



Sécurité des imprimantes HP DesignJet

La sécurité des équipements fait face à des menaces qui ne cessent d'évoluer. Tout équipement connecté au réseau d'une entreprise est un point de vulnérabilité, y compris les imprimantes.



64 %

des responsables informatique estiment que leurs imprimantes sont sans doute infectées par un logiciel malveillant¹



73 %

des RSSI s'attendent à subir une atteinte à la sécurité majeure dans les 12 prochains mois²



26 %

des atteintes aux données signalées par les responsables informatiques ont impliqué leurs imprimantes³

Clients ciblés

Quelle que soit leur taille, leur implantation géographique ou leur secteur d'activité, les entreprises souhaitent sécuriser leurs environnements partagés d'impression et d'imagerie.

Cibles à contacter

- Directeur ou responsable de la sécurité informatique
- DSI
- Responsables de la sécurité ou de la conformité
- Gestionnaires et décideurs informatiques

Profil du client idéal

- Souhaite renforcer la sécurité de l'environnement informatique pour faire face aux menaces ou/et pour respecter les exigences réglementaires de conformité
- Ne peut pas prendre le risque d'ouvrir son réseau à des attaques
- Risque des amendes coûteuses pour non conformité du traitement des données clients
- Manipule des données hautement confidentielles dans le cadre de ses opérations quotidiennes

Situation actuelle du marché

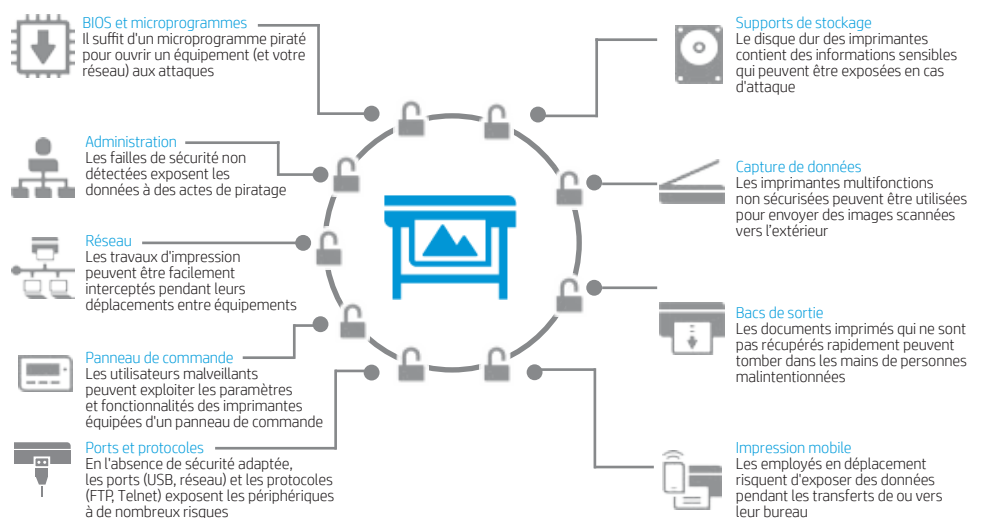
En raison de la sophistication croissante et de l'acharnement des cybercriminels, les pare-feu de réseau sont désormais des mesures de sécurité insuffisantes. Les entreprises doivent donc envisager de protéger les matériels situés derrière le pare-feu, y compris les imprimantes connectées au réseau.

Qu'il s'agisse d'une cyber-attaque malveillante, d'un incident interne ou du non-respect d'une loi ou d'une norme, les atteintes à la sécurité peuvent coûter très cher aux entreprises. Le coût annuel moyen de ces événements est d'environ 4 millions de \$US⁴ dû à des amendes, perte d'activité, réputation ternie, plaintes en nom collectif, etc.

De leur côté, les exigences réglementaires et de conformité deviennent toujours plus complexes. Les entreprises doivent donc se tourner vers des équipements et des solutions qui les protègent et qui les aident à respecter la conformité applicable à leurs activités.

Problèmes de sécurité de ces clients

Bien que de nombreux départements informatiques appliquent rigoureusement des mesures de sécurité efficaces aux postes de travail et au réseau de l'entreprise, les équipements d'impression et d'imagerie sont plus souvent négligés et de ce fait plus vulnérables.



Besoins de sécurité des clients

Vos clients ont besoin de solutions simples pour protéger leurs équipements, leurs données et leurs documents. Par ailleurs, ils souhaitent réduire la charge de travail de leur personnel informatique en disposant de solutions efficaces pour l'administration de la sécurité d'impression et la génération de rapports de conformité.

