



Protégez votre réseau avec la solution d'impression la plus sécurisée au monde¹

94 %

des entreprises financières déclarent que la sécurité du photocopieur ou de l'imprimante est importante ou très importante²



61 %

des organisations ont déjà signalé au moins une fuite de données sur une imprimante l'année passée³



43 %

des entreprises ne connaissent pas la stratégie de protection des points de terminaison de leurs imprimantes⁴





Seulement 18 % des entreprises contrôlent leurs imprimantes pour éviter les menaces.⁴ Et vous ?

Reconnaissez les risques cachés

L'équipe informatique se charge continuellement de protéger les informations confidentielles, y compris les identités des employés et les données des clients, parmi les nombreux périphériques et environnements. Bien que de nombreux départements informatiques appliquent rigoureusement des mesures de sécurité aux ordinateurs individuels et au réseau, les périphériques d'imagerie et d'impression sont souvent négligés et vulnérables. Lorsque des périphériques ne sont pas protégés, c'est l'intégralité du réseau qui est exposée aux attaques des pirates.

« Témoin de son investissement à long terme en matière de sécurité des imprimantes, HP détient la gamme la plus large et la plus étendue de solutions et de services de sécurité sur le marché ».

– Quocirca, janvier 2017⁵

Comprendre les coûts potentiels

Même une brèche de sécurité peut être coûteuse. Si des informations privées sont menacées à cause d'un environnement d'impression et de numérisation non-sécurisé, cela peut entraîner une usurpation d'identité, un vol d'informations confidentielles, une image de marque et une réputation ternies, ainsi que des poursuites judiciaires. En outre, une non-conformité juridique peut entraîner de lourdes amendes.

