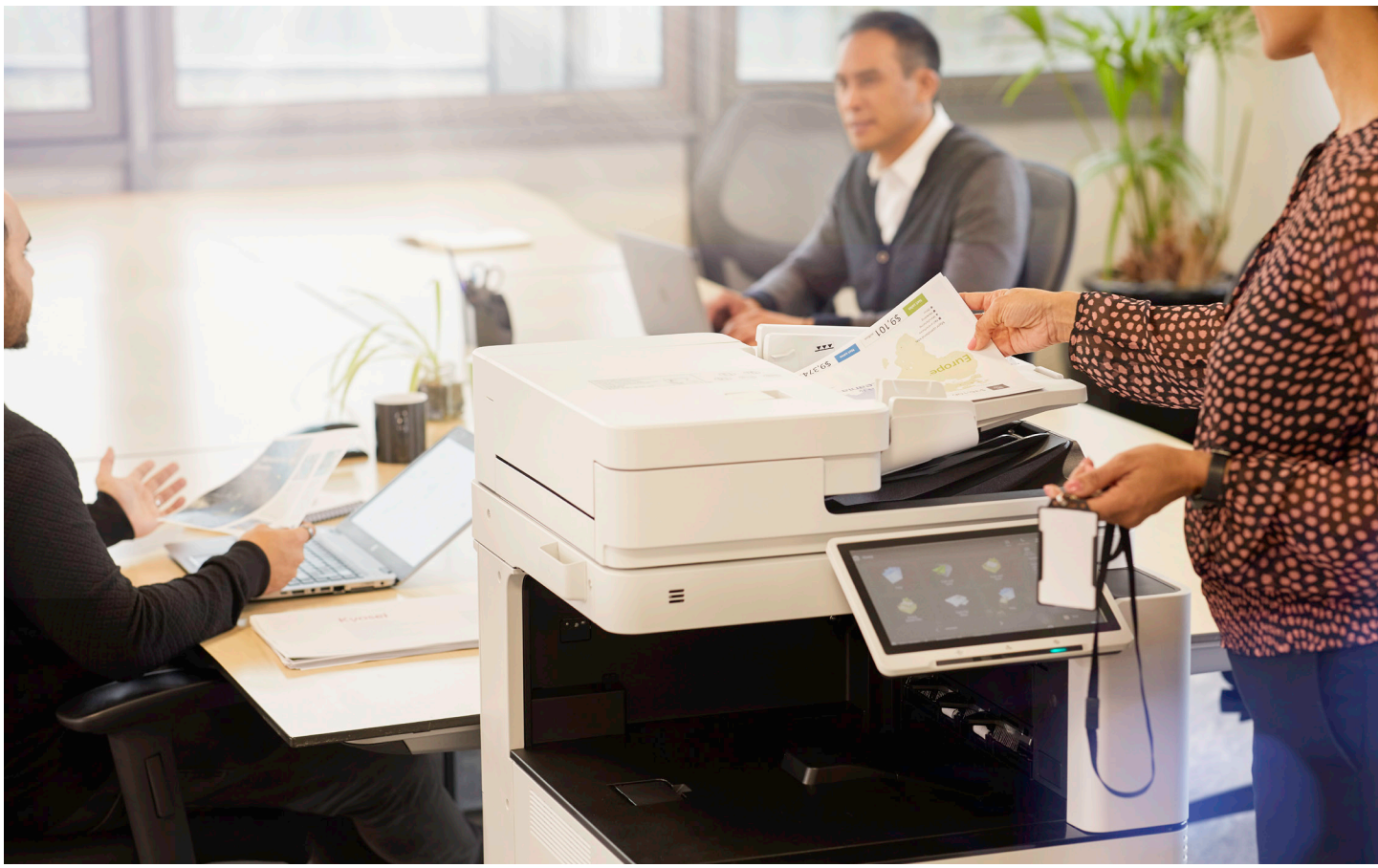


PROTÉGER VOTRE BUREAU

McAfee PROTECTED

COPIER MFP LINE OF THE YEAR 2018 BLI BUYERS LAB LINE OF THE YEAR

BLI BUYERS LAB 2019 PICK

Canon uniFLOW Online
Outstanding Cloud Output-Management Solution

COPIER MFP LINE OF THE YEAR 2020 BLI BUYERS LAB LINE OF THE YEAR

Canon

LES INFORMATIONS SONT-ELLES SÉCURISÉES DANS VOTRE BUREAU ?

