Xerox et la sécurité des informations

Vos données, votre entreprise :
Un partenariat pour protéger vos ressources les plus importantes

Sommaire

Présentation générale

Les informations constituent des ressources clés pour les entreprises et la sécurité est essentielle au bureau, que ce soit pour les documents ou pour tous les périphériques, imprimantes et multifonctions notamment, connectés au réseau. De plus, au 21e siècle, le réseau est le centre névralgique de la quasi-totalité des activités d'entreprise.

Presque toutes les entreprises, et tous les collaborateurs qui y travaillent, sont connectés à Internet. Votre entreprise, et toutes les organisations avec lesquelles vous collaborez, font partie d'un système global de réseaux et serveurs informatiques interconnectés. D'innombrables utilisateurs effectuent des tâches simultanément, consultent et partagent des informations, achètent et vendent des produits et des services, et communiquent par courrier électronique, par messagerie instantanée, via Skype™, Twitter et de nombreux autres services.

La menace sur la sécurité est bien réelle et les enjeux se multiplient à une vitesse exponentielle. Une faille dans la sécurité des documents d'une organisation peut entraîner une acquisition ou une utilisation non autorisée d'informations confidentielles ou de nature exclusive. Elle peut conduire à leur divulgation malveillante, au vol ou compromettre la propriété intellectuelle et les secrets commerciaux. Et pour de nombreuses organisations, ces failles de sécurité peuvent se solder par des amendes et des litiges coûteux, pouvant s'élever à des centaines de milliers voire des millions de dollars.

Aujourd'hui, les menaces de sécurité sont plus nombreuses, prennent diverses formes et ont des degrés de gravité variables. Avec la prolifération explosive des appareils en réseau, les intrus disposent d'un nombre croissant de points d'entrée potentiellement vulnérables. Et la menace de piratage informatique est constante, avec des programmes qui tournent 24 heures sur sur 24, 7 jours sur 7 recherchant et exploitant automatiquement les failles de sécurité.

Les menaces de sécurité varient, des pourriels, relativement inoffensifs, aux menaces persistantes capables de bloquer des réseaux entiers.

Avec une telle activité Internet, vous devez veiller à garantir la sécurité des informations confidentielles de votre société. Cependant, les exigences évoluent et changent chaque jour.

Les imprimantes et multifonctions réseau, qui sont capables d'imprimer, de copier, de numériser vers des destinations réseau, d'envoyer des fichiers joints à des courriels et de traiter les télécopies entrantes et sortantes, sont particulièrement vulnérables.

Pour les spécialistes de la sécurité de l'information, il est primordial pour la sécurité du réseau de l'organisation d'empêcher les infractions de sécurité via les imprimantes et les multifonctions réseau ou sur les périphériques mêmes. Après tout, les attaques peuvent se produire par des moyens inattendus :

- La ligne téléphonique à laquelle est raccordé un multifonction peut être utilisée pour accéder au réseau.
- Le serveur Web utilisé pour gérer les imprimantes et les multifonctions peut être vulnérable aux attaques.
- Les données électroniques non protégées peuvent faire l'objet d'un accès non autorisé lorsqu'elles résident sur le disque dur ou lorsqu'elles circulent entre les périphériques.
- Des courriels malveillants peuvent être envoyés depuis un multifonction ne disposant pas d'une piste de vérification.

Les imprimantes et les imprimantes multifonctions constituent des plateformes IT sophistiquées, comportant de nombreux sous-systèmes. Par conséquent, pour être efficaces, les mesures de sécurité doivent couvrir chacun des éléments de ces plateformes.

Les imprimantes et les multifonctions actuels sont tout à fait différents des PC et des serveurs.

- Les imprimantes et les multifonctions sont des périphériques partagés comptant plusieurs utilisateurs et administrateurs.
- Les imprimantes et les multifonctions sont des périphériques intégrés :
  - Il peut y avoir un véritable système d'exploitation au sein du système.
  - Le système d'exploitation peut avoir une interface externe accessible directement.
  - Le système d'exploitation peut être un système propriétaire.
  - Le système d'exploitation peut être un système Microsoft® Windows®.

Présentation générale

- Les imprimantes et les multifonctions présentent les caractéristiques suivantes, toutes généralement associées à des nœuds de calcul plus avancés :
  - Piles de protocole réseau
  - Fonctions d'autorisation et d'authentification
  - Cryptage
  - Gestion du périphérique
  - Serveurs Web

L'hétérogénéité de mise en œuvre des imprimantes et des multifonctions pose des difficultés.

- Les périphériques sont beaucoup plus divers que les PC traditionnels.
- Les systèmes d'exploitation sous-jacents varient grandement d'un constructeur à l'autre et même d'une gamme à l'autre chez un même constructeur.

Les contrôles habituels mis en place sur les serveurs et les PC ne sont pas optimisés pour les imprimantes et les multifonctions.

- Approche anti-virus
  - Peut ne pas être disponible pour le type de système d'exploitation utilisé dans l'imprimante ou le multifonction
  - Généralement inefficace contre les logiciels malveillants
  - Difficulté à gérer les mises à jour des fichiers de données en environnement distribué
- Installation de correctifs sur les imprimantes et les multifonctions
  - Le contrôle des versions logicielles des imprimantes et multifonctions n'est pas cohérent.
  - La gestion des configurations entraîne des surcoûts opérationnels.
- Gestion des informations et des événements de sécurité (SIEM)
  - Les alertes provenant des imprimantes et des multifonctions sont de niveau inégal.
  - La remise en état des imprimantes et des multifonctions n'est pas standardisée.

C'est une situation tout à fait différente de celle des imprimantes et copieurs d'hier.

N'importe qui ou presque est capable de lancer une attaque contre le réseau et les actifs informationnels d'une entreprise si l'accès physique et électronique aux imprimantes et aux multifonctions n'est pas rigoureusement contrôlé et protégé. Ces attaques peuvent aller des plus simples aux plus sophistiquées : d'une personne qui ramasse des documents laissés dans le bac de réception d'une imprimante ou d'un multifonction aux codes malveillants, tels que les vers, qui récupèrent des documents sensibles sur le réseau.

L'intégralité du système qui compose une imprimante ou un multifonction, ainsi que tout logiciel de gestion de périphériques sur le réseau, doit être évaluée et certifiée pour que le service chargé de la sécurité de l'information et l'ensemble des collaborateurs d'une organisation soient certains que leurs documents et le réseau sont à l'abri des prédateurs, voire des failles de sécurité internes.

Sur ce plan, toutes les imprimantes et tous les multifonctions ne sont pas égaux. Par conséquent, il est essentiel de mettre en place une approche globale reposant sur une sécurité fondamentale, fonctionnelle, avancée et opérationnelle, pour protéger les actifs informationnels des entreprises d'aujourd'hui.

Heureusement, Xerox dispose de solutions de sécurité pour vous aider. Depuis 20 ans, Xerox est leader dans la fourniture de solutions documentaires sécurisées à divers secteurs d'activités partout dans le monde. En fait chaque produit et service Xerox® que nous proposons est conçu pour une sécurité accrue et pour s'intégrer de manière transparente dans les cadres de sécurité existants. De plus, la sécurité est assurée tout au long du cycle de vie des produits, de l'analyse des besoins à la mise au rebut, en passant par la conception, le développement, la fabrication et l'installation. Vous et vos clients bénéficiez ainsi d'une protection accrue et pouvez travailler l'esprit tranquille.

Chez Xerox, nous vous aidons à protéger vos données à tous les points de vulnérabilité possibles, pour que vous n'ayez pas à le faire. En restant concentrés sur ce que nous faisons le mieux, vous serez en mesure d'en faire de même.

Objectifs de sécurité Xerox

Nous avons identifié cinq domaines de protection qui nous permettent de fournir des solutions fiables et sûres à chacun de nos clients :

CONFIDENTIALITÉ

- Aucune donnée n'est divulguée sans autorisation pendant le traitement, la transmission ou le stockage.

INTÉGRITÉ

- Aucune donnée ne peut être modifiée sans autorisation.
- Le système fonctionne selon l'usage prévu et il est protégé contre les manipulations non autorisées.

DISPONIBILITÉ

- Le système fonctionne correctement.
- Aucun refus de service pour les utilisateurs autorisés.
- Protection contre tout usage frauduleux.

RESPONSABILITÉ

- Les actions d'une entité peuvent être tracées directement jusqu'à celle-ci.

NON-RÉPUDIATION

- Assurance réciproque que l'authenticité et l'intégrité des communications réseau sont maintenues.

Vulnérabilités de sécurité : Risques du secteur et coûts

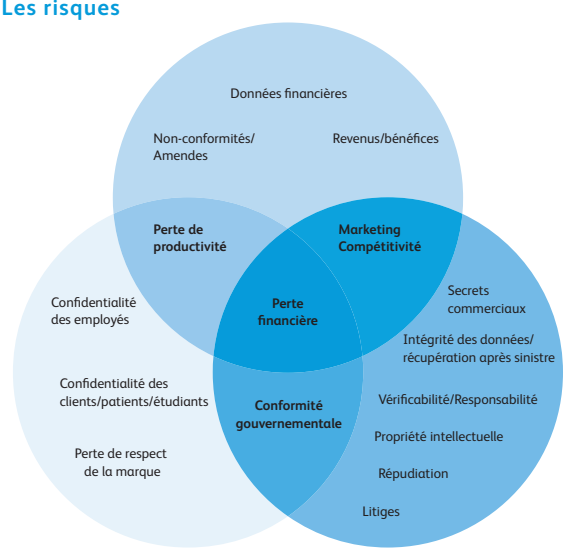
Les entreprises de toute taille détiennent des informations sensibles qui intéressent intéressent les cybercriminels et qui doivent être protégées. Le paysage des menaces change constamment. Avec l'augmentation du BYOD (Bring Your Own Devices), de la technologie prêt-à-porter pour le suivi des données médicales, des systèmes mobiles de paiement, de l'archivage cloud et de l'Internet des objets, la menace est bien réelle et continue de s'intensifier.