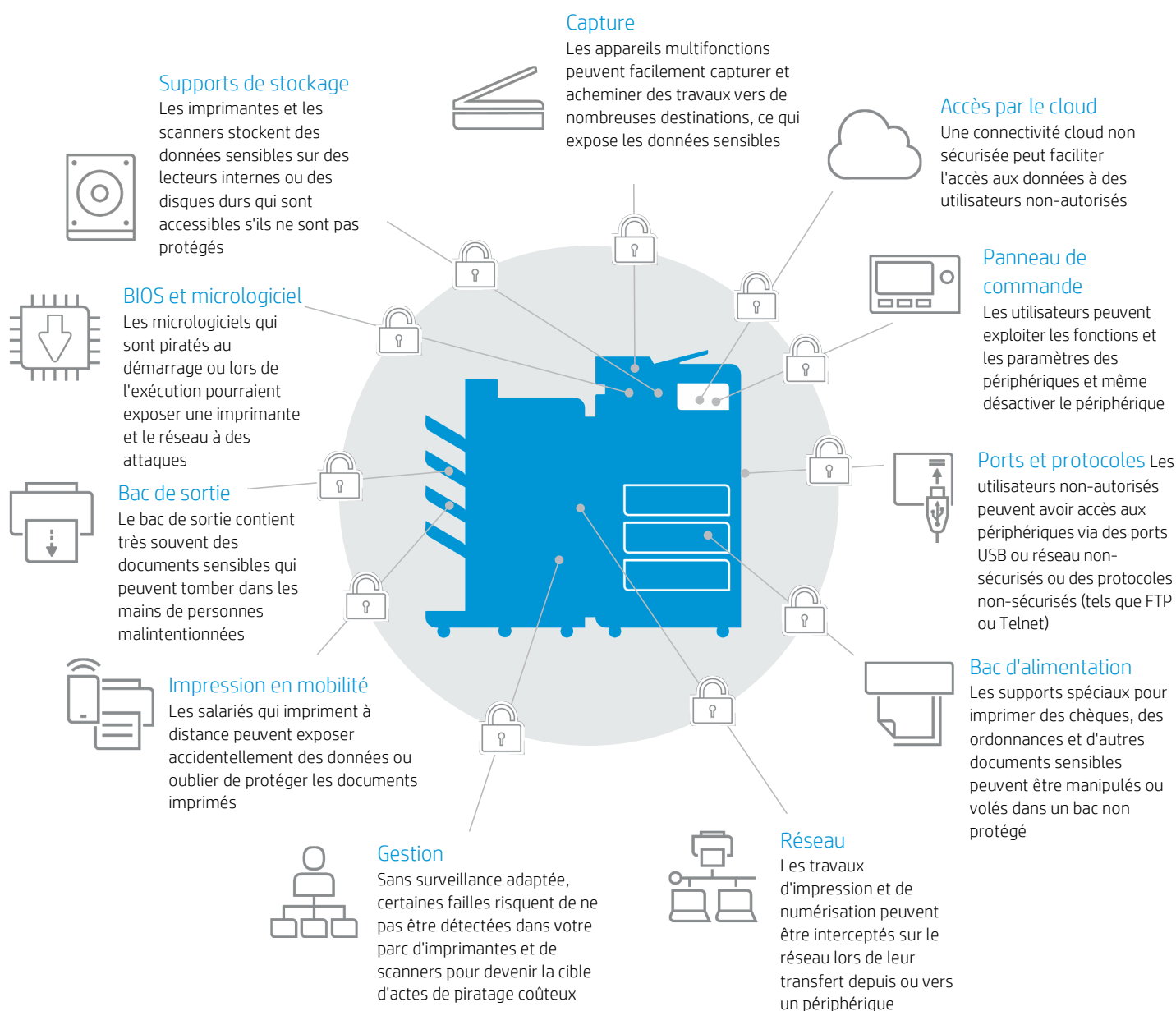
HP peut vous aider

Protégez votre réseau avec la solution d'impression la plus sécurisée au monde.¹ Les imprimantes HP sont toujours sur leurs gardes, et détectent continuellement les menaces pour les bloquer, tout en s'adaptant aux nouvelles. HP peut vous aider à automatiser la protection de vos appareils, données et documents grâce à un large éventail de solutions. Nos experts en sécurité peuvent vous aider à développer et à déployer une stratégie de sécurité d'impression et d'imagerie de bout en bout.

Protégez vos périphériques, vos données et vos documents,

Vous pouvez avoir de graves lacunes dans votre environnement de numérisation et d'impression, et cela dans de multiples endroits. Mais, à partir du moment où vous identifiez ces différentes vulnérabilités, vous pouvez facilement réduire les risques.

Points faibles des imprimantes et des scanners





Protéger le périphérique



En savoir plus

HP Custom Recycling Services
hp.com/go/businessrecycling

Services HP Secure MPS
hp.com/go/securemps

Les imprimantes HP sont conçues pour fonctionner avec les solutions de surveillance de la sécurité et de gestion afin de réduire le risque, d'améliorer la conformité et de protéger votre réseau de bout en bout. (Les fonctionnalités et solutions ne sont pas toutes disponibles sur tous les appareils HP.⁶⁾)

Pratiques de sécurité de base

Stockage crypté avec effacement sécurisé

Toute information sensible stockée sur un lecteur interne ou un disque dur est potentiellement exposée au vol. De nombreux appareils HP disposent d'un cryptage intégré pour protéger les données. Lorsque les données stockées ne sont plus nécessaires, utilisez des fonctionnalités intégrées à l'appareil pour écraser les données et supprimer les informations sensibles en toute sécurité.

Élimination sécurisée

Les *services de recyclage personnalisés HP* garantissent la suppression des données des disques durs avant de recycler de manière responsable les anciens produits.

Accès sécurisé à la réparation des imprimantes

La connaissance des pratiques de sécurité des mainteneurs d'imprimantes vous aidera à protéger vos données sensibles. Choisissez les *services HP Secure MPS* ou des partenaires HP pour obtenir une assistance qualifiée.

Désactivation des ports et protocoles inutilisés

Réduisez la vulnérabilité de vos appareils grâce à une configuration appropriée. Désactivez les ports physiques et les protocoles non utilisés (comme FTP ou Telnet) pour prévenir tout accès ou usage non autorisé.

Contrôle de l'accès à l'appareil par l'administrateur

Définissez des mots de passe d'administrateur afin que seuls les personnels informatiques ou autres personnels autorisés puissent configurer les appareils.

Liste blanche du microcode

Consultez la page suivante pour découvrir comment la liste blanche peut protéger votre parc contre les logiciels malveillants.

Pratiques de sécurité avancées

Certification de critères communs

Les imprimantes de bureau HP sont certifiées conformes aux normes de sécurité reconnues au niveau international, telles que les Critères communs (CCC) et FIPS 140. Assurez-vous que les mises à jour du micrologiciel de l'appareil sont signées par un code afin de confirmer l'intégrité et l'authenticité de celui-ci et garantir la conformité.



