AYI NEDJIMI Consultants

# L'IA dans Windows 11 : Copilot, NPU et Recall - Guide Com...

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

*Découvrez comment Microsoft intègre l'IA dans Windows 11 : Copilot, NPU (Neural Processing Unit), Windows Recall et les fonctionnalités natives.*

## Introduction : Windows 11 entre dans l'ere de l'IA

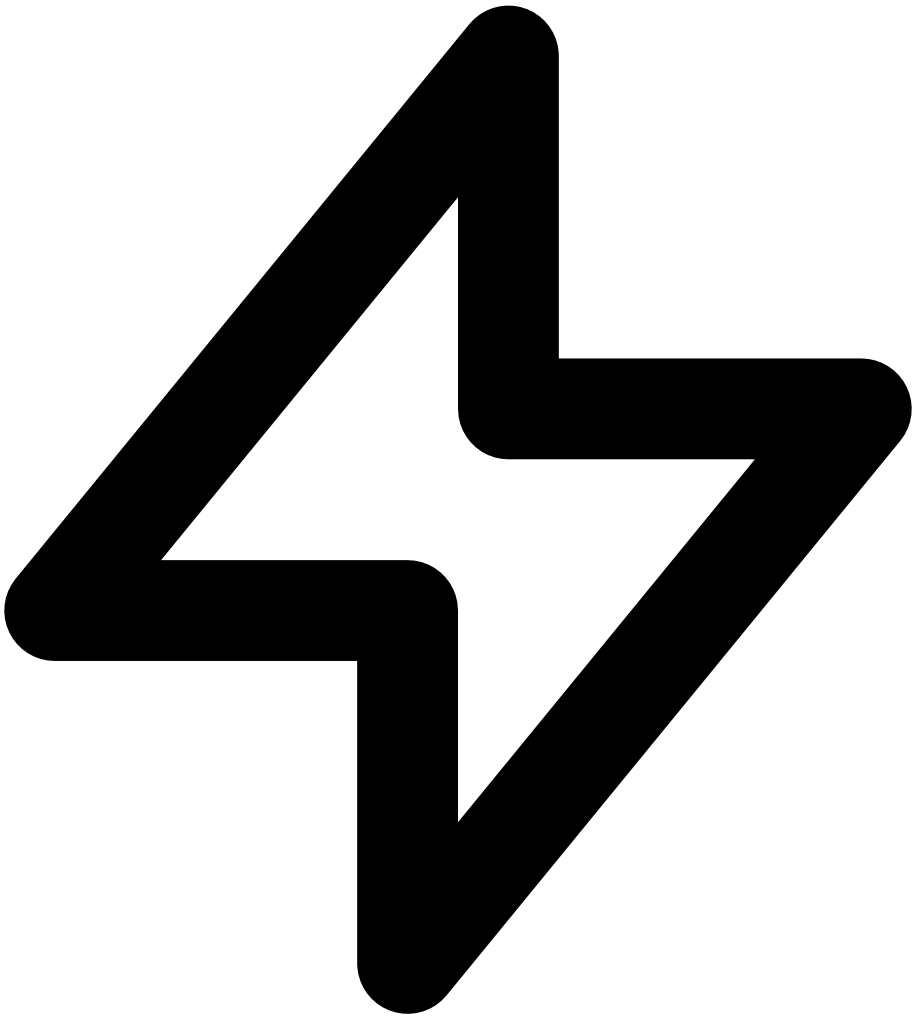
Cette integration profonde de l'IA dans le systeme d'exploitation souleve des questions fondamentales : quelles sont reellement ces technologies ? Comment fonctionnent-elles ? Et surtout, quelles sont les implications en termes de securite et de confidentialite ? Cet article propose une analyse technique complete de l'ecosysteme IA de Windows 11. Découvrez comment Microsoft intègre l'IA dans Windows 11 : Copilot, NPU (Neural Processing Unit), Windows Recall et les fonctionnalités natives. Dans un contexte où l'intelligence artificielle transforme les pratiques de cybersécurité, la maîtrise de ia windows 11 copilot npu devient un avantage stratégique pour les équipes techniques. Nous abordons notamment : introduction : windows 11 entre dans l'ere de l'ia, 1 microsoft copilot : l'assistant ia au centre de windows et 2 le npu : processeur neural pour l'ia locale. 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.