Sécurité des équipements

- Protection du BIOS et du microprogramme contre les attaques et les logiciels malveillants
- Protection des mises à niveau du microprogramme
- Sécurisation des paramètres et des mots de passe des équipements

Sécurité des données

- Cryptage des données en transit vers ou de l'imprimante et des données au stockées dans l'imprimante
- Support des certificats numériques signés par une autorité de certification/CA (avec clés publiques/PKI)
- Sécurisation des opérations d'effacement et de destruction des disques durs
- Authentification et contrôle des accès des utilisateurs
- Sécurisation des fonctionnalités d'impression mobile

Sécurité des documents

- Solutions d'impression sécurisées par code PIN

Supervision et conformité de la sécurité du parc d'équipements

- Contrôle de la sécurité du parc à l'aide de nombreuses fonctions de configuration et de supervision
- Rapports avancés qui permettent de démontrer la conformité du parc

Proposition de valeur pour les clients

- Réduction des risques des cyber-attaques coûteuses
- Protection des données et documents sensibles
- Gain de temps par administration automatisée de la sécurité du parc d'équipements
- Conformité avec les réglementations et accès facile aux données nécessaires aux rapports de conformité

Proposition de valeur pour les partenaires

- Une opportunité de croissance, car les clients investissent activement dans la sécurité de leurs impressions
- Une conversation axée sur la valeur, qui vous permet de faire remonter vos propositions dans la hiérarchie de l'entreprise : l'importance de la sécurité permet de déplacer la conversation du prix à la valeur ajoutée

Questions de qualification

Posez les questions suivantes à vos clients ou prospects :

- Avez-vous déjà mis en place une stratégie de sécurité pour vos équipements d'impression et de numérisation ?
- Êtes-vous amené à gérer des informations sensibles, par exemple l'identité de vos employés ou les données de vos clients ?
- Avez-vous déjà mis en place une solution de cryptage pour vos travaux d'impression ?
- Vos imprimantes sont-elles protégées contre les logiciels malveillants et les virus ?
- Avec quelle fréquence appliquez-vous les mises à jour du microprogramme de vos imprimantes ?

- Avez-vous pour pratique d'associer des mots de passe administrateur à vos imprimantes, ou est-il possible à n'importe quel individu d'accéder aux équipements et de modifier leurs paramètres ?
- Combien de temps votre personnel informatique passe-t-il à configurer vos imprimantes ?

Solutions de sécurité HP pour imprimantes HP DesignJet

Les fonctionnalités de sécurité intégrées aux imprimantes HP DesignJet peuvent aider les entreprises à protéger leurs équipements, leurs données et leurs documents. De plus, elles aident vos clients à gérer la sécurité et la conformité de leur parc d'équipements.

Imprimantes sécurisées

- **Packages de microprogrammes signés par HP** – Les packages de microprogrammes sont signés numériquement par HP Code Signing Group. Les nouvelles installations de microprogramme sont vérifiées systématiquement.
- **Amorçage sécurisé via UEFI (UEFI Secure Boot)** – Valide l'intégrité du système d'exploitation au démarrage.
- **Cryptage du disque dur** – HP utilise le standard AES avec clés de 256 bits pour le cryptage et le cryptage des données stockées sur disque dur.
- **Effacement sécurisé des fichiers et des disques durs** – Procédures visant à garantir que les données présentes dans les systèmes de stockage sont supprimées définitivement et ne permettent plus aucune récupération.
- **Verrouillage de l'accès au panneau de commande** – Verrouille le panneau de commande de l'imprimante pour empêcher les utilisateurs non autorisés de modifier les paramètres de celle-ci.

Logiciels sécurisés




En complément de la sécurité des équipements, HP propose des solutions pour détecter, protéger, superviser et administrer un parc d'équipements et sécuriser les données et les documents à long terme.

