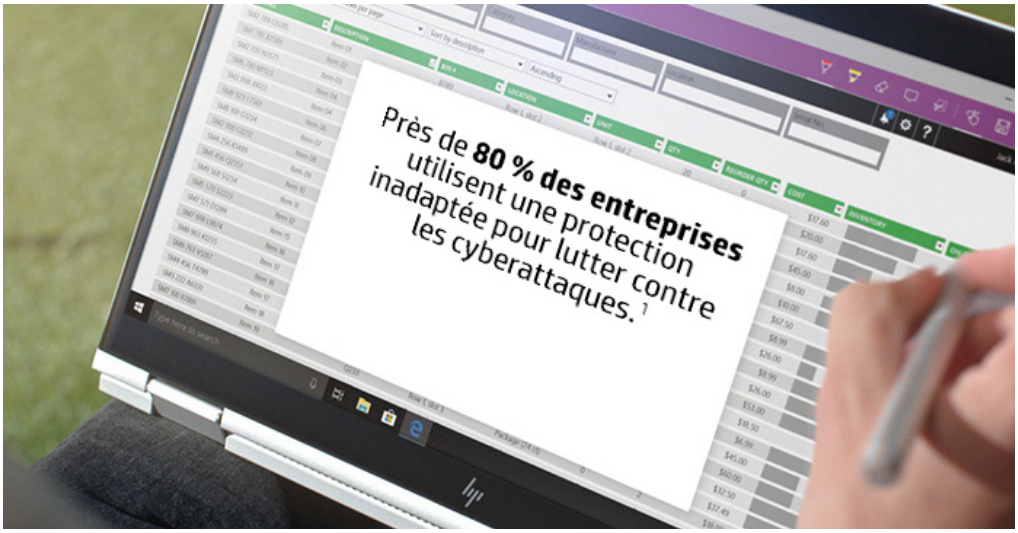
# Comment des défenses automatiques peuvent-elles protéger la flotte informatique de votre entreprise ?

En savoir plus




**Comment combattre une menace qui déjoue vos défenses ? Grâce à l'automatisation.**

600 milliards de dollars en un an. C'était le coût de la cybercriminalité dans le monde en 2017[2]. Ce nombre s'accroît à mesure que les pirates perfectionnent leurs techniques et leurs compétences. Selon une étude récente, 20 % des PME ont dû interrompre leurs activités professionnelles immédiatement suite à une cyberattaque, et 12 % ont subi des pertes de revenu[3]. L'une des dernières attaques insidieuses, nouveau cauchemar des responsables informatiques, est le piratage ciblant le micrologiciel lors du processus de démarrage des PC : les attaques du BIOS.

Des millions d'ordinateurs présentent des vulnérabilités basiques au niveau du BIOS, ce qui signifie qu'ils peuvent être piratés par des personnes qui ont des compétences modestes. Il y a quelques années, les chercheurs Xeno Kovah et Corey Kallenberg ont présenté un nouveau type d'attaque lors d'une conférence, révélant ainsi qu'en quelques heures, ils pouvaient pirater à distance le BIOS de plusieurs systèmes et le contaminer[4]. Étant donné que la plupart des BIOS partagent le même code, une fois que le premier est piraté, ce n'est plus qu'une question de temps avant que les mêmes techniques ne finissent par déjouer les défenses des autres appareils.

Ce type d'attaque est extrêmement dangereux, car il vise un élément qui n'est pas protégé. Il existe un espace caché entre le système d'exploitation et le matériel informatique, qui a longtemps été ignoré. Même si votre réseau semble étanche et que votre appareil est protégé par le meilleur logiciel de sécurité antivirus au monde, il existe tout de même un bref instant de vulnérabilité entre le démarrage et le lancement des défenses. C'est à ce moment que les attaques contre le BIOS se produisent.

