CLOUDFLARE

КРАТКИЙ ОБЗОР ПРОДУКТА

Брокер безопасности облачного доступа (CASB)

Комплексный мониторинг и контроль над SaaS, ИИ и облачными средами — защита данных без замедления инноваций.

Безопасность SaaS для эпохи ИИ

Защитите свои SaaS, ИИ и облачные среды без снижения производительности. Мгновенно обнаруживайте неправильные конфигурации, теневые ИТ и риски данных в вашей гибридной рабочей среде с помощью Cloudflare CASB.

- **Автоматизация соблюдения нормативных требований.** Мгновенно обнаруживайте и устраняйте бреши в безопасности, такие как несанкционированный обмен файлами или уязвимая многофакторная аутентификация (MFA), в Microsoft 365, Google Workspace и GitHub.
- **Блокировка теневого ИИ/ИТ.** Обнаруживайте несанкционированные приложения и блокируйте доступ к несанкционированным облачным хранилищам или сайтам обмена файлами.
- **Безопасное использование ИИ.** Обеспечьте мониторинг внедрения инструментов ИИ и применяйте ограничения для клиентов на таких платформах, как ChatGPT и Gemini, чтобы обеспечить доступ только для корпоративных клиентов.
- **Управление рисками сторонних поставщиков.** Выявляйте и отзывайте рискованные сторонние интеграции, которые имеют доступ к вашим корпоративным данным.

Основанное на нашей глобальной сети, решение Cloudflare CASB с управлением через API и встроенной защитой обеспечивает быстрое и экономичное развертывание средств безопасности в любых масштабах.

Поставщик инфраструктуры

Выявленные уязвимости SaaS — например, широкий доступ к конфиденциальным файлам SharePoint — помогают предотвратить потерю данных.

Читать пример использования

Поставщик программного обеспечения для страхования

Безопасное внедрение генеративного ИИ путем блокировки ввода конфиденциальных данных в такие инструменты, как ChatGPT, без ущерба для производительности персонала.

Читать пример использования

Поставщик услуг телемедицины

Обеспечена защита конфиденциальных данных пациентов (PHI/HIPAA) и ускорен доступ для быстрорастущих удаленных сотрудников с помощью DLP и CASB.

Преимущества Cloudflare

Мгновенное развертывание без использования клиентов

Подключайтесь к SaaS и приложениям ИИ, таким как Microsoft 365, GitHub, Slack и ChatGPT, за несколько минут через API. Немедленное сканирование на наличие исторических рисков, неправильных конфигураций и утечек данных без установки клиентов.

Непрерывное управление состоянием SaaS и облачных данных

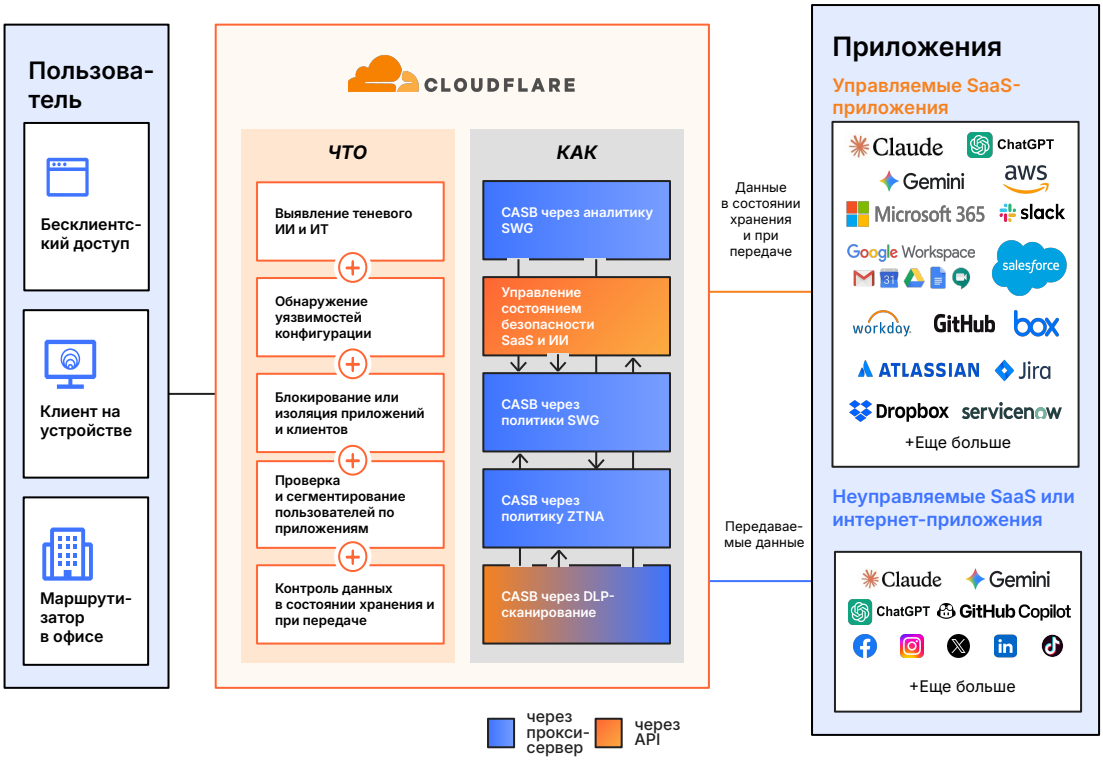
Выявляйте отклонения в системе безопасности и небезопасные настройки в SaaS и облачных хранилищах. Обнаруживайте и возвращайте критически важные ошибки в конфигурации, такие как общедоступные корзины S3 или открытые разрешения для проектов, до того, как они приведут к взлому.

Унифицированное управление теневыми ИТ

Хватит переключаться между консолями. Используйте аналитические данные CASB для обнаружения несанкционированных приложений, а затем мгновенно инициируйте политики Zero Trust для блокировки или изоляции этого трафика через Cloudflare Gateway, управляя всеми компонентами через единую информационную панель.

Хотите подробнее узнать об этом продукте? Ознакомьтесь с нашей эталонной архитектурой или обсудите с экспертом.

Комплексная безопасность для SaaS, ИИ и теневых ИТ



Как это работает

Многомодовый CASB от Cloudflare помогает обеспечить унифицированную облачную безопасность для SaaS-приложений. Для защиты хранимых данных есть простые API-интеграции, которые непрерывно сканируют используемые приложения на предмет уязвимостей и потенциальных угроз.

Наши средства управления доступом на основе Zero Trust (ZTNA), шлюза (SWG) и изоляции браузера (RBI) легко развертываются как встроенный CASB — сочетая простую настройку с надежной безопасностью.

Внеполосная защита данных и средства обеспечения безопасности SaaS (управляемые API)	
Управление состоянием безопасности SaaS (SSPM)	Сканируйте SaaS-приложения и облачные хранилища через API, чтобы обнаружить неправильные настройки и рискованные интеграции сторонних платформ (например, общедоступные корзины S3, неавторизованные приложения OAuth или нарушения MFA).
Защита данных SaaS (DLP)	Обнаруживайте конфиденциальные файлы (PCI, персональная идентифицирующая информация (PII), секреты) с помощью сканирования хранящихся данных и автоматически устраняйте нарушения (например, удаляйте общедоступные файлы), чтобы обеспечить соблюдение нормативных требований.
Встроенная защита данных (на основе прокси-сервера)	
Теневой ИИ и обнаружение ИТ	Мгновенный мониторинг несанкционированного использования приложений. Автоматически классифицируйте и блокируйте/изолируйте рискованные приложения (например, неодобренные конвертеры PDF или инструменты ИИ) на основе оценки надежности приложений.
Встроенные DLP и OCR	Обнаруживайте конфиденциальные данные в трафике с помощью Точного совпадения данных (EDM) и усовершенствованных классификаторов. Используйте оптическое распознавание символов (OCR), чтобы распространить эти средства защиты на изображения, блокируя утечку данных.
Защита промптов GenAI	Предотвратите вставку конфиденциальных данных (исходный код, персональная идентифицирующая информация (PII) клиентов) в общедоступные большие языковые модели (LLM). Проверяйте HTTPS-запросы к таким инструментам, как ChatGPT или Gemini, чтобы обеспечить безопасное использование ИИ.
Контроль клиента	Обеспечьте только корпоративный доступ для приложений, таких как Microsoft 365, Google Workspace и Slack, чтобы предотвратить вход в личные учетные записи на корпоративных устройствах.
Унифицированное управление	
Один клиент	При этом отдельный клиент CASB не требуется. Унифицированный клиент обрабатывает ZTNA, SWG и CASB с проверкой в один проход.
Оценка рисков пользователей	Выявляйте скомпрометированных пользователей путем сопоставления результатов CASB с поведенческими аномалиями для присваивания динамических оценок риска.
Отправка (push) журналов	Полное журналирование фиксирует все запросы, пользователей и устройства. Мгновенный экспорт журналов CASB в Splunk, Datadog или S3 для анализа SIEM.

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

REV:BDES-8793.2026JAN15