PROTÉGEZ VOS BUREAUX

Canon

LES INFORMATIONS CIRCULANT DANS VOS BUREAUX SONT-ELLES BIEN PROTÉGÉES ?

Aujourd'hui, les entreprises dépendent énormément des informations. Elles créent des réseaux complexes qui relient technologies, processus, personnes et entreprises bien au-delà des frontières d'un territoire national. De nouvelles pratiques de travail agiles font leur apparition, ce qui modifie la vie de bureau et la façon dont les professionnels créent, partagent et consomment les informations. La complexité de cet environnement rend la protection des données plus difficile que jamais et la plupart des entreprises investissent dans des technologies avancées telles que des pare-feux robustes, une protection anti-virus moderne, des logiciels de sécurité et bien d'autres encore. Néanmoins, elles ne se rendent souvent pas compte qu'elles devraient étendre cette protection à leurs imprimantes de bureau, demeurant plus vulnérables qu'elles ne le pensent.

PENSEZ À VOS IMPRIMANTES

Les imprimantes multifonction (MFP) modernes sont devenues aujourd'hui des outils puissants qui, à l'instar des ordinateurs et des serveurs, sont équipés d'un système d'exploitation, d'énormes disques durs, d'une connexion au réseau local et à Internet. Elles sont partagées entre de nombreux utilisateurs et traitent tous les jours une quantité impressionnante de documents de la plus haute importance.

QUELS SONT LES RISQUES ?

- Des utilisateurs non autorisés risquent de voir des informations sensibles sur les MFP non protégées
- La disponibilité du système d'impression peut être compromise par une erreur de manipulation
- Des personnes malveillantes extérieures à l'entreprise peuvent accéder à votre réseau via l'imprimante et l'utiliser pour mener des attaques
- L'exposition de documents confidentiels oubliés dans le bac de réception après impression
- Le mélange de documents imprimés appartenant à différents utilisateurs
- L'envoi de documents par télécopie ou par e-mail au mauvais destinataire suite à une faute de frappe
- Les données d'impression ou de numérisation en transit peuvent être interceptées par des pirates informatiques
- La perte de données suite à un manque de précaution au moment de la suppression des imprimantes au terme du contrat de location.

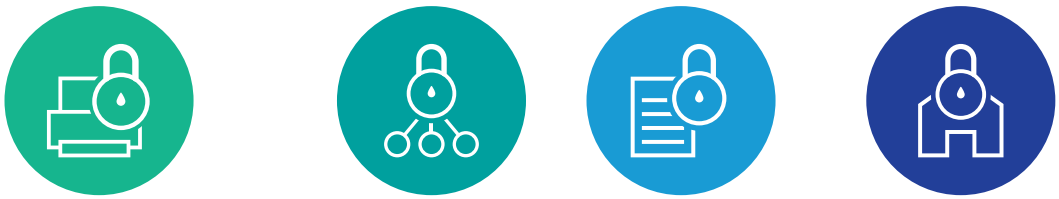
« Il est fortement recommandé d'adopter des normes fondamentales de sécurité informatique dans vos bureaux, où vous manipulez certainement des quantités de données colossales. Aujourd'hui, une imprimante n'est plus une simple machine toute bête : c'est un serveur qui, entre autres choses, imprime sur papier. »

(CISO, groupe Publicis)

DES SOLUTIONS D'IMPRESSION SÉCURISÉE POUR VOTRE ENTREPRISE

Conçues pour offrir sécurité et confidentialité

Lorsque nous concevons ou sélectionnons des technologies, des produits ou des services pour nos clients, nous tenons compte de leur impact en termes de sécurité sur l'environnement de nos clients. C'est pourquoi nos imprimantes de bureau multifonction sont équipées d'une vaste gamme de fonctionnalités de sécurité, en standard et en option, qui permettent aux entreprises de toutes tailles d'atteindre le degré de protection souhaité pour leurs :



PÉRIPHÉRIQUES | RÉSEAUX | DOCUMENTS | VOTRE ENTREPRISE

NORMES ET CERTIFICATIONS RECONNUES SUR LE PLAN INTERNATIONAL

Nos imprimantes multifonction imageRUNNER ADVANCE sont régulièrement évaluées et certifiées à l'aide de la méthode Critères Communs et conformément aux exigences des normes IEEE2600 relative à la sécurité des appareils d'impression.

