# Xerox et la sécurité de l'information

Vos données, votre entreprise :
Partenariat pour protéger
ce qui est le plus important

# Table des matières

# Vue d'ensemble

L'information est l'atout clé de chaque entreprise, et la sécurité est essentielle pour le bureau; pour les documents et pour tous les périphériques, y compris les imprimantes et les imprimantes multifonctions, connectés au réseau. Et au 21e siècle, le réseau est le centre de pratiquement toutes les activités commerciales.

Presque toutes les entreprises, et toutes les personnes qui s'y trouvent, sont connectées à Internet. Votre entreprise, et toutes les organisations avec lesquelles vous collaborez, fait partie d'un système global de réseaux et de serveurs informatiques interconnectés. Il existe d'innombrables utilisateurs effectuant simultanément des tâches, qui accèdent et partagent de l'informations, qui font des achats et de la vente de biens et de services et la communication par courrier électronique, messagerie instantanée, SkypeMC, Twitter et bien d'autres services.

La menace à la sécurité est très réelle et les enjeux augmentent à des vitesses exponentielles. Une violation de la sécurité des documents d'une entreprise peut entraîner l'acquisition ou l'utilisation non autorisée d'informations sensibles ou exclusives. Cela peut conduire à une divulgation préjudiciable de propriété intellectuelle et des secrets commerciaux volés ou compromis. Et pour de nombreuses entreprises, ces violations de sécurité peuvent se terminer par des amendes et des litiges coûteux, d'une valeur de centaines de milliers à des millions de dollars.

Les menaces de sécurité croissantes d'aujourd'hui sont sous diverses formes et dans des degrés de gravité divers. La prolifération explosive de dispositifs en réseau signifie un nombre toujours croissant de points d'entrée potentiellement vulnérables pour les intrus. Et la menace des pirates informatiques est constante avec des programmes fonctionnant 24 heures sur 24, 7 jours sur 7 qui cherchent et exploitent automatiquement les défauts de sécurité réseau.

Les menaces de sécurité varient des messages indésirables relativement inoffensifs aux menaces persistantes qui peuvent faire effondre des réseaux entiers.

Avec une activité Internet si constante, vous devez être sûr que l'information confidentielle de votre entreprise reste sécurisée. Mais les demandes changent et elles changent quotidiennement.

Les imprimantes et les imprimantes multifonctions ou les imprimantes multifonctions en réseau, qui peuvent imprimer, copier, numériser vers des destinations de réseau, envoyer des pièces jointes et gérer les transmissions de télécopie entrantes et sortantes sont particulièrement vulnérables.

Pour ceux qui sont en sécurité de l'information, il est essentiel pour la sécurité du réseau d'une entreprise de veiller à ce que les infractions de sécurité ne puissent pas se produire au moyen d'imprimantes et de multifonctions connectés au réseau, ni aux périphériques eux-mêmes. Après tout, les attaques peuvent se produire de façon inattendue :

- La ligne téléphonique reliée à un MFP pourrait être utilisée pour accéder au réseau.
- Le serveur Web utilisé pour gérer les MFP et les imprimantes peut être vulnérable aux attaques.
- Les données électroniques non protégées peuvent être consultées de manière inappropriée en reposant sur le disque dur ou en mouvement à partir du/vers le périphérique.
- Les messages malveillants peuvent être envoyés à partir d'un MFP sans piste d'audit.

Les imprimantes et les imprimantes multifonctions sont sophistiquées, plusieurs plateformes informatiques de sous-systèmes et des mesures de sécurité significatives doivent comprendre tous les éléments de la plateforme.

**Les imprimantes et les MFP d'aujourd'hui sont très différents des PC et des serveurs.**

- Les imprimantes et les MFP sont des périphériques partagés avec plusieurs utilisateurs et administrateurs.
- Les imprimantes et les multifonctions sont des périphériques intégrés :
  - Il peut y avoir un système d'exploitation réel dans le système.
  - Le système d'exploitation peut avoir une interface externe directe.
  - Le système d'exploitation peut être propriétaire.
  - Le système d'exploitation peut être Microsoft® Windows®.

# Vue d'ensemble

- Les imprimantes et les MFP ont les éléments suivants qui sont généralement associés à des noeuds informatiques plus avancés :
  - Piles de protocole réseau
  - Fonctions d'authentification et d'autorisation
  - Cryptage
  - Gestion d'appareils
  - Serveurs Web

**L'hétérogénéité des implémentations d'imprimantes et de MFP pose des défis.**

- Beaucoup plus diversifié que les PC traditionnels
- Un degré élevé de diversité concernant les systèmes d'exploitation sous-jacents parmi les différents fabricants et même dans les gammes de produits d'un seul fabricant

**Les commandes traditionnelles de PC et de serveurs ne sont pas optimisées pour les imprimantes et les MFP.**

- Approche antivirus
  - **Peut** ne pas être disponible pour le type de système d'exploitation utilisé dans l'imprimante et le MFP
  - En général, perte de la guerre contre les logiciels malveillants de toute façon
  - Complexité de la gestion des mises à jour des fichiers de données dans un environnement distribué
- Correction des imprimantes et MFP
  - Le contrôle de la version logicielle des imprimantes et des MFP est incompatible
  - La gestion de la configuration crée des frais généraux opérationnels
- Information de sécurité et gestion des événements (SIEM)
  - Les alertes et la sensibilisation des imprimantes et des MFP sont inégales
  - La remise en état des imprimantes et des MFP n'est pas normalisée

**C'est une situation très différente des imprimantes et copieurs d'hier.**

À peu près n'importe qui peut lancer des attaques contre un réseau et les actifs d'information d'une entreprise si l'accès physique et électronique de l'imprimante et du MFP n'est pas contrôlé et protégé de manière sécurisée. Ces attaques peuvent être aussi simples que quelqu'un qui récupère des documents laissés sur l'imprimante et le bac de réception du MFP aux vers malveillants tirant des documents sensibles hors du réseau.

Tout le système de l'imprimante et du MFP, ainsi que tout logiciel de gestion de périphériques sur le réseau, doit être évalué et certifié afin que la sécurité de l'information et de tous les travailleurs d'une entreprise soient certains que leurs documents et leur réseau sont sécurisés contre les prédateurs d'informations ou même des failles de sécurité internes.

À cet égard, les imprimantes et les MFP ne sont pas tous égaux. Par conséquent, une approche globale, basée sur la sécurité fondamentale, fonctionnelle, avancée et utilisable, est essentielle pour protéger les actifs d'information des entreprises d'aujourd'hui.

Heureusement, Xerox a les capacités de sécurité nécessaires. Au cours des 20 dernières années, Xerox a été un chef de file dans la prestation de solutions documentaires sécurisées à une variété d'industries à travers le monde. En fait, tous les produits et services Xerox® que nous offrons ont été conçus en toute sécurité et pour être intégrés de manière transparente aux cadres de sécurité existants. De plus, la sécurité est gérée tout au long du cycle de vie du produit à partir de l'analyse des besoins, de la conception, du développement, de la fabrication, du déploiement et de l'élimination, vous offrant ainsi à vous et à vos clients plus de protection et de tranquillité d'esprit.

À Xerox, nous aidons à protéger vos données à tous les points potentiels de vulnérabilité, donc vous n'avez pas à le faire. En restant concentré sur ce que nous faisons le mieux, vous pouvez rester concentré sur ce que vous faites le mieux.

### Objectifs de sécurité Xerox

Nous avons identifié cinq principaux objectifs de sécurité dans notre quête pour fournir des solutions sécurisées à chacun de nos clients :

**CONFIDENTIALITÉ**

- Aucune divulgation non autorisée de données pendant le traitement, la transmission ou le stockage

**INTÉGRITÉ**

- Aucune altération non autorisée des données
- Le système fonctionne comme prévu, sans manipulation non autorisée

**DISPONIBILITÉ**

- Le système fonctionne correctement
- Aucun déni de service pour les utilisateurs autorisés
- Protection contre l'utilisation non autorisée du système

**RESPONSABILITÉ**

- Les actions d'une entité peuvent être retracées directement à cette entité

**NON-RÉPUDIATION**

- L'assurance mutuelle que l'authenticité et l'intégrité des communications réseau sont maintenues

# Vulnérabilités de sécurité : risques et coûts de l'industrie.

Les entreprises de toutes tailles ont des informations sensibles utiles utiles aux cybercriminels qui doivent être protégées. Le paysage de la menace change constamment. Avec une augmentation d'Apportez vos propres appareils (BYOD), des portables pour les données de suivi de la santé, les systèmes de paiement mobile, le stockage infonuagique et l'Internet des objets, la menace est réelle et continue de croître.

Les cybercriminels concentrent de plus en plus leur attention sur les petites et moyennes entreprises (PME), car elles sont des cibles plus faciles que les grandes entreprises et parce que les PME n'ont généralement pas les ressources nécessaires pour se protéger contre les attaques. Les violations des données pour les grandes entreprises font des nouvelles, mais malheureusement, nous n'avons pas beaucoup d'informations sur les cyberattaques de PME.

Les enjeux pour les PME sont encore plus élevés que pour les grandes entreprises. L'information du client maintenue dans les PME est devenue un produit plus précieux et les coûts de ces infractions peuvent dévaster une PME. Selon une étude menée en 2015 par IBM et Ponemon Institute, le coût total moyen d'une violation de données pour les entreprises participantes a augmenté de 23 % sur deux ans à 3,79 millions de dollars.1 Le coût moyen payé pour chaque dossier perdu ou volé contenant des informations sensibles et confidentielles est passé de 145 $ en 2014 à 154 $ en 2015.[1]

Cela ne tient pas compte des éventuelles amendes, de la perte de réputation et de la perturbation des activités. La sécurité peut ne pas toujours être une priorité commerciale principale, mais garder l'information protégée est essentielle pour la santé de l'entreprise.