Les cybercriminels se focalisent de plus en plus sur les petites et moyennes entreprises (PME) parce qu'elles constituent des cibles plus faciles que les grandes entreprises et qu'elles ne disposent généralement pas des ressources nécessaires pour se protéger des attaques. Si les violations de données dans les grandes entreprises font la une des journaux, nous entendons malheureusement moins parler des cyberattaques dont sont victimes les PME.

Les enjeux pour les PME sont bien plus importants que pour les grands groupes. Les informations clients que gèrent les PME prennent davantage de valeur et les coûts d'une violation de données peuvent avoir des conséquences dévastatrices pour une PME. Selon une étude réalisée en 2015 pat IBM et le Ponemon Institute, le coût moyen total des violations de données pour les entreprises participantes avaient augmenté de 23 % en deux ans pour atteindre 3,79 millions de dollars.1 Le montant moyen payé pour chaque enregistrement perdu ou volé contenant des informations sensibles et confidentielles est passé de 145 dollars en 2014 à 154 dollars en 2015.1

Ce montant ne prend pas en compte les amendes, la perte de réputation et les interruptions d'activité éventuelles. Si la sécurité n'est pas toujours la priorité n°1 des entreprises, il est primordial de protéger les informations pour garantir la santé de l'organisation.

Les risques



Santé

Les progrès des technologies de l'information, notamment l'utilisation d'ordinateurs de poche, ont rendu nécessaire le partage électronique de données médicales et de renseignements sur les patients. La sécurité devient alors un enjeu majeur.

Aux États-Unis, la loi HIPAA (Health Insurance Portability & Accountability Act), relative à la transférabilité de l'assurance maladie et à la responsabilité des assureurs, de 1996 a été instaurée par le gouvernement fédéral pour contraindre toutes les organisations de soins de santé à appliquer des pratiques de gestion des données standardisées afin de protéger les informations des patients ainsi que leur vie privée en toute circonstance. Cette loi exige l'utilisation d'une piste de vérification pour identifier les personnes qui consultent les données, la date de la consultation et déterminer si elles possèdent les autorisations adéquates.

La loi HITECH (Health Information Technology for Economic and Clinical Health Act), relative aux technologies de l'information de la santé, a considérablement intensifié les efforts du gouvernement des États-Unis pour l'instauration d'un système national de gestion des dossiers médicaux électroniques destiné au secteur de la santé. La loi HITECH a été promulguée dans le cadre de l'American Recovery and Reinvestment Act de 2009 pour promouvoir l'adoption et l'utilisation appropriée des technologies d'information de santé.

Le non-respect de la loi HIPAA peut entraîner des sanctions pénales ou civiles, même en l'absence d'infraction.

Administrations

Aujourd'hui, les administrations fédérales, des états et locales mettent l'accent sur la simplification des processus et l'amélioration de la collaboration entre organismes afin de fournir un service de meilleure qualité à leurs administrés. Pour ce faire, elles lancent diverses initiatives afin de tirer parti des toutes dernières technologies tout en mettant en place des réglementations strictes pour garantir la sécurité des informations partagées. On peut citer pour exemple la loi relative aux violations de données de l'état du Massachusetts, l'une des plus agressives du pays. Les systèmes, logiciels et services Xerox® respectent ces directives strictes ainsi que d'autres.

En 2014, le Département de la Défense américain (U.S. Department of Defence) a adopté les normes 800-53 du NIST, l'Institut national des normes et de la technologie (National Institute of Standards and Technology). Ces normes recommandent des contrôles de sécurité pour les systèmes d'information fédéraux et les organisations et documente les contrôles de sécurité pour tous les systèmes d'information fédéraux à l'exception de ceux destinés à la sécurité nationale.

1. 2015 Cost of Data Breach Study: Global Analysis, IBM etPonemon Institute, Mai 2015.

Vulnérabilités de sécurité : Risques du secteur et coûts

Le Département de la Défense a également adopté des mesures de sécurité avec l'utilisation des cartes CAC (Common Access Cards, cartes d'accès commun) et leur équivalent pour les administrations civiles, les cartes PIV (Personal Identity Verification, vérification d'identité personnelle). Ces cartes nécessitent une infrastructure PKI (infrastructure à clé publique) pour assurer un environnement d'authentification et de communication sécurisé. De plus, la plupart des agences du gouvernement fédéral ont adopté la norme FIPS 140-2 pour certifier les modules de cryptage utilisés dans les imprimantes et les multifonctions. Enfin, de nombreux clients du gouvernement fédéral exigent des produits certifiés conformes à la norme Critères communs.

Services financiers

Les services de dépôt direct, de banque en ligne, de cartes de débit et autres progrès des technologies de l'information révolutionnent le secteur des services financiers. Bien qu'elle soit plus pratique pour les clients et les entreprises, cette utilisation massive de technologies pose ses propres problèmes de sécurité.

L'échange sécurisé d'informations de carte de crédit est vital et le respect des normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS) permet de limiter les vulnérabilités et de protéger les données des détenteurs de cartes. La norme PCI DSS est une norme de sécurité de l'information exclusive des organisations qui utilisent des cartes de crédit, notamment Visa®, Mastercard®, American Express®, Discover® et JCB.

La GLBA (Gramm-Leach-Bliley Financial Services Modernisation Act), la loi de modernisation des services financiers de 1999, a été instaurée afin de garantir que les institutions financières qui collectent ou reçoivent des données privées de clients disposent d'un plan de sécurité adéquat pour les protéger. Pour être en conformité, les organisations doivent réaliser une analyse de risque sur leurs processus courants et mettre en œuvre des parefeu, restreindre l'accès des utilisateurs, surveiller l'impression, et plus encore.

La loi Dodd-Frank relative à la réforme de Wall Street et à la protection des consommateurs (Wall Street Reform and Consumer Protection Act) de 2010 renforce la nécessité de procéder à la collecte et à la communication des données financières de manière précise. Le Bureau de recherche financière (Office of Financial Research) et les agences membres sont chargés de collecter et d'analyser les données afin d'identifier et surveiller les risques émergents pour l'économie et de rendre ces informations publiques par le biais de rapports périodiques et d'une présentation annuelle au Congrès.

Éducation

Aujourd'hui, dans la plupart des établissements d'enseignement – du primaire à l'université – il est possible d'effectuer en ligne toutes sortes de démarches : demandes de relevé de notes, demandes de bourses et même consultation des notes de cours. De plus, les établissements qui disposent de leur propre centre médical doivent également stocker et partager des informations médicales sous forme électronique. Cet environnement interactif améliore l'expérience des étudiants et augmente la productivité du personnel, mais il rend dans le même temps les établissement d'enseignement vulnérables aux attaques de sécurité.

Comme ces institutions gèrent des données variées, elles sont soumises à de nombreuses réglementations fédérales et des états, telles que la loi relative à la fraude et à la malveillance informatique (Computer Fraud and Abuse Act), le USA Patriot Act ou encore les lois HIPAA et GLBA. Toutefois, la principale réglementation applicable au secteur de l'éducation reste la FERPA (Family Education Rights and Privacy Act), la loi relative aux droits à l'instruction et à la protection de la vie privée des familles. Cette loi interdit la divulgation de renseignements personnels d'éducation sans l'autorisation écrite de l'étudiant ou de son responsable légal.

Face à cette multitude d'obligations réglementaires et de conformité que doivent respecter les établissements d'enseignement, Xerox a pris comme lignes directrices les exigences du gouvernement fédéral, entre autres. En développant des solutions visant à respecter les normes de sécurité les plus strictes, nous pouvons offrir à tous nos clients, quel que soit leur secteur d'activité, des solutions extrêmement sûres.

Présentation de la sécurité

Chez Xerox, notre philosophie « Sécurité = Sûreté » guide le développement de produits, services et technologies qui intègrent la sécurité à tous les niveaux.

La sécurité occupe une place prépondérante quand il s'agit de concevoir nos « multifonctions intelligents ». En tant que chef de file du développement des technologies numériques, Xerox a montré son engagement en faveur de la sécurité et de la protection des informations numériques en identifiant les vulnérabilités potentielles et en les traitant de manière proactive afin de limiter le risque. Les clients ont été réceptifs à cette démarche et considèrent Xerox comme un fournisseur de confiance proposant des solutions sécurisées qui offrent de nombreuses fonctions de sécurité de pointe, en standard et en option.

Notre stratégie de sécurité

Le développement des produits Xerox® s'effectue selon un processus de cycle de développement sécurisé qui tient compte des recommandations du modèle SAMM (Software Assurance Maturity Model) du projet OWASP (Open Web Application Security Project) et du SANS Institute. Le processus consiste à définir des exigences de sécurité, à évaluer les risques, à analyser les vulnérabilités et à réaliser des tests d'intrusion. Nous utilisons également les informations émanant du projet OWASP et du SANS Institute. Cette stratégie comporte trois éléments clés :

Fonctions de sécurité de pointe

Les imprimantes et les imprimantes multifonctions constituent des plateformes sophistiquées, comportant de nombreux sous-systèmes. Xerox propose la gamme de fonctions de sécurité la plus vaste de marché, telles que cryptage, authentification, autorisation par utilisateur et audit.

Certification

Les Critères communs d'évaluation de la sécurité des technologies de l'information (ISO 15408) constituent la seule norme internationalement reconnue pour la certification de sécurité. Xerox a été le premier fabricant à demander et à obtenir la certification des périphériques pour l'ensemble de leurs composants. Parce que chaque élément de la plateforme multifonctions est un point d'entrée potentiel, une certification efficace doit englober tous les éléments, y compris les systèmes d'exploitation, l'interface réseau, les unités de disques, le serveur Web, les interpréteurs PDL, l'interface utilisateur du multifonction, les ports matériels locaux et le système de télécopie.

