Сетевой доступ с нулевым доверием (Zero Trust)

Cloudflare Zero Trust, в частности, Access, повышает производительность команды и снижает риски, поскольку все пользователи получают доступ к вашим размещаемым на собственных серверах, SaaS- или не веб-приложениям — без VPN.

Простой и безопасный доступ для гибридной работы

Сетевой доступ с нулевым доверием (ZTNA) на основе Интернета

Современная распределенная рабочая среда требует распределенного подхода к безопасности. «Периметра» больше не существует, и традиционные решения удаленного доступа, такие как VPN, не могут соответствовать современным ожиданиям в области безопасности и производительности.

ZTNA обеспечивает простой и безопасный доступ между любым пользователем и приложением, на любом устройстве и в любой локации, постоянно проверяя детальный контекст, такой как идентификация и состояние устройства, для каждого ресурса. Благодаря совершенно новому подходу больше не существует «балансирования» между безопасностью и удобством использования. ZTNA расширяет возможности вашего бизнеса, улучшая и то, и другое.

Это также делает организации более гибкими и способными лучше ориентироваться в изменениях, будь то миграция в облако, деятельность по слияниям и поглощениям или инновации и быстрое масштабирование. Cloudflare — это «сердце» стратегии Zero Trust или модернизации безопасности, предоставляющей ZTNA в нашем программируемом глобальном облаке соединений.

80 % Сокращение среднего времени, затрачиваемого на разрешение заявок в службу поддержки в отношении удаленного доступа, связанных с использованием VPN [1]

72 % Экономия времени на ежемесячную настройку политики по сравнению с предыдущим поставщиком [1]

68 % Отметили значительное влияние на оптимизацию процесса аутентификации для сотрудников и подрядчиков [1]

Расширьте возможности своего бизнеса с помощью модернизированного доступа

Улучшение удобства использования

Повысьте производительность команды с помощью модернизированной системы безопасности, благодаря которой работа локальных приложений становится аналогичной приложениям SaaS. Больше никаких медленных, неудобных VPN и жалоб сотрудников.

Устранение бокового перемещения (внутри сети)

Снижайте киберриски и уменьшайте вашу поверхность атаки, предоставляя контекстно-ориентированный доступ с наименьшими привилегиями для каждого ресурса, а не доступ на уровне сети.

Масштабирование Zero Trust без особых усилий

Повышайте техническую эффективность за счет защиты критически важных приложений или групп пользователей с наибольшим риском, а затем расширьте встроенную в Интернет ZTNA для защиты всего вашего бизнеса.

Основные варианты использования для Access

Внедряйте Zero Trust и обезопасьте гибридную работу

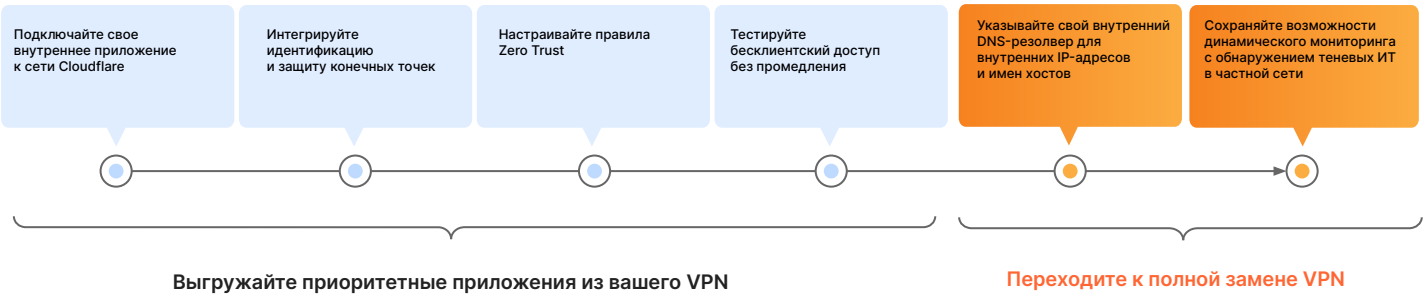
- ★ **Расширение и замена VPN** — Доступ быстрее и безопаснее, чем при традиционных VPN. Начните выгружать критически важные приложения для повышения безопасности и удобства конечных пользователей.
- ★ **Доступ для подрядчиков** — Аутентификация сторонних пользователей, таких как подрядчики, с помощью бесклиентских опций, социальных IdP и т. д.
- **Доступ для разработчиков** — Предоставьте привилегированным техническим пользователям безопасный доступ к критически важной инфраструктуре без ущерба для производительности.

