Платформа AITalon

AITalon AIGate

Единая платформа управления AI-доступом, политиками безопасности моделей и агентов и контроль биллинга

AIGate ставит понятный контроль между сотрудниками, AI-агентами и внешними моделями: проверяет запросы, скрывает чувствительные данные и сохраняет полный журнал действий.

1	100%	0
Единая точка входа	Полный журнал действий	Прямых ключей в приложениях

Единая точка управления AI-доступом и политиками

AIGate разделяет управляющий и исполнительный контуры, чтобы централизованно управлять доступом, политиками, аудитом и биллингом без перегрузки прикладных систем.

Управляющий контур AIGate

- ✓ **Защита от утечек:** Персональные данные, ключи, секреты, лимиты и настройки доступа остаются в защищенном контуре.
- ✓ **Понятное масштабирование ИИ:** Встраивание в вашу архитектуру ИИ станет значительно легче через включение компонентов шлюза как безопасного барьера.

Контур исполнения и шлюзы

- ✓ **LLM Gate:** Применяет лимиты, проверки запросов и маршрутизацию к провайдерам через совместимый API.
- ✓ **Agent Gate и Edge:** Контролируют MCP, API и действия агентов с изоляцией, auth и понятным журналом.

Единая точка входа для LLM, API и MCP

Один контур доступа снижает хаос интеграций: запросы проходят через проверку, маршрутизацию и сервисную аутентификацию до обращения к модели или приложению.

Маршрутизация и совместимость

- ✓ **Один API для команд:** Поддержка общих точек входа для сотрудников, приложений, LLM и AI-агентов.
- ✓ **Гибкие маршруты:** Переключение между провайдерами, моделями и бэкенд-сервисами без переписывания клиентского кода.

Пограничная защита

- ✓ **Проверка доверия:** На входе удаляются поддельные служебные заголовки и применяется единая схема сервисной аутентификации.
- ✓ **Безопасное расширение:** Edge-контур поддерживает HTTP, API и MCP-сценарии с изоляцией контуров и применением политик на лету.

Защита данных и политик безопасности

AIGate проверяет входящие и исходящие данные до модели: маскирует чувствительную информацию, блокирует рискованные запросы и фиксирует причины срабатывания.

Проверка запросов и ответов

- ✓ **Маскирование данных:** Телефоны, email, PII, секреты и коммерческая тайна скрываются до отправки во внешнюю модель.
- ✓ **Контроль контента:** Политики выявляют prompt injection, обход защит и запрещенные сценарии до выполнения запроса.

Режимы применения

- ✓ **Наблюдение / Маскирование / Блокировка:** Политики можно включать поэтапно: сначала видеть срабатывания в журнале, затем скрывать чувствительные данные и блокировать подтвержденные риски.
- ✓ **Единый формат ответов:** Разные провайдеры и модели приводятся к одному интерфейсу для приложений и команд.

Контроль AI-агентов и инструментов

Платформа позволяет подключать MCP и API как управляемые инструменты для агентов, не отдавая им прямой и бесконтрольный доступ к корпоративным системам.

MCP и API под контролем

- ✓ **Подключение инструментов:** Корпоративные сервисы и API публикуются как управляемые MCP- и API-точки.
- ✓ **Явные разрешения:** Агент получает только те действия, маршруты и методы, которые разрешены политикой.

Ограничение последствий

- ✓ **Временные окна и режимы:** Запись, удаление и чувствительные операции можно разрешать только в нужные интервалы и роли.
- ✓ **Защита от runaway-сценариев:** Платформа ограничивает повторные вызовы, цепочки инструментов и несанкционированные изменения.

Ограничение рискованных действий агентов

AIGate не дает агенту выходить за пределы разрешенных действий: политика определяет, что можно читать, что можно менять и какие операции должны блокироваться сразу.

Что блокируется политикой

- ✓ **Опасные изменения:** Удаление, массовое обновление, restart и другие чувствительные write-операции можно запрещать на уровне маршрута и метода.
- ✓ **Выход за рамки доступа:** Обращения к неразрешенным инструментам, MCP-методам и API-маршрутам отсекаются до выполнения действия.

Что получает бизнес

- ✓ **Явные границы для агента:** Агент работает только в рамках разрешенных инструментов, ролей и временных окон.
- ✓ **Понятный разбор инцидентов:** Полный журнал событий и причин блокировки упрощает расследование и настройку политики.

Быстрое подключение команд и разработчиков

AIGate снимает хаос с ключами и ручными настройками: команды получают единый доступ к AI через знакомые интерфейсы и централизованные правила.

Удобное внедрение

- ✓ **Совместимость с клиентами:** Один адрес и единый способ подключения для IDE, внутренних сервисов и прикладных команд.
- ✓ **Роли и доступ:** SSO, RBAC и интеграции управляются централизованно, без раздачи секретов по рабочим местам.

Контроль среды

- ✓ **Безопасные песочницы:** Можно разделять прод, пилоты, стенды и команды без смешения трафика и политик.
- ✓ **Полная журнализация:** Запросы, ответы, tool-вызовы и служебные события доступны для ИТ, ИБ и расследований.

Понятные политики вместо разрозненных настроек

Интерфейс AIGate позволяет задавать политики простыми действиями: разрешить, замаскировать, отправить на согласование или заблокировать.

Публикация без простоя

- ✓ **Версионирование правил:** Каждое изменение собирается в снимок конфигурации и безопасно публикуется на исполнительные узлы.
- ✓ **Пошаговое включение:** Политику можно проверить в режимах наблюдения и предупреждения перед жестким включением.

Понятные действия политики

- ✓ **Разрешить / Маскировать / Блокировать / Согласовать:** Поведение правила ясно видно в интерфейсе без погружения в сложный DSL.
- ✓ **Гибкость для ролей:** Разные наборы правил применяются к моделям, агентам, интеграциям и пользователям.

Аудит, аналитика и контроль затрат

Платформа показывает, кто использует AI, что именно происходит в LLM и agent-контуре и во сколько это обходится компании.

Сквозной аудит

- ✓ **Полная трассировка:** Запросы, ответы, tool-вызовы, блокировки и служебные события связываются одним контекстом.
- ✓ **Отчетность для ИТ и ИБ:** Экспорт, расследование инцидентов и интеграция с SIEM строятся на едином журнале.

Финансовый контроль

- ✓ **Лимиты и бюджеты:** Ограничения задаются по пользователям, моделям, периодам, ключам и командам.
- ✓ **Прозрачность расходов:** Видно потребление токенов, стоимость, причины перерасхода и источники нагрузки.
- ✓ **Теневые режимы:** Можно сначала собирать сигналы и предупреждения без блокировки рабочих процессов.

Поэтапное внедрение в локальный и защищенный контур

AIGate подходит для пилота, демо и продуктивной эксплуатации: платформу можно запускать в локальном контуре, в частном облаке или на инфраструктуре заказчика.

Тестовые стенды и пилоты

- ✓ **Локальные полигоны:** Отдельные стенды помогают проверить политики, маршруты, аудит и биллинг до выхода в продуктив.
- ✓ **Smoke и диагностика:** Контрольные проверки подтверждают готовность сервисов перед подключением реальных пользователей.

Размещение для enterprise

- ✓ **Локальный контур и частное облако:** Конфиденциальные данные, политики и журналы остаются в контролируемом контуре компании.
- ✓ **Изоляция контуров:** Можно разделять команды, дочерние компании и tenants в одном развертывании.

AI в компании под контролем

AIGate переводит AI из экспериментов в управляемую корпоративную систему: с понятным доступом, защитой данных, аудитом действий агентов и контролем расходов.