Points cles de cet article :

- •Comprendre Microsoft Copilot et son integration systeme
- •Demystifier le NPU : qu'est-ce que c'est et pourquoi c'est important
- •Analyser Windows Recall : fonctionnement technique et risques

- •Evaluer les implications securite de l'IA native dans Windows

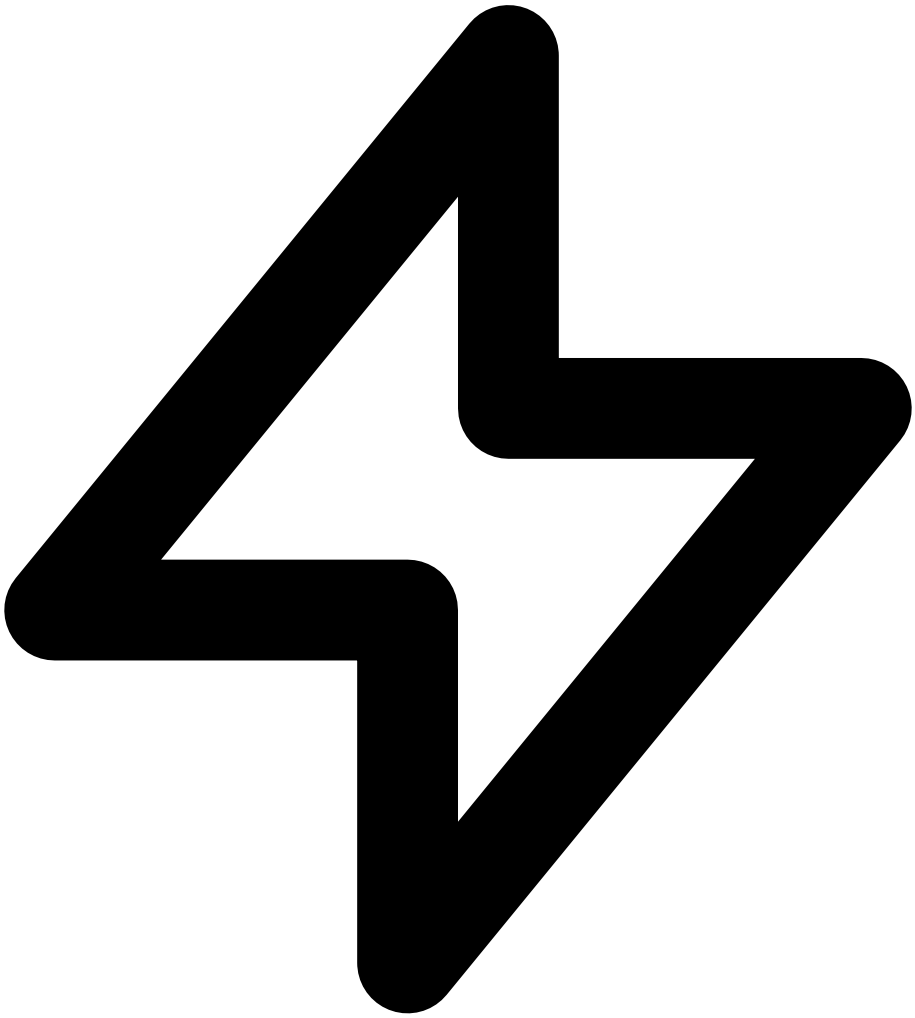
# 1Microsoft Copilot : L'Assistant IA au centre de Windows



## 1.1 Qu'est-ce que Microsoft Copilot ?

**Microsoft Copilot** est l'assistant IA de Microsoft, integre directement dans Windows 11. Base sur les modeles de langage **GPT-4** et **GPT-4o** d'OpenAI, il permet aux utilisateurs d'interagir en langage naturel avec leur systeme d'exploitation. Accessible via le raccourci `Win + C` ou l'icone dans la barre des taches, Copilot peut :

- ✓**Repondre aux questions** : recherche web, explications techniques, aide contextuelle
- ✓**Controler Windows** : modifier les parametres, lancer des applications, gerer les fichiers
- ✓**Generer du contenu** : textes, emails, resumes, traductions
- ✓**Analyser des images** : description, extraction de texte (OCR), analyse visuelle
- ✓**Creer des images** : generation via DALL-E 3 integre



## 1.2 Architecture technique de Copilot

Copilot fonctionne selon une architecture hybride cloud/local :

