

# Sécurité et mobilité Windows 8

pour les utilisateurs nomades

UEFI • BitLocker et AppLocker • DirectAccess • VPN  
• SmartScreen • Windows Defender...

**Arnaud Jumelet**  
**Stanislas Quastana**  
**Pascal Saulière**

Préface de Bernard Ourghanlian



# Préface

## « La sécurité est un voyage... »

---

*SEHOP, DEP, UAC, ASLR, LUA, SRP, Applocker, Bitlocker, AppContainer, SDL... voici une liste non exhaustive des cailloux qui sont venus progressivement paver le long chemin de Windows vers une meilleure sécurité depuis plus de 10 ans.*

Voici, sans attendre ce qui sera détaillé dans cet ouvrage, la signification de ces différents sigles et acronymes. SEHOP : Structured Exception Handling Overwrite Protection. DEP : Data Execution Prevention. UAC : User Account Control. ASLR : Address Space Layout Randomization. LUA : Least-privilege User Account. SRP : Software Restriction Policies. AppLocker : pour appliquer des listes blanches ou des listes noires d'applications dans un environnement d'entreprise, peut être utilisé pour permettre ou empêcher l'exécution d'un logiciel en fonction du nom, du numéro de version ou de l'éditeur. BitLocker : chiffrement des volumes disque. AppContainer : fonctionnalité de Windows 8 faisant fonctionner les applications du Windows Store dans un « bac à sable ». SDL : Security Development Lifecycle.

Qu'il me soit permis de revenir brièvement sur quelques-unes de ces étapes. Nous sommes le 15 janvier 2002 et Bill Gates envoie son désormais célèbre e-mail à l'ensemble des collaborateurs de Microsoft, lançant l'initiative pour l'informatique de confiance. Y sont détaillées les qualités premières d'une plate-forme digne de confiance (disponibilité, sécurité et respect de la vie privée) et soulignée l'importance de fournir des solutions informatiques aussi « fiables et sécurisées que le sont les services de téléphonie et de distribution d'eau et d'électricité ». Cet e-mail va affecter durablement et profondément la culture de développement des logiciels chez Microsoft en faisant accomplir à l'entreprise la révolution copernicienne par laquelle ses logiciels sont désormais conçus, en plaçant la sécurité au centre.

Ce changement de culture commença à prendre racine au début du mois de mars 2002, quand Microsoft prit la décision – pour la première fois de son histoire – de stopper net le développement, alors en cours, de Windows Server 2003 afin de former l'ensemble

des développeurs de Windows à l'écriture de code sécurisé. En effet, bien peu de développeurs avaient eu l'opportunité de bénéficier d'une telle formation, souvent absente des curriculums. Depuis, ce type de formation est désormais obligatoire pour tous les nouveaux développeurs embauchés par Microsoft ; et tous les développeurs, testeurs et *program managers* doivent désormais subir une « piqure de rappel » annuelle en participant à une formation d'environ une semaine afin de se maintenir à jour. Puis, pendant toute l'année 2003, a été développée la méthodologie dont l'usage allait devenir obligatoire pour tous les produits logiciels développés par Microsoft : SDL (Security Development Lifecycle). La première version de SDL à être ainsi rendue d'usage obligatoire, la version 2.0, a été déployée en mars 2004. Depuis cette mise en place initiale, de nombreuses évolutions de SDL – ainsi que de nombreuses versions de Windows – ont vu le jour afin de tenir compte tout à la fois des évolutions technologiques et des nouvelles menaces. Ainsi, au moment où cet ouvrage est mis sous presse, la dernière version applicable à l'ensemble des développements effectués par Microsoft est la version 5.2, qui est en vigueur depuis le 3 octobre 2011. C'est donc cette version de la méthodologie SDL qui s'est appliquée à Windows 8.

Au-delà de la poursuite inlassable de l'amélioration d'une méthodologie qui a désormais fait ses preuves, Windows 8, en matière de sécurité, prend le parti de l'innovation en commençant par se débarrasser de certains de ses oripeaux : c'est notamment le cas avec le BIOS. Le BIOS vient de célébrer récemment son 30<sup>e</sup> anniversaire et force est de constater que ce dernier n'avait guère évolué au cours des années : les BIOS d'aujourd'hui s'exécutent toujours en mode 16 bits, ne disposent que d'un maximum de 1 Mo d'espace adressable et ne fonctionnent que sur les architectures x86. C'est un peu comme si le monde s'était arrêté il y a 30 ans... Avec l'arrivée de nouveaux types de terminaux (tablettes, hybrides...), de nouvelles architectures (notamment l'architecture ARM), et de nouveaux scénarios d'usage, il était devenu urgent que le BIOS se mette au goût du jour sous la forme d'UEFI (Unified Extensible Firmware Interface).

