qCloudy

qGateway

чего не хватает вашему корпоративному ИИ



Артем Прима
Developer Advocate
qCloudy

qCloudy

Локальная команда, глобальная практика

5 лет

на Cloud и AI проектах в Казахстане

50+

сертификаций AWS у команды

100+

проектов на AWS

AWS Advanced Tier Partner

Первый локальный в Центральной Азии

AWS AI Competency

Подтверждённая экспертиза в AI/ML

AWS Authorized Reseller

Ресурсы AWS в тенге, по договору с местным юрлицом

qCloudy

ИИ уже используется — вне контура и без правил

Доступ находят сами

Claude уже стоит на личных устройствах и оплачивается с личных карт

Нечего показать на проверке

Нет журнала: кто и какие данные передавал в модель

Утечка в открытом виде

Запрос с ИИН или служебной информацией уже не отозвать

Запрет не снижает риск — он снижает видимость.

КРИТЕРИИ ПРОВЕРКИ

Четыре вопроса к использованию ИИ

01 · ДОСТУП

Кто имеет доступ?

Какие модели и инструменты разрешены каждой группе?

02 · ДАННЫЕ

Какие данные покидают контур?

Какие данные заменяются метками или блокируются до отправки?

03 · РАСХОДЫ

Сколько это стоит?

Как учитываются расходы и где задаются лимиты?

04 · АУДИТ

Как ИБ узнает о нарушении?

Какие события защиты поступают в SIEM?

РЕШЕНИЕ

qGateway контролирует доступ и данные

ДОСТУП

Корпоративный вход

Модели и инструменты доступны по группам IdP.

ЛИМИТЫ

Расходы под контролем

Учёт использования и лимиты по организации, подразделениям и сотрудникам.

АУДИТ

События защиты в SIEM

ИБ видит, кто отправил запрос, какой тип данных обнаружен и как сработала политика.

ЗАЩИТА ДАННЫХ

Персональные данные

qShield заменяет обнаруженные данные метками до отправки в модель или блокирует запрос.

КАК ЭТО РАБОТАЕТ

Где проходит граница периметра

КЛИЕНТЫ

Claude
Desktop · Code · модели Claude

Codex BETA
Только модели OpenAI

qChat BETA
Модели по правам группы

qGateway в периметре

- Корпоративный вход через IdP
- Модели и права по группам
- Лимиты: компания, отдел, сотрудник
- Учёт расходов и использования
- qShield: обработка до модели
- Журнал аудита и события в SIEM
- Каталог MCP и плагинов

РАЗМЕЩЕНИЕ МОДЕЛЕЙ

Amazon Bedrock
Claude, GPT, DeepSeek, Qwen, Mistral

Локальная LLM
В ЦОД заказчика

qCloudy

Как обрабатываются персональные данные

Claude Desktop / Code

Подтверди получение заявки.

ИИН: 000000000000

→

qGateway в периметре

Проверяет запрос перед отправкой

qShield

Заменяет ИИН меткой [ИИН_1]

→

Amazon Bedrock

Подтверди получение заявки.

ИИН: [ИИН_1]

Условный пример. Исходный ИИН остаётся в периметре.

Что получает сотрудник после проверки

Запрос прошёл проверку

Модель отвечает на обработанный запрос. Например: «Заявка получена».

В ответе есть обратимая метка

qGateway может подставить исходное значение внутри периметра.

Значение скрыто или хешировано

Скрытая часть значения не восстанавливается.

Запрос заблокирован

qGateway останавливает запрос до вызова модели.

Пример условный. Результат зависит от политики обработки данных.

qCloudy

Как Claude получает настройки

Консоль qGateway

ИТ назначает профиль группе. В профиле задаются модели и инструменты.

→

Доставка настроек

ИТ развёртывает настройки через MDM или другой поддерживаемый способ управления клиентом.

→

Claude Desktop / Code

Клиент получает настройки от шлюза при входе и применяет их на устройстве сотрудника.

IdP и доступ

Сотрудник входит корпоративной учётной записью. qGateway использует группы, чтобы проверить доступ к моделям и инструментам.

КОРПОРАТИВНАЯ ИНТЕГРАЦИЯ

Инструмент для ИБ

qShield

Применяет политику.
В примере ИИН заменён меткой [ИИН_1].

→

qGateway

Фиксирует, кто и когда отправил запрос, тип данных и результат проверки.

→

Корпоративная SIEM

Получает событие. ИБ использует его для мониторинга и разбора.

