Guide des bases de la sécurité de Ricoh

Favoriser la transformation d'affaires dans les milieux de travail numériques modernes grâce à la sécurité à plusieurs niveaux

La nécessité de s'insérer dans un environnement axé sur le numérique a accéléré le changement transformationnel chez les entreprises modernisant leurs capacités pour répondre aux demandes des marchés en évolution. Ce changement crée un paysage souvent fragmenté d'outils et de technologies dont découlent des lacunes liées à la sécurité, à la confidentialité et aux opérations.

Le maintien de la sécurité et de la conformité, notamment la protection contre les brèches de données pour les gens, les procédures et les technologies, est un effort constant qui doit être abordé de manière holistique, dans toutes les facettes des affaires.

Même si l'atteinte des importants objectifs d'affaires dépend de la sécurité, cette dernière est trop peu souvent intégrée à la stratégie d'affaires globale. Comment les organisations peuvent-elles faire de la sécurité un élément stratégique de leur transformation d'affaires pour favoriser l'atteinte d'objectifs liés, notamment, à l'image de marque de confiance, à la conformité, à l'innovation, à la continuité des affaires et à la durabilité?

Image de marque de confiance	Conformité	Innovation	Continuité des affaires	Durabilité
Penser pour la transparence et la confiance	Respecter les réglementations et surpasser les attentes	Croître avec confiance et acquérir un avantage concurrentiel	Garantir le succès face à tous les défis	Protéger la communauté

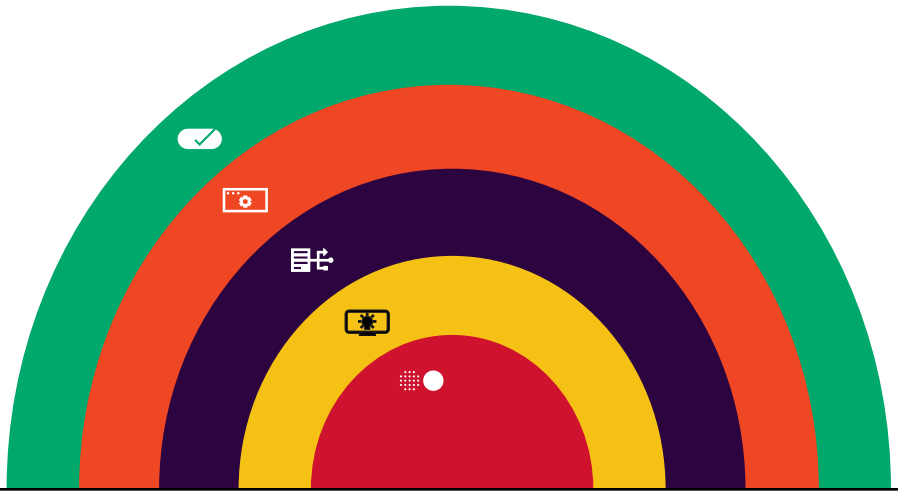
Ricoh offre les outils et les conseils d'experts dont ont besoin les organisations d'aujourd'hui pour protéger leur information et pour favoriser leur succès. Nous le faisons en adoptant une approche stratégique à plusieurs niveaux qui gouverne l'information et qui assure une protection contre les vulnérabilités dans tous les secteurs de l'entreprise.

La conception de nos services, de nos solutions et de nos appareils est basée sur la sécurité et sur les données, de la création initiale à la mise en œuvre. Nos services de sécurité à la fine pointe, y compris nos services gérés et nos services de consultation, complètent les niveaux de protection de nos appareils et de nos solutions dans le but d'optimiser la sécurité des documents, des données, des appareils ainsi que de l'information.

Ce n'est que lorsque la sécurité devient une priorité dans plusieurs facettes d'une organisation que des changements significatifs et répandus peuvent survenir.

Dans cet aperçu, vous découvrirez comment Ricoh fait appel à une approche à plusieurs niveaux pour rendre la sécurité et la conformité stratégiques dans le cadre de la transformation d'affaires.

- Sécurité du personnel
- Sécurité de l'information
- Sécurité des appareils
- Sécurité des réseaux
- Sécurité des applications



1er niveau — Sécurité du personnel

Créer une culture de sécurité au sein du personnel

En cette époque où les cybermenaces ciblent les entreprises de toute taille, l'établissement d'une culture de sécurité au sein du personnel n'est pas qu'un objectif lié aux TI, c'est un impératif. Les organisations sont les cibles de brèches de sécurité qui peuvent entraîner des pertes financières, endommager leur réputation ou les soumettre à une surveillance réglementaire. Même si la technologie est un élément essentiel à toute stratégie de sécurité, les spécialistes de la sécurité savent que le facteur humain ne doit pas être négligé.

