

Bletchley Park : l'IA locale garde vos secrets au manoir

Ultra décodait sur place et rien n'en sortait. Vos agents IA peuvent faire de même : quelles données traitez-vous, et où ?

Le débat n'est plus « cloud ou local », c'est « quelles données, et où ? »

■ MESSAGE CLÉ

La fuite moyenne coûte un record de 4,99 M\$ et 1 fuite sur 4 est activée par l'IA. Avec Muse Glimmer (30B, 24 Go de VRAM), la puissance souveraine tient dans un poste standard : le lieu de traitement redevient une décision de commandement.

- 1 Ultra s'est décodé sur place : la machine dans le manoir, le matériau entrant par des canaux contrôlés.
- 2 Le débat n'est pas cloud ou local : c'est quelles données traitons-nous, et où.
- 3 Un agent local sans RAG à jour est une Bombe sans interceptions : le matériau décide de l'utilité.
- 4 La souveraineté n'est pas l'autarcie : gateway = Y-stations, classification = compartimentage.

Le manoir d'IA locale protège vos trois leviers de direction à la fois

CROISSANCE

Agents always-on, hors ligne

Résumés d'appels, clauses, scoring de pipeline tournent en client, en avion, sous VPN coupé : le travail continue partout.

IMPACT 24 Go de VRAM suffisent

RISQUES

Ce qui ne circule pas ne fuit pas

Les données sensibles ne quittent pas le périmètre : zéro entraînement tiers, zéro télémétrie, zéro copie à l'étranger.

IMPACT 4,99 M\$ par fuite évitée

COÛTS

Coût marginal proche de zéro

Après amortissement du matériel, les workloads récurrents ne paient plus de token à chaque appel : le récurrent passe au fixe.

IMPACT Zéro token par requête

Chaque requête d'agent emporte un morceau de votre pipeline hors du manoir

Le coût de la fuite n'a jamais été aussi haut, et l'IA en est l'accélérateur : le lieu de traitement est un arbitrage de commandement.

4,99 M\$

Coût moyen d'une fuite de données, un record en hausse de 12 % (IBM 2026).

1/4

des fuites malveillantes sont activées par l'IA, pour 6 M\$ en moyenne (IBM).

25 %

des apps GenAI d'entreprise subiront 5+ incidents mineurs/an d'ici 2028 (Gartner).

Sources : IBM Cost of a Data Breach Report 2026 ; Gartner, avril 2026.

Bletchley a déjà tranché le débat : la machine n'était rien sans le matériau

■ LE PRÉCÉDENT — BLETCHLEY PARK, 1939-1945

- Station X décodait Enigma sur place : Bombe et Colossus dans le manoir, matériau entrant par les Y-stations.
- Une Bombe isolée tourne sans rien voir : sans interceptions triées et indexées, la machine est aveugle.
- Compartimentage need-to-know : chaque hutte ignorait les autres, rien ne sortait sans décision.

=

■ LA TRANSPOSITION COMMERCIALE

- Votre modèle local (Muse Glimmer, Ollama) est la Bombe : construit et exploité dans votre périmètre.
- Sans RAG à jour, l'agent sait lire mais ne sait pas ce que votre entreprise sait : un moteur sans carburant.
- Votre gateway joue les Y-stations : tout entre par des canaux contrôlés, seules les tâches autorisées sortent.

Trois manœuvres pour installer votre manoir : la machine, le matériau, les canaux

01

Installer la machine dans le périmètre

La Manœuvre

Identifier 2-3 workloads sensibles récurrents et les basculer en local cette semaine, avec une identité contrôlée par agent.

Outils Ollama, LM Studio, Muse Glimmer

02

Nourrir la machine : le RAG avant tout

La Manœuvre

Cartographier les données et programmer la synchro RAG avant tout fine-tuning : déléguer sans données, c'est déléguer sans munitions.

Outils Chroma, Qdrant, index vectoriel

03

Contrôler les canaux : le gateway

La Manœuvre

Définir trois classes de données (reste au manoir, sort anonymisé, sort en clair) et router le gateway en conséquence, avec audit.

Outils ngrok, Tailscale, Cloudflare Tunnel

90 jours pour passer de l'IA dans le cloud à l'IA au manoir

0-30 JOURS

- Basculer 2-3 workloads sensibles en local
- Installer Muse Glimmer sur une station 24 Go

Pilote RevOps / IT

KPI Workloads basculés

30-60 JOURS

- Cartographier les données et bâtir le RAG
- Définir les 3 classes de données

Pilote Data / DSI

KPI Index RAG opérationnel

60-90 JOURS

- Router le gateway selon les classes
- Auditer les sorties et durcir la classification

Pilote CISO / DSI

KPI Sorties 100 % auditées

« Ultra n'a jamais quitté le manoir. Pourquoi votre pipeline, lui, part-il chaque nuit ? »

À ENGAGER — Choisissez le terrain : décidez dès cette semaine quelles données traitent en local, et où le reste est autorisé à sortir.

Une réflexion adossée aux références stratégiques, business et historiques

■ RÉFÉRENCES STRATÉGIQUES

- Hinsley, British Intelligence in the Second World War
- Liddell Hart, History of the Second World War

■ ÉTUDES BUSINESS

- IBM, Cost of a Data Breach Report 2026 (4,99 M\$)
- Gartner — 25 % des apps GenAI à 5+ incidents d'ici 2028
- Meta / VentureBeat — Muse Glimmer, open-weight 30B (10/08/2026)

■ SOURCES HISTORIQUES

- Bletchley Park Trust — Station X, la Bombe et Colossus
- Welchman, The Hut Six Story — le criblage d'Enigma