Argumentaire de vente

Sécurité d'impression HP

Les menaces de sécurité évoluent tous les jours. Chaque imprimante sur le réseau d'une entreprise constitue un point sensible, y compris les imprimantes réseau. Grâce à la sécurité innovante des périphériques, des données et des documents de HP, vous protégez votre parc, répondez aux exigences de conformité et identifiez de façon proactive les failles du système de défense.

64 %

des responsables informatiques considèrent que leurs imprimantes sont probablement infectées par un programme malveillant[1]

73 %

des RSSI s'attendent à une faille de sécurité importante au cours de l'année[2]

26 %

des failles de sécurité importantes signalées par les responsables informatiques proviennent des imprimantes[3]

Clients cibles

Les organisations, quelle que soit leur taille, partout dans le monde, tous les secteurs ayant besoin de sécuriser leurs environnements partagés de numérisation et d'impression.

Contact cible

- Chef de la sécurité de l'information ou Responsable de la sécurité informatique
- Directeur des systèmes d'information
- Responsables sécurité/conformité
- Responsables informatiques et décideurs

Particularités des clients

- Ils augmentent les configurations de sécurité requises en raison de menaces et de conformité réglementaire
- Ils refusent d'accepter les risques d'une ouverture de leur réseau à des failles
- Ils sont confrontés à d'importantes amendes de mises en conformité en raison de réglementations impliquant la gestion des données des clients
- Ils utilisent des données fortement confidentielles dans le cadre de leurs activités quotidiennes (ex. FSI, HC et PS)

Situation du marché

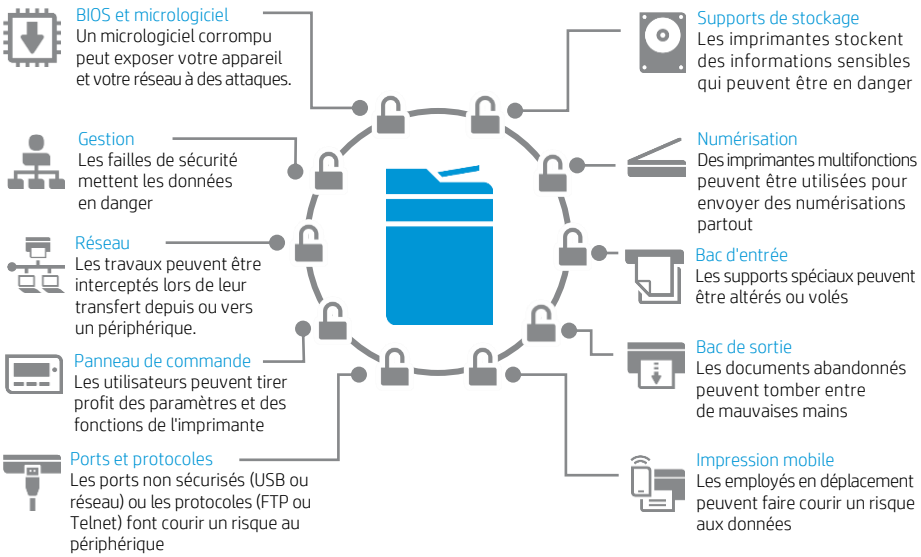
Si de nombreuses organisations ont signé un contrat avec un prestataire de services d'impression pour optimiser leur infrastructure d'impression afin d'augmenter leurs rendements et réduire les coûts d'impression, la sécurité d'impression a été largement négligée dans les exigences contractuelles. Mais en raison d'une complexité croissante et de la persévérance des cybercriminels, les pare-feu réseau s'avèrent des mesures de sécurité insuffisantes. Il faut que les entreprises renforcent leurs points d'extrémité derrière le pare-feu, y compris les imprimantes réseau.

Qu'il s'agisse d'une cyberattaque malveillante, d'une faille interne accidentelle, ou de non-conformité, réglementaire ou légale, le coût de la résolution d'une faille de sécurité peut s'avérer énorme. Le coût annuel moyen est d'environ 7,7 millions USD[4] et peut comprendre des amendes, une perte d'activité, une réputation ternie et des recours collectifs.

Les exigences réglementaires et de conformité se complexifient sans cesse. Les organisations ont besoin de périphériques et de solutions qui leur permettent de respecter les réglementations.

Difficultés de la sécurité des clients

De nombreux départements informatiques appliquent avec rigueur des mesures de sécurité aux ordinateurs individuels et au réseau de l'entreprise, cependant les dispositifs de numérisation et d'impression sont souvent négligés et restent exposés.