Aujourd'hui, le fonctionnement des entreprises repose fortement sur des informations, créant ainsi des réseaux complexes de technologies, de processus, de personnes et d'organisations, tous reliés entre eux et dépassant les frontières. Dans l'ère de la transformation numérique, de nouvelles pratiques de travail agiles font leur apparition et restructurent le bureau et la façon dont les gens créent, partagent et consomment les informations. La sécurisation des données dans cet environnement complexe est plus délicate que jamais, et la plupart des entreprises investissent dans des technologies sophistiquées telles que des pare-feu robustes, des protections antivirus ultra modernes, des logiciels de sécurité et bien plus encore. Toutefois, elles échouent souvent à reconnaître la nécessité d'étendre cette protection à leurs imprimantes de bureau, et deviennent alors plus vulnérables qu'elles ne le réalisent.

PENSEZ À VOS IMPRIMANTES

Les imprimantes multifonctions modernes ont évolué en de puissants outils qui, comme les PC et les serveurs, sont dotés de systèmes d'exploitation, d'énormes disques durs, se connectent au réseau et à Internet, et sont partagés par les utilisateurs pour gérer au quotidien un grand nombre de documents professionnels sensibles.

QUELS SONT LES RISQUES ?

- Utilisateurs non autorisés consultant des informations sensibles stockées sur des imprimantes multifonctions non protégées
- Disponibilité de votre infrastructure d'impression compromise en raison d'une mauvaise opération
- Intrus malveillants qui accèdent à votre réseau via l'imprimante et l'utilisent pour d'autres attaques
- Divulgation de documents confidentiels oubliés dans le bac de sortie après leur impression
- Documents imprimés mélangés et appartenant à différents utilisateurs
- Documents envoyés par fax ou par e-mail à des destinataires incorrects en raison de fautes de frappe
- Données d'impression ou de numérisation en transit interceptées par des pirates informatiques
- Pertes de données dues à un traitement sans attention des retraits d'imprimantes à la fin de leurs contrats de location.

« Il est particulièrement judicieux d'adopter des normes de base en matière de sécurité des informations au bureau si vous gérez de grands volumes de données. Aujourd'hui, une imprimante n'est plus une simple machine, c'est un serveur qui imprime également du papier. »

(CISO, Publicis Groupe)

SOLUTIONS D'IMPRESSION SÉCURISÉE POUR VOTRE ENTREPRISE

Sécurité et confidentialité par nature

Lors de la conception ou du choix des technologies, produits et services pour nos clients, nous prenons en compte leur impact probable en matière de sécurité des informations sur l'environnement de nos clients. C'est pourquoi nos imprimantes multifonctions de bureau sont équipées d'un large éventail de fonctionnalités de sécurité, à la fois standard et en option, qui permettent aux entreprises de toute taille d'atteindre le niveau de protection désiré pour :

IMPRIMANTE | RÉSEAUX | DOCUMENTS | VOTRE ENTREPRISE

NORMES ET CERTIFICATIONS RECONNUES INTERNATIONALEMENT

Nos imprimantes multifonctions imageRUNNER ADVANCE sont régulièrement évaluées et certifiées à l'aide de la méthodologie Critères Communs (CC) et conformément aux exigences des normes IEEE2600 pour la sécurité des périphériques d'impression.

TESTS DE SÉCURITÉ

Canon emploie une des méthodes de test de sécurité les plus rigoureuses dans le secteur des équipements de bureau. Les technologies adoptées pour notre gamme de produits sont soumises aux mêmes normes élevées de tests attendues dans notre propre entreprise.

En tant que leader du secteur dans le développement de solutions innovantes d'impression et de gestion de l'information pour le bureau et l'entreprise, Canon travaille en collaboration avec les clients pour les aider à adopter une approche inclusive en matière de sécurité des informations, qui tient compte des implications de sécurité de notre technologie de bureau dans leur écosystème de l'information étendu.

