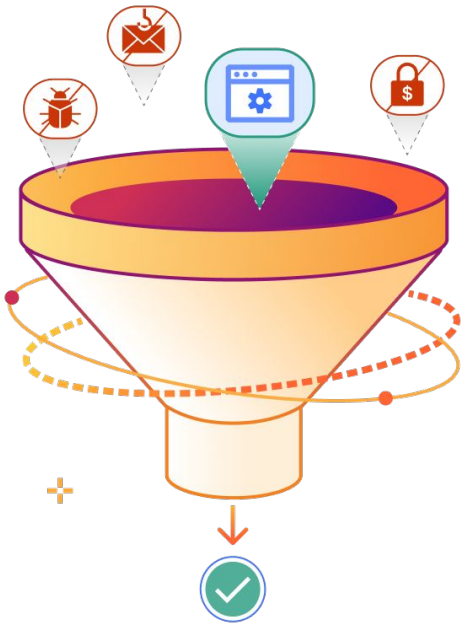
CLOUDFLARE

ОБЗОР ПРОДУКТА

Защищенный веб-шлюз (SWG)

Cloudflare Gateway, комбинируемый сервис в составе Cloudflare One, защищает пользователей и данные от киберугроз с помощью основанной на личных данных интернет-фильтрации.



Простая и современная защита от угроз

Замена сложных устаревших средств веб-безопасности

Киберугрозы существуют повсеместно, а их создатели неустанно ищут уязвимости в увеличивающейся поверхности атаки вашей организации. Одновременное использование нескольких специализированных решений (таких как DNS-резолверы, веб-шлюзы и межсетевые экраны) только лишь увеличивает стоимость, сложность и опасность.

Cloudflare Gateway упрощает обеспечение безопасности благодаря постоянной защите и мониторингу доступа к сети Интернет и внутренним ресурсам. Уменьшите количество киберугроз, внедрив основанные на личных данных политики, которые помогут вашей организации:

- **Блокировать интернет-угрозы** , такие как программы-шантажисты, фишинг, командные серверы и многие другие
- **Контролировать и отслеживать трафик уровней L4–L7** с использованием правил для DNS, HTTP, сети и изоляции браузера
- **Внедрять приемлемые политики использования** среди удаленных и офисных сотрудников

В однопроходной архитектуре весь трафик проверяется, фильтруется, анализируется и изолируется от угроз.

SWG сегодня, периферийный сервис безопасности (SSE) завтра

Модернизация средств контроля SWG — это распространенный шаг в направлении консолидации безопасности с использованием архитектуры SSE и внедрения эффективных методов модели Zero Trust.

Узнайте, каким может быть такой путь с решениями от Cloudflare.

Почему Cloudflare?

Объединенная безопасность

Одна сеть

и плоскость управления для всех сервисов при использовании периферийного сервиса безопасности Edge (SSE), защиты веб-приложений и API (WAAP), защиты электронной почты и других доменов.

Широкомасштабный сбор и анализ информации об угрозах

2 триллиона

DNS-запросов, обслуживаемых ежедневно. Эта возможность в реальном времени отслеживать новые, вновь обнаруженные и сомнительные домены позволяет моделям на основе искусственного интеллекта и машинного обучения обеспечить защиту от новых угроз.

Создан для масштабирования

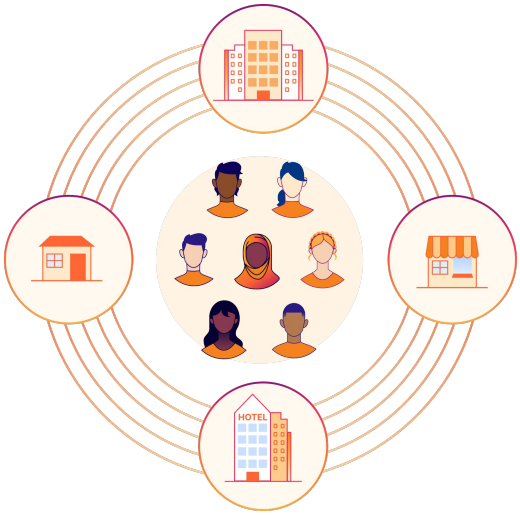
Более 310

сетевых локаций в более чем 120 странах. Все функции SWG и Zero Trust/SSE доступны клиентам в любой локации, благодаря чему их внедрение всегда осуществляется быстро и последовательно.

