Aperçu de la sécurité de Ricoh

RICOH
imagine. change.
imaginer. changer.

Vos appareils sont-ils vulnérables?

Les menaces informatiques ne sont plus limitées aux ordinateurs personnels, aux serveurs ou aux réseaux. Les appareils d'impression — même les simples imprimantes laser — doivent être protégés contre une vaste gamme de menaces. À mesure que les imprimantes multifonctions se sont transformées en de véritables terminaux informatiques, elles sont devenues des actifs essentiels des TI à part entière. La capacité informatique des appareils appelés traditionnellement « imprimantes et copieurs » a évolué, mais il en est de même pour les menaces potentielles, qui incluent notamment :

- L'accès malveillant par réseau
- L'exploitation et la modification de l'information sur le réseau
- Des fuites de l'information stockée sur DD ou autres médias de stockage
- L'accès non autorisé par le panneau de commande d'un appareil
- L'accès inadéquat par lignes de télécopieur
- Des fuites d'information au moyen de copies papier
- Des violations de politique de sécurité par inadvertance

Espérer simplement que vous ne serez pas atteint n'est pas une solution. La technologie, l'engagement et le savoir-faire de pointe sont essentiels. Ricoh peut vous aider à surmonter des problèmes potentiels causés par les points vulnérables de vos appareils, des données qu'ils traitent ou des réseaux auxquels ils sont connectés.

L’approche multidimensionnelle de Ricoh

Notre modèle de sécurité est axé sur l’appareil. Le système d’exploitation (SE) au cœur de tous les appareils actuels de Ricoh a été conçu précisément et renforcé par Ricoh pour notre équipement. De plus, nombre de nos modèles d’appareils MFP sont certifiés selon le profil de protection standard IEEE 2600.2 pour terminaux d’impression. Le chiffrement de disque dur et la sécurité par écrasement de données sont compris avec certains de nos appareils afin d’assurer que les données traitées demeurent confidentielles. Ricoh a travaillé d’arrache-pied pour garantir que la sécurité de ses appareils ne soit pas affaiblie par l’introduction du panneau de commande intelligent, qui utilise également un SE propre à Ricoh. Ricoh n’installe que les composants nécessaires et il est impossible d’obtenir un accès complet au système. Les applications intégrées doivent réussir le test de compatibilité de Ricoh et recevoir une signature numérique avant de pouvoir être lancées sur le panneau de commande intelligent. Ricoh s’engage à travailler avec ses clients pour livrer des produits et des services qui sont compatibles avec les politiques de sécurité de votre réseau et de vos TI. Nous utilisons plusieurs techniques pour contrer les menaces intermédiaires ou internes, y compris le chiffrement complet des fichiers imprimés et numérisés, le chiffrement des données sur les serveurs, et la séparation des tâches d’administrateur. Une gamme de services de sécurité chefs de file de l’industrie, dont des services gérés et de conseil, englobe tous les niveaux de votre système afin de surveiller, d’optimiser et de gérer efficacement la sécurité des documents et de l’information.

Applications intégrées

- Offrent des fonctions avancées
- Vérifiées, certifiées compatibles et signées numériquement par Ricoh
- Ex. : authentification, impression sécurisée, chiffrement, flux de travaux

Réseau (couche de liaison de données et de transport)

- Exploitation et respect des politiques et des mesures de sécurité du réseau du client
- Chiffrement complet des fichiers imprimés et numérisés pour contrer les menaces intermédiaires

Interface utilisateur (panneau de commande intelligent)

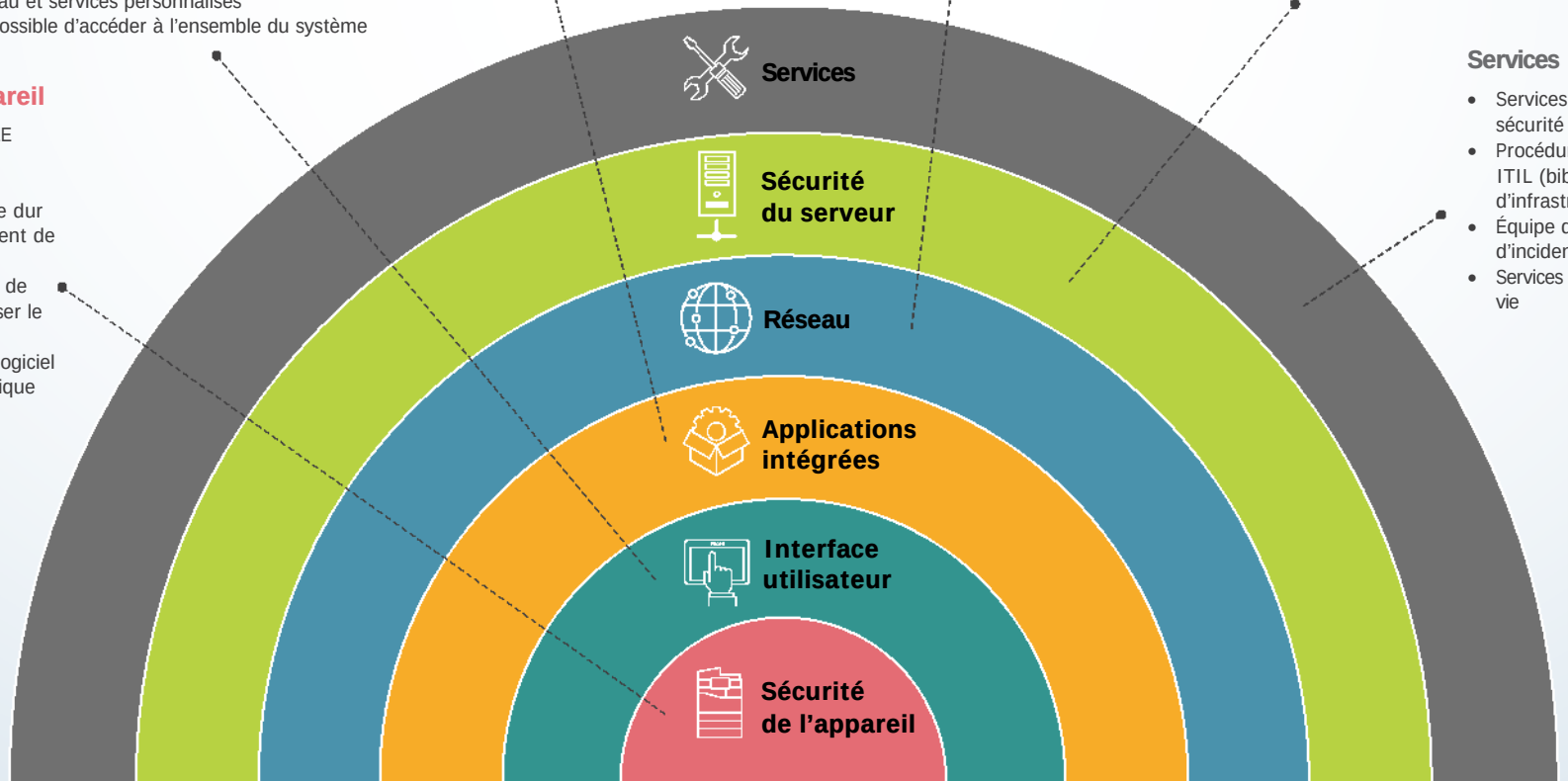
- SE renforcé par Ricoh basé sur l’utilisation de modules particuliers
- Les outils et composants inutiles et les outils avec problèmes connus ne sont pas installés
- Noyau et services personnalisés
- Impossible d’accéder à l’ensemble du système