**Ce qui est en danger**


## Soins de santé

Les progrès dans les technologies de l'information, y compris l'utilisation d'ordinateurs de poche, ont créé la nécessité de partager des données médicales importantes et des informations sur les patients par voie électronique et c'est là que la sécurité devient une préoccupation majeure.

La loi Health Insurance Portability and Accountability Act de 1996 (HIPAA) a été mise en place par le gouvernement fédéral américain pour obliger toutes les organisations de soins de santé à appliquer des pratiques uniformes de gestion des données afin de protéger l'information des patients et la vie privée du patient en tout temps. Sous HIPAA, une piste d'audit est requise pour suivre qui a vu les données, lorsqu'elles l'ont vu et si elles avaient l'autorisation appropriée de le faire.

La loi Health Information Technology for Economic and Clinical Health (HITECH) a considérablement élargi les efforts du gouvernement américain pour établir un système national de tenue de dossiers électroniques pour l'industrie de la santé. HITECH a été promulguée dans le cadre de la loi American Recovery and Reinvestment de 2009 afin de promouvoir l'adoption et l'utilisation significative des technologies de l'information sur la santé.

Le non-respect de l'HIPAA peut entraîner des sanctions civiles et pénales, même si aucune violation ne se produit.

## Gouvernement

Aujourd'hui, les gouvernements locaux, étatiques et fédéraux ont mis l'accent sur la simplification des processus et l'amélioration de la collaboration entre organismes afin de fournir de meilleurs résultats aux citoyens qu'ils servent. Pour ce faire, ils utilisent diverses initiatives pour tirer parti des dernières technologies, tout en mettant des règles strictes en place pour s'assurer que l'information partagée est sécurisée. Un exemple est la loi sur la violation des données de l'État du Massachusetts, qui est l'une des plus agressives du pays. Les systèmes, les logiciels et les services de Xerox® sont conformes à ces directives strictes, ainsi qu'à d'autres.

En 2014, le Department of Defence a adopté les normes 800-53 de la National Institute of Standards and Technology (NIST), qui est une publication qui recommande des contrôles de sécurité pour les systèmes et organisations fédéraux d'information et les contrôles de sécurité des documents pour tous les systèmes d'information fédéraux, à l'exception de ceux conçus pour la sécurité nationale.

1. Étude des coûts de la violation des données 2015 : analyse globale, IBM et Ponemon Institute, mai 2015.

# Vulnérabilités de sécurité : risques et coûts de l'industrie.

En outre, le Department of Defence a adopté des mesures de sécurité supplémentaires avec l'utilisation de cartes d'accès commun (CAC) et de leurs homologues du gouvernement civil, cartes PIV (Personal Identity Verification). De telles cartes nécessitent une infrastructure PKI pour assurer un environnement d'authentification et de communication sécurisé. De plus, la plupart des organismes du gouvernement fédéral ont adopté la norme FIPS 140-2 pour certifier les modules de cryptage utilisés dans les produits d'imprimante et de MFP. Et enfin, de nombreux clients du gouvernement fédéral exigent que les produits soient certifiés conformes à la norme Critères communs.

## Services financiers

Le dépôt direct, la banque en ligne, les cartes de débit et autres avancées dans les technologies de l'information révolutionnent l'industrie des services financiers. Bien que plus pratique pour les clients et les entreprises, cette utilisation intensive de la technologie a ses propres problèmes de sécurité.

Un échange sécurisé d'informations sur les cartes de crédit est essentiel et la conformité aux normes de sécurité des données (DSS) de l'industrie de la carte de paiement (PCI) permet d'atténuer les vulnérabilités et de protéger les données des titulaires de carte. PCI DSS est une norme de sécurité d'information exclusive pour les entreprises qui gèrent des cartes de crédit, y compris Visa®, Mastercard®, American Express®, Discover® et JCB.

La loi Gramm-Leach-Bliley Financial Services Modernisation de 1999 (GLBA) a été instituée pour s'assurer que les institutions financières qui collectent ou reçoivent des données privées ont un plan de sécurité en place pour les protéger. Pour atteindre la conformité, les entreprises doivent effectuer une analyse des risques sur leurs processus actuels et implémenter des pare-feux, restreindre l'accès des utilisateurs, surveiller l'impression et plus encore.

La loi Dodd-Frank Wall Street Reform et Consumer Protection de 2010 augmente encore le besoin de recueil et de déclaration précis des données financières. Grâce au Bureau de la recherche financière et aux organismes membres, les données seront recueillies et analysées afin d'identifier et de surveiller les risques émergents pour l'économie et de rendre cette information publique dans les rapports périodiques et les témoignages annuels au Congrès.

## Éducation

Avec les établissements d'enseignement actuels, y compris le primaire et le secondaire, les collèges et les universités, les transcriptions de demandes, les demandes d'aide financière et même les notes de classe sont disponibles en ligne. Parce que certaines écoles ont leurs propres centres médicaux, elles doivent également stocker et partager des informations médicales par voie électronique. Cet environnement interactif améliore l'expérience des étudiants et la productivité du personnel, mais il rend également les écoles sensibles aux menaces de sécurité.

Parce que ces institutions gèrent une variété d'informations, de nombreuses réglementations fédérales et fédérales s'appliquent, y compris la loi Computer Fraud and Abuse, la loi Patriot des États-Unis, HIPAA et GLBA. Cependant, la réglementation la plus applicable à l'industrie de l'éducation est la loi Family Education Rights and Privacy (FERPA). Cette loi interdit la divulgation d'informations sur l'éducation personnellement identifiables sans l'autorisation écrite de l'élève ou du tuteur de l'élève.

Avec tant de mesures réglementaires et de conformité exigeant une réponse, Xerox a examiné les exigences du gouvernement fédéral, entre autres, comme lignes directrices. En développant des solutions qui s'efforcent de respecter les normes de sécurité les plus strictes, nous pouvons offrir des solutions hautement sécurisées à tous nos clients, quel que soit le secteur d'activité.

# Vue d'ensemble de la sécurité

À Xerox, notre philosophie « Sécurité » permet de développer des produits, des services et des technologies imprégnés de sécurité à tous les niveaux.

La sécurité est avant à l'avant-plan lors de la conception de nos « MFP intelligent ». En tant que chef de file dans le développement de la technologie numérique, Xerox a démontré son engagement à maintenir les informations numériques en toute sécurité en identifiant les vulnérabilités potentielles et en les abordant de manière proactive pour limiter les risques en les abordant de manière proactive pour limiter les risques. Les clients ont répondu en se tournant vers Xerox en tant que fournisseur de solutions sécurisées qui offrent une multitude de fonctionnalités de sécurité standard et optionnelles.

## Notre stratégie de sécurité

Le développement des produits Xerox® est guidé par un processus de cycle de vie de développement sécurisé, qui prend en compte les directives du Open Web Application Security Project (OWASP), Software Assurance Maturity Model (SAMM) et du SANS Institute. Cela implique de définir les exigences de sécurité, d'évaluer les risques, d'analyser les vulnérabilités et les tests de pénétration, ainsi que les informations obtenues auprès de l'OWASP et du SANS Institute. Cette stratégie repose sur trois piliers :

### Fonctionnalités de sécurité à la fine pointe de la technologie

Les imprimantes et les périphériques multifonctions sont sophistiqués, plusieurs plateformes informatiques de sous-systèmes et Xerox offre la plus large gamme de fonctionnalités de sécurité sur le marché, y compris le cryptage, l'authentification, l'autorisation par utilisateur et l'audit.

### Certification

ISO 15408 Critères communs pour l'évaluation de la sécurité des technologies de l'information est la seule norme internationalement reconnue pour la certification de sécurité. Xerox a été le premier fabricant à rechercher et à obtenir des certifications pour les périphériques MFP « complets ». Parce que chaque élément de la plateforme du multifonction est un point d'entrée potentiel, une certification de sécurité significative doit comprendre tous les éléments, y compris les systèmes d'exploitation, l'interface réseau, les lecteurs de disque, le serveur Web, les interpréteurs PDL, l'interface utilisateur du MFP, les ports matériels locaux et le système de télécopie.

### Entretien

À Xerox, le maintien de la sécurité de notre imprimante et des périphériques multifonctions tout au long de leur durée de vie nécessite une diligence constante pour assurer une protection continue contre les exploitations nouvellement découvertes. Ceci est accompli :

- En s'assurant que les mises à jour logicielles sont publiées de manière continue
- Par notification de nouveaux bulletins de sécurité avec flux RSS
- En répondant aux vulnérabilités identifiées
- En fournissant des instructions d'installation et d'utilisation sécurisées
- En fournissant des informations sur les Critères communs
- En rendant les correctifs disponibles à www.xerox.com/security

Le modèle de sécurité Xerox, de concert avec le cycle de vie de développement sécurisé, est un engagement que toutes les fonctionnalités et les fonctions du système, pas seulement un ou deux, sont sécurisées.

## Une approche complète pour la sécurité de l'imprimante et du MFP

Depuis longtemps, Xerox a reconnu et accepté ce changement de technologie et les besoins changeants du milieu de travail. Nous offrons un ensemble complet de fonctionnalités de sécurité pour garder vos imprimantes/MFP et vos données en toute sécurité. Xerox sécurise chaque partie de la chaîne de données, y compris l'impression, la copie, la numérisation, la télécopie, les téléchargements de fichiers et les logiciels système. Il existe quatre aspects clés de notre approche multicouches.