Пример использования: защита от угроз для удаленных и офисных сотрудников

Проблема

Гибридная работа увеличивает поверхность атаки в вашей организации, а из-за уязвимостей в системе безопасности, возникающих вследствие использования разрозненных инструментов, программы-шантажисты, фишинговые атаки и другие киберугрозы могут навредить как вашим финансам, так и репутации вашего бренда.



Решение

Cloudflare SWG позволяет обеспечить надежную веб-безопасность для удаленных и офисных сотрудников. Чтобы добиться быстрой окупаемости, большинство организаций начинают с фильтрации DNS, а уже потом добавляют более комплексные методы проверки и контроля для всей активности в Интернете.

Начало работы

Отправляйте трафик сначала в сеть Cloudflare для разрешения DNS (а затем для полной проверки HTTP)

Внедрите фильтрацию DNS по личным данным или устройствам для удаленных сотрудников или по локациям для работающих в офисах

Добавляйте более детализированные средства контроля, включая правила для HTTP, сети и изоляции браузера.

Внедрите сервис для защиты электронной почты — как часть более широкого решения (MX), через API или в мультимодальном режиме (объединяющем оба варианта)

Сначала обеспечьте безопасную работе в Интернете как для удаленных, так и для офисных пользователей

Затем добавляйте уровни защиты электронной почты

Снижение рисков и повышение эффективности команды

Простое и гибкое развертывание

Используйте сетевые маршрутизаторы для разрешения DNS. Отправляйте трафик L3 через туннели GRE/IPsec, соединитель WAN или имеющуюся сеть SD-WAN.

Или внедрите наше клиентское устройство для перенаправления трафика через прокси-сервер.

Быстрая и постоянная защита

Проверка в один проход во всей нашей сети для быстрого и последовательного внедрения политик повсеместно.

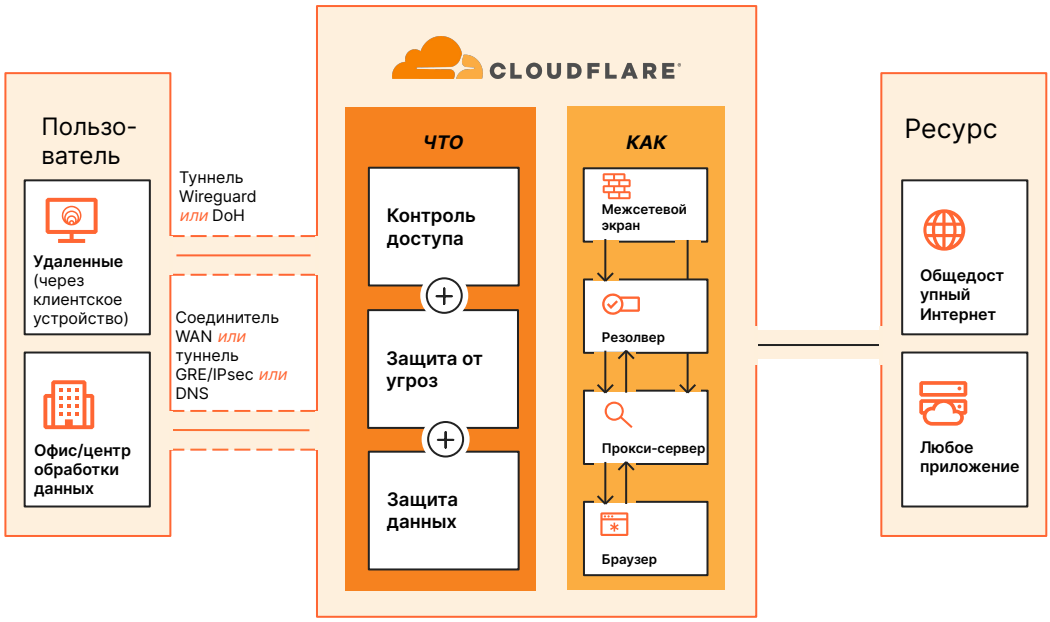
Подтвержденная более высокая скорость, чем у других поставщиков сервисов, таких как Zscaler, Netskope и Palo Alto Networks.

