Association Loisirs et culture

6 outils de cybersécurité intégrés à Windows 11 dont vous ignoriez probablement l'existence.

Jean Marie Herbaux

Table des matières

Cette semaine, la cybersécurité est sur toutes les lèvres. Comment protéger ses données ? Éviter les pièges en ligne ? Adopter les bons réflexes ? Si vous utilisez Windows 11, bonne nouvelle : votre système d'exploitation regorge d'outils efficaces et méconnus pour renforcer votre sécurité, sans rien débourser.

Du chiffrement des fichiers à la protection contre les ransomwares, en passant par des technologies avancées pour bloquer les exploits, Windows 11 a tout ce qu'il faut pour éviter bien des désagréments. Le hic ? Ces fonctionnalités sont souvent cachées ou désactivées par défaut. En cette semaine européenne de la cybersécurité, c'est le moment idéal pour les découvrir et les mettre en place !

I. Chiffrement de l'appareil : vos données, votre contrôle

Vous connaissez peut-être BitLocker, réservé aux versions Pro de Windows. Mais l'édition Famille a, elle aussi, son outil de protection des données : le chiffrement de l'appareil. Certes moins personnalisable, il est largement suffisant pour sécuriser vos fichiers contre un accès non autorisé. Une fois activé, vos données deviennent illisibles sans votre compte Microsoft.

a) Comment ça marche ?

Une clé de chiffrement est générée et liée au module TPM (présent sur la plupart des PC récents). Cette clé est stockée en toute sécurité et ne se libère qu'après authentification réussie. En clair, même si quelqu'un démonte votre disque dur pour l'examiner ailleurs, il n'y trouvera que des données inexploitables.

b) Comment l'activer ?

Rendez-vous dans *Paramètres* > *Confidentialité et sécurité* > *Chiffrement de l'appareil* et activez l'interrupteur.
Le chiffrement de l'appareil conditionne l'accès à votre disque dur à vos identifiants
Le petit plus : Cette protection est transparente une fois en place et n'affecte pas les performances de votre PC. Une sécurité automatisée, comme on les aime.

II. Accès contrôlé aux dossiers : la barrière anti-ransomware

S'il est vrai que les ransomwares ciblent souvent les entreprises, personne n'est à l'abri d'un clic malencontreux. Une fausse facture ou un lien frauduleux… et voilà vos documents personnels pris en otage. Heureusement, l'accès contrôlé aux dossiers est là pour éviter ce genre de drame – simple à configurer et efficace au quotidien.

a) Comment ça marche ?

Cette fonctionnalité interdit l'accès à vos dossiers importants à tout logiciel non approuvé. Vous pouvez même créer votre propre liste d'applications "de confiance" pour garder le contrôle.

b) Comment l'activer ?

Allez dans *Paramètres* > *Confidentialité et sécurité* > *Sécurité Windows* > *Protection contre les virus et menaces* > *Protection contre les ransomwares* > *Gérer la protection contre les ransomwares*.
Activez l'option *Dispositif d'accès contrôlé aux dossiers* et renseignez vos applications de confiance.
Le dispositif d'accès contrôlé aux dossiers est une bonne parade contre les dégâts occasionnés par les ransomwares.
Le petit plus : Totalement personnalisable, cette protection s'adapte à vos besoins en deux clics, sans aucun réglage complexe.

III. Windows Hello : la sécurité sans mots de passe

Les mots de passe, avouons-le, sont une plaie. Trop simples, ils sont une porte ouverte aux pirates. Trop complexes, ils finissent souvent oubliés. Avec Windows Hello, votre visage, votre empreinte digitale ou un code PIN deviennent vos clés d'accès au système et aux applications sensibles qui y sont installées.

a) Comment ça marche ?

Windows Hello stocke votre code PIN ou vos données biométriques localement, et les utilise pour générer des clés d'accès uniques, appelées passkeys. Votre visage ou empreinte digitale est analysé pour créer une signature chiffrée, uniquement lisible par votre appareil.

b) Comment l'activer ?

Allez dans *Paramètres* > *Comptes* > *Options de connexion* et configurez l'option *biométrique* de votre choix ou un code PIN si votre appareil n'a pas de capteur.
Le petit plus : Ces données ne quittent jamais votre appareil, ce qui les rend inutilisables en cas de fuite de données. Oubliez les mots de passe ; vous êtes la clé.