### 1. Prévention des intrusions

Votre première et la plus évidente vulnérabilité est l'interface utilisateur, qui a un accès physique à votre imprimante et ses fonctionnalités. Utilisateur L'authentification est la base de l'accès aux imprimantes et aux périphériques multifonctions de Xerox® pour les utilisateurs libre-service autorisés et les utilisateurs du réseau. Une fois authentifié, l'utilisateur peut interagir avec l'appareil ou accéder aux données du client, qui est soumis à des restrictions en fonction du rôle de l'utilisateur. Les imprimantes et les MFP de Xerox® utilisent une variété de technologies pour garantir un accès autorisé aux fonctions des périphériques par les utilisateurs et autres périphériques réseau. Ensuite, nous abordons des points d'intrusion moins évidents, ce qui est envoyé à l'imprimante et comment la technologie ConnectKey® de Xerox® intercepte les attaques de fichiers corrompus et de logiciels malveillants. Notre logiciel système, y compris les DLM et les Weblets, est signé numériquement; toute tentative d'installation de versions infectées et non signées entraînera le rejet automatique du fichier. Les fichiers d'impression seront également supprimés si une partie n'est pas reconnue comme légitime.

#### AUTHENTIFICATION RÉSEAU

L'authentification réseau permet aux utilisateurs de s'authentifier sur le périphérique en validant les noms d'utilisateur et les mots de passe avant l'utilisation. L'authentification réseau autorise un individu à accéder à l'un ou à une combinaison des services suivants : Impression, copie, télécopie, serveur de télécopie, réimpression de travaux enregistrés, courrier électronique, télécopie Internet et le serveur de numérisation de flux de travail. En outre, les utilisateurs peuvent être autorisés à accéder à l'un ou à n'importe quelle combinaison des chemins de l'appareil suivants : Services, État travail ou État de l'appareil.

**1. Prévention des intrusions**

Empêcher l'accès général aux périphériques restreints avec accès utilisateur et pare-feu interne sur l'imprimante.

**2. Détection de périphériques**

Soyez alerté au démarrage ou à la demande si des modifications nuisibles à votre imprimante ont été détectées.

**3. Protection des données et des documents**

Gardez les informations personnelles et confidentielles en toute sécurité avec un disque dur crypté (AES 256 bits, FIPS validé pour de nombreux produits) et l'écrasement d'image.

**4. Partenariats externes**

Protégez vos données et vos périphériques contre les intrusions malveillantes grâce à la technologie de liste blanche McAfee, l'intégration du moteur des services d'identité (ISE) de Cisco®, aux organismes de certification et de test de conformité.

#### MICROSOFT® ACTIVE DIRECTORY® SERVICES

La fonction Microsoft Active Directory Services (ADS) permet à l'appareil d'authentifier les comptes d'utilisateurs sur une base de données de compte d'utilisateur centralisée, au lieu d'utiliser exclusivement la base de données de compte utilisateur qui est gérée localement sur le périphérique.

#### AUTHENTIFICATION LDAP

L'authentification LDAP (BIND) est prise en charge pour l'authentification avec les serveurs LDAP pour la recherche d'informations et l'accès. Lorsqu'un client LDAP se connecte au serveur, l'état d'authentification par défaut de la session est défini sur anonyme. L'opération BIND établit l'état d'authentification pour une session.

#### AUTHENTIFICATION SMTP

Cette fonctionnalité valide le compte de messagerie de l'utilisateur et empêche les utilisateurs non autorisés d'envoyer des courriels à partir du périphérique. Les administrateurs système peuvent activer TLS pour toutes les opérations d'envoi et de réception SMTP.

# Vue d'ensemble de la sécurité

### AUTHENTIFICATION POP3 AVANT SMTP

En tant que couche de sécurité supplémentaire, les MFP de Xerox® prennent en charge la capacité des administrateurs système d'activer ou de désactiver l'authentification POP3 avant la fonctionnalité SMTP. L'authentification POP3 avant SMTP oblige une connexion réussie à un serveur POP3 avant d'envoyer un courrier par le biais de SMTP.

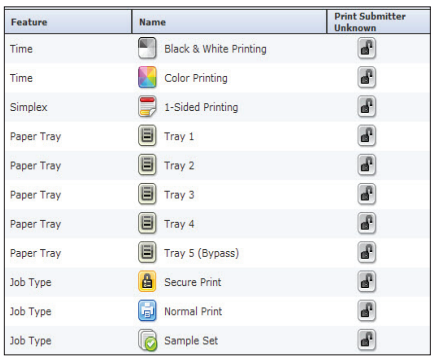
### CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES (RBAC)

La fonctionnalité RBAC garantit que les utilisateurs authentifiés sont affectés à un rôle de l'utilisateur non connecté ou de l'utilisateur enregistré, de l'administrateur système ou de l'administrateur de comptabilisation. Chaque rôle a des privilèges associés avec des niveaux d'accès appropriés aux fonctionnalités, aux travaux et aux attributs de la file d'impression. Il permet aux administrateurs de choisir précisément les fonctions autorisées pour un rôle donné. Une fois qu'un utilisateur se connecte au périphérique avec le nom et le mot de passe de l'utilisateur, l'appareil peut déterminer quels rôles sont attribués à cet utilisateur particulier. Les restrictions sont appliquées en fonction des rôles assignés. Si une fonction entière est restreinte, elle peut apparaître bloquée à l'utilisateur après l'authentification ou ne pas apparaître du tout.

| Utilisateur non connecté/utilisateur connecté | Administrateur système | Administrateur comptable |
|---|---|---|

### PERMISSIONS D'IMPRESSION UTILISATEUR

Les permissions utilisateur Xerox permettent de restreindre l'accès aux fonctionnalités d'impression par utilisateur, par groupe, par heure et par application. Les utilisateurs et les groupes peuvent être configurés avec différents niveaux d'accès aux fonctions d'impression. Par exemple, des limites peuvent être définies autorisant les travaux d'impression couleur uniquement pendant certaines heures de la journée; les présentations Microsoft® PowerPoint® s'impriment automatiquement en mode recto verso ou les courriels Microsoft Outlook® s'impriment toujours en noir et blanc.




Définissez les permissions utilisateur pour la couleur et d'autres restrictions d'impression avec des interfaces graphiques intuitives.

### AUTHENTIFICATION PAR CARTE À PUCE

Aussi connu sous le nom de carte de proximité ou carte à puce sans contact L'authentification par carte à puce protège votre imprimante et votre MFP contre tout accès non autorisé. Les appareils de Xerox® prennent en charge plusieurs cartes intelligentes (CAC/PIV, .NET, Rijkspas et autres cartes à puce et de proximité) soit environ 30 différents types de lecteurs de cartes et 65 cartes de proximité différentes. Avec l'authentification par carte à puce, les utilisateurs peuvent être authentifiés à l'aide d'un système à deux facteurs Système d'identification, la possession de la carte et un numéro d'identification personnel entré à l'interface utilisateur de l'appareil, pour accéder aux fonctionnalités de démarrage sur l'appareil et sur le réseau.

La carte d'accès commun/vérification de l'identité personnelle (CAC/PIV) est une carte à puce du Department of Defence des États-Unis émise délivrée en tant qu'identification standard pour le personnel militaire actif, le personnel de la réserve, les employés civils, les autres employés non gouvernementaux et le personnel des entrepreneurs admissibles. La carte CAC/PIV peut être utilisée pour l'identification générale, l'accès contrôlé au bâtiment et l'authentification d'ordinateurs personnels, en plus des imprimantes/MFP et des réseaux qui les connectent.

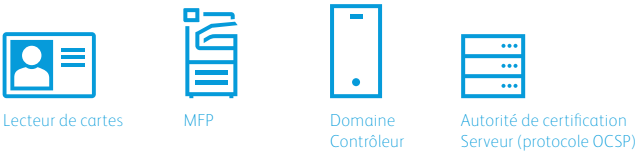
# Vue d'ensemble de la sécurité

La CAC/PIV 144k est une version de la carte à puce. Les utilisateurs peuvent être authentifiés à l'aide d'une identification à deux facteurs pour accéder aux services libre-service du périphérique.

La CAC/PIV 144k offre les avantages suivants :

- Numérisation vers courriel avec chiffrement S/MIME à soi-même ou à tout autre destinataire dans le carnet d'adresses global local ou LDAP du MFP
- Signature numérique à l'aide du certificat de signature par courrier électronique de la carte de l'utilisateur
- Remplissage automatique du champ « À : » lors de l'utilisation de la fonction Numérisation vers courriel du MFP
- Clé de certificat jusqu'à 2 048 bits
- Limiter les transmissions sortantes aux destinataires avec des certificats valides
- Recevoir des rapports de confirmation par courrier électronique et conserver des journaux d'audit
- Connexion unique pour la Numérisation vers un ordinateur et LDAP

**Diagramme de configuration pour carte d'accès commune (CAC)/ vérification de l'identité personnelle (PIV)**

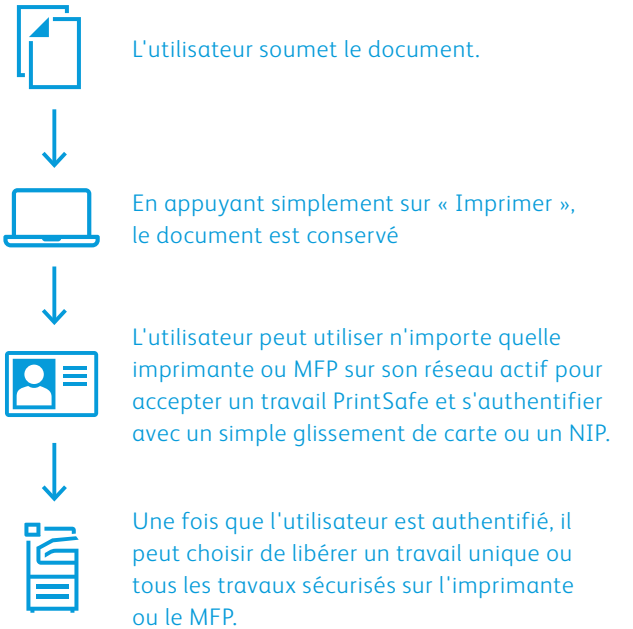



1. Une carte est insérée dans le lecteur et l'utilisateur est invité à entrer un NIP dans le MFP.
2. Le MFP vérifie le serveur OCSP pour confirmer que le certificat de la carte n'a pas expiré puis vérifie la « chaîne de confiance » avec une autorité de certification connue.
3. Le MFP lance un dialogue de défi/réponse crypté entre le contrôleur de domaine et la carte d'accès commun. En cas de succès, le contrôleur de domaine émet un ticket initial (TGT) et l'autorisation est terminée.
4. L'autorisation déverrouille les fonctions libre-service du MFP :
   - Numérisation vers courriel
   - Copie
   - Télécopie
   - Services personnalisés
   - Numérisation de flux de travail

**LOGICIEL PRINTSAFE DE XEROX®**

Le logiciel PrintSafe de Xerox® offre une authentification d'impression sécurisée pour les données imprimées sur la plupart des imprimantes et des MFP, y compris les appareils Xerox® et les périphériques d'autres fournisseurs. Ce logiciel est ouvert pour fonctionner avec une variété de lecteurs et de cartes sécurisés standard de l'industrie.s.