Ускорение внедрения модели Zero Trust

Одна унифицированная плоскость управления с одним администратором политик для всех комбинируемых сервисов SSE/SASE.

Начните с защиты для Интернета и электронной почты и добавляйте другие элементы контроля Zero Trust по мере необходимости.

Как работает SWG



Упростите инфраструктуру безопасности.

Задействуйте межсетевой экран, резолвер, прокси-сервер и элементы контроля браузера как для интернет-трафика, так и для трафика внутренних ресурсов.

Внедряйте политики от одного администратора политик.

Добавление элементов контроля SSE к основе SWG

Выполняя проксирование трафика через Cloudflare SWG, ваша организация может еще больше расширить контроль безопасности и мониторинг путем использования возможностей наших изначально интегрированных и комбинируемых сервисов SSE.

Защита веб-сайтов и приложений путем удаленной изоляции браузера

- Защитите локальные устройства от вредоносного ПО, запустив весь код браузера в глобальной сети Cloudflare с небольшой задержкой
- Изолируйте приложения для защиты данных с использованием сканирований DLP и элементов контроля браузера (например, блокировка копирования и вставки, запрет на загрузку файлов или печать) — с клиентским устройством или без него

Защита данных с использованием мультимодальных DLP и CASB

- Не допускайте утечки данных путем обнаружения и блокировки конфиденциальных данных в трафике HTTP(S) и файлах с использованием предварительно установленных (например, данных о финансах или состоянии) или собственных профилей (например, точное соответствие данных)
- Сканируйте пакеты SaaS, чтобы выявить неправильные конфигурации с помощью интегрированных средств обнаружения DLP для конфиденциальных данных и выполнить предписания по устранению рисков.

Расширение политик доступа с учетом личных данных с ZTNA

- Применяйте правила Zero Trust, которые ограничивают доступ к корпоративным приложениям, размещаемым на собственной инфраструктуре, SaaS-приложениям и IP-адресам или именам хостов в частных сетях.
- Один раз интегрируйте поставщиков решений для защиты личных данных и конечных точек и выполняйте проверку состояний среди правил доступа к Интернету и к приложениям, используя один и тот же компоновщик правил

Дополнительные возможности мониторинга

- Храните подробные журналы аудита для контролируемых и неконтролируемых устройств (в договорных планах журналы DNS хранятся 6 месяцев, а журналы HTTP и сети — 30 дней)
- Отправляйте журналы своему предпочитаемому SIEM для сопоставления и дальнейшего анализа