PROTÉGER VOTRE PÉRIPHÉRIQUE

Protection complète de vos ressources physiques

SOLUTIONS D'AUTHENTIFICATION DE L'UTILISATEUR

Protégez votre périphérique contre toute utilisation non autorisée en mettant en place un contrôle d'accès utilisateur via une authentification. Cela a également l'avantage de fournir aux utilisateurs un accès plus rapide à leurs paramètres et travaux d'impression préférés, tout en améliorant la responsabilité et le contrôle. Nos imprimantes de service sont équipées d'uniFLOW Online Express, une solution de connexion flexible qui permet l'authentification de l'utilisateur par rapport à une base de données utilisateur créée sur le périphérique, l'authentification du domaine via Active Directory ou le serveur uniFLOW. Les entreprises peuvent ainsi contrôler l'accès aux périphériques, tout en obtenant le juste équilibre entre le confort et la sécurité de l'utilisateur.

PROTECTION DES DONNÉES SUR LE DISQUE DUR

L'imprimante multifonction contient en permanence une grande quantité de données qui doivent être protégées, qu'il s'agisse des travaux en attente d'impression, des télécopies reçues, des données numérisées, des carnets d'adresses, des journaux d'activité ou de l'historique des travaux. Les périphériques Canon proposent un certain nombre de mesures pour protéger vos données à chaque étape de la durée de vie du périphérique et pour assurer la confidentialité, l'intégrité et la disponibilité des données.

SYSTÈME DE GESTION DE L'ACCÈS

Cette fonctionnalité fournit un contrôle granulaire de l'accès aux fonctions du périphérique. Les administrateurs peuvent utiliser les rôles standard disponibles ou créer des rôles sur mesure avec un niveau souhaité de privilèges d'accès. Par exemple, certains utilisateurs peuvent être restreints et incapables de copier des documents ou d'utiliser la fonction d'envoi.

PARAMÉTRAGE DE LA POLITIQUE DE SÉCURITÉ

Les derniers périphériques imageRUNNER ADVANCE DX sont également équipés d'une fonction de politique de sécurité, ce qui permet à l'administrateur d'accéder à tous les paramètres liés à la sécurité dans un menu unique et de les modifier avant leur mise en place sur la machine. Une fois appliqués, l'utilisation du périphérique et les modifications des paramètres doivent se conformer à la politique. La politique de sécurité peut être protégée par un mot de passe séparé, de sorte que l'accès à cette zone soit limité au responsable de la sécurité informatique, ce qui ajoute un niveau de contrôle et d'assurance supplémentaire.

ADMINISTRATION DU CONTRÔLE DU PÉRIPHÉRIQUE

La configuration du périphérique, comme les paramètres réseau et d'autres options de contrôle, est proposée uniquement aux utilisateurs qui ont des privilèges d'administrateurs, ce qui empêche les modifications intentionnelles et accidentelles.

SÉCURITÉ PRÉVENTIVE

Les produits imageRUNNER ADVANCE DX offrent un certain nombre de paramètres de sécurité qui permettent de protéger les imprimantes contre des attaques. La fonctionnalité de vérification du système au démarrage assure l'intégrité de l'appareil une fois l'ordinateur démarré, tandis que McAfee Embedded Control garantit l'intégrité tout au long de la durée de vie de l'appareil, en empêchant les programmes d'être manipulés ou les programmes non autorisés de fonctionner lorsque l'appareil est en marche. En outre, les données Syslog fournissent des informations en temps réel sur l'intégrité du système de sécurité du périphérique, ainsi que des fonctionnalités de surveillance (les données peuvent être lues par un système SIEM tiers approprié).

VOS PÉRIPHÉRIQUES SONT-ILS SÉCURISÉS ?