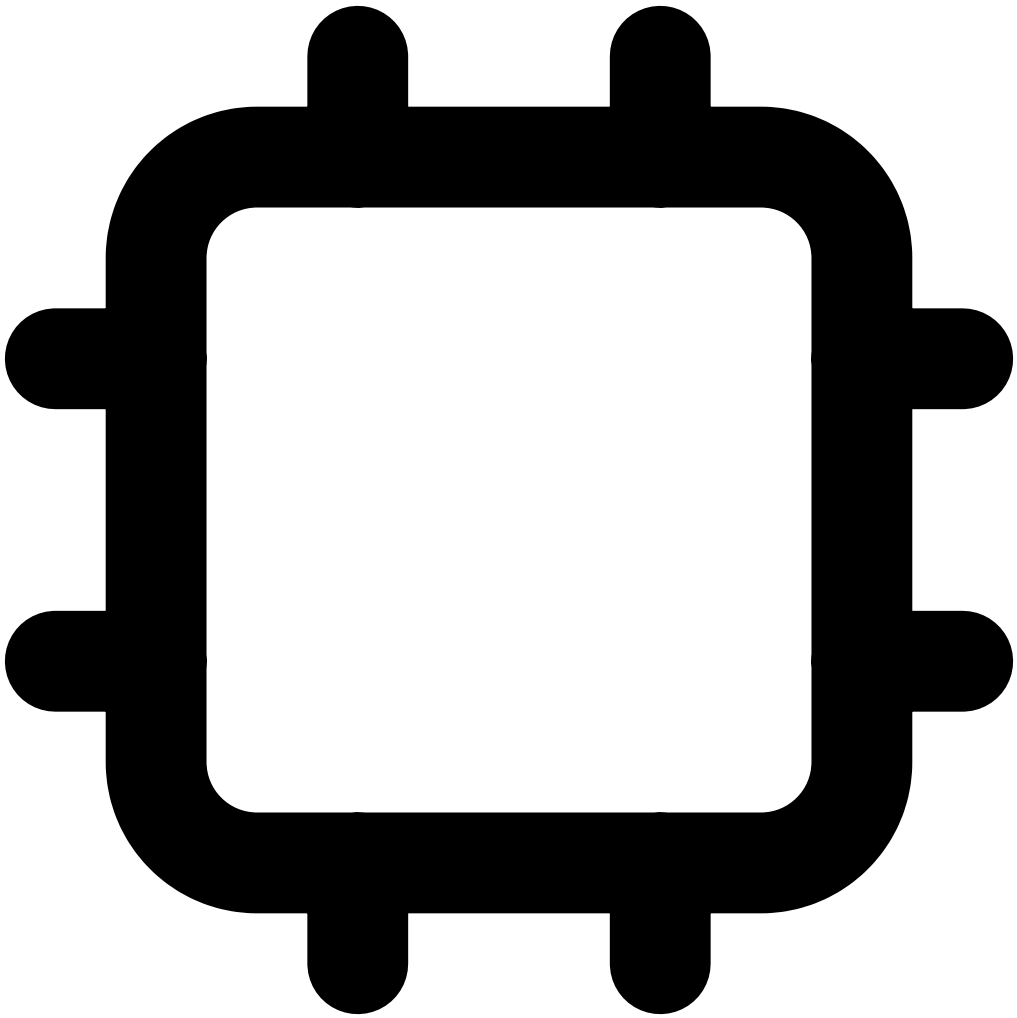
| Composant | Localisation | Fonction |
|---|---|---|
| Interface utilisateur | Local (Windows) | Capture des requetes, affichage des reponses |
| Modele LLM (GPT-4/4o) | Cloud Azure | Traitement du langage naturel, generation |
| Plugins systeme | Local | Execution des actions Windows (parametres, apps) |
| Recherche Bing | Cloud | Informations temps reel, recherche web |
| DALL-E 3 | Cloud Azure | Generation d'images |
| Phi-3/SLM | Local (NPU) | Taches simples sans connexion (Copilot+ PC) |

**Notre avis d'expert**

L'IA responsable n'est pas un luxe — c'est une nécessité opérationnelle. Nos audits révèlent que 70% des déploiements IA en entreprise manquent de mécanismes de détection des biais et de garde-fous contre les injections de prompt. Il est temps d'intégrer la sécurité dès la conception des pipelines ML.

Comment garantir que vos modèles de machine learning ne deviennent pas des vecteurs d'attaque ?

