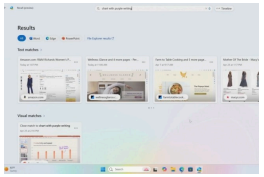
# Windows Recall, un vrai cauchemar pour la vie privée

**Matthew Finnegan, Computerworld (adaptation Jean Elyan)** , publié le 28 Mai 2024

**Annoncée par Microsoft la semaine passée, la fonction d'IA de Windows a rapidement suscité des critiques en raison des captures d'écran régulières effectuées par l'OS au point qu'un expert en sécurité l'a comparée à un logiciel d'enregistrement de frappe.**



La dernière fonctionnalité de Windows 11, baptisée Windows Recall, enregistre un grand nombre de données personnelles pour

Windows Recall, la fonctionnalité qui enregistre l'écran d'un utilisateur à intervalles réguliers, a été qualifiée de « cauchemar pour la vie privée » en raison des

alimenter la GenAI de Microsoft./ (Crédit MS)

risques qu'elle introduit en matière de confidentialité et de sécurité des données. Annoncé lundi dernier par Microsoft, l'outil, basé sur l'IA générative, enregistre des « instantanés » de l'écran de l'utilisateur toutes les cinq secondes pour fournir un historique consultable des actions sur une période de trois mois. La fonction sera disponible en avant-première dans les PC Copilot+ que Microsoft et d'autres fournisseurs commenceront à vendre à la mi-juin.

« Des mesures ont été mises en place pour protéger les données Recall », a déclaré Microsoft. Les données enregistrées sont stockées et traitées localement et protégées par chiffrement sur le terminal de l'utilisateur, et celui-ci peut exclure les applications et les sites web qu'il souhaite garder privés. Il est également possible d'interrompre Recall

à tout moment. Cependant, comme l'a indiqué Microsoft, Recall, qui est activé par défaut, n'effectue pas de « modération de contenu », ce qui signifie que l'outil ne dissimulera pas les informations confidentielles comme les mots de passe, les numéros de comptes bancaires ou tout autre élément pouvant apparaître sur l'écran d'un PC.

Cette capacité de Recall à enregistrer et à stocker autant de données sensibles de l'utilisateur a vite suscité des critiques sur les risques de confidentialité et de sécurité des données. « Un enregistreur de frappe et un outil de capture d'écran intégrés qui capturent parfaitement tout ce que l'on fait sur sa machine dans un certain laps de temps est un véritable cauchemar pour la vie privée, et je doute que l'utilisateur moyen en tirera des bénéfices », a déclaré Jeff Pollard, vice-

président et analyste principal chez Forrester. « Mon premier sentiment, c'est que cela pourrait très vite mal tourner », a estimé John Scott, chercheur principal en sécurité chez le fournisseur de logiciels de sécurité CultureAI. « Ce sont les risques de sécurité qui posent le plus gros problème », a renchéri Douglas McKee, directeur exécutif de la recherche sur les menaces pour l'entreprise de sécurité du réseau SonicWall. « L'annonce de Microsoft Recall nous rappelle une fois de plus que les progrès de l'intelligence artificielle et des technologies peuvent être très pratiques au détriment de la sécurité », a-t-il déclaré dans un communiqué. « Même si Microsoft Recall suscite de nombreuses inquiétudes en matière de protection de la vie privée, la véritable menace réside dans l'utilisation potentielle que les attaquants feront de cette fonctionnalité », a-t-il ajouté.

## Une porte ouverte sur les données de l'utilisateur

Selon M. McKee, gagner l'accès initial à un appareil facilite grandement une attaque, et c'est bien plus simple que d'obtenir l'élévation des privilèges, « mais avec Microsoft Recall, l'accès initial offre l'essentiel de ce qui est nécessaire pour potentiellement voler des informations sensibles comme des mots de passe ou des secrets commerciaux de l'entreprise ». Les pirates qui parviennent à s'introduire dans un PC sur lequel Recall est installé auront potentiellement accès à tout ce qu'a fait l'utilisateur sur une période de trois mois environ, y compris les mots de passe, les données bancaires en ligne, les messages sensibles, les dossiers médicaux ou tout autre document confidentiel. Recall pourrait rendre le vol de données sensibles

beaucoup plus simple que d'autres modalités d'attaques comme l'installation d'un logiciel d'enregistrement de frappe ou d'écran, qui pourraient attirer davantage l'attention. (Selon Microsoft, une icône Recall est placée dans la barre d'état de Windows pour indiquer que des clichés sont pris). « Pourquoi installer un logiciel d'enregistrement de frappe quand on peut simplement activer une fonction intégrée au système », a demandé M. Scott. C'est une façon différente d'attaquer, mais c'est une façon qui n'existait pas avant que Microsoft ne dise : « Nous faisons une capture d'écran toutes les cinq secondes » et, plus important encore, une capture d'écran consultable toutes les cinq secondes. Pour M. Pollard, « avec cette version, Microsoft franchit une nouvelle étape dans l'exploitation des données ». Microsoft a refusé de

répondre à une demande de commentaires sur ces problèmes de sécurité.