Maintenance

Chez Xerox, pour préserver la sécurité de nos imprimantes et de nos multifonctions tout au long de leur vie utile, nous devons veiller à assurer une protection constante contre les exploits nouvellement découverts. Nous y parvenons grâce à :

- la publication régulière de mises à jour logicielles ;
- la notification des nouveaux bulletins de sécurité via des fils RSS ;
- la réponse aux vulnérabilités identifiées ;
- la fourniture de recommandations d'installation et de fonctionnement sécurisés ;
- la fourniture d'informations sur les critères communs ;
- la mise à disposition de correctifs sur le site www.xerox.com/security

Le modèle de sécurité Xerox, associé au cycle de développement sécurisé, est la garantie que toutes les fonctionnalités et les fonctions du système sont protégées et sûres.

Une approche globale de la sécurité des imprimantes et des multifonctions

Xerox a très tôt compris et intégré cette migration technologique ainsi que les nouveaux besoins des lieux de travail. Nous proposons une gamme complète de fonctionnalités de sécurité afin de préserver vos imprimantes/multifonctions et vos données. Xerox sécurise toutes les étapes de la chaîne de données, y compris l'impression, la copie, la numérisation, le téléchargement de fichiers et le logiciel système. Notre approche à plusieurs niveaux comporte quatre aspects principaux.

1. Prévention des intrusions

Votre première vulnérabilité et la plus manifeste réside dans l'interface utilisateur - qui dispose d'un accès physique à votre imprimante et à ses fonctionnalités. L'authentification de l'utilisateur est l'option de base pour permettre l'accès aux imprimantes et aux multifonctions Xerox® aux utilisateurs réseau ou locaux autorisés. Une fois authentifié, l'utilisateur peut interagir avec le périphérique ou accéder aux données client selon le rôle qui lui est attribué. Les imprimantes et multifonctions Xerox® mettent en œuvre diverses technologies pour garantir que seuls les utilisateurs et autres périphériques réseau autorisés accèdent aux fonctionnalités et aux fonctions du périphérique. Nous abordons ensuite des points d'intrusion moins manifestes - ce qui est envoyé vers l'imprimante et de quelle façon. La technologie Xerox® ConnectKey® intercepte les attaques issues de fichiers corrompus et de logiciels malveillants. Notre logiciel système, y compris les DLM et les weblets, comporte une signature numérique : toute tentative d'installation de versions infectées ne comportant pas de signature provoquera le rejet automatique du fichier. Les fichiers d'impression seront également supprimés si l'un de leurs éléments n'est pas reconnu comme légitime.

AUTHENTIFICATION RÉSEAU

L'authentification réseau permet aux utilisateurs de s'authentifier sur le périphérique en validant leur nom d'utilisateur et leur mot de passe avant utilisation. Cette fonction l'accès à un ou plusieurs des services suivants : Impression, Copie, Fax, Fax serveur, Réimpression de travaux enregistrés, Courrier électronique, Fax Internet et Serveur de flux de numérisation. Les utilisateurs peuvent également être autorisés à accéder à un ou plusieurs des menus suivants : Services, État des travaux ou État machine.

1. Prévention des intrusions

Empêche l'accès général aux périphériques via le contrôle d'accès des utilisateurs et le parefeu interne de l'imprimante.

2. Détection des programmes malveillants sur le périphérique

Soyez alerté au démarrage ou à la demande en cas de détection de modifications sur votre périphérique.

3. Protection des documents et des données

Assure la protection des données personnelles et confidentielles via le cryptage (AES 256 bits, FIPS validé sur de nombreux produits) et le nettoyage du disque dur.

4. Partenariats externes

Protection de vos données et de vos périphériques contre toute intrusion malveillante grâce à la technologie de liste blanche (« whitelisting ») de McAfee, à l'intégration du moteur de services d'identité Cisco® ISE (Identity Services Engine), organismes de certification et organisations de tests de conformité.

MICROSOFT® ACTIVE DIRECTORY® SERVICES

La fonction ADS (Microsoft Active Directory Services) permet au périphérique d'authentifier les comptes utilisateurs par rapport à une base de données centralisée plutôt que par rapport à la base de données de comptes utilisateurs gérée en local sur le périphérique.

AUTHENTIFICATION LDAP

L'authentification LDAP (BIND) est prise en charge et permet de rechercher des informations sur les serveurs LDAP et d'y accéder. 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 de la session.

AUTHENTIFICATION SMTP

Cette fonction vérifie le compte de messagerie de l'utilisateur et empêche les utilisateurs non autorisés d'envoyer des courriers électroniques depuis le périphérique. Les administrateurs système peuvent activer le protocole TLS pour toutes les opérations de réception et d'envoi.

Présentation de la sécurité

AUTHENTIFICATION POP3 AVANT SMTP

Pour fournir un niveau supplémentaire de sécurité, les multifonctions Xerox® permettent aux administrateurs système d'activer ou de désactiver l'authentification POP3 avant la fonction SMTP. Lorsque ce mode d'authentification est activé, une connexion réussie à un serveur POP3 est nécessaire pour pouvoir envoyer des courriers électroniques via SMTP.

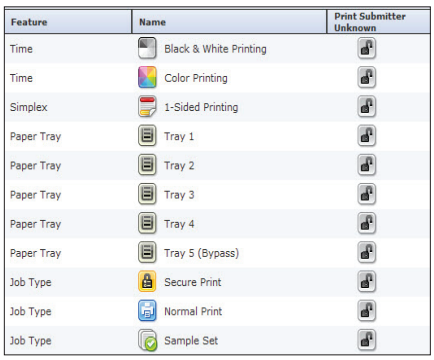
CONTRÔLE DE L'ACCÈS PAR RÔLE

La fonction de contrôle de l'accès par rôle permet d'attribuer aux utilisateurs authentifiés l'un des rôles suivants : Utilisateur non connecté/Utilisateur connecté, Administrateur système ou Administrateur de comptes. Chaque rôle est associé à des privilèges correspondant à divers niveaux d'accès aux fonctions, aux travaux et aux attributs de file d'impression ce qui permet aux administrateurs de choisir précisément les fonctions qui peuvent être utilisées par chaque rôle. Lorsqu'un utilisateur se connecte au périphérique au moyen de son nom d'utilisateur et de son mot de passe, le périphérique détermine les rôles qui lui sont affectés et les restrictions qui s'appliquent en fonction de ces rôles. En cas d'interdiction d'accès à l'intégralité d'une fonction, la fonction est verrouillée sur l'interface utilisateur ou n'apparaît pas du tout après authentification de l'utilisateur.

Utilisateur non connecté/Utilisateur connectéconnecté	Administrateur systèmesystème	Administrateur de comptes

AUTORISATIONS UTILISATEUR

Les autorisations utilisateur permettent de restreindre l'accès aux fonctions d'impression par utilisateur, par groupe, par plage horaire ou par application. Les utilisateurs et les groupes peuvent être définis avec divers niveaux d'accès aux fonctions d'impression. Par exemple, des limites peuvent être définies pour n'autoriser les travaux d'impression couleur qu'à certaines heures de la journée, pour que les présentations Microsoft® PowerPoint® soient automatiquement imprimées en mode recto verso ou pour que les courriers électroniques Microsoft® Outlook® soient toujours imprimés en noir et blanc.



Pour définir les autorisations d'utilisateur pour la couleur et d'autres restrictions d'impression, vous disposez d'interfaces graphiques intuitives.

AUTHENTIFICATION PAR CARTE À PUCE

Également appelée authentification par carte sans contact ou carte de proximité, l'authentification par carte à puce protège vos imprimantes et vos multifonctions de toute accès non autorisé sur la machine même. Les périphériques Xerox® prennent en charge la plupart des cartes à puce (CAC/PIV, .NET, Rijkspas et autres), une trentaine de types de lecteurs de carte et 65 modèles de carte de proximité. L'authentification par carte à puce utilise un système d'identification à deux facteurs pour authentifier les utilisateurs et leur permettre d'accéder aux fonctions du périphérique sur la machine ou sur le réseau : la possession de la carte et un numéro d'identification personnel à entrer dans l'interface du périphérique.

Les cartes CAC (Common Access Card, carte d'accès commun) et PIV (Personal Identity Verification, vérification d'identité personnelle) sont utilisées par le Département de la Défense américain pour l'identification du personnel militaire en service actif, des troupes de réserve, du personnel civil du DoD et d'autres organismes non-gouvernementaux et du personnel contractuel admissible. Elles peuvent également être utilisées pour l'accès aux bâtiments et pour l'authentification des ordinateurs personnels, en plus des imprimantes/périphériques et des réseaux qui les connectent.

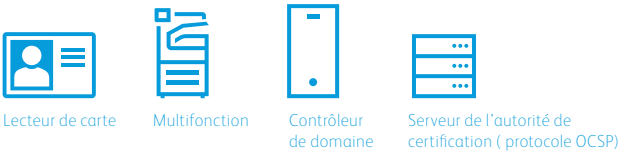
Présentation de la sécurité

La carte CAC/PIV 144k est une version de la carte à puce. Elle utilise un système d'identification à deux facteurs pour authentifier les utilisateurs qui veulent accéder aux services directement sur le périphérique.