TESTS DE SÉCURITÉ

Canon applique l'un des régimes de tests de sécurité les plus stricts du secteur de la bureautique. Les technologies incluses dans notre gamme de produits sont soumises à des normes d'essai aussi exigeantes que celles que nous attendons de nos propres fournisseurs.

En tant que leader dans le développement de solutions d'impression et de gestion de l'information innovantes pour les bureaux et les entreprises, Canon accompagne ses clients pour qu'ils adoptent une stratégie globale de protection des informations qui tienne compte de l'impact des technologies de bureau employées sur la sécurité de leur écosystème d'informations.

PROTÉGEZ VOTRE IMPRIMANTE

Une protection complète de votre matériel

SOLUTIONS D'AUTHENTIFICATION DES UTILISATEURS

Protégez vos périphériques de toute utilisation par des personnes non autorisées en mettant en place un contrôle d'accès utilisateur basé sur l'authentification. Cela permettra également aux utilisateurs d'accéder plus rapidement à leurs préférences et à leurs travaux d'impression, tandis que les fonctionnalités de contrôle et d'établissement des responsabilités seront renforcées. Nos imprimantes sont équipées de la solution de connexion flexible Universal Login Manager, qui permet d'authentifier les utilisateurs à l'aide d'une base de données utilisateurs stockée sur l'imprimante et d'authentifier les domaines à l'aide d'Active Directory ou du serveur uniFLOW. Ainsi, les entreprises peuvent contrôler l'accès à leurs imprimantes tout en gardant le juste équilibre entre convivialité pour les utilisateurs et protection.

CONTRÔLE DES FONCTIONS D'ADMINISTRATION DES IMPRIMANTES

La configuration des imprimantes, notamment celle des paramètres réseau, et d'autres options de contrôle, sont disponibles uniquement pour les utilisateurs dotés des privilèges administrateur, ce qui évite ainsi les modifications volontaires ou accidentelles.

SYSTÈME DE GESTION D'ACCÈS

Cette fonctionnalité offre un contrôle plus précis de l'accès aux fonctions de l'imprimante. Les administrateurs peuvent utiliser les rôles standard disponibles ou créer des rôles sur mesure dotés des droits d'accès spécifiquement requis. Par exemple, certains utilisateurs peuvent être privés de l'accès aux fonctions de copie ou d'envoi de documents.

PARAMÈTRE DE POLITIQUE DE SÉCURITÉ

Les modèles les plus récents de la gamme imageRUNNER ADVANCE sont également équipés d'une fonction de politique de sécurité qui permet à l'administrateur d'accéder à tous les paramètres de sécurité dans le même menu afin de les modifier et de les appliquer à l'imprimante. Une fois les paramètres appliqués, l'utilisation de l'imprimante et la modification de ses paramètres sont soumises à cette politique. La politique de sécurité peut être protégée par un mot de passe spécifique afin d'en réserver l'accès au responsable de la sécurité informatique, pour plus de contrôle et de protection.

PROTECTION DES DONNÉES SUR LE DISQUE DUR

Les imprimantes multifonction contiennent en permanence de grandes quantités de données qui doivent être protégées, qu'il s'agisse des travaux d'impression en attente, des fax reçus, des données numérisées, des carnets d'adresses, des journaux d'activité ou de l'historique des travaux. Les imprimantes Canon offrent différents moyens de protéger vos données à chaque étape du cycle de vie de l'appareil et garantissent la confidentialité, l'intégrité et la disponibilité des données.

COMMENT SÉCURISER VOS IMPRIMANTES ?

