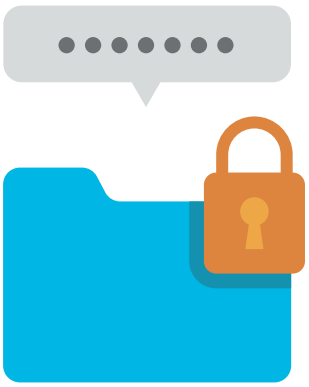
Livre blanc pour les entreprises

La sécurité commence aux points d'extrémité

Pourquoi prioriser la sécurité des points d'extrémité

Synthèse



En France, 68 % des entreprises ont déclaré avoir été victimes d'une fraude au cours des 24 derniers mois. Le nombre de fraudes reportées par les entreprises françaises a encore augmenté en 2016 (+ 13 points par rapport à 2014)[1]. Ces attaques informatiques sont de plus en plus conséquentes, fréquentes et coûteuses.

Le paradigme de sécurité « Défendre et protéger » - défense d'un périmètre réseau au moyen de pare-feux - est révolu. Détecter et réagir en amont est aujourd'hui devenu nécessaire.

Mais les budgets du SI ne suivent pas l'évolution de la cybersécurité. 77 % des dépenses vont toujours à la défense et la protection.[2] Seuls 36 % des responsables de la sécurité informatique considèrent qu'ils ont un budget suffisant pour sécuriser efficacement les points d'extrémité.[3]

Une protection renforcée des données est possible. Avec la bonne technologie, la bonne stratégie et des ressources suffisantes, les organisations peuvent se protéger des cyberattaques.

Faute d'augmenter les investissements en cybersécurité et d'adapter les investissements aux besoins d'une défense vraiment efficace, les entreprises laissent leur porte ouverte aux menaces informatiques, augmentant le risque de dégâts financiers sévères pour l'organisation.

Introduction

La cybersécurité : un défi majeur pour les entreprises
60 % des responsables informatiques pensent que leurs défenses sont dépassées par la sophistication et le nombre des cyberattaques. 80 % des responsables sécurité considèrent que les Menaces persistantes avancées (Advanced Persistent Threats ou APT), les entreprises criminelles, les hackers activistes et le piratage d'État s'accentuent et représentent le principal défi de la sécurité informatique.[4]

L'explosion de la cybercriminalité positionne la France comme l'un des pays les plus touchés dans le monde.[5] Le coût de la cybercriminalité a été chiffré en France en 2015 à 3,7 milliards de dollars selon l'enquête 2016 de PwC sur la sécurité de l'information.

Les attaques venues de l'extérieur - virus, logiciels malveillants, phishing - prédominent, mais celles provenant de l'intérieur sont plus coûteuses.[6] Et une bonne part de ces attaques externes proviennent de vulnérabilités internes, d'employés négligents qui ne respectent pas les consignes de sécurité, de machines non protégées raccordées au réseau - ce que 81 % des personnes interrogées dans l'enquête Ponemon considéraient comme la plus grande menace en matière de sécurité informatique.

Et avec le temps, cela ne fera qu'empirer. Le point d'extrémité est le nœud le plus faible de n'importe quel réseau et, avec l'accroissement du BYOD (« Bring Your Own Device »), du télétravail et de l'Internet de Objets, les points d'extrémité prolifèrent. Ce qui signifie que les points d'entrée des hackers se multiplient eux aussi.

Le temps du réseau d'ordinateurs de bureau reliés par Ethernet est bien loin. Les réseaux d'entreprise sont devenus amorphes et complexes : ce sont aujourd'hui une combinaison d'appareils personnels et professionnels, donnant librement accès aux données via des points d'accès Wi-Fi internes ou externes.

A partir de ce constat, il est nécessaire d'actualiser sa ligne de défense, et de l'adapter aux nouvelles menaces.

Dans ce livre blanc, nous allons examiner la nature et l'importance de la menace - pour mieux connaître notre ennemi - avant d'aborder la cybersécurité à l'époque des appareils multiples, des réseaux non sécurisés et du Cloud.