IV. SmartScreen : le garde-fou contre les arnaques

Internet, c'est un peu le Far West : des promesses partout, mais aussi des pièges à chaque coin de clic. Un site douteux, un fichier suspect : il suffit d'un rien pour télécharger un malware. Heureusement, SmartScreen veille au grain. Ce filtre intégré bloque les contenus dangereux avant qu'ils n'aient une chance de s'exécuter.

a) Comment ça marche ?

SmartScreen analyse les sites web et les fichiers que vous essayez d'ouvrir. Il compare leur réputation à une base de données en ligne et les bloque, ou vous avertit, si quelque chose cloche.

b) Comment l'activer ?

Par défaut, SmartScreen est actif, mais vérifiez dans *Paramètres* > *Confidentialité et sécurité* > *Sécurité Windows* > *Contrôle des applications et du navigateur*. Activez toutes les options dans *Protection fondée sur la réputation.*
Le petit plus : Contrairement aux idées reçues, SmartScreen ne se limite pas à Edge : il surveille aussi les fichiers et applications téléchargés via d'autres navigateurs.

V. Core Isolation : une armure pour votre système

Certaines attaques visent directement le noyau de votre système, là où tout est géré. Pour contrer ce genre de menaces, Windows 11 propose Core Isolation, qui utilise la virtualisation pour isoler les processus critiques.

a) Comment ça marche ?

Cette technologie empêche les malwares d'accéder aux zones sensibles de votre système en les isolant dans un environnement sécurisé. Une option appelée *Intégrité de la mémoire* garantit que seuls des codes vérifiés peuvent être exécutés.

b) Comment l'activer ?

Allez dans *Paramètres* > *Confidentialité et sécurité* > *Sécurité Windows* > *Sécurité de l'appareil* et activez *Intégrité de la mémoire*. En cas de conflit avec des pilotes, Windows vous guidera pour les résoudre.
Le petit plus : Cette protection fonctionne en arrière-plan et n'impacte pas les performances. Invisible, mais essentielle.

VI. Exploit Protection : un rempart invisible

Même les logiciels fiables peuvent devenir des portes ouvertes pour des cyberattaques. Avec Exploit Protection, Windows anticipe ces scénarios et bloque ces failles avant qu'elles ne puissent être exploitées.

a) Comment ça marche ?

Par défaut, Exploit Protection applique des règles avancées pour protéger vos applications et votre système contre les attaques. Vous pouvez même personnaliser ces règles pour chaque logiciel.

b) Comment l'activer ?

Ouvrez *Paramètres* > *Confidentialité et sécurité* > *Sécurité Windows* > *Contrôle des applications et du navigateur* > *Paramètres Exploit Protection*. Vérifiez que tous les paramètres sont activés par défaut.
Le petit plus : Pas besoin d'être un expert : les paramètres par défaut couvrent déjà l'essentiel. Mais si vous aimez garder la main, tout est personnalisable.

VII. Bonus : Microsoft Defender, l'injustement mal-aimé

Microsoft Defender est souvent critiqué pour son rôle "d'antivirus par défaut", mais il n'est pas à sous-estimer. Gratuit et directement intégré à Windows 11, il offre une protection en temps réel, des mises à jour régulières et même des fonctionnalités avancées comme le mode "*Analyse hors ligne*", capable de traquer les menaces furtives avant que le système ne soit complètement chargé.
Pas un foudre de guerre, mais solide. Microsoft Defender n'a pas la prétention de rivaliser avec des suites de sécurité tout-en-un, mais pour une navigation responsable et des usages classiques du web, il fait très bien le travail. Tant que vous évitez les sites douteux et ne téléchargez pas à l'aveugle, il vous protège efficacement au quotidien.
Pourquoi l'utiliser ? Il est déjà là, configuré et opérationnel dès le premier jour, sans frais supplémentaires ni installation nécessaire. Que demander de plus ?
Une sécurité Windows intégrée pour partir du bon pied
Windows 11 ne prétend pas rivaliser avec les solutions antivirus les plus sophistiquées, mais il offre une panoplie d'outils intégrés qui permettent de partir du bon pied.
Simples, efficaces et déjà à votre disposition, ces fonctionnalités couvrent les besoins essentiels pour protéger vos données et naviguer en toute tranquillité. De quoi renforcer votre sécurité sans (trop d') effort.