Sécurité du serveur

- Exploitation et respect des politiques et des mesures de sécurité des serveurs du client
- Fichiers chiffrés
- Séparation des tâches d’administrateur

Sécurité de l’appareil

- Certification ISO / IEEE 15408 / IEEE 2600.2
- SE propre à Ricoh
- Chiffrement de disque dur
- Sécurité par écrasement de données
- Module de plateforme de confiance pour sécuriser le démarrage
- Mises à jour de micrologiciel avec signature numérique



Services

- Services d’optimisation de la sécurité
- Procédures de service certifiées ITIL (bibliothèque d’infrastructure TI) et ISO
- Équipe d’intervention en cas d’incident de sécurité
- Services de recyclage en fin de vie

La sécurité est inscrite dans notre ADN

La sécurité est un aspect fondamental de la conception, la fabrication et la mise en œuvre des appareils de Ricoh. Le raisonnement axé sur la sécurité est présent dès le départ, et ce à toutes les étapes : de la conception à la vente des produits. Cela fait partie de notre ADN — informer tant notre philosophie de conception que notre engagement afin de travailler continuellement pour appuyer nos clients avec des solutions qui évoluent en fonction des menaces.

Sécurité de l'appareil

- Mises à jour de micrologiciel avec signature numérique
- Système de sécurité par écrasement de données
- Ligne de télécopie sécurisée
- Authentification des utilisateurs de l'appareil
- Certification IEEE 2600
- Chiffrement de disque dur

Sécurité des données

- Solutions de numérisation sécurisées
- Impression verrouillée
- Comptabilité et récupération des coûts
- Impression sécuritaire obligatoire
- Sécurité des données copiées

Sécurité du réseau

- Authentification des utilisateurs du réseau
- Fermeture des ports réseau non utilisés
- Chiffrement du réseau
- Device Manager NX
- @Remote
- Chiffrement des flux d'impression

Programmes et ressources

- Soutien technique à l'échelle nationale et mondiale
- Formation des utilisateurs finaux et des administrateurs
- Programmes de fin de vie d'équipement
- Documentation de soutien de la sécurité

Gouvernance de l'information et cybersécurité

L'expertise, les compétences et les services de Ricoh en matière de sécurité s'étendent au-delà des appareils (voir la page 33).

Sécurité de l’appareil

Les fonctions de sécurité de nos appareils peuvent protéger les appareils multifonctions et les imprimantes laser contre des menaces potentielles, y compris des micrologiciels nuisibles, le disque dur d’un appareil, la mémoire non volatile, des ports réseau ouverts, et un système d’authentification. Ricoh a obtenu la certification pour une vaste gamme de produits basés sur des critères communs (ISO/IEC 15408). Sur les appareils en cours de certification, des fonctions de sécurité sont vérifiées par des laboratoires indépendants et accrédités par le gouvernement afin d’assurer qu’elles aient un bon rendement et qu’elles soient conformes aux normes gouvernementales et industrielles.

Dans le cadre de notre engagement continu à protéger vos importants actifs informationnels contre les menaces, nous concevons et offrons des produits et des fonctions de sécurité pour aider à protéger vos documents papier et électroniques, et ce sans nuire à la productivité ni à la convivialité des procédures.

Les micrologiciels non sécurisés peuvent être compromis

Mises à jour de micrologiciel avec signature numérique

Si le logiciel intégré, ou micrologiciel, d'un MFP ou d'une imprimante est modifié ou compromis, l'appareil peut alors être utilisé comme méthode d'infiltration dans le réseau d'entreprise, comme moyen de causer des dommages à l'appareil, ou comme plateforme pouvant servir à d'autres fins malicieuses. Les appareils conçus par Ricoh sont fabriqués à partir d'un module de plateforme sécurisé (TPM) propre à Ricoh et sont conçus de manière à ne pas amorcer en cas d'atteinte au micrologiciel. Le TPM de Ricoh est un module de sécurité de l'équipement qui valide les programmes de base du contrôleur, le système d'exploitation, le BIOS, le programme d'amorçage et le micrologiciel des applications.

Les MFP et les imprimantes de Ricoh emploient une signature numérique pour évaluer la validité des micrologiciels. La clé publique utilisée pour cette vérification est stockée dans un secteur du TPM de Ricoh qui est non volatil et protégé par écrasement. Une clé de chiffrement élémentaire et des fonctions cryptographiques figurent également dans le TPM et ne peuvent pas être modifiées de l'extérieur. Ricoh utilise un processus d'amorçage validé qui emploie deux méthodes pour vérifier la validité des programmes et des micrologiciels :

1. Détection des modifications

2. Validation des signatures numériques

Les appareils de Ricoh ne démarreront pas tant que l'authenticité et la sécurité de ses programmes et micrologiciels ne soient pas confirmées.

Les données temporaires sont vulnérables

Système de sécurité par écrasement de données (DOSS)

Lorsqu'un document est numérisé ou lorsque des données sont reçues d'un ordinateur, certaines données peuvent être sauvegardées temporairement sur le disque dur ou sur un dispositif de mémoire. Cela peut inclure des données d'images numérisées, imprimées ou copiées; des données entrées par l'utilisateur; et la configuration de l'appareil. Ces données temporaires, ou « latentes », constituent des failles de sécurité potentielles.

Le système de sécurité par écrasement de données (DOSS) de Ricoh élimine ces points faibles en détruisant les données sauvegardées temporairement sur le disque dur d'un MFP en les écrasant avec des séquences aléatoires de « 1 » et de « 0 ». Les données temporaires sont activement écrasées et donc effacées chaque fois qu'une tâche est effectuée.