# 2Le NPU : Processeur Neural pour l'IA Locale



## 2.1 Qu'est-ce qu'un NPU ?

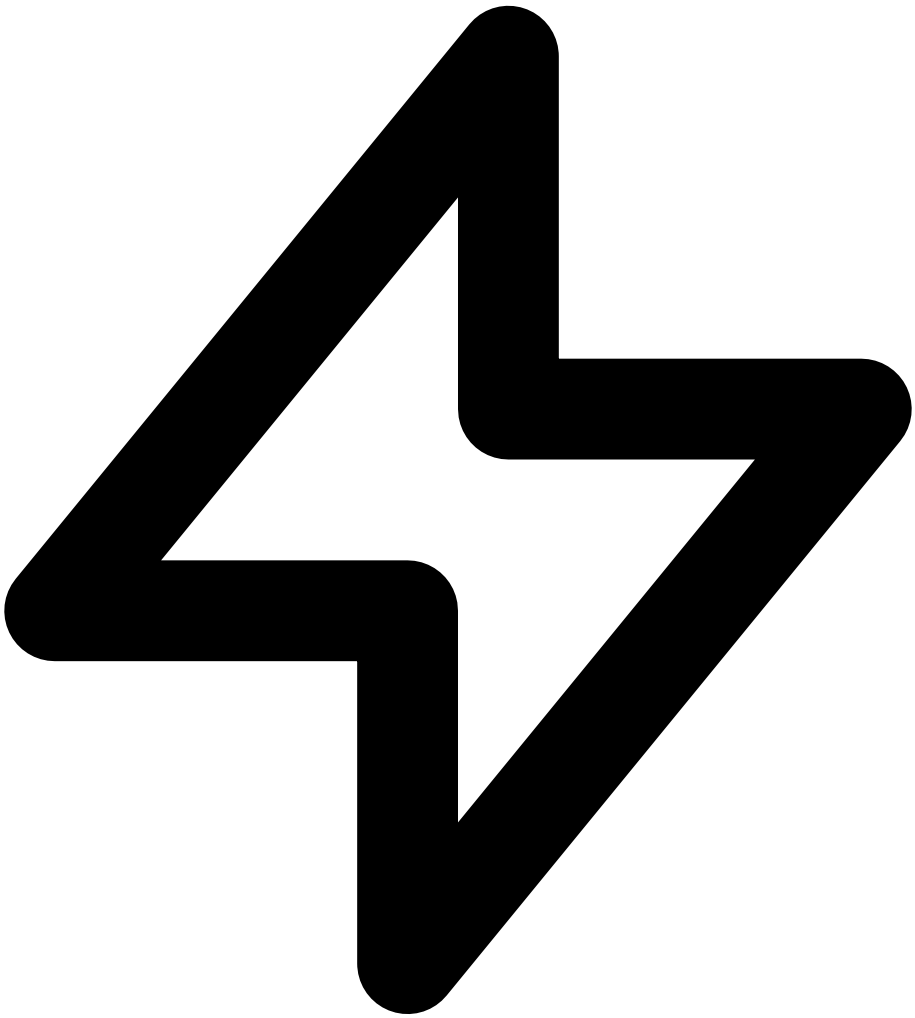
Le **NPU (Neural Processing Unit)** est un processeur specialise dans l'execution des operations de reseaux de neurones. Contrairement au CPU (generaliste) ou au GPU (optimise pour le calcul parallele graphique), le NPU est concu specifiquement pour les operations matricielles caracteristiques de l'apprentissage automatique. Pour approfondir, consultez IA Multimodale : Texte, Image et Audio.

Pourquoi le NPU est-il crucial ?

Le NPU permet d'executer des modeles d'IA **localement**, sans envoyer de donnees au cloud. Cela garantit :

- • **Confidentialite** : vos donnees restent sur votre machine
- • **Latence reduite** : reponses instantanees sans aller-retour reseau
- • **Fonctionnement hors-ligne** : IA disponible sans connexion Internet

• • **Efficacite energetique** : consommation inferieure au GPU pour les taches IA