Возможности шлюза

Защита от угроз и безопасный доступ	
Защита и категории приложений	Комплексный охват программ-шантажистов, фишинговых атак, доменов DGA, туннелирования DNS, новых и недавно замеченных доменов, командных серверов и ботнетов и других угроз безопасности. Встроенный охват CASB 25 категорий приложений, включая ИИ.
Рекурсивная фильтрация DNS	Разрешение, блокировка или переопределение доменов и IP-адресов по безопасности или категориям контента. Управление фильтрацией DNS может осуществляться через наш Tenant API конфигурируемости родительских и дочерних элементов.
Фильтрация и проверка HTTP(S)	Управляйте трафиком на основе источника, пункта назначения, доменов, методов HTTP, URL-адресов и т. д. Проверка HTTP1/2/3 позволяет контролировать антивирус и сканирования DLP, файлы, состояние устройства, клиентов, удаленную изоляцию браузера и многое другое.
Неограниченная проверка TLS 1.3	Неограниченная проверка TLS 1.3 по умолчанию. Весь трафик HTTPS дешифруется, применяются политики, затем снова зашифровывается с использованием нашего сертификата или вашего настраиваемого сертификата — все выполняется с наименьшей на рынке задержкой. Стандарты DNS over TLS (DoT) и DNS over HTTP (DoH) поддерживаются. Используйте только наборы шифров, совместимые с FIPS 140-2.
FWaaS уровня L4	Сетевые политики уровня L4 распространяются на все публичные/частные пакеты TCP/UDP, контролируя доступ к не-HTTP ресурсам путем определения протокола, геолокации, домена, SNI и т. д. Проверяйте трафик SSH через порт 22. (Возможности FWaaS уровня L3 встроены в сетевые сервисы WAN).
Антивирусная проверка	Сканируйте загружаемые или скачиваемые файлы самых разных типов (PDF, ZIP, RAR и т. д.) на вирусы.
Идентификация и проверка состояния устройства	Устанавливайте политики на основании всех крупных корпоративных сервисов авторизации, входа через социальные сети или стандартов SAML и OIDC. Проверяйте состояние устройства с использованием клиентского устройства или собственного стороннего поставщика сервисов защиты конечных точек.
Интегрированная функция сбора и анализа информации об угрозах	Выявление угроз осуществляется с использованием наших собственных моделей искусственного интеллекта/машинного обучения и аналитической информации третьих сторон. Данные собственного анализа получаются из глобальной телеметрии в качестве одного из крупнейших авторитетных и рекурсивных DNS-резолверов (более 2 трлн запросов в день). Наш поисковый робот также каждые несколько недель индексирует всю сеть (более 8 млрд страниц) для выявления инфраструктуры новых кампаний. Настраиваемые потоки данных об угрозах и подписи (IP-адреса, URL-адреса, домены и т. д.) также поддерживаются.
Возможности входящего и исходящего сетевого подключения	
С использованием клиентского устройства	Выполняйте проксирование трафика через наше клиентское устройство (WARP) через полные туннели WireGuard или по DoH. Выполняйте самостоятельную регистрацию или развертывание через MDM. Активирует проверки состояния устройства. Определяет, находится ли устройство в сети.
Варианты без использования клиента	Варианты включают в себя: маршрутизируемые по сети DNS-запросы от докаций клиента; туннели Anycast GRE/IPsec; соединитель WAN, конечные точки прокси-сервера через файлы PAC и бесклиентская веб-изоляция через переопределенный URL-адрес.
Поддержка IPv4 и IPv6	Все функции доступны для подключения IPv4 и IPv6 (будь то только IPv6 и двойного стека).
Маршрутизация трафика	
Выделенные исходящие IP-адреса и политики исходящего трафика	Выделенный диапазон статических IP-адресов (IPv4 или IPv6), которые можно использовать, чтобы разрешить трафик на основании исходного IP. Используйте политики исходящего трафика, чтобы выбрать, какой исходящий IP-адрес может использоваться, на основании идентификации, геолокации или состояния устройства. Каждый исходящий IP-адрес является уникальным для отдельной учетной записи и не используется другими клиентами.
Политики резолвера	Направляйте DNS-запросы к настраиваемым DNS-резолверам, чтобы достичь непублично маршрутизируемых доменов, таких как сервисы частных сетей и внутренние приложения. (По умолчанию DNS-запросы используют собственный публичный DNS-резолвер Cloudflare, 1.1.1.1, один из самых быстрых и надежных в мире).
Раздельное туннелирование	Включайте или исключайте IP-адреса или домены для частных сетей или работы вместе с VPN.
Мониторинг и расширяемость	
Ведение журнала	Комплексное протоколирование для всех DNS-запросов, сетевых пакетов уровня L4 и HTTP-запросов, проверяемых на каждом порту. Используйте отправку журналов или API для интеграции с уже действующими инструментами SIEM, координации и анализа. Администраторы могут исключить или редактировать коллекцию персональной идентифицирующей информации (PII) для пользователей.
Обнаружение теневых ИТ-приложений	Отслеживайте, анализируйте и утверждайте источники SaaS частных сетей, к которым подключаются ваши конечные пользователи через встроенный CASB.
Настройка страницы	Загружайте настраиваемые страницы блокировки HTTP в соответствии с вашим брендингом или для передачи инструкций для обеспечения большего удобства использования.
Автоматизация	Интуитивно понятные API и поставщик Terraform доступны для программного управления всеми аспектами реализации SSE/Zero Trust. Также предлагается беспользовательская поддержка сервисных токенов для автоматических сервисов.