Обеспечение цифровой модернизации

- **Ускорение слияний и поглощений** — Возможность полностью избежать традиционных сетевых слияний. Интеграция с несколькими поставщиками удостоверений и предоставление внутреннего доступа для каждого приложения в ходе слияний и поглощений.
- **Устойчивый к фишингу MFA** — Внедряйте надежную аутентификацию, например ключи безопасности, соответствующие требованиям FIDO2, повсюду.
- **Обеспечьте безопасность рабочих процессов DevOps** — Защитите межсервисные рабочие процессы с помощью межсетевого/P2P (одноранговая сеть) подключения, поддерживающего двунаправленный трафик.

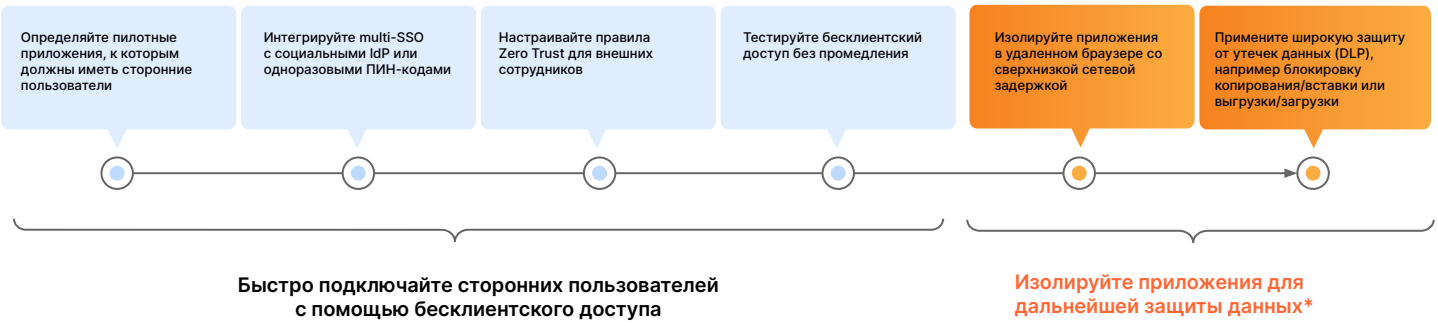
Начало работы с расширением и заменой VPN

Отдайте приоритет критически важным приложениям или рискованным пользователям, чтобы пилотный проект ZTNA дополнил вашу VPN. Используйте бесклиентский доступ для веб-приложений или SSH в браузере, чтобы ускорить тестирование. Со временем внедряйте расширенные возможности, чтобы перейти к полной замене VPN и поддерживать динамический мониторинг при изменении вашей сети.



Начало работы с доступом подрядчика (третьих лиц)

Обеспечьте бесперебойное удобство использования и одновременно снижайте риски, связанные с неуправляемыми устройствами. Настраивайте простые параметры аутентификации для подрядчиков — программное обеспечение для конечного пользователя не требуется. Со временем внедряйте расширенные возможности для обеспечения дополнительной защиты данных.