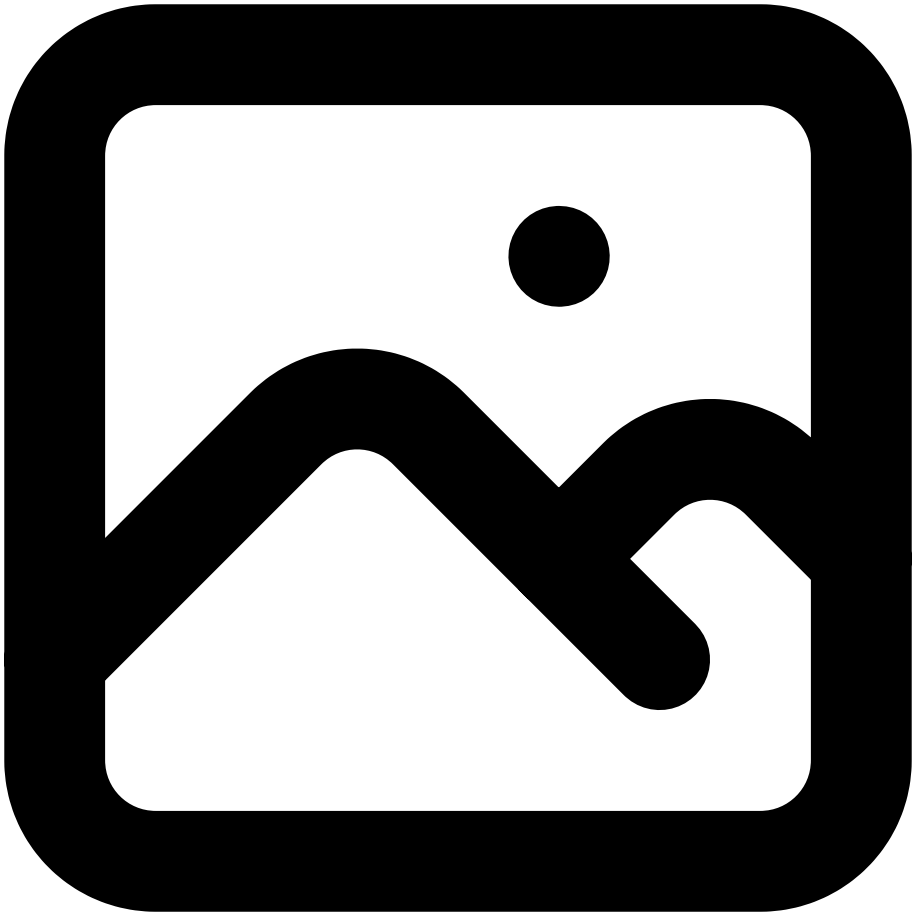


## 2.2 Specifications techniques des NPU actuels

| Fabricant | NPU | Performance | Processeurs compatibles |
|---|---|---|---|
| Qualcomm | Hexagon | 45+ TOPS | Snapdragon X Elite/Plus |
| Intel | Intel AI Boost | 10-48 TOPS | Core Ultra (Meteor Lake, Lunar Lake) |
| AMD | Ryzen AI | 16-50 TOPS | Ryzen 8000/9000 series |
| Apple | Neural Engine | 38 TOPS | M3/M4 (reference macOS) |

**TOPS** (Tera Operations Per Second) mesure la puissance de calcul IA. Microsoft exige un minimum de **40 TOPS** pour la certification "Copilot+ PC", permettant d'executer des modeles comme Phi-3 ou des taches Recall en local.

# 3Windows Recall : La Memoire Visuelle Controversee



## 3.1 Concept et fonctionnement

**Windows Recall** est une fonctionnalite bouleversant (et controversee) qui capture periodiquement des screenshots de votre ecran, les analyse via IA, et cree un index semantique interrogeable. L'objectif : vous permettre de retrouver "tout ce que vous avez vu sur votre PC" en utilisant le langage naturel. Les recommandations de OWASP Top 10 LLM constituent une reference essentielle.

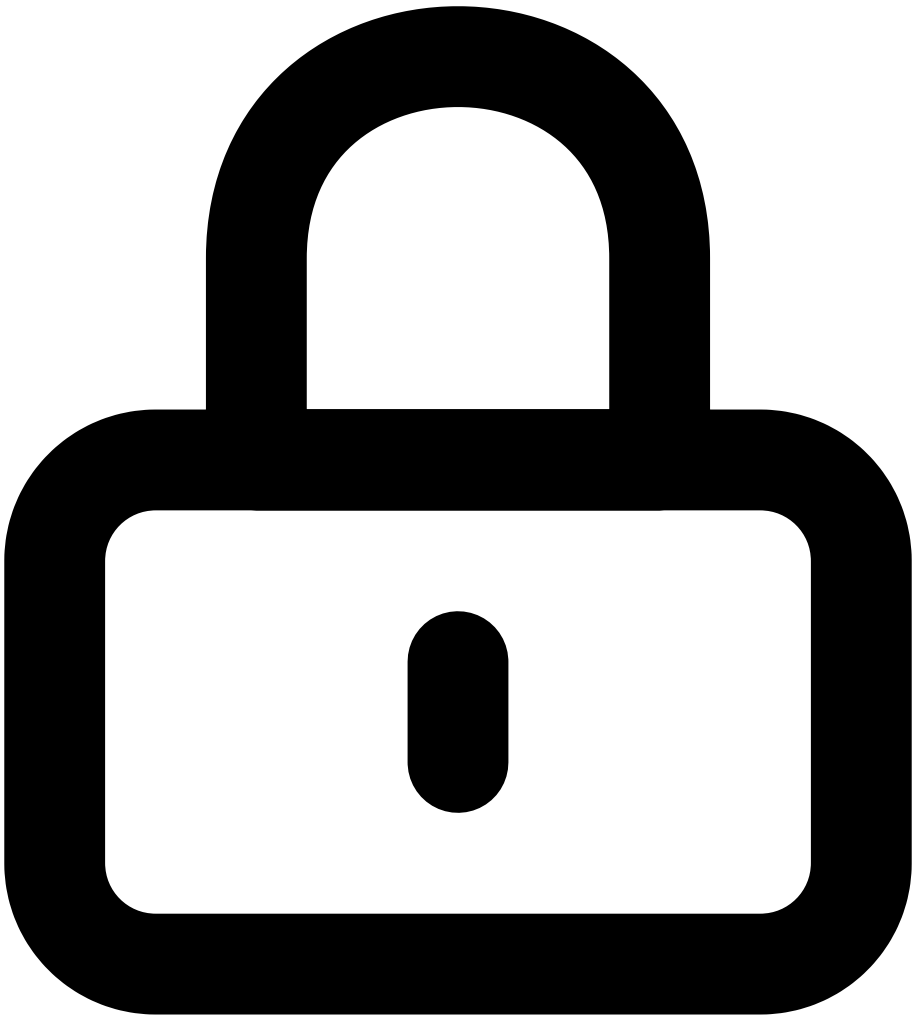
Le pipeline technique de Recall : Pour approfondir, consultez Orchestration d'Agents IA : Patterns et Anti-Patterns.