Как клиенты используют наш SWG

Безопасный доступ к Интернету от Cloudflare и Accenture для Агентства кибербезопасности и безопасности инфраструктуры (CISA) США

100+ **гражданских агентств США**

Узнать больше

с офисными локациями, защищенными с помощью фильтрации DNS от Cloudflare

Скандинавское консалтинговое агентство по ИТ и цифровым коммуникациям

«Мы рассчитываем, что Cloudflare уменьшит поверхность атаки за счет защиты наших портов, фильтрации угроз и очистки нашего трафика».

— Виктор Перссон, руководитель по безопасности операций

Читать пример использования

Японская компания по интеграции облачных сред и консультациям

4 тыс. **заблокированных запросов в неделю**

Читать пример использования

к опасному и нежелательному интернет-контенту среди сотен сотрудников

Пример сравнения с конкурентом: Cloudflare и Zscaler

Критерии	Cloudflare Gateway	Zscaler Internet Access
Архитектура	✓ Одна облачная платформа, Единая плоскость управления	✗ Много фрагментированных облачных сред много плоскостей управления
Интерфейс управления	✓ Единый интерфейс для всех SSE	✗ Отдельный для SWG и ZTNA
Проверка в один проход	✓ ДА для всех сервисов SSE	✗ Нет
Поддержка только IPv6	✓ Да	✗ Нет
Гарантия доступности по SLA	✓ 100 % для всех сервисов	✗ 99,999 % для большинства сервисов 99,9 % для DNS-резолвера

Продолжить сравнение Cloudflare и Zscaler

Более быстрая защита

13–58 %

быстрее для защищенного веб-шлюза (SWG)