**Flux de travail d'impression sécurisés, pratiques et flexibles**




Le logiciel PrintSafe de Xerox® ne se limite pas aux appareils Xerox®. Toute imprimante ou MFP* enregistré avec le logiciel PrintSafe de Xerox® peut générer des travaux PrintSafe.

Des flux de travail flexibles permettent à l'utilisateur de charger un logiciel sur leur PC client pour une impression directe ou sur un serveur d'impression existant, qui peut facilement être configuré pour le logiciel PrintSafe de Xerox®.

*Les périphériques non Xerox® nécessitent un accessoire réseau. Consultez votre représentant commercial Xerox pour plus de détails sur les marques/modèles pris en charge.

**INTERFACE UTILISATEUR DE L'APPAREIL ET ACCÈS À L'INTERFACE UTILISATEUR À DISTANCE**

Les administrateurs système peuvent bloquer l'accès aux écrans de configuration du périphérique pour les utilisateurs non autorisés à partir du panneau de commandes et de l'utilitaire de l'interface utilisateur à distance afin de protéger ses informations de configuration.

## 2. Détection de périphériques

Dans le cas improbable où vos données et votre défense réseau sont contournés, La technologie ConnectKey® de Xerox® exécutera un test complet de vérification du micrologiciel, soit au démarrage*, soit activé par des utilisateurs autorisés. Cela vous informe si des modifications nuisibles à votre imprimante ou MFP ont été détectées. Si des anomalies sont détectées, l'appareil affiche un message indiquant à l'utilisateur de recharger le micrologiciel. Nos solutions intégrées les plus avancées utilisent la technologie de liste blanche** de McAfee® qui surveille constamment et empêche automatiquement tout programme malveillant de fonctionner.

En partenariat avec Cisco, Xerox a mis en œuvre le profilage de l'appareil dans le moteur de services d'identité de Cisco® (MSI). L'intégration avec le moteur de services d'identité de Cisco (MSI) détecte automatiquement les périphériques Xerox sur le réseau et les classe en tant qu'imprimantes pour la mise en œuvre de la politique de sécurité et la conformité.

Pour plus d'informations, reportez-vous aux livres blancs suivants :

Livre blanc Liste blanche McAfee (anglais seulement) :
**http://www.office.xerox.com/latest/SECWP-03.PDF**

Livre blanc MSI de Cisco (anglais seulement) :
**http://www.office.xerox.com/latest/SECWP-04.PDF**

*Imprimantes et imprimantes multifonctions VersaLink® de Xerox®.
**Imprimantes multifonctions AltaLink® et i-Series de Xerox®.

## 3. Protection des données et des documents

### Protection des documents

Même si toutes les mesures de sécurité de réseau nécessaires sont en place pour protéger efficacement les données essentielles au fur et à mesure qu'elles se déplacent entre les ordinateurs des utilisateurs et les appareils d'impression bureautique, les technologies de sécurité doivent également s'assurer que vos documents imprimés sensibles sont reçus et visionnés uniquement par leurs destinataires. Xerox utilise les dernières technologies pour sauvegarder votre sortie, que ce soit en imprimant des copies papier ou en distribuant des documents électroniques.

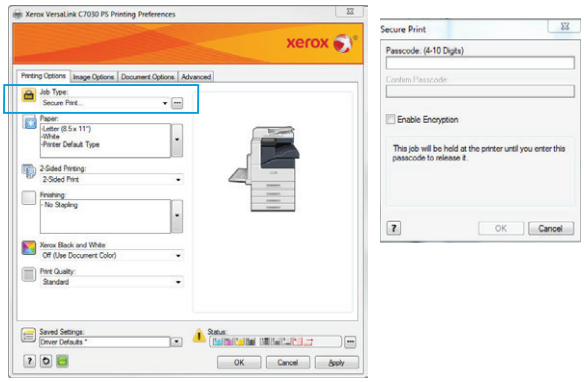
#### CRYPTAGE DES DONNÉES DE NUMÉRISATION

Les utilisateurs de notre technologie ConnectKey® de Xerox® activées sur les MFP intelligents i-Series, VersaLink® et AltaLink® ont également la possibilité de crypter des fichiers PDF avec un mot de passe lors de l'utilisation du service Numérisation vers courriel.

- Protection hors du pare-feu
  - Sécurisation des données dans un environnement non sécurisé
  - Utilisation de protocoles standard de l'industrie tels que TLS et PDF sécurisé

#### CRYPTAGE DU FLUX D'IMPRESSION

Le pilote Global Print® de Xerox® et certains pilotes de produits prennent en charge le cryptage des documents lors de l'envoi de travaux d'impression sécurisés sur les périphériques compatibles avec la technologie ConnectKey. Les imprimantes multifonctions AltaLink et i-Series de Xerox® prennent également en charge le cryptage des documents pour les travaux d'impression réguliers. Aucun matériel supplémentaire n'est nécessaire pour le cryptage par le pilote d'imprimante.




#### IMPRESSION SÉCURISÉE

Les travaux d'impression sensibles sont conservés à l'imprimante ou au MFP jusqu'à ce que le propriétaire des documents les libère en entrant leur NIP unique par le biais de l'interface utilisateur du périphérique. Cela garantit que le destinataire prévu d'un document est physiquement présent lors de l'impression d'informations sensibles et peut immédiatement supprimer la sortie de l'imprimante ou du MFP avant de l'exposer à d'autres utilisateurs du périphérique.


L'impression sécurisée basée sur la technologie de carte d'accès commun (CAC)/vérification de l'identité personnelle (PIV) joint le certificat d'identité de l'expéditeur d'impression au travail d'impression. Sur l'appareil, l'utilisateur doit s'authentifier avec la carte CAC/PIV de l'utilisateur avant que le travail ne soit relâché.

#### PDF CHIFFRÉ/PDF PROTÉGÉ PAR MOT DE PASSE

Lors de la numérisation d'un document papier pour la distribution électronique au moyen de la fonction Numériser vers courriel, les MFP de Xerox® peuvent créer des fichiers PDF cryptés AES 128 bits ou 256 bits, qui sont transmis en toute sécurité sur le réseau et peuvent être ouverts, imprimés ou modifiés uniquement par ceux qui possèdent le bon mot de passe.

#### TRANSFERT DE TÉLÉCOPIE VERS LE COURRIEL ET LE RÉSEAU

Les multifonctions de Xerox® avec capacité de transfert de télécopie peuvent acheminer les télécopies entrantes vers les boîtes de réception de courrier électronique de destinataires spécifiques et (ou) vers un référentiel réseau sécurisé, qui ne peuvent être accessibles que par les utilisateurs autorisés.

#### CONFIRMATION D'ENVOI DE TÉLÉCOPIE

Un expéditeur de télécopie reçoit une confirmation automatisée que la télécopie de l'expéditeur a été reçue avec succès par le destinataire prévu.

# Vue d'ensemble de la sécurité

### SIGNATURES NUMÉRIQUES

Une signature numérique est un schéma mathématique pour démontrer l'authenticité d'un message ou d'un document numérique. Une signature numérique est utilisée pour protéger le micrologiciel de l'appareil contre les modifications non détectées et pour fournir une authentification d'origine de données. Avec les cartes à puce, les courriels peuvent être signés numériquement avec le certificat de l'expéditeur. Une signature numérique valide confère au destinataire la confiance que le message a été créé par un expéditeur connu et qu'il n'a pas été modifié en transit.

### FILIGRANES SÉCURISÉS

Certaines imprimantes et certains MFP de Xerox® disposent d'une fonction Filigrane sécurisé qui permet d'éviter l'impression de copies originales avec des informations sensibles. Si un document avec un filigrane sécurisé est copié, l'image du filigrane devient visible, en précisant que le document contient des informations sensibles et a été dupliqué illégalement.

### TAMPON UTILISATEUR/HEURE/DATE

Grâce aux pilotes Xerox®, un tampon utilisateur/heure/date peut être appliqué à tout document imprimé par un périphérique réseau. Cela fournit une piste de vérification de qui a imprimé quoi et à quelle heure.

### FILTRAGE D'ADRESSE IP

Le filtrage du protocole Internet (IP) permet aux administrateurs système de créer des règles pour accepter ou rejeter des informations provenant de l'appareil MFP en fonction d'adresses IP spécifiques ou d'une plage d'adresses. Cela permet à l'administrateur système de contrôler qui peut et ne peut pas accéder au périphérique.


**Adresses IP enregistrées :**
disponible




**Adresses IP non enregistrées :**
Indisponible

### SSL (SECURE SOCKET LAYER)/TLS (TRANSPORT LAYER SECURITY)

De nombreuses entreprises sont tenues de se conformer aux politiques de sécurité qui exigent que toutes les transactions entre le client et l'imprimante ou MFP soient sécurisées au moyen des transactions Web sécurisées, des transferts de fichiers sécurisés et des courriels sécurisés. Les données transmises sur le réseau sans chiffrement peuvent être lues par quiconque renifle le réseau. Xerox atténue ce problème avec Secure Sockets Layer/Transport Layer Security pour des transmissions de données sur certains protocoles tels que HTTP et IPP.