1. **Capture** : Screenshots automatiques toutes les quelques secondes
2. **Analyse OCR** : Extraction du texte visible via NPU
3. **Embeddings** : Vectorisation semantique du contenu (texte + visuel)
4. **Indexation** : Stockage dans une base vectorielle locale SQLite

5. **Recherche** : Requetes en langage naturel converties en recherche vectorielle

Attention : Risques de securite potentiels

Windows Recall stocke des captures d'ecran qui peuvent contenir des informations sensibles : mots de passe visibles, donnees bancaires, conversations privees, documents confidentiels. Bien que chiffrees localement, ces donnees representent une cible de choix pour les attaquants ayant un acces local a la machine.



### 3.2 Mesures de securite implementees

Suite aux critiques initiales, Microsoft a renforce la securite de Recall :

- ✓**Opt-in obligatoire** : Recall est desactive par defaut, activation explicite requise
- ✓**Chiffrement BitLocker** : Base de donnees chiffree au repos
- ✓**Isolation VBS** : Traitement dans une enclave securisee (Virtualization-Based Security)
- ✓**Windows Hello** : Authentification biometrique pour acceder aux donnees Recall

- ✓**Filtrage automatique** : Exclusion des champs de mot de passe, navigation privee, apps sensibles
- ✓**Controle utilisateur** : Possibilite de supprimer des periodes, exclure des apps

**Cas concret**
En 2023, des chercheurs ont démontré qu'il était possible de manipuler Bing Chat (Copilot) pour exfiltrer des données personnelles via des techniques d'injection de prompt indirecte. Cette attaque exploitait la capacité du LLM à accéder aux résultats de recherche web, transformant un assistant en vecteur d'exfiltration.

## 4Applications IA Natives de Windows 11

Au-dela de Copilot et Recall, Windows 11 integre l'IA dans de nombreuses applications natives :

| Application | Fonctionnalite IA | Traitement |
|---|---|---|
| Photos | Suppression arriere-plan, amelioration, recherche visuelle | NPU local |
| Paint | Cocreator (generation d'images), suppression objets | Cloud (DALL-E) + NPU |
| Clipchamp | Silence auto, generation sous-titres, voix synthetique | NPU + Cloud |
| Snipping Tool | Extraction texte (OCR), traduction | NPU local |
| Notepad | Rewriting, resume, aide a la redaction | Cloud (Copilot) |
| Explorer | Recherche semantique fichiers | NPU local |
| Camera | Effets temps reel, flou arriere-plan, eye contact | NPU local |
| Traduction Live | Sous-titres temps reel multilingues | NPU local |

