Окупаемость инвестиций в Zero Trust

5 способов уменьшить поверхность атаки с помощью стратегии безопасности с нулевым доверием (Zero Trust), которые позволяют обеспечить экономию времени и средств для вашего бизнеса

CLOUDFLARE

01

Уменьшение поверхности атаки

Исходя из предположений Gartner, организации, которые изолируют использование браузеров с высоким риском от систем конечных пользователей и изолируют доступ приложений от сетей, добьются сокращения атак, которые могут достичь их среды, на 91 %.[1]

02

Снижение затрат на устранение нарушений

С уменьшением поверхности атаки обеспечивается более высокая защита от разрушительных утечек данных. Согласно отчету IBM «Стоимость утечки данных», организации с высоким уровнем внедрения Zero Trust меньше платят за восстановление после утечек данных: организации с высоким уровнем Zero Trust платят 3,28 млн долл. США по сравнению с 5,04 млн долл. для организаций без стратегии Zero Trust.[2]

03

Ускорение подключения

Когда внедрение Zero Trust идет параллельно с заменой устаревших подходов к удаленному доступу, таких как средства контроля на основе VPN и IP, организации, в частности, клиент Cloudflare, eTeacher Group, сообщают, что они тратят меньше времени на подключение новых пользователей, сокращая время, необходимое для предоставления доступа новому пользователю, на целых 60 %.

04

Сокращение затрат времени на обработку ИТ-заявок в техподдержку

Когда у пользователей нет необходимости иметь дело с VPN-клиентом на своем устройстве, организации начинают замечать значительное сокращение времени, которое они тратят на обработку заявок, связанных с доступом, при этом некоторые организации сообщают о сокращении времени, затрачиваемого на обслуживание проблем пользователей, до 80 %.

05

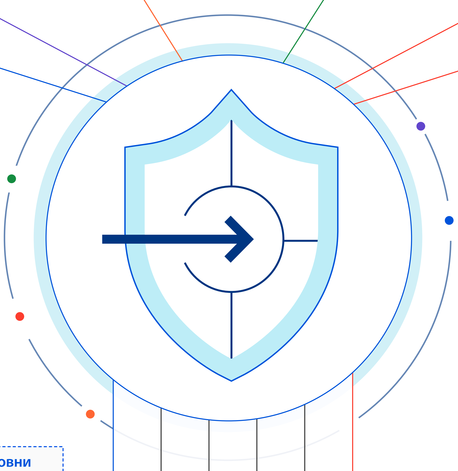
Уменьшение сетевой задержки

Принятие подходов Zero Trust к использованию интернет-браузеров и доступу к приложениям значительно влияет на скорость подключения вашего бизнеса. Это позволяет обеспечить возврат пакетов трафика в центр обработки данных, расположенный далеко от пользователей или ресурсов. Когда пользователи подключаются к ресурсам через сеть Cloudflare, а не через стандартные маршруты Интернета, публичные и частные веб-приложения загружаются на 30 % быстрее, а время приема-передачи TCP-соединения сокращается на 17 %.

Начало работы менее чем за 30 минут

Масштабирование без всяких усилий

Окончание работы с лучшим в отрасли соотношением окупаемости инвестиций к затратам времени



Это означает встроенные уровни защиты от:

- бокового перемещения ПО;
- программ-шантажистов;
- фишинга;
- уязвимостей VPN;
- атак на цепочку поставок или атак на основе обхода MFA.

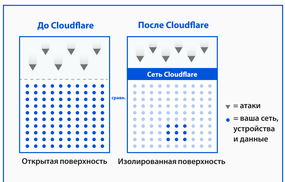
Уменьшение поверхности атаки

Снижение затрат на устранение нарушений

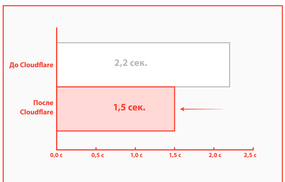
Ускорение подключения

Сокращение затрат времени на обработку ИТ-заявок в техподдержку

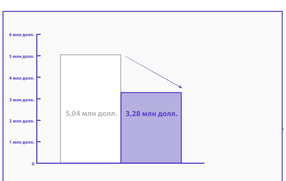
Уменьшение сетевой задержки



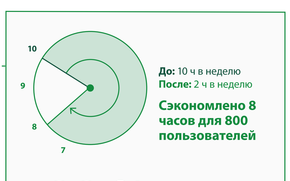
91 %
Уменьшает количество успешных атак до 91 %



30 %
Позволяет на 30 % быстрее подключаться к приложениям и сервисам

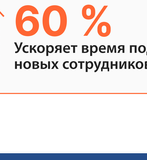


35 %
Снижает среднюю стоимость утечки данных на 35 %, с 5,04 млн долл. до 3,28 млн долл.



До: 10 ч в неделю
После: 2 ч в неделю
Сэкономлено 8 часов для 800 пользователей

80 %
Сокращение времени, затрачиваемого на обработку ИТ-заявок в техподдержку по удаленному доступу, до 80 %



60 %
Ускоряет время подключения новых сотрудников до 60 %

01

Начало работы менее чем за 30 минут

Платформа безопасности Zero Trust от Cloudflare расширяет возможности мониторинга, устраняет сложности и снижает риски при подключении сотрудников к приложениям и Интернету. Чтобы начать работу, потребуется всего 30 минут на выполнение настроек.

02

Масштабирование без всяких усилий

Быстрое масштабирование политик безопасности Zero Trust для новых пользователей по всему миру, поскольку сервисы Zero Trust от Cloudflare последовательно развернуты в каждом из наших 250+ городов по всему миру.

03

Окончание работы с лучшим в отрасли соотношением окупаемости инвестиций к затратам времени

Поддержка широкого спектра типов приложений и протоколов с быстрым и простым подключением. Вам никогда не придется вручную управлять пропускной способностью или платить больше по мере роста запросов.

Готовы начать работу?

Нажмите здесь

[1]Объединяет допущения из двух публикаций Gartner — "Innovation Insight for Remote Browser Isolation" («Инновационный подход к удаленной изоляции браузеров»), от 8 марта 2018 г., и "It's Time to Isolate Your Services From Internet Cesspool" («Пришло время изолировать ваши услуги от "помойки" Интернета», от 17 ноября 2017 г.)

[2]IBM, отчет "Cost of a Data Breach" («Стоимость утечки данных»), 2021 г.

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/ru-ru/