

Considérations concernant la sécurité de l'imprimante



Aspects importants de la sécurité à prendre en considération lors de l'évaluation des solutions d'impression

Table des matières

Les dispositifs d'impression et d'imagerie non sécurisés représentent l'immobilisme	2
Cinq domaines clés de la sécurité de l'impression	2
Processus de démarrage sécurisé	2
Intégrité du code du micrologiciel	2
Détection des intrusions en cours de fonctionnement	3
Garantie permanente des paramètres de politique sécuritaire	3
Analyse et détection des menaces en temps réel	3
Dispositifs FutureSmart compatibles et disponibilité de la fonctionnalité	4

Les dispositifs d'impression et d'imagerie non sécurisés représentent l'immobilisme

Les responsables informatiques se voient constamment confier la tâche de protéger des informations confidentielles, y compris l'identité des employés et les données des clients, sur plusieurs dispositifs. Face à la nécessité de répondre aux besoins de nombreuses personnes ayant différents modes de travail dans l'ensemble de l'organisation, les menaces sécuritaires non anticipées constituent un défi permanent.

De nombreux départements informatiques appliquent avec rigueur des mesures de sécurité aux ordinateurs individuels et au réseau de l'entreprise, cependant les dispositifs d'imagerie et d'impression sont souvent négligés et restent exposés. Les menaces de sécurité sont pourtant attestées, et les dispositifs d'imagerie et d'impression devenant de plus en plus sophistiqués, ils offrent aux attaquants davantage de possibilités de compromettre le dispositif, sinon la totalité du réseau.

Cinq domaines clés de la sécurité de l'impression

Ce document a pour objectif de vous fournir, non seulement un cadre, mais aussi des aspects très spécifiques concernant la sécurité de l'impression que vous devez prendre en considération lors de l'achat, du déploiement ou de l'utilisation d'imprimantes et de solutions d'impression. Les imprimantes HP qui supportent les 3 grandes fonctions de sécurité (HP Sure Start, Liste blanche, et la détection des intrusions en cours de fonctionnement) lancées à l'automne 2015 correspondront aux critères de chacune des sections (lorsqu'elles sont associées au gestionnaire de sécurité JetAdvantage et ArcSight)¹. Les dispositifs FutureSmart qui ne sont pas compatibles avec HP Sure Start répondront à la totalité des critères, sauf ceux listés en section #1 (Processus de démarrage sécurisé). Voir le tableau des dispositifs ci-dessous pour les informations relatives à la compatibilité des dispositifs de sécurité.

Vous devez vous concentrer sur cinq secteurs clés de la sécurité de l'imprimante :

1. Sécurisation du processus de démarrage
2. Intégrité du code du micrologiciel
3. Détection des intrusions en cours de fonctionnement
4. Garantie permanente des paramètres de politique sécuritaire
5. Détection et analyse des menaces en temps réel

Sécurisation du processus de démarrage

Les éléments suivants sont des aspects du processus de démarrage sécurisé que HP recommande pour une sécurité maximale :

- Au démarrage, le dispositif doit valider l'intégrité du BIOS.
- Le dispositif doit « auto-réparer » un BIOS infecté en le remplaçant par une golden copy matérielle protégée du BIOS.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'événements standard, y compris les systèmes SIEM.
- Le dispositif doit revenir à un état fonctionnel connu après la détection d'un BIOS infecté et son remplacement par une golden copy.

Intégrité du code du micrologiciel

Les éléments suivants sont des aspects de l'intégrité du code du micrologiciel qui devraient être intégrés à la demande de proposition.

- Le dispositif doit valider l'intégrité du code du micrologiciel pendant le temps de chargement et permettra uniquement au micrologiciel correct de s'exécuter.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'événements standard, y compris les systèmes SIEM.

Détection des intrusions en cours de fonctionnement

Les éléments suivants sont des aspects de la détection des intrusions en temps réel que HP recommande pour une sécurité maximale :

- Le dispositif doit fournir un contrôle permanent pour les attaques par injection de logiciels malveillants en mémoire.
- Le dispositif doit informer l'administrateur de tous les problèmes via les mécanismes d'événements standard, y compris les systèmes SIEM.
- Le dispositif doit interrompre le fonctionnement normal lorsqu'une anomalie est détectée et redémarrer à un état correct antérieur.
- L'algorithme de détection des intrusions doit être inséré au hasard en différents endroits dans l'image de code pour prévenir sa propre détection.

L'algorithme de détection des intrusions doit s'exécuter suffisamment fréquemment pour détecter l'injection de logiciels malveillants avant qu'un logiciel malveillant ne puisse compromettre l'intégrité du dispositif.

Garantie permanente des paramètres de politique sécuritaire

La garantie permanente des paramètres de politique sécuritaire est assurée en grande partie par l'utilisation d'un outil de mise en conformité de la sécurité. Les éléments suivants sont des aspects de l'outil de mise en conformité de la sécurité que HP recommande pour une sécurité maximale :

- L'outil de mise en conformité de la sécurité doit mettre en conformité les imprimantes/multifonctions qui ne le sont pas, en se basant sur la politique de sécurité.
- L'outil de mise en conformité de la sécurité doit faire en sorte que les dispositifs nouveaux ou réinitialisés sur le réseau s'annoncent et soient immédiatement mis en conformité.
- L'outil de mise en conformité de la sécurité doit inclure un éditeur intuitif de la politique de sécurité qui guide l'administrateur lors de la sélection des paramètres appropriés en signalant les dépendances conflictuelles.
- L'outil de mise en conformité de la sécurité doit gérer et installer des certificats avec un processus automatisé via un parc d'imprimantes/multifonctions.