1
Vos périphériques sont-ils partagés et situés dans des espaces publics ?

2
Les utilisateurs peuvent-ils accéder de manière non sécurisée aux périphériques ?

3
Avez-vous des mesures en place pour protéger les informations sur le disque dur du périphérique ?

4
Les utilisateurs non autorisés peuvent-ils modifier les paramètres du périphérique ?

5
Avez-vous pensé au cycle de vie de votre périphérique et à son élimination sécurisée ?

CRYPTAGE DU DISQUE DUR

Nos périphériques imageRUNNER ADVANCE DX cryptent toutes les données sur le disque dur, améliorant la sécurité. La puce de sécurité responsable du cryptage des données est conforme à la norme de sécurité FIPS 140-2 de niveau 2 établie par le gouvernement américain et est certifiée par le programme CMVP (Cryptographic Module Validation Program) établi par les États-Unis et le Canada, ainsi que par le programme JCMVP (Japan Cryptographic Module Validation Program).

EFFACEMENT DU DISQUE DUR

Certaines données, telles que les données d'image copiées ou numérisées, ainsi que les données de documents imprimés à partir d'un ordinateur, sont uniquement stockées de façon temporaire sur le disque dur et supprimées après l'opération. Afin de s'assurer qu'aucune donnée résiduelle n'est conservée, nos périphériques équipés d'un disque dur proposent d'effacer régulièrement les données résiduelles dans le cadre du traitement des travaux.

INITIALISATION DE TOUTES LES DONNÉES ET PARAMÈTRES

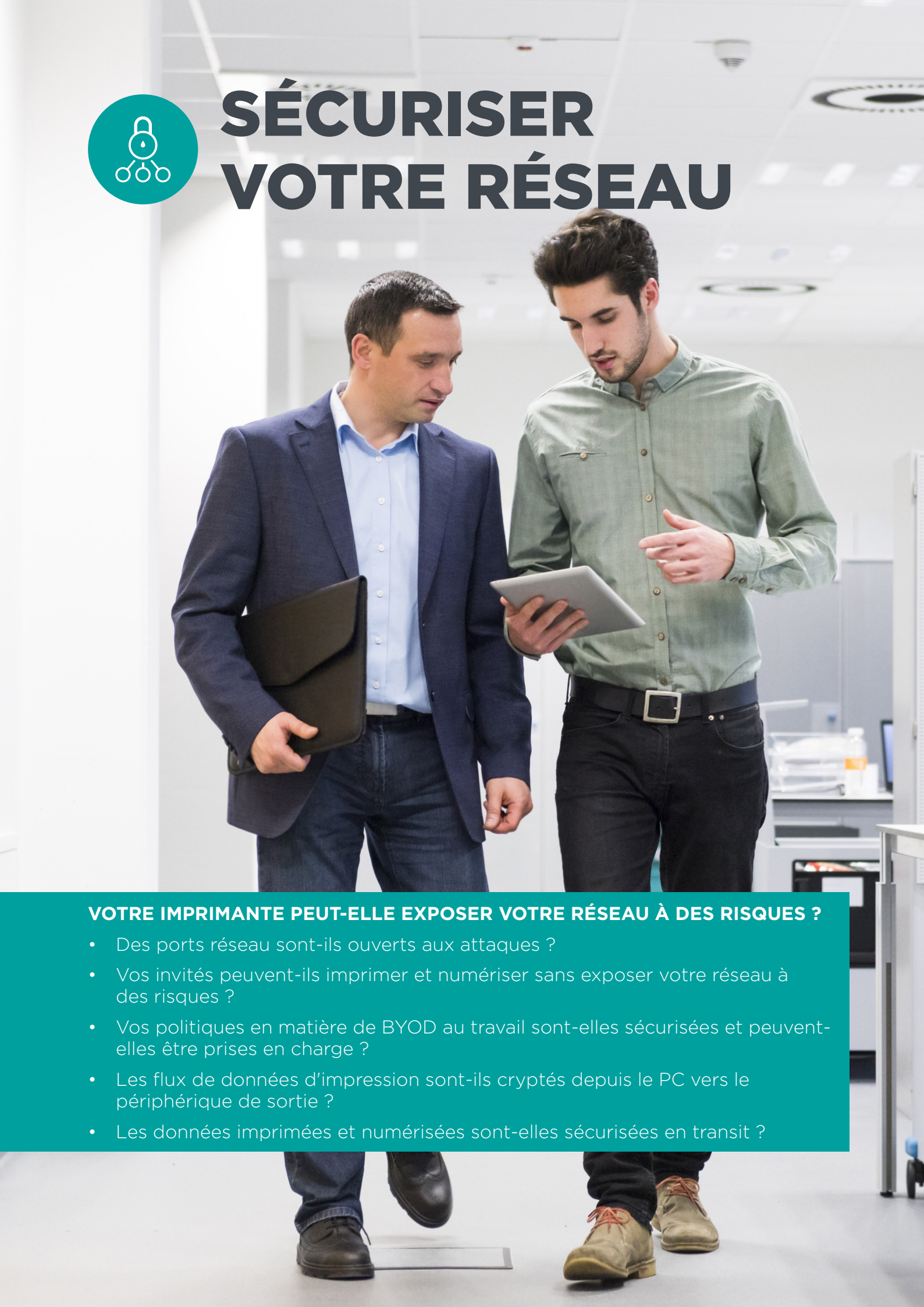
Pour éviter la fuite de données lors du remplacement ou de l'élimination du disque dur, vous pouvez écraser tous les documents et les données sur le disque dur, et restaurer les paramètres par défaut de la machine.