La création d'un milieu de travail axé sur la sécurité et d'une culture organisationnelle sécuritaire devrait être la priorité de toutes les planifications des organisations modernes.

Le facteur humain : atout et vulnérabilité

Les employés, même s'ils sont l'un de vos plus importants atouts, peuvent devenir vulnérables s'ils ne sont pas équipés des connaissances et des outils nécessaires à la prise de décisions intelligentes et sécuritaires. La vigilance est au cœur de cet enjeu, et son maintien dépend autant de la culture que de la technologie.

Pour limiter les risques, il est essentiel d'offrir aux employés les éléments suivants :

- **Expériences de travail sécuritaires :** créer un environnement de travail fluide qui comprend des outils intelligents et des procédures sécurisées.
- **Politiques :** transmettre clairement les directives de gouvernance de l'information liées à l'accès et traitement des données, au signalement et à la reprise.
- **Autonomisation :** inculquer la confiance et les capacités nécessaires pour repérer et éviter les éventuelles menaces de sécurité.
- **Solutions de rechange à l'informatique de l'ombre :** utiliser des solutions sécurisées officiellement approuvées qui éliminent le besoin, pour les employés, de trouver des solutions de contournement non sécurisées.

Éducation favorisant l'autonomisation

La formation de sensibilisation à l'égard de la cybersécurité est conçue pour aborder la sécurité avec les personnes qui se retrouvent souvent aux premières lignes. En s'assurant que les membres de l'équipe connaissent les risques et en leur transmettant les pratiques exemplaires, on peut transformer ces employés, qui pourraient autrement représenter un risque, en vigilants gardiens de la forteresse numérique de leur organisation.

Voici ce que comprend la formation de sensibilisation :
- **Programmes de formation holistique :** éducation continue évoluant selon les menaces émergentes
- **Renforcement régulier :** rappels continus visant à maintenir la sécurité au premier plan
- **Stratégies efficaces :** recours à des anecdotes et à des scénarios qui illustrent les tâches quotidiennes du personnel
- **Évaluation des connaissances :** suivi de la progression et test de compréhension qui garantissent la préparation

Adoption d'une approche de sécurité du personnel à plusieurs niveaux

Puisque les menaces de cybersécurité comportent de multiples facettes, il est essentiel d'adopter une approche globale qui comprend la sécurité, la confidentialité et les risques liés aux affaires. Ce type d'approche permet aux dirigeants d'entreprise d'accomplir les tâches suivantes :

- **Évaluer l'impact du risque :** bien comprendre les répercussions possibles des diverses menaces
- **Repérer les vulnérabilités :** cibler proactivement les faiblesses de votre posture de sécurité avant qu'elles ne soient exploitées
- **Faire preuve de prévention :** faire appel à des stratégies de gestion du risque pour limiter la vulnérabilité aux brèches de sécurité
- **Limiter les dommages potentiels :** concevoir un plan d'intervention en cas d'incident et réaliser régulièrement des formations et des exercices

En offrant des consultations et en mettant en place un cadre de gouvernance basé sur les pratiques exemplaires liées aux risque et à la conformité, les entreprises peuvent établir une culture de travail robuste, sécurisée et axée sur les données. L'objectif est de former le personnel à l'égard des mécanismes des menaces de sécurité pour qu'il soit entièrement intégré aux mécanismes de défense de l'organisation.

Bâtir sur la confiance

La culture de sécurité au sein du personnel ne se traduit pas que par la défense contre les menaces. Elle sert également à favoriser la croissance et l'innovation au sein d'un cadre de travail bâti sur la confiance. Les employés qui font confiance à leur environnement de travail et aux politiques de sécurité de leur organisation sont plus susceptibles d'utiliser de manière complète et responsable les ressources de l'entreprise et de représenter sa marque avec intégrité.

Le parcours de création d'une culture de sécurité au sein du personnel évolue continuellement et il est sans fin. Tous les niveaux de l'organisation, en commençant par la haute direction, doivent s'engager à y participer. Les organisations qui investissent dans la formation, dans l'adoption des pratiques exemplaires et dans l'établissement d'une culture qui valorise la vigilance sont en mesure de se défendre contre les menaces, mais aussi de façonner un avenir sécuritaire.

