Cloudflare AI Security Suite

Обеспечьте безопасное взаимодействие с ИИ посредством контроля данных и управления рисками на протяжении всего жизненного цикла ИИ.

Масштабируйте ИИ уверенно

Риски, связанные с ИИ, требуют современных средств безопасности

Ваши команды используют ИИ для более быстрого внедрения инноваций, однако это создает критические риски для безопасности. Старая тактика блокировки ИИ или добавления сложных точечных решений больше не работает, поскольку она подавляет инновации и игнорирует реальность:

- **85 % сотрудников** используют инструменты ИИ до того, как ИТ-служба успевает их проверить.[1]
- **93 % признают,** что вводят корпоративные данные в ИИ без разрешения.[2]
- **63 % организаций, подвергшихся утечкам данных, не имеют политики управления ИИ.**[1]

Научитесь давать вашим командам больше возможностей — и получать выгоду от повышения продуктивности с помощью ИИ — сохраняя при этом безопасность и контроль, необходимые вашему бизнесу.

Унифицированная платформа для защиты агентного и генеративного ИИ

Cloudflare предоставляет единую платформу, позволяющую вашей организации уверенно использовать ИИ. Мы даем руководителям по безопасности возможность управлять рисками, технологическим командам — повышать продуктивность, а инженерам платформ — создавать безопасные решения, обеспечивая совместное и защищенное внедрение инноваций.

Начните работу с Cloudflare AI Security Suite

Cloudflare AI Security Suite предоставляется на унифицированной платформе для обеспечения безопасности использования в рабочих пространствах инструментов ИИ и публично доступных приложений. Выявляйте теневой ИИ, защищайте модели от злоупотреблений, обеспечьте безопасный доступ агентов и предотвращайте утечку данных в промптах — чтобы ваша организация могла безопасно и эффективно осваивать инновации, с улучшенным мониторингом и усиленным контролем.

Расширьте возможности мониторинга

во всех ИИ-приложениях, конечных точках API и подключениях ИИ-агентов.

Нейтрализуйте риски

с помощью защитных барьеров, контроля состояния безопасности и нейтрализации угроз в режиме реального времени

Защищайте данные

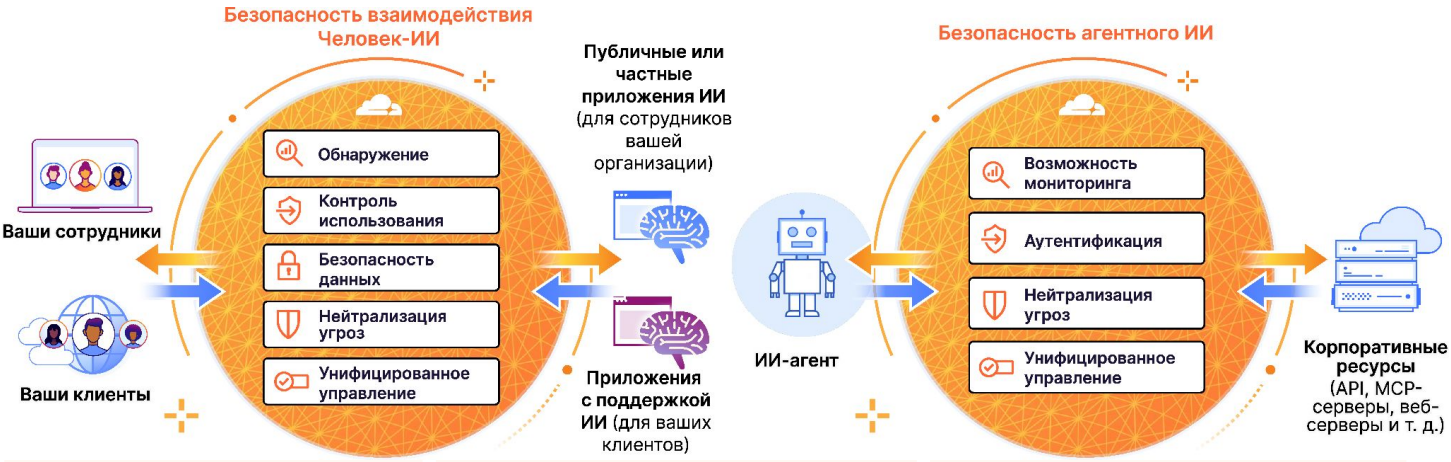
с помощью защиты от промптов и контроля доступа для сотрудников и агентов ИИ

Безопасность встроена
при разработке ИИ на Cloudflare.

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

Обеспечьте безопасное взаимодействие с генеративным и агентным ИИ с помощью Cloudflare AI Security Suite.