** использование возможностей посредством других частей платформы Zero Trust*

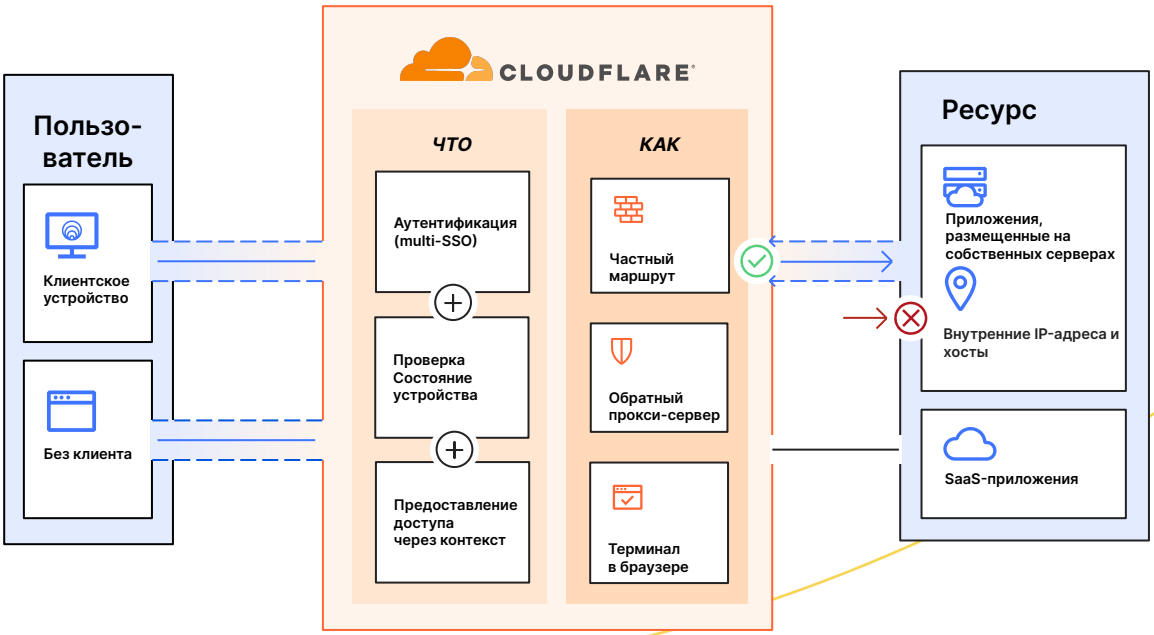
Как работает Access

Cloudflare Access — это гибкий уровень агрегации, который постоянно проверяет детализированный контекст, такой как идентификация и состояние устройства, чтобы обеспечить простой и безопасный доступ ко всем ресурсам организации по отдельности, создавая программно-определяемый периметр. Когда пользователь проходит проверку подлинности и соответствует всем критериям политики доступа, Access выдает подписанный веб-токен JSON, действительный в течение указанной продолжительности сеанса. Мы выполняем проверку в единый проход всех запросов пользователей через нашу составную платформу, а наш опыт централизованного администрирования политик позволяет профилировать изменения политики по всему миру за считанные секунды благодаря нашей уникальной сетевой архитектуре Anycast.

Унифицированное бесклиентское и осуществляющееся на стороне клиента функционирование позволяет обрабатывать все типы устройств. Мы используем единый клиент устройства для всех сервисов Zero Trust, который шифрует трафик в нашей сети для обеспечения конфиденциальности данных наших клиентов. Мы также обеспечиваем простой и безопасный доступ к устройствам за пределами предприятия посредством нашей бесклиентской установки. Наши ZTNA, DNS и ведущие на рынке сервисы защиты WAF и защиты от DDoS атак работают вместе, чтобы создавать и защищать общедоступные имена хостов, доступные сторонним пользователям и гибридным сотрудникам на любом устройстве. Наши варианты беспользовательской аутентификации (токены или сертификаты mTLS) также подходят для сценариев использования автоматических сервисов и устройств Интернета вещей.

Для средств управления Zero Trust ресурсы используют общедоступные имена хостов для обратного прокси-сервера для приложений, размещаемых на собственных серверах (в облаке/локально) или SSH/VNC в браузере, прокси-сервер идентификации для приложений SaaS или частной маршрутизации на основе клиента/туннеля через прямой прокси-сервер уровней L4–7 для любого веб- или не веб-ресурса (например, произвольный TCP/UDP) ресурс в частной подсети. Наше глобальное программное обеспечение для подключения к сети и приложениям в совокупности поддерживает любую вычислительную среду — общедоступное облако, включая Kubernetes и контейнеры, или устаревшие локальные сетевые ресурсы — без необходимости инфраструктуры виртуальных машин и без ограничений пропускной способности в отличие от других поставщиков Zero Trust.

Сторонние инструменты идентификации, конечных точек, возможностей сетевого подключения, ведения журнала/аналитики и SIEM интегрированы в нашу панель управления наряду с собственными опциями для нашего клиента устройств и аналитики, что позволяет администраторам сохранять гибкость и создавать инструменты, которые они уже используют.



