AYI NEDJIMI Consultants

Windows Recall : Analyse Technique Complete - Fonctionnem...

Catégorie : Intelligence Artificielle Lecture : 6 min Publié le : 19/01/2026 Auteur : Ayi NEDJIMI

Analyse technique approfondie de Windows Recall : capture d'ecran, traitement NPU, embeddings vectoriels, indexation SQLite, recherche semantique.

Cet article propose une analyse technique approfondie de Windows Recall : comment fonctionne le pipeline de capture et d'indexation ? Quelles technologies sont utilisees pour le traitement local ? Comment les donnees sont-elles securisees ? Et quels sont les risques reels pour les utilisateurs ? Analyse technique approfondie de Windows Recall : capture d'ecran, traitement NPU, embeddings vectoriels, indexation SQLite, recherche semantique. Dans un contexte où l'intelligence artificielle transforme les pratiques de cybersécurité, la maîtrise de windows recall analyse technique devient un avantage stratégique pour les équipes techniques. Nous abordons notamment : 1 architecture technique de windows recall, 2 mecanisme de capture d'ecran et 3 traitement npu : ocr et embeddings. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

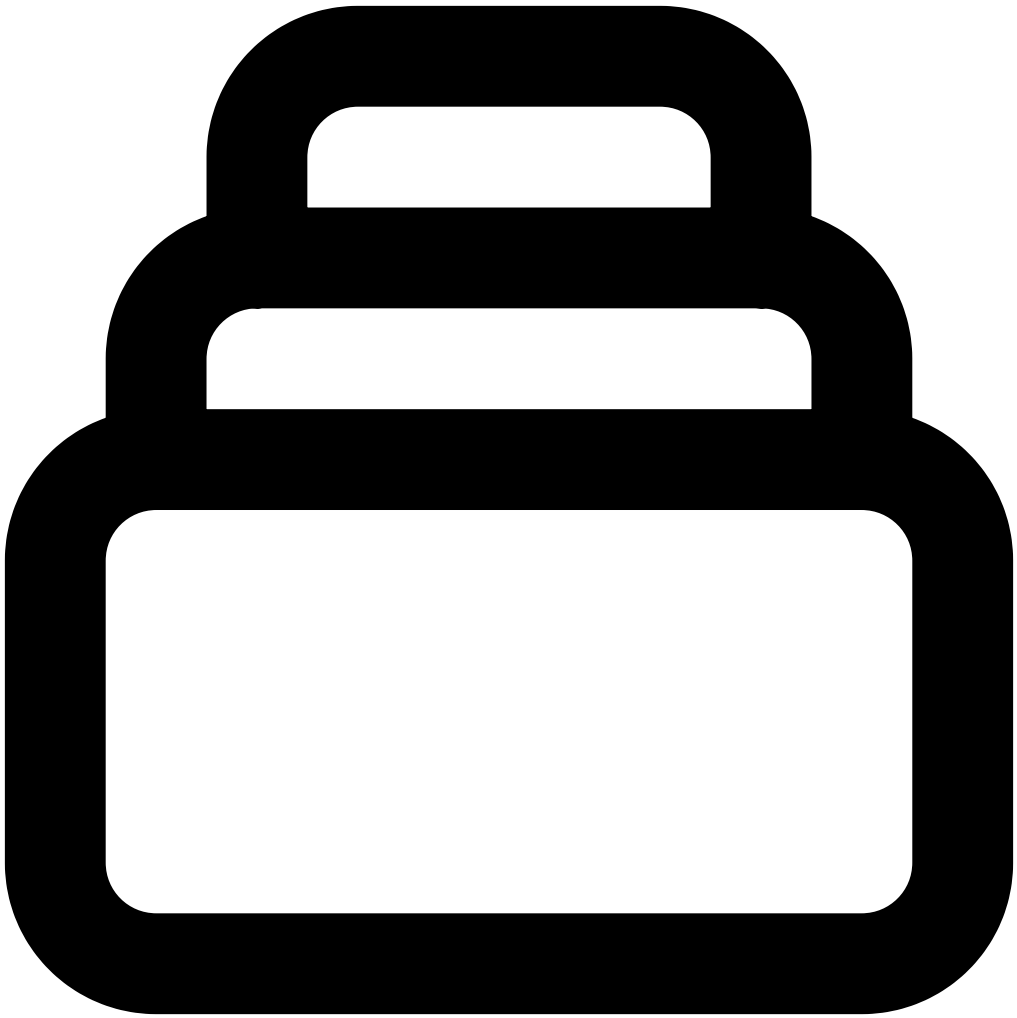
Avertissement important

Windows Recall capture potentiellement tout ce qui apparait sur votre ecran, y compris des informations sensibles : mots de passe saisis, documents confidentiels, conversations privees, donnees bancaires. Meme avec les protections implementees, cette fonctionnalite represente une surface d'attaque significative pour les acteurs malveillants.