Обеспечьте безопасность всех взаимодействий с ИИ, контролируя данные, которые ваши сотрудники используют в генеративном ИИ, и управляя рисками безопасности, создаваемыми автономными агентами.

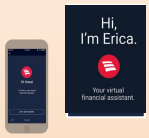


- **Ваши персонал:** сотрудники, подрядчики, разработчики и т. д.
- **Ваши клиенты:** посетители ваших веб-сайтов и приложений

- **Приложения генеративного ИИ**: автономные или встроенные

Gemini Claude ChatGPT Copilot

- **Приложения с поддержкой ИИ**
Пример: ИИ чат-бот Эрика от Bank of America



- **API** и **MCP-серверы** для любых приложений.

Google Workspace

- **Веб-серверы** для вывода данных и генерации ответов, дополненной результатами поиска (RAG)

Ускорьте внедрение ИИ со встроенной безопасностью на протяжении всего жизненного цикла ИИ

Обеспечьте безопасное использование ИИ для персонала

Внедряйте средства контроля использования ИИ и управление безопасностью ИИ (AI-SPM) для снижения рисков и защиты данных.

Защитите приложения на основе ИИ

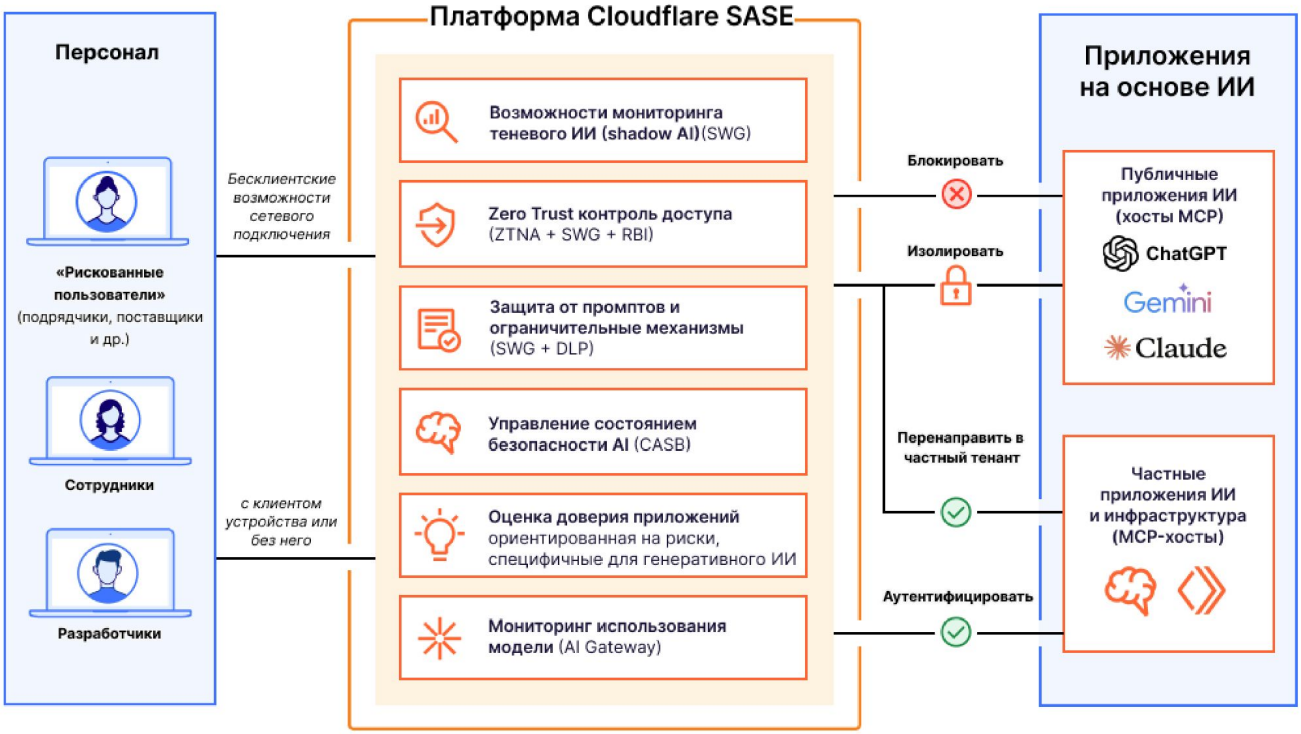
Защищайте свои приложения и API на базе ИИ от промпт-инъекций и утечек данных в режиме реального времени.

Разрабатывайте ИИ безопасно

Предоставьте разработчикам возможность безопасно создавать ИИ-приложения, используя интегрированные средства мониторинга, ограничение числа запросов и встроенные защитные барьеры на основе ИИ.