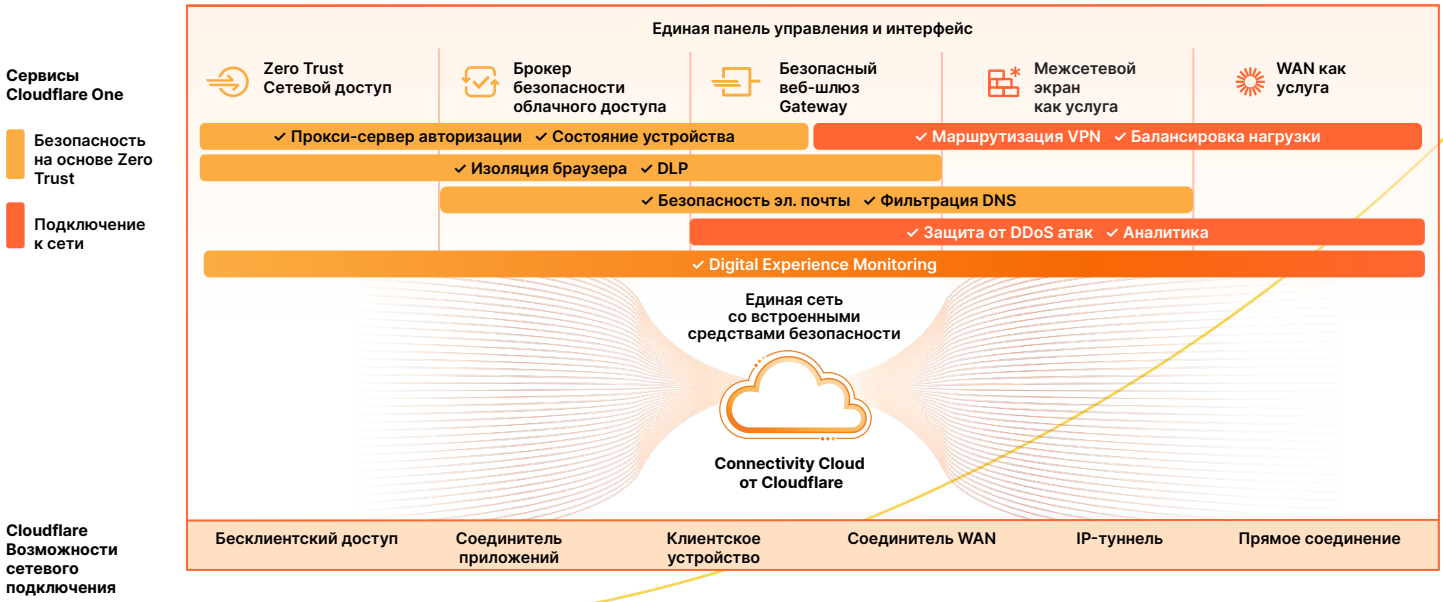
Access является частью платформы Cloudflare's SSE и SASE

В то время как SSE и SASE часто предполагают многолетний стратегический путь, согласно практике Cloudflare, организации часто начинают с ZTNA, поскольку сюда входят действенные и доступные шаги для ИТ-команд, и при этом демонстрируется значительная краткосрочная ценность для бизнеса. ИТ-руководители стремятся обеспечить гибридную работу, защититься от угроз и защитить свои данные на пути к консолидации, и они все чаще выбирают Cloudflare в качестве своего надежного партнера.

Гибкость развертывания и компонуемая архитектура Cloudflare позволяют любой организации защищать и повышать производительность устройств, приложений и целых сетей, обеспечивая безопасность и продуктивность гибридной работы. Для этого мы поддерживаем возможность самостоятельного подключения конечных пользователей, бесклиентскую веб-изоляцию для сдерживания небезопасного трафика, а также унифицированную информационную панель управления, которая позволяет контролировать все службы безопасности и сетевые сервисы, независимо от того, откуда подключаются администраторы или пользователи. Широта глобальной сети Cloudflare позволяет обеспечить безопасность ближе к конечным пользователям, сводя к минимуму задержки и обеспечивая удобство работы сотрудников. Наша архитектура Anycast помогает обойти сбои в работе Интернета, поддерживать работу команд в сети и обеспечивать непрерывность бизнеса.

Благодаря нашей унифицированной платформе SSE и SASE общий контекст между нашими политиками ZTNA, CASB, DLP и SWG помогает повысить уровень безопасности, одновременно упрощая реализацию за счет согласованного рабочего процесса администрирования. Одни и те же атрибуты идентификации и состояния устройства могут использоваться в политиках доступа для ZTNA и CASB, а также в политиках SWG, упрощая управление политиками в организациях.