Пример события

10:42 · сотрудник А · тип данных: ИИН · действие: токенизация.
События шлюза передаются в SIEM как метаданные, без текста запроса.

qCloudy

Как qGateway защищает данные

Шлюз в периметре

Политики, настройки и журналы хранятся у заказчика.

Защита до модели

qShield обрабатывает обнаруженные ИИН, ФИО и реквизиты.

Fail-closed

При сбое проверки запрос не отправляется в модель.

Вход через IdP

Корпоративная учётная запись без раздачи AWS-ключей.

SIEM и оповещения

События поступают в SIEM и ответственному за комплаенс.

Журнал аудита

Запросы, отказы и действия администраторов.

99,9% SLA
Доступность по договору

Поддержка 8/5
24/7 по запросу

50+ сертификаций AWS
у команды qCloudy

qCloudy

Кто использует ИИ и сколько это стоит

Расходы

Разбивка по моделям, подразделениям и сотрудникам.

Лимиты

Для организации, отдела и сотрудника. Видно, кто достиг лимита.

Активность

Запросы, активные сотрудники и срабатывания защиты.



Демонстрационные данные. Сумма не является тарифом.

КОММЕРЧЕСКАЯ МОДЕЛЬ

Подписка и фактическое потребление

QGATEWAY

За пользователя

Подписка рассчитывается по числу пользователей

МОДЕЛИ

По тарифам AWS

Оплата за фактическое потребление моделей

ЗАКУПКА

Договор в Казахстане

Договор, тендер или госзакупки. Оплата в тенге.

AWS GenAI Funding — софинансирование старта по одобренной заявке

qCloudy готовит заявку на софинансирование. Условия и объём подтверждаются AWS.

ВНЕДРЕНИЕ

Четыре этапа до промышленной эксплуатации

01

Дизайн контура

Типы данных и режимы обработки, группы AD, критерии приёмки

02

Развёртывание

Шлюз в контуре, AD и журнал. HSM — по требованиям заказчика.

03

Первое подразделение

Реальные запросы, лимиты, разбор блокировок с ИБ

04

Вся организация

Остальные подразделения, общие навыки, плагины и подключения к системам

Один контрагент на полный цикл: договор, внедрение, разработка под ваши процессы и поддержка.

ВОПРОСЫ

Корпоративный ИИ под контролем ИБ

Проверим на вашем сценарии?

gateway.qcloudy.kz

sales@qcloudy.io

+7 700 333 8990

+7 700 555 8990

Наведите камеру телефона

qCloudy

qCloudy

Четыре режима обработки данных

Tokenize — заменить меткой

ИИН → [ИИН_1]. Соответствие хранится в периметре. Значение можно вернуть в ответ сотруднику.

Hash — вычислить отпечаток

ИИН → 9f2a… . Обратная подстановка из хеша не предусмотрена. Сравнение зависит от настроек.

Mask — показать часть

ИИН → ********9012. Видна только разрешённая часть, поэтому Mask доступен не для всех типов данных.

Block — остановить запрос

Обнаружен запрещённый тип данных — запрос не отправляется в модель.

ЦЕННОСТЬ ДЛЯ РОЛЕЙ

Каждая функция получает своё

ИТ / СТО

Доступ и установка у сотрудников из одной консоли — без нагрузки на команду

ИБ

qShield обрабатывает обнаруженные чувствительные данные до отправки запроса в модель.

КОМПЛАЕНС

Аудит использования ИИ и настройки под внутренние политики

ФИНАНСЫ

Лимиты по подразделениям и оплата в тенге по договору в РК

qCloudy

Модели, клиенты и размещение

КЛИЕНТ	МОДЕЛИ И РАЗМЕЩЕНИЕ
Claude Desktop и Claude Code Документы и разработка	**Claude в Amazon Bedrock** В AWS-аккаунте организации
Codex BETA Инструмент для разработки	**Только модели OpenAI** Например, GPT
qChat BETA Чат с несколькими моделями	**Облачные и локальные модели** Claude, GPT, DeepSeek, Qwen, Mistral или локальная LLM