- Respecte les recommandations de la National Security Agency (NSA) et du département de la Défense (DoD) relatives au traitement de l'information protégée
- Empêche quasiment tout accès aux données latentes des tâches de copie, d'impression, de numérisation et de télécopie une fois le processus d'écrasement terminé (ce processus peut être sélectionné jusqu'à 9 fois)
- Fonctionne avec le système de sécurité de disque dur amovible de Ricoh pour fournir une approche multidimensionnelle
- Aide les clients à se conformer aux exigences de la HIPAA, la GLBA et la FERPA
- Fournit de la rétroaction visuelle sur l'état du processus d'écrasement (c.-à-d. « complété » ou « en cours ») au moyen d'une simple icône sur le panneau d'affichage

Le chiffrement assure une protection contre le vol de données

Chiffrement de disque dur

Même si le disque dur est retiré d'un appareil Ricoh, les données chiffrées sont impossibles à lire. La fonction de chiffrement de disque dur peut assurer la protection du disque dur d'une imprimante multifonction contre le vol de données tout en aidant des organisations à se conformer aux politiques de sécurité d'entreprise. Le chiffrement inclut les données sauvegardées dans le carnet d'adresses d'un système, ce qui réduit le risque de détournement ou d'atteinte de l'information des employés, des clients et de détaillants d'une organisation. Les types de données suivants — sauvegardés dans la mémoire non volatile ou sur le disque dur des imprimantes multifonctions — peuvent être chiffrés :

- Carnet d'adresses
- Information d'authentification de l'utilisateur
- Documents sauvegardés
- Documents sauvegardés temporairement
- Registres
- Réglages d'interface de réseau
- Information de configuration

La méthode utilisée par Ricoh pour le chiffrement de disque dur est la norme AES (Advanced Encryption Standard) à 256 bits.

Votre ligne de télécopie constitue-t-elle une voie d'entrée?

Ligne de télécopie sécurisée

L'activation de la fonction de télécopie d'un appareil peut nécessiter une connexion externe par ligne téléphonique, ce qui signifie qu'il est important de bloquer tout accès non autorisé via la ligne de télécopie. Le logiciel intégré de Ricoh est conçu pour traiter uniquement les types de données appropriés (c.-à-d. les données de télécopie) et envoyer ces données directement aux bonnes fonctions au sein de l'appareil. Puisque seules les données de télécopie peuvent être reçues d'une ligne de télécopie, le risque d'accès non autorisé au réseau ou aux programmes de l'appareil depuis la ligne de télécopie est éliminé.

Ricoh emploie plusieurs méthodes pour sécuriser les activités de télécopie :

- Le contrôleur de télécopie ne contient qu'un modem de télécopie (et non un modem de données), donc toute communication se fait selon le protocole de télécopie G3
- Les données d'image ne sont pas sauvegardées dans la mémoire de page du contrôleur de copie ou dans l'emplacement de stockage temporaire, ce qui empêche l'accès à ces données depuis le contrôleur de télécopie
- Les données sauvegardées dans la mémoire de page du contrôleur de copie ou dans l'emplacement de stockage temporaire ne peuvent être envoyées qu'à l'unité d'impression
- Il n'existe aucune connexion active entre les bus vidéo d'impression ou de numérisation et le contrôleur de copie, ce qui empêche l'accès aux données sauvegardées dans la mémoire de page du contrôleur de copie ou dans l'emplacement de stockage temporaire depuis le contrôleur de télécopie
- Les données de l'emplacement des pages sont supprimées après chaque tâche

Certification de sécurité indépendante

IEEE 2600

La norme de sécurité IEEE 2600 établit les exigences minimales des fonctions de sécurité utilisées par les appareils nécessitant un haut niveau de sécurité des documents. Elle représente un point de référence pour les attentes en matière de sécurité, tant pour les MFP que pour les imprimantes. Afin d'assurer que le fonctionnement d'un appareil soit conforme à la norme établie, un laboratoire indépendant vérifie les fonctions de sécurité du fabricant.

Les fonctions suivantes — considérées comme étant les plus vulnérables aux violations de données potentielles — ont été validées dans de nombreux appareils de Ricoh par rapport à la norme IEEE 2600 et peuvent être activées :

- Systèmes d'identification et d'authentification de l'utilisateur
- Technologie de chiffrement des données pour imprimantes multifonctions
- Validation des micrologiciels du système
- Séparation de la ligne de télécopie analogique et du contrôleur de copie, d'impression et de numérisation
- Validation des algorithmes de chiffrement des données
- Processus de sécurité par écrasement de données

Ricoh offre un large éventail d'imprimantes et de MFP certifiés conformes à la norme de sécurité IEEE 2600, et notre portefeuille de produits est amélioré continuellement afin de répondre aux exigences changeantes de nos clients.

Contrôler l’accès et réduire les risques

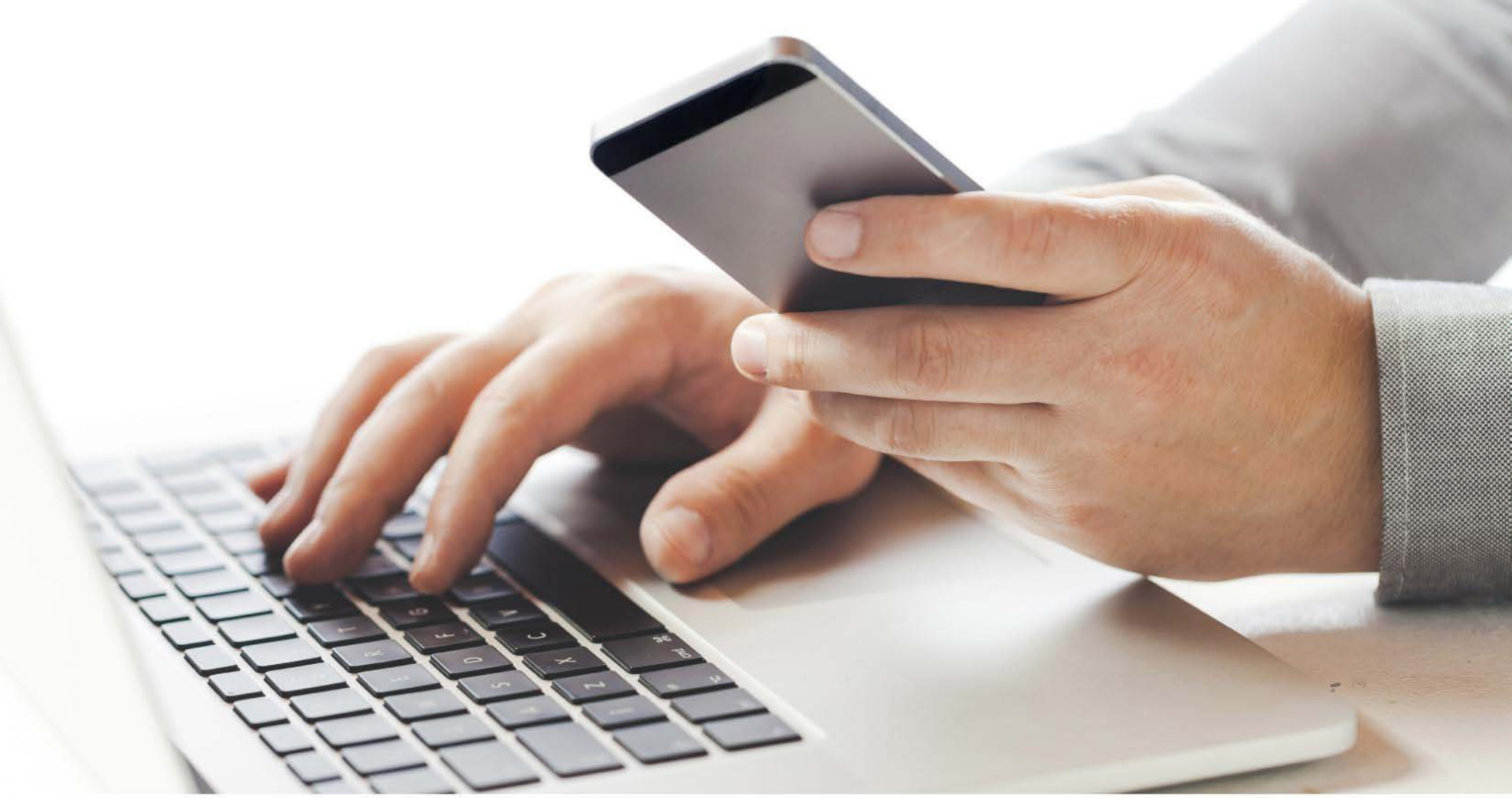
Authentification des utilisateurs de l’appareil

