Le petit livret fuchsia Windows 10 sur la sécurité

Insight

Microsoft

Introduction

La cybersécurité est un sujet de préoccupation permanent pour les entreprises. En tant que mise à jour majeure pour Microsoft, Windows® 10 apporte de grandes améliorations en matière de sécurité.

- Scanner Device Guard
- Secure Boot
- Autorisation d'utilisateur Windows Hello
- Authentification sécuritaire Microsoft® Passport
- Chiffrement nouvelle génération BitLocker®
- Virtual Secure Mode

Voyons de plus près ces fonctionnalités.

Device Guard

Décrit comme un « videur vraiment costaud » pour vos dispositifs par la revue CIO, Device Guard inspecte minutieusement toutes les applications que vous essayez de télécharger sur n'importe quel dispositif sous Windows 10 ®. Il vous avertit par la suite si une application a été développée de façon anonyme ou si elle a été approuvée par la boutique Microsoft®.1

Device Guard se charge de plusieurs questions portant sur la sécurité mais n'a pas vocation à se substituer à un antivirus cautionné par Microsoft. En vérité, il aide le logiciel à être plus efficace. Device Guard peut être utilisé sur des PC, ordinateurs portables, tablettes, téléphones intelligents, systèmes de point de vente, ATM et même sur des dispositifs à venir de l'Internet des objets.

Vous pouvez configurer le degré d'agressivité de Device Guard selon vos souhaits. Acer, Fujitsu, HP, Lenovo, NCR, Par et Toshiba travaillent en collaboration avec Microsoft pour l'installer sur tous leurs dispositifs sous Windows.

Secure Boot

Secure Boot va un peu plus loin que Device Guard, n'autorisant que l'exécution des applications approuvées par votre administrateur TI. Cette fonctionnalité était déjà disponible sur Windows® 8, mais du fait que la configuration par défaut était désactivée, peu d'entreprises l'ont utilisé. Secure Boot est conçu pour empêcher les pirates informatiques de pénétrer dans vos systèmes à l'aide d'une USB ou d'un port SD.

Windows Hello

Windows Hello est le saut vers le futur de Microsoft, allant au-delà des mots de passe, qui, comme vous le savez, viennent en deux saveurs pas très appétissantes : simples à pirater ou impossibles à mémoriser.

Hello utilise la technologie biométrique — lecteurs d'empreintes digitales ou scanners d'iris — afin d'identifier les utilisateurs autorisés. Le seul hic est que vous devez disposer d'ordinateurs avec le matériel et les logiciels nécessaires pour prendre en charge Windows Biometric Framework.

Certains ordinateurs disposent déjà de lecteurs d'empreintes digitales. Microsoft affirme être en plein travail avec ses partenaires afin de préparer davantage de dispositifs avec une technologie qui place Hello au bout des doigts ou à portée de vue, selon vos préférences.

Microsoft Passport

Les dispositifs avec Windows® Hello peuvent également utiliser Microsoft® Passport. Ce dernier prodigue une authentification à deux facteurs pour accéder aux applications et programmes avec un seul code d'accès. Au lieu différents mots de passe pour vous connecter aux applications et aux sites, vous vous connectez au dispositif directement. Par la suite, vous pouvez accéder à tout sans mots de passe.

BitLocker nouvelle génération

Avec Windows 10, Microsoft a étendu les capacités de BitLocker®. BitLocker active un chiffrement automatique des applications, données, courriels et sites Web d'entreprise pour en faire un flux de données vers un seul dispositif. Si les utilisateurs désignent les nouveaux documents comme étant corporatifs, ces derniers seront chiffrés. Vous pouvez configurer vos dispositifs afin qu'ils désignent toutes les données comme étant corporatives et chiffrées. Vous pouvez également prendre des mesures pour prévenir que vos données ne soient copiées.

Virtual Secure Mode

La version d'entreprise de Windows® 10 contient également une fonctionnalité intitulée Virtual Secure Mode (VSM) qui se sert de la virtualisation pour protéger les données et les accréditations sur le disque dur d'un système.