### CRYPTAGE IPSEC

IPsec (Internet Protocol Security) sécurise toute communication sur la couche IP et est principalement utilisé pour chiffrer les publications imprimées sur le périphérique. Il crypte tout le trafic entre le point A et le point B de telle sorte que seuls les utilisateurs fiables peuvent envoyer et recevoir les informations, les données ne sont pas modifiées lors de leur transmission et seuls les utilisateurs autorisés peuvent recevoir et lire les informations.

IPsec est conçu pour offrir les services de sécurité suivants :

- Cryptage du trafic (empêchant les parties non intentionnelles de lire des communications privées)
- Validation d'intégrité (assurant que le trafic n'a pas été modifié sur son chemin)
- Authentification par les pairs (en veillant à ce que le trafic provienne d'une partie de confiance)
- Anti-relecture (protection contre la lecture de la session sécurisée)

### ACTIVATION/DÉSACTIVATION DES PORTS RÉSEAU

Avec la fonction d'activation/désactivation des ports réseau, les ports et les services inutiles peuvent être désactivés pour empêcher un accès non autorisé ou malveillant. Sur les petits appareils de bureau, ces options peuvent être réglées par le biais de leur panneau de commandes ou de leur logiciel de configuration PC. Sur les MFP plus gros, des outils sont fournis pour définir les niveaux de sécurité et désactiver les ports et les services spécifiques.

# Vue d'ensemble de la sécurité

### CERTIFICATS NUMÉRIQUES

Les certificats numériques sont des documents électroniques qui utilisent une signature numérique pour lier une clé publique avec des informations d'identité telles que le nom d'une personne ou d'une entreprise, leur adresse, etc. Le certificat peut être utilisé pour vérifier qu'une clé publique appartient à un individu.

Les MFP peuvent ajouter des signatures numériques qui vérifient la source et l'authenticité d'un document PDF. Lorsque les destinataires ouvrent un fichier PDF qui a été enregistré avec une signature numérique, ils peuvent afficher les propriétés du document pour examiner le contenu de la signature, y compris l'autorité de certification, le nom du système du produit, le numéro de série et le tampon date/heure de création. Si la signature est une signature d'appareil, elle contiendra également le nom du périphérique qui a créé le document, tandis qu'une signature d'utilisateur vérifie l'identité de l'utilisateur authentifié qui a envoyé ou enregistré le document.

Les MFP de Xerox® peuvent être chargés avec un certificat signé par une autorité de certification telle que VeriSign ou votre administrateur système peut créer un certificat auto-signé sur le périphérique lui-même. En configurant un certificat sur votre appareil, vous pouvez activer le cryptage pour des types de flux de travaux spécifiques.

### SNMP V3

Le protocole de gestion de réseau simple (SNMP) est un protocole standard Internet pour la gestion des périphériques sur les réseaux IP, ce qui permet une plus grande sécurité en protégeant les données contre la falsification, en s'assurant que l'accès est limité aux utilisateurs autorisés par l'authentification et le cryptage des données envoyées sur un réseau.

Les périphériques qui prennent généralement en charge SNMP comprennent les routeurs, les commutateurs, les serveurs, les postes de travail, les imprimantes, les modems en montage en baie et plus encore. Il est utilisé principalement dans les systèmes de gestion de réseau pour surveiller les périphériques connectés au réseau pour des conditions qui justifient une attention administrative. SNMP est un composant de Internet Protocol Suite tel que défini par Internet Engineering Task Force (IETF). Le protocole SNMPv3 fournit des fonctions de sécurité considérablement améliorées, y compris le cryptage et l'authentification des messages.

### CHAÎNES DE NOM DE COMMUNAUTÉ SNMP

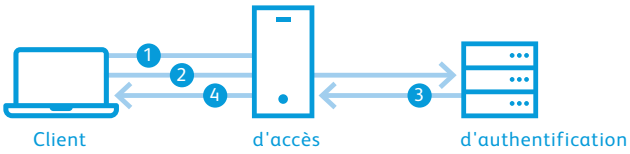
Les données types de base d'informations de gestion (MIB) en lecture seule utilisent la chaîne « public » et les chaînes de communauté de lecture-écriture définies sur « privé ». En utilisant les chaînes de noms de communauté de lecture-écriture, une application peut modifier le paramètre de configuration du périphérique en utilisant les variables MIB. Les chaînes de noms de communauté de lecture-écriture sur les appareils Xerox® peuvent être modifiées par l'administrateur système pour augmenter la sécurité lors de la gestion des MFP à l'aide de SNMP.

### AUTHENTIFICATION 802.1X

IEEE 802.1X est une norme IEEE pour le contrôle d'accès au réseau (PNAC). Elle fait partie du groupe de protocoles réseau IEEE 802.1. Elle fournit un mécanisme d'authentification aux périphériques souhaitant s'attacher à un réseau local (LAN) ou à un réseau local sans fil (WLAN). La fonctionnalité IEEE 802.1X est prise en charge par de nombreux commutateurs Ethernet et peut empêcher les systèmes invités, déloyaux ou non gérés qui ne peuvent pas effectuer une authentification réussie de la connexion à votre réseau.

**Comment ça fonctionne : Authentification 802.1X**

L'authentification 802.1X pour les réseaux locaux (LAN) sans fil fournit une authentification centralisée basée sur le serveur des utilisateurs finaux.




1. Un client envoie un message de « démarrage » à un point d'accès qui qui demande l'identité du client.
2. Le client répond avec un paquet réponse contenant une identité et le point d'accès renvoie le paquet vers un serveur d'authentification.
3. Le serveur d'authentification envoie un paquet « accepter » au point d'accès.
4. Le point d'accès place le port client dans un état autorisé et le trafic est autorisé à continuer.

# Vue d'ensemble de la sécurité

Le protocole 802.1X est devenu plus répandu avec la popularité accrue des réseaux sans fil. De nombreuses entreprises verrouillent l'accès au port à leurs réseaux internes en utilisant ce protocole. Cela empêche toute information de passer sur le réseau jusqu'à ce que l'appareil soit authentifié. Du point de vue de la gestion des risques, cela permet à la fois aux appareils sans fil et filaires de prouver leur identité avant que des informations ne soient transmises au réseau. Si un accès non autorisé est tenté, le port est verrouillé jusqu'à ce qu'il soit débloqué par l'administrateur système.

Le protocole d'authentification extensible (EAP) est un cadre d'authentification qui exécute ses fonctions dans le cadre de l'authentification 802.1X. Les types EAP actuellement pris en charge par les MFP de Xerox® sont :

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (produits AltaLink®et i-Series)

**PARE-FEU**

Un pare-feu fait partie d'un système informatique ou d'un réseau conçu pour bloquer l'appareil contre les menaces externes et l'accès non autorisé tout en autorisant les communications autorisées. Le dispositif peut être configuré pour autoriser ou refuser des transmissions réseau en fonction d'un ensemble de règles et d'autres critères. Les administrateurs réseau peuvent restreindre l'accès aux segments de réseau, aux services et aux ports des périphériques pour sécuriser les périphériques.

**SÉPARATION TÉLÉCOPIEUR ET RÉSEAU**

La séparation de l'interface du télécopieur du contrôleur de réseau élimine le risque de sécurité de piratage dans un réseau de bureau au moyen de la ligne du télécopieur.

Le MFP ne fournit pas une fonction pour accéder au réseau au moyen de la ligne téléphonique du télécopieur. Le protocole de télécopieur de classe 1 utilisé sur le MFP répond uniquement aux commandes de télécopie qui permettent l'échange de données de télécopie. Les données transmises par le PC client ne peuvent être que des données d'image compressées avec des informations de destination. Toutes les données autres que les informations d'image (comme un virus, un code de sécurité ou un code de contrôle qui accède directement au réseau) sont abandonnées à ce stade et le MFP met immédiatement fin à l'appel. Ainsi, il n'existe aucun mécanisme permettant d'accéder au sous-Çsystème réseau au moyen de la ligne du télécopieur.

## Protection des données

La technologie a transformé la façon dont les employés mènent leurs activités. Aujourd'hui, les documents prennent forme non seulement dans les formes imprimées traditionnelles, y compris les notes manuscrites et les brouillons des communications papier, mais aussi sous forme électronique sur les ordinateurs de bureau et dans les courriels. Parce que les employés créent, stockent, partagent et distribuent ces documents électroniques différemment des documents papier traditionnels, ces informations peuvent faire l'objet de nouveaux types de risques. Pour rester compétitif, une entreprise doit s'attaquer à ces menaces en sécurisant les documents et les systèmes de gestion de documents qui contiennent un atout le plus précieux de l'entreprise, la connaissance.

Les systèmes de gestion de l'information et du document font face à un large éventail de menaces de sécurité. Ces menaces incluent des actes d'espionnage intentionnels, comme le piratage informatique, le vol, la fraude et le sabotage, ainsi que des actes involontaires tels que les erreurs humaines et les catastrophes naturelles. La sécurité de l'information est plus que la protection. Il s'agit d'assurer l'accès en temps opportun et la disponibilité du contenu du document pour améliorer les processus et les performances de l'entreprise. Il s'agit également de gérer le contenu original et de se conformer aux règlements fédéraux.

Dès l'introduction des premiers produits numériques, Xerox a reconnu le risque que les données conservées soient récupérées de manière inappropriée à partir d'un stockage non volatile et des fonctionnalités et des contre-mesures intégrées dans nos appareils pour aider les clients à sauvegarder leurs données.

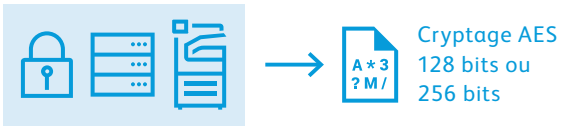
**CRYPTAGE DES DONNÉES D'IMAGE**

En utilisant le cryptage AES 128 bits ou 256 bits, de nombreux périphériques Xerox® disposent du cryptage des données, y compris les données de travail, d'image et de client, qui protègent les données de votre MFP de Xerox® contre tout accès non autorisé. Avec le chiffrement des données, le disque est partitionné et seule la partition de données utilisateur est cryptée. Les partitions du système d'exploitation ne sont pas et ne peuvent pas être cryptées.