L'intégration des plus récentes tendances en matière de formation, de technologie et de consultation stratégique favorise la transformation d'affaires qui offre aux organisations une protection contre les menaces numériques d'aujourd'hui, mais qui les préparent aussi aux défis de l'avenir.

2e niveau — Sécurité de l'information

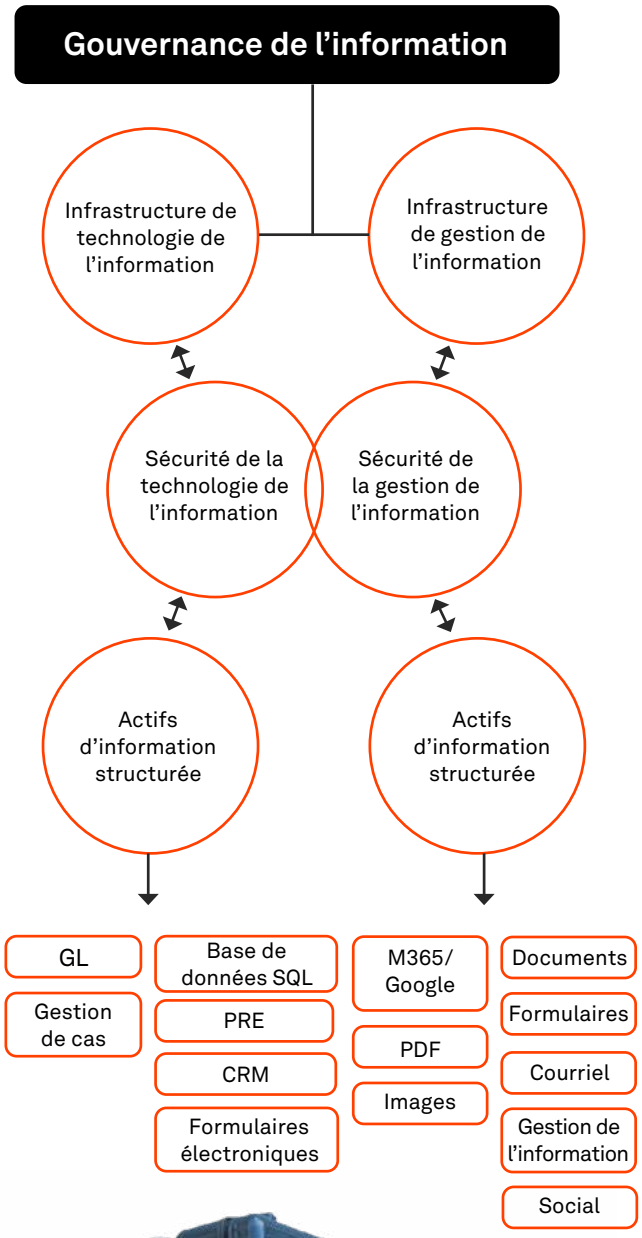
Pour protéger votre information, vous devez d'abord savoir quel type d'information vous possédez, où vous la stocker et les risques que cette information entraîne pour votre organisation. En transformant les données brutes en renseignements structurés et exploitables pouvant faire l'objet de recherches, vous pouvez découvrir de l'information qui vous aidera à prendre de meilleures décisions et à mettre en place les niveaux appropriés de protection.