Notre avis d'expert
Chez Ayi NEDJIMI Consultants, nous constatons que la majorité des organisations sous-estiment les risques liés aux modèles de langage déployés en production. La sécurité des LLM ne se limite pas au prompt engineering : elle exige une approche systémique couvrant les embeddings, les pipelines de données et les mécanismes de contrôle d'accès aux API.

Votre organisation est-elle prête à faire face aux attaques basées sur l'IA ?

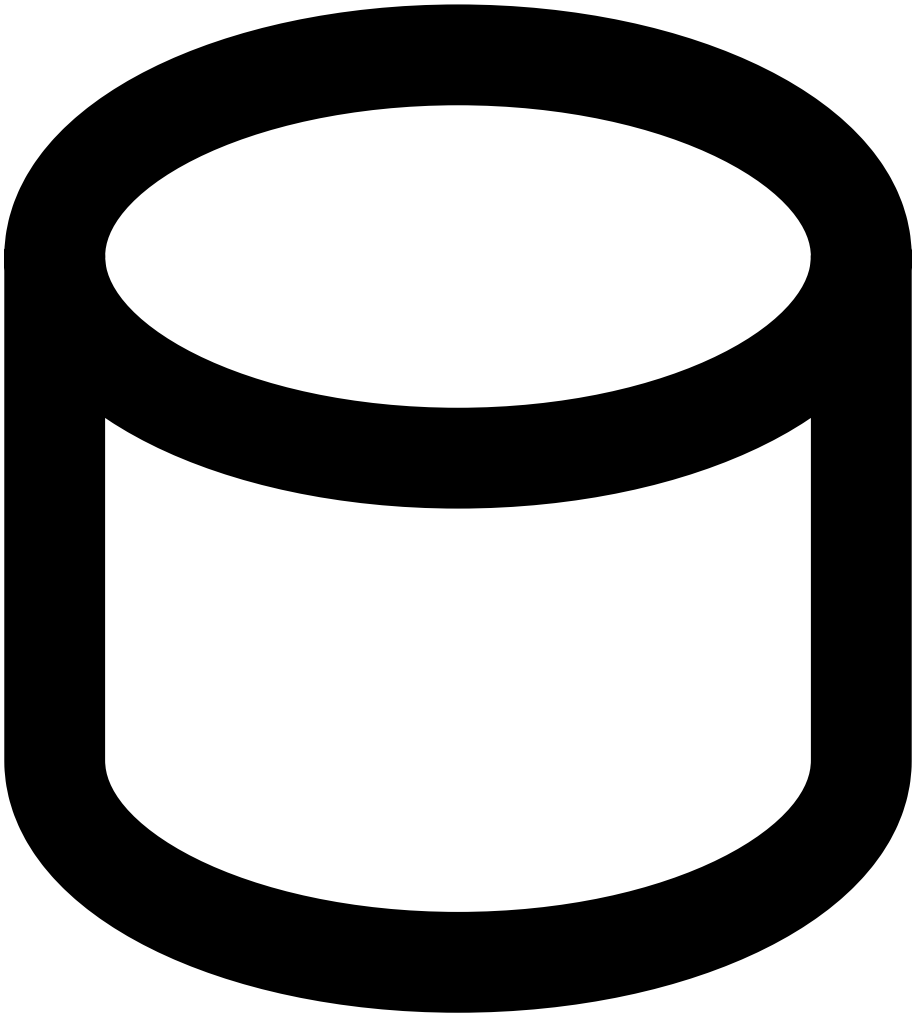
1Architecture Technique de Windows Recall



1.1 Composants principaux

Windows Recall s'appuie sur plusieurs composants systeme integres :

Composant	Role	Technologie
Screen Capture Service	Capture periodique des screenshots	Windows.Graphics.Capture API
CoreAIPlatform	Orchestration du traitement IA	Windows AI Runtime
NPU Driver Stack	Execution des modeles sur NPU	DirectML, ONNX Runtime
OCR Engine	Extraction du texte des images	Windows.Media.Ocr
Embedding Model	Generation des vecteurs semantiques	Phi-Silica / modele proprietaire
SQLite + Vector Index	Stockage et recherche	SQLite + index HNSW
VBS Enclave	Isolation securisee	Virtualization-Based Security



1.2 Structure des donnees

Les donnees Recall sont stockees localement dans le profil utilisateur :

```
C:\Users\[username]\AppData\Local\CoreAIPlatform.00\UKP\ |-- ImageStore\ # Screenshots comprimes (PNG) |-- ukg.db # Base SQLite principale |-- vector_index.db # Index vectoriel HNSW |-- metadata.json # Configuration et metadonnees
```

La base `ukg.db` contient les tables suivantes : Pour approfondir, consultez AI Act 2026 : Implications pour les Systèmes Agentiques et.