Les fonctions d’authentification permettent aux utilisateurs autorisés d’utiliser une imprimante multifonction de Ricoh tout en empêchant l’accès pour les personnes sans permission. Ricoh vous offre également la capacité d’établir les fonctionnalités accessibles pour chaque utilisateur ou groupe d’utilisateurs. Par exemple, vous pouvez limiter leur capacité de modifier les réglages de l’appareil et de consulter les entrées du carnet d’adresses, ou leur accorder l’accès à des flux de numérisation et à des serveurs de documents ainsi qu’à d’autres fonctions particulières. De plus, la fonction de verrouillage des utilisateurs — qui est déclenchée si l’appareil détecte une haute fréquence de tentatives de connexion réussies ou échouées — vous aide à éviter les attaques par déni de service et le perçage de mot de passe par force.

Les méthodes d’authentification incluent :

L’authentification de base — les utilisateurs entrent un nom d’utilisateur et un mot de passe qui sont enregistrés localement dans le carnet d’adresses de l’imprimante multifonction.

- L’authentification par code d’utilisateur — les utilisateurs entrent un code (jusqu’à 8 caractères) qui est comparé aux données enregistrées dans le carnet d’adresses.
- L’authentification Windows/LDAP — l’accès aux imprimantes multifonctions de Ricoh peut être lié à des contrôleurs de domaine Windows ® et à des serveurs LDAP.
- L’authentification par carte — Au lieu d’entrer un nom d’utilisateur et un mot de passe, les utilisateurs placent une carte enregistrée sur un lecteur de carte NFC facultatif pour s’authentifier.
- L’authentification par carte d’accès commune (CAC) — La carte d’accès commune est un système d’authentification spécialisé par carte d’identité du département de la Défense des États-Unis conçu pour les utilisateurs du gouvernement qui doivent se conformer à la directive présidentielle 12 du département de la Sécurité intérieure (HSPD-12).
- La vérification de l’identité personnelle (PIV) — La vérification de l’identité personnelle constitue la version civile de la CAC.
- La solution d’authentification par jeton SIPRNet — Le jeton SIPRNet est une variante de l’authentification par CAC conçue pour les réseaux contrôlés.



Sécurité des données

L'information peut facilement être divulguée par inadvertance. Un document laissé dans le bac de sortie d'une imprimante multifonction peut constituer un risque pour la sécurité tout comme un fichier numérique détourné ou l'impact d'une erreur humaine. Les imprimantes multifonctions de Ricoh aident à protéger vos données, que vous imprimiez, copiiez, numérisiez ou télécopiiez. Le système de chiffrement de données de Ricoh — qui utilise un module de chiffrement RSA BSAFE Crypto et qui est conforme à FIPS 140-2 — aide à protéger vos données lorsqu'elles sont en circulation ou au repos.

174 millions

de dossiers numériques ont été compromis par des pirates informatiques en 2011 — une hausse de plus de 4 000 % par rapport à 2010.*

*Rapport des enquêtes sur les violations de données de 2012, Verizon®

Ricoh aide à protéger vos données avec des technologies et des fonctions conçues pour appuyer les politiques de sécurité, protéger les données contre l'utilisation inappropriée ou négligente et encourager la conformité par la responsabilisation.

Protection pour les documents numérisés

Solutions de numérisation sécurisées

Le processus de numérisation des documents papier et d'acheminement des fichiers électroniques résultants — soit vers un système administratif ou par courriel — peut exposer les données à la violation si celles-ci ne sont pas sécurisées convenablement. La numérisation, quoique conçue pour être un processus convivial, doit également offrir une protection solide pour l'information numérique acheminée. Il faut d'abord restreindre l'accès. Limitez les activités de numérisation aux utilisateurs autorisés avec plusieurs options d'authentification, dont la connexion par réseau, l'authentification Kerberos en option et l'ouverture de session unique par carte.