Outils d'évaluation
Encourager vos clients à utiliser les outils HP pour évaluer la sécurité de leur environnement d'impression.

- Étude d'analyse de HP Secure : auto-évaluation en ligne pour déterminer s'ils suivent les meilleures pratiques dans le domaine de la sécurité d'impression : hp.com/go/SPA
- Évaluation rapide HP : évaluation technique rapide de jusqu'à 13 installations sur un maximum de 20 imprimantes HP : hp.com/go/quickassess

Besoins de sécurité des clients

Il faut à vos clients des moyens faciles pour protéger leurs périphériques, données et documents. Ils veulent aussi une gestion rationalisée de la sécurité d'impression et des rapports de sécurité pour gagner du temps informatique.

Sécurité de l'appareil

- Protection du BIOS et des micrologiciels des attaques et des programmes malveillants.
- Micrologiciel pouvant être mis à jour
- Sécurisation des paramétrages et les mots de passe des périphériques

La sécurité des données

- Cryptage des données stockées ou en transit
- Périphériques de niveau CA-certificats numériques signés
- Effacement et élimination du disque dur sécurisé
- Authentification avancée et contrôle de l'accès
- Solutions d'impression mobile sécurisée

Sécurité des documents

- Solutions d'impression à la demande sécurisée
- Solutions anti-fraude et anti-contrefaçons

Contrôle de la sécurité du parc et conformité

- Affectation et remise en état automatique des paramètres de sécurité des périphériques dans l'ensemble du parc d'impression (une imprimante multifonction Enterprise compte plus de 250 paramètres de sécurité)
- Détection de vulnérabilités de sécurité proactive et signalement
- Création de rapports avancés pour aider à établir la conformité

Proposition de valeur pour le client

- Limitation du risque de cyberattaques coûteuses
- Protection des données et documents sensibles
- Gain de temps en automatisant la gestion de la sécurité du parc
- Maintien de la conformité de votre entreprise aux normes industrielles – et bénéficiez d'un accès facile aux données pour les rapports de conformités

Proposition de valeur pour le partenaire

- Une possibilité de croissance, puisque les clients investissent de façon active dans la sécurité d'impression (« Améliorer la sécurité » est désormais la raison n°1 pour laquelle les organisations passent aux MPS[5])
- Conduit à une conversation sur la valeur qui vous permet de vendre plus haut dans l'organisation ; les innovations de sécurité HP dans le domaine de la sécurité peuvent faire basculer la conversation du prix à la valeur ajoutée.
- Signale à vos clients que HP investit activement dans l'innovation de la sécurité d'impression et maintient son leadership dans le domaine de la sécurité.

Questions de sélection

Posez à ces questions à votre client :

- Disposez-vous d'une stratégie de sécurité pour vos périphériques de numérisation et d'impression ?
- Gérez-vous actuellement des informations sensibles, telles que l'identité des employés ou des données clients ?
- Cryptez-vous les travaux d'impression ?
- Vos imprimantes sont-elles protégées des programmes malveillants et des virus ?
- À quelle fréquence appliquez-vous les mises à jour de micrologiciel de votre imprimante ?
- Avez-vous installé des mots de passe administratifs à vos imprimantes, ou tout le monde a-t-il la possibilité de modifier librement les réglages des périphériques ?
- Combien de temps le service informatique consacre-t-il à la configuration des imprimantes ?

Offres de sécurité HP

Les fonctions de sécurité intégrées aux périphériques HP, associées aux solutions logicielles leaders de l'industrie de HP, peuvent aider les entreprises à protéger leurs périphériques, données et documents. En outre, elles aident vos clients à gérer plus facilement la sécurité de leur parc et la conformité.