ÉCRITURE SUR DISQUE DUR*

Les entreprises ont la possibilité de sauvegarder les données du disque dur de leur périphérique à l'aide d'un disque dur supplémentaire en option. Une fois l'écriture terminée, les données des deux disques durs sont entièrement cryptées.

*En option pour certains modèles. Pour obtenir des informations détaillées sur la disponibilité des fonctionnalités et des options dans la gamme d'impression de bureau, veuillez contacter votre représentant Canon.

SÉCURISER VOTRE RÉSEAU



VOTRE IMPRIMANTE PEUT-ELLE EXPOSER VOTRE RÉSEAU À DES RISQUES ?

- Des ports réseau sont-ils ouverts aux attaques ?
- Vos invités peuvent-ils imprimer et numériser sans exposer votre réseau à des risques ?
- Vos politiques en matière de BYOD au travail sont-elles sécurisées et peuvent-elles être prises en charge ?
- Les flux de données d'impression sont-ils cryptés depuis le PC vers le périphérique de sortie ?
- Les données imprimées et numérisées sont-elles sécurisées en transit ?

Canon propose une gamme de solutions de sécurité pour sécuriser votre réseau et vos données contre les attaques internes et externes.

FILTRAGE PAR ADRESSE MAC ET IP

Protégez votre réseau contre tout accès non autorisé par des tiers en autorisant uniquement les communications avec les périphériques dotés d'une adresse MAC ou IP spécifique pour les communications entrantes et sortantes.

CONFIGURATION D'UN SERVEUR PROXY

Configurez un proxy à la place de votre machine pour gérer les communications et utilisez-le lorsque vous vous connectez à des périphériques en dehors du réseau.

AUTHENTIFICATION 802.1X IEEE

L'accès réseau non autorisé est bloqué par un commutateur LAN qui donne uniquement les privilèges d'accès aux périphériques clients qui sont autorisés par le serveur d'authentification.

COMMUNICATION IPSEC

La communication IPSec empêche les tiers d'intercepter ou d'altérer les paquets IP transportés sur le réseau IP.

Utilisez les communications cryptées TLS pour empêcher le reniflage, l'usurpation et l'altération des données échangées entre la machine et d'autres périphériques comme des ordinateurs.

CONTRÔLE DES PORTS

La configuration des ports fait partie intégrante du paramétrage de votre politique de sécurité.

INSCRIPTION AUTOMATIQUE DES CERTIFICATS

Grâce à cette fonctionnalité, la corvée liée au maintien des certificats de sécurité est considérablement réduite. À l'aide d'une technologie reconnue par le secteur, un administrateur système peut mettre à jour et délivrer automatiquement les certificats, en s'assurant que les politiques de sécurité sont respectées à tout moment.

CONTRÔLE DES JOURNAUX

Différents journaux vous permettent de contrôler l'activité autour de votre périphérique, y compris les demandes de communication bloquées.

WI-FI DIRECT

Activez la connexion peer-to-peer pour l'impression mobile sans que l'appareil mobile ne soit obligé d'accéder à votre réseau.