1
Vos imprimantes sont-elles partagées et situées dans des zones accessibles à tous ?

2
Les utilisateurs peuvent-ils accéder librement aux imprimantes ?

3
Prenez-vous des mesures de protection des informations contenues sur le disque dur de vos imprimantes ?

4
Les utilisateurs non autorisés peuvent-ils modifier les paramètres de vos imprimantes ?

5
Avez-vous réfléchi à tout le cycle de vie de vos imprimantes et à leur élimination sécurisée ?

CRYPTAGE DU DISQUE DUR

Sur les modèles imageRUNNER ADVANCE, toutes les données du disque dur sont cryptées pour plus de sécurité. La puce de sécurité responsable du chiffrement des données est conforme à la norme de sécurité FIPS 140-2 Niveau 2 fixée par le gouvernement américain et est certifiée par le Programme de Validation des Modules Cryptographiques (PVMC) mis en place par les États-Unis et le Canada, ainsi que par le Programme Japonais de Validation des Modules Cryptographiques (JCMVP).

EFFACEMENT DU DISQUE DUR

Certaines données, telles que les données d'images copiées ou numérisées, ainsi que les données relatives aux documents imprimés depuis un ordinateur, ne sont stockées que temporairement sur le disque dur : elles sont supprimées une fois la tâche terminée. Pour s'assurer qu'il ne reste pas de données résiduelles, nos imprimantes sont équipées d'un disque dur offrant la possibilité d'inclure l'effacement des données résiduelles dans les étapes du traitement des travaux.

INITIALISATION DE L'ENSEMBLE DES DONNÉES ET PARAMÈTRES

Pour éviter de perdre des données lorsque vous remplacez ou supprimez le disque dur, vous pouvez écraser l'ensemble des données et documents présents sur le disque dur, puis rétablir les paramètres par défaut de l'imprimante.

MISE EN MIROIR DU DISQUE DUR*

Les entreprises effectuent parfois des sauvegardes des données enregistrées sur le disque dur de leur imprimante vers un disque dur supplémentaire. Lors d'une mise en miroir, les données des deux disques durs sont entièrement cryptées.

KIT DISQUE DUR AMOVIBLE*

Cette option vous permet de déconnecter le disque dur de l'imprimante et de le stocker en lieu sûr lorsque l'appareil n'est pas en service.

* En option. Pour plus de renseignements sur la disponibilité des différentes fonctionnalités et options sur nos modèles d'imprimantes de bureau, veuillez contacter votre interlocuteur Canon.

SÉCURISEZ VOTRE RÉSEAU

VOTRE IMPRIMANTE MET-ELLE VOTRE RÉSEAU EN DANGER ?

- Certains ports de votre réseau sont-ils vulnérables aux attaques ?
- Les visiteurs peuvent-ils imprimer et numériser des documents sans mettre votre réseau en danger ?
- Vos politiques autorisant les employés à utiliser leurs périphériques personnels sont-elles gérables et sûres ?
- Les flux de données d'impression entre les ordinateurs et les périphériques de sortie sont-ils cryptés ?
- Le transit des données d'impression et de numérisation est-il sécurisé ?

Canon offre une gamme de solutions de sécurité qui protègent votre réseau et vos données des attaques internes et externes.

FILTRAGE DES ADRESSES IP ET MAC

Protégez votre réseau contre les accès non autorisés par des tiers en limitant les communications entrantes et sortantes aux seuls périphériques dotés d'une adresse IP ou MAC spécifique.

CONFIGURATION DU SERVEUR PROXY

Chargez un serveur proxy de la communication entre votre imprimante et les périphériques externes à votre réseau.

AUTHENTIFICATION IEEE 802.1X

L'accès non autorisé au réseau est bloqué par un commutateur de réseau local qui n'accorde l'accès qu'aux périphériques clients autorisés par le serveur d'authentification.

COMMUNICATION IPSEC

La communication sécurisée IPSec empêche les tiers d'intercepter ou d'altérer les paquets IP qui circulent sur le réseau IP.
Utilisez la communication cryptée TLS pour éviter le reniflage, la falsification ou l'altération des données échangées entre l'imprimante et d'autres périphériques, tels que des ordinateurs.

CONTRÔLE DES PORTS

Configurez les ports à l'aide des paramètres de politique de sécurité.

SURVEILLANCE À L'AIDE DE JOURNAUX

Divers journaux vous aident à surveiller les activités impliquant l'imprimante, y compris les demandes de communication refusées.

WI-FI DIRECT

Cette fonctionnalité permet d'établir une connexion P2P entre l'imprimante et un périphérique mobile, sans que ce dernier n'ait besoin d'accéder à votre réseau.

