическое устранение уязвимостей	✓	✓	✓
Защита домена от мошенничества		✓	✓
Безопасность в Интернете		✓	✓
Активный поиск и реагирование на угрозы		✓	✓
Автоматизированные рабочие процессы		✓	✓
Интеграция SIEM/SOAR/XDR		✓	✓
Архивирование в облаке			✓
Межоблачное резервирование			✓
Инспектор данных			✓
Имитация атак			✓
Обучение мерам безопасности			✓
Доступ с нулевым доверием к Microsoft 365			✓

Barracuda®
Your journey, secured.