En savoir plus

Fonctions de sécurité d'impression intégrées

- HP Sure Start (intégrité du BIOS)
- Liste blanche du microcode
- Détection des intrusions à l'exécution
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager :

hp.com/go/securitymanager

Les fonctions de sécurité d'impression détectent et arrêtent automatiquement les attaques. Les imprimantes professionnelles HP intègrent des fonctionnalités de sécurité qui les protègent afin qu'elles ne deviennent pas un point d'entrée en cas d'attaque de votre réseau. Seule la sécurité de l'impression HP offre une détection en temps réel, une surveillance automatisée et une validation logicielle intégrée pour arrêter les menaces dès qu'elles se présentent.⁷

Les imprimantes professionnelles HP, de la gamme Pro⁸ à la gamme Enterprise,⁷ sont toujours sur leurs gardes, elles détectent et bloquent les menaces pendant toutes les phases de leur fonctionnement :

- **Au démarrage.** Le code de démarrage (pour les modèles HP Pro) ou le BIOS (pour les modèles HP Enterprise) se présente sous la forme d'un jeu d'instructions exécutées pour charger les modules matériels critiques et activer le microprogramme. L'intégrité du code est validée à chaque cycle de démarrage, permettant ainsi de protéger votre périphérique des attaques.
- **Lors du chargement du micrologiciel.** La *liste blanche* vérifie automatiquement le microprogramme au démarrage pour déterminer si le code est authentique et correct—signé numériquement par HP. Si une anomalie est détectée, le périphérique se réinitialise en un état sécurisé hors-ligne et avertit le service informatique.
- **Lors de l'exécution.** Les fonctionnalités HP intégrées protègent la mémoire des appareils pendant leur fonctionnement et leur connexion au réseau, soit lorsque la plupart des attaques se produisent. En cas d'attaque, l'appareil s'éteint.

Les appareils HP Enterprise peuvent se rétablir automatiquement

En plus de pouvoir détecter et bloquer les menaces, les imprimantes HP Enterprise s'autorétablissent après les attaques, afin que les personnels informatiques n'aient pas à intervenir.⁷ Ces fonctionnalités déclenchent automatiquement un redémarrage en cas d'attaque ou d'anomalie. Les administrateurs peuvent être avertis des incidents ou des attaques par des outils de gestion de la sécurité (SIEM) tels qu'ArcSight, Splunk et SIEMonster.

- *HP Sure Start* est le seul BIOS auto-réparant du secteur.⁷ Si le BIOS est compromis, HP Sure Start redémarre avec une copie garantie authentique de son BIOS.
- La *détection des intrusions à l'exécution* surveille les opérations complexes du microprogramme et de la mémoire, arrête automatiquement l'intrusion et redémarre en cas d'attaque.
- *HP Connection Inspector* évalue les connexions sortantes du réseau pour déterminer ce qui est normal, arrêter les demandes suspectes, repousser les logiciels malveillants en déclenchant automatiquement un redémarrage.

En plus de la pérennisation de l'investissement assurée par le microcode évolutif HP FutureSmart, vous pouvez ajouter la liste blanche, la détection des intrusions à l'exécution, et HP Connection Inspector à de nombreuses imprimantes HP Enterprise existantes.⁷

HP JetAdvantage Security Manager exécute les dernières étapes du cycle de vérification

Après redémarrage, ou dès l'ajout d'un nouvel appareil au réseau, *HP JetAdvantage Security Manager* effectue une évaluation automatiquement et, si nécessaire, fait en sorte que les paramètres de sécurité de l'équipement soient en conformité avec les stratégies de configuration préétablies.⁹ Aucune intervention n'est requise des services informatiques.

Comment cela fonctionne ?

Les fonctionnalités de sécurité intégrées s'appliquent aux quatre étapes principales du cycle de démarrage des équipements HP.

En cas d'attaque, l'équipement HP Enterprise redémarre et se corrige automatiquement.

HP JetAdvantage Security Manager exécute les dernières étapes du cycle de vérification.

Quatre. Surveillance continue

Protège les opérations et arrête les attaques au cours du fonctionnement de l'appareil.