- •**snapshots** : Metadonnees des captures (timestamp, app active, URL)
- •**ocr_text** : Texte extrait par OCR
- •**embeddings** : Vecteurs de 768-1536 dimensions
- •**exclusions** : Apps et sites exclus

2Mecanisme de Capture d'Ecran

2.1 Declenchement et frequence

Windows Recall ne capture pas en continu mais detecte les **changements significatifs** a l'ecran :

- •Intervalle minimal : environ 5 secondes entre captures
- •Detection de changement : analyse des differences de pixels
- •Seuil de declenchement : ~30% de changement visuel
- •Pause automatique : inactivite, lecture video, jeux

2.2 Exclusions automatiques

Certains contenus sont automatiquement exclus :

- ✓ **Navigation privee** : InPrivate (Edge), Incognito (Chrome)
- ✓ **Champs de mot de passe** : Detection heuristique des inputs password
- ✓ **DRM content** : Contenu protege (Netflix, Disney+)
- ✓ **Apps sensibles** : Gestionnaires de mots de passe (configurable)
- ✓ **Sessions RDP** : Bureaux distants

Cas concret
En février 2024, une entreprise de Hong Kong a perdu 25 millions de dollars après qu'un employé a été trompé par un deepfake vidéo lors d'une visioconférence. Les attaquants avaient recréé l'apparence et la voix du directeur financier à l'aide de modèles d'IA générative, démontrant les risques concrets de cette technologie en contexte corporate.

3Traitement NPU : OCR et Embeddings

3.1 Pipeline de traitement

Chaque screenshot passe par le pipeline suivant, execute entierement sur le NPU :

1. **Preprocessing** : Redimensionnement, normalisation

2. **OCR** : Extraction du texte visible (multilangue)
3. **Object Detection** : Identification des elements UI
4. **Text Embedding** : Vectorisation du texte extrait
5. **Visual Embedding** : Vectorisation de l'image
6. **Fusion** : Combinaison en vecteur final

3.2 Modeles utilises

Modele	Tache	Taille	Dimensions output
Windows OCR Engine	Extraction texte	~50 MB	Texte brut
Phi-Silica (text)	Embeddings texte	~500 MB	768 dimensions
CLIP-like (visual)	Embeddings visuels	~300 MB	512 dimensions
Fusion layer	Combinaison	~50 MB	1280 dimensions

4Stockage et Indexation

4.1 Base de donnees SQLite

Les donnees sont stockees dans une base SQLite chiffree : Les recommandations de OWASP Top 10 LLM constituent une reference essentielle.

```
-- Schema simplifie de la table snapshots CREATE TABLE snapshots ( id INTEGER PRIMARY KEY, timestamp DATETIME NOT NULL, app_name TEXT, window_title TEXT, url TEXT, image_path TEXT, ocr_text TEXT, embedding BLOB, -- Vecteur serialise is_sensitive BOOLEAN DEFAULT 0 ); CREATE INDEX idx_timestamp ON snapshots(timestamp); CREATE INDEX idx_app ON snapshots(app_name);
```

4.2 Index vectoriel HNSW

Pour la recherche semantique rapide, Recall utilise un index **HNSW (Hierarchical Navigable Small World)** :

- •**Complexite** : O(log n) pour la recherche
- •**Metrique** : Similarite cosinus
- •**Precision** : Recall@10 > 95%
- •**Capacite** : ~3 mois de captures (configurable)

4.3 Chiffrement et protection

Mecanismes de protection des donnees : Pour approfondir, consultez Orchestration d'Agents IA : Patterns et Anti-Patterns.

