

Sécurité et disponibilité de HP PrintOS



Table des matières

Introduction.....	2
Datacenter	2
Sécurité.....	3
Datacenters sécurisés à haute disponibilité.....	3
Structure de conformité	3
Communications sécurisées et protection des données	3
Gestion de comptes et audit sécurisés	3
Confidentialité des données	3
Reprise après incident et sauvegardes	4
Supervision et gestion de la sécurité	4
Sphère de sécurité et règles d'entreprise contraignantes	4
Disponibilité.....	4
Conclusion	4

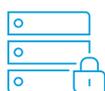
HP PrintOS est un système d'exploitation dédié à la production d'impression, doté d'un ensemble d'applications Web et mobiles, qui simplifient et automatisent votre production, afin de rentabiliser au mieux vos imprimantes graphiques et presses HP. Avec cette solution, améliorez constamment vos opérations, inspirez vos collaborateurs et prenez plus rapidement de meilleures décisions. Profitez de PrintOS pour gérer différents travaux, de la soumission à l'expédition, pour collaborer avec vos partenaires et collègues, mais aussi pour découvrir de nouvelles opportunités de croissance. Enfin, accédez à tout instant et de n'importe où à cette plateforme PrintOS ouverte et sécurisée sur le cloud.

HP s'engage intensément dans la sécurité des données sur le cloud pour qu'elles soient protégées au niveau le plus élevé. Les informations du présent document sont axées sur la sécurité et la disponibilité de la solution HP PrintOS. Elles décrivent les mesures que nous prenons dans différents domaines pour pallier aux éventuelles préoccupations que vous auriez en matière de confidentialité, d'intégrité et de disponibilité de vos systèmes et données.

Datacenter

(Certification ISO 27001 et prestataire de services de niveau 1 en vertu de la norme de sécurité des données de l'industrie des cartes de paiement.)

(Les datacenters sont soumis tous les ans à des audits SOC 1 et ont acquis le niveau « Moderate » pour les systèmes du gouvernement fédéral des États-Unis, ainsi que le niveau DIACAP 2 pour les systèmes du ministère de la défense.)



Entrepôt des données (Data Warehouse)

Les données au repos sont stockées sur un système de fichiers cryptés selon la norme LUKS avec une clé de 1 024 bits ou un cryptage AES 256.

Les mots de passe sont salés et hachés (techniques cryptographiques) avec la méthode SHA-256.



iMPACT Big Data



Le pare-feu et les sous-réseaux privés bloquent l'accès à nos environnements.



Transfert de données à l'aide de la connexion TLS 1.2



PrintOS

L'accès aux données est protégé par authentification, autorisation, gestion de compte et journalisation d'audit.

Applications relatives à la presse



Gestionnaire de supports



PrintBeat



Events sur le cloud

Applications relatives au DFE



Resource Manager



Site Flow



Box



Composeur



Imposeur

Transfert de l'entrepôt des données via connexion TLS 1.2

Réseau / Pare-feu client



Presse/imprimante HP



DFE/RIP HP



PC client



Tablette



Smartphone

Sécurité

HP s'efforce de maintenir les plus hautes normes de sécurité afin de protéger vos informations. Lorsque les données sont envoyées vers la plateforme cloud PrintOS, les utilisateurs peuvent être assurés que HP a fait tout son possible pour protéger les informations en sa possession. Afin de répondre aux exigences et aux défis chaque jour plus nombreux de l'environnement de cloud moderne, HP supervise et améliore constamment les applications, systèmes et processus essentiels à la solution HP PrintOS.

Pour que la sécurité et la haute disponibilité des datacenters adhèrent strictement à la supervision et à la gestion de la sécurité, HP adopte une approche stratifiée de la protection de vos informations et de vos activités d'impression.

Datacenters sécurisés à haute disponibilité

La stratégie de sécurité de HP se concentre avant tout sur les datacenters qui hébergent vos informations. Même si vous ne pouvez pas visiter les datacenters que HP utilise pour héberger la plateforme PrintOS, notre processus de contrôle vérifie que les emplacements concernés sont audités et certifiés par des agences tierces. Les datacenters ont obtenu la certification ISO 27001 et ont été validés en tant que prestataires de services de niveau 1 selon les normes de sécurité des données dans le cadre des paiements par carte (PCI-DSS). De plus, les datacenters sont soumis tous les ans à des audits SOC 1 et ont également acquis le niveau « Moderate » pour les systèmes du gouvernement fédéral des États-Unis, ainsi que le niveau DIACAP 2 pour les systèmes du ministère de la défense. Les datacenters sont protégés 24h/24, 7j/7 par des agents de sécurité entraînés ; et leur accès est autorisé strictement sur la base d'un droit d'accès minimal.

Structure de conformité

HP respecte les normes internationales, ce qui facilite pour vous le respect de vos propres spécifications nationales et locales. Nous maintenons une structure de conformité dynamique en assurant un suivi proactif des normes et réglementations en constante évolution. La structure de conformité PrintOS a été conçue pour constamment tenir compte des multiples certifications, spécifications réglementaires et attestations tierces.