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

Обеспечьте безопасное использование сотрудниками ИИ-приложений и рабочих нагрузок на платформе SASE от Cloudflare



SSE для защиты взаимодействия человека с ИИ

- **Возможности мониторинга:** выявляйте и анализируйте использование теневого ИИ через встроенную инспекцию трафика. Оценивайте риски, создаваемые этими ИИ-приложениями, с помощью прозрачного скоринга.
- **Средства контроля доступа:** блокируйте, изолируйте, перенаправляйте или разрешайте подключения пользователей. Применяйте правила Zero Trust на основе идентификации для каждого приложения.
- **Защита от промптов и защитные барьеры**: обнаруживайте и блокируйте пользовательские промпты по намерению (например, попытки взлома, злоупотребление кодом, запросы персональной идентифицирующей информации).
- **Безопасность данных:** предотвращайте утечку конфиденциальных данных с помощью технологий ИИ для предотвращения потери данных (DLP) в отношении персональной идентифицирующей информации, исходного кода и многого другого.
- **Управление состоянием безопасности с помощью ИИ:** интегрируйте с инструментами генеративного ИИ через API для выявления неправильных конфигураций с помощью нашегоброкера безопасности доступа к облаку (CASB). Теперь доступно для ChatGPT, Claude и Google Gemini.

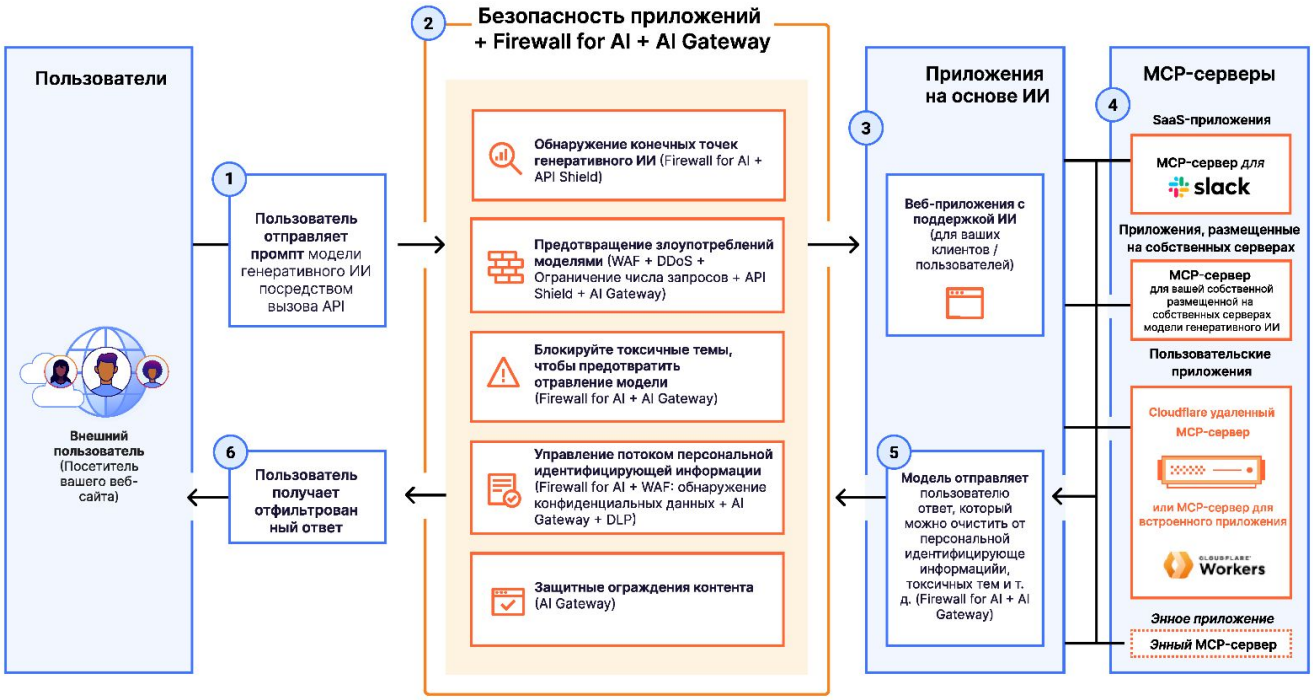
Порталы MCP-серверов для защиты обмена данными между ИИ и ресурсами

- **Возможности мониторинга:** агрегируйте все журналы запросов протокола контекста модели (MCP) для аудита и анализа. Проверяйте и утверждайте каждый MCP-сервер перед добавлением в портал.
- **Аутентификация:** обеспечьте проверку доступа пользователей к порталу на основе идентификации. Ограничьте доступ к MCP-серверам на основе принципа минимальных привилегий.
- **Подключения:** подключайте все доступные MCP-серверы с помощью одного URL-адреса вместо индивидуальной настройки каждого MCP-сервера.
- **Унифицированное управление:** применяйте те же детальные политики доступа для подключений ИИ, что и для подключений обычных пользователей.