- ✓ **BitLocker** : Chiffrement du volume au repos (AES-256)
- ✓ **DPAPI** : Protection des cles par credentials utilisateur
- ✓ **VBS Enclave** : Isolation du traitement dans une VM securisee

- ✓ **Windows Hello** : Authentification biometrique requise pour l'acces
- ✓ **ACL strictes** : Seul le compte utilisateur a acces

5Recherche Semantique

5.1 Pipeline de requete

Quand l'utilisateur effectue une recherche :

1. **Authentification** : Windows Hello valide l'identite
2. **Tokenisation** : La requete est tokenisee
3. **Embedding** : Conversion en vecteur via le meme modele
4. **Recherche ANN** : Query sur l'index HNSW
5. **Reranking** : Tri par pertinence + temporalite
6. **Affichage** : Presentation des snapshots correspondants

5.2 Types de requetes supportees

- •**Texte naturel** : "document budget du trimestre dernier"
- •**Nom d'application** : "PowerPoint presentation"
- •**Temporel** : "hier apres-midi", "la semaine derniere"
- •**Visuel** : "graphique avec des barres bleues"
- •**Combine** : "email de Jean concernant le projet Alpha"

6Analyse de Securite Approfondie

6.1 Vecteurs d'attaque identifies

Risques de securite majeurs :

- **1. Acces local malveillant** : Un attaquant avec privileges eleves peut extraire la base de donnees
- **2. Malware cible** : Infostealers concus pour exfiltrer les donnees Recall
- **3. Acces physique** : Vol de laptop = acces potentiel a toute l'historique visuel
- **4. Compromission du compte** : L'attaquant herite de l'acces Recall
- **5. Shoulder surfing ameliore** : Les captures peuvent reveler des informations sensibles vues brievement

6.2 Mitigations implementees vs limites

Protection	Efficacite	Limite
BitLocker	Bonne	Inutile si attaquant a deja acces post-boot
VBS Enclave	Excellente	Bypass possibles via vulnerabilites kernel
Windows Hello	Bonne	Contournable si session deja authentifiee
Exclusions auto	Moyenne	Detection heuristique imparfaite
Opt-in	Excellente	Utilisateurs peuvent l'activer sans comprendre les risques

6.3 Cas d'attaque : TotalRecall

Peu apres l'annonce de Recall, le chercheur en securite **Kevin Beaumont** a publie l'outil **TotalRecall** demontrant la facilite d'extraction des donnees :

```
# Extraction des donnees Recall (necessite privileges admin) # Localisation de la base $recallPath = "$env:LOCALAPPDATA\CoreAIPlatform.00\UKP\ukg.db" # Copie de la base (si non verrouillee) Copy-Item $recallPath -Destination "C:\exfil\recall_dump.db" # Extraction des images Get-ChildItem "$env:LOCALAPPDATA\CoreAIPlatform.00\UKP\ImageStore" -Recurse
```

Cet outil a force Microsoft a renforcer les protections et a retarder le deploiement de Recall.

7Configuration et Bonnes Pratiques

7.1 Desactiver Windows Recall

Pour desactiver completement Recall :

1. Parametres > Confidentialite et securite > Recall
2. Desactiver "Enregistrer les instantanes"
3. Cliquer sur "Supprimer tous les instantanes" pour purger l'historique

7.2 Configuration securisee (si activation)

Recommandations pour une utilisation securisee : Pour approfondir, consultez Pydantic AI et les Frameworks d'Agents Type-Safe en 2026.

1. Activer BitLocker sur tous les volumes
2. Configurer Windows Hello (biometrie obligatoire)
3. Exclure toutes les applications sensibles (gestionnaires de MDP, apps bancaires)
4. Reduire la periode de retention au minimum necessaire
5. Auditer regulierement le contenu et supprimer les captures sensibles
6. Ne pas activer sur des machines partagees ou professionnelles sensibles

7.3 GPO pour l'entreprise

En environnement entreprise, Recall peut etre desactive via GPO :

```
Computer Configuration > Administrative Templates > Windows Components > Windows AI > "Turn off saving snapshots for Windows" = Enabled
```

FAQ

Qu'est-ce que Windows Recall ?

Windows Recall désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

Pourquoi windows recall analyse technique est-il important ?

La maîtrise de windows recall analyse technique est devenue essentielle pour les équipes de sécurité. Les enjeux et le contexte opérationnel sont développés tout au long de l'article.

Comment appliquer ces recommandations en entreprise ?