[1] Global Economic Crime Survey 2016 – PwC France https://www.pwc.fr/fr/assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_v3.pdf
[2] Gestion de la Réponse aux Incidents - étude PAC 2015 : https://www.pac-online.com/download/19443/155514
[3] Rapport Ponemon 2016 sur l'État du point d'extrémité
[4] Évaluation d'IBM CISO en 2014
[5] Global Economic Crime Survey 2016 – PwC France https://www.pwc.fr/fr/assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_v3.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

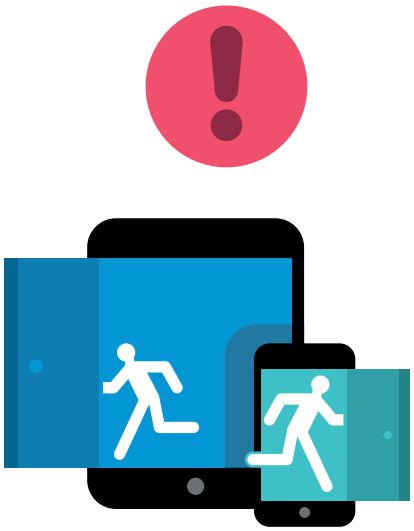
L'ampleur de la menace

1,8 milliard d'euros. C'est le coût global représenté par les cyberattaques qui ont touché 13,7 millions de Français en 2016.[7]

La cybercriminalité coûte cher. Pertes de valeur pour ce qui a été volé ou endommagé. Perte de chiffre d'affaires dû à une détérioration de l'image et à une perte de productivité. Ressources perdues en remise en état - temps de service support, déploiement de nouvelles politiques de sécurité, départ de collaborateurs et autres réactions en interne. Amendes et pénalités infligées par les autorités de contrôle, et baisse du cours de bourse.

La menace ne pourra que croître avec le nombre d'appareils connectés au réseau. En raison de l'Internet des Objets, Gartner Group prévoit 11,4 milliards d'appareils connectés en 2018, contre 6,4 milliards en 2016. En 2020, plus de 25 % des attaques subies par les entreprises seront liées à l'Internet des Objets, mais l'Internet des Objets représentera moins de 10 % des budgets sécurité.[8]

La cybercriminalité représente une menace considérable, et elle s'aggrave.



Quels types de menaces en France ?

Les entreprises subissent d'innombrables attaques tous les jours. La plupart sont des virus ou logiciels malveillants de faible intensité. Mais des attaques plus sérieuses sont de plus en plus courantes. Selon PwC, 73% des entreprises françaises en 2016 anticipaient des actes de cybercriminalité au cours des 24 prochains mois, mais seules 37% des entreprises françaises disposent d'un plan de réponse opérationnel pour faire face aux incidents de cybercriminalité.[9]

Face à ces menaces malheureusement bien réelles, les entreprises ont pourtant fortement augmenté leurs investissements dans le domaine de la sécurité. Le budget moyen annuel relatif aux coûts de cybersécurité est passé de 3,7 à 4,8 millions de dollars entre 2014 et 2015 en France, soit une augmentation de 29%, selon l'enquête 2016 de PwC sur la sécurité de l'information.

Selon la même enquête, le nombre d'attaques d'ampleur, de type DDoS (Attaque par déni de service), coordonnées et souvent perpétrées par des réseaux criminels a doublé en France au cours des douze derniers mois.

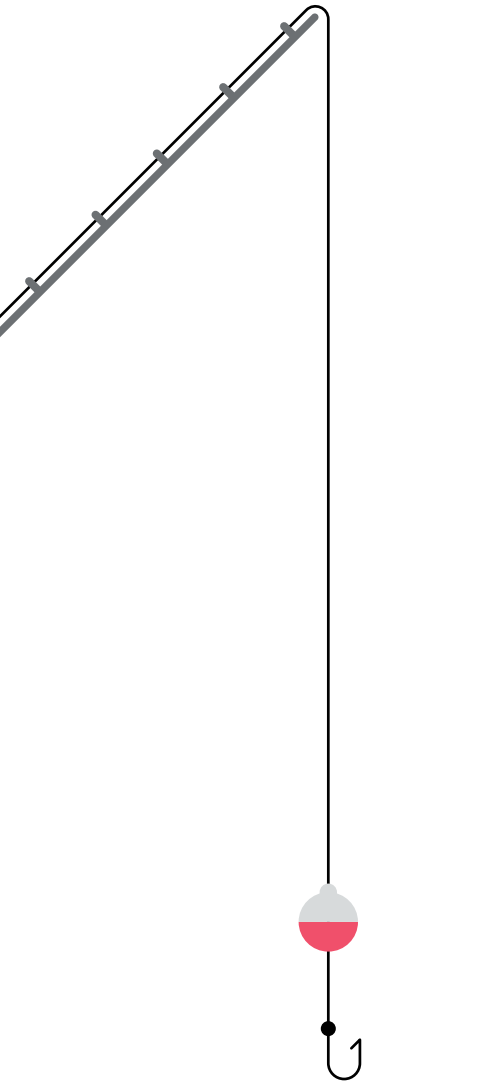
On parle maintenant de cybercriminalité collaborative dans la mesure où les organisations criminelles associent des compétences diverses : informatique, comptabilité, finance et expertise métier. Mais quelles sont les données visées par ce type d'attaque ? Selon PwC, sont ciblées en priorité les données relatives aux clients (37%), puis celles concernant les employés (32%), sachant que l'on a assisté au cours des derniers mois à une progression fulgurante des vols de données relatives à la propriété intellectuelle (26%) qui ont plus que doublé.