La carte CAC/PIV 144k offre les avantages suivants :

- Cryptage S/MIME des numérisations vers courrier électronique à destination d'un utilisateur figurant dans le carnet d'adresses local du multifonction ou le carnet d'adresses LDAP général
- Signature numérique au moyen du certificat de signature de courrier électronique enregistré sur la carte de l'utilisateur
- Renseignement automatique du champ « À » lors de l'utilisation de la fonction de numérisation vers courrier électronique du périphérique
- Clé de certificat de 2 048 bits
- Restriction des transmissions sortantes aux destinataires possédant des certificats valides
- Rapports de confirmation de courrier électronique et journal d'audit
- Connexion unique à Numérisation vers un répertoire principal et LDAP

Schéma de configuration Carte d'accès commun (CAC) / Carte de vérification d'identité personnelle (PIV)

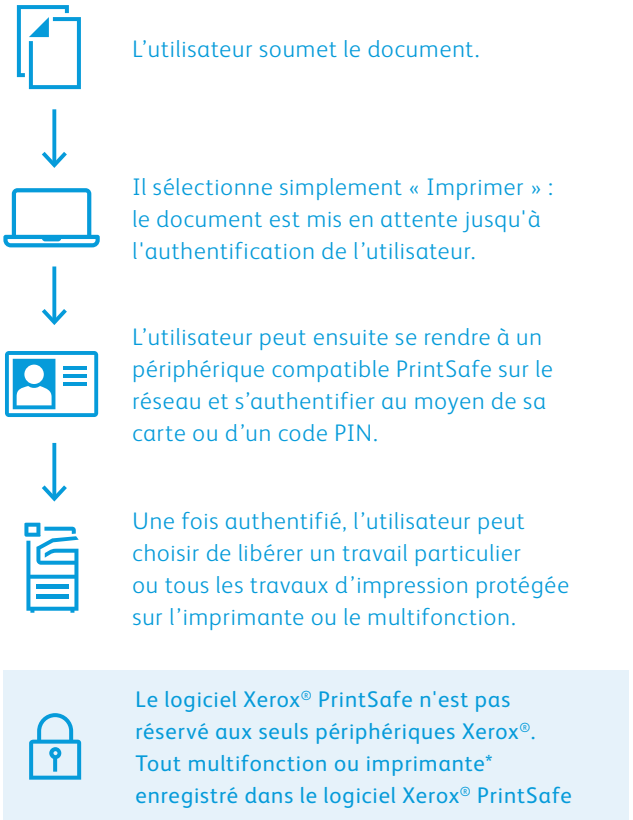


1. L'utilisateur introduit sa carte dans le lecteur. Il est invité à entrer un code PIN sur le périphérique.
2. Le périphérique se connecte au serveur OCSP pour vérifier que le certificat correspondant à la carte est toujours valide puis il confirme la « chaîne de confiance » à une autorité de certification connue.
3. Le périphérique initie un dialogue crypté de questions/réponses entre le contrôleur de domaine et la carte d'accès commun. S'il est concluant, le contrôleur de domaine émet un ticket initial («Ticket Granting Ticket ») qui valide l'autorisation.
4. L'autorisation déverrouille les fonctions suivantes accessibles directement depuis le périphérique :
   - Numérisation vers un courrier électronique :
   - Copie
   - Télécopie
   - Services personnalisés
   - Numérisation de flux de travail

LOGICIEL XEROX® PRINT SAFE

Avec le logiciel Xerox® PrintSafe, il est possible d'authentifier les données d'impression de façon sécurisée sur toutes les imprimantes et tous les multifonctions, notamment sur les périphériques Xerox® et ceux d'autres fabricants. Ce logiciel ouvert est compatible avec une grande variété de lecteurs et cartes standards.

Flux d'impression flexibles, pratiques et sécurisés



Le logiciel Xerox® PrintSafe n'est pas réservé aux seuls périphériques Xerox®. Tout multifonction ou imprimante* enregistré dans le logiciel Xerox® PrintSafe

Des flux de travail flexibles permettent à l'utilisateur de charger un logiciel d'impression directe sur son client PC ou sur un serveur d'impression existant, qu'il est ensuite facile de configurer pour le logiciel Xerox® PrintSafe.

*Les périphériques non Xerox® nécessitent un accessoire réseau ; consultez votre commercial Xerox pour connaître les marques et modèles pris en charge.

INTERFACE UTILISATEUR ET ACCÈS ÀDISTANCE À L'INTERFACE UTILISATEUR

Afin de protéger les informations de configuration du périphérique, l'administrateur système peut verrouiller l'accès aux écrans de configuration pour les utilisateurs non autorisés depuis le panneau de commande et depuis l'utilitaire Interface utilisateur à distance.

2. Détection des programmes malveillants sur le périphérique

Dans le cas peu probable que les défenses de vos données et de votre réseau soient contournées, la technologie Xerox® ConnectKey® réalisera un test complet de vérification du microprogramme, au moment du démarrage* ou après activation par des utilisateurs autorisés. Ce test vous alerte dès qu'il détecte des modifications de votre multifonction. En cas d'anomalies, le périphérique affiche un message invitant l'utilisateur à recharger le microprogramme. Nos solutions intégrées les plus avancées utilisent la technologie McAfee® d'accréditation (ou « whitelisting », liste blanche)** qui réalise un contrôle permanent et empêche automatiquement toute exécution de logiciel malveillant.

En collaboration avec Cisco, Xerox a mis en œuvre le profilage des périphériques dans Cisco® Identity Services Engine (ISE). L'intégration avec Cisco® Identity Services Engine (ISE) permet de détecter automatiquement les périphériques sur le réseau et de les placer dans la catégorie Imprimantes pour l'application de la politique de sécurité et son respect.

Pour en savoir plus, reportez-vous aux Livres blancs suivants :

McAfee Whitelisting White Paper (an anglais seulement) :
http://www.office.xerox.com/latest/SECWP-03.PDF

Cisco ISE White Paper (en anglais seulement) :
http://www.office.xerox.com/latest/SECWP-04.PDF

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

3. Protection des documents et des données

Protection des documents

Même lorsque toutes les mesures de sécurité réseau nécessaires sont en place pour protéger efficacement les données critiques lors de leur acheminement entre les ordinateurs des utilisateurs et les périphériques d'impression de bureau, les technologies de sécurité doivent également assurer la protection de vos documents papier qui ne doivent être accessibles qu'aux seuls destinataires prévus. Xerox met en œuvre des technologies de pointe pour protéger vos documents, qu'il s'agisse d'impressions papier ou de documents électroniques à distribuer.

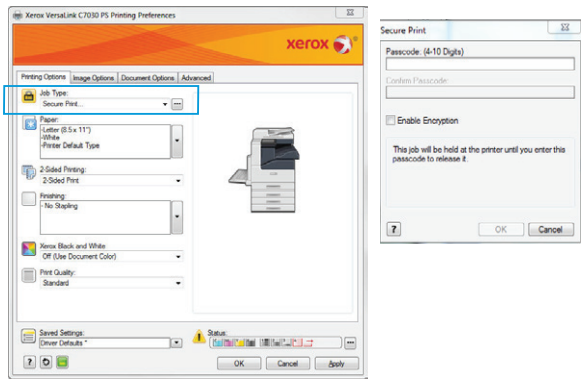
CRYPTAGE DES DONNÉES DE NUMÉRISATION

Les utilisateurs de multifonctions intelligents Xerox® ConnectKey® des gammes i-Series, VersaLink® et AltaLink® ont également la possibilité de crypter les fichiers PDF et de les protéger par mot de passe lorsqu'ils utilisent Le service Numérisation vers courrier électronique.

- Protection au-delà du parefeu
  - Protection des données dans un environnement non sécurisé
  - Utilisation des protocoles standards tels que SSL et Secure PDF

CRYPTAGE DES FLUXD 'IMPRESSION

Les pilotes Xerox® Global Print Driver® et les pilotes des produits prennent désormais en charge le cryptage des documents lors de la soumission de travaux d'impression protégée aux périphériques ConnectKey. Les imprimantes multifonctions Xerox® AltaLink et i-Series prennent également en charge le cryptage pour les travaux d'impression standards. Aucun matériel supplémentaire n'est requis.



IMPRESSION PROTÉGÉE

Les travaux d'impression confidentiels sont conservés jusqu'à ce que le propriétaire du document les libère en saisissant son code PIN unique sur l'interface utilisateur du périphérique. Ceci garantit que le destinataire du document est physiquement présent lors de l'impression d'informations confidentielles et peut retirer les impressions de l'imprimante ou du multifonction avant que d'autres utilisateurs du périphérique y aient accès.

L'impression protégée basée sur les technologies CAC (carte d'accès commun)/PIV (vérification d'identité personnelle) joint le certificat d'identité de l'expéditeur au travail d'impression. Au périphérique, l'utilisateur doit s'authentifier au moyen de la carte CAC/PIV avant de pouvoir libérer le travail.

PDF CRYPTÉ/PDF PROTÉGÉ PAR MOT DE PASSE

Lors de la numérisation d'un document papier pour distribution électronique via la fonction Numérisation vers courrier électronique, les multifonctions Xerox® peuvent créer des fichiers PDF cryptés AES 128 bits ou 256 bits ou des fichiers PDF protégés par mot de passe. Ces fichiers sont ensuite transmis en toute sécurité sur le réseau et peuvent être ouverts, imprimés ou modifiés uniquement par les utilisateurs en possession du mot de passe correct.

TRANSFERT DE FAX VERS UN COURRIER ÉLECTRONIQUE ET VERS LE RÉSEAU

Les multifonctions Xerox® dotés de la fonction de transfert de fax peuvent acheminer les télécopies entrantes vers les boîtes de réception des destinataires spécifiés et/ou vers un référentiel réseau, dans lesquels ils seront accessibles aux seuls utilisateurs autorisés.

CONFIRMATION DE DESTINATION DEZ FAX

L'expéditeur d'un fax reçoit une confirmation automatique de réception de son fax par le destinataire.

Présentation de la sécurité

SIGNATURES NUMÉRIQUES

Une signature numérique utilise une fonction mathématique pour démontrer l'authenticité d'un message ou d'un document numérique. Elle permet de protéger le microprogramme du périphérique contre les modifications non détectées et fournit un moyen d'authentifier l'origine des données. Avec les cartes à puce, les courriers électroniques peuvent être signés avec le certificat de l'expéditeur. Une signature numérique valide est la garantie pour le destinataire que le message a été rédigé par un expéditeur connu et qu'il n'a pas été altéré lors de son acheminement.

