CLOUDFLARE

ОБЗОР ПРОДУКТА

Защита электронной почты от Cloudflare

Обеспечение автономной многоканальной защиты для безопасной коммуникации в рабочей среде

Обеспечьте защиту от целевых фишинговых атак

С легкостью блокируйте и изолируйте угрозы, которые пропускаются другими решениями

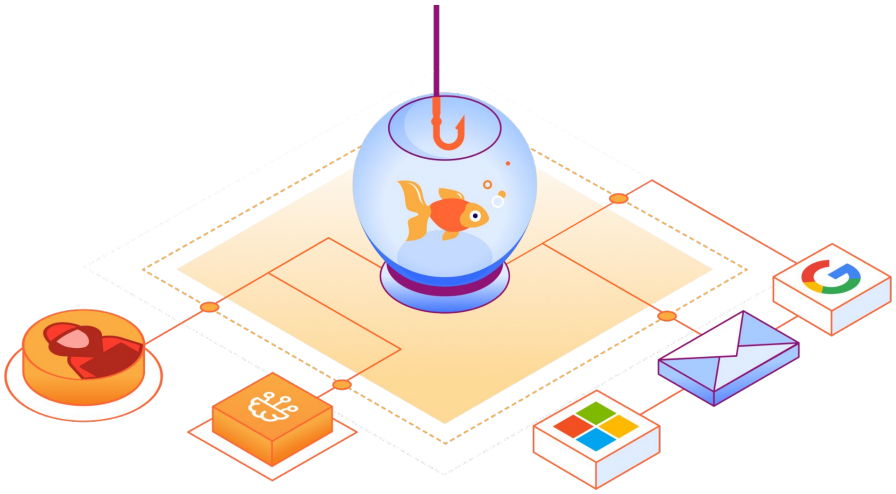
Поскольку электронная почта является самым распространенным и самым используемым бизнес-приложением, как никогда важно защитить пользователей от фишинговых атак, направленных на манипулирование их доверием. По мере того как организации продолжают все чаще внедрять облачные службы эл. почты через Microsoft 365 и Google Workspace для обеспечения эффективной поддержки сотрудников, работающих в гибридном формате, злоумышленники переключились на более целевые, небольшие по объему атаки, которые способны обойти традиционные безопасные шлюзы электронной почты (SEG), такие как Proofpoint и Mimecast.

Именно поэтому облачно-ориентированное решение для обеспечения безопасности электронной почты Cloudflare было специально разработано для реализации превентивного сбора и проверки информации о кампаниях, анализа контента на основе машинного обучения с использованием унифицированной платформы Zero Trust для предотвращения фишинговых угроз до того, как они достигнут ваших сотрудников.

91 %
всех кибератак начинается с фишингового электронного письма[1]

50 млрд
потерь от BEC-атак за последнее десятилетие[2]

81 %
организаций подверглось комбинированным атакам за последние 12 месяцев[3]



Предотвратите компрометацию корпоративной электронной почты (BEC)

Обнаруживайте подмениваемые и скомпрометированные учетные записи с помощью многоуровневого контекстного анализа на основе машинного обучения.

Изолируйте отложенные и комбинированные атаки

Защитите пользователей от вредоносного веб-контента, который доставляется через неизвестные и фальсифицированные ссылки.

Блокируйте программы-шантажисты и вредоносные приложения

Предотвратите попытки вымогательства и внедрения вредоносных кодов, представляющих угрозу для вашей организации.

Повышенная защита и простота

Внедрите многоуровневую защиту, которая обеспечивает более высокую степень защиты при меньших затратах