Imprimantes sécurisées

Les imprimantes les plus sécurisées au monde[7] pour protéger, détecter et rétablir : imprimantes HP LaserJet et PageWide Enterprise et imprimantes multifonctions. Les fonctionnalités de sécurité uniques comprennent :

- **HP FutureSmart** – Micrologiciel optimisable pour protéger son investissement ; ajouter facilement de nouvelles fonctions à votre parc existant
- **HP Sure Start** – Valide l'intégrité du code BIOS ; si le BIOS est corrompu, le périphérique redémarre et charge une copie saine et viable de celui-ci
- **Les listes blanches** – Elles permettent de vous assurer que seul le code HP connu et authentique est chargé au sein de la mémoire
- **La détection des intrusions en cours de fonctionnement** – permet de détecter les anomalies potentielles lors des opérations complexes réalisées par le micrologiciel et la mémoire
- **Cryptage du module du disque dur** – HP utilise le cryptage et décryptage du module du disque dur 256 bits Advanced Encryption Standard (AES)
- **Intégration SIEM** – Il est possible de configurer les imprimantes HP Enterprise pour fournir les données de l'imprimante à ArcSight, Splunk, ou SIEMonster pour contrôler les menaces de sécurité

Logiciel sécurisé

Au-delà du périphérique, HP offre des solutions de détection, protection, contrôle et gestion du parc, et de sécurisation des données et documents avec le temps.

- **HP JetAdvantage Security Manager** – Le seul outil de conformité basé sur la politique du secteur[6] automatise la gestion de la sécurité du parc.
  - Supporte la création de la politique de sécurité et son déploiement dans le parc
  - La fonction de sécurité Instant-on configure automatiquement les nouveaux périphériques ou les périphériques qui ont été redémarrés
  - Les rapports basés sur les risques permettent à l'équipe informatique de visualiser rapidement le statut du parc et de prouver la conformité
  - Application automatisée et mise à jour de certificats de Certificats de périphérique signés par CA uniques
- **HP Access Control** – Ce puissant logiciel de gestion permet de sécuriser les tâches d'impression et les périphériques, d'améliorer le flux des tâches, de contrôler les pratiques d'impression, – tout en réduisant vos coûts et en prenant en charge la sécurité, la conformité et les initiatives environnementales à l'échelle de votre entreprise. L'authentification avancée limite l'accès aux dispositifs, et l'impression sécurisée à la demande protège les documents.
- **HP JetAdvantage Impression sécurisée** – Une solution d'impression sécurisée à la demande basée sur le cloud abordable conçue pour les PME. Les tâches peuvent être archivées dans le cloud, ou sur le bureau de l'utilisateur. Facile à installer, à utiliser, il est compatible avec des dispositifs multi-vendeurs, et permet aux utilisateurs d'obtenir leurs impressions à partir d'un dispositif mobile[8].
- **HP JetAdvantage Connect** – L'impression mobile intuitive, fiable, conçue pour l'entreprise. S'appuyer sur les outils informatiques de réseau et les politiques pour gérer l'impression mobile[9]. Les utilisateurs peuvent imprimer de façon sécurisée à partir de leurs smartphones et leurs tablettes – où et quand ils en ont besoin.
- **HP et TROY Solution d'impression de documents sécurisés** – Technologies de prévention des fraudes intégrées aux documents les plus importants, ce qui permet de respecter les exigences de conformité administratives, réglementaires et internes. Permet à 5 imprimantes HP LaserJet noir et blanc PCL 5 d'imprimer des documents sécurisés sur papier ordinaire.

Services sécurisés

- **Les services de recyclage personnalisés HP** – suppriment les données des disques durs avant de recycler les anciens produits de façon responsable. Plus d'informations sur hp.com/go/businessrecycling.

HP JetAdvantage Security Manager
Assurez la sécurité de votre parc d'impression HP avec cette solution qualifiée de novatrice par Buyers Laboratory (BLI)[6].

Sécurité HP par rapport à la concurrence

Bien que certains concurrents proposent quelques-unes des multiples fonctionnalités de sécurité de base offertes par HP de manière standard, ces derniers arrivent difficilement à la cheville de notre gamme complète de solutions et outils de contrôle de la sécurité basés sur des règles, compatibles avec le logiciel HP JetAdvantage Security Manager proposé en option[10].

		HP	Xerox	Lexmark	Ricoh	Konica Minolta	Kyocera	Canon
Périphérique	Sure Start (protection du BIOS)	✓	⊘	⊘	⊘	⊘	⊘	⊘
	Liste blanche	✓	✓	✓	⊘	⊘	⊘	⊘
	Détection d'intrusion en cours de fonctionnement	✓	⊘	⊘	⊘	⊘	⊘	⊘
	Affectation de la politique de sécurité et remise en état	✓	⊘	⊘	⊘	⊘	⊘	⊘
Données	Contrôle de l'accès	✓	✓	✓	✓	✓	✓	✓
	Moyens de communication cryptés	✓	✓	✓	✓	✓	✓	✓
	Disponibilité TPM	✓	⊘	⊘	✓	✓	⊘	✓
	Disques durs cryptés intégrés avec effacement du stockage de sécurité	✓	✓	✓	En option	✓	✓	✓
Solutions documents	Solutions d'impression à la demande via numéro d'identification personnel	✓	✓	✓	✓	✓	✓	✓
	Mesures anti-fraude et anti-contrefaçon	✓	✓	✓	✓	✓	✓	✓