FILIGRANES SÉCURISÉS

Certains multifonctions et imprimantes Xerox® proposent une fonction de filigrane sécurisé qui empêche la reproduction des impressions originales contenant des informations sensibles. Si un document avec un filigrane sécurisé est copié, l'image du filigrane devient visible, indiquant que le document contient des informations sensibles et a été copié illégalement.

MARQUE UTILISATEUR/HEURE/DATE

Les pilotes Xerox® permettent d'apposer un tampon utilisateur/heure/date sur les documents imprimés sur un périphérique réseau. Cette fonction fournit une piste d'audit et permet de savoir qui imprime quoi et à quelle heure.

FILTRAGE DES ADRESSES IP

Le filtrage IP permet aux administrateurs système de créer des règles d'acceptation ou de rejet des informations entrant sur le multifonction en fonction des adresses IP ou des plages d'adresses IP spécifiées. Cette fonction permet à l'administrateur système de contrôler qui peut accéder ou non au périphérique.

Adresses IP enregistrées :
Disponible

Adresses IP non enregistrées :
Non disponible

SSL (SECURE SOCKETS LAYER) / TLS (TRANSPORT LAYER SECURITY)

De nombreuses organisations doivent respecter des politiques de sécurité qui exigent que toutes les transactions entre le client et l'imprimante ou le multifonction s'effectuent de manière sécurisée via des transactions Web sécurisées, des transferts de fichier sécurisés et des courriers électroniques sécurisés. Les données transmises sur le réseau sans être cryptées peuvent être lues par tout programme « reniflant » le réseau. Xerox limite ce risque en utilisant les protocoles SSL et TLS pour les transmissions de données via certains protocoles tels que HTTPs et IPP.

CRYPTAGE IPSEC

Le protocole IPsec (Internet Protocol Security) sécurise toutes les communication au niveau de la couche IP et s'utilise principalement pour crypter les soumissions d'impression au périphérique. Il crypte tout le trafic entre un point A et un point B de manière à ce que seuls les utilisateurs de confiance peuvent envoyer et recevoir les informations, à ce que les données ne soient pas altérées pendant leur transmission et à ce que seuls les utilisateurs autorisés puissent recevoir et lire les informations.

IPsec est conçu pour fournir les services de sécurité suivants :

- Cryptage du trafic (pour empêcher toute lecture de communications privées par des parties non concernées)
- Vérification de l'intégrité (pour garantir que le trafic n'a pas été modifié en cours d'acheminement)
- Authentification des pairs (pour garantir que le trafic provient d'un tiers de confiance)
- Anti-réitération (pour éviter que la session sécurisée ne soit réitérée)

ACTIVATION/DÉSACTIVATION DES PORTS RÉSEAU

La fonction d'activation / désactivation des ports réseau permet de désactiver les ports et les services superflus pour prévenir tout accès non autorisé ou malveillant. Sur les petits périphériques de bureau, ces options peuvent être réglées sur le panneau de commande ou via un logiciel de configuration installé sur PC. Sur les multifonctions plus importants, des outils sont fournis pour définir les niveaux de sécurité et désactiver des ports et des services spécifiques.

Présentation de la sécurité

CERTIFICATS NUMÉRIQUES

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

Les multifonctions peuvent ajouter des signatures numériques qui vérifient la source et l'authenticité d'un document PDF. Lorsque les destinataires ouvrent un fichier PDF enregistré avec une signature numérique, ils peuvent visualiser les propriétés du document pour vérifier le contenu de la signature, notamment l'autorité de certification, le nom de produit du système, le numéro de série et l'heure et la date à laquelle il a été créé. Si la signature est une signature de périphérique, elle contient également le nom du périphérique qui a créé le document, tandis qu'une signature d'utilisateur indique l'identité de l'utilisateur authentifié qui a envoyé ou enregistré le document.

Un certificat signé par une autorité de certification telle que VeriSign peut être chargé sur les multifonctions Xerox®. Votre administrateur système peut également créer un certificat auto-signé sur le périphérique. En configurant un certificat sur votre périphérique, vous pouvez activer le cryptage pour des types de flux de travail spécifiques.

SNMPV3

Le protocole SNMP (Simple Network Management SNMP) est un protocole Internet standard qui permet de gérer les périphériques sur les réseaux IP. Il renforce la sécurité en protégeant les données de toute falsification, en utilisant l'authentification pour limiter l'accès aux seuls utilisateurs autorisés et en cryptant les données envoyées sur le réseau.

Les périphériques qui prennent en charge le protocole SNMP incluent généralement des routeurs, des commutateurs, des serveurs, des postes de travail, des imprimantes, des modems et plus encore. Ce protocole est principalement utilisé dans les systèmes de gestion de réseau pour surveiller l'état des périphériques connectés au réseau nécessitant une intervention de l'administrateur. SNMP fait partie de l'Internet Protocol Suite tel que défini par l'IETF (Internet Engineering Task Force). Le protocole SNMPv3 fournit des fonctions de sécurité grandement améliorées notamment le cryptage des messages et l'authentification.

SNMP COMMUNITY NAME STRINGS

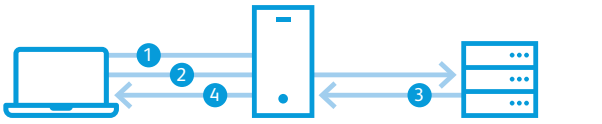
Les données MIB (Management Information Base) en lecture seule utilisent généralement la community string « public » et des community strings en lecture-écriture définies sur « private ». En utilisant des community name strings en lecture-écriture, une application peut modifier les paramètres de configuration du périphérique à l'aide de variables MIB. Les community name strings en lecture-écriture sur les périphériques Xerox® peuvent être modifiées par l'administrateur système pour renforcer la sécurité lors de la gestion des multifonctions via SNMP.

AUTHENTIFICATION 802.1X

IEEE 802.1X est une norme IEEE pour le contrôle d'accès réseau basé sur les ports (PNAC). Elle fait partie du groupe de protocoles réseau IEEE 802.1. Elle fournit un mécanisme d'authentification aux périphériques qui veulent se connecter à un réseau local (LAN) ou 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, douteux ou non gérés qui ne réussissent pas à s'authentifier d'accéder à votre réseau.

Fonctionnement - Authentification 802.1X

L'authentification 802.1X pour les réseaux LAN sans fil assure l'authentification centralisée, via un serveur, des utilisateurs finaux.



1. Un client envoie un message « start » à un point d'accès qui demande l'identité du client.
2. Le client répond au moyen d'un paquet de réponse contenant une identité ; le point d'accès transmet ce paquet au serveur d'authentification.
3. Le serveur d'authentification envoie une paquet « accept » au point d'accès.
4. Le point d'accès place le port client dans l'état autorisé et le trafic est autorisé.

Le protocole 802.1X est beaucoup plus répandu depuis que les réseaux sans fil ont gagné en popularité. De nombreuses organisations verrouillent l'accès aux ports de leurs réseaux internes au moyen de ce protocole. Ceci permet d'empêcher le passage des informations sur le réseau tant que le périphérique n'a pas été authentifié. D'un point de vue de la gestion des risques, ceci permet aux périphériques sans fil et aux périphériques filaires d'apporter une preuve de leur identité avant que toute information ne passe sur le réseau. En cas de tentative d'accès non autorisé, le port est verrouillé jusqu'à son déverrouillage par l'administrateur système.

Le protocole EAP (Extensible Authentication Protocol) est un référentiel d'authentification qui exécute sa fonction dans le cadre de l'authentification 802.1X. Les multifonctions Xerox® prennent actuellement en charge les types EAP suivants :

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

PAREFEU

Élément d'un système informatique ou d'un réseau, le parefeu est conçu pour protéger le périphérique des menaces externes et de tout accès non autorisé tout en permettant les communications autorisées. Le périphérique peut être configuré pour permettre ou refuser les transmissions réseau selon des règles définies ou d'autres critères. Les administrateurs réseau peuvent restreindre l'accès à des segments du réseau, à des services et aux ports des périphériques pour protéger les périphériques.

SÉPARATION ENTRE FAX ET RÉSEAU

Pour éliminer tout risque d'intrusion dans le réseau via la ligne de fax, il convient de séparer l'interface de télécopie du contrôleur réseau.

Le multifonction ne propose aucune fonction d'accès au réseau via la ligne de fax. Le protocole Fax Class 1 utilisé sur le multifonction répond uniquement aux commandes de télécopie qui autorisent l'échange de données de fax. Les données transmises depuis le PC client peuvent être uniquement des données d'image compressées accompagnées d'informations de destination. Toute autre donnée (telle que virus, code de sécurité ou code de contrôle accédant directement au réseau) est abandonnée à ce stade et le multifonction met immédiatement fin à l'appel. Ainsi, aucun mécanisme ne permet d'accéder au sous-système réseau via la ligne de fax.

Protection des données

Les technologies ont transformé la manière de travailler des employés. Aujourd'hui, les documents ne sont plus au seul format papier, comme les notes manuscrites ou les versions préliminaires des communications, mais aussi au format électronique, créés sur les bureaux d'ordinateur et dans les courriers électroniques. Comme la création, le stockage, le partage et la distribution de ces documents électroniques diffèrent de celles des documents papier, les données qu'ils contiennent peuvent être exposées à de nouveaux types de risque. Pour rester compétitive, une entreprise doit faire face à ces menaces en sécurisant ses documents et ses systèmes de gestion de documents qui contiennent ses ressources les plus importantes, ses connaissances.