VSM divise le système d'exploitation en plusieurs contenants afin qu'un pirate ne puisse pas avoir accès aux jetons nécessaires pour naviguer à travers le système sans mots de passe en cas de dispositif compromis. VSM est uniquement destiné aux ordinateurs disposant de la virtualisation.

Des mises à jour continues

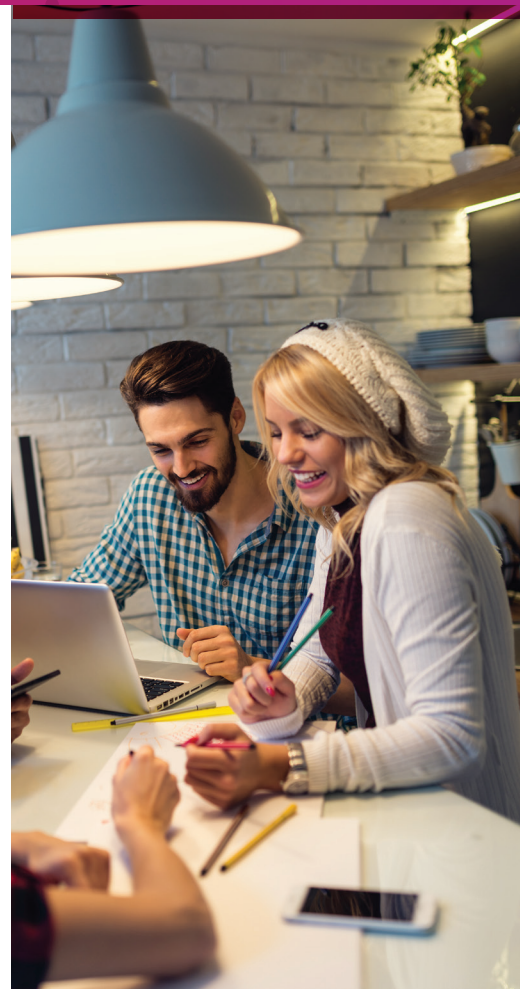
Une fonctionnalité additionnelle et de qualité de Windows 10 : correctifs de sécurité automatiques et mises à jour. Si vous préférez les programmer manuellement vous pouvez toujours le faire.

Les mises à jour poste à poste permettent aux bureaux avec une bande passante limitée de distribuer les mises à jour eux-mêmes au lieu de laisser les PC les télécharger séparément. Autrement dit, vous n'avez pas à vous en soucier. Les mises à jour sont appliquées à vos dispositifs dès qu'elles deviennent disponibles.

Pourquoi Insight pour Windows 10?

Insight est le revendeur de licences de solutions Microsoft le plus important à l'échelle globale, et ce, depuis plus de 25. Nous plaçons Microsoft au centre de notre stratégie de bout en en bout pour aider les entreprises à mener leurs affaires de façon plus efficace. Ensemble, nous fournissons des solutions de technologie intelligente qui répondent à vos besoins stratégiques et optimisent vos investissements.

- Partenaire Microsoft Gold
- Plus de 80 professionnels certifiés Microsoft
- Premier revendeur mondial d'accords de licences pour fournisseurs de services
- Plus de 55 ingénieurs systèmes certifiés Microsoft



À propos d'Insight

Qu'il s'agisse d'entreprises, d'organismes gouvernementaux, d'instituions des soins de la santé ou de l'éducation, Insight offre à ses clients les solutions de technologie intelligente nécessaires à l'accomplissement de leurs objectifs. Avec notre expertise, nous vous conseillons quant à vos choix, implémentations et gestions de solutions technologiques complexes afin de stimuler des résultats commerciaux.

Insight®

Pour en savoir plus, veuillez composer le 1.800.INSIGHT ou visiter ca.insight.com.

[1] Shelton, L. (2015, Sept. 10). Top 3 New Security Features of Windows 10. CIO.com.