Puisque la plupart des logiciels de sécurité informatique se trouvent au niveau du système d'exploitation, tout maliciel placé dans le BIOS (avant le démarrage et qui pénètre dans le Mode de gestion de système) ne pourra être détecté par le logiciel de sécurité du terminal. C'est ainsi que les pirates prennent le contrôle total de votre système. Ils peuvent alors voler vos données, les rendre illisibles ou propager d'autres maliciels dans le réseau de votre entreprise. Pire encore, il est quasi impossible de détecter cette brèche et la contamination subséquente.

La meilleure façon de protéger les appareils de votre entreprise est d'utiliser un système de sécurité à plusieurs volets. Les compétences de votre équipe informatique ne devraient pas se confiner aux scans constants et aux dépannages manuels. HP propose une réponse automatique, HP Sure Start[5], qui fait partie d'une gamme de solutions de sécurité.

« Ce produit est le fruit d'une collaboration avec HP Labs. Il permet aux entreprises de mieux gérer les risques et de protéger les utilisateurs ainsi que la productivité informatique contre les attaques malveillantes, les mises à jour échouées ou toute autre cause accidentelle ou inconnue. »

**– Vali Ali, chef de la technologie en matière de sécurité et de confidentialité au sein de l'unité commerciale PC de HP.**

## Comment des défenses automatiques peuvent-elles protéger les appareils de votre entreprise ?

HP Sure Start est un moyen de protection auto-réparant au niveau du BIOS. Nous appelons cette approche l'élasticité cybernétique. Le système repose sur la création d'un « maître » du BIOS qui procède directement au chiffrement de l'appareil. Dès lors, si quelqu'un tente de pirater votre BIOS, votre système se réinitialisera avant de charger le « maître », qui détruira le fichier contaminé et vous informera, vous et votre équipe, de l'attaque. En bref, la machine se répare toute seule.

Ce qui se traduit par une productivité ininterrompue. Par une réduction des coûts. Par des appareils plus conformes. Et surtout, par une façon plus simple de travailler.

Si vous vous demandez quelle est la façon la plus simple de vous procurer des appareils de pointe qui intègrent la technologie HP Sure Start, pensez à HP Device as a Service (DaaS)[6]. Il s'agit d'un modèle de service moderne pour ordinateur qui simplifie la façon dont les organisations commerciales fournissent à leur personnel un matériel et des accessoires adaptés. Le DaaS permet également de gérer une flotte multi-OS tout en obtenant des services dotés d'un cycle de vie plus long. HP DaaS propose des forfaits simples et flexibles, à un prix fixe par appareil, qui permettent à votre entreprise de fonctionner efficacement, sans accrocs.

Il est indispensable de surveiller les terminaux et les points d'accès à tous les niveaux. L'heure est venue de vous soucier des parties cachées de vos appareils. Chaque personne, entreprise et organisation du monde entier gagne en sûreté et en résistance grâce à la gamme de produits HP, qui inclut les PC HP EliteBook x360, avec en option la 8e génération de processeurs Intel® Core™ i7. En tant que produit de la gamme HP Elite, cet appareil met à votre disposition une technologie de sécurité grâce à ses caractéristiques intégrées telles que HP Sure Start.

**Découvrez les avantages des solutions de sécurité HP pour votre entreprise.**

---

**Sources :**


1. ID d'étude Statista 622857, «Small and medium sized enterprises in the U.S by Statista », octobre 2016
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Recherches menées par Osterman, commanditées par Malwarebytes : « Second Annual State of Ransomware Report: US Survey Results », juillet 2017
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems
5. Différentes générations d'HP Sure Start sont disponibles pour certaines configurations des systèmes HP Elite et HP Pro.
6. Les plans HP DaaS et/ou les composants inclus peuvent varier selon la région ou en fonction du partenaire de service HP DaaS agréé. Veuillez contacter votre représentant HP local ou votre partenaire DaaS agréé pour plus de détails dans votre région. Les services HP sont régis par les conditions générales d'utilisation HP applicables fournies ou indiquées au client lors de l'achat. Le client peut bénéficier de certains droits supplémentaires conformément aux lois locales applicables, et ces droits ne sont en aucun cas affectés par les conditions générales d'utilisation HP ou la garantie limitée HP fournie avec votre produit HP.




4AA7-3219FRE, avril 2019