Les systèmes de gestion des informations et des documents sont exposés à des risques de sécurité très variés : actes intentionnels d'espionnage, tels que piratage informatique, fraude, vol et sabotage d'équipements, ainsi que des actes non intentionnels tels que erreurs humaines ou catastrophes naturelles. La sécurité des informations va au-delà d'une simple protection. Elle consiste à assurer l'accès en temps utile aux documents ainsi que la disponibilité de leur contenu afin d'améliorer les processus métiers et les performances de l'entreprise. Elle implique également la gestion des contenus originaux et la conformité réglementaire.

Depuis l'introduction des premiers produits numériques, Xerox a reconnu le risque que des données conservées sur des dispositifs de stockage rémanent puissent être récupérées de manière illégale. C'est pourquoi nous avons intégré dans nos périphériques des fonctions et des contremesures qui permettent aux clients de protéger leurs données.

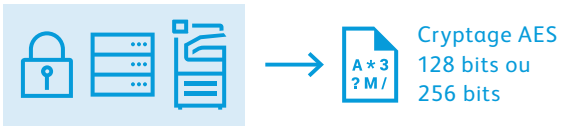
CRYPTAGE DES DONNÉES IMAGE

De nombreux périphériques Xerox® utilisent la technologie AES 128 bits ou 256 bits pour proposer des fonctions de cryptage des données (données de travaux, données image et données client) qui protègent les données résidant sur les multifonctions de tout accès non autorisé. Avec le cryptage des données, le disque est partitionné et seul la partition des 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 FIPS (Federal Information Processing Standard) 140-2
- Toutes les données image des utilisateurs résidant sur le disque dur sont cryptées

Présentation de la sécurité

AES est une norme de cryptage simple, rapide et difficile à casser, pouvant être mise en œuvre sur un grand nombre de périphériques ou d'applications. Elle allie, de manière inédite, sécurité, performance, efficacité, facilité de mise en œuvre et souplesse. De nombreux périphériques Xerox® peuvent être placés en mode FIPS 140-2. Dans ce cas, ils utiliseront uniquement les algorithmes de cryptage FIPS 140-2.



NETTOYAGE DU DISQUE DUR

Cette fonction efface les données image du disque dur de votre périphérique Xerox® lorsqu'elles ne sont plus nécessaires. Elle peut être exécutée automatiquement à la fin du traitement de chaque travail, programmée régulièrement ou effectuée à la demande de l'administrateur système. Les périphériques Xerox® proposent une fonction de nettoyage immédiat et de nettoyage à la demande.

MOIRE VOLATILE ET MÉMOIRE NON VOLATILE

Dans chaque multifonction Xerox®, le contrôleur inclut une mémoire volatile (RAM) et une mémoire non volatile (disque dur). Avec la mémoire volatile, toutes les données image sont perdues à la mise hors tension ou à la réinitialisation du système. Avec la mémoire non volatile, les données image sont généralement stockées dans la mémoire flash ou sur le disque dur du multifonction où elles sont conservées jusqu'à leur effacement.

Les clients, toujours plus soucieux de la sécurité de leurs données, veulent savoir comment et à quel niveau elles risquent d'être compromises. Les déclarations de volatilité sont des documents créés pour permettre de localiser les données image des clients sur les périphériques Xerox®. Elles décrivent les emplacements, les capacités et le contenu des dispositifs de mémoire volatile et de mémoire non volatile dans un périphérique Xerox® donné.

Ces déclarations de volatilité, disponibles pour de nombreux périphériques Xerox®, sont destinées aux clients soucieux de la sécurité et peuvent être obtenues auprès de votre équipe d'assistance Xerox locale (pour les clients existants), un commercial Xerox (pour les nouveaux clients) ou sur le site www.xerox.com/security.

FAX SÉCURISÉ

Les fax entrants confidentiels sont mis en attente jusqu'à leur libération par l'administrateur système.

PROTECTION PAR MOT DE PASSE DES NUMÉRISATIONS VERS BOÎTE AUX LETTRES

Lorsque vous utilisez la fonction Numérisation vers boîte aux lettres, vous pouvez protéger la boîte aux lettres désignée par un mot de passe afin que seuls les utilisateurs autorisés puissent accéder aux numérisations qu'elle contient. La sécurité de cette fonction est renforcée grâce au cryptage de la partition de données image du disque dur.

S/MIME POUR LES NUMÉRISATIONS VERS COURRIER ÉLECTRONIQUE

Le protocole S/MIME (Secure/Multipurpose Internet Mail Extensions) fournit les services de cryptage suivants à la fonction de numérisation vers courrier électronique : authentification, intégrité des messages et non répudiation de l'origine (au moyen de signatures électroniques), protection des données personnelles et sécurité des données (au moyen du cryptage).

Dans les communications S/MIME, lors de l'envoi des données, une signature est ajoutée dans chaque message électronique selon les informations de certification conservées sur le périphérique. Le cryptage est effectué lors de l'envoi des données en fonction du certificat correspondant à chaque adresse désignée du message électronique. Le certificat est vérifié lorsque les informations relative à la transmission des données sont entrées et au moment de l'envoi des données. La communication S/MIME n'est réalisée que lorsque la validité du certificat est confirmée.

CRYPTAGE DES NUMÉRISATIONS VERS COURRIER ÉLECTRONIQUE

Le cryptage des courriers électroniques via l'authentification par carte à puce permet aux utilisateurs d'envoyer jusqu'à 100 courriers électroniques cryptés à plusieurs destinataires figurant dans l'annuaire LDAP d'une entreprise en utilisant les clés publiques des destinataires. La plupart des multifonctions Xerox® utilisant l'authentification par carte à puce permettent également de signer électroniquement les emails. Les utilisateurs peuvent afficher les certificats des destinataires potentiels avant d'envoyer un courrier électronique. Le multifonction interdit l'envoi de messages aux utilisateurs ne possédant pas de certificat de cryptage. D'autre part, il consigne tous les enregistrements de courrier électronique, avec la possibilité, pour l'administrateur, de recevoir des rapports de confirmation.

MASQUAGE DU JOURNAL DES TRAVAUX

Lorsque cette fonction standard est activée, les travaux traités sur le périphérique ne sont pas visibles à l'utilisateur ni sur le périphérique ni sur l'interface à distance. Les informations contenues dans le journal des travaux sont également masquées mais sont accessibles à l'administrateur système, qui peut imprimer le journal pour connaître le nombre de travaux de copie, de télécopie, d'impression et de numérisation réalisés sur le périphérique.

Présentation de la sécurité

OFFRE DE CONSERVATION DU DISQUE DUR

Le service de conservation du disque dur proposé par Xerox s'adresse aux clients qui estiment que les données résidant sur le disque dur de leurs périphériques Xerox® sont confidentielles voire classifiées. Ce service payant permet aux clients de conserver les disques durs et de les nettoyer ou de les détruire selon la méthode qu'ils considèrent la plus sûre pour protéger leurs données image.

VALIDATION DES DONNÉES DE SERVICES DISTANTS

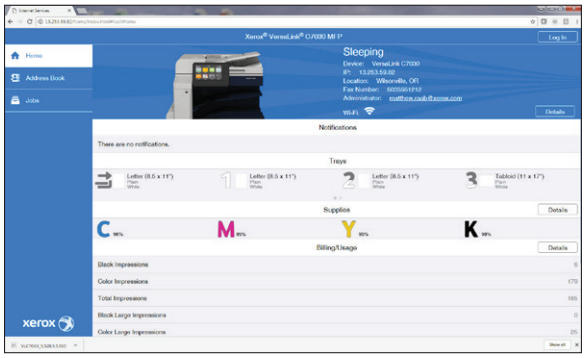
Sur de nombreux périphériques Xerox®, l'adhésion préalable du client est requise pour la transmission à Xerox d'informations personnelles identifiables et d'informations client identifiables dans le cadre des services distants.

MOTS DE PASSE POSTSCRIPT

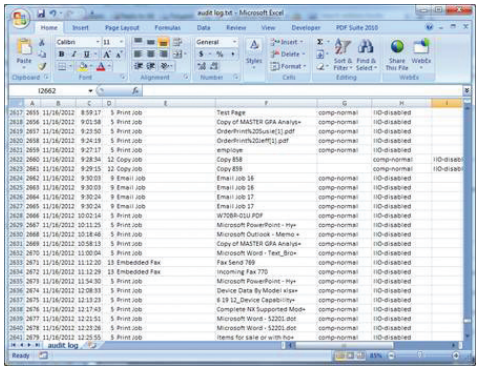
L'utilisation du langage de description de page (PDL) Adobe® PostScript® pour l'impression pose également un certain nombre de risques. PostScript inclut des commandes qui permettent aux travaux d'impression de changer les comportements par défaut du périphérique, ce qui expose le périphérique. Comme le langage PostScript comporte des fonctionnalités très puissantes pouvant être utilisées pour compromettre la sécurité du périphérique, les administrateurs peuvent configurer celui-ci de manière à ce que les travaux PostScript incluent obligatoirement 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 latitude pour contrôler le fonctionnement du sous-système PosScript.

LISTE DE CONTRÔLE

Sur les multifonctions Xerox® et nombre de nos imprimantes, des listes de contrôle permettent de suivre l'activité par document, utilisateur et fonction. Activée par défaut sur les modèles les plus récents, cette fonction peut être activée ou désactivée par l'administrateur système. Elle permet de suivre l'accès et les tentatives d'accès au périphérique et de transmettre ces informations à un système de gestion des informations et des événements de sécurité (SIEM) ou à un serveur de listes de contrôle. Exemple d'entrée de liste de contrôle : « L'utilisateur xx s'est connecté au multifonction Xerox® AltaLink® à 12h48 et a télécopié 10 pages à 888.123.1234. » Pour les imprimantes multifonctions Xerox® ConnectKey®, la liste de contrôle peut être automatiquement envoyée de manière sécurisée à un système SIEM afin d'assurer la surveillance en continu du multifonction.



L'accès à l'interface de liste de contrôle s'effectue depuis un poste de travail Administrateur système via un navigateur Web standard.