UEFI est une interface firmware construite au-dessus – ou pouvant le remplacer purement et simplement – du BIOS traditionnel. Quand elle est construite au-dessus du BIOS, UEFI en remplace la plupart des fonctions traditionnelles, laissant simplement au BIOS des fonctions telles que la configuration du système et le *Setup*. UEFI est indépendante de l'architecture qui fournit à la fois l'initialisation et le fonctionnement du terminal. C'est ainsi que l'environnement précédant l'amorçage du système peut autoriser une expérience utilisateur riche avec notamment la prise en charge d'une souris, du graphique, etc.

Sur le plan de la sécurité, UEFI joue un rôle clé dans la mesure où elle offre la possibilité d'un boot sécurisé, la prise en charge des disques chiffrés en hardware (*Encrypted Hard Drives*) et un certain nombre d'autres éléments complémentaires qui vous seront présentés dans cet ouvrage et qui font certainement de Windows 8 la version de ce système d'exploitation la plus sécurisée jusqu'à aujourd'hui.

Un autre élément de la sécurité de Windows 8 est TPM.Next. Windows Vista a introduit la gestion de TPM (Trusted Platform Module) pour le chiffrement de volumes disques grâce à la fonctionnalité BitLocker. Pourtant, ce TPM et sa prise en charge

n'ont pas été sans présenter un certain nombre de défis jusqu'à présent ; ainsi, tous les PC n'en disposaient pas pour des raisons de coûts ou de restrictions territoriales (ainsi, des pays comme la Chine, la Russie, le Bélarus, le Kazakhstan n'autorisent pas l'accès aux données ou aux clés stockées dans un TPM), sans parler des difficultés de provisionnement du TPM par les utilisateurs finaux. Pour relever ces défis, le TCG (Trustworthy Computing Group), qui est responsable des spécifications du TPM, a apporté des améliorations très significatives à ce module dans la version dite TPM.Next. Parmi ces améliorations, on pourra noter la possibilité d'étendre les algorithmes de chiffrement afin d'accommoder les besoins de territoires spécifiques, ou encore la possibilité d'implémenter un TPM en firmware afin de ne pas exiger la mise en œuvre d'une puce TPM discrète (ainsi TPM.Next peut être implémenté au sein des environnements TrustZone® d'ARM ou Platform Trust Technology® d'Intel). La prise en charge de TPM.Next est d'ailleurs une exigence pour tous les terminaux AOAC (Always On/Always Connected) afin d'obtenir le Logo Windows.

Windows 8 mise donc de manière délibérée sur les améliorations du matériel afin de faire progresser la sécurité, en ancrant la confiance dans ce matériel.

Cependant, Windows 8 se veut aussi un acteur engagé de la mobilité, y compris dans des scénarios innovants comme ceux promus par le phénomène de la consommation de l'informatique. Rappelons brièvement ici de quoi il s'agit. Ce phénomène se manifeste sous trois formes principales.

- Les usages innovants sont importés au sein de l'entreprise depuis la maison : contrairement à ce qui se passait il y a une dizaine d'années, quand les innovations apparaissaient d'abord au sein des entreprises, c'est l'inverse qui se produit désormais. Il suffit de considérer l'adoption des réseaux sociaux, de la messagerie instantanée, de la téléphonie mobile, des solutions collaboratives ou de création de contenu telles que blogs ou Wikis : toutes ces solutions ont été d'abord adoptées dans l'univers personnel avant de rentrer progressivement – quelquefois à contrecœur – au sein des systèmes d'information.
- Les univers privés et professionnels s'interpénètrent de plus en plus, à tel point que l'on peut parler de « floutage » entre les deux. Doter ses collaborateurs de solutions mobiles (PC portables ou smartphones) a pour conséquence qu'ils peuvent travailler depuis n'importe où et à n'importe quel moment en restant connectés au système d'information ; cela permet notamment la mise en œuvre du « temps choisi », du « travail à distance » ou du télétravail... La contrepartie, c'est que les collaborateurs ne comprendraient pas qu'ils ne puissent pas accéder au système d'information depuis n'importe où et n'importe quand.
- Dans un certain nombre d'organisations, les métiers qui, demandant à l'informatique la fourniture d'un certain service, trouvent trop long le temps de fourniture de ce dernier, se comportent comme de véritables consommateurs en allant acheter directement ce service (par exemple dans le cloud) dont ils ont besoin, sans nécessairement en référer à l'informatique, ce qui n'est pas sans poser des problèmes de sécurité, de gouvernance, de mode de responsabilité...

