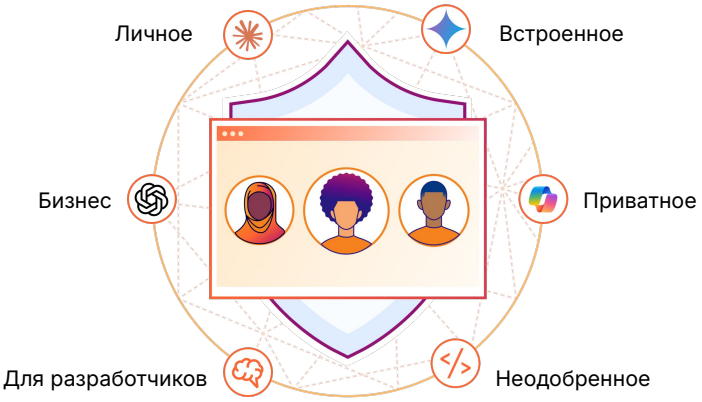
CLOUDFLARE

Обзор решения

Безопасное использование генеративного и агентного ИИ сотрудниками

Предоставьте своим командам возможность безопасно использовать любые инструменты ИИ благодаря защите, обеспечиваемой платформой SASE от Cloudflare.



Восстановите контроль, повысьте продуктивность

Стремительное внедрение ИИ ведет к увеличению рисков, включая утечки данных, нарушения нормативных требований и расширяющуюся поверхность атак. Полная блокировка ИИ напрямую приводит к потере конкурентных преимуществ, а эксперименты с отдельными решениями лишь добавляют сложностей.

Cloudflare обеспечивает защиту вашей организации при использовании ИИ, расширяя возможности мониторинга, снижая риски и обеспечивая комплексную защиту данных во всех средах ИИ:

- **Выявляйте теневой ИИ** и управляйте политиками для всех санкционированных и несанкционированных инструментов ИИ.
- **Укрепите систему управления ИИ** с помощью контроля доступа на основе идентификации и управления уровнем безопасности.
- **Предотвращайте утечку данных**, блокируя конфиденциальную информацию в пользовательских промптах, применяя тематические ограничители и проверяя инструменты ИИ на ошибки конфигурации.

Расширьте возможности Cloudflare для безопасного внедрения ИИ, независимо от того, включает ли ваша стратегия ограничение использования конкретными приложениями или эксперименты с более широким спектром инструментов.

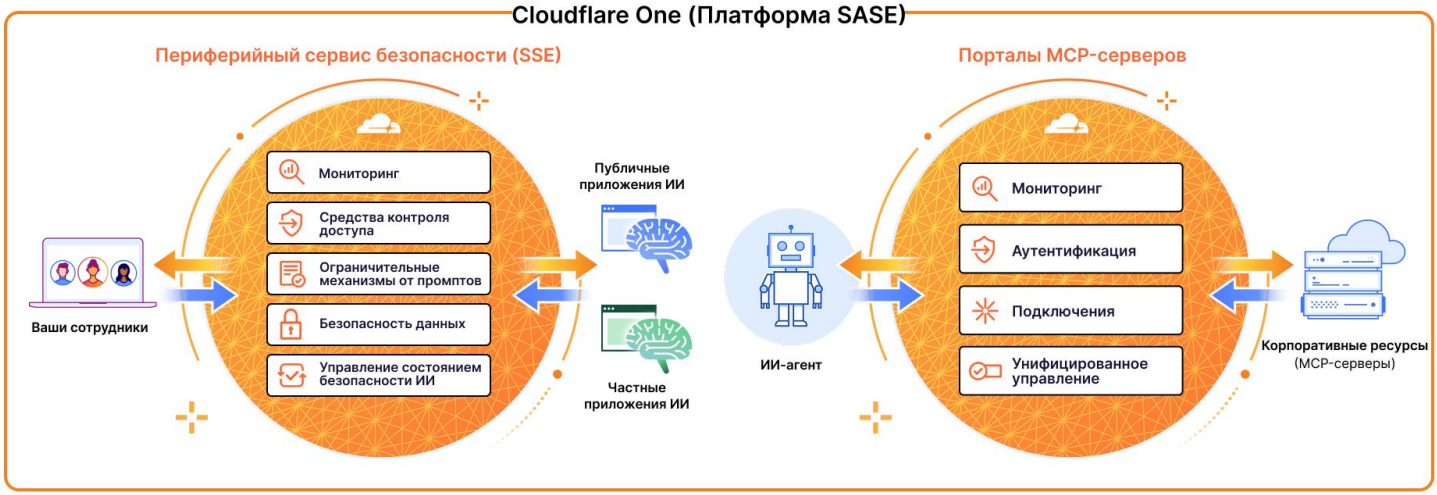
Зачем SASE для безопасного использования ИИ сотрудниками