CRYPTAGE DES DONNÉES EN TRANSIT VERS ET DEPUIS LE PÉRIPHÉRIQUE

Cette option permet de crypter les travaux d'impression en transit depuis le PC de l'utilisateur vers l'imprimante multifonction. En activant l'ensemble de fonctionnalités de sécurité universelles, les données numérisées au format PDF peuvent également être cryptées.

IMPRESSION INVITÉ MOBILE

Notre logiciel de gestion d'impression et de numérisation réseau sécurisé traite les risques de sécurité communs pour l'impression mobile et invité en fournissant des voies de soumission des travaux externes via e-mail, Web et application mobile. Cela réduit les vecteurs d'attaque en verrouillant l'imprimante multifonction sur une source sécurisée.

DOUBLE RÉSEAU

La dernière technologie offre désormais une double capacité de réseau : même si le réseau principal est toujours câblé, la ligne secondaire peut désormais être câblée ou sans fil pour une séparation plus stricte des réseaux.

PROTÉGER VOS DOCUMENTS

Toutes les entreprises gèrent des documents sensibles tels que des accords contractuels, des informations relatives aux salaires du personnel, des données client, des plans de recherche et de développement et plus encore. Si ces documents tombent entre de mauvaises mains, les conséquences peuvent être nombreuses, d'une réputation ternie jusqu'à de lourdes amendes ou même une action en justice.

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

CONFIDENTIALITÉ DES DOCUMENTS IMPRIMÉS

Impression sécurisée
L'utilisateur peut définir un code PIN pour l'impression, de sorte que le document peut être imprimé seulement si le code PIN correct est saisi sur la machine. Cela permet aux utilisateurs de sécuriser les documents qu'ils estiment confidentiels.

Attente de tous les travaux d'impression
Sur imageRUNNER ADVANCE DX, l'administrateur peut appliquer une attente à tous les travaux d'impression soumis, de sorte que les utilisateurs doivent commencer par se connecter avant que les travaux ne puissent être imprimés pour protéger la confidentialité de tous les documents imprimés.

Boîtes aux lettres
Les travaux d'impression ou les documents numérisés peuvent être stockés dans une boîte aux lettres pour un accès ultérieur. Les boîtes aux lettres peuvent être protégées par un code PIN pour s'assurer que seul leur propriétaire désigné peut consulter les documents qui y sont stockés. Cet espace sécurisé sur la machine est adapté pour conserver les documents qui doivent être fréquemment produits (comme des formulaires), mais qui nécessitent une gestion minutieuse.

Impression sécurisée uniFLOW*
Avec l'impression sécurisée uniFLOW MyPrintAnywhere, les utilisateurs envoient les travaux d'impression via le pilote universel et les récupèrent sur n'importe quelle imprimante du réseau.

DÉCOURAGER OU EMPÊCHER LA DUPLICATION DE DOCUMENTS

Impression avec des filigranes visibles
Les pilotes ont la possibilité d'imprimer des marques visibles sur la page, en surimpression sur ou sous le contenu du document. Cela décourage la copie en sensibilisant l'utilisateur quant à la confidentialité du document.

Impression/copie avec des filigranes invisibles
Quand cette option est activée, les documents peuvent être imprimés ou copiés avec du texte masqué intégré en arrière-plan, de sorte que le texte s'affiche lors de la duplication du document et exerce un effet dissuasif.

Prévention de la perte des données au niveau de l'entreprise
Mettez à niveau vos fonctionnalités de prévention de la perte des données standard vers iW SAM Express en combinaison avec uniFLOW. Cette solution serveur vous permet de capturer et d'archiver les documents envoyés vers et depuis l'imprimante, d'effectuer des analyses et des interprétations à l'aide de textes ou d'attributs avec comme objectif de contrer les menaces de sécurité.

Suivi de l'origine du document*
Par le biais d'un code intégré, l'origine du document peut être suivie jusqu'à la source.

VOS DOCUMENTS SONT-ILS SÉCURISÉS ?

1
Les utilisateurs non autorisés sont-ils empêchés d'accéder aux documents sensibles sur l'imprimante ?

2
Pouvez-vous garantir la confidentialité de tous les documents des utilisateurs qui transitent par le périphérique partagé ?