[7] Rapport annuel 2016 Symantec - https://www.symantec.com/content/dam/symantec/fr/docs/reports/2016-norton-cyber-security-insights-comparisons-france-fr.pdf

[8] http://www.gartner.com/newsroom/id/3291817

[9] Global Economic Crime Survey 2016 – PwC France https://www.pwc.fr/fr/assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_v3.pdf

Comment les violations se produisent-elles



Les médias décrivent la plupart du temps des pirates informatiques rusés et intelligents, parvenant à déjouer les défenses de réseaux sécurisés des entreprises, mais la réalité est en général plus prosaïque.

Les virus peuvent profiter de réseaux compromis, mais les logiciels malveillants s'appuient le plus souvent sur les erreurs humaines. Les attaques de type phishing en dépendent entièrement. Les attaques à grande échelle, par déni de service et vols de données, sont aussi causées bien souvent par la négligence d'utilisateurs.

Le piratage de Dropbox serait dû à un employé de l'entreprise qui utilisait son mot de passe LinkedIn pour accéder aux systèmes internes de l'entreprise.[10] Plus récemment, une attaque informatique massive s'est déclarée en Europe en juin 2017, touchant dans un premier temps l'Ukraine avant de se répandre à plusieurs pays européens dont la France.[11]

Les pirates n'ont pas besoin d'une aide active pour réussir. L'ignorance ou le non-respect des protocoles de sécurité sont tout aussi pernicieux. L'utilisation de leur propre équipement au travail et l'usage de logiciels du Cloud par les employés est une menace croissante : les deux introduisent des éléments non sécurisés dans un réseau par ailleurs sûr, échappant au contrôle de la direction informatique, et causant une vulnérabilité non prise en compte.

La plupart du temps, les pirates n'ont pas besoin d'algorithmes perfectionnés ou de technologies de pointe, il leur suffit que l'un de nous soit peu vigilant.

Le pare-feu est rompu

Jusqu'à récemment, les remparts de sécurité étaient constitués par des logiciels anti-virus et des pare-feux, afin de créer un périmètre sécurisé. Dans l'environnement de travail actuel, cette stratégie n'est tout bonnement plus suffisante.

Selon le rapport Ponemon, 81 % des personnes interrogées indiquent que les appareils mobiles de leur réseau ont été la cible de logiciels malveillants. Parmi les autres risques, l'usage par les employés d'applications commerciales sur le Cloud - cité par 72 % des personnes interrogées -, le BYOD (69 %) et le télétravail, de chez soi ou depuis d'autres sites (62 %), représentent des failles de sécurité grandissantes.[12]

Dit simplement, un pare-feu se justifiait quand vous-même, en tant qu'administrateur, détenait le contrôle des appareils connectés. Mais dans une époque où les employés viennent au travail avec leurs propres appareils - souvent plusieurs - et où un nombre croissant de collaborateurs se connectent à distance, protéger le périmètre n'est tout simplement plus possible. Chaque appareil non vérifié est un point d'extrémité vulnérable que les pirates peuvent exploiter.

[10] http://www.numerama.com/tech/191949-une-base-de-68-millions-de-comptes-dropbox-circule-chez-les-pirates.html

[11] http://www.zdnet.fr/actualites/ransomware-nouvelle-attaque-informatique-d-ampleur-visant-les-entreprises-en-europe-maj-39854266.htm

[12] Rapport Ponemon 2016 sur l'État du point d'extrémité

La perspective HP : aller au-delà de la sécurité du réseau

Michael Howard, Directeur des solutions de sécurité pour la division imagerie et impression de HP, sur la politique de sécurisation des points d'extrémité.