CRYPTAGE DES DONNÉES ENTRANT ET SORTANT DE L'IMPRIMANTE

Cette option permet de crypter les travaux d'impression lors de leur envoi vers l'imprimante multifonction depuis l'ordinateur d'un utilisateur. Lorsque toutes les fonctionnalités de sécurité universelles sont activées, il est également possible de crypter les données numérisées vers un format PDF.

IMPRESSION MOBILE POUR LES VISITEURS

Il est possible de sécuriser l'envoi de travaux par e-mail émanant d'une source externe via une plateforme Web ou une application mobile. En effet, notre logiciel de gestion d'impression et de numérisation sécurisée permet de renforcer la sécurité de l'impression depuis des périphériques mobiles appartenant à des visiteurs.
Ainsi, les possibilités d'attaques sont réduites, puisque l'imprimante multifonction est reliée à une source sécurisée.

SERVICE DE CONTRÔLE D'INTÉGRITÉ DE VOS BUREAUX

Ce service analyse l'intégralité du réseau local d'un client afin d'identifier les vulnérabilités internes et externes potentielles en matière de sécurité des données. Les conclusions et des recommandations sont réunies dans un rapport détaillé afin que le client puisse prendre les mesures appropriées.

PROTÉGEZ VOS DOCUMENTS

Toutes les entreprises manipulent des documents sensibles tels que des contrats, des fiches de paye, des données clients, des plans de recherche et de développement et bien d'autres encore. Si ces documents tombent entre de mauvaises mains, cela peut endommager la réputation de l'entreprise, occasionner de lourdes amendes ou même des poursuites.

Canon offre une gamme de solutions de sécurité pour protéger vos documents sensibles tout au long de leur cycle de vie.

CONFIDENTIALITÉ DU DOCUMENT IMPRIMÉ

Impression sécurisée
L'utilisateur peut définir un code PIN d'impression, afin que l'imprimante ne lance l'impression du document qu'après la saisie d'un code PIN valide. Ainsi, les utilisateurs peuvent protéger les documents qu'ils considèrent comme confidentiels.

Mise en attente de tous les travaux d'impression
Sur les modèles imageRUNNER ADVANCE, l'administrateur peut suspendre tous les travaux d'impression envoyés, obligeant les utilisateurs à s'identifier avant de pouvoir exécuter un travail d'impression, afin de protéger la confidentialité de tous les documents imprimés.

Boîtes de réception
Les travaux d'impression ou les documents numérisés peuvent être stockés dans une boîte de réception, d'où ils seront accessibles à un stade ultérieur. Ces boîtes de réception peuvent être protégées par un code PIN afin de garantir que seul le propriétaire désigné puisse afficher leur contenu. Cet espace sécurisé sur l'imprimante permet de stocker des documents qui ont souvent besoin d'être imprimés (tels que des formulaires), mais doivent faire l'objet de précautions.

Impression sécurisée uniFLOW*
L'impression sécurisée uniFLOW MyPrintAnywhere permet aux utilisateurs d'envoyer des travaux d'impression via un pilote d'impression universel et de réceptionner les travaux sur l'imprimante réseau de leur choix.

DÉCOURAGEZ OU EMPÊCHEZ LA CRÉATION DE MULTIPLES EXEMPLAIRES

Filigrane visible sur le document imprimé
Les pilotes peuvent imprimer une marque visible sur la page, à l'arrière-plan ou par-dessus le contenu du document. Cela décourage les tentatives de copie en attirant l'attention de l'utilisateur sur le caractère confidentiel du document.

Filigrane invisible sur le document imprimé/copié
Lorsque cette option est activée, un texte masqué peut être intégré à l'arrière-plan du document imprimé ou copié. Ce texte apparaît sur les copies du document original afin de décourager ce genre de tentative.

Verrouillage des scans*
Cette option intègre un code masqué dans les documents imprimés ou copiés, qui empêche toute création d'un nouvel exemplaire de ces documents sur toutes les imprimantes sur lesquelles cette fonction est activée. L'administrateur peut choisir d'appliquer le verrouillage à tous les travaux ou de rendre son utilisation facultative. Le code intégré peut être soit un code TL, soit un code QR.