Détection et analyse des menaces en temps réel

La détection et l'analyse des menaces en temps réel sont en grande partie effectuées par l'intermédiaire du système d'information de sécurité et gestion des événements (SIEM). Les éléments suivants sont des aspects du système SIEM que HP recommande pour une sécurité maximale :

- Le SIEM doit récupérer les événements critiques de sécurité des imprimantes.
- Le SIEM doit autoriser les analyses de sécurité à personnaliser les rapports et les alertes à partir de messages indiquant les alertes en temps réel.
- Le SIEM doit s'intégrer à d'autres actifs informatiques (serveurs, routeurs, etc.) qui sont contrôlés pour la détection des menaces en temps réels.
- Le SIEM doit transformer Big Data en renseignements de sécurité permettant d'engager une action sur la base d'une corrélation en temps réel associée à une puissante analyse de la sécurité.
- Le SIEM doit repérer le comportement anormal des utilisateurs et prévenir les menaces envers les données sensibles.

Dispositifs FutureSmart compatibles et disponibilité de la fonctionnalité

La grille suivante montre comment les nouvelles fonctionnalités de sécurité intégrées seront supportées dans l'ensemble du parc HP Enterprise FutureSmart à partir de la fin de l'automne 2015. La totalité des dispositifs FutureSmart lancés après l'automne 2015 sera compatible avec les 3 nouvelles fonctions de sécurité intégrées prises en compte. (HP Sure Start, Liste blanche et Détection des intrusions). En raison des limitations matérielles du dispositif, certaines fonctionnalités ne seront pas supportées sur certaines plates-formes plus anciennes.

Catégorie de Demande de proposition		Sécurisation du processus de démarrage	Intégrité du code du micrologiciel	Détection des intrusions en cours de fonctionnement	Assurance permanente des paramètres de politique sécuritaire	Analyse et détection des menaces en temps réel
Plate-forme du dispositif (inclut tous les packages et les options gérées)	Nouvelle disponibilité de la fonctionnalité de sécurité intégrée	HP Sure Start	Liste blanche	Détection des intrusions en cours de fonctionnement	HP JetAdvantage Security Manager	Intégration de HP ArcSight
HP LaserJet Enterprise MFP M527	Automne 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M577	Automne 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M506	Automne 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M552 et M553	Automne 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M604, M605 et M606	Automne 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise 700 color MFP M775	Printemps 16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 color MFP M575	Printemps 16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 MFP M525	Printemps 16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise MFP M725	Printemps 16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise flow MFP M830	Printemps 16	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M806	Printemps 16	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M855	Printemps 16	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise flow MFP M880	Printemps 16	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color MFP X585	Printemps 16	⊘	✓	✓	✓	✓

Catégorie de Demande de proposition		Sécurisation du processus de démarrage	Intégrité du code du micrologiciel	Détection des intrusions en cours de fonctionnement	Assurance permanente des paramètres de politique sécuritaire	Analyse et détection des menaces en temps réel
Plate-forme du dispositif (inclut tous les packages et les options gérées)	Nouvelle disponibilité de la fonctionnalité de sécurité intégrée	HP Sure Start	Liste blanche	Détection des intrusions en cours de fonctionnement	HP JetAdvantage Security Manager	Intégration de HP ArcSight
HP OfficeJet Enterprise Color X555	Printemps 16	⓪	✓	✓	✓	✓
HP Color LaserJet Enterprise M651	Printemps 16	⓪	✓	✓	✓	✓
HP Color LaserJet Enterprise MFP M680	Printemps 16	⓪	✓	✓	✓	✓
HP LaserJet Enterprise MFP M630	Printemps 16	⓪	✓	✓	✓	✓
HP LaserJet Enterprise 700 M712	Printemps 16	⓪	✓	✓	✓	✓
HP Color LaserJet Enterprise M750	Printemps 16	⓪	✓	✓	✓	✓
HP LaserJet Enterprise 600 M601, M602 et M603	Printemps 16	⓪	✓	✓	✓	✓
HP LaserJet Enterprise couleur M551	Printemps 16	⓪	✓	✓	✓	✓
Multifonction HP LaserJet Enterprise M4555	Non pris en charge	⓪	⓪	⓪	✓	✓
HP Color LaserJet CM4540 MFP	Non pris en charge	⓪	⓪	⓪	✓	✓
HP LaserJet Enterprise CP5525	Non pris en charge	⓪	⓪	⓪	✓	✓
HP Digital Sender Flow 8500 fn1	Non pris en charge	⓪	⓪	⓪	✓	✓
HP ScanJet Enterprise 7000n	Non pris en charge	⓪	⓪	⓪	✓	⓪

¹ Une mise à jour du pack de services FutureSmart peut s'avérer nécessaire pour activer les fonctionnalités de sécurité.

Abonnez-vous sur hp.com/go/getupdated



Partagez avec des collègues

© Copyright 2015 HP Development Company, L.P. Les informations figurant dans ce document sont susceptibles d'être modifiées sans préavis. Les seules garanties pour les produits et services HP sont celles stipulées dans les déclarations formelles de garantie accompagnant ces produits et services. Les informations contenues dans ce document ne constituent en aucun cas une garantie supplémentaire. HP décline toute responsabilité en cas d'erreurs ou d'omissions techniques ou rédactionnelles constatées dans ce document.