- **HP JetAdvantage Security Manager** – Avec cette solution, le seul outil du marché capable de garantir la conformité de la sécurité d'impression par application de politiques internes, vos clients peuvent automatiser l'administration de la sécurité de leur parc d'équipements.⁶
 - Permet la création et le déploiement de politiques de sécurité permettant de protéger efficacement un parc d'équipements.
 - Des rapports analysent les risques, déterminent très rapidement le statut des différents équipements et démontrent leur conformité.
 - Opérations automatisées d'application et de mise à jour des certificats uniques des équipements, signés par une autorité de certification.
- **HP Web Jetadmin** – Solution de gestion des impressions la plus efficace du marché et lauréate de nombreuses distinctions, pour améliorer la productivité et réduire les coûts d'exploitation. Très facile à utiliser, HP Web Jetadmin inclut une interface Web très efficace pour installer, configurer, dépanner et administrer les équipements d'impression HP et non HP connectés au réseau ou aux postes de travail des employés.⁷

Services sécurisés

- **Services HP de recyclage personnalisé** – Ces services garantissent la suppression des données présentes sur les disques durs, puis recyclent de manière responsable les produits en fin de vie. Pour plus de détails : hp.com/go/businessrecycling.

Sécurité des modèles HP DesignJet – Comparaison avec la concurrence

		HP DesignJet (1)	Canon (2)	Epson (3)	Ricoh (4)
ÉQUIPEMENT 	Fonctions de sécurité pour l'administration du réseau par SNMP v3	✓	✓	⊘	✓
	Effacement sécurisé des fichiers (Secure File Erase)	✓	⊘ (6)	⊘	✓
	Effacement sécurisé des disques (Secure Disk Erase)	✓	✓ (5)	✓	✓
DONNÉES 	Compatibilité 802.1x	✓	⊘ (6)	✓	✓
	Cryptage des disques durs	✓	⊘	✓	✓
	Protocole de sécurité réseau IPsec	✓	⊘ (6)	✓	✓
DOCUMENT 	Impressions sécurisées par code PIN	✓	⊘	⊘	✓

- (1) Modèles comparés : HP DesignJet T930, T1530, T2530 MFP, T3500 MFP
- (2) Modèles comparés : Canon iPF785, iPF770, iPF850, iPF770L36, scanner M40
- (3) Modèles comparés : SC-T5200/D, SC-T5200F MFP
- (4) Modèles comparés : Ricoh MP CW2201SP
- (5) Modèles équipés d'un disque dur
- (6) Scanner M40 : Oui

HP et la sécurité des équipements

Les entreprises doivent impérativement prendre au sérieux la sécurité de leurs impressions. HP propose des produits et des solutions efficaces qui peuvent les aider à protéger les équipements, les données et les documents.

¹ « Insecurity of Network Connected Printers » (Ponemon Institute, octobre 2015)

² « Why enterprise security priorities don't address the most serious threats » (Help Net Security, juillet 2015)

³ 26,2 % des répondants à cette enquête ont subi une atteinte sérieuse à leur sécurité informatique qui a exigé des mesures de correction (plus de 26,1 % de ces incidents impliquaient l'impression). « IT and Print Security Survey 2015 » (IDC n° US40612015, septembre 2015)

⁴ « Cost of Data Breach Study Global Analysis » (Ponemon Institute, 2016)

⁵ « Managed Print Services Landscapes for 2014 and 2015 » (Quocirca)

⁶ Sur la base de recherches internes HP portant sur les offres des concurrents (Device Security Comparison, janvier 2015) et du rapport Solutions Report on HP JetAdvantage Security Manager 2.1 établi par Buyers Laboratory LLC en février 2015. HP JetAdvantage Security Manager est vendu séparément. Pour plus de détails : hp.com/go/securitymanager.

⁷ HP Web Jetadmin est une solution gratuite qui peut être téléchargée à partir de la page suivante : hp.com/go/wja

Partagez ce document avec des collègues

© Copyright 2017 HP Development Company, L.P. Les informations présentées dans ce document peuvent être modifiées à tout moment et sans préavis. Les seules garanties applicables aux produits et aux services HP sont présentées dans les déclarations de garantie explicites qui accompagnent ces produits ou ces services. Aucune information du présent document ne saurait être considérée comme constituant une garantie complémentaire. HP décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document.

Les noms « Android » et « Google Chrome » sont des marques déposées reconnues comme appartenant à la société Google Inc. Le nom « Microsoft » est une marque déposée aux États-Unis et reconnue comme appartenant au groupe Microsoft.

Confidentiel HP 2017 Le présent document contient des informations confidentielles ou relevant du secret professionnel. Il est strictement réservé à l'usage interne de HP et de ses partenaires de distribution.

Si ce document ne vous est pas destiné (si votre nom ne figure pas dans la liste de destinataires présente sur sa couverture), il vous est strictement interdit de le consulter, de le transmettre, de le distribuer ou, de quelque manière que ce soit, d'utiliser ou de faire référence à la lettre ou l'esprit de son contenu.