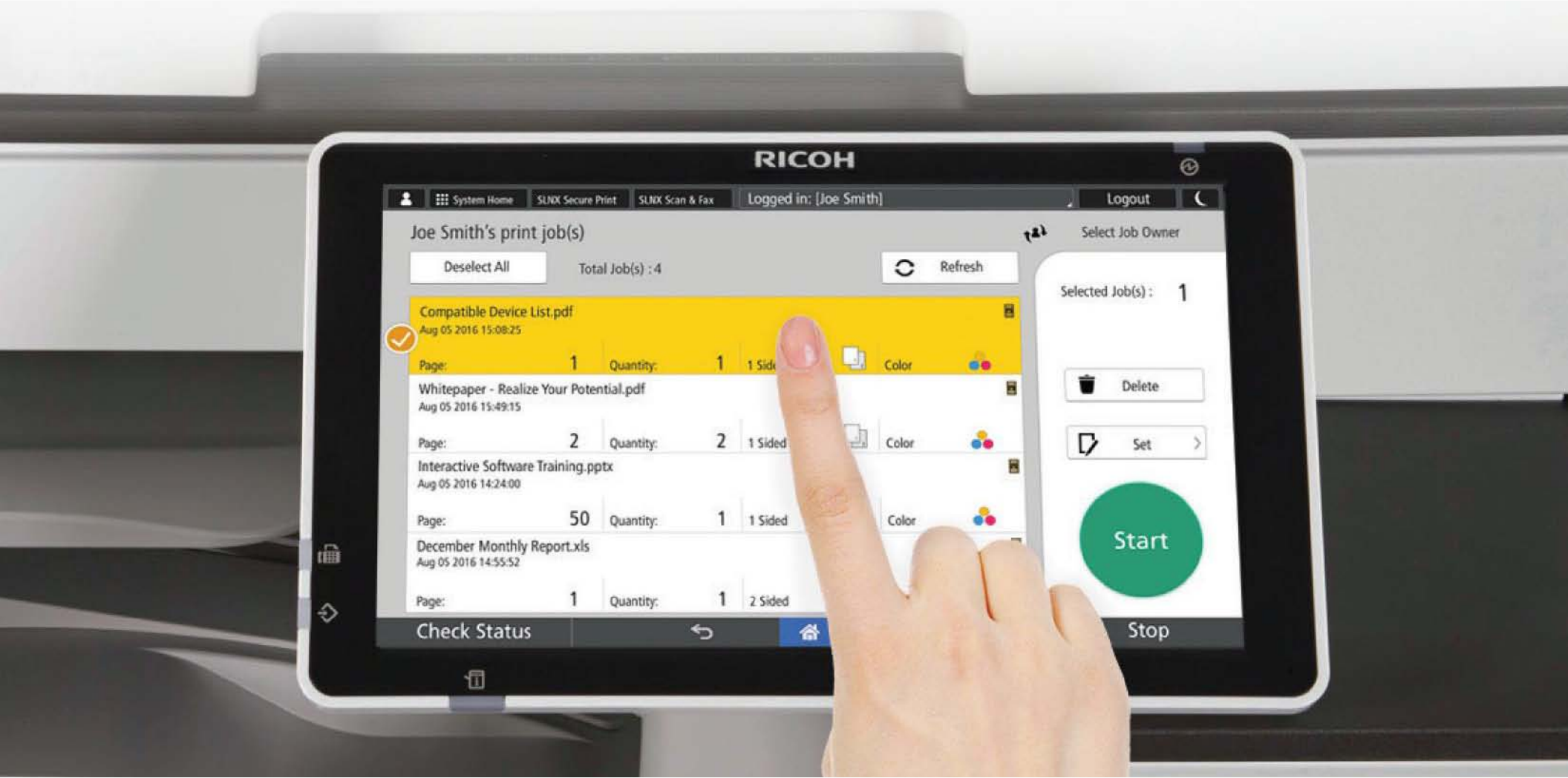
Le chiffrement des communications de numérisation vers courriel contribue à la réduction du risque de violation de données. Envoyez des courriels en utilisant le chiffrement à clé publique et un certificat de vérification de l'utilisateur qui a été enregistré dans le carnet d'adresses de l'appareil de numérisation. Vous pouvez également prévenir la mystification de courriel et la modification des messages en apposant une signature électronique qui utilise une clé secrète basée sur le certificat d'un appareil.

Les imprimantes, copieurs et numériseurs multifonctions conçus par Ricoh sont équipés de protocoles sécurisés SSL et TLS et peuvent utiliser de puissants algorithmes de chiffrement (AES à 256 bits et SHA-2) — ainsi que fournir des pistes de vérification et des contrôles administratifs.

Les impressions laissées sans surveillance peuvent entraîner des fuites d'information

Impression verrouillée

N'importe qui peut ramasser des documents imprimés qui ont été laissés dans le bac de sortie ou à découvert. Cela risque de compromettre l'information contenue dans ces documents et les répercussions potentielles prennent énormément d'ampleur lorsqu'il s'agit de documents confidentiels. La fonction d'impression verrouillée de Ricoh peut conserver des documents chiffrés sur le disque dur de l'appareil jusqu'à ce que leur propriétaire arrive et entre le bon code NIP. En plus de cette fonction basée sur le pilote, Ricoh peut également offrir une option d'impression verrouillée avancée qui est liée aux comptes utilisateurs et qui peut être jumelée à l'authentification par carte. Si vous désirez profiter d'encore plus de fonctionnalités, des logiciels tels que Streamline NX de Ricoh (représenté ci-dessous) peut vous offrir une capacité de relâchement d'impression sécurisée haut de gamme qui permet aux utilisateurs de gérer leur file d'attente d'impressions tout en laissant le plain contrôle aux administrateurs.



Assurer une protection contre la copie non autorisée

Sécurité des données copiées

Ricoh offre des fonctions pour empêcher la copie non autorisée de documents papier, ce qui aide à prévenir des fuites d'information potentielles. La fonction de copie protégée imprime et copie des documents avec un motif invisible spécial filigrané sur l'ensemble des pages. Si les documents imprimés ou copiés avec cette fonction sont photocopiés de nouveau, le motif filigrané sera visible sur les copies résultantes.

La fonction de contrôle de copie non autorisée protège les documents contre les copies non autorisées de deux façons. Le texte masqué pour copie inscrit un message en motif masqué derrière le contenu original du document imprimé. Si des copies non autorisées sont produites, le message filigrané apparaît sur la copie. Ce message peut inclure le nom de l'auteur du document ou un avertissement. La sécurité des données copiées aide à protéger l'information elle-même. Lorsque l'appareil de Ricoh détecte le motif masqué, les données imprimées sont obscurcies par une boîte grise qui recouvre l'ensemble du motif masqué en ne laissant qu'une marge de 4 mm.

Les documents anonymes sont difficiles à contrôler

Impression sécuritaire obligatoire

Estampillez des documents avec des renseignements d'identification clés pour accroître la responsabilisation le contrôle de la gestion. L'impression obligatoire de l'information de sécurité est une fonction qui impose l'impression de l'information essentielle dans un document, à savoir l'auteur du document, la date de l'impression et l'appareil utilisé pour l'impression. Cette fonction peut être activée pour la copie, l'impression et la télécopie ainsi que pour des fonctions du serveur de documents. Les administrateurs peuvent choisir la position de l'impression et les types de renseignements qui seront imprimés automatiquement à la sortie du document, notamment :

- La date et l'heure de l'impression
- Le nom ou nom d'utilisateur de la personne ayant effectué l'impression
- L'adresse IP ou le numéro de série de l'appareil utilisé

Protéger les appareils contre l'utilisation abusive

Comptabilité et récupération des coûts

L'utilisation incontrôlée de l'équipement d'imagerie peut entraîner des dépenses imprévues et des violations potentielles des politiques de l'entreprise. Le logiciel de comptabilité et de récupération des coûts de Ricoh surveille l'utilisation à l'échelle des employés individuels et automatise le processus de répartition des coûts aux utilisateurs ou aux services. Renforcez la responsabilisation en fixant des quotas pour les utilisateurs ainsi que des limites de comptes budgétaires. Établissez des permissions d'utilisateur pour limiter l'accès à certaines fonctions selon les besoins — par exemple, la capacité d'imprimer en couleur. Le contrôle de l'utilisation de l'équipement au moyen de l'authentification et en la désignation des fonctions autorisées et non autorisées réduisent les possibilités d'utilisation abusive et fournissent des indications utiles quant à la gestion.

