

Solutions de sécurité des appareils, des données et des documents pour le gouvernement

Solutions d'information d'affaires

RICOH
imagine. change.
imaginer. changer.

Les technologies numériques peuvent permettre une meilleure mobilité de l'information. Pourtant, les menaces à la sécurité et à la confidentialité présentent des risques importants. Il est essentiel d'assurer la sûreté de l'information lorsque nous la rendons mobile.



Est-ce que ce scénario ressemble à votre situation actuelle?

Les ministères gouvernementaux, les sociétés d'État et les organismes gouvernementaux traitent de grandes quantités de documents secrets, personnels, confidentiels ou autrement sensibles. Malheureusement, le risque que cette information soit lue par des personnes non autorisées, volée ou utilisée de façon abusive est omniprésent – des incidents de risque et de conformité sérieux ont été blâmés sur des procédures de documents inefficaces dans 76,1 % des organismes gouvernementaux et établissements d'enseignement. Par conséquent, les ministères fédéraux et les sociétés d'État doivent avoir en place de solides pratiques de gestion du risque pour la sécurité des TI afin d'être conformes aux exigences en matière de sécurité de l'information en vigueur.

À risque : information secrète, personnelle, confidentielle et sensible

La technologie numérique a transformé les affaires en permettant d'échanger instantanément des données. En même temps, les technologies mobiles et les innovations dans les méthodes de travail changent la façon dont les ministères et les organismes fédéraux communiquent et collaborent. Mais la rapidité et l'efficacité ne sont pas les seuls résultats de ces changements – l'augmentation des risques de sécurité peut créer de sérieuses vulnérabilités au niveau de l'appareil, des données ou des documents. Ricoh travaille avec nos clients du gouvernement afin d'aider à identifier les écarts dans leur environnement et de mettre en place un plan pour mieux protéger les données qu'elles soient en transit (déplacements au sein du réseau), pendant leur utilisation (utilisateurs finaux accédant aux données) ou inactives (stockage à court ou long terme).

Votre défi : Protéger les données en circulation

Notre solution : Web Image Monitor de Ricoh – un utilitaire Web intégré pour la gestion d'appareils – permet aux administrateurs de bloquer ou de restreindre des adresses IP clientes, d'équilibrer les volumes dans l'ensemble des nombreux appareils et d'empêcher les adresses IP non autorisées de se connecter à un contrôleur d'impression. Web Image Monitor permet aussi de prévenir le vol des noms d'utilisateurs et mots de passe, d'assurer une défense contre les attaques par déni de service (attaque DOS) et d'aider à empêcher les virus de s'infiltrer par les ports inutilisés. L'équipement de Ricoh supporte la transmission PDF sécurisée en embrouillant et en chiffrant les données au moyen du chiffrement à 128 bits. L'expéditeur peut établir les droits de modification ou d'extraction du contenu pour le destinataire qui devra utiliser un mot de passe de 32 caractères pour visionner le PDF.

Votre défi : Assurer la sûreté des données utilisées

Notre solution : Ricoh offre des solutions efficaces pour aider à protéger les données pendant que les utilisateurs finaux accèdent à celles-ci et les utilisent. Par exemple, Web Image Monitor de Ricoh fournit une capacité d'audit centralisée – créant une piste pour l'information numérisée, télécopiée (via un serveur de télécopie) et imprimée. Les solutions de production de Ricoh permettent aux organisations d'analyser le contenu du flux d'impression pour trouver des données d'identification personnelles (PII) et les remplacer par « XXXX ». Ces solutions chiffrent aussi les données en transit pour Linemode, Xerox ou Metacode DJDE. En outre, Ricoh offre une fonctionnalité permettant aux organismes et aux ministères de protéger les PII, les secrets de fabrication et l'information classifiée. Les administrateurs peuvent établir des politiques pour bloquer l'impression d'information sensible et exiger des filigranes sur les copies imprimées et électroniques pour une sécurité additionnelle.

Votre défi : Protéger les données inactives

Notre solution : Ricoh offre plusieurs caractéristiques pour aider à protéger les données inactives. Entre autres : chiffrement du disque dur pour protéger contre le vol, chiffrement du carnet d'adresses pour empêcher une organisation d'être la cible de courriels malveillants et le système de sécurité par écrasement des données (DOSS), l'outil puissant de Ricoh qui protège les images latentes en les écrasant à l'aide de séquences de 1 et de 0.

*Source – « Its Worse Than you Think », IDC, 2012



Solutions de sécurité des appareils, des données et des documents pour le gouvernement



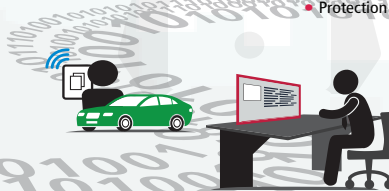
PROTÉGER LES DONNÉES EN CIRCULATION

- Flux de données brutes
 - Chiffrement de 128 bits
- Fichiers
 - Droits des destinataires
 - SSL/TLS sur IPP
- Mots de passe
 - Surveillance par Web Image Monitor
 - Filtrage d'adresses Web
 - Désactivation de ports IP



ASSURER LA SÛRETÉ DES DONNÉES UTILISÉES

- Contrôle de l'accès
 - Authentification par carte d'accès sécurisée
- Censure des copies
 - Protection par NIP et code d'utilisateur
- Gestion des droits numériques
 - Chiffrement de mot de passe
 - Impression d'accueil
 - Protection PII



PROTÉGER LES DONNÉES INACTIVES

- Protection du stockage à l'appareil
 - Chiffrement du disque dur
 - Sécurité par écrasement des données
 - Purge des données



Protocole SSL

- Pour aider à empêcher les flux de données brutes, les fichiers et les mots de passe d'être interceptés, Ricoh transmet les documents numérisés, télécopiés ou imprimés au moyen du protocole sécurisé SSL dans le protocole HTTPS. La transmission SSL est conforme à FIPS 140-2, une norme américaine de sécurité informatique émise par la *National Institute of Standards and Technology*.

Carte d'accès sécurisée

- La carte d'accès sécurisée est un système d'authentification qui se fonde sur des cartes d'identification spécialisées. Une fois que l'utilisateur autorisé insère une carte et entre son numéro d'identification, une demande est envoyée à Active Directory et l'utilisateur se voit accorder l'accès à l'information appropriée et à la fonctionnalité de production.

Architecture de sécurité avancée

La solution de Ricoh inclut les éléments suivants :

- Capacité de préparer chaque appareil avec des paramètres de sécurité normalisés et prédéfinis avant que chaque unité soit déployée à chaque emplacement.
- Un logiciel placé sur le disque dur permet de purger les données de ce dernier conformément à la norme d'effacement et de déclassification des supports d'information électronique (ITSG 06) du CST (au minimum).
- Inclut un logiciel de chiffrement qui écrit par-dessus les données du disque dur.
- Capacité de fournir une fonctionnalité de disque dur amovible pour le retrait quotidien du disque dur dans les installations secrètes et très secrètes.
- Utilise la puce de sécurité TPM (module de plateforme sécurisée) pour stocker des clés, des signatures et des fonctions cryptographiques.
- Option de remettre le disque dur au GOC sans frais additionnels à la fin de la période de location et avant que l'appareil quitte les édifices fédéraux. De nombreux appareils MFD de Ricoh sont certifiés au moyen du profil de protection IEEE 2600, une norme de sécurité de technologie de l'information développée par l'industrie de la bureautique. La norme définit les exigences minimales des caractéristiques de sécurité.

Relier le tout

Les ministères fédéraux, les sociétés d'État et les organismes gouvernementaux doivent lutter contre un large éventail de menaces de sécurité de l'information. Vous devez aussi aborder de nombreuses exigences en matière de sécurité de l'information – incluant la conformité aux Services partagés Canada, au Centre de la sécurité des télécommunications Canada et au Conseil du Trésor.

Les solutions de sécurité des appareils, des données et des documents de Ricoh pour le gouvernement offrent un ensemble complet de fonctions de sécurités et d'outils pour aider à protéger l'information secrète, personnelle, confidentielle et sensible. Ricoh aide ses clients dans le secteur du gouvernement à mieux exploiter l'information en fournissant l'accès à l'information à partir de n'importe où et en tout temps tout en aidant à respecter les normes de sécurité de l'information prescrites.

RICOH
imagine. change.
imaginer. changer.