Платформа периферийного сервиса безопасного доступа (SASE) от Cloudflare располагается между вашими сотрудниками и инструментами ИИ. Таким образом, SASE становится идеальной отправной точкой для многих, чтобы начать безопасно использовать ИИ.

Независимо от того, общаются ли сотрудники с ChatGPT или ИИ-агенты собирают информацию из корпоративных ресурсов, платформа SASE от Cloudflare обеспечивает согласованный контроль безопасности.

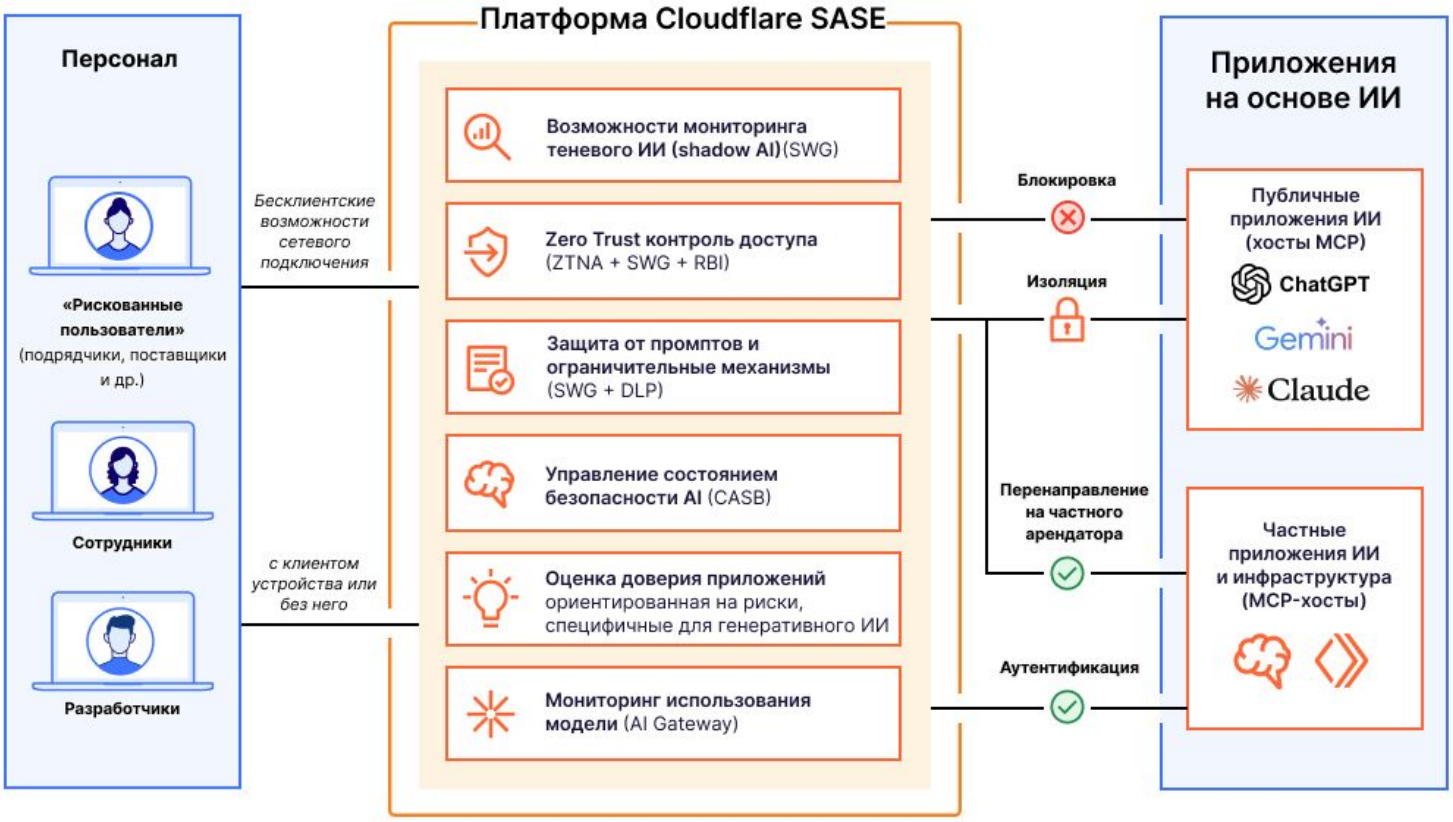
Безопасная коммуникация генеративного и агентного ИИ