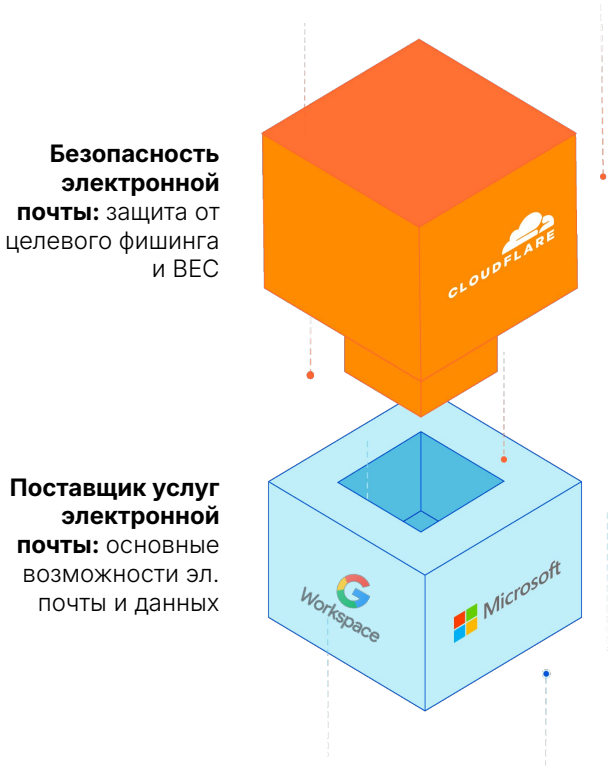
Поскольку фишинговые атаки распространяются все так же активно, Microsoft и Google продолжают создавать собственные функции, которые обеспечивают основные возможности защиты электронной почты и данных, такие как аутентификация, архивирование и шифрование на стороне клиента. Однако злоумышленники усовершенствовали свою тактику для проведения более целенаправленных и трудноуловимых атак, которые часто обходят встроенные средства безопасности и обеспечивают более высокий уровень успеха.

Используя Cloudflare, организации могут автоматически блокировать или изолировать целевые фишинговые атаки, которые используют вредоносные ссылки, вложения и скомпрометированные учетные записи для кражи конфиденциальной информации и финансового мошенничества.

Дополните существующие средства контроля безопасности сообщений электронной почты

Облачно-ориентированное решение по защите электронной почты от Cloudflare можно развернуть за считанные минуты, чтобы улучшить существующие развертывания SEG или дополнить встроенные возможности электронной почты, предоставляемые Microsoft и Google. За счет использования решения, практически не требующего настройки, организации могут добиться более эффективной защиты от фишинга, тратя меньше времени и усилий на постоянное управление средствами безопасности.

> «После внедрения Cloudflare [поверх M365] мы фиксируем на 50 % меньше вредоносных или подозрительных электронных писем, которые наши пользователи получают каждый день. Это высвобождает несколько часов, которые мы можем потратить на решение других задач».
>
> **Werner Enterprises**
> (Fortune 1000)



Реинвестируйте часы, сэкономленные за счет повышения автоматизации

Автоматизированное легкое решение Cloudflare обеспечивает бесшовную интеграцию с рабочими процессами Microsoft и Google, а также предлагает единый интуитивно понятный пользовательский интерфейс, упрощающий работу аналитиков.

Достигайте эффективность обнаружения 99,997 %

Сочетание собственных возможностей поставщика электронной почты с разработанными Cloudflare средствами защиты от фишинга и компрометации корпоративной электронной почты (BEC) гарантирует организациям полный охват с минимальным риском.

Получите больше результатов с меньшими затратами

Замена устаревших, дорогих и сложных развертываний на автоматизированное решение Cloudflare может снизить эксплуатационные расходы, избыточные функции и чрезмерную настройку.

Остановите изощренные BEC-атаки

Заявленные убытки составляют 50 млрд долл., и их рост продолжается

Учитывая, что за последнее десятилетие BEC-атаки привели к ошеломляющим потерям, удивительно, что некоторые организации до сих пор не уделяют приоритетного внимания борьбе со столь эффективной формой финансового мошенничества. Хотя BEC-атаки составляют гораздо меньший процент фишинговых угроз, они часто остаются незамеченными для SEG и поставщиков облачных почтовых сервисов, что приводит к большим финансовым потерям. Такие целевые атаки трудно обнаружить, поскольку они используют поддельные или скомпрометированные учетные записи и контекст бесед для маскировки под сотрудника или проверенного поставщика.