Inspecte les connexions réseau sortantes pour bloquer les demandes suspectes (Enterprise

Trois. Vérification des paramètres

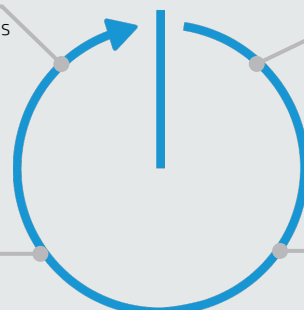
Après un redémarrage, HP JetAdvantage Security Manager vérifie les paramètres de sécurité du périphérique affecté et les corrige.

Un. Vérification du code BIOS/de démarrage

Empêche l'exécution des codes malveillants au démarrage en garantissant que seul le code conçu par HP et signé numériquement est chargé.

Deux. Vérification du microprogramme

Autorise uniquement le chargement d'un code authentique et validé, signé numériquement par HP.





Protéger les données



En savoir plus

HP Web Jetadmin
hp.com/go/wja

Pilote HP Universal Print intégrant l'impression
chiffree sécurisée
hp.com/go/upd

Solutions de flux de production HP JetAdvantage
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Qu'elles soient stockées ou en transit, vos données requièrent une protection constante. Voici quelques étapes essentielles pour vous aider à transférer et utiliser vos données en toute sécurité.⁶

Pratiques de sécurité de base

Normes réseau 802.1X ou IPsec

Utilisez les normes réseau pour protéger les données qui circulent sur le réseau entre l'appareil et des outils de gestion comme *HP Web Jetadmin* ou le *serveur Web intégré HP*.

Cryptage des données transmises

Protégez vos tâches d'impression acheminées vers l'appareil avec un cryptage tel que Internet Print Protocol over TLS (IPPS). Ou, le pilote d'impression universel HP (UPD) propose un cryptage et un décryptage à symétrie parfaite AES256 des travaux d'impression du client jusqu'à la page à l'aide d'un mot de passe défini par l'utilisateur qui utilise les bibliothèques cryptographiques validées FIPS 140 de Microsoft®.

Lors de l'analyse, les *solutions de flux de travail HP JetAdvantage* peuvent protéger les informations sensibles tout en améliorant l'efficacité. Par exemple, HP Capture and Route s'intègre sans problème avec HP Access Control pour plus de sécurité, avec l'avantage d'une authentification unique et la possibilité de gérer du contenu pour la gouvernance des informations.¹⁰

Cryptage des données au repos

Protégez les informations d'entreprise sensibles qui sont stockées sur le disque dur avec un cryptage intégré. Pour renforcer le niveau de sécurité, le module de plateforme sécurisée (TPM) peut être ajouté en option au périphérique pour renforcer la protection des données et des informations d'authentification chiffrées en intégrant automatiquement les clés de chiffrement au TPM. Il fournit une identité du périphérique sécurisé en générant et en protégeant les clés privées de certificat.

Protection via pare-feu

Empêchez les logiciels malveillants et les virus d'accéder à votre réseau en limitant l'accès des imprimantes aux ordinateurs de votre réseau.

Authentification utilisateur native

Réduisez les coûts et les risques en obligeant les utilisateurs à s'authentifier par PIN/PIC, LDAP ou Kerberos. Vous pouvez également intégrer ces outils à Active Directory.

Contrôles d'accès basés sur les rôles

HP Access Control Rights Management vous aide à réduire les coûts et les risques à travers une restriction des fonctionnalités au niveau de l'imprimante. Les contrôles d'accès fondés sur les rôles vous permettent d'attribuer des fonctions à différents types d'utilisateurs ou de services, en fonction de leurs besoins. Vous pouvez ainsi limiter les personnes autorisées à envoyer des télécopies, des numérisations vers une adresse e-mail ou des numérisations par télécopie.

Pratiques de sécurité avancées

Authentification et suivi avancés

Déployez une authentification avancée (avec mots de passe, cartes de proximité, cartes à puce ou biométrie, par exemple) et des solutions de suivi pour une sécurité et un contrôle supplémentaires.



En savoir plus

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

- *HP Access Control Secure Authentication* rétablit le contrôle, renforce la sécurité et réduit les coûts. Bénéficiez d'un ensemble d'options et de contrôles, y compris l'authentification tactile avec les appareils mobiles activés NFC.
- La fonction de *Comptabilisation des travaux de HP Access Control* permet d'assurer avec précision le suivi et la collecte des données, l'analyse des résultats et la création et l'envoi de rapports. Appliquez des données analysées en profondeur pour répartir les coûts d'impression, inciter les salariés à imprimer plus consciencieusement et fournir les informations nécessaires au service informatique pour améliorer les prévisions pour à l'échelle du parc.