Comme se plaisent à le rappeler certains sociologues – notamment Patrick Flichy – les usages et les technologies sont codéterminés. Autrement dit, les technologies influencent les usages, mais la réciproque est vraie. C'est la raison pour laquelle il faut considérer que la consomérisation de l'informatique est un phénomène de nature essentiellement sociologique et qu'il serait donc vain de chercher à en contrarier l'épanouissement. C'est pour cela qu'il faut s'y préparer dès maintenant.

Une de ses manifestations est sans nul doute l'apparition dans certaines organisations du phénomène du BYOD (Bring Your Own Device), par lequel les collaborateurs sont autorisés (souvent contre une certaine compensation financière) à utiliser leur propre équipement informatique (PC, tablette, smartphone) pour travailler. Cette mise en place n'est pas non plus sans poser un certain nombre de problèmes de toutes natures : RH, juridique, fiscal, sécurité, technique, gouvernance...

Afin d'aider les utilisateurs et les entreprises à faire face aux défis posés par de tels usages, Windows 8 (et son compagnon d'aventure, Windows Server 2012) apportent, à mon sens, deux innovations tout à fait fondamentales. La première concerne la prise en charge native de ce que l'on appelle des « revendications », c'est-à-dire des affirmations telles que « je suis membre de la division RH », « j'ai plus de 18 ans », « j'ai un CDI »... Un contrôleur de domaine Windows Server 2012 va donc être capable d'émettre des groupes, mais aussi des revendications ! Et ces dernières concerneront non seulement l'utilisateur, mais aussi le terminal qu'il utilise, afin de créer une identité composite qui fait correspondre un utilisateur au terminal qui sera autorisé comme un principal (au sens Kerberos). De même, un jeton Windows 8 dispose de sections données utilisateur et terminal et des revendications ! Ceci va permettre de donner vie à la deuxième des innovations fondamentales de Windows 8/Windows Server 2012 : la notion de contrôle d'accès dynamique. Cette notion fonde l'accès aux ressources de type fichiers sur la base d'étiquettes, qui peuvent être ajoutées dynamiquement aux ressources en fonction de la localisation, de l'application, ou être ajoutées manuellement par le possesseur du contenu concerné. Ainsi, un système de contrôle intelligent sera mis en place, qui tirera dynamiquement parti des propriétés des utilisateurs et des états du terminal utilisé pour prendre des décisions d'autorisation.

Et l'on arrive au cœur de ce qui permet la mise en œuvre efficace et sécurisée d'une politique de BYOD. L'utilisateur obtiendra ou non l'accès à la ressource qu'il demande en fonction d'un contexte déterminé dynamiquement à l'aide des éléments suivants :

- la qualité de l'identité (identité Facebook ou identité interne, authentification à deux facteurs ou simple couple nom/mot de passe) ;
- la nature du terminal (approuvé, authentifié, en kiosque, géré, autogéré ou pas géré du tout) ;
- l'emplacement du terminal (derrière le pare-feu ou connecté à un hotspot Wi-Fi, depuis quel pays ?) ;
- les données (confidentielles ou non) et les applications (approuvées ou non, signées ou non) ;
- le rôle (collaborateur ou sous-traitant, membre de la direction...).

Une telle approche qui se définit par un niveau d'accès et une expérience utilisateur variable en fonction du contexte est, à mon sens, l'une des clés essentielles pour mettre en place le BYOD sans faire courir à l'entreprise des risques majeurs en termes de sécurité.

« Ceux qui comprennent ne comprennent pas qu'on ne comprenne pas » nous disait Paul Valéry. C'est parce que ceux qui ont choisi d'écrire cet ouvrage ne croyaient pas que cette citation leur était destinée qu'ils ont chaussé leurs bottes de pédagogues et mis tout leur talent pour porter au plus grand nombre des concepts quelquefois bien peu évidents.

« La sécurité est un voyage, pas une destination » dit-on souvent. Windows 8 sera donc pour vous, ami lecteur, une étape sur ce voyage. Voyageur, prenez donc le temps de visiter Windows 8 et sa sécurité au sein de cet ouvrage : vous ne serez pas déçu !

Bernard Ourghanlian  
Directeur Technique et Sécurité  
Microsoft France