Архитектура, която може да бъде проверена.

Публичната демонстрация е отделена от клиентските системи. Идентичността и правата върху документите се проверяват, преди съдържанието да достигне модела.

Контролирано търсене и отговор

Идентичност Удостоверен потребител и разрешена организация	**Търсене** Проверка на правата преди класиране	**Модел** Одобрен контекст, ограничен отговор, без инструменти	**Преглед** Източници, ограничения и одитно събитие

Приемането започва с разрешени източници, ограничена обработка, произход, класификация и индексиране. Променени документи или права изискват обновяване на индекса и достъпа.

Граници на доверие

Граница	Необходим контрол
Браузър към приложение	TLS, удостоверена сесия, валидация, проверка на произхода и лимити
Приложение към данни	Частна мрежа, минимални права, филтри по организация и документ
Приложение към модел	Фиксиран адрес, времеви лимит, ограничени токени и отделена мрежа
Експлоатация към система	MFA, преглед на ролите, журнал, контролирана поддръжка и възстановяване

Моделите са заменяеми; проверката е задължителна

Адаптерите позволяват локално изпълнение без обвързване с един модел. Кандидатите се избират според задачите и лицензите. Българският и английският се оценяват отделно, включително таблици, терминология, липсващи доказателства и точност на цитатите.

Режимът само с търсене показва пасажи, без да твърди, че модел е генерирал отговор. Включването на модел променя поведението и изисква оценка преди продукционна употреба.

Какво не доказва тази архитектура

Локалното разполагане не премахва инжектиране на инструкции, отравяне на източници, грешки в правата или оперативен риск. Извлеченият текст е недоверен вход. Изходът на модела се обработва като текст и се преглежда преди значими действия. Материалът не е сертификат или специфична клиентска оценка за сигурност.