3
Pouvez-vous retrouver l'origine des documents imprimés ?

4
Une personne peut-elle s'emparer de documents sensibles sur votre imprimante ?

5
Pouvez-vous éviter les erreurs courantes lors de l'envoi de documents à partir du périphérique ?

EXERCER UN CONTRÔLE SUR L'ENVOI ET LA TÉLÉCOPIE DE DOCUMENTS

Limiter les destinations pour l'envoi
Pour réduire le risque de fuite d'informations, les administrateurs peuvent restreindre les destinations d'envoi disponibles uniquement à celles figurant dans le carnet d'adresses ou sur le serveur LDAP, à l'adresse de l'utilisateur connecté ou à certains domaines.

Désactiver la saisie automatique des adresses
Empêchez l'envoi de documents vers de mauvaises destinations en désactivant la saisie automatique des adresses e-mail.

Protection du carnet d'adresses
Définissez un code PIN pour protéger le carnet d'adresses du périphérique contre les modifications non autorisées par les utilisateurs.

Confirmation du numéro de télécopie
Empêchez l'envoi de documents à des destinataires non désirés en obligeant les utilisateurs à saisir deux fois le numéro de télécopie pour confirmation avant l'envoi.

Confidentialité des télécopies reçues
Configurez la machine pour stocker les documents dans la mémoire sans les imprimer. Vous pouvez également protéger la confidentialité des télécopies reçues en appliquant des conditions permettant de déterminer l'emplacement de stockage pour une boîte de réception confidentielle, mais aussi définir des codes PIN.

VÉRIFIER L'ORIGINE ET L'AUTHENTICITÉ DES DOCUMENTS GRÂCE AUX SIGNATURES NUMÉRIQUES

Signature du périphérique
Une signature de périphérique peut être appliquée à des documents numérisés au format PDF ou XPS à l'aide d'une clé et d'un certificat, de sorte que le destinataire peut vérifier l'origine du document ainsi que son authenticité.

Signature de l'utilisateur*
L'option permet aux utilisateurs d'envoyer un fichier PDF ou XPS avec une signature utilisateur numérique unique obtenue à partir d'une autorité de certification. De cette façon, le destinataire est en mesure de vérifier l'utilisateur qui a signé le document.

APPLIQUER DES POLITIQUES AVEC L'INTÉGRATION D'ADOBE LIFECYCLE MANAGEMENT ES

Les utilisateurs peuvent sécuriser des fichiers PDF et appliquer des politiques persistantes et dynamiques pour contrôler l'accès et les droits d'utilisation, afin de protéger les données sensibles et les informations de grande valeur contre les divulgations involontaires ou malveillantes. Les politiques de sécurité sont gérées au niveau du serveur, de sorte que les droits peuvent être modifiés même après la distribution d'un fichier. La série imageRUNNER ADVANCE DX peut être configurée pour intégrer Adobe® ES.

*Optionnel. Pour obtenir des informations détaillées sur la disponibilité des fonctionnalités et des options dans la gamme d'impression de bureau, veuillez contacter votre représentant Canon.

SÉCURITÉ DES INFORMATIONS DE L'ENTREPRISE

Canon peut contribuer à la protection générale des informations dans votre société.

CONTRÔLE COMPLET POUR VOS BESOINS DE CAPTURE ET DE SORTIE DE BOUT EN BOUT

Grâce à notre logiciel de gestion de sortie modulaire, les entreprises bénéficient d'un partage sécurisé des périphériques réseau, ce qui leur permet d'imprimer leurs travaux en toute sécurité sur toute imprimante connectée au serveur de gestion de sortie. Les utilisateurs mobiles sont pris en charge par un service contrôlé de façon centralisée, où les utilisateurs internes ainsi que les utilisateurs invités ont un accès sécurisé à l'impression à partir d'appareils mobiles.
Pour les besoins de capture des entreprises, le module de numérisation permet la capture, la compression, la conversion et la distribution de documents à partir du périphérique multifonction vers un large éventail de destinations, y compris les systèmes Cloud. Vous pouvez également rediriger en toute sécurité les travaux d'impression vers l'imprimante la mieux adaptée pour optimiser le coût d'impression de chaque document. Notre solution améliore la sécurité des documents dans toute votre entreprise, combinée avec la comptabilisation de documents pour une visibilité complète de l'activité par utilisateur, périphérique et service.