Sécurité du réseau

Les imprimantes multifonctions échangent de l'information essentielle avec des ordinateurs et des serveurs sur des réseaux. Sans protection, cette information risque d'être modifiée par des personnes malintentionnées qui pourraient infiltrer le réseau. Les produits et les technologies de Ricoh offrent des fonctions qui peuvent aider à empêcher l'accès non autorisé via les réseaux. Des techniques courantes incluent le chiffrement des communications et des flux d'impression sur le réseau, l'authentification des utilisateurs du réseau ainsi que diverses contre-mesures administratives, telles que la fermeture des ports de réseau, et la gestion proactive des appareils.

Les fonctions de sécurité de Ricoh peuvent aider à réduire le risque d'exploitation de réseau ou de fuite d'information découlant de l'atteinte d'un appareil ou d'une imprimante multifonction.

Les utilisateurs non autorisés peuvent constituer une menace

Authentification des utilisateurs du réseau

Les appareils de Ricoh offrent la fonction d'authentification des utilisateurs du réseau afin de limiter l'accès pour les utilisateurs non autorisés. Par exemple, l'authentification Windows® vérifie l'identité d'un utilisateur à l'imprimante multifonction en comparant ses données de connexion (nom d'utilisateur et mot de passe) à la base de données des utilisateurs autorisés sur le serveur de réseau Windows. En cas d'accès au carnet d'adresses général, l'authentification LDAP valide un utilisateur auprès du serveur LDAP (Light-weight Directory Access Protocol). Ainsi, seules les personnes ayant un nom d'utilisateur et un mode de passe valides peuvent rechercher et sélectionner des adresses courriel stockées sur le serveur LDAP.

Les logiciels tels que Streamline NX de Ricoh — une suite modulaire qui couvre la numérisation, la télécopie, la gestion d'appareils, la sécurité et les procédures de comptabilité — fournissent des options supplémentaires pour l'authentification de réseau. Ces options incluent l'authentification LDAP, l'authentification Kerberos et une trousse SDK pour des intégrations personnalisées.

Rendez vos appareils « invisibles » pour le monde extérieur

Fermeture des ports réseau non utilisés

Afin de faciliter l'ajout d'appareils au réseau existant du client, les systèmes en réseau de nombreux fournisseurs de bureautique sont livrés avec tous les ports réseau « ouverts ». Les ports ouverts non utilisés des imprimantes et des MFP présentent toutefois un risque pour la sécurité. Les ports compromis peuvent ouvrir la voie à diverses menaces externes et entraîner la destruction ou la falsification de données sauvegardées, des attaques par déni de service et l'entrée de virus ou de logiciels malveillants dans le réseau. Il existe cependant une solution simple, mais souvent négligée, à cette source de risque particulière : la fermeture des ports. Les administrateurs des appareils de Ricoh peuvent facilement fermer les ports réseau non utilisés — aidant ainsi à rendre les appareils pratiquement « invisibles » aux pirates informatiques. De plus, des protocoles spécifiques, tels que SNMP ou FTP, peuvent être complètement désactivés pour éliminer le risque d'exploitation.

Les données non chiffrées sur le réseau sont à risque

Chiffrement du réseau

À mesure que les données circulent sur le réseau, un pirate informatique expérimenté pourrait intercepter des flux de données brutes, des fichiers et des mots de passe. Sans protection, l'information intelligible peut être volée, modifiée ou falsifiée, puis réinsérée dans le réseau à des fins malicieuses. Ricoh utilise des protocoles de sécurité de réseau robustes qui peuvent également être configurés en fonction des besoins du client. Le protocole de sécurité TLS (Transport Layer Security) est utilisé pour aider à maintenir l'intégrité des données communiquées entre deux terminaux.

Les appareils de Ricoh sont compatibles avec WPA2, WPA2-PSK avec chiffrement AES (accès protégé Wi-Fi), un système de chiffrement pour les réseaux sans fil qui offre une meilleure sécurité que le système de chiffrement WEP (confidentialité équivalente aux transmissions par fil) traditionnels. WPA2, WPA2-PSK est muni d'une fonction d'authentification de l'utilisateur et d'un protocole de chiffrement appelé CCMP (AES), qui met à jour automatiquement la clé de chiffrement à certains intervalles.

Les données envoyées aux imprimantes peuvent être exploitées

Chiffrement des flux d'impression

Les données non chiffrées envoyées dans un flux d'impression peuvent être exploitées si elles sont saisies en transit. Ricoh peut activer le chiffrement des données d'impression au moyen des protocoles SSL/TLS (Secure Sockets Layer/Transport Layer Security) via IPP (Internet Printing Protocol) — chiffrant ainsi les données des postes de travail jusqu'aux appareils ou aux imprimantes multifonctions en réseau. Cela peut également se faire en utilisant IPP plutôt que SSL/TLS. Puisqu'il s'agit d'un protocole qui aide à maintenir l'intégrité des données, les tentatives d'intercepter les flux de données d'impression chiffrés en transit ne produiraient que des données indéchiffrables.

La gestion des appareils peut demander beaucoup de temps

Device Manager NX

Puisque la gestion des appareils peut exiger beaucoup de temps, des lacunes en matière de sécurité apparaissent par inadvertance lorsque des aspects de la gestion des appareils sont négligés. Les logiciels de gestion des appareils de Ricoh tels que Device Manager NX et Streamline NX offrent aux gestionnaires des TI un point de contrôle centralisé afin qu'ils puissent surveiller et gérer un nombre quasiment infini d'appareils d'impression en réseau — qu'ils soient répartis sur plusieurs serveurs ou emplacements géographiques. Les communications chiffrées par SNMPv3 sont utilisées pour surveiller l'état de fonctionnement des appareils et de leurs services en incorporant des fonctions d'authentification de l'utilisateur et de chiffrement de données qui aident à protéger les données des utilisateurs et l'information des appareils en réseau.

Grâce au contrôle centralisé, les administrateurs peuvent déterminer qui peut accéder à un appareil ou à une imprimante multifonction et l'utiliser, surveiller les réglages de la solution de sécurité par écrasement des données (DOSS), et gérer les certificats des appareils. Des tâches automatisées peuvent également réduire le risque d'exposition lié aux micrologiciels désuets. Le micrologiciel des appareils de Ricoh est comparé soit à la version approuvée par le client ou à la version la plus récente pour l'appareil du Centre de logiciel mondial de Ricoh. Si le micrologiciel est différent, le bon micrologiciel peut être mis en place sur l'appareil automatiquement.