Appareils mobiles inclus à l'accès réseau

Utilisez vos appareils mobiles dans le cadre de votre stratégie globale de sécurité de l'impression pour le contrôle de l'accès aux imprimantes HP propose des solutions basées sur un serveur qui permettent l'impression à partir du panneau commande sécurisée en plus de possibilités avancées de production de rapports et de gestion.

- *HP JetAdvantage Connect* garantit une impression mobile fiable et intuitive conçue pour votre activité. Gagnez du temps et de l'argent en tirant parti de façon ininterrompue des outils et stratégies de vos réseaux informatiques pour gérer l'impression mobile.¹¹ Les utilisateurs peuvent imprimer en toute sécurité à partir de différents smartphones et tablettes—où et quand ils en ont besoin—aussi facilement qu'à partir d'un ordinateur.
- *HP Access Control* offre des possibilités de gestion des impressions mobiles. Cette fonction exploite l'infrastructure e-mail existante, ce qui permet aux utilisateurs nomades d'envoyer par courrier électronique une tâche d'impression en file d'attente, puis de la sortir d'une imprimante simple ou multifonction équipée de la solution. Protégez les périphériques d'impression réseau avec des fonctionnalités d'authentification sécurisées, dont Mobile Release.

Stoppez les fuites de données avant qu'elles ne se produisent

Les solutions HP vous aide à vous protéger contre la perte de données. Avec le service *HP Capture and Route Data Loss Prevention*, vous pouvez interdire la numérisation ou l'envoi par télécopie des informations sensibles. Le service de *HP Access Control Print Data Loss Prevention* vous permet d'interdire l'impression des documents sensibles. Suivez vos données les plus importantes pour décourager et empêcher les violations, sans ralentir les flux de travail. Obtenez des alertes de sécurité intelligentes basées sur les conditions de votre choix.

En appliquant des certificats numériques aux imprimantes

Améliorez la sécurité de votre environnement d'impression en appliquant des certificats numériques aux imprimantes et multifonctions en réseau. Gagnez du temps en utilisant HP JetAdvantage Security Manager, qui permet d'installer et de renouveler automatiquement les certificats.⁹



Protéger le document

Intégrez des solutions matérielles et logicielles intelligentes à votre plan global de sécurité informatique afin de protéger les informations sensibles de vos documents imprimés.⁶

Pratiques de sécurité de base

Contrôlez l'accès aux formulaires préimprimés

Équipez vos imprimantes simples et multifonctions de bacs d'alimentation munis de dispositifs de verrouillage pour empêcher les vols de papiers spéciaux utilisés pour l'impression des chèques, ordonnances ou autres documents sensibles.

Utilisez les options d'impression avec numéro d'identification personnel ou d'impression à partir du panneau commande pour protéger vos documents sensibles

Les utilisateurs peuvent choisir l'impression à partir du panneau commande ou l'impression avec numéro d'identification personnel, ce qui réduit à la fois la dépendance vis-à-vis des imprimantes personnelles ainsi que le risque de vol des tâches d'impression. Ces mesures de sécurité permettent également de limiter le nombre d'impressions non réclamées, ce qui réduit les coûts et le gaspillage.

En cas d'impression avec numéro d'identification personnel, lorsque les utilisateurs envoient des tâches d'impression confidentielles, ils leur attribuent un numéro d'identification personnel, qu'ils doivent saisir au niveau de l'appareil pour récupérer la tâche.

L'impression à partir du panneau commande stocke les tâches d'impression dans le cloud ou sur l'ordinateur de l'utilisateur. Les utilisateurs s'authentifient sur l'emplacement d'impression de leur choix pour lancer et imprimer leurs travaux. HP propose deux solutions d'impression à partir du panneau commande basées sur le cloud :

- *HP JetAdvantage Secure Print* est une solution abordable pensée pour les PME qui stocke les travaux dans le cloud ou sur le bureau de l'utilisateur. Facile à configurer et à utiliser, elle offre la possibilité de lancer des travaux depuis un périphérique portable et prend en charge les équipements multifournisseurs.¹²
- *HP JetAdvantage Private Print* est la solution basée sur le cloud de HP, vous avez les avantages de l'impression à partir du panneau commande sans la complexité. Elle est simple à configurer et ne nécessite aucun serveur, aucune installation et aucune maintenance.¹³

Pratiques de sécurité avancées

Exigez l'impression à partir du panneau commande pour toutes les tâches d'impression

HP Access Control Secure Pull Printing protège les informations confidentielles, améliore la sécurité de l'appareil et augmente l'efficacité. Cette solution robuste sur serveur offre plusieurs formes d'authentification, notamment l'émission de badges, ainsi que des fonctions de sécurité et de gestion de niveau professionnel.