Comparaisons avec la concurrence

Aucun des concurrents figurant ci-dessous ne propose d'outils de gestion des applications de sécurité de parc, fondé sur la politique. Ils ont aussi de graves manquements en comparaison de la Sécurité des périphériques HP[10].

Xerox : Démarrage sécurisé, détection des intrusions pendant le fonctionnement, et l'intégration SIEM n'est pas disponible. Xerox mise sur son partenariat avec McAfee (Intel Security) pour fournir des listes blanches et une protection/notification pour une tentative de falsification de fichier système (à un coût supplémentaire par périphérique). Xerox ne propose pas le Trusted Platform Module (TPM) pour une sécurité supplémentaire.

Lexmark : La fonction de démarrage sécurisé de Lexmark ne s'auto-répare pas – une intervention est nécessaire pour corriger le dispositif. La détection d'intrusion pendant le fonctionnement et le TPM ne sont pas disponibles. Pour la gestion de la sécurité, Lexmark alimente des configurations spécifiques au modèle, auxquelles les paramètres clés ont défaut.

Ricoh : La fonction de démarrage sécurisé de Ricoh ne s'auto-répare pas – une intervention est nécessaire pour corriger le dispositif. Les listes blanches, la détection des intrusions pendant le fonctionnement, et l'intégration SIEM ne sont pas disponibles.

Konica Minolta : La fonction de démarrage sécurisé ne s'auto-répare pas – une intervention est nécessaire pour corriger le dispositif. Les listes blanches, la détection des intrusions pendant le fonctionnement, et l'intégration SIEM ne sont pas disponibles.

Kyocera : Les listes blanches, la détection des intrusions pendant le fonctionnement, et l'intégration SIEM ne sont pas disponibles.

Canon : Les listes blanches, la détection des intrusions pendant le fonctionnement, et l'intégration SIEM ne sont pas disponibles.

Répondre aux objections

La sécurité d'impression n'est pas notre priorité dans l'immédiat. Nous sommes occupés à d'autres projets.

En raison de l'augmentation de la cybercriminalité et des infractions d'impression, la sécurité devrait être une priorité absolue. Une violation peut entrainer une perte d'activité, de coûteuses amendes de secteurs et une réputation compromise.

Nous avons un pare-feu (ex. Cisco, Juniper, etc.). Tous les périphériques derrière un pare-feu, y compris vos imprimantes réseau, sont protégés.

Déployer des imprimantes derrière un pare-feu est une bonne pratique de sécurité, mais n'élimine pas tous les risques de violation. Près de 65 % des atteintes sont accidentelles, dues à la négligence des employés ou à une défaillance informatique/des processus[11]. Renforcer vos imprimantes à l'intérieur du pare-feu permet de réduire les menaces internes, qu'elles soient accidentelles ou malveillantes.

Les périphériques HP sont-ils sécurisés immédiatement ?

Les nouveaux périphériques HP Enterprise sont équipés de dispositifs de sécurité intégrés comme HP Sure Start, l'émission de listes blanches, et la détection des intrusions pendant le fonctionnement. (Les dispositifs HP LaserJet Enterprise existants peuvent être mis à jour avec les microprogrammes les plus récents, pour permettre l'émission de listes blanches et la détection d'intrusion pendant le fonctionnement.)

Les périphériques HP comportent aussi des paramètres de sécurité qui peuvent être configurés pour répondre à vos exigences particulières. En général, les fournisseurs d'imprimantes livrent leurs dispositifs « ouverts », pour que les clients puissent les utiliser immédiatement dans leur environnement. HP est le seul fabricant d'imprimantes à proposer un logiciel de conformité à la sécurité d'impression basé sur les politiques pour permettre de rationaliser le processus de configuration des paramètres de sécurité sur les imprimantes HP et les imprimantes multifonctions[6].

HP investit en permanence dans des dispositifs, des solutions et des services de sécurité pour aider nos clients à améliorer la sécurité de leur position. Depuis le printemps 2015, HP a désactivé FTP et Telnet par défaut, et a mis en place à l'automne 2016 des exigences de passeport plus fortes pour les imprimantes Enterprise. HP continue à explorer des façons supplémentaires de réduire la surface d'attaque de nos périphériques.