ZTNA, RBI и безопасность электронной почты также можно использовать вместе для обеспечения условного доступа к ресурсам, одновременно изолируя пользователей от вредоносного контента (ссылок, вложений), которому они подвергаются через электронную почту и инструменты совместной работы. Подрядчикам и пользователям на неуправляемых устройствах может быть предоставлен ограниченный доступ к корпоративным ресурсам с отключением взаимодействия с пользователем (например, выгрузка/загрузка, копирование/вставка, ввод с клавиатуры) для предотвращения компрометации данных, а для обнаружения конфиденциальных данных могут применяться другие политики DLP уровня 7.



Что говорят клиенты

«Cloudflare Access — отличная альтернатива традиционным VPN. Пользователи просто открывают свои браузеры и входят в систему, без необходимости загружать и настраивать дополнительное программное обеспечение».

— **Platzi**, руководитель отдела облачной инженерии

«Cloudflare Access стал доступен как раз вовремя, чтобы нам не пришлось проходить через хлопоты по развертыванию VPN. Для нас это был простой выбор, и его было поразительно просто реализовать».

— **ezCater**, руководитель службы безопасности

«Доступ намного проще и безопаснее, чем VPN, поскольку он позволяет ограничить доступ к внутренним активам. Мы просто активируем его и добавляем пользователей. Он просто работает!"

— **Bitpanda**, технический директор и соучредитель

«До того как мы внедрили Cloudflare, подготовка приложения к безопасному развертыванию занимала от двух до четырех недель. С Zero Trust от Cloudflare мы экономим почти 90 % этого времени».

— **Creditas**, руководитель группы сетевых технологий

Что говорят аналитики

Cloudflare названа лидером согласно отчету IDC MarketScape за 2023-й год в категории «Сетевой доступ с нулевым доверием (Zero Trust)»

IDC отмечает «агрессивную стратегию продуктов для поддержки потребностей корпоративной безопасности» Cloudflare. Мы считаем, что наше признание подтверждает наш подход, помогающий компаниям любого размера начать работу с Zero Trust и безопасным доступом любого пользователя к любому ресурсу без VPN.

Cloudflare названа лидером согласно отчету KuppingerCole Leadership Compass за 2024-й год в категории ZTNA

В рамках анализа рынка ZTNA за 2024 год KuppingerCole Analysts AG отметила несколько сильных сторон Cloudflare, таких как наша полностью интегрированная, органично разработанная платформа безопасности, крупная глобальная облачная инфраструктура и огромное присутствие на рынке.

