CLOUDFLARE

ОБЗОР ПРЕДЛАГАЕМЫХ РЕШЕНИЙ

Защитите свои конфиденциальные данные

Лучшая сетевая архитектура для более эффективной, продуктивной и гибкой защиты данных.

Унифицированная защита данных повсюду всему миру

Защита данных не является новой задачей, но переход к архитектурам гибридного облака наряду с быстрым внедрением ИИ создаёт новые проблемы:

- **93 % сотрудников** признают, что вводят информацию в инструменты ИИ без разрешения [1]
- **79 % стран** имеют законы о защите данных [2]

Cloudflare обеспечивает единообразные средства контроля на протяжении всего жизненного цикла ваших данных:

- **Безопасность повсюду:** обеспечьте единообразные средства контроля для веб-трафика, SaaS, электронной почты и облачного трафика.
- **Предотвращение эксфильтрации данных через ИИ:** анализируйте промпты генеративного ИИ, чтобы блокировать передачу конфиденциальных данных и контролировать использование ИИ.
- **Управление рисками данных:** выявляйте и контролируйте теневые ИТ- и ИИ-сервисы, а также сканируйте SaaS-и облачные приложения с помощью CASB.

«Появление всех этих несанкционированных инструментов искусственного интеллекта заставляет нас пересмотреть наш подход к безопасности». Сейчас мы рассматриваем SASE», — *руководитель отдела информационной безопасности,* ***AllSaints***

Почему SASE, а не корпоративная защита от утечек данных (DLP)?

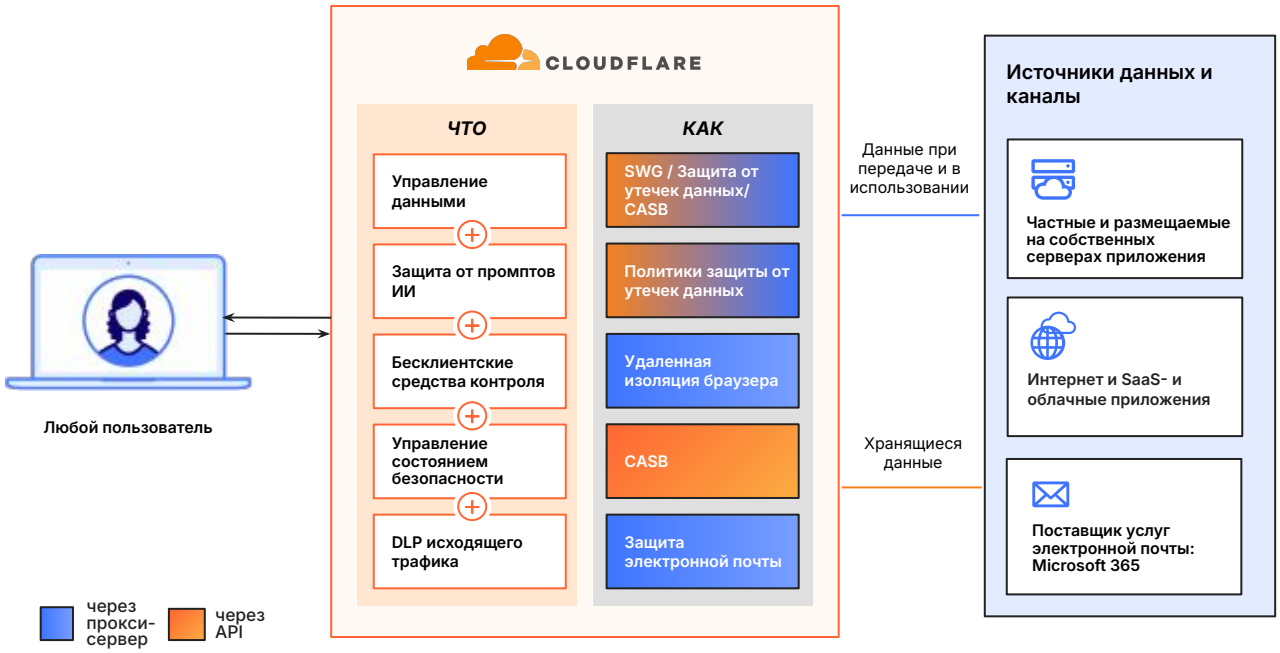
Платформа периферийного сервиса безопасного доступа (SASE) от Cloudflare создана для того, чтобы располагаться между вашими сотрудниками и каждым приложением и источником данных. Таким образом, SASE становится идеальной отправной точкой для начала комплексной защиты данных.

Независимо от того, получают ли сотрудники данные в SaaS-приложениях, загружают конфиденциальные файлы или общаются с помощью инструментов генеративного ИИ, платформа SASE от Cloudflare обеспечивает единообразный контроль безопасности при всех взаимодействиях с данными.

Как это работает

Платформа SASE от Cloudflare встроена в поток трафика между вашими сотрудниками и ресурсами, обеспечивая унификацию мониторинга и контроля.

Защита данных с использованием ИИ на платформе SASE от Cloudflare
в веб-трафике, трафике SaaS-приложений, почтовом трафике и облачном трафике



Встроенная защита данных в режиме реального времени

- **Гранулярная защита от утечек данных:** предотвращайте раскрытие конфиденциальных данных с помощью обнаружений с учетом контекста для персональной идентифицирующей информации, исходного кода, данных клиентов и др.
- **Защита от утечек данных в исходящей электронной почте:** автоматически помечайте конфиденциальные данные в исходящих электронных письмах, чтобы предотвратить случайные утечки данных.
- **Защита от промптов:** обнаруживайте и блокируйте рискованные промпты и ответы ИИ на основе намерения (например, попытки взлома, злоупотребление кодом, запросы персональной идентифицирующей информации).