Nous utilisons un produit SIEM (ex. McAfee Nitro, Splunk, LogRhythm, ou ArcSight), pour être ainsi protégés.

Les outils SIEM utilisent des données de journal pour fournir des analyses en temps réel et informer les administrateurs de possibles intrusions, mais ils ne réparent pas les problèmes. La plupart des applications SIEM se concentrent sur les dispositifs informatiques et la sécurité de réseau, et souvent, les imprimantes ne sont pas incluses dans le contrôle du point final. HP a poussé l'industrie à développer des connecteurs pour ArcSight, Splunk et SIEMonster.

Et lorsque vous déployez HP JetAdvantage Security Manager, vous pouvez automatiser le processus de maintien de la conformité des imprimantes de réseau.[6] La solution gère les paramètres de sécurité pour garantir que le périphérique est renforcé aux normes de l'entreprise.

HP Web Jetadmin n'offre-t-il pas les mêmes fonctions que Security Manager ?

HP Web Jetadmin est un robuste outil de gestion de parc qui peut aider à pousser les paramètres vers le parc. Il n'est pas destiné à répondre à la conformité de sécurité comme HP Security Manager.

HP Security Manager est la seule solution de politique d'impression[6] qui automatise le processus de maintien de la conformité des périphériques avec les politiques d'une entreprise, faisant gagner du temps au personnel informatique. La solution bénéficie aussi d'Instant-On qui permet à une imprimante nouvellement déployée de recevoir la politique de sécurité quelques minutes seulement après son ajout au réseau. Il peut en outre gérer les certificats d'identité signés CA dans l'ensemble du parc.

HP JetAdvantage Security Manager est-il compatible avec les périphériques d'autres fabricants ?

Non. Security Manager exige l'accès au microprogramme du périphérique pour pouvoir le gérer, et ne fonctionne actuellement que sur les imprimantes réseau et imprimantes multifonctions HP.

Quelles normes de sécurité sont utilisées par HP JetAdvantage Security Manager ?

La politique de base dans Security Manager repose sur les normes de l'Institut National des Standards et Technologies américaines (NIST).

Placez vos services à part
Incluez les pratiques de sécurité dans tous les aspects de vos services d'impression gérés:

- Formez l'ensemble de votre personnel à la sécurité
- Vendez des offres de sécurité HP à partir des imprimantes avec une protection intégrée contre les logiciels malveillants aux outils de gestion de sécurité – ces offres uniques contribuent grandement à établir des défenses
- Intégrez les meilleures pratiques de sécurité orientées vers l'industrie à vos capacités de gestion des services d'impression

Contactez votre représentant HP pour les dernières informations concernant la formation à la sécurité, les offres de sécurité, les outils de vente de sécurité et l'assistance.

Quel sera le degré de difficulté pour installer et configurer HP Security Manager pour maintenir une sécurité permanente ?

HP Security Manager est une installation rapide et les capacités complètes sont déverrouillées avec un simple ficher de licence. Afin d'ajouter les périphériques, vous pouvez importer un dispositif à partir d'outils comme HP Web Jetadmin ou lancer une découverte automatique sur votre réseau[12].

Une fois les périphériques ajoutés, vous devrez élaborer votre politique de sécurité. Pour faciliter ceci, HP Security Manager fournit une politique de base, établit en fonction des normes de sécurité NIST.

Une fois la ou les politique(s) créée(s), HP Security Manager peut être paramétré pour évaluer automatiquement la conformité de votre périphérique, et le réparer de façon quotidienne, hebdomadaire ou mensuelle.

Si vous utilisez Security Manager pour gérer les certificats d'identification de votre périphérique, cela peut vous faire gagner environ 15 minutes par périphérique sur le temps demandé si vous le faites un par un avec le Serveur Web intégré. Ceci équivaut à un gain de temps significatif si on considère tout un parc de périphériques.

Les raisons de notre supériorité

Il est essentiel pour les entreprises de prendre sérieusement la sécurité d'impression. HP propose des produits et des services leaders de l'industrie qui participent à la protection des périphériques, des données et des documents.