Возможности доступа

Создание/редактирование политик Zero Trust для безопасного доступа	
Детальные, настраиваемые политики доступа	Централизованное администрирование политики. Приложения уровня L7 защищены на уровне поддомена и пути с помощью подстановочных знаков и поддержки нескольких имен хостов, а также поддерживают запросы CORS. Изменения политики распространяются глобально за считанные секунды. Включает тестер политик.
Широкий спектр ресурсов: что и как мы можем защитить	Ресурсы используют общедоступные имена хостов для обратного прокси-сервера для приложений, размещаемых на собственных серверах (в облаке/локально) или в браузере SSH/VNC, прокси-сервера авторизации для SaaS-приложений или частной маршрутизации на основе клиента/туннеля через прямой прокси-сервер уровней L4–7 для любого веб- или не веб-ресурса (например, произвольный TCP/UDP) в частной подсети. Также поддерживает ресурсы/рабочие процессы в рамках двунаправленного трафика (например, поток трафика VoIP/SIP или CI/CD).
Прокси-сервер	Аутентификация через всех основных поставщиков корпоративных и социальных удостоверений (IdPs), включая несколько IdPs одновременно. Может также использовать общие соединители SAML и OIDC. Поддерживает (и может подкреплять) любой метод AuthN, предоставляемый IdP, временную AuthN, обоснование цели, интервалы повторной AuthN для глобального сеанса или для каждого приложения, а также возможность немедленного отзыва сеанса для каждого приложения или для каждого пользователя.
Состояние устройства	Проверка состояния устройства с помощью интеграции клиента устройства и стороннего поставщика защиты конечных точек (EPP). Использование интеграций между услугами для включения оценки рисков EPP в политики Zero Trust.
Контекстуальные сигналы для политик	Конфигурирование сигналов, таких как группа электронной почты, диапазоны IP-адресов, геолокация, метод входа в систему (например, тип MFA, тип IdP), действительный сертификат mTLS или SSH, сервисный токен, список серийных номеров, атрибуты состояния устройства, установленный клиент устройства, продолжительность сеанса, применение правил SWG. или сигналы от внешних вызовов API. Также может напрямую ссылаться на политики условного доступа Microsoft Entra ID (Azure AD).
Другая сопутствующая поддержка	• **SCIM:** автоматическая подготовка/деинициализация пользователей для приложений, размещаемых на собственных серверах, и приложений SaaS (примеры для Okta и Azure AD) • **Внутренний DNS:** настройка перехода локального домена в аварийный режим и разрешение запросов частных сетей • **Раздельное туннелирование:** включение/исключение IP для частных сетей или работы вместе с VPN • **Аутентификация mTLS:** аутентификация на основе сертификатов для IoT и других вариантов использования mTLS • **Изоляция приложений:** с помощью одного флажка изолируйте приложения в нашем молниеносно быстром удаленном браузере*
Возможности входящего и исходящего сетевого подключения	
Соединитель приложений	Простая координация нашего легкого коннектора приложений (Cloudflare Tunnel) ускоряет подключение ресурсов к Cloudflare, не требуя инфраструктуры виртуальных машин и ограничений пропускной способности. Включает мониторинг, виртуальные сети (на случай перекрытия IP-адресов), а также возможности резервирования и аварийного переключения.
Клиентское устройство: когда использовать	• **Бесклиентский доступ:** распространение политик Zero Trust на сторонних пользователей на неуправляемых устройствах; также хорошо сочетается с бесклиентскими RBI политиками DLP уровня L7*. Бесклиентский доступ поддерживает веб-приложения и SSH/VNC в браузере. • **На стороне клиента:** наше клиентское устройство (Cloudflare WARP) расширяет безопасный доступ к частным сетям, обеспечивает интеграцию состояния устройств между сервисами и учитывает местоположение, чтобы применять индивидуальные политики для локальных пользователей. Также можно подключить любые два или более устройств, работающих под управлением WARP, для создания частных сетей. Пользователи могут регистрироваться самостоятельно или выполнять развертывание через MDM.
Расширяемость и возможности мониторинга	
Настройка страницы	Выгружайте собственный HTML-код для экранов запуска блоков и приложений, чтобы он соответствовал вашему брендингу, или передайте конкретные инструкции по доступу, чтобы упростить взаимодействие с конечным пользователем.
Ведение журнала	Комплексное ведение журнала для всех запросов, пользователей и устройств. Может использовать logpush или API для интеграции с существующим SIEM, координацию и инструменты анализа. Для неизвестных ресурсов наши теневые ИТ для внутренней инфраструктуры пассивно каталогизируют уникальный трафик, охватывающий все источники.
Автоматизация	Интуитивно понятные API и поставщик Terraform 4 доступны для программного управления всеми аспектами реализации Zero Trust. Также предлагается беспользовательская поддержка сервисных токенов для автоматических сервисов.

** использование возможностей посредством других частей платформы Zero Trust*

Почему Cloudflare?

Удобная настройка и управление

Радикально упростите настройку и управление доставкой трафика к частным ресурсам с помощью программного обеспечения коннектора приложений и координации туннелей.

Бесперебойная работа в режиме постоянного включения

Достигните максимальной производительности конечных пользователей и устойчивости к сбоям в сети с помощью глобальной технологии Anycast от Cloudflare, обеспечивающей надежность.

Быстрые инновации для ранних пользователей

Идите в ногу с развитием самого Интернета с помощью поставщика, который постоянно внедряет инновации, опережающие своих конкурентов, чтобы сделать доступ к приложениям более быстрым и безопасным.

Давайте обсудим простой и безопасный доступ для вашей организации

Запрос семинара

CLOUDFLARE

Пока не готовы к беседе в режиме онлайн?

Продолжайте узнавать больше о нашей эталонной архитектуре SASE.

1. Опрос 2023: techvalidate.com/product-research/cloudflare/charts