Безопасный доступ и элементы управления клиента

- **Безопасный доступ к приложениям:** применяйте правила сетевого доступа с нулевым доверием (ZTNA) — такие как детализированное сканирование на утечки данных для подключений агентов ИИ — во всех корпоративных приложениях.
- **Проверки состояния устройств:** контролируйте доступ на основе детальных проверок состояния, таких как шифрование диска и включенная защита от утечек данных на конечных точках.
- **Бесклиентные средства управления:** применяйте средства управления данными на основе браузера для защиты стороннего доступа и политик использования личных устройств (BYOD) сотрудниками.

Риски, связанные с теневыми ИТ и состоянием безопасности

- **Обнаружение теневых ИТ/ИИ:** находите и управляйте теневыми ИТ/ИИ в вашей среде. Проводите количественную оценку рисков с помощью оценок доверия к приложениям и метрик передачи данных, чтобы быстро снижать их воздействие.
- **Управление состоянием безопасности:** сканируйте SaaS-приложения и облачные среды на предмет состояния безопасности. Примите предписанные меры для устранения выявленных проблем безопасности.
- **Управление тенантами:** блокируйте персональные тенанты SaaS-приложений, чтобы предотвратить эксфильтрацию данных.

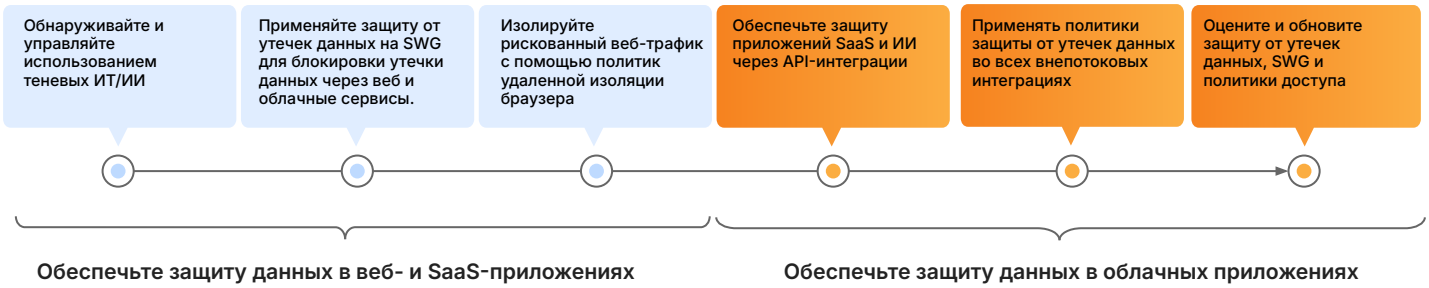
Интеграции и отчетность

- **Интеграции CASB:** бесшовно интегрируйтесь с ведущими платформами SaaS и ИИ (включая Microsoft 365, Google Workspace и ChatGPT) для сканирования CASB на основе API.
- **Интеграция Microsoft MIP:** постоянно синхронизируйтесь с метками Microsoft Information Protection (MIP) для обеспечения согласованности политик защиты от утечек данных.
- **Observability & форензика**: безопасно регистрируйте данные в выбранной SIEM для аудита или мгновенно анализируйте логи через информационную панель или API.

Пример процесса защиты данных

Начните с выявления теневых ИТ и использования искусственного интеллекта для оценки видимости поверхности атаки. Настройте основные политики защиты от утечек данных на SWG, чтобы блокировать утечку данных высокого риска из неконтролируемых облачных приложений, а также разверните удаленную изоляцию браузера для несанкционированного веб-трафика.

Затем разверните CASB, чтобы защитить санкционированные приложения SaaS и ИИ, исправляя ошибки конфигурации и обеспечивая соблюдение внутренних политик совместного использования. Уточните и интегрируйте детализированные политики защиты от утечек данных и доступа в SWG, электронной почте и CASB, дчтобы обеспечить автоматизированную и единую защиту по всем основным каналам передачи данных.



Примеры использования для начала работы

- **Блокируйте передачу персональной идентифицирующей информации и защищённой медицинской информации в режиме реального времени** через все несанкционированные каналы связи и хранения.
- **Защитите исходный код и интеллектуальную собственность** от кражи инсайдерами и от несанкционированного распространения.
- **Применяйте политики защиты промптов** для приложений генеративного ИИ, чтобы предотвратить утечку конфиденциальных данных и заражение моделей.
- **Предотвращайте ошибки конфигурации** и обеспечивайте детализированный контроль доступа во всех приложениях SaaS и ИИ.

Достижения клиентов

EESTI RAUDTEE

Поставщик инфраструктуры
Читать пример использования

Предотвратите потерю данных и устраните уязвимости в SaaS

путём выявления утечек данных и ошибочных конфигураций.

APPLIED

Страховые технологии
Читать пример использования

Изолируйте общедоступные инструменты генеративного ИИ, такие как ChatGPT,

чтобы заблокировать копирование и вставку конфиденциальных данных.

Flo

Ведущее приложение в сфере здравоохранения
Прочитать кейс-стади

Защитите данные пациентов

и обеспечьте соответствие требованиям с помощью безопасности электронной почты и модели Zero Trust.

CREDIT SAISON INDIA

Небанковский финансовый кредитор (NBFC)
Читать пример использования

Обеспечьте защиту персональной идентифицирующей информации и соблюдение нормативных требований,

чтобы предотвратить нежелательную утечку данных.

Готовы обсудить ваши потребности в защите данных?

Запросить семинар

1. Исследование Manage Engine, 2025 г.: Источник
2. Конференция Организации Объединённых Наций по торговле и развитию, 2025 г.: Источник