Une préoccupation actuelle réside dans le constat que les entreprises ont du mal à sécuriser chaque point d'extrémité par manque de prise de conscience et de connaissance de certains appareils et des risques qu'ils comportent. Elles se sentent à l'abri derrière un pare-feu, bien que celui-ci ne soit plus une protection suffisante en cas d'attaque. Les équipes de sécurité doivent connaître chaque point d'extrémité de l'infrastructure et vérifier qu'il dispose de couches de protection multiples contre des attaques de plus en plus sophistiquées.

Les équipes de sécurité informatique doivent connaître chaque recoin de leur infrastructure informatique d'entreprise et construire une couche protectrice supplémentaire au-dessus du périmètre réseau standard. Les pare-feux à eux seuls ne peuvent lutter contre des attaques sophistiquées, et une politique de défense avec des couches de protections multiples à chaque point d'extrémité est un must-have pour garantir la conformité de votre entreprise avec les réglementations et éviter des amendes importantes.

La politique d'HP est de se préoccuper en premier lieu de la sécurité pour tout nouveau produit, service ou solution développé(e). Les équipes de développement savent qu'elles doivent adapter les innovations et répondre aux niveaux de sécurité les plus évolués.

Plus que jamais, la sécurité doit être native, et non surajoutée. C'est la politique d'HP depuis des années.

La sécurité en profondeur

Une nouvelle approche de la cybersécurité se doit d'être une protection multicouche.
La sécurité du réseau conserve son importance, mais doit être constituée elle-même à partir de réseaux segmentés. De nombreuses violations reposent sur une effraction initiale donnant accès à l'intégralité du système. Pour éviter que le vol d'une seule clé ne fasse tomber l'ensemble du réseau, il est essentiel d'entourer les informations sensibles de plusieurs barrières concentriques.

La prise en compte de la totalité des appareils est indispensable. La principale difficulté rencontrée par les Responsables informatiques réside dans la couverture de chaque appareil connecté au réseau, qui doit être protégé par un logiciel de sécurité - contre les virus, les logiciels espions et malveillants - mis à jour régulièrement et régulièrement inspecté pour détecter des anomalies. Mieux vaut utiliser les appareils eux-mêmes comme capteurs, collectant des informations en temps réel pour donner l'alerte en cas de violation du périmètre du réseau dont ils font partie.

Une gouvernance ne laissant rien au hasard en matière de sécurité doit être en place, chaque employé étant formé aux protocoles de cybersécurité. L'erreur humaine - cliquer sur le mauvais lien, se connecter à partir d'un appareil grand public - est l'ennemi numéro un du réseau. La formation des employés permet de répondre à la négligence humaine.

Sécurité des appareils

L'une des premières préoccupations est de contrôler quels appareils ont accès au réseau.
La solution simple souvent choisie consiste à avoir des réseaux Wi-Fi séparés pour les visiteurs et pour les employés, de sorte que les appareils externes non sécurisés ne puissent avoir accès au réseau principal. Ceci va de pair avec l'habitude à donner aux employés pour utiliser ce dernier réseau avec leurs appareils personnels.

L'autre solution consiste à assurer le contrôle des appareils des employés. Cette préoccupation doit alimenter la politique de la société concernant le BYOD (Bring your own device) ou le CYOD (Choose your own device). Un argument fort en faveur d'une politique CYOD réside dans la possibilité de contrôler quels équipements sont utilisés, de choisir ceux qui ont la meilleure sécurité, de gérer leur configuration et de mieux les surveiller.

Privilégier l'un des PC de notre gamme Elite à un portable bon marché vous assure de bénéficier d'une protection optimale. Chaque PC Elite dispose de la technologie HP SureStart qui vérifie le BIOS tous les quarts d'heure et réinitialise la machine si une anomalie est détectée, bloquant l'accès aux visiteurs indésirables. C'est cette fonction - ajoutée à beaucoup d'autres - qui a valu à nos PC de la série Elite 800 d'être déclarés « les PC les plus sûrs au monde. »[13] Mais il est peu probable que des employés possèdent eux-mêmes un PC HP Elite.