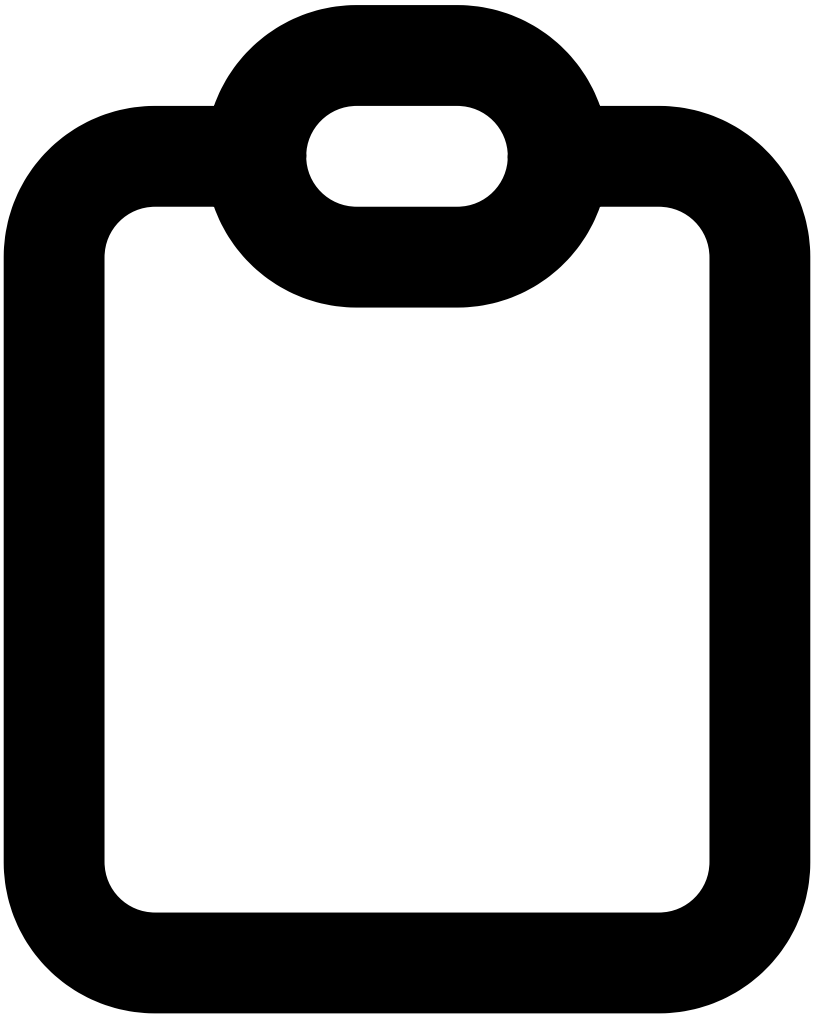
## 5Securite et Confidentialite : Analyse Critique

### 5.1 Avantages du traitement local (NPU)

- ✓**Donnees non transmises** : Le traitement NPU garde vos donnees sur l'appareil
- ✓**Pas de dependance cloud** : Fonctionnement hors-ligne possible
- ✓**Latence minimale** : Reponses instantanees

### 5.2 Risques et preoccupations

- ✗ **Surface d'attaque elargie** : Recall cree une base de donnees exhaustive de l'activite utilisateur
- ✗ **Acces physique** : Un attaquant avec acces local pourrait extraire les donnees Recall
- ✗ **Telemetrie Copilot** : Les requetes cloud sont loguees par Microsoft
- ✗ **Malwares cibles** : Emergence de malwares visant specifiquement les donnees Recall



### 5.3 Recommandations de securite

Bonnes pratiques pour securiser l'IA Windows 11 : Pour approfondir, consultez Gouvernance LLM et Conformité : RGPD, AI Act et Auditabilité.

1. Activer BitLocker sur tous les volumes
2. Configurer Windows Hello (biometrie) pour l'acces Recall
3. Exclure les applications sensibles de Recall (gestionnaire de mots de passe, apps bancaires)
4. Auditer regulierement le contenu Recall et supprimer les periodes sensibles
5. Desactiver Recall en environnement entreprise sensible
6. Maintenir Windows Defender a jour pour la protection contre les malwares cibles IA

## FAQ

### Qu'est-ce que L'IA dans Windows 11 ?

L'IA dans Windows 11 désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

### Pourquoi ia windows 11 copilot npu est-il important ?

La maîtrise de ia windows 11 copilot npu 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 ?

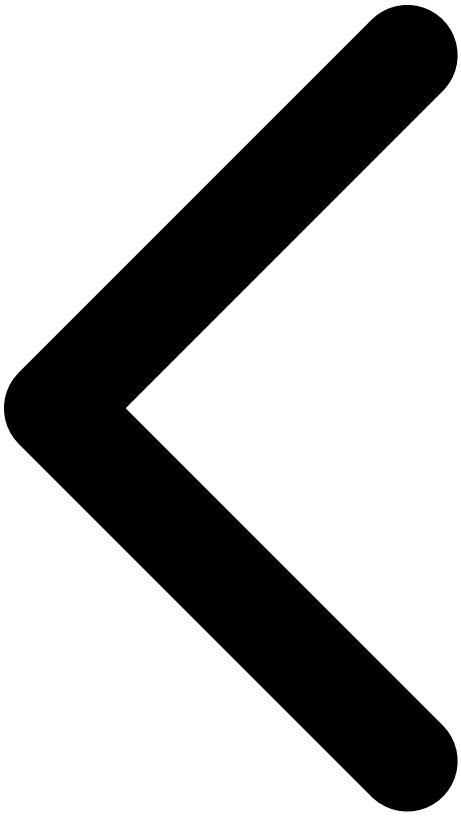
Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

## Conclusion

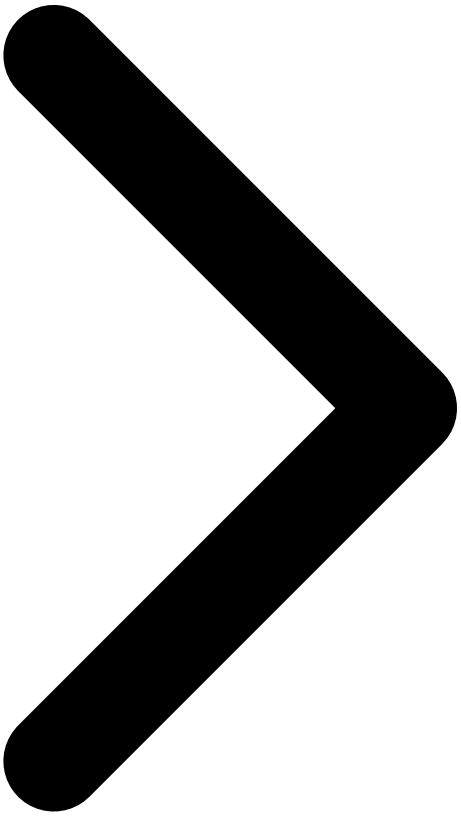
L'integration de l'IA dans Windows 11 marque un tournant majeur dans l'evolution des systemes d'exploitation. Microsoft propose une vision ambitieuse ou l'assistant Copilot, le traitement neural local via NPU, et la memoire visuelle Recall convergent pour creer une experience utilisateur augmentee par l'intelligence artificielle.

Cependant, cette transformation s'accompagne de defis significatifs en matiere de securite et de confidentialite. L'accumulation de donnees personnelles par des fonctionnalites comme Recall necessite une vigilance accrue et une configuration rigoureuse. Le traitement local via NPU offre des garanties de confidentialite interessantes, mais ne resout pas tous les problemes. Pour approfondir, consultez Phishing IA : Quand les Defenses Traditionnelles Echouent.

Pour les professionnels de la securite et les utilisateurs avertis, il est essentiel de comprendre ces technologies, leurs implications, et de configurer adequatement leur environnement Windows 11 pour beneficier des avantages de l'IA tout en minimisant les risques.



Securite Conclusion FAQ



Pour approfondir, consultez les ressources officielles : Hugging Face, arXiv et ANSSI.

**Sources et références :** ArXiv IA · Hugging Face Papers

## FAQ : Questions Frequentes

**Qu'est-ce que Microsoft Copilot dans Windows 11 ?**
Microsoft Copilot est un assistant IA integre a Windows 11, base sur GPT-4 et GPT-4o. Il permet d'interagir en langage naturel pour controler le systeme, obtenir de l'aide, generer du contenu et automatiser des taches. Accessible via Win+C ou l'icone dans la barre des taches.

**Qu'est-ce qu'un NPU et pourquoi est-il important ?**
Un NPU (Neural Processing Unit) est un processeur specialise pour le traitement des reseaux de neurones. Il permet d'executer des modeles IA localement avec une efficacite energetique superieure au CPU/GPU. Les PC Copilot+ requierent 40+ TOPS pour des fonctionnalites comme Recall.

**Windows Recall est-il securise ?**

Recall utilise le chiffrement BitLocker, l'isolation VBS, et l'authentification Windows Hello. Cependant, il stocke des captures d'ecran potentiellement sensibles. Il est recommande d'exclure les applications sensibles et de desactiver Recall en environnement haute securite.

**Puis-je utiliser Copilot sans connexion Internet ?**

Les fonctionnalites principales de Copilot necessitent une connexion cloud (GPT-4). Cependant, sur les PC Copilot+ avec NPU, certaines taches peuvent etre executees localement via des modeles comme Phi-3, permettant un fonctionnement limite hors-ligne.

> **Ressources open source associées :**
>
> • AppRaiserres — DLL bypass Windows 11

---

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

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