Платформа SASE от Cloudflare предоставляет единую панель и унифицированную плоскость управления для взаимодействий между человеком и ИИ, а также между машинами во всей организации.



В отличие от других поставщиков SASE, Cloudflare также помогает подключать и защищать общедоступные приложения и рабочие нагрузки с поддержкой ИИ (такие как чат-бот на основе искусственного интеллекта на вашем веб-сайте или системы рекомендаций).

Защитите взаимодействие пользователей с приложениями генеративного ИИ
с помощью инструментов контроля использования ИИ на платформе SASE от Cloudflare



- **Возможности мониторинга:** выявляйте и анализируйте использование теневого ИИ с помощью встроенного анализа трафика. Оценивайте риски, связанные с этими приложениями ИИ, с использованием прозрачного скоринга.
- **Средства контроля доступа:** блокируйте, изолируйте, перенаправляйте или разрешайте подключения пользователей. Применяйте правила Zero Trust на уровне отдельных приложений.
- **Защита от промптов и ограничители:** обнаруживайте и блокируйте пользовательские промпты на основе намерений (например, попытки взлома, злоупотребление кодом, запросы персональной идентифицирующей информации).
- **Безопасность данных:** предотвращайте раскрытие конфиденциальных данных с помощью DLP-обнаружения на базе ИИ для персональной идентифицирующей информации, исходного кода и многого другого.
- **Управление состоянием безопасности ИИ:** интегрируйте инструменты генеративного ИИ через API (в настоящее время доступно для ChatGPT, Claude, Google Gemini) для проверки конфигураций на ошибки с помощью нашего брокера безопасности облачного доступа (CASB).