- Cryptage AES 128 bits ou 256 bits, validé Federal Information Processing Standard (FIPS) 140-2
- Toutes les données d'image de l'utilisateur sur le disque dur sont cryptées

# Vue d'ensemble de la sécurité

AES est une norme de cryptage rapide, difficile à craquer et adaptée à une large gamme de périphériques ou d'applications. C'est la combinaison de pointe de la sécurité, de la performance, de l'efficacité, de la facilité d'implémentation et de la flexibilité. Plusieurs périphériques Xerox® peuvent être mis en mode FIPS 140-2, ce qui signifie qu'ils n'utiliseront que des algorithmes de cryptage certifiés FIPS 140-2




### ÉCRASEMENT DE L'IMAGE

L'écrasement d'image efface les données d'image du disque dur de votre périphérique Xerox® une fois que les données ne sont plus nécessaires. Cela peut être effectué automatiquement après l'achèvement du traitement de chaque travail, programmé périodiquement, ainsi qu'à la demande de l'administrateur système. Les appareils Xerox® disposent de l'effacement d'image immédiate et à la demande.


### MÉMOIRE VOLATILE ET NON VOLATILE

Dans chaque MFP Xerox®, le contrôleur comprend la mémoire volatile (RAM) et la mémoire non volatile (disque dur). Avec la mémoire volatile, toutes les données d'image sont perdues lors de l'arrêt ou du redémarrage du système. Avec la mémoire non volatile, les données d'image sont généralement stockées en flash ou sur le disque dur du MFP, et sont préservées jusqu'à ce qu'elles soient effacées.

Au fur et à mesure que la sécurité des données augmente, les clients souhaitent savoir comment et où les données peuvent être compromises. Les énoncés de volatilité sont des documents créés pour aider à identifier les données d'image du client situées dans les appareils Xerox®. Un énoncé de volatilité décrit les emplacements, les capacités et le contenu des dispositifs de mémoire volatiles et non volatiles dans un périphérique Xerox®.

Des énoncés de volatilité ont été créées pour de nombreux appareils Xerox® pour aider les clients conscients de la sécurité. Ces documents peuvent être obtenus en contactant votre équipe de soutien Xerox locale (pour les clients existants), un professionnel de vente Xerox (pour les nouveaux clients) ou peut être consulté à www.xerox.com/security.

### TÉLÉCOPIE SÉCURISÉE

Les télécopies sensibles reçues sont conservées jusqu'à ce qu'elles soient libérées par l'administrateur système.

### PROTECTION PAR MOT DE PASSE DE LA NUMÉRISATION VERS BOÎTE AUX LETTRES

Lors de l'utilisation de la fonction Numérisation vers boîte aux lettres d'un MFP, la boîte aux lettres désignée peut être protégée par mot de passe pour s'assurer que seules les personnes autorisées peuvent accéder aux numérisations stockés dans celle-ci. La sécurité de la numérisation vers boîte aux lettres est encore augmentée par un cryptage de la partition de données d'image du disque dur.

### S/MIME POUR LA NUMÉRISATION VERS COURRIEL

S/MIME (Secure/Multipurpose Internet Mail Extensions) fournissent les services de sécurité cryptographique suivants pour la fonctionnalité Numériser vers courriel : authentification, intégrité du message et non-répudiation d'origine (à l'aide de signatures numériques) et sécurité des données personnelles et des données (utilisation du cryptage).

Dans la communication S/MIME, lors de l'envoi de données au réseau, une signature est ajoutée à chaque message électronique en fonction des informations du certificat conservées dans le périphérique. Le cryptage est effectué lors de l'envoi de données en fonction du certificat correspondant à l'adresse désignée de chaque message. Le certificat est vérifié lorsque des informations de transmission de données entrent, ainsi que lorsque les données doivent être envoyées. La communication S/MIME est effectuée uniquement lorsque la validité du certificat est confirmée.

### CRYPTAGE NUMÉRISATION VERS COURRIEL

Le cryptage du courrier électronique au moyen de l'authentification par carte à puce permet aux utilisateurs d'envoyer jusqu'à 100 courriels cryptés à plusieurs destinataires dans le répertoire LDAP d'une entreprise à l'aide des clés p ubliques des destinataires. La plupart des MFP Xerox® utilisant l'authentification par carte à puce offrent également la possibilité de signer numériquement des courriels. Les utilisateurs peuvent afficher les certificats des destinataires potentiels avant d'envoyer un courrier électronique. Le MFP interdit l'envoi aux utilisateurs sans certificat de cryptage. En outre, le MFP enregistre tous les enregistrements de courrier électronique envoyé avec une option permettant à l'administrateur de recevoir des rapports de confirmation.

### JOURNAL DE TRAVAIL DISSIMULÉ

La fonction standard Journal de travail dissimulé garantit que les travaux traités par l'appareil ne sont pas visibles pour un utilisateur libre-service ou au moyen de l'interface utilisateur à distance. Les informations du journal des travaux, bien cachées, sont encore accessibles par l'administrateur système, qui peut imprimer le journal des travaux pour afficher l'utilisation de la copie, de la télécopie, de l'impression et de la numérisation sur l'appareil.

# Vue d'ensemble de la sécurité

### OFFRE DE RÉTENTION DU DISQUE DUR

Xerox offre une offre de rétention de disque dur pour les appareils Xerox® aux clients qui craignent que les données d'image sur leur disque dur soient plus sensibles ou même classées secrètes. Ce service permet à un client, moyennant des frais, de conserver ses disques dur et de les expurger ou de les détruire de manière à ce qu'ils gardent leurs données d'image sécurisées.

### VALIDATION DES DONNÉES DES SERVICES À DISTANCE

De nombreux appareils Xerox® obtiennent l'achat du client avant de transmettre des informations personnelles identifiables (IPI) et des informations identifiables par le client (IIC) au moyen des services à distance à Xerox.

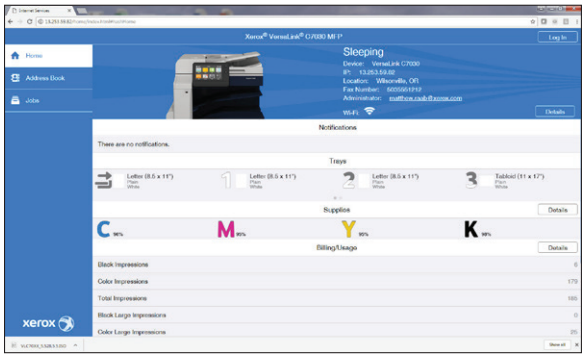
### MOTS DE PASSE POSTSCRIPT

Une autre zone de risque liée à l'impression consiste à imprimer avec le langage de description de page (PDL) PostScript® d'Adobe®. PostScript comprend des commandes qui permettent aux travaux d'impression de modifier les comportements par défaut de l'appareil, ce qui pourrait exposer le périphérique. Étant donné que le langage PostScript comprend des utilitaires très puissants qui pourraient être utilisés pour compromettre la sécurité d'un périphérique, les administrateurs peuvent configurer le périphérique afin que les travaux PostScript soient requis pour inclure un mot de passe pour modifier les comportements par défaut du périphérique. Les privilèges de base de l'interpréteur PostScript dans le contrôleur sont limités par la conception, mais les administrateurs ont une certaine capacité pour gérer le fonctionnement du sous-système PostScript.

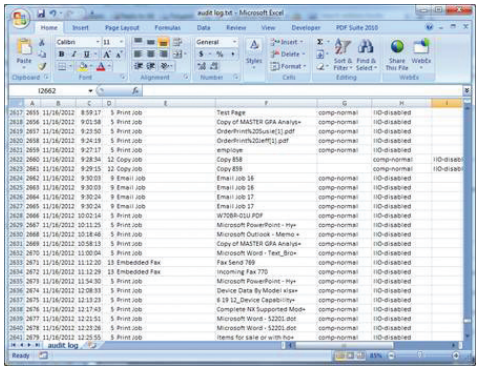
### JOURNAL D'AUDIT

Les multifonctions Xerox® et plusieurs de nos imprimantes peuvent conserver les journaux d'audit pour suivre l'activité par document, utilisateur et fonction. Le journal d'audit est activé par défaut sur des périphériques plus récents et peut être activé ou désactivé par l'administrateur système. Il peut suivre l'accès et la tentative d'accès au périphérique et transmettre les journaux d'audit à un système SIEM ou à un serveur de journal d'audit. Un exemple d'entrée du journal d'audit : « Utilisateur xx connecté sur le MFP AltaLink® de Xerox® à 12:48 AM et télécopie de 10 pages au 888.123.1234. »

Pour les imprimantes multifonctions compatibles avec la technologie ConnectKey® de Xerox®, le journal d'audit peut être envoyé automatiquement et en toute sécurité à un système SIEM pour assurer une surveillance continue du MFP.




L'interface du journal d'audit est accessible depuis le poste de travail d'un administrateur système à l'aide d'un navigateur Web standard.



Le journal peut ensuite être exporté vers un fichier .text et ouvert avec Microsoft® Excel®.

## 4. Partenariats externes

Xerox travaille avec des organismes de test de conformité et des chefs de l'industrie de la sécurité tels que McAfee pour envelopper leurs normes et savoir-faire généraux autour des nôtres. Les fonctions de protection contre les logiciels malveillants suivantes sont disponibles sur les MFP compatibles avec la technologie ConnectKey® de Xerox® (Imprimantes multifonctions AltaLink® et i-Series de Xerox®).