Распространение принципов Zero Trust на электронную почту

Используя скомпрометированную учетную запись электронной почты сотрудника или поставщика, злоумышленники могут обходить традиционные средства безопасности, которые лишь пытаются подтвердить легитимность учетной записи отправителя. Cloudflare делает еще один шаг вперед, анализируя широкий спектр поведенческих атрибутов, паттернов написания, индикаторов тональности и истории бесед, чтобы определить подлинность отправителя. Модели угроз Cloudflare на основе машинного обучения и обширный сбор и анализ сетевой информации обеспечивают наиболее эффективное оружие против скомпрометированных учетных записей, которые используются для получения мошеннических платежей.

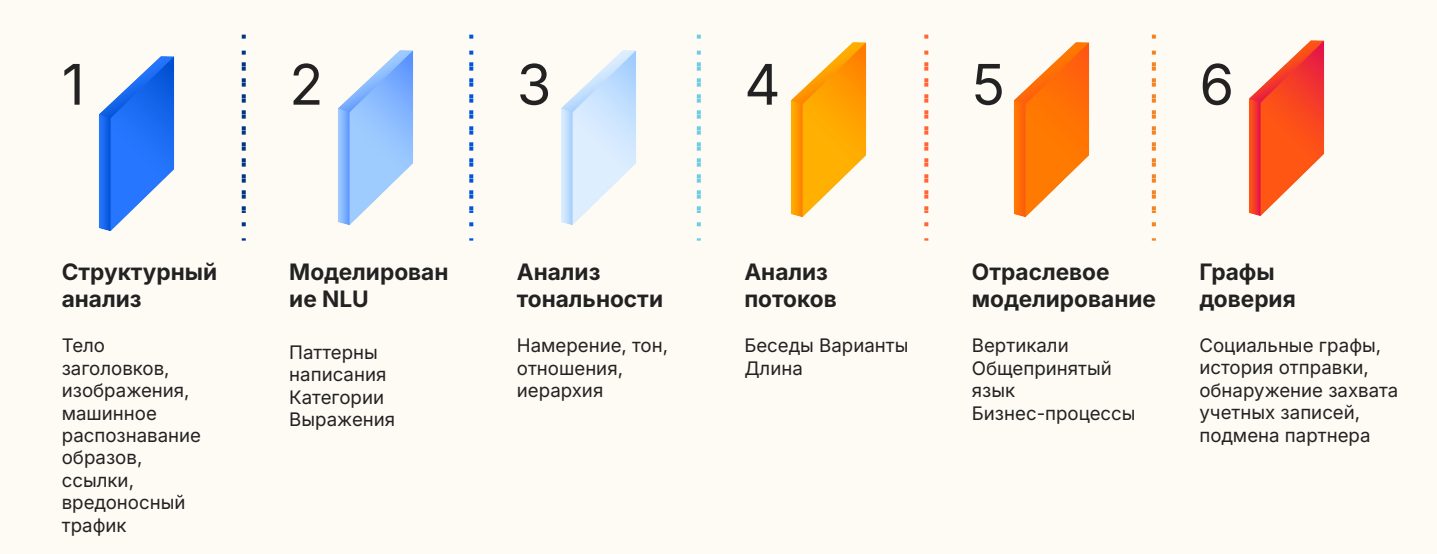


Рис. 1. Анализ сообщения

Обнаружение BEC с помощью контекстного анализа на основе машинного обучения

Точная идентификация BEC-атак требует большего, чем просто структурный анализ сообщения. Успешное обнаружение также предполагает детальное понимание различий в стиле и намерениях бесед. Обширная сетевая телеметрия Cloudflare (более 1 трлн DNS-запросов в день) и развивающиеся модели машинного обучения обеспечивают работу механизма аналитики мелких паттернов, который детально анализирует каждый аспект сообщения электронной почты для оценки моделей написания, тональности, исторического контекста и широкого спектра других переменных, которые помогают раскрыть подлинность отправителя.