Utilisez CMC7, les filigranes et d'autres fonctionnalités pour empêcher la copie ou la modification

Les solutions de lutte contre la contrefaçon HP et TROY incluent l'utilisation de toners sécurisés qui tachent le papier s'il est chimiquement falsifié, ajoutent des données variables en filigrane aux pages imprimées ou des codes lisibles par la machine, permettant de tracer et de contrôler différents documents. Les multifonctions peuvent intégrer des fonctionnalités anti-fraude (notamment des signatures personnalisées, des logos d'entreprise et des polices d'écriture sécurisées) aux documents sensibles imprimés tels que les ordonnances, certificats de naissance ou transcriptions.



En savoir plus

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Protection des documents HP et TROY
hp.com/go/HPandTROY



Surveiller et gérer votre environnement d'impression



En savoir plus

HP JetAdvantage Security Manager :
hp.com/go/securitymanager

La surveillance et les solutions de gestion de la sécurité peuvent vous aider à identifier les failles de sécurité pour établir une stratégie unifiée de protection des données, de réduction des risques et de maintenance de la conformité.⁶ Empêchez les lacunes de protection pour éviter des amendes coûteuses.

Pratiques de sécurité de base

Mettez à jour les appareils avec les derniers microprogrammes/Systèmes d'exploitation

Utilisez HP Web Jetadmin¹⁴ pour appliquer les mises à jour de micrologiciels à l'ensemble du parc, pour que les équipements soient munis des dernières fonctions de protection et de sécurité.

Vérification du journal des événements de sécurité des imprimantes

Les appareils HP envoient des notifications à un serveur syslog pour que les services informatiques puissent corriger les problèmes, au besoin.

Évaluer et corriger les paramètres des appareils

Gérez les paramètres de sécurité de base des imprimantes à l'échelle du parc avec *HP Print Manageability Integration Kit (MIK)*, un module d'extension pour Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM est une solution de gestion pour planifier, déployer, configurer et surveiller les points de terminaison à distance. HP Print MIK peut découvrir, évaluer et corriger les 15 principaux paramètres de sécurité et produire un rapport sur les résultats.

Pour une gestion de la sécurité complète à l'échelle du parc, choisissez *HP JetAdvantage Security Manager*.⁹ Cette solution vous aide à réduire les coûts et les ressources nécessaires pour établir la stratégie de sécurité de l'ensemble du parc, automatiser la correction des paramètres des appareils, et installer et renouveler des certificats uniques tout en produisant les rapports nécessaires pour prouver votre conformité.



En savoir plus

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Pratiques de sécurité avancées

Déployez des logiciels SIEM pour détecter et documenter les menaces

Les données d'événement émises par les appareils HP FutureSmart peuvent être envoyées à des outils de détection des incidents tels qu'ArcSight, Splunk et SIEMonster pour une surveillance en temps réel. Les terminaux d'imprimantes peuvent être facilement contrôlés par le service de sécurité informatique dans le cadre d'un écosystème plus large en vue de détecter et de résoudre les alertes de sécurité des imprimantes.

Configuration automatique des nouveaux appareils d'impression lorsqu'ils sont ajoutés au réseau

La fonctionnalité Instant-on Security intégrée à HP JetAdvantage Security Manager configure automatiquement les nouveaux appareils lorsqu'ils sont ajoutés au réseau ou après un redémarrage.

Rapport d'audit de conformité de la sécurité du parc d'imprimantes

Utilisez HP JetAdvantage Security Manager pour fournir des rapports attestant de la conformité afin d'apporter la preuve de l'application de politiques pour la sécurité des imprimantes et la protection des données de vos clients.

Toute infraction à la conformité peut nuire à votre entreprise

Des points de terminaison non-protégés ou sous-protégés sont des opportunités supplémentaires pour le crime informatique. Face à cette menace croissante, les autorités gouvernementales du monde entier mettent en œuvre des règles de sécurité strictes en demandant aux organisations de mieux protéger les informations des clients.