Примечание: Порталы MCP-серверов поддерживают любой MCP-сервер, включая, помимо прочего, удаленные MCP-серверы, которые вы создаете или развертываете в Cloudflare. Эта функция доступна качестве средства управления сетевым доступом с нулевым доверием (ZTNA).

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

Защищайте приложения и рабочие нагрузки с поддержкой ИИ при помощи универсальной встроенной системы безопасности Cloudflare.



Защищайте общедоступный ИИ с помощью средств защиты приложений и Firewall for AI

- **Обнаружение конечных точек генеративного ИИ:** используйте автоматическое обнаружение всех моделей ИИ и API на ваших веб-ресурсах.
- **Защита моделей ИИ от злоупотреблений:** используйте специально разработанный Firewall for AI для блокировки внедрения вредоносных промптов, отравления моделей, чрезмерного использования и других угроз, способных обходить традиционные меры безопасности.
- **Контроль потоков персональной идентифицирующей информации:** сканируйте пользовательские промпты и ответы моделей, чтобы блокировать раскрытие конфиденциальных данных и обеспечивать соблюдение нормативных требований безопасности и соответствия.
- **Защитные барьеры для контента:** блокируйте небезопасные или вредоносные промпты, используя интегрированные модели, такие как Llama Guard. Создавайте настраиваемые правила WAF, чтобы легко блокировать или регистрировать подозрительные взаимодействия с ИИ.

Защитите создаваемый вами ИИ с помощью платформы для разработчиков и AI Gateway

- **Унифицированная панель управления ИИ:** управляйте всеми своими ИИ-приложениями из единой панели управления. Маршрутизируйте запросы, кэшируйте ответы, контролируйте затраты и отслеживайте производительность.
- **Защищайте учетные данные на периферии:** безопасно храните ключи API и секреты на периферии, предотвращая их раскрытие на стороне клиента и упрощая ротацию ключей между поставщиками.
- **Обеспечьте защитные барьеры для контента:** автоматически выявляйте и блокируйте / редактируйте вредоносный контент и персональную идентифицирующую информацию в промптах и ответах.

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

Cloudflare — единственный поставщик, обеспечивающий безопасность как публичных, так и приватных ИИ-сред

Установите надлежащие защитные барьеры, чтобы внедрять ИИ уверенно, обеспечивая безопасность, которая ускоряет ваши инновации, а не препятствует им.

- **Унифицированная защита экосистемы ИИ:** сложные стеки безопасности увеличивают риск. Используйте единую платформу для защиты данных и обеспечения соответствия требованиям на протяжении всего жизненного цикла ИИ.
- **Глобальная архитектура, ориентированная на будущее:** предотвращайте завтрашние угрозы уже сегодня с помощью защищенной от постквантового шифрования сети. Она масштабируется под любые объемы трафика, постоянно адаптируется к новым угрозам и программируется для поддержки новых сценариев использования.
- **Безопасность на базе ИИ:** наши системы защиты на базе ИИ анализируют промпты и ответы для обнаружения угроз в режиме реального времени.
- **Доказанное лидерство в области ИИ:** уверенно внедряйте инновации на платформе, которой доверяют 80 % ведущих компаний из списка 50 лучших в сфере генеративного ИИ.
- **Развертывание без привязки к модели:** средства контроля безопасности работают для всех ИИ-моделей в вашей среде, обеспечивая единый унифицированный подход к управлению развертываниями ИИ.

Что говорят клиенты

indeed

№ 1 сайт по поиску работы в мире
Читать пример использования

Выявляйте и контролируйте теневой ИИ

— параллельно с проектом замены VPN

APPLIED

Страховые технологии
Читать пример использования

Изолируйте общедоступные инструменты генеративного ИИ, такие как ChatGPT

— чтобы заблокировать копирование и вставку конфиденциальных данных

SaaS-компания с поддержкой ИИ:

Защищайте персональные идентифицирующие данные

— предотвращая отправку клиентами конфиденциальной идентифицирующей информации на общедоступные конечные точки генеративного ИИ

Cyndx

Финтех компания на основе ИИ

Снижение затрат на вывод на 95 %

— благодаря использованию Cloudflare для кэширования и выполнения ответов от провайдеров ИИ-моделей.

Готовы обсудить вопросы безопасности ИИ в вашей организации?

Свяжитесь с экспертом специалистом

1. Исследование Manage Engine, 2025 г.: Источник
2. Отчет IBM о стоимости утечки данных за 2025 г.: Источник

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