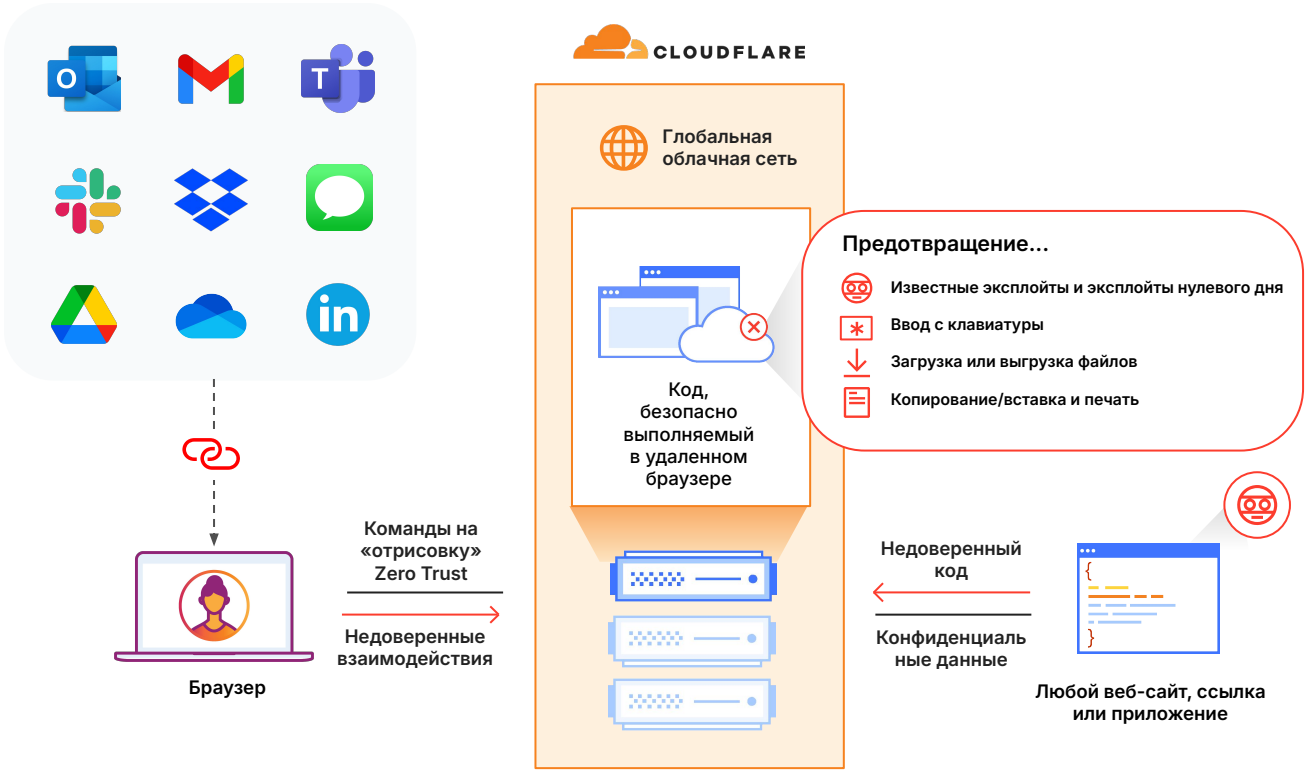
Изолируйте атаки с использованием ссылок

Атаки с использованием ссылок стали популярным методом кражи учетных данных, загрузки вредоносного ПО и программ-шантажистов, а также извлечения конфиденциальной информации. Использование комбинации электронной почты, чата, SMS, социальных сетей и других приложений для доставки этих ссылок еще больше усложняет процесс обеспечения защиты как сотрудников, так и данных от целенаправленных фишинговых атак.

Cloudflare борется с фишинговыми атаками с использованием ссылок, удаленно отображая весь веб-код в нашей глобальной облачной сети, а не на локальном устройстве пользователя. Это позволяет нейтрализовать вредоносное ПО и угрозы zero-day в браузере, а также обеспечивает детальный контроль над действиями пользователя (например, отключение ввода с клавиатуры) для предотвращения сбора учетных данных и утечки данных.