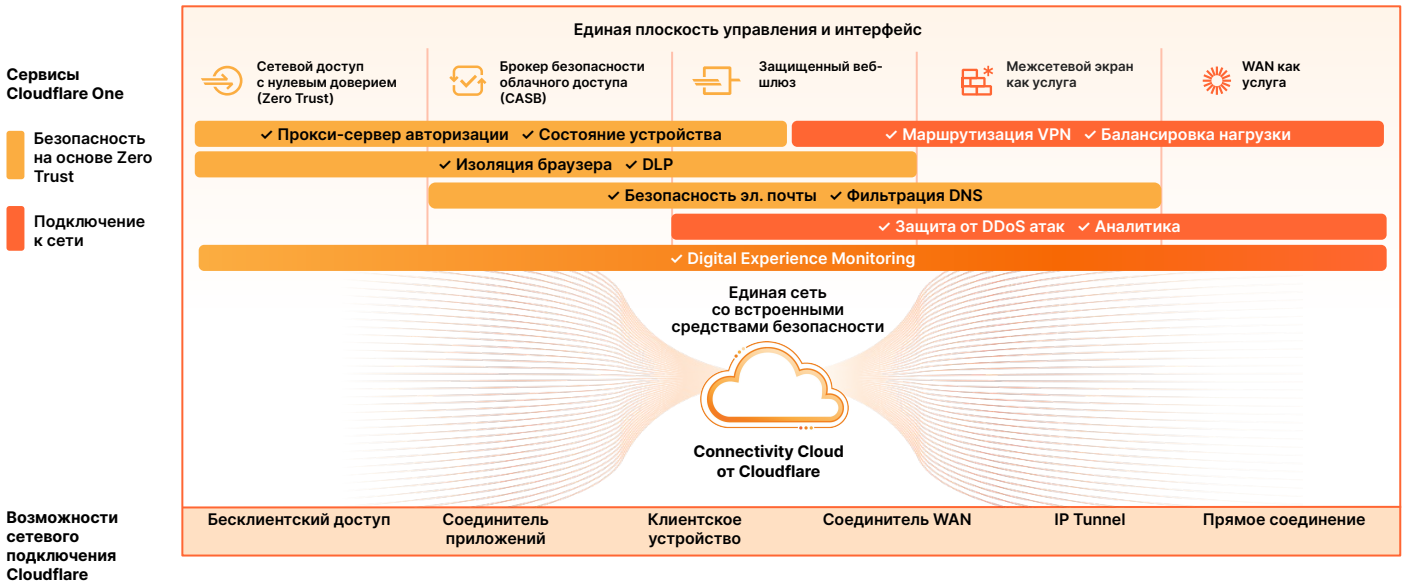
45-64%

быстрее для удаленной изоляции браузера (RBI)

На основании собственного тестирования и тестирования третьей стороной

Модернизация защиты с платформой SSE от Cloudflare

Cloudflare Gateway — это комбинируемый сервис на Cloudflare One, нашей платформе SSE. Начните создавать на основе SWG и расширьте возможности мониторинга и контроля благодаря взаимозаменяемым функциям безопасности платформы Cloudflare One в Интернете, а также в средах SaaS и частных приложений.

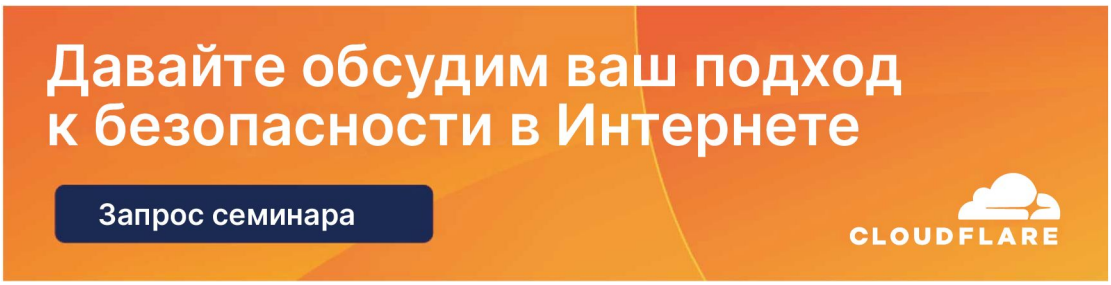


Единая унифицированная платформа

- **Безопасный доступ** за счет проверки и сегментирования любого пользователя по отношению к любому ресурсу
- **Защита от угроз** путем охвата всех каналов с помощью искусственного интеллекта/машинного обучения на основе анализа сети и сбора и анализа информации об угрозах
- **Защита данных** путем улучшения возможностей мониторинга сети и контроля данных при передаче, хранении и использовании

Единая программируемая сеть

- **Более эффективная** за счет упрощения сетевого сервиса и управления политикой
- **Более продуктивная** за счет обеспечения быстрого, надежного и последовательного удобства использования повсеместно
- **Более гибкая** за счет быстрого внедрения инноваций для удовлетворения растущих требований безопасности



Пока не готовы к беседе в режиме онлайн?

Продолжайте знакомиться с нашей эталонной архитектурой SASE, или узнайте, как это работает, посмотрев интерактивный тур по нашей платформе Zero Trust.