Les organisations qui ne sont pas en conformité peuvent subir des coûts importants, notamment des amendes,

manque à gagner, atteintes à la réputation et actions collectives

Il est essentiel de déployer des appareils et des solutions—tels que des imprimantes HP Enterprise et HP JetAdvantage Security Manager—qui peuvent vous aider à respecter les exigences de conformité et à protéger votre entreprise contre les menaces pour la sécurité.



Obtenez l'aide dont vous avez besoin

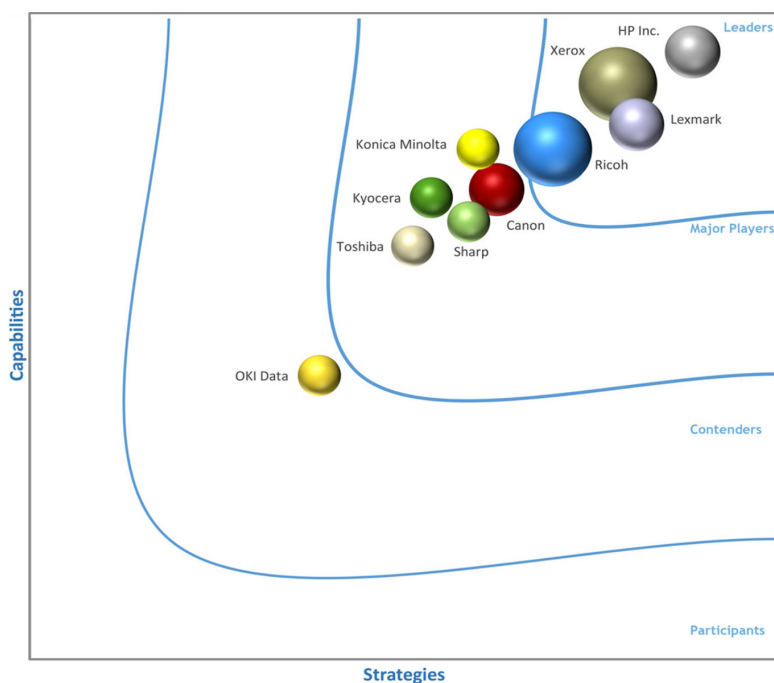
Vous n'avez pas à vous charger de la protection et de la sécurité. Une équipe support de consultants peut vous montrer comment améliorer la sécurité de vos données, appareils et documents.

Collaborez avec des experts en sécurité des imprimantes pour évaluer vos vulnérabilités actuelles en la matière. Nous pouvons vous aider à établir une politique de sécurité complète basée sur les meilleures pratiques et les besoins de votre entreprise ainsi qu'à élaborer un plan visant à améliorer la sécurité dans votre environnement.

Reconnu comme leader sur le marché

HP a été désigné leader dans le premier rapport IDC MarketScape dans la catégorie Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment. (Vous pouvez consulter le rapport [ici](#).) Selon le rapport, « l'approche de sécurité HP englobe l'intégralité de l'infrastructure d'impression et de gestion de documents, en commençant par le verrouillage du périphérique et l'inclusion de tous les aspects de l'utilisation du périphérique et de la protection du contenu. » Le graphique présenté ici provient de l'étude IDC 2017 Vendor Assessment.¹⁵

Le modèle d'analyse des fournisseurs IDC MarketScape vise à fournir une vue d'ensemble des fournisseurs ICT concurrents sur un marché donné. La méthode de recherche emploie un système de notation rigoureux, associant critères qualitatifs et quantitatifs, et produit une illustration graphique de la position de chaque fournisseur sur un marché donné. La note Capacités évalue les produits des fournisseurs, la commercialisation et l'exécution commerciale à court terme. La note Stratégie évalue l'alignement des stratégies des fournisseurs sur les exigences des clients sur une durée de 3 à 5 ans. La part de marché des fournisseurs est représentée par la taille des icônes.¹⁵



Pour commencer...

Prenez contact avec votre représentant pour avoir de plus amples informations sur les fonctions, solutions et services de sécurité HP et choisir une meilleure protection pour plus de sérénité.