Suivi de l'origine du document*
Un code intégré au document permet d'en retracer la source.

VOS DOCUMENTS SONT-ILS BIEN PROTÉGÉS ?

1
L'accès aux documents sensibles sur l'imprimante est-il bloqué pour les utilisateurs non autorisés ?

2
Pouvez-vous garantir la confidentialité de tous les documents traités par votre imprimante partagée ?

3
Pouvez-vous retracer l'origine de vos documents imprimés ?

4
Est-il possible pour quelqu'un d'emporter des documents sensibles sortis de l'imprimante ?

5
Prenez-vous des mesures pour prévenir les erreurs souvent commises lors de l'envoi de documents depuis l'imprimante ?

AMÉLIOREZ VOTRE CONTRÔLE DE L'ENVOI DE DOCUMENTS ET DES TÉLÉCOPIES

Limitation des destinations d'envoi
Pour réduire le risque de fuite d'informations, les administrateurs peuvent limiter les destinations d'envoi disponibles aux seules adresses présentes dans le répertoire ou sur le serveur LDAP, à l'adresse de l'utilisateur connecté ou à des domaines spécifiques.

Désactivation de la saisie automatique des adresses
Empêchez les erreurs de destinataire lors de l'envoi de documents en désactivant la saisie automatique des adresses e-mail.

Protection du carnet d'adresses
Configurez un code PIN afin d'empêcher les utilisateurs non autorisés à modifier le carnet d'adresses de l'imprimante.

Confirmation du numéro de fax
Évitez les erreurs de destinataire lors de l'envoi d'un document par télécopie en demandant aux utilisateurs de saisir deux fois le numéro de fax avant d'envoyer le document.

Confidentialité des fax reçus
Configurez l'imprimante multifonction pour qu'elle stocke les documents dans sa mémoire sans les imprimer. Vous pouvez également protéger la confidentialité des documents reçus par télécopie en créant des conditions déterminant l'emplacement de stockage vers des boîtes de réception confidentielles, éventuellement verrouillées par un code PIN.

VÉRIFIEZ L'ORIGINE DU DOCUMENT ET SON AUTHENTICITÉ GRÂCE AUX SIGNATURES NUMÉRIQUES

Signature de l'imprimante
La signature de l'imprimante peut être intégrée aux documents numérisés dans les formats PDF et XPS, sous forme d'une clé et d'un certificat. Ainsi, le destinataire peut vérifier l'origine du document ainsi que son authenticité.

Signature de l'utilisateur
Cette option permet aux utilisateurs d'envoyer un fichier PDF ou XPS doté d'une signature utilisateur numérique unique obtenue auprès d'une autorité de certification. Ainsi, le destinataire peut s'assurer que l'utilisateur a bien signé le document.

APPLIQUEZ VOS POLITIQUES À L'AIDE D'UN SERVEUR ADOBE LIVECYCLE MANAGEMENT ES INTÉGRÉ

Les utilisateurs peuvent sécuriser les fichiers PDF et appliquer des politiques dynamiques et persistantes afin de contrôler les droits d'accès et d'utilisation des documents, protégeant ainsi les informations sensibles et précieuses contre toute divulgation accidentelle ou malveillante.

L'administration des politiques de sécurité est effectuée au niveau du serveur, de sorte que les droits restent modifiables après la distribution du fichier. La gamme imageRUNNER ADVANCE est compatible avec Adobe® ES.

SERVICE DE SUPPRESSION DES DONNÉES*

Un service complet de suppression des données physiques et numériques sur vos imprimantes et appareils multifonctions Canon en fin de vie, conçu pour minimiser le risque d'atteinte à la sécurité des données.

* En option. Pour plus de renseignements sur la disponibilité des différentes fonctionnalités et options sur nos modèles d'imprimantes de bureau, veuillez contacter votre interlocuteur Canon.

SÉCURITÉ DES INFORMATIONS DE L'ENTREPRISE

Canon peut contribuer à la protection globale des informations au sein de votre entreprise.