Достижения клиентов

indeed
Крупнейший в мире сайт по поиску работы

Выявление и контроль теневого ИИ

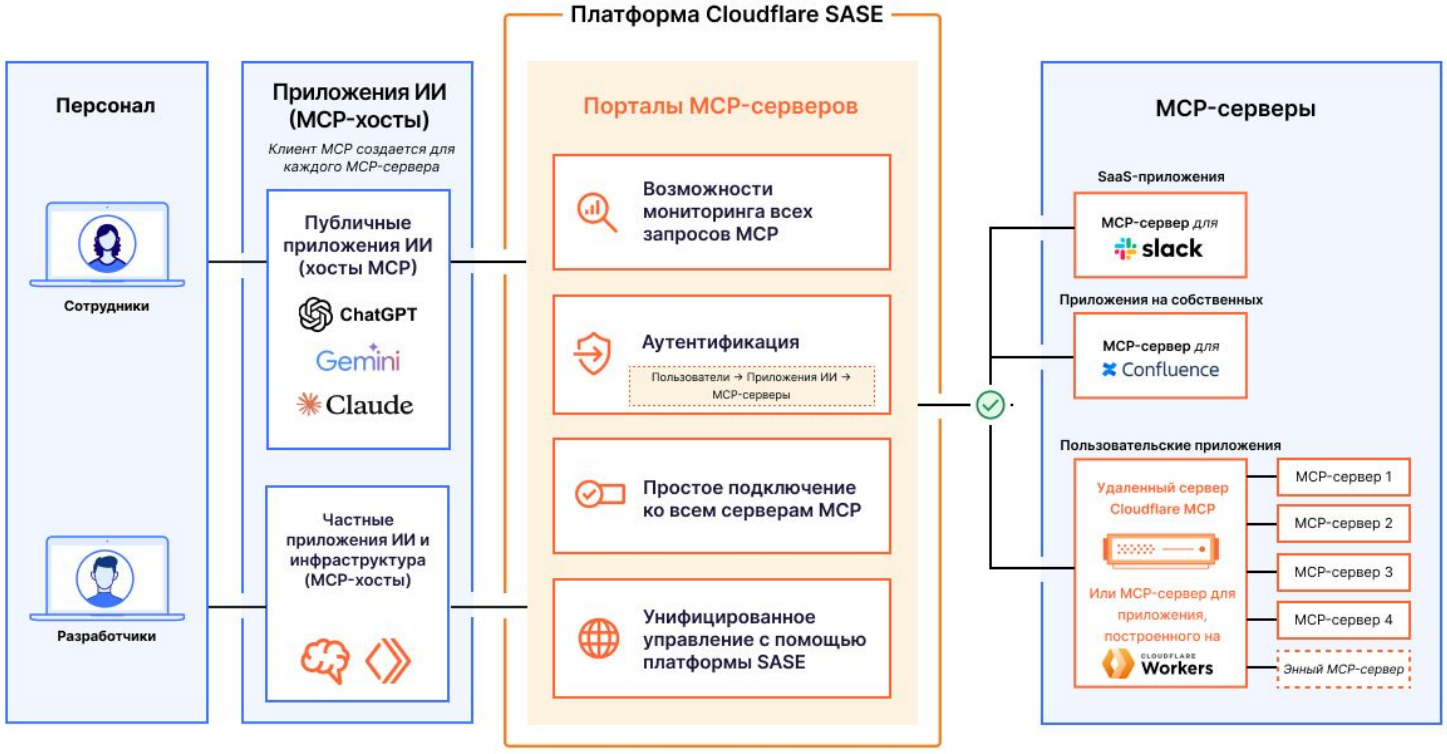
параллельно с проектом замены VPN.

APPLIED
Страховые технологии

Изоляция общедоступных инструментов генеративного ИИ, таких как ChatGPT,

для предотвращения копирования и вставки конфиденциальных данных

Обеспечьте безопасное взаимодействие агентного ИИ (AI-to-resource) через порталы MCP-серверов на платформе SASE от Cloudflare



- **Возможности мониторинга:** Агрегируйте все журналы запросов протокола контекста модели (MCP) для аудита и анализа. Просматривайте и утверждайте каждый MCP-сервер перед добавлением в портал.
- **Аутентификация:** аутентификация доступа пользователей к порталу на основе идентификации. Ограничьте доступ к серверам MCP на основе принципа наименьших 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 к подключениям ИИ, что и к пользователям.
- **Настройте инструменты для каждого портала:** Выберите конкретные инструменты и шаблоны промптов, доступные для каждого пользователя.

Примечание: порталы MCP-серверов Cloudflare поддерживают любые MCP-серверы, включая удаленные, созданные или развернутые на Cloudflare. Эта функция доступна как элемент контроля сетевого доступа с нулевым доверием (ZTNA).

Узнайте больше о нашем видении в этом блоге.

Готовы узнать, как Cloudflare помогает безопасно использовать ИИ?

Запросить семинар

 | +44 20 3514 6970 | enterprise@cloudflare.com | Cloudflare.com