Pour plus de détails

hp.com/go/printsecurity

¹ « Une impression davantage sécurisée », selon la revue HP concernant les fonctions de sécurité publiées en 2017 sur les imprimantes de cette catégorie. Seul HP propose une telle combinaison de fonctionnalités de sécurité capables de superviser les équipements efficacement, de détecter les attaques, de les bloquer et de valider l'intégrité des logiciels par un redémarrage. Pour consulter la liste des imprimantes : hp.com/go/PrintersThatProtect. Pour plus de détails : hp.com/go/printersecurityclaims.

² InfoTrends, « Conception de matériels et de solutions » ; Brendan Morse, octobre 2016.

³ Quocirca, « Gestion de l'environnement de services d'impression, 2016 », quocirca.com/content/managed-print-services-landscape-2016, juillet 2016.

⁴ Enquête de Spiceworks concernant 309 décideurs informatiques en Amérique du Nord, zones EMEA et Asie-Pacifique, réalisée pour le compte de HP en novembre 2016.

⁵ Quocirca, « Sécurité de l'imprimante : Une question essentielle à l'époque de l'internet des objets, » quocirca.com/content/print-security-imperative-iot-era, janvier 2017.

⁶ Des solutions peuvent ne pas être prises en charge par certains appareils HP ; certaines solutions nécessitent des achats supplémentaires.

⁷ Les fonctions de sécurité intégrées les plus avancées de HP sont disponibles sur les appareils HP de niveau professionnel dotés du micrologiciel FutureSmart 4.5 ou version supérieure ; résultat basé sur l'enquête comparative HP publiée en 2017 et portant sur les fonctions de sécurité intégrées des imprimantes concurrentes de même catégorie. Seul HP propose des fonctionnalités de sécurité qui vérifient l'intégrité des équipements d'impression jusqu'au niveau du BIOS et avec des capacités d'auto-correction. Pour obtenir la liste des produits compatibles, consultez hp.com/go/PrintersThatProtect. Pour de plus amples renseignements, consultez le site hp.com/go/printersecurityclaims.

⁸ Les périphériques HP LaserJet Pro et PageWide Pro sélectionnés incluent des fonctionnalités intégrées capables de détecter et arrêter une attaque. Pour de plus amples informations, rendez-vous sur hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager est vendu séparément. Pour en savoir plus, visitez hp.com/go/securitymanager.

¹⁰ Un mot de passe supplémentaire est requis lorsque vous envoyez des informations vers un référentiel protégé par un mot de passe.

¹¹ HP JetAdvantage Connect fonctionne avec la plupart des appareils mobiles. Un module d'extension doit être installé sur les équipements qui exécutent les systèmes d'exploitation Android™, Google Chrome™ et Microsoft®. Pour consulter la liste des systèmes d'exploitation pris en charge : hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print : Travaux d'impression sur équipement d'impression relié au réseau (imprimante ou multifonction). L'authentification directe sur l'équipement est disponible pour de nombreux modèles HP LaserJet, HP PageWide et HP OfficeJet Pro et certains modèles d'autres marques. Certains équipements pourront nécessiter une mise à niveau de leur microprogramme. Une connexion Internet est nécessaire pour stocker et récupérer les travaux d'impression dans le cloud. Le lancement des travaux d'impression depuis un terminal mobile exige une connexion réseau et un code QR. Pour plus de détails et pour consulter la liste des imprimantes et multifonctions prises en charge : hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print est disponible sans frais et nécessite que l'imprimante soit connectée à Internet avec les services Web activés. Non disponible dans certains pays. Pour en savoir davantage, rendez vous sur hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin peut être téléchargé gratuitement sur la page hp.com/go/webjetadmin.

¹⁵ Basé sur l'analyse IDC des fournisseurs d'impression et sur l'opinion concernant la position de leader de HP : « HP présente un avantage avec ses solides services et capacités informatiques...et sa stratégie de sécurité complète et intégrée qui s'applique à l'ensemble de l'infrastructure informatique. » SOURCE : [IDC MarketScape : Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](#), par Allison Correia et Robert Palmer, octobre 2017, IDC Doc #US41988517.

Abonnez-vous :

hp.com/go/getupdated



Partagez ce document avec des collègues

© Copyright 2014-2018 HP Development Company, L.P. Les informations données dans ce document peuvent faire l'objet de modifications à tout moment. 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 contenue dans le 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.

Android et Google Chrome sont des marques de Google Inc. Microsoft est une marques de commerce déposée du groupe Microsoft aux États-Unis.

4AA3-1295FRE, janvier 2018, rév. 11