- Les imprimantes les plus sûres au monde – HP est le seul à offrir une gamme complète de fonctionnalités de sécurité permettant de contrôler l'intégrité du périphérique, ainsi qu'un BIOS capable de s'autoréparer[7]
- HP JetAdvantage Security Manager est le seul outil de conformité basé sur la politique du secteur[6]
- HP prend en charge la sécurité au-delà du périphérique – ce qui comprend l'impression à partir de dispositifs mobiles, les données en transit, et l'accès au cloud
- Les données de l'imprimante HP peuvent être intégrées à l'aide d'outils SIEM, tels qu'ArcSight, Splunk, ou SIEMonster
- HP compte plus de 40 ans d'innovation dans le domaine de la sécurité

En savoir plus sur
hp.com/go/printsecurity

[1] Ponemon Institute, « Insecurity of Network-Connected Printers » (« Risques de sécurité encourus par des imprimantes connectées en réseau »), octobre 2015.
[2] Help Net Security, « Why enterprise security priorities don't address the most serious threats » (« Pourquoi les menaces les plus graves ne font pas partie des priorités des entreprises en matière de sécurité »), juillet 2015.
[3] 26,2 % des participants à l'enquête ont subi une sérieuse atteinte à la sécurité, ayant nécessité une réparation, et plus de 26,1 % de ces incidents impliquaient l'impression. IDC, « IT and Print Security Survey 2015 » (« Enquête sur la sécurité informatique et relative à l'impression 2015 ») IDC #US40612015, septembre 2015. IDC, « IT and Print Security Survey 2015 » IDC #US40612015, septembre, 2015.
[4] Ponemon Institute, « 2015 Global Cost of Cyber Crime Study » (« Étude sur le coût moyen de la cybercriminalité internationale »), octobre 2015.
[5] Quocirca, Paysages des services d'impression gérés pour 2014 et 2015.
[6] Affirmation basée sur des études internes réalisées par HP sur les offres des concurrents (comparaison de la sécurité des périphériques, janvier 2015) et le rapport sur la solution HP JetAdvantage Security Manager 2.1 de Buyers Laboratory LLC, février 2015. HP JetAdvantage Security Manager est vendu séparément. Pour en savoir plus, veuillez vous rendre sur hp.com/go/securitymanager.
[7] L'argument « imprimantes les plus sûres » porte sur les appareils HP Enterprise commercialisés à partir de 2015 et s'appuie sur une étude HP de 2016 sur les fonctions de sécurité intégrées publiées des imprimantes concurrentes de même catégorie. HP est le seul à offrir une gamme complète de fonctionnalités de sécurité permettant de contrôler l'intégrité du périphérique, ainsi qu'un BIOS capable de s'autoréparer. Une mise à jour du service FutureSmart peut s'avérer nécessaire pour activer les fonctionnalités de sécurité. Pour obtenir la liste des produits compatibles, consultez hp.com/go/PrintersThatProtect. Pour en savoir plus, consultez hp.com/go/printersecurityclaims.
[8] HP JetAdvantage Secure Print : les travaux d'impression à la demande fonctionnent avec toutes les imprimantes ou MFP connectées au réseau. L'authentification sur le dispositif est disponible sur de nombreux périphériques HP LaserJet, PageWide, et OfficeJet Pro, ainsi que certains périphériques non HP. Certains périphériques peuvent nécessiter une mise à niveau du micrologiciel. Connexion Internet requise pour un stockage dans le cloud et la récupération des travaux d'impression. Le lancement de travaux d'impression depuis un périphérique mobile nécessite une connexion réseau et un code QR. Pour plus d'informations et une liste d'imprimantes et de MFP compatibles, consultez hp.com/go/JetAdvantageSecurePrint. Les partenaires HP n'y ont pas accès dans tous les pays.
[9] HP JetAdvantage Connect travaille avec des dispositifs mobiles de premier plan. Un plug-in unique doit être installé pour les périphériques fonctionnant sur Android™, Google Chrome™, et les systèmes d'exploitation Microsoft. Pour les informations et une liste de systèmes d'exploitation compatibles, consulter hp.com/go/JetAdvantageConnect. Les partenaires HP n' y ont pas accès dans tous les pays.
[10] D'après les spécifications du produit publiées par le fabricant en août 2016.
[11] Ponemon Institute, « 2015 Global Cost of Cyber Crime Study » (« Étude sur le coût moyen des violations de données »), octobre 2015.
[12] Vous pouvez télécharger gratuitement HP Web Jetadmin sur hp.com/go/webjetadmin.

4AA6-8888FRE, décembre 2016