GESTION DE PARC CENTRALISÉE

Notre logiciel de gestion de périphérique IW MC permet de mettre à jour et d'étendre les paramètres de périphérique, les politiques de sécurité, les mots de passe et les certificats, ainsi que les micrologiciels à votre parc de périphériques Canon sur le réseau. Votre équipe informatique gagne ainsi un temps précieux et la sécurité de votre infrastructure d'impression demeure actualisée.

AUDITS COMPLETS DE DOCUMENTS

Notre architecture de services de documents de bureau peut être améliorée grâce à des options à commander pour capturer un enregistrement complet (c'est-à-dire métadonnées des travaux et des numérisations) de tous les documents traités par le biais de périphériques imageRUNNER ADVANCE DX.

SERVICES DE GESTION D'IMPRESSION

Canon MPS intègre une technologie novatrice et des logiciels avec les services adéquats, afin de vous fournir l'expérience d'impression et de documents de votre choix sans tracas supplémentaire pour vos équipes informatiques. Grâce à la gestion proactive et à l'optimisation continue de votre infrastructure d'impression et des flux de travail de documents, nous pouvons vous aider à atteindre vos objectifs de sécurité tout en optimisant les coûts et en améliorant la productivité dans toute votre entreprise.

DÉVELOPPEMENT PERSONNALISÉ

Nous disposons d'une équipe de développeurs en interne qui peut proposer et élaborer une solution personnalisée correspondant à votre situation spécifique ou à vos besoins uniques.

L'APPROCHE DE LA SÉCURITÉ DE VOTRE ENTREPRISE EST-ELLE GLOBALE ?

- Votre politique de sécurité s'étend-elle également à votre parc de périphériques multifonctions ?
- Comment garantissez-vous la mise à jour de votre infrastructure d'impression et l'implémentation opportune et efficace des améliorations et des corrections de problèmes ?
- Vos invités peuvent-ils imprimer et numériser sans exposer votre réseau à des risques ?
- Vos politiques en matière de BYOD sont-elles sécurisées et peuvent-elles être prises en charge dans l'ensemble de votre parc d'impression ?
- Votre équipe informatique a-t-elle le temps d'examiner les problèmes de sécurité ?
- Obtenez-vous le juste équilibre entre la sécurisation et le confort de l'utilisateur ?

POURQUOI CANON ?

EXPERTISE

L'intégration logicielle et matérielle réduit les risques de violations de système.

PARTENARIAT

Nous aidons nos clients à être plus efficaces en **gérant de façon proactive les menaces de sécurité des données.**

SERVICE

La **même équipe de sécurité des informations** des clients gère notre propre sécurité informatique interne.

Nous prenons en compte toutes les menaces potentielles, aussi bien au sein du pare-feu de l'entreprise qu'au-delà.

INNOVATION

Nos produits et services **intègrent des options plus intelligentes** afin de réduire les risques les plus courants pour la sécurité des informations.

SC 2017 awards EUROPE

BLI PACESETTER MOBILE Print 2017-2018

Mention « Highly Commended » (mention d'honneur) dans la catégorie de la meilleure équipe de sécurité aux **SCA Awards Europe de 2017**, qui récompensent l'expertise en matière de cybersécurité.

Canon États-Unis a reçu deux **prix BLI PaceSetter Awards 2017** (Sécurité d'imagerie documentaire et Impression mobile).

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Canon France S.A.
17, quai du Président Paul Doumer
92414 Courbevoie Cedex
Tél. : 01 41 99 77 77
canon.fr

Canon Belgium NV/SA
Berkenlaan 3
1831 Diegem
Tel. 02-722 04 11
Fax 02-721 32 74
canon.be

Canon Luxembourg SA
Rue des Joncs 21
L-1818 Howald - Luxembourg
Tél: 48 47 96 218
Fax: 48 98 79 235
canon.lu

Canon (Suisse) SA
Richtistrasse 9
CH-8304 Wallisellen
Tel. +41 (0)22 567 58 58
canon.ch

French edition

Canon

McAfee PROTECTED