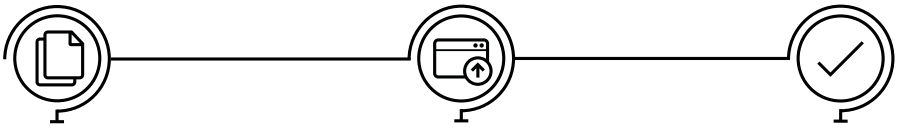
SERVICE DE SÉCURISATION DES PÉRIPHÉRIQUES

Sécurisation des périphériques de Canon. Amélioration des performances d'un périphérique d'impression afin de le protéger contre les incidents de sécurité. Notre service améliore la sécurité native des périphériques Canon en appliquant un profil sécurisé pour une protection accrue sans effort supplémentaire.



RECOMMANDER **CONFIGURER** **VALIDER**

BÉNÉFICES POUR VOTRE ENTREPRISE :

- Réduire le risque de perte de données en protégeant les données stockées sur les périphériques tout au long de leur cycle de vie.
- Étendre les politiques de confidentialité des données aux périphériques d'impression afin de maintenir un environnement sécurisé.
- Réduire le risque de failles de sécurité liées aux imprimantes et éviter le risque d'amendes réglementaires et d'atteinte à la réputation de la marque.

MENACES POTENTIELLES POUR VOTRE ENTREPRISE

- Vos périphériques stockent et traitent des données confidentielles, telles que des rapports financiers et d'autres informations sensibles.
- Vos périphériques sont connectés au réseau, ce qui peut les exposer à un risque d'attaque.
- Vos périphériques ne sont souvent pas considérés comme présentant un risque de sécurité, ce qui peut les rendre plus vulnérables.

Canon

SERVICE DE SÉCURISATION DES PÉRIPHÉRIQUES

CONFIGURATION POUR LA SÉCURISATION DES PÉRIPHÉRIQUES

Une configuration de profil sécurisée entièrement testée et intégrant les meilleures pratiques de cybersécurité recommandées et les attentes des acheteurs de solutions de sécurité.

Canon propose également un service sur mesure pour répondre aux besoins spécifiques des clients.

FONCTIONNALITÉ	DESCRIPTION
Activer l'option d'effacement sécurisé des données	Les données sont automatiquement effacées du stockage du périphérique après chaque tâche, une fois que toutes les pages ont été imprimées/faxées/numérisées/copiées.
Définir le mot de passe de l'interface utilisateur distante	L'interface utilisateur distante permet d'accéder aux paramètres du périphérique via l'interface Web. Le mot de passe autorise l'accès à cette interface.
Définir le mot de passe de l'administrateur système	L'administrateur système permet d'accéder au périphérique avec des privilèges administrateur. Le mot de passe par défaut est modifié pour une protection renforcée.
Définir le mot de passe de l'outil de gestion à distance	Le kit logiciel de l'opérateur distant permet d'accéder à distance à l'écran tactile et aux commandes du périphérique à des fins de maintenance. Le mot de passe offre une sécurité supplémentaire.
Activer la vérification de l'intégrité du système au démarrage	Le démarrage sécurisé est une fonction native du périphérique qui vérifie toute altération du code de démarrage, du micrologiciel et des applications MEAP au démarrage du périphérique.
Masquer les journaux des tâches du périphérique	Bloque l'affichage des journaux de tâches générés sur le périphérique, car ils peuvent inclure des noms de fichiers et des noms d'utilisateur.
Désactiver les protocoles et services inutilisés	Certains protocoles et ports actifs peuvent augmenter le risque d'attaques, de sorte que les paramètres inutilisés sont désactivés. C'est notamment le cas des protocoles SMB et FTP et du fax sur réseau IP.
Restreindre l'utilisation USB	Le périphérique ne peut pas être connecté à un PC via USB afin d'utiliser les fonctions d'impression et de numérisation. Les documents numérisés ne peuvent pas être enregistrés sur une clé USB.
Restreindre la connectivité aux réseaux sans fil	Le périphérique ne peut pas être connecté au réseau d'entreprise en Wi-Fi.
Interdire l'accès aux utilisateurs invités	Les utilisateurs non enregistrés ne peuvent pas s'identifier pour utiliser les fonctions du périphérique, ni imprimer des travaux envoyés via une impression sécurisée sur le périphérique.
Forcer la déconnexion automatique	Les utilisateurs sont automatiquement déconnectés si aucune opération n'est effectuée pendant plus de 30 secondes.
Restreindre l'utilisation d'algorithmes de cryptage faibles	La connexion aux systèmes prenant en charge le chiffrement faible relatif à IPSec, TLS, Kerberos, S/MIME, au LAN sans fil et à SNMPv3 est désactivée.

CONTACT

Pour plus d'informations, veuillez contacter votre bureau Canon local.

Canon Inc.
canon.com

Canon Europe
canon-europe.com

French edition

Canon France SAS
14 Rue Emile Borel
CS 28646
75809 PARIS CEDEX 17
Tél : 01 85 14 40 00
canon.fr, canon.be,
canon.lu, canon.ch