La liste peut ensuite être exportée dans un fichier .txt et ouverte dans Microsoft® Excel®.

4. Partenariats externes

Xerox travaille avec des organisations de tests de conformité et des entreprises leaders du marché comme McAfee afin de combiner leurs normes prépondérantes et leur savoir-faire aux nôtres. Les fonctions de protection contre les logiciels malveillants suivantes sont disponibles sur les multifonctions Xerox® ConnectKey® (Xerox® AltaLink® et i-Series).

MCAFEE® EMBEDDED CONTROL – ENHANCED SECURITY

Les multifonctions Xerox® dotés de la technologie Xerox® ConnectKey® intègrent le logiciel McAfee Embedded Control optimisé par Intel® Security, créant ainsi la toute première gamme d'imprimantes multifonctions capables de se protéger contre les menaces extérieures. La technologie McAfee d'accréditation (ou « whitelisting », liste blanche) envoie des alertes en cas de détection de tentatives non autorisées de lecture, écriture ou ajout exécutées sur les fichiers et répertoires protégés. D'autre part, l'intégration transparente avec le logiciel Xerox® CentreWare® Web, les outils Xerox® MPS et McAfee ePolicy Orchestrator® (McAfee ePO™) permet de surveiller les périphériques depuis la console de votre choix.

MCAFEE EMBEDDED CONTROL – INTEGRITY CONTROL

Le logiciel Integrity Control s'appuie sur les fonctionnalités de la solution Enhanced Security et empêche l'exécution de nouveaux fichiers par des moyens non fiables. Seule est autorisée l'exécution des logiciels approuvés, ce qui empêche toute attaque générale ou ciblée. Particulièrement utiles pour un déploiement au niveau de l'entreprise, les solutions de sécurité Xerox et Intel Security proposent des technologies de liste blanche qui garantissent que les périphériques exécutent uniquement les fonctions correspondant aux services que vous voulez fournir. Cette même technologie est utilisée pour protéger les serveurs, les distributeurs automatiques, les terminaux de paiement et les terminaux intégrés tels que les appareils mobiles.

MCAFEE EPOLICY ORCHESTRATOR (EPO)

McAfee's ePolicy Orchestrator (ePO) est un outil logiciel de gestion de la sécurité qui facilite la gestion des risques et de la conformité pour les organisations de toute taille. Les tableaux de bord avec fonction glisser-déposer fournissent à l'utilisateur des renseignements sur la sécurité des terminaux, des données, des équipements mobiles et des réseaux. Il bénéficie ainsi d'informations immédiatement exploitables qui permettent de réduire les délais de réponse. ePolicy tire parti des infrastructures IT existantes en connectant la gestion des solutions de sécurité McAfee et d'éditeurs tiers à LDAP, aux opérations IT et aux outils de gestion de configurations.

Afin d'attester de façon indépendante de notre excellent niveau de conformité, des organismes de certification tels que les Critères communs (ISO/ IEC 15408) et FIPS 140-2 mesurent nos performances par rapport aux normes internationales. Ils reconnaissent notre approche exhaustive en matière de sécurité des imprimantes.

INTÉGRATION DE CISCO® ISE (IDENTITY SERVICES ENGINE)

Cette plate-forme centralisée permet de gérer et de déployer les politiques de sécurité sur les imprimantes. Grâce à notre partenariat avec Cisco, nous disposons de plus grandes capacités de détection de périphériques Xerox®, et pouvons donc appliquer les politiques de sécurité de manière plus fine. Les périphériques Xerox® sont automatiquement reconnus et classés par CISCO ISE, ce qui permet un meilleur contrôle d'accès au réseau et une réduction des coûts généraux en éliminant la saisie manuelle des paramètres de sécurité des imprimantes. Notre profilage des imprimantes avec Cisco ISE empêche les tentatives d'usurpation d'identité par des saboteurs d'accéder sans entrave aux systèmes cruciaux. L'intégration des périphériques d'impression Xerox® avec Cisco ISE fournit une approche opérationnelle efficace pour atteindre les objectifs des politiques de sécurité.

Conformité réglementaire et respect des politiques

La conformité est importante sur les imprimantes et les multifonctions modernes en raison des données personnelles et confidentielles qu'ils doivent traiter et qu'ils conservent sur leur disque dur. La non-conformité peut entraîner la perte d'opportunités commerciales, de clientèle existante voire des actions en justice. Les niveaux de conformité requis varient en fonction du pays et du marché vertical.

La loi HIPAA (Health Insurance Portability & Accountability Act) aux États-Unis et la loi sur la protection des données (Data Protection Act) au Royaume-Uni sont des exemples de réglementations à respecter pour exercer une activité légalement.

La certification Critères communs est une norme de sécurité internationalement reconnue qui respecte les exigences du Département de la Défense américain.

Dotés de fonctions de sécurité de pointe et proposant une approche souple de la configuration et du déploiement, les périphériques Xerox® peuvent respecter toutes les normes et intègrent les contrôles nécessaires pour répondre à toutes les exigences.

Les systèmes, logiciels et services Xerox® répondent aux normes reconnues du secteur, ainsi qu'aux dernières réglementations officielles de sécurité en date. Nos produits proposent des fonctionnalités qui permettent à nos clients de respecter ces normes, dont voici quelques exemples :

- Normes de sécurité de l'industrie des cartes de paiement (PCI DSS) Version 3.0
- Sarbanes-Oxley
- Cadre de Bâle II
- Loi HIPAA (Health Insurance Portability and Accountability Act)
- Directive vie privée et communications électroniques (2002/58/CE)
- Loi GLBA (Gramm-Leach-Bliley Act)
- Loi FERPA (Family Educational Rights and Privacy Act)
- Loi HITECH (Health Information Technology for Economic and Clinical Health Act)
- Loi Dodd-Frank relative à la réforme de Wall Street et à la protection des consommateurs (Wall Street Reform and Consumer Protection Act)
- Critères communs pour l'évaluation de la sécurité des technologies de l'information ISO-15408
- Normes des systèmes de gestion de sécurité de l'information ISO-27001
- Objectifs de contrôle pour les technologies de l'information et les technologies connexes (normes COBIT)
- SAS 70 (Statement on Auditing Standards No. 70)
- NIST 800-53, adopté par le gouvernement fédéral et le DoD américains en 2014
- Programme FedRAMP (Federal Risk and Authorisation Program)

Évaluation de la sécurité des produits

La sécurité des documents est synonyme de tranquillité d'esprit. L'une des caractéristiques de la gamme de produits Xerox® est l'engagement pour la sécurité des informations. Les systèmes, logiciels et services Xerox® intègrent et respectent les normes reconnues du secteur, ainsi que les dernières réglementations officielles de sécurité.

Certification Critères communs

La Certification Critères communs est une évaluation indépendante et objective de la fiabilité, de la qualité et de la sécurité des produits informatiques. C'est une norme sur laquelle les clients peuvent s'appuyer pour prendre des décisions éclairées lors de l'achat de produits IT. Les Critères communs définissent des objectifs d'assurance spécifiques, notamment des niveaux très stricts d'intégrité, de confidentialité et de disponibilité pour les systèmes et les données, et de responsabilité au niveau individuel ainsi que l'assurance que tous les objectifs sont atteints. Aux États-unis, le gouvernement fédéral exige la certification Critères communs pour les dispositifs matériels et logiciels utilisés sur les systèmes de sécurité nationale.

Obtenir la certification Critères communs

L'obtention de la certification est soumise à un processus rigoureux d'évaluation de la sécurité des produits par un organisme tiers agréé par le programme NVLAP (National Voluntary Laboratory Accreditation Program). Les produits sont testés par rapport à des exigences fonctionnelles basées sur des niveaux d'assurance prédéfinis, les EAL (Evaluation Assurance Level) ou des exigences d'assurance spécialisées.

Dans les domaines de la santé, des services financiers et autres secteurs, la sécurité est tout aussi importante. Qu'il s'agisse de protéger la vie privée de leurs clients, ou des actifs financiers ou intellectuels, l'assurance que leurs réseaux, disques durs et lignes téléphoniques sont sûrs et protégés contre les piratages, les virus ou autres activités malveillantes est essentielle pour les entreprises. La certification Critères communs, bien qu'elle ne soit pas exigée en dehors du gouvernement fédéral, fournit une validation indépendante.

Avec environ 150 périphériques certifiés, Xerox propose l'une des gammes les plus larges de multifonctions certifiés Critères communs. Premier fabricant à certifier un périphérique dans son ensemble, Xerox est à ce jour le seul à systématiquement assurer cette certification.

Visitez le site www.xerox.com/information-security/common-criteria-certified pour consulter la liste des multifonctions Xerox® certifiés Critères communs.

Évaluation et atténuation des risques

Une sécurité proactive pour les risques émergents

Vous offrir les produits et les solutions les plus sécurisées du marché fait partie de notre mission. Nos chercheurs et nos ingénieurs travaillent d'arrache-pied pour développer une nouvelle génération de technologies de sécurité innovantes qui permettront de combattre les menaces de demain et de protéger la sécurité de vos documents : micro-impression, utilisation d'encres fluorescentes et infrarouges, technologies Xerox® Glossmark® et Correlation Marks, pour n'en citer que quelques-unes. Pour plus d'informations sur ces technologies, rendez-vous sur le site www.xerox.com/security.

D'autres choses que nous faisons chez Xerox :

Suivre de près l'évolution des questions de sécurité

Nous surveillons de près les centres d'échange d'informations sur les vulnérabilités afin de nous tenir informés des derniers développements en la matière, pour que vous n'ayez pas à le faire.

Publier des bulletins de sécurité

Nous adoptons une démarche proactive afin de vous fournir les correctifs de sécurité et les mises à jour nécessaires à la protection de votre équipement et de vos données.

Diffuser des fils RSS

Dès leur annonce, les dernières mises à jour sont distribuées automatiquement sur les lecteurs de flux RSS des clients.

