Windows Sandbox pour Windows 10 : haro sur les applications « infectées »

Microsoft veut garantir la sécurité informatique des machines exploitant son OS Windows 10 (Windows 10 Pro et Enterprise).

La politique du moindre risque

Vecteurs de malwares ou autres virus, les applications peuvent infecter les machines.

C'est la raison pour laquelle Microsoft présente Windows Sandbox (littéralement le bas à sable de Windows). Cet environnement cloisonné permet de lancer en toute quiétude des applications émanant de sources dont la fiabilité n'est pas garantie.

La firme de Redmond apostrophe les utilisateurs de son OS bureau dans un billet de blog : « Combien de fois avez-vous téléchargé un fichier exécutable sans avoir peur de l'exécuter? » Et d'ajouter que dans certain cas, l'utilisateur peut être contraint de réinstaller Windows.

Windows Sandbox se présente ainsi comme un environnement de bureau temporaire et isolé, dans lequel il est possible d'exécuter des logiciels non fiables sans risque pour le PC.

Ne laisse aucune trace

Le groupe dirigé par Satya Nadella de préciser que « tout logiciel installé dans le bac à sable Windows reste uniquement dans le bac à sable et ne peut affecter votre hôte ».

De surcroît, dès que Windows Sandbox est fermé, tous les logiciels avec tous leurs fichiers et leur état sont définitivement supprimés. Ainsi, rien ne persiste sur la machine.

Techniquement, Microsoft procède à une virtualisation matérielle, en exploitant son propre hyperviseur afin « d'exécuter un noyau distinct qui isole le bac à sable Windows de l'hôte ».