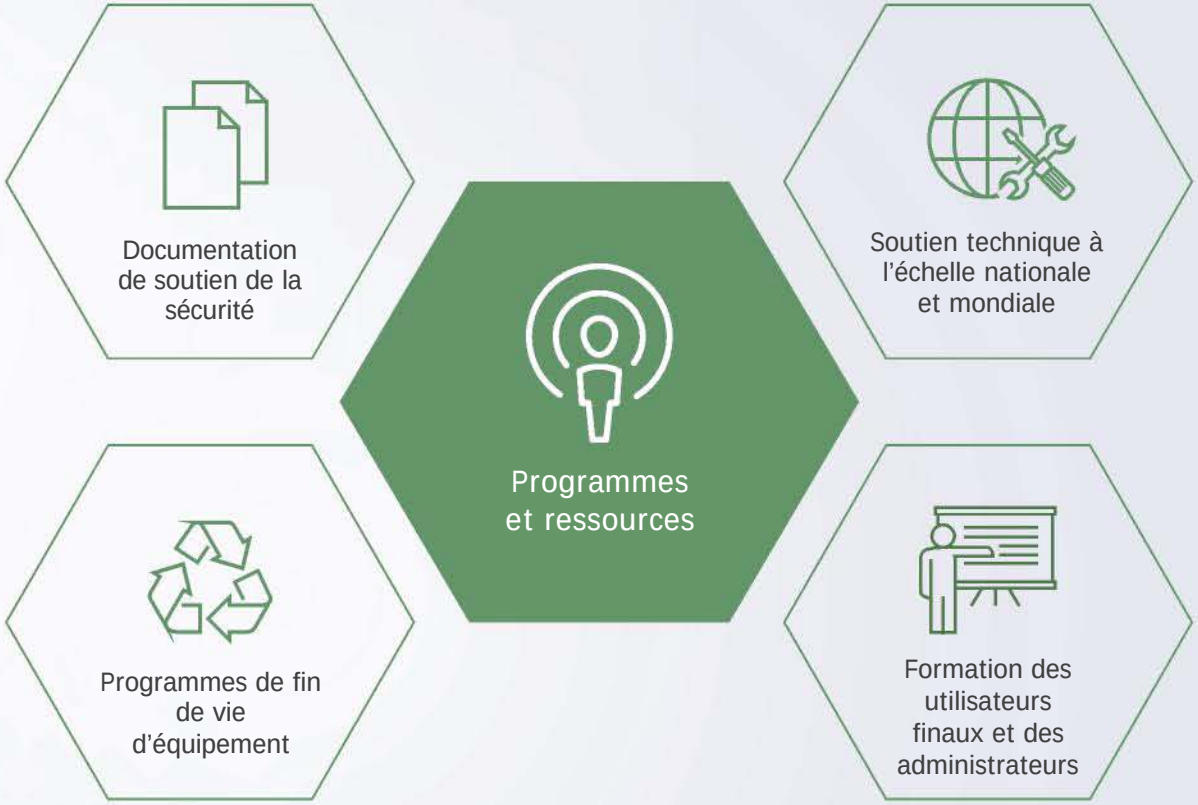
Aider les fournisseurs de service à répondre rapidement

@Remote

@Remote Connector NX de Ricoh collecte des alertes de service critiques et les transmet directement à votre fournisseur de service en utilisant une méthode sécurisée. Votre fournisseur peut prévoir des mises à jour de micrologiciel à distance au moyen du connecteur afin d'installer immédiatement les mises à jour critiques. Le connecteur @Remote collecte également les lectures des compteurs de vos appareils — ainsi que des notifications signalant les niveaux de fournitures — et les rend accessibles selon un horaire prédéfini afin de maintenir le temps de fonctionnement et de réduire la charge administrative.

Programmes et ressources

Les organisations qui utilisent et qui conservent de l'information médicale, financière, nominative ou d'autres types de données sensibles peuvent être assujetties à diverses exigences réglementaires telles que la HIPAA, la GLBA et la FERPA. Que votre organisation ait besoin d'adhérer à des exigences de conformité externes ou de démontrer le soutien de ses propres politiques de sécurité, Ricoh peut aider. Nous approvisionnons nos clients en programmes et en ressources pour les aider à respecter leurs exigences de conformité réglementaire particulières.



À Ricoh, nous appuyons nos clients en offrant le soutien technique, les connaissances et la formation ainsi que la documentation de sécurité nécessaires concernant notre équipement. De plus, nous offrons également un service de suppression de données des appareils en fin de vie.

n

Programmes de fin de vie d’équipement

La présence d’information latente sur de l’équipement mis hors service peut présenter un risque de sécurité jusqu’à ce que celui-ci soit complètement détruit. Si cette information est compromise, de tierces parties mal intentionnées pourraient s’en servir afin d’exécuter de plus importantes brèches de sécurité. Les programmes de Ricoh effacent toute information stockée sur l’équipement à la fin de sa vie utile ou lorsqu’il est retourné à la fin d’un contrat de location.

Services d’écrasement des données de disque dur

Effectué généralement lorsqu’un appareil est mis hors service ou à la conclusion d’un contrat de location d’équipement, le service d’écrasement de données de disque dur écrase complètement les données du client sur le disque dur de l’appareil en question. Diverses méthodes d’écrasement de données sont offertes, dont des méthodes conformes à la National Security Agency (NSA) et au département de la Défense (DoD) des États-Unis. De plus, le contenu de la mémoire vive non volatile (NV-RAM) est initialisé aux valeurs par défaut afin de prévenir l’exposition d’information nominative — à savoir des adresses IP, des carnets d’adresses ainsi que d’autres données administratives — à de tierces parties.

Services d’élimination de disque dur

Le programme de cession de disque dur permet aux clients de récupérer le disque dur de leur MFP ou de leur imprimante à la fin d’un contrat de location ou à la fin de la vie utile de l’appareil. Un technicien certifié de Ricoh enlève le disque dur de l’appareil avant que celui-ci ne soit retiré du site du client et le remet à un représentant du client. Les clients conservent le contrôle de leur information et peuvent décider de la faire détruire selon la méthode de leur choix.

Services de nettoyage de MFP

Le service de nettoyage de MFP est conçu pour effacer toute information nominative d’un MFP ou d’une imprimante avant que l’appareil ne soit retiré de l’emplacement d’un client. L’information stockée dans la mémoire de l’appareil, telle que les carnets d’adresses et l’information d’adresse du réseau, est supprimée. Des marques d’identification comme des étiquettes portant des noms de services, des adresses IP ainsi que d’autres renseignements du centre d’assistance sont également retirées — de même que tout papier ou stock de formulaires du client. L’élimination de tels renseignements peut aider à prévenir des tentatives malicieuses d’obtenir l’information des TI d’une entreprise.