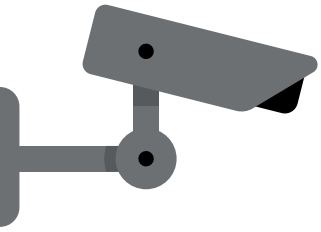
Les employés préfèrent se servir de leurs propres appareils pour deux raisons :
1. La technologie grand public est souvent supérieure à celle qu'on leur fournit sur le lieu de travail
2. Les employés aiment utiliser la technologie qui leur est familière

En offrant une politique CYOD disposant des bonnes ressources, avec les équipements les plus récents mis à jour régulièrement, les organisations peuvent fournir aux employés des matériels supérieurs aux leurs, et assurer un meilleur contrôle de sécurité. C'est la raison pour laquelle nous proposons HP Device as a Service (DaaS - l'Appareil en tant que service).

Il est primordial d'inclure tous les appareils dans la stratégie de sécurité, même ceux que l'on oublie souvent. Une enquête récente menée par Spiceworks met en évidence le manque de considération des entreprises concernant la protection des imprimantes en réseau.[14] Seuls 16% des participants pensent que les imprimantes représentent une grande faille de sécurité pour leur réseau.

La moyenne des violations de sécurité avant la mise en place d'une politique de sécurité des imprimantes était de 9,9 par an, pour un coût moyen de 456 500 € (amendes comprises). Suite à la mise en place d'une politique de sécurité des imprimantes, ce nombre était tombé à 1,5, économisant 200 heures de temps d'employé par an et 218 000 € de frais connexes, y compris d'audit et de mise en conformité.[15]

[13] http://store.hp.com/FranceStore/Merch/Offer.aspx?p=b-elite-pc-portable
[14] https://h30657.www3.hp.com/t5/BusinessBlog-fr/Ne-sous-estimez-pas-le-danger-des-imprimantes-non-sécurisées-pour-votre-réseau/ba-p/9095
[15] La valeur pour l'entreprise de la sécurisation des imprimantes - étude IDC 2015



Détection et mesures proactives

77 % des dépenses de sécurité informatique vont aux technologies de prévention et de protection telles que les logiciels anti-virus et les pare-feux, selon une étude de PAC. Mais cette approche n'est pas efficace. L'étude a également montré que 67 % des entreprises interrogées avaient subi une violation de sécurité au cours des 12 derniers mois, et 100 % dans le passé.[16]

Les logiciels anti-virus, en particulier, sont d'une inefficacité choquante. Le fournisseur de sécurité Damballa a effectué des tests au cours desquels ils attaquaient délibérément un réseau pour mesurer la réaction aux virus.[17] Il aura fallu plus de six mois avant que 100 % des fichiers malveillants soient identifiés. Il a fallu entre un et six mois avant que les entreprises découvrent qu'elles avaient été attaquées.

La sécurisation des points d'extrémité ne peut plus reposer seulement sur la prévention. Le nombre croissant d'incidents dus aux virus et aux logiciels malveillants, plus les risques inhérents au BYOD et au télétravail, signifie que des violations sont inévitables. Personne ne propose d'abandonner complètement la prévention et la protection, mais à l'évidence, détection et réaction doivent remonter dans l'ordre des priorités.

Une surveillance continue en temps réel s'impose, idéalement en utilisant les points d'extrémité eux-mêmes comme capteurs - donnant l'alerte à l'ensemble du réseau en cas de violation. Ceci permet à la sécurité informatique de réagir, en employant des processus tels que :

- Éteindre un appareil à distance
- Arrêter un processus infecté ou qui répand un logiciel malveillant
- Mettre en quarantaine un fichier ou un groupe de fichiers particuliers
- Interrompre les communications réseau pour isoler les appareils infectés

Accepter que des violations peuvent se produire et mettre en place les protocoles de réaction adéquats - ainsi que la technologie nécessaire pour les appliquer - voilà la seule solution pour garantir la cybersécurité des entreprises.

« Aucune technologie ne peut fournir de sécurité si les gens la compromettent. »

– Joseph Steinberg [18]

Sécurité des employés

La sécurisation des appareils implique la sécurisation des utilisateurs.
Chaque employé doit être formé à la cybersécurité. Les collaborateurs doivent être conscients du risque de phishing, et du risque lié à la visite de sites web douteux ou du téléchargement des pièces jointes suspectes. Ils doivent être conscients de la politique concernant d'utilisation de mots de passe fiables, spécifiques pour chaque accès, et de l'importance de les stocker avec un bon gestionnaire de mots de passe.