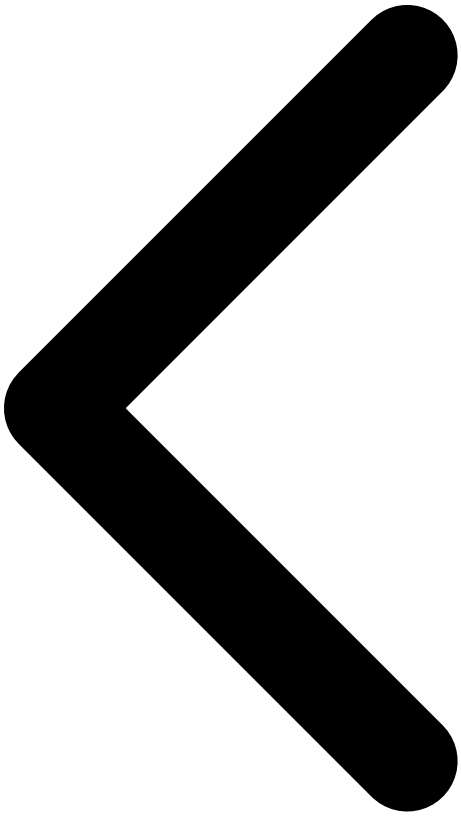
Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

Conclusion

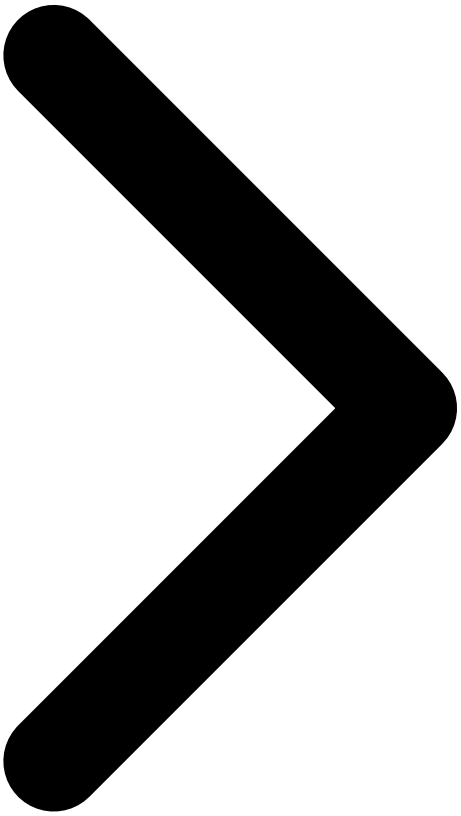
Windows Recall represente une avancee technologique impressionnante dans l'integration de l'IA au niveau systeme d'exploitation. L'architecture technique, combinant capture intelligente, traitement NPU local, et recherche semantique vectorielle, demontre le potentiel des "PC IA" de nouvelle generation.

Cependant, cette fonctionnalite souleve des preoccupations legitimes en matiere de securite. La creation d'une base de donnees exhaustive de l'activite utilisateur, meme chiffree et protegee, represente une cible de choix pour les attaquants. Les mesures de protection implementees par Microsoft sont solides mais pas infaillibles. Pour approfondir, consultez Tendances Futures des Embeddings.

Pour les utilisateurs et les entreprises, la decision d'activer Recall doit resulter d'une analyse risques/benefices eclairee. Dans les environnements sensibles, la desactivation complete reste la recommandation prudente.



Configuration Conclusion FAQ



Pour approfondir, consultez les ressources officielles : ANSSI, CERT-FR Panorama 2025 et MITRE ATT&CK.

Sources et références : ArXiv IA · Hugging Face Papers

FAQ : Questions Frequentes

Comment fonctionne Windows Recall techniquement ?
Recall capture des screenshots periodiques, les traite via le NPU pour extraire le texte (OCR) et generer des embeddings vectoriels. Ces donnees sont indexees dans une base SQLite locale chiffree, permettant une recherche semantique en langage naturel.

Ou sont stockees les donnees Recall ?
Dans `C:\Users\[username]\AppData\Local\CoreAIPlatform.00\UKP\`. Les images sont dans ImageStore, les metadonnees et vecteurs dans ukg.db. Tout est chiffre par BitLocker et protege par les ACL Windows.

Les donnees Recall sont-elles envoyees au cloud ?
Non, tout le traitement est effectue localement sur le NPU. Les captures, l'OCR, les embeddings et la recherche restent sur l'appareil. Aucune donnee Recall n'est transmise a Microsoft.

Puis-je supprimer mes donnees Recall ?
Oui, via Parametres > Confidentialite > Recall, vous pouvez supprimer tout l'historique, des periodes specifiques, ou les captures d'applications particulieres. La suppression est definitive.

Ressources open source associées :

- AppRaiserres — DLL bypass Windows 11

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr