

Предотвращение утечек данных

Защитите конфиденциальные данные и обеспечьте соответствие нормативным требованиям в веб-, частных, SaaS-, облачных, ИИ-приложениях и приложениях электронной почты.

Самое интегрированное решение для предотвращения потери данных (DLP) в эпоху агентного ИИ

С Cloudflare DLP вы можете обнаруживать и блокировать утечку конфиденциальных данных по всей вашей сети и приложениям (SaaS, ИИ, облачных, частных и почтовых сервисах) без нарушения или снижения производительности пользователей.

Защитите свою интеллектуальную собственность, исходный код, персональную идентифицирующую информацию клиентов и другие данные, чтобы:

- **Обеспечивать соблюдение нормативных требований**, используя готовые профили для финансовых данных, медицинских карт и номеров социального страхования.
- **Защищать корпоративные данные**, заблокировав выгрузку конфиденциальных данных в неавторизованное облачное хранилище или на сайты обмена файлами.
- **Обеспечивать защиту промптов ИИ**, сканируя и редактируя конфиденциальные данные или исходный код во входных данных для таких инструментов, как ChatGPT и GitHub.
- **Обеспечивать возможность мониторинга перемещения данных** среди всех ваших сотрудников, работающих в гибридном формате.

Проверка происходит на глобальной периферии Cloudflare в миллисекундах от пользователя, обеспечивая быструю и экономичную защиту в масштабе.

Преимущества Cloudflare



Упрощение безопасности SaaS и ИИ

Контролируйте использование ИИ сотрудниками, блокируя подозрительный контент, и снижайте риски эксфильтрации за счет выявления и устранения конфиденциальных данных, хранящихся в SaaS и облачных средах.



Унифицированное управление политиками

Настройте профили DLP, записи обнаружения и метки конфиденциальности Microsoft Purview для консолидации защиты исходящего трафика, документов, PDF и изображений.



Адаптивные средства управления данными

Предоставляйте обратную связь по каждому обнаружению, чтобы обучить контекстному анализу на базе ИИ и повысить точность обнаружения. DLP адаптируется к вашим конкретным типам данных и трафику, чтобы уменьшить количество ложных срабатываний.



Поставщик инфраструктуры

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

[Читать пример использования](#)



Ведущий цифровой банк

Выполнено объединение средств безопасности на единой информационной панели, обеспечив строгое соблюдение нормативных требований и защиту от программ-шантажистов для банковской платформы банка, ориентированной на мобильные устройства.



Поставщик услуг телемедицины

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

Хотите подробнее узнать об этом продукте? Ознакомьтесь с нашей [эталонной архитектурой](#) или [обсудите с экспертом](#).

Защита данных по всем рабочим каналам