### CONTRÔLE INTÉGRÉ DE MCAFEE® – SÉCURITÉ RENFORCÉE

Les multifonctions Xerox® intégrés à la technologie ConnectKey® de Xerox®incluent l'intégration du contrôle intégré McAfee optimisée par la sécurité Intel®, ce qui se traduit par la première gamme d'imprimantes multifonctions de l'industrie qui se protège contre les menaces extérieures potentielles. La technologie de liste blanche McAfee détecte les tentatives non autorisées de lecture, d'écriture ou d'ajout à des fichiers et répertoires protégés et envoie des alertes s'ils surviennent. En outre, une intégration transparente avec le logiciel CentreWare® Web de Xerox®, l'ensemble d'outils MPS de Xerox® et McAfee ePolicy Orchestrator®(McAfee ePOMC) permet de surveiller à partir de la console préférée.

### CONTRÔLE INTÉGRÉ DE MCAFEE – CONTRÔLE D'INTÉGRITÉ

Le contrôle d'intégrité s'appuie sur les fonctionnalités de sécurité améliorée et ajoute la prévention que des nouveaux fichiers soient exécutés à partir de n'importe quel emplacement par des moyens non approuvés. Seul un logiciel approuvé est autorisé s'exécuter, ce qui empêche les attaques générales et ciblées. Utile spécialement pour les mises en œuvre de sécurité à l'échelle de l'entreprise, la technologie de liste blanche de l'offre de sécurité Xerox et Intel qui garantit que les seules fonctions que ces périphériques exécutent sont les services que vous souhaitez offrir. Cette même technologie est utilisée pour protéger les serveurs, les GAB, les terminaux de point de vente et les périphériques intégrés tels que les appareils mobiles.

### MCAFEE EPOLICY ORCHESTRATOR (EPO)

McAfee ePolicy Orchestrator (ePO) est un outil logiciel de gestion de la sécurité qui rend la gestion des risques et de la conformité plus facile pour les entreprises de toutes tailles. Il présente aux utilisateurs des tableaux de bord glisser-déposer qui fournissent des informations de sécurité à travers les points d'extrémité - données, mobiles et réseaux - pour un aperçu immédiat et des temps de réponse plus rapides. EPolicy s'appuie sur les infrastructures informatiques existantes en connectant la gestion de McAfee et des solutions de sécurité tierces à LDAP, aux opérations informatiques et aux outils de gestion de la configuration.

Pour une preuve indépendante par un tiers, nous obtenons les meilleurs niveaux de conformité, les organismes de certification tels que les Critères communs (ISO/CEI 15408) et FIPS 140-2 mesurent notre performance par rapport aux normes internationales. Ils nous reconnaissent pour notre approche globale de la sécurité de l'imprimante.

### INTÉGRATION DU MOTEUR DES SERVICES D'IDENTITÉ (ISE) DE CISCO®

Gère et déploie de manière centralisée les stratégies de sécurité de l'imprimante. Notre partenariat avec Cisco offre de meilleures capacités de détection des périphériques d'impression Xerox®, ce qui se traduit par une application plus stricte des stratégies de sécurité. Les périphériques Xerox® sont automatiquement reconnus et classés par ISE de Cisco, ce qui permet de contrôler l'accès au réseau et de réduire les frais généraux en éliminant la saisie manuelle des attributs de l'imprimante. Notre profilage des imprimantes avec ISE de Cisco contrecarre les tentatives d'usurpation d'identité par les saboteurs pour accéder sans entrave aux systèmes sensibles. L'intégration du périphérique d'impression Xerox® avec ISE de Cisco offre une approche opérationnelle efficace pour atteindre les objectifs des stratégies de sécurité.

# Conformité réglementaire et politique

Les imprimantes et les multifonctions modernes sont axés sur la conformité en raison des données personnelles et sensibles qu'elles accèdent, stockent et communiquent. La non-conformité peut entraîner des occasions d'affaires perdues, perdre des clients existants ou même des actions en justice. Les niveaux de conformité requis varient selon le marché national et le marché vertical.

La Loi sur la transférabilité et la responsabilité en matière d'assurance maladie (Health Insurance Portability and Accountability Act - HIPAA) aux États-Unis et la Loi sur la protection des données au Royaume-Uni (Data Protection Act) sont des exemples de normes qui devront être respectées pour poursuivre les activités légalement.

La certification Critères communs est une norme de sécurité reconnue internationalement qui répond aux spécifications du ministère de la Défense des États-Unis.

Grâce aux fonctionnalités de sécurité chefs de file de l'industrie et à une approche flexible de la configuration et du déploiement, les périphériques Xerox® peuvent être conformes à toutes les normes et disposent des contrôles pour répondre aux besoins.

Les systèmes, les logiciels et les services Xerox® sont conformes aux normes reconnues de l'industrie et aux dernières réglementations gouvernementales en matière de sécurité. Nos produits offrent des fonctionnalités qui permettent à nos clients de respecter ces normes. Les normes suivantes en sont des exemples :

- Normes de sécurité des données de l'industrie des cartes de paiement (PCI) version 3.0
- Sarbanes-Oxley
- Basel II Framework
- La loi Health Insurance Portability and Accountability Act (HIPAA)
- Directive ePrivacy (2002/58/CE)
- La loi Gramm-Leach-Bliley Act
- La loi Family Educational Rights and Privacy Act
- La loi Health Information Technology for Economic and Clinical Health Act
- La loi Dodd-Frank Wall Street Reform and Consumer Protection Act
- ISO-15408 Critères communs pour l'évaluation de la sécurité des technologies de l'information
- ISO-27001 Normes du système de gestion de la sécurité de l'information
- Objectifs de contrôle de l'information et la technologie concernée
- Déclaration sur les normes d'audit n° 70
- NIST 800-53, adopté par le gouvernement fédéral américain et la DOD en 2014
- Programme fédéral de risque et d'autorisation (FedRAMP)

## Évaluation de la sécurité du produit

La sécurité des documents signifie une tranquillité d'esprit. L'une des caractéristiques de la gamme de produits Xerox® est un engagement envers la sécurité de l'information. Nos systèmes, nos logiciels et nos services comprennent et se conforment aux normes reconnues de l'industrie et aux dernières réglementations de sécurité gouvernementales.

### Certification Critères communs

La certification Critères Communs fournit une validation tierce et indépendante de la fiabilité, de la qualité et de la fiabilité des produits informatiques. C'est une norme sur laquelle les clients peuvent compter pour les aider à prendre des décisions éclairées sur leurs achats informatiques. Les Critères communs définissent des objectifs spécifiques d'assurance de l'information, y compris des niveaux stricts d'intégrité, de confidentialité, de disponibilité pour les systèmes et les données, la responsabilisation au niveau individuel et l'assurance que tous les objectifs sont atteints. La certification Critères communs est une exigence de dispositifs matériels et de logiciels utilisés par le gouvernement fédéral sur les systèmes de sécurité nationale.

### Obtention de la certification Critères communs

La certification Critères communs est un processus rigoureux qui comprend des tests de produits par un laboratoire tiers accrédité par le Programme national d'accréditation des laboratoires bénévoles (NVLAP) pour effectuer l'évaluation des produits en fonction des exigences de sécurité. Les produits sont testés en fonction des exigences fonctionnelles de sécurité en fonction des niveaux d'assurance d'évaluation prédéfinis (EAL) ou des exigences d'assurance spécialisées.

Pour les soins de santé, les services financiers et d'autres industries, le besoin de sécurité n'est pas moins important. Qu'ils protègent la vie privée de leurs clients ou leurs actifs intellectuels et financiers, l'assurance que les réseaux, les disques durs et les lignes téléphoniques sont sécurisées contre les pirates informatiques, les virus et autres activités malveillantes. Bien qu'elle n'est pas exigence hors du gouvernement fédéral, la certification Critères communs peut fournir une validation indépendante.

Avec environ 150 appareils ayant terminé le processus de certification, Xerox possède l'un des plus grands nombres de MFP certifiés Critères communs. En outre, Xerox a été le premier fabricant à certifier l'intégralité de l'appareil et Xerox est le seul fabricant à toujours certifier l'intégralité du périphérique.

Visitez www.xerox.com/information-security/common-criteria-certified pour voir quels MFP Xerox® ont obtenu la certification Critères communs.

# Évaluation des risques et atténuation

## Sécurité proactive pour les menaces émergentes

Cela fait partie de notre histoire; vous offrir les produits et les solutions les plus sûrs du marché aujourd'hui. Nos scientifiques et nos ingénieurs travaillent dur en développant la prochaine génération de technologies de sécurité innovantes pour lutter contre les menaces de demain et garder vos documents en sécurité : la technologie d'impression de micro-impression, de fluorescence et d'impression infrarouge, la technologie de marque d'impression GlossMark® et Correlation Marks de Xerox®, pour n'en citer que quelques-unes. Pour plus d'informations sur ces technologies, visitez www.xerox.com/security.

Autres choses que Xerox fait :

### Surveiller les derniers risques

Nous surveillons de près les centres d'accès à la vulnérabilité afin de vous tenir au courant des dernières informations, de sorte que vous n'avez pas le faire.

### Publier des bulletins de sécurité

Nous sommes proactifs en vous fournissant des correctifs de sécurité et des mises à jour si nécessaire, en gardant votre matériel à jour et vos données sécurisées.

### Distribuer des flux RSS

Les mises à jour à la minute sont automatiquement distribuées aux lecteurs de flux RSS des clients.

### PFournir une multitude d'informations

Si vous souhaitez en savoir plus de votre propre initiative, nous offrons une bibliothèque en constante expansion d'articles de sécurité, de livres blancs et de guides.

Visitez www.xerox.com/security pour accéder à notre large éventail de ressources de sécurité.