Soutien technique à l’échelle nationale et mondiale

Ricoh a établi des centres de technologie dans toutes les régions afin d’offrir du soutien technique à nos clients partout dans le monde en répondant à leurs besoins de façon rapide et efficace. L’équipe des services mondiaux de Ricoh fournit des solutions standards, uniformes et complètes. Couvrant quelque 200 pays et territoires à l’échelle mondiale, Ricoh compte plus de 30 000 professionnels de prestation de services. Notre réseau de soutien inégalé de ventes directes et de partenaires détaillants a la capacité de desservir 95 % des employés des entreprises du Fortune 500. Vous pouvez donc vous fier à un seul partenaire pour tous vos besoins à l’échelle mondiale. Grâce à nos bureaux et à nos professionnels de prestation de services situés dans autant de pays dans le monde, nous pouvons répondre rapidement aux demandes des clients — où qu’ils soient.

Documentation de soutien de la sécurité

Ricoh fournit de la documentation technique pour répondre aux exigences en matière de sécurité de l'information de nos clients, y compris des documents de certification IEEE 2600 et ISO 15408 pour certains produits offerts. Cette documentation présente la validation des déclarations de sécurité de l'entreprise par un tiers indépendant et peut être fourni sur demande. De plus, des livres blancs de la sécurité portant sur les paramètres du réseau et des appareils ainsi que des guides d'installation de la sécurité des appareils sont également offerts aux clients. Ces guides fournissent de l'information détaillée sur la façon dont l'équipement de Ricoh communique des données à l'intérieur des appareils et l'interaction des appareils avec le réseau.

Formation des utilisateurs finaux et des administrateurs

Le maintien d'un niveau de vigilance élevé et l'adhérence aux meilleures pratiques en matière de sécurité demandent beaucoup plus que de la technologie — il faut également des gens. Ricoh offre de la formation sur nos appareils qui vise tant les utilisateurs finaux que les administrateurs. Équipée des connaissances nécessaires, votre équipe peut comprendre les capacités de sécurité disponibles et apprendre comment les exploiter pour aider votre organisation à protéger son information et à se conformer aux politiques.


JISEC
Common Criteria
Certification Report
MP C4504/C6004
Security Target
Japan IT Security Evaluation and Certification Scheme
Certificate
is awarded to
Certification Number: C0539
RICOH COMPANY, LTD.
Product Name: MP C4504/C6004(Ricoh/Savin/Lanier/nashuatec/Rex-Rotary/Gestetner/infotec), MP C5504 (Ricoh/nashuatec/Rex-Rotary/Gestetner/infotec)
Version: E-1.01
Type of IT Product: Multi Function Product
Original Signed
IPA
Information-technology Promotion Agency, Japan

La sécurité au-delà de l'appareil

Les meilleures pratiques de la sécurité demandent une défense en profondeur qui va au-delà de l'appareil. Ricoh répond aux préoccupations croissantes de nos clients en matière de sécurité en offrant les services de gestion de la sécurité et de gouvernance, risque et conformité (GRC). Ces services englobent l'évaluation et la gestion du cycle de vie des données et des risques, la découverte électronique, la sécurité de serveurs et des terminaux, l'accès par authentification, la sécurité de courriels et la protection contre les menaces avancées pesant sur les réseaux.

Fiez-vous à Ricoh pour relever vos plus grands défis en matière de sécurité

Perte ou vol des données

La perte de données constitue l'une des principales préoccupations des dirigeants de niveau C et le maintien de la sécurité et de la confidentialité des données représente une lutte constante. Les pirates cherchent constamment à repérer des failles dans votre armure afin de les exploiter. L'équipement d'imagerie de Ricoh peut jouer un rôle important dans la prévention de la perte de données.

Corruption ou modification des données

Les attaques virales font les manchettes partout dans le monde et soulignent à quel point les organisations sont vulnérables aux cyberattaques. Les logiciels malveillants, les virus, les chevaux de Troie et les vers informatiques attaquent des plateformes largement utilisées avec des faiblesses reconnues. Les plateformes de Ricoh, quoique largement utilisées, emploient des systèmes d'exploitation uniques afin de contrecarrer les tentatives de manipulation.

Accessibilité des données

L'accessibilité de l'information et des données demande un équilibre multidimensionnel entre l'autorisation et l'interdiction de l'accès. Les produits de Ricoh abordent ces deux aspects en accélérant les échanges approuvés de l'information par impression, copie, numérisation et acheminement, en appliquant des contrôles pour ces procédures, en chiffrant les données en circulation et en déterminant qui peut consommer l'information traitée par notre équipement.

Compréhension des règlements

Les organisations doivent respecter de nombreux règlements mondiaux, nationaux et industriels — sans parler des politiques de sécurité et des exigences de vérification des entreprises mandatées par la communauté internationale. Ricoh fournit des outils et de l'expertise pour répondre aux besoins en matière de conformité de nos clients.

Preuve de conformité

Les pénalités en cas de non-conformité peuvent être sévères et de nouveaux règlements haussent la barre en ce qui concerne l'impact négatif potentiel sur les organisations. La documentation appropriée joue un rôle important lorsqu'il s'agit de démontrer efficacement la conformité d'une entreprise. La certification IEEE 2600 offre la validation d'un tiers indépendant pour confirmer le bon fonctionnement des TI. Ricoh peut offrir cette certification ainsi que d'autres documents pour appuyer nos clients.

Amorcer une évaluation des risques de sécurité

Une évaluation des risques de sécurité menée par Ricoh englobe l'équipement, les logiciels et les données et est basée sur les normes NIST* acceptées. Les cotes de risque, allant de « faible » à « élevé », sont calculées selon les normes du DoD** et du gouvernement fédéral des États-Unis — de même que la perte annuelle estimée pour les actifs de données, les trouvailles et les recommandations. L'évaluation des risques de sécurité sert d'indication pour le plan de gestion des risques, la création de politiques et la rectification des risques et la vérification par un tiers indépendant.

Communiquer avec nos professionnels de la sécurité

Les clients recherchent des organisations fiables qui peuvent les aider à demeurer sécurisés et à prouver leur conformité. Ricoh s'engage à approvisionner nos clients en technologies, en services, en programmes et en ressources de pointe — tout en démontrant une volonté d'aider nos clients à respecter leurs exigences de politique de sécurité. Si vous avez des questions ou si vous voulez obtenir de plus amples renseignements, veuillez communiquer avec votre professionnel des ventes de Ricoh ou visiter notre site Web.

Pour en savoir plus : **www.Ricoh-USA.com**

** National Institute of Standards and Technology*
*** Département de la Défense*

RICOH
imagine. change.
imaginer. changer.

Ricoh USA, Inc., 70 Valley Stream Parkway, Malvern, PA 19355, 1-800-63-RICOH

090717