Vous fournir une mine d'informations

Si vous voulez intensifier vos recherches personnelles sur la sécurité, nous vous proposons une bibliothèque en constante expansion d'articles, de livres blancs et de guides sur ce sujet.

Rendez-vous sur www.xerox.com/security pour accéder à toutes nos ressources de sécurité.

Outre nos tests exhaustifs réalisés en interne, Xerox surveille de près les centres d'échange d'informations sur les vulnérabilités mis en place par des entités telles que l'US-CERT et utilise les ressources publiées dans le domaine de la veille sécurité : mises à jour de patchs critiques Oracle® (Critical Patch Updates), bulletins de sécurité Microsoft® relatifs aux vulnérabilités de sécurité présentes dans divers logiciels et systèmes d'exploitation, liste de diffusion bugtraq, informations publiées sur les sites SANS.org et secunia.com pour les vulnérabilités open source. Un programme rigoureux de tests de sécurité interne a également été mis en place. Il implique l'analyse des vulnérabilités ainsi que des tests de pénétration destinés à fournir des correctifs intégralement testés. Rendez-vous sur le site www.xerox.com/security pour consulter notre politique de divulgation et de gestion des vulnérabilités.

Security Bulletins and Patch Deployment

Pour gérer les problèmes de sécurité, les développeurs Xerox suivent un cycle de développement formel comprenant les étapes suivantes : identification, analyse, priorisation, codage et 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 le produit, le correctif peut être déployé séparément ou prendre la forme d'une nouvelle version du logiciel du produit concerné.

Les clients peuvent télécharger les correctifs de sécurité destinés à certains produits Xerox® sur le site www.xerox.com/security. Pour les autres produits Xerox®, le correctif de sécurité sera intégré à une nouvelle version du logiciel système. Vous pouvez vous inscrire pour recevoir régulièrement ces bulletins. Aux États-unis, les clients peuvent s'inscrire aux fils RSS sur la sécurité. Hors des États-Unis, contactez votre centre d'assistance Xerox local.

Sur le site Web www.xerox.com/security, vous avez accès à des informations régulièrement mises à jour et à d'importantes ressources :

- Bulletins de sécurité
- RSS Feed: (Fils RSS :) Get Security Bulletins (Obtenir les bulletins de sécurité)
- FAQ sur la sécurité des produits Xerox
- Information Assurance Disclosure Papers
- Produits certifiés Critères communs
- Politique de divulgation et de gestion des vulnérabilités
- Conseils sur la sécurité des produits
- Articles et livres blancs
- Déclarations de volatilité
- Software Release Quick Lookup Table (Table de recherche rapide des versions logicielles)
- Guide FTC des copieurs et multifonctions numériques

Le portail www.xerox.com/security vous donne accès à un large éventail d'informations et de mises à jour de sécurité : bulletins, livres blancs, correctifs et bien plus encore.

Fabrication et Approvisionnement - Pratiques de sécurité

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

Xerox entretient également des relations contractuelles avec ses fournisseurs principaux et secondaires qui l'autorisent à réaliser des audits sur site afin de garantir l'intégrité de l'ensemble du processus, jusqu'au niveau des composants.

Xerox est également membre du programme C-TPAT, le partenariat douanes-commerce contre le terrorisme, dont l'objectif est d'assurer la sécurité de la chaîne d'approvisionnement. Citons comme exemples de pratiques adoptées par Xerox dans le cadre de ce programme, celles mises en place pour prévenir les vols ou attaques de véhicules. En Amérique du Nord, toutes les remorques circulant entre l'usine et les centres de distribution des produits (PDC) et entre les PDC et les centres logistiques des transporteurs sont scellées sur le lieu d'origine. Tous les camions sont équipés de localisateurs GPS et sont surveillés en continu.

Retours produits et mise au rebut

Service de conservation du disque dur pour les produits Xerox®

Ce service payant permet aux clients qui louent des produits Xerox® aux États-Unis de conserver le disque dur de leurs systèmes. Il s'adresse aux clients qui traitent des données confidentielles, voire classifiées, ou qui font l'objet de politiques internes ou de normes réglementaires qui exigent des processus particuliers de mise au rebut des disques durs.

Lorsqu'un client demande à bénéficier de ce service, un technicien de maintenance Xerox se rend sur son site, retire le disque dur de la machine et le remet en l'état à un représentant du client. Pour le moment, Xerox ne fournit pas de service de nettoyage, de désinfection ou de destruction de disque dur sur le site des clients. Ces derniers doivent prévoir les modalités appropriées de mise au rebut définitive du disque dur qui leur a été remis par le technicien.

Pour déterminer si votre produit Xerox® contient un disque dur ou vérifier les fonctions de sécurité disponibles pour protéger les données enregistrées sur le disque dur, rendez-vous sur le site www.xerox.com/harddrive.

Pour plus d'informations sur ce programme, contactez votre commercial Xerox ou rendez-vous sur le site www.xerox.com/security puis accédez à la section Articles and White Papers (Articles et livres blancs) dans la rubrique Security Resources (Ressources de sécurité).

En outre, la quasi-totalité des nouvelles imprimantes et imprimantes multifonctions Xerox® bénéficient en standard du cryptage du disque dur AES 256 bits, ainsi que du nettoyage du disque en 3 passages pour garantir la sécurité des données du client sur ses nouveaux équipements dès le premier jour.

Récapitulatif

La sécurité des réseaux et des données représente l'un des nombreux défis que doivent relever les entreprises au quotidien. Et comme les imprimantes et les multifonctions sont devenus des périphériques réseau essentiels dans l'entreprise, qui reçoivent et envoient des données importantes via de nombreuses fonctions, il est primordial d'assurer leur sécurité intégrale.

L'intégralité du système qui compose un multifonction, ainsi que tout logiciel de gestion de périphériques sur le réseau, doit être évalué et certifié pour que le service chargé de la sécurité de l'information et l'ensemble des collaborateurs d'une organisation soient certains que leurs documents et le réseau sont à l'abri des prédateurs, voire des failles de sécurité internes. À cet égard, les multifonctions Xerox® sont n°1 du secteur. Notre approche globale reposant sur une sécurité fondamentale, fonctionnelle, avancée et opérationnelle, est donc essentielle pour protéger les actifs informationnels de nos clients.

Conscient de cet enjeu, Xerox continue de développer et de concevoir tous ses produits de manière à garantir le niveau de sécurité optimal à tous les points de vulnérabilité possibles. Nous nous engageons à protéger vos données afin que vous puissiez vous concentrer sur les projets et les activités susceptibles d'assurer le succès de votre entreprise ou de votre organisation.

Pour plus d'informations sur les nombreux avantages offerts par Xerox en matière de sécurité, rendez-vous sur le site www.xerox.com/security.

Liste de contrôle de sécurité

Les responsables de la sécurité informatique sont déjà très occupés à gérer les exigences de sécurité. Les petites entreprises doivent s'appuyer sur des systèmes et des logiciels de sécurité efficaces pour faire la plupart du travail à leur place. Vous et votre personnel n'avez vraiment pas besoin d'activités à fort contenu humain ou d'interventions manuelles pour surveiller et mettre à jour chaque périphérique et flux de données de votre environnement, notamment vos multifonctions.

Un plan de sécurité réseau complet doit être tridimensionnel, chaque dimension ayant sa stratégie propre.

1. Périphériques résilients aux nouvelles attaques grâce à des fonctionnalités automatiques d'auto-protection
2. Conformité aux normes et réglementations de sécurité les plus récentes
3. Visibilité complète sur le réseau

La nouvelle norme de sécurité pour l'âge moderne

- La sécurité ne doit pas être pensée après coup.
- L'information constitue une propriété intellectuelle de plus en plus précieuse.
- Les parefeu ne suffisent pas ; les politiques de sécurité doivent être globales et omniprésentes.
- La protection des dispositifs intégrés fait aujourd'hui partie de l'impératif de sécurité.

Xerox propose une sécurité globale, à plusieurs niveaux, facile à déployer et à gérer, qui permet à votre entreprise de respecter les normes du secteur et les normes gouvernementales. La technologie Xerox® est testée et validée pour garantir la protection contre les accès, les données et les identités non autorisés .

Lorsque vous comparez les multifonctions Xerox® avec les produits d'autres fabricants, utilisez la liste de vérification ci-contre pour déterminer si les périphériques concurrents fournissent le même niveau de sécurité de bout en bout que les produits Xerox.

		Concurrent		
	Xerox	**1**	**2**	**3**
Filtrage des adresses IP/MAC	✓			
Cryptage IPsec	✓			
IPv6	✓			
Authentification 802.1X	✓			
Impression protégée	✓			
Cryptage des numérisations vers courrier électronique	✓			
PDF crypté/PDF protégé par mot de passe	✓			
Signatures numériques	✓			
Cryptage du disque dur AES 256 bits	✓			
Nettoyage du disque dur	✓			
Fax sécurisé	✓			
Blocage des ports	✓			
Protection par mot de passe des numérisations vers boîte aux lettres	✓			
Service de conservation du disque dur	✓			
Restrictions d'impression	✓			
Journal d'audit	✓			
Contrôle d'accès par rôle	✓			
Authentification par carte à puce	✓			
Carte d'accès commun/ Vérification d'identité personnelle	✓			
Permissions utilisateur	✓			
Certification Critères communs de l'intégralité du système	✓			
Intégration avec les outils de gestion réseau standard	✓			
Mises à jour de sécurité via des fils RSS	✓			
Protection McAfee intégrée optimisée par Intel® Security	✓			
McAfee® Integrity Control	✓			
Intégration de McAfee® ePolicy Orchestrator®	✓			
Intégration de Cisco® ISE (Identity Services Engine)	✓			

Pour en savoir plus, rendez-vous sur **www.xerox.com**.

05/18 BR21699 SECGD-01FC