En plus de nos propres tests internes étendus, Xerox surveille régulièrement les centres de compensation de vulnérabilité mis à disposition par ces entités et ressources telles que le rapport US-CERT et le rapport Critical Patch Updates d'Oracle®; les bulletins de sécurité de Microsoft®, pour diverses vulnérabilités de logiciels et de systèmes d'exploitation; et Bugtraq, SANS.org et secunia.com pour les vulnérabilités source ouverte. Un programme robuste de test de sécurité interne est également engagé, ce qui implique une analyse de vulnérabilité et des tests de pénétration pour fournir des correctifs complètement testés.
Visitez www.xerox.com/security pour lire la Politique sur la gestion de la vulnérabilité et la divulgation.

## Bulletins de sécurité et déploiement de correctifs

Les développeurs de Xerox suivent un cycle formel de développement de la sécurité qui gère les problèmes de sécurité grâce à l'identification, l'analyse, la hiérarchisation, le codage et les tests. Nous nous efforçons de fournir des correctifs le plus rapidement possible en fonction de la nature, de l'origine et de la gravité de la vulnérabilité. Selon la gravité de la vulnérabilité, la taille du correctif et du produit, le correctif peut être déployé séparément ou prendre la forme d'une nouvelle version de logiciel pour ce produit.

Selon le produit Xerox® qui nécessite un correctif, les clients peuvent télécharger des correctifs de sécurité au www.xerox.com/security. Pour d'autres produits Xerox® le correctif de sécurité sera mis à disposition dans le cadre d'une nouvelle version du logiciel système. Vous pouvez vous inscrire pour recevoir des bulletins régulièrement. Aux États-Unis, les clients devraient s'inscrire au flux RSS de sécurité. À l'extérieur des États-Unis, contactez votre centre de soutien Xerox local.

Vous avez accès à des mises à jour d'informations et à des ressources importantes en temps opportun sur le site www.xerox.com/security :

- Bulletins de sécurité
- Flux RSS : obtenir des bulletins de sécurité
- Questions fréquemment posées sur la sécurité des produits Xerox®
- Documents sur la divulgation de l'assurance de l'information
- Produits certifiés Critères communs
- Politique sur la gestion de la vulnérabilité et la divulgation
- Guide de sécurité du produit
- Articles et livres blancs
- Déclarations de volatilité
- Tableau de recherche rapide de publication de logiciel
- Guide FTC pour les copieurs et les multifonctions numériques

www.xerox.com/security est votre portail pour une large gamme d'informations et de mises à jour liées à la sécurité, y compris des bulletins, des livres blancs, des correctifs et bien plus encore.

# Pratiques de fabrication et de sécurité des fournisseurs

Xerox et ses principaux partenaires de fabrication sont membres de l'Electronic Industry Citizenship Coalition (http://www.eicc.info). En souscrivant au code de conduite de l'EICC, Xerox et d'autres entreprises démontrent qu'elles maintiennent une surveillance rigoureuse de leurs processus de fabrication.

En outre, Xerox a des relations contractuelles avec ses fournisseurs primaires et secondaires qui permettent à Xerox de réaliser des audits sur place afin d'assurer l'intégrité du processus au niveau des composants.

Xerox est également membre du Partenariat commercial contre le terrorisme de l'Agence des douanes des États-Unis. Cette initiative porte sur la sécurité de la chaîne d'approvisionnement. Les exemples de pratiques adoptées par Xerox dans le cadre de ce programme sont ceux mis en place pour contrer le vol ou le détournement. En Amérique du Nord, toutes les remorques se déplaçant entre l'usine et les centres de distribution de produits (PDC) et entre les PDC et les Centres logistiques des transporteurs (CLC) sont scellés au point d'origine. Tous les camions ont des localisateurs GPS installés et sont surveillés en permanence.

# Retours et élimination de produits

## Offre de rétention de disque dur pour les produits Xerox®

Xerox fournit une offre de rétention de disque dur pour permettre aux clients aux États-Unis, moyennant des frais, de conserver le disque dur sur les produits Xerox® loués. Ce service peut être nécessaire pour les clients ayant des données très sensibles, peut-être classées ou avec des politiques internes ou des normes réglementaires qui exigent des processus de disposition spécifiques pour les disques durs.

Sur demande pour cette offre de service, un technicien de service Xerox se rendra à l'emplacement du client, supprime le disque dur et le fournit « tel quel » à un représentant du client. À l'heure actuelle, Xerox ne fournit pas de services d'assainissement, de nettoyage ou de destruction sur disque dur sur les sites des clients. Les clients devront prendre des dispositions pour la disposition finale du disque dur physique reçu du technicien.

Pour déterminer si votre produit Xerox® contient un disque dur ou pour examiner les fonctions de sécurité disponibles pour sécuriser les données sur les disques durs, veuillez visiter www.xerox.com/harddrive.

Pour plus de détails sur ce programme, contactez votre représentant commercial Xerox ou visitez www.xerox.com/security sous la rubrique Ressources de sécurité dans la section Articles et livres blancs.

En outre, pratiquement toutes les nouvelles imprimantes et MFP Xerox® sont compatibles avec le cryptage du disque AES 256 bits, ainsi que l'écrasement des données d'image à 3 passages pour garantir que les données de nos clients sont protégées dès le premier jour sur leur nouveau matériel.

# Résumé

La sécurité des réseaux et des données fait partie des nombreux défis auxquels les entreprises sont confrontées quotidiennement. Et parce que les imprimantes et les multifonctions d'aujourd'hui sont des périphériques réseau critiques pour l'entreprise qui reçoivent et envoient des données importantes grâce à diverses fonctions, la sécurité globale est primordiale.

Le système entier d'un MFP, ainsi que tout logiciel de gestion de périphérique sur le réseau, doit être évalué et certifié afin que la sécurité de l'information et tous les travailleurs d'une entreprise soient certains que leurs documents et leur réseau sont sécurisés contre les prédateurs d'informations ou même de violations de sécurité internes.

À cet égard, les MFP Xerox® sont les chefs de file de l'industrie. Notre approche globale, basée sur la sécurité fondamentale, fonctionnelle, avancée et utilisable, est essentielle pour protéger les actifs d'information de nos clients.

Reconnaissant cela, Xerox continue à concevoir tous ses produits afin d'assurer le plus haut niveau possible de sécurité pour tous les points potentiels de vulnérabilité. Nous nous engageons à sauvegarder vos données afin que vous puissiez vous concentrer sur les activités qui rendent votre entreprise ou votre organisation la plus efficace possible.

Pour plus d'informations sur les nombreux avantages de sécurité offerts par Xerox, visitez www.xerox.com/security.

# Liste de contrôle de sécurité

Les responsables de la sécurité informatique sont déjà confrontés à la gestion des exigences de sécurité. Les petites entreprises doivent compter sur des systèmes efficaces et des logiciels de sécurité pour faire une grande partie du travail pour eux. La dernière chose que vous et votre personnel avez besoin est une activité plus élevé ou des interventions manuelles pour surveiller et tenir à jour tous les périphériques et les flux de données dans votre environnement, y compris vos MFP et vos imprimantes.

Un plan complet de sécurité du réseau devrait inclure trois points d'importance, avec une stratégie en place pour que chacun puisse vous assurer d'avoir un plan qui fonctionne.

1. Appareils « mains libres, autoprotection » qui résistent aux nouvelles attaques
2. Conformité aux normes et réglementations de sécurité les plus récentes
3. Visibilité complète sur le réseau

## La nouvelle norme de sécurité pour un nouvel âge

- La sécurité ne peut pas être une réflexion ultérieure.
- L'information est une propriété intellectuelle de plus en plus précieuse.
- Les pare-feux ne suffisent pas; les politiques de sécurité doivent être holistiques et omniprésentes.
- La protection intégrés des périphériques fait maintenant partie intégrante de l'impératif de sécurité d'aujourd'hui.

Xerox offre une sécurité complète et multicouches qui est facile à déployer et à gérer, et permet de garder votre entreprise conforme aux normes de l'industrie et du gouvernement. La technologie Xerox® est testée et validée pour protéger contre les accès non autorisés, les données et l'identité.

Lors de la comparaison des MFP Xerox® avec les produits d'autres fabricants, utilisez la liste de contrôle suivante pour déterminer si les périphériques des concurrents offrent le même niveau de sécurité de bout en bout livré par Xerox.

| | | Concurrent | | |
|---|---|---|---|---|
| | Xerox | 1 | 2 | 3 |
| Filtrage d'adresses IP/MAC | ✓ | | | |
| Cryptage IPsec | ✓ | | | |
| IPv6 | ✓ | | | |
| Authentification 802.1X | ✓ | | | |
| Impression sécurisée | ✓ | | | |
| Cryptage Numérisation vers courriel | ✓ | | | |
| PDF crypté/PDF protégé par mot de passe | ✓ | | | |
| Signatures numériques | ✓ | | | |
| AES 256 bits Cryptage du disque dur | ✓ | | | |
| Écrasement d'image | ✓ | | | |
| Télécopie sécurisée | ✓ | | | |
| Blocage de port | ✓ | | | |
| Protection par mot de passe Numérisation vers boîte aux lettres | ✓ | | | |
| Offre de rétention de disque dur | ✓ | | | |
| Restrictions d'impression | ✓ | | | |
| Journal d'audit | ✓ | | | |
| Contrôle d'accès basé sur les rôles | ✓ | | | |
| Authentification par carte à puce | ✓ | | | |
| Carte d'accès commune/ vérification de l'identité personnelle | ✓ | | | |
| Permissions utilisateur | ✓ | | | |
| Certification Critères communs « Système complet » | ✓ | | | |
| Intégration avec outils de gestion de réseau standard | ✓ | | | |
| Mises à jour de sécurité au moyen de flux RSS | ✓ | | | |
| Protection intégrée McAfee optimisée par la sécurité Intel® | ✓ | | | |
| Contrôle d'intégrité McAfee® | ✓ | | | |
| Intégration ePolicy Orchestrator® de McAfee® | ✓ | | | |
| Intégration du moteur des services d'identité (ISE) de Cisco® | ✓ | | | |

Pour en savoir plus, visitez **www.xerox.com**.


05/18 BR21699 SECGD-01QC