Outre le risque de cyberattaque, la question de la confidentialité des données a également soulevé quelques inquiétudes. Au Royaume-Uni, l'Information Commissioner's Office, un organisme public chargé de faire respecter les droits en matière de confidentialité des données, a déclaré mercredi dernier avoir écrit à Microsoft au sujet de la fonction Recall afin de « comprendre les garanties mises en place pour protéger la vie privée des utilisateurs ». La quantité de données enregistrées et collectées sur l'ordinateur d'un utilisateur peut devenir problématique lorsqu'il s'agit de respecter les règles de protection des données. « L'un des aspects de la directive

RGPD de l'UE est la proportionnalité », a rappelé M. Scott. « Avec Recall, l'utilisateur constitue un énorme trésor de données personnelles, les siennes et celles d'autres personnes, et il ne semble pas y avoir de raison très claire de le faire », a-t-il poursuivi. Outre les informations personnelles de l'utilisateur, Recall pourrait collecter et stocker des données de collègues, de clients ou d'autres tiers. Par exemple, lors d'un appel vidéo, « Recall peut-il prendre un cliché de l'écran toutes les cinq secondes sans autorisation explicite des interlocuteurs d'enregistrer des images avec leurs noms ? » D'autant qu'il y a « suffisamment d'éléments pour identifier avec certitude le correspondant, ce qui pose un énorme problème ». Et si les données sont stockées localement, on peut se demander si demain elles ne pourraient pas être sauvegardées

ailleurs, voire hébergées sur les serveurs cloud de Microsoft.

## Une fonctionnalité très inquiétante pour la sécurité

Justin Lam, analyste principal de la sécurité de l'information chez S&P Global Market Intelligence, estime pour sa part que les entreprises ont l'habitude de gérer des risques liés à la sécurité et à la protection de la vie privée et que cela ne devrait pas nécessairement empêcher l'utilisation d'outils dont les avantages pour les utilisateurs et les entreprises ont été démontrés. « Les entreprises doivent trouver un équilibre entre la protection de la vie privée et la productivité des utilisateurs, la gestion des risques internes, la surveillance et la conformité », a-t-il déclaré. « Cela dit, elles devraient également prendre en compte les gains de productivité individuels globaux que

peuvent apporter des outils tels que Recall et Copilot ». D'autres, cependant, recommandent aux entreprises d'éviter d'utiliser un tel outil. « « Même si la possibilité de rechercher un historique d'utilisation peut faire gagner du temps et augmenter la production, le risque pour les petites entreprises d'utiliser cette fonction est trop grand », a ajouté McKee de SonicWall. « Déjà, si c'est possible, faites-en sorte de ne pas l'activer », a conseillé M. Pollard de Forrester. « Je préfèrerais aussi qu'on puisse la supprimer par le biais d'une stratégie de groupe si elle est disponible. De plus si la fonction est activée à un moment donné, je voudrais que la télémétrie m'informe de son activation afin que je puisse déterminer si un utilisateur a eu l'intention de l'activer ou si c'est le fait d'un attaquant qui cherche à collecter des données ». Selon la page

d'administration de Microsoft, ceux qui ne souhaitent pas utiliser Recall peuvent désactiver la fonction à l'aide de la stratégie « Désactiver l'enregistrement d'instantanés pour Windows », ce qui supprimera aussi tous les instantanés déjà enregistrés sur l'appareil. « Pour les entreprises, les administrateurs IT peuvent désactiver l'enregistrement automatique des instantanés à l'aide d'une stratégie de groupe ou d'une stratégie de gestion des appareils mobiles », explique Microsoft sur son site d'assistance.

La fonction Recall étant en cours de prévisualisation, des modifications pourraient être apportées avant qu'elle ne soit généralement disponible. Selon M. Lam, l'éditeur pourrait améliorer la fonction et atténuer les inquiétudes liées à la sécurité et à la confidentialité. « Recall

pourrait, par exemple, « oublier » davantage d'actions qu'il a enregistrées », a-t-il suggéré. « Recall pourrait conserver un historique sur une période plus courte ou se limiter à un champ d'application plus restreint. Ce qu'il perdrait en précision, il le gagnerait en confiance pour l'utilisateur ». Les capacités d'intelligence artificielle de Windows pourraient également s'améliorer au point de permettre une classification plus efficace des données enregistrées par Recall. Windows Copilot pourrait par ailleurs fournir un « guidage forcé », en anticipant et en invitant les utilisateurs à arrêter complètement l'enregistrement de l'écran. « Pour l'instant, il est difficile de voir comment utiliser cette fonction en toute sécurité. Elle représente un risque dans son ensemble, et aucun contrôle de sécurité ou de confidentialité ne

m’inciterait aujourd’hui à l'activer sur un système que j'utilise », a-t-il tranché.

Article rédigé par

**Matthew Finnegan, Computerworld (adaptation Jean Elyan)**