Ils doivent avoir conscience de l'importance de mettre à jour régulièrement les logiciels de sécurité, pour alléger le travail de contrôle des équipes informatiques. Ils doivent être attentifs à n'utiliser que des appareils sûrs pour se connecter aux réseaux de l'organisation et à éviter d'utiliser des appareils personnels sur des réseaux externes non sécurisés pour accéder à des données sensibles.

De nombreux experts de haut niveau en cybersécurité recommandent d'effectuer des simulations d'attaques par phishing - allant jusqu'à construire de faux sites web, pour exercer chaque employé - et de créer de véritables cursus de formation à la cybersécurité. Car la plupart des attaques reposent sur l'exploitation des faiblesses humaines, qu'il s'agisse de négligences ou de malveillances.

Les Responsables informatiques ne doivent pas oublier que les employés constituent le maillon faible de n'importe quel réseau.

[16] Gestion de la Réponse aux Incidents - étude PAC 2015
[17] https://www.tomsguide.fr/actualite/antivirus-malwares,46524.html
[18] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusion

La sécurité informatique doit évoluer vers une politique de détection aux points d'extrémité comprenant les réactions proactives adaptées.
La protection des données de l'organisation dans le climat informatique actuel - confronté à la montée de la menace de la cybercriminalité et à la perte de contrôle du périmètre du réseau - demande deux choses : une prise de conscience et plus de ressources.

Le concept de réseau doit évoluer. L'idée du réseau en tant que barrière entourant un ensemble d'appareils n'a plus cours. Il est temps de voir la réalité en face. « Le réseau » est une chimère. Il émerge à partir des appareils connectés - chacun étant un point d'extrémité. Sécuriser le réseau signifie sécuriser le point d'extrémité, en prenant en compte deux composantes : l'appareil et l'utilisateur.

Mais assurer la sécurité avec ce nouveau paradigme est bien plus complexe que dans l'environnement PC-connecté-via-Ethernet d'antan. Il faut plus de ressources, et il faut les réclamer. Et cela, 61 % des personnes interrogées par Ponemon en sont conscientes.

Pour y parvenir, l'astuce consiste à faire adhérer le reste de l'organisation. Seulement 36 % des personnes interrogées considéraient qu'elles disposaient du budget et des effectifs adéquats pour la sécurité des points d'extrémité. 69 % disent que le département informatique ne peut faire face à la demande de support des employés. 71 % estiment que les politiques de sécurisation du point d'extrémité sont difficiles à faire appliquer.[19]

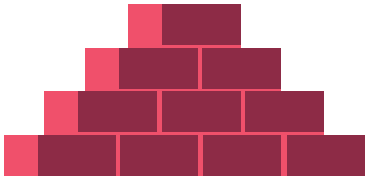
80 % des Responsables sécurité informatique considèrent que le meilleur argument pour assurer le financement de leurs programmes de sécurité est le respect des contraintes légales, mais jugent également que ce n'est pas là, de loin, la principale raison de dépenser de l'argent.[20]

Les décideurs informatiques doivent se rapprocher des cadres dirigeants pour souligner l'importance de la sécurité. Montrer ce que coûte une sécurité laxiste - frais de remise en état, perte de chiffre d'affaires, cours de bourse en berne - et insister sur les économies à long terme. Beaucoup de solutions de sécurité génèrent également des améliorations. Songez à la productivité accrue résultant de la sécurisation des imprimantes, et aux gains de productivité qu'apporte une technologie régulièrement remise à niveau dans le cadre d'un programme de CYOD souple, fourni par un abonnement à un tiers (tel que HP DaaS).

Le défi est colossal. Et, au fil du temps - avec l'explosion de l'Internet des Objets et la sophistication de la cybercriminalité - il deviendra encore plus conséquent. Mais on peut y faire face. Avec la bonne technologie, la bonne stratégie, et les ressources adéquates, nous pouvons défendre nos points d'extrémité. Nous pouvons faire en sorte que nos données soient en sécurité.

Pour plus d'informations et des conseils pratiques donnés par les experts chez HP, consultez notre guide sur « La cybersécurité et votre entreprise».

Pour vous aider à appliquer un programme complet, souple et sécurisé de CYOD, découvrez **HP Device as a Service.**



Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA7-1089FRE

[19] Rapport Ponemon 2016 sur l'État du point d'extrémité
[20] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697