qCloudy

Персональные данные и ИИ: требования в РК

Закон № 94-V о персональных данных

ИИН и ФИО заменяются метками до отправки, шлюз в вашем контуре

ПП РК № 832

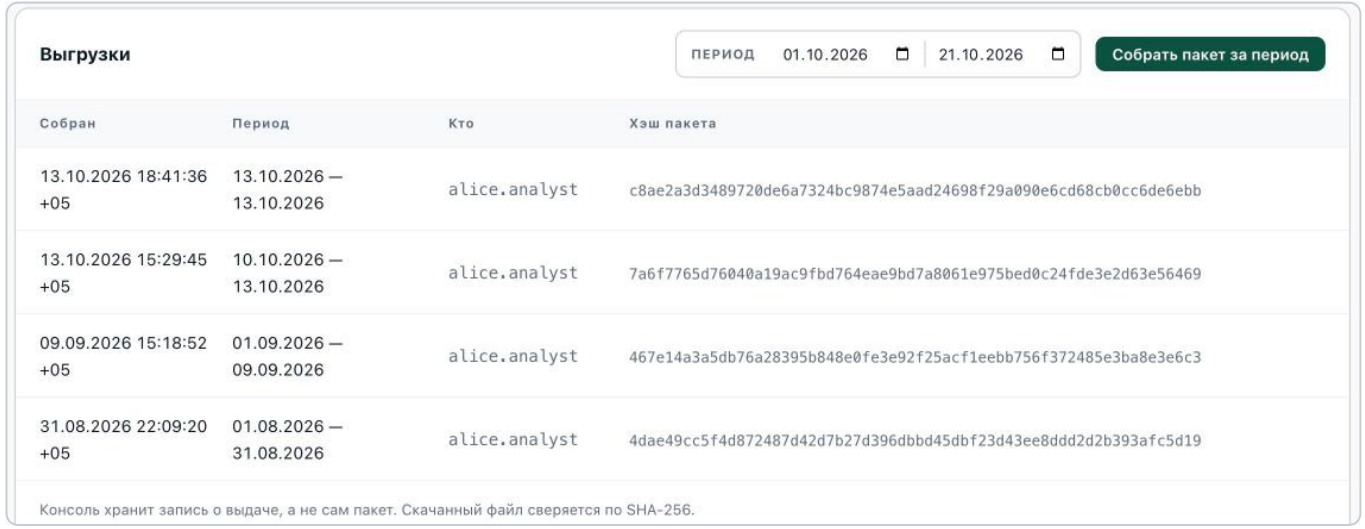
Доступ по группам AD, журнал в вашем SIEM

Закон об ИИ № 230-VIII

ИИ под контролем организации, с защитой персональных данных

Банковская тайна, тайна связи

Соответствие меток и значений — только в периметре



ЧТО ПОКАЗЫВАЕМ НА ПРОВЕРКЕ

- ✓ Журнал: кто, когда, тип данных
- ✓ Отчёт по доступам и группам AD
- ✓ Политика обработки по типам данных
- ✓ Документы о размещении шлюза в контуре

qCloudy

Что подготовить ИТ и ИБ заказчика

Площадка и сеть

Место размещения, DNS и TLS, сетевые маршруты к моделям и канал настройки клиентов.

Корпоративный вход

Подключение IdP, тестовые учётные записи и группы. Матрица доступа к моделям и инструментам.

Политики данных

Типы защищаемых данных, выбранные режимы, тестовые примеры и критерии приёмки.

Журнал и реагирование

Приёмник SIEM, доступ к журналам, сроки хранения и ответственные за разбор событий.

qCloudy

Как сотрудники подключаются к моделям

КЛИЕНТ	ШЛЮЗ	МОДЕЛИ
Claude Desktop и Claude Code Документы и разработка	**qGateway** Доступ и политики	**Claude** Рабочий поток · Amazon Bedrock
Codex BETA Инструмент для разработки	**qGateway** Доступ и политики	**Только модели OpenAI** Например, GPT
qChat BETA Чат с несколькими моделями	**qGateway** Доступ и политики	**Разрешённые модели** По правам группы, облачные или локальные

qCloudy

Что уточнить при техническом воркшопе

Вложения и OCR

Распознавание текста в сканах и изображениях перед применением политики данных.

HSM и PKCS#11

Хранение ключа в HSM и подключение через PKCS#11. Уточнить устройство и порядок работы с ключами.

Инструменты и MCP

Результаты инструментов проходят ту же проверку, что и запрос. MCP-серверы подключаются из каталога и доступны по группам.

Guardrails и хранение

Контентная политика Bedrock Guardrails, регион обработки, срок жизни меток и хранения событий.

Контроль после подключения сотрудников

Модели по группам

Согласовать доступные модели и инструменты для каждой группы сотрудников.

Политики ИБ

Определить типы данных для обезличивания и блокировки. Назначить ответственных за события.

Расходы

Задать лимиты на организацию, подразделения и сотрудников. Контролировать предупреждения.

MCP и плагины

Вести общий каталог подключений, назначать владельцев и отключать ненужные инструменты.