Устраните риск фишинга, не замедляя работу сотрудников

Благодаря интеграции возможностей изоляции браузера нового поколения, основанных на нашей уникальной технологии сетевого векторного рендеринга (NVR), Cloudflare может предоставить надежное, безопасное и масштабируемое решение для изоляции потенциально вредоносных ссылок. В отличие от методов, требующих высокой пропускной способности, NVR передает на устройство безопасные потоковые команды на отрисовку. Это помогает устранить риск вредоносного веб-контента, не влияя на удобство использования для конечных пользователей. Благодаря NVR и сети Cloudflare с низкой задержкой, организации могут изолировать многоканальные угрозы, обеспечивая при этом бесперебойную производительность своих сотрудников.



Быстрое расследование и решение проблем

Интуитивное автоматизированное управление средствами безопасности

Благодаря большей автоматизации и минимальной настройке, необходимой для достижения оптимальных результатов, Cloudflare значительно сокращает время и усилия, необходимые для непрерывного контроля безопасности электронной почты. Специалисты по безопасности могут немедленно получить полное представление обо всех основных показателях и тенденциях на информационной панели, а также получить более подробные сведения о помеченных сообщениях. Детализация тенденций позволяет быстро обнаружить частые типы атак, нацеленные на руководителей, нейтрализовать отложенные атаки и получить другие критически важные данные.

Вся аналитика, телеметрия, наблюдаемые угрозы и индикаторы компрометации (IOC) доступны через обширный API для удобной интеграции в существующие рабочие процессы аналитиков и инструменты координации.

«Я часто рассказываю сотрудникам, что Cloudflare — это простое и удобное в использовании облачное SaaS-решение, и что я чрезвычайно доволен его высоким уровнем точности».

Japan Airlines

Управляемое обнаружение и реагирование (PhishGuard)

Управляемый сервис безопасности электронной почты от Cloudflare, PhishGuard дополняет ваших специалистов SOC, избавляя их от необходимости исследовать проблемы безопасности и обеспечивая важный сбор и анализ информации об угрозах. PhishGuard может способствовать нейтрализации фишинговых кампаний, помогая в расследованиях, оценке внутренних угроз, активном устранении мошенничества и выполнении комплексных мер по исправлению ситуации. PhishGuard расширяет ресурсы и опыт обеспечения безопасности, чтобы активно уведомлять о потенциальном мошенничестве и внутренних угрозах, а также осуществлять поиск угроз по электронной почте.

Функциональные возможности и преимущества PhishGuard:

- Управление защитой от фишинговых сообщений и реагированием на инциденты для более быстрого решения проблем.
- Превентивные уведомления о BEC и мошенничестве, позволяющие организациям быстро реагировать на ранних стадиях атаки.
- Выделенные ресурсы для мониторинга в режиме реального времени, проведения периодических проверок учетных записей и постоянной оценки угроз.
- Пользовательские сигнатуры блокировки на основе анализа угроз управляемой среды.

1100+

Часов экономится ежегодно за счет автоматизации ручной сортировки

Автоматизированное решение Cloudflare устраняет трудоемкие, выполняемые вручную задачи, сокращая время реакции и позволяя разблокировать дополнительные циклы.

50 %

Снижение количества доставленных вредоносных или подозрительных писем (поверх M365)

Размещение Cloudflare поверх Microsoft 365 позволяет организациям перехватывать целевые атаки и сокращать общее количество вредоносных писем.

40

Часов суммарно, потраченных за семь лет на настройку безопасности электронной почты

Автоматизированный сервис защиты электронной почты Cloudflare требует небольшого объема предварительного конфигурирования и текущей настройки, обеспечивая высокую эффективность обнаружения сразу же после установки.