UN CONTRÔLE TOTAL DE VOS FLUX DE NUMÉRISATION ET D'IMPRESSION

Grâce à notre logiciel de gestion des sorties modulaire, les entreprises peuvent partager des imprimantes réseau en toute sécurité. Ainsi, elles peuvent imprimer leurs documents de manière sécurisée sur n'importe quelle imprimante connectée au serveur de gestion des sorties. Les utilisateurs de périphériques mobiles bénéficient d'un service centralisé offrant un accès sécurisé à l'impression depuis des appareils mobiles, pour les utilisateurs internes et externes.
En ce qui concerne la numérisation, un module de scanner assure la capture, la compression, la conversion et la distribution des documents à partir de l'appareil multifonction vers un large éventail de destinations, dont des systèmes Cloud. Vous pouvez également rediriger des travaux d'impression vers l'imprimante la plus appropriée afin d'optimiser le coût d'impression de chaque document.
Notre solution améliore la sécurité des documents dans toute l'entreprise et permet d'assurer un suivi complet des documents grâce à une visibilité totale de l'activité par utilisateur, par imprimante et par service.

GESTION CENTRALISÉE DU PARC D'IMPRIMANTES

Notre logiciel IW MC de gestion de parc d'imprimantes permet de mettre à jour et d'appliquer les paramètres des imprimantes, leurs politiques de sécurité, les mots de passe et les certificats, ainsi que la mise à jour des microprogrammes de manière synchronisée sur toutes les imprimantes Canon de votre réseau. Ainsi, votre service informatique gagne un temps précieux et il vous sera plus facile d'effectuer les mises à jour de sécurité sur votre parc d'imprimantes.

AUDITS COMPLETS DES DOCUMENTS

Votre structure de services documentaires peut être optimisée à l'aide d'options sur mesure visant à enregistrer toutes les informations (par exemple, en enregistrant les métadonnées des travaux de numérisation) relatives aux documents traités par des imprimantes imageRUNNER ADVANCE.

SOLUTION INTÉGRÉE DE PRÉVENTION CONTRE LA PERTE DES DONNÉES

Canon vous permet d'étendre votre stratégie de prévention des pertes de données à votre réseau d'impression, grâce à la journalisation de toutes les données d'impression, de copie et de numérisation.

SERVICES DE GESTION DE L'IMPRESSION

Les services de gestion de l'impression (MPS) de Canon allient des technologies et logiciels innovants à des services adaptés afin de vous offrir l'expérience d'impression et de gestion documentaire que vous souhaitez sans alourdir la tâche de votre service informatique. En assurant la gestion proactive et l'optimisation en continu de votre infrastructure d'impression et de vos flux documentaires, nous vous aidons à atteindre vos objectifs en matière de sécurité, à réduire vos coûts et à améliorer la productivité dans toute l'entreprise.

CONCEPTION SUR MESURE

Nous disposons d'une équipe interne de développeurs qui peuvent concevoir pour vous une solution sur mesure, parfaitement adaptée à votre situation ou à vos besoins uniques.

SERVICE D'ÉVALUATION DE LA CONFORMITÉ AVEC LE RGPD

Cet audit des renseignements personnels conservés par l'entreprise l'aide à comprendre en quoi elle est concernée par le Règlement Général sur la Protection des Données (RGPD) afin de mieux protéger ses employés et ses clients.

LA STRATÉGIE DE PROTECTION DES DONNÉES DE VOTRE ENTREPRISE EST-ELLE SUFFISAMMENT ÉTENDUE ?

- Votre politique de sécurité s'étend-elle à votre parc d'imprimantes multifonction ?
- Veillez-vous à ce que votre parc d'imprimantes soit à jour et à ce que les améliorations et les correctifs soient appliqués promptement et efficacement ?
- Les visiteurs peuvent-ils imprimer et numériser des documents sans mettre votre réseau en danger ?
- Vos politiques autorisant les employés à utiliser leurs périphériques personnels sont-elles gérables et sûres pour l'ensemble de votre parc d'imprimantes ?
- Votre service informatique a-t-il le temps d'examiner les problèmes de sécurité ?
- Avez-vous trouvé le juste équilibre entre sécurité des données et convivialité pour les utilisateurs ?