Communications sécurisées et protection des données

Pour garantir un haut niveau de protection des données, HP applique de multiples mesures. Nous protégeons les données transmises à l'aide d'une connexion TLS 1.2. Les données au repos sont stockées sur un système de fichiers crypté selon la norme LUKS avec une clé de 1 024 bits ou un cryptage AES 256. Les mots de passe sont salés et hachés (techniques cryptographiques) avec la méthode SHA-256. Et la plateforme PrintOS doit obligatoirement suivre un processus de contrôle complet qui inclut la validation de la liste de contrôle de l'architecture de sécurité interne, la vérification du code par des experts et le test de vulnérabilité à données aléatoires.

Gestion de comptes et audit sécurisés

L'accès à vos données est protégé par authentification, autorisation, gestion de compte et journalisation d'audit. Ces facteurs sont évalués dans le cadre du processus de vérification de la sécurité de l'architecture.

HP tient à jour des journaux d'audit détaillés qui collectent des informations telles que le nom du compte, l'horodatage, ainsi que l'activité exécutée. L'accès à la base de données est limité aux seuls personnels autorisés. Et les journaux d'audit sont régulièrement sauvegardés et tenus à jour.

Confidentialité des données

HP a documenté et publié une déclaration de confidentialité qui interdit strictement la vente, la location, le transfert, la commercialisation ou la divulgation d'informations personnelles à des tiers. Les normes de confidentialité de HP sont mondiales et accessibles sur le site Web PrintOS ou en allant sur hp.com/go/privacy.

HP fournit et exige une formation à la sécurité et à la confidentialité pour ses employés qui manipulent des informations confidentielles ou personnelles. HP adhère également aux normes et aux processus mondiaux relatifs aux informations d'identification personnelles (PII).

HP utilise des mesures de protection administratives, techniques et physiques pour les environnements des clients et tire parti de programmes du secteur tels que « Safe Harbor » (Sphère de sécurité), ISO et autres pour que vos informations restent confidentielles.

Reprise après incident et sauvegardes

L'information est une ressource qui doit être disponible à tout moment. PrintOS s'exécute selon une conception de cloud de pointe, pour offrir une redondance physique et logique au niveau de chaque couche. Chaque couche de virtualisation est redondante pour assurer une haute disponibilité et une grande évolutivité.

Supervision et gestion de la sécurité

Nous empêchons également vos informations de tomber entre de mauvaises mains. Le pare-feu et des sous-réseaux privés bloquent l'accès à nos environnements ; et nos systèmes de détection des intrusions fonctionnent en permanence, offrant ainsi de hauts niveaux de protection aux données des clients. HP contrôle régulièrement l'environnement en matière de vulnérabilité des applications et infrastructures ; et, en cas d'incident, notre équipe d'intervention arrive pour résoudre le problème.

Sphère de sécurité et règles d'entreprise contraignantes

HP est conforme aux cadres « Sphère de sécurité » États-Unis-UE et États-Unis -Suisse, tels que définis par le ministère américain du commerce en matière de collecte, utilisation et rétention des données de pays membres de l'Union européenne et de la Suisse. HP certifie adhérer aux principes de confidentialité de la Sphère de sécurité en matière d'avertissement, de choix, de transfert, de sécurité, d'intégrité des données, d'accès et de mise en application. Pour en savoir plus sur le programme Sphère de sécurité et pour consulter la certification de HP, consultez export.gov/safeharbor/

HP a également établi un ensemble de règles d'entreprise contraignantes (BCR) approuvées par tous les organismes de réglementation de la protection des données dans l'Espace économique européen (EEE), dès juin 2011. Les BCR garantissent que les données personnelles des individus concernés de l'EEE sont protégées de façon appropriée lors de leur traitement par une entité mondiale de HP.

Disponibilité

Vos informations et vos activités sont précieuses pour HP, la disponibilité du site de la plateforme de cloud PrintOS est donc au minimum de 99,9 %.

Comme pour toute solution de service logiciel (SaaS), HP va occasionnellement planifier des interruptions pour maintenance ou pour améliorer, ajouter ou supprimer des fonctionnalités, selon ce qui nous semble le mieux pour nos activités et nos clients. Les interruptions planifiées pour ces raisons ne sont pas incluses dans le calcul de la disponibilité de la solution PrintOS.

La disponibilité de la solution PrintOS n'inclut pas non plus les indisponibilités de service provoquées par des circonstances qui échappent au contrôle de HP. Ces exceptions incluent, mais sans s'y limiter, la défaillance des systèmes de l'infrastructure informatique sur le site du client ou des défauts de transmission d'informations causés par des catastrophes naturelles, des mesures gouvernementales, des inondations, des incendies, des tremblements de terre, des troubles civils, des attentats, des grèves ou tout autre problème de personnel.

HP va, conformément aux usages du commerce, planifier et avertir les clients d'une indisponibilité prévue.

Conclusion

Tandis que le cloud crée de nouvelles opportunités dans la façon dont nous fournissons et consommons la technologie, HP PrintOS transforme la façon dont les prestataires de services d'impression, petits et grands, exercent leurs activités et génèrent des bénéfices. Ce qui différencie la solution de HP, c'est que nous allons plus loin pour nous assurer que vos données et systèmes sont sécurisés lorsque vous utilisez l'application. Avec la confidentialité, la protection des données et la disponibilité au cœur de notre stratégie de sécurité, vous pouvez faire confiance à HP et à la plateforme PrintOS pour protéger vos informations et votre entreprise.

Pour en savoir plus :

hp.com/go/printos

Abonnez-vous sur :
hp.com/go/getupdated



Partagez ce document avec vos collègues