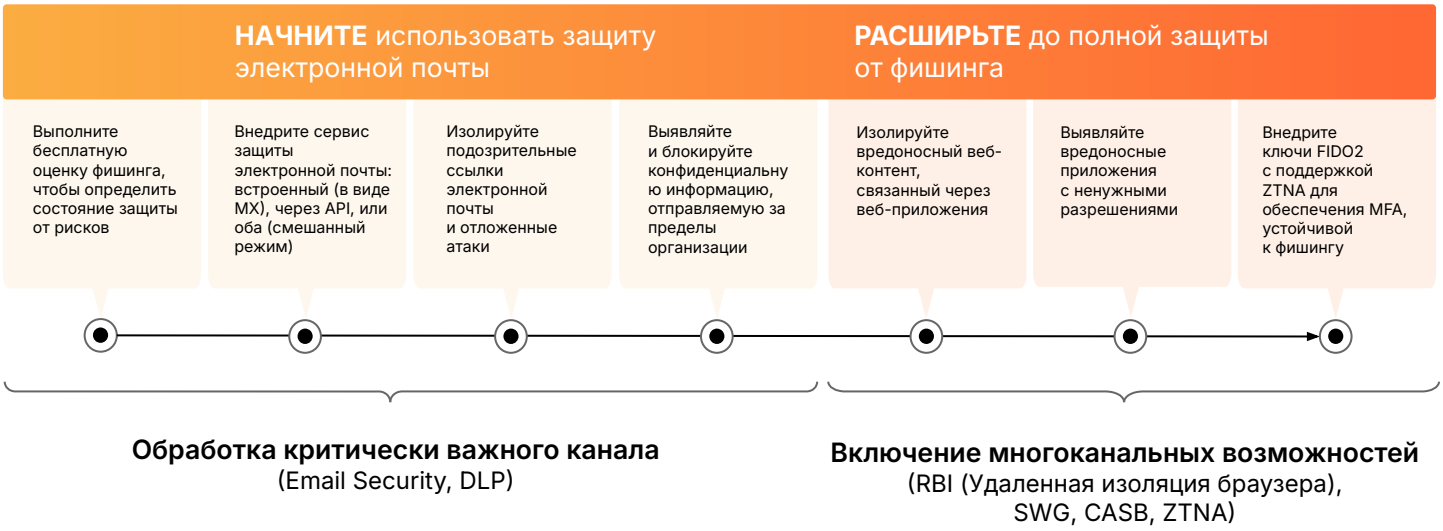
ПРЕИМУЩЕСТВА

Комплексная многоканальная защита

Поскольку фишинговые кампании быстро выходят за рамки электронной почты, организациям сейчас как никогда важно внедрить антифишинговое решение, которое обеспечивает быстрый и простой путь к полной многоканальной защите.

Благодаря унифицированной платформе безопасности Cloudflare организации могут сначала развернуть ведущую в отрасли систему безопасности электронной почты, чтобы быстро обеспечить защиту критически важного канала, подвергающегося фишингу; затем легко включить сервисы Zero Trust, чтобы распространить защиту на все каналы, эффективно блокируя известные и возникающие угрозы фишинга.

- **Автоматизированная, высокоэффективная защита:** Сведите к минимуму риск фишинга благодаря лучшей в отрасли эффективности обнаружения, требующей минимальной настройки.
- **Более эффективная консолидация, более низкие затраты:** Сократите расходы с помощью единой полностью интегрированной платформы, которая подходит для всех вариантов использования фишинга.
- **Быстрое развертывание, удобное управление:** Обеспечьте немедленную защиту, одновременно сократив время и усилия, необходимые для постоянного управления.



Оценка и сравнение

Оцените свои имеющиеся средства защиты электронной почты и узнайте, какие угрозы остаются незамеченными

Проведите бесплатное ретро-сканирование за несколько минут, чтобы узнать, каким фишинговым угрозам удалось проникнуть за последние 14 дней, или запросите оценку риска фишинга (PRA), чтобы отслеживать входящие сообщения на предмет фишинга по мере их доставки. Сравните с другими поставщиками услуг с нулевой готовой настройкой, чтобы определить, какое решение для обеспечения безопасности электронной почты обеспечивает наиболее быструю и простую защиту.

Запустить ретро-сканирование | Запрос оценки риска фишинга

1. Исследование Deloitte, 2020 г.: Источник
2. 2023 FBI IC3 PSA: Источник
3. Обзор возможностей Forrester, 2023 г.: Источник