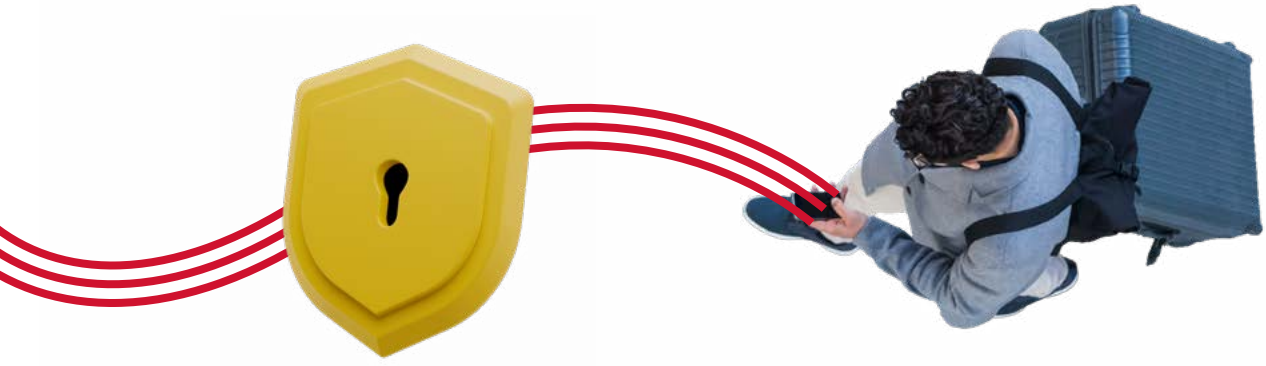
Gouvernance de l'information

Maintenir le contrôle de votre information pour optimiser vos activités et votre protection contre les menaces ainsi que pour garantir votre conformité réglementaire et juridique exige des politiques et des programmes globaux basés sur des normes internationales. La gouvernance de l'information concerne l'orchestration de la création, de la cueillette, de la gestion, de la rétention et de l'élimination de l'information à l'échelle de l'organisation.

L'élaboration de politiques de gouvernance de l'information qui respectent les normes exige l'expertise de spécialistes certifiés orientés par des directives visant à respecter les besoins de votre organisation. Les services de gouvernance de l'information aident les organisations à respecter les politiques de sécurité et à atteindre la conformité à l'égard de diverses réglementations fédérales, provinciales et municipales ainsi que divers règlements de l'industrie, en plus de leur donner la capacité d'effectuer des vérifications et de prouver leur conformité d'une manière efficace.

Toute transaction entre une entreprise et un intervenant laisse une trace de données. Il peut s'agir de données hautement confidentielles, comme des renseignements d'identification personnelle ou de l'information de l'industrie de carte de paiement, qui exigent des mesures de sécurité, de confidentialité et de contrôle de la découverte. D'autres données, que l'on nomme les données redondantes, obsolètes ou insignifiantes (ROT, redundant, obsolete, trivial), n'ont aucune valeur et occupent inutilement de l'espace. On estime que les données ROT comptent pour, au minimum, 25 à 30 % des données d'entreprise. Certaines sources estiment que ce pourcentage est beaucoup plus élevé.





Plus de 90 % des données ne sont pas structurées[1]

Les données non structurées sont des renseignements n'ayant pas été organisés dans une base de données traditionnelle et structurée, ce qui signifie qu'ils sont inaccessibles, qu'ils ne font pas l'objet d'un suivi et qu'ils ne peuvent être utilisés à titre d'information d'affaires. Si vous ne gérez pas votre répertoire de données, dont la plupart sont non structurées, vous risquez de stocker des volumes élevés de données ROT, vous exposez votre organisation à des risques et la rendez vulnérable aux brèches.

Les données non structurées sont un important facteur pouvant entraîner des atteintes à la sécurité, des violations à la vie privée, des coûts élevés en matière de TI ainsi que de pénalités liées à la non-conformité. Lorsqu'on pense à la cybersécurité, il faut savoir que les données non structurées sont souvent des cibles faciles pour les cybercriminels qui tentent d'accéder plus profondément aux systèmes. Ces derniers cherchent des renseignements monétisables comme des noms, des adresses, des dates de naissance, des numéros d'assurance sociale, des mots de passe, des numéros de cartes de crédit, des données bancaires ou des contrats. Malheureusement, les données confidentielles se trouvent souvent au sein même de l'infrastructure, ce qui complexifie leur suivi et leur protection.

Voici quatre domaines clés d'amélioration de la gouvernance de l'information qui permettent de limiter les risques :

1

Plateforme de gestion des dossiers et de l'information

La mise en place d'un programme de gestion des dossiers et de l'information (RIM, records information management) garantit que les organisations respectent les exigences réglementaires et juridiques en plus d'améliorer l'efficacité de l'accès à l'information. Les pratiques adéquates de gestion des dossiers et de l'information, appuyées par une plateforme sécurisée, contribuent à la protection de l'information grâce à un stockage sécurisé, à un contrôle des accès, à des pistes de chiffrement et d'audits ainsi qu'à la réduction des risques de sécurité et de confidentialité.

Il est essentiel d'établir des politiques de gouvernance, élaborées en collaboration avec des spécialistes certifiés de la gestion des dossiers, qui englobent l'information de toute l'organisation, qui sont soutenues par des pratiques et des technologies qui favorisent la gouvernance tout au long du cycle de vie des renseignements, de leur collecte à leur élimination, en passant par leur stockage. Ce faisant, les organisations peuvent se protéger contre les brèches et maintenir l'intégrité et la confidentialité des données critiques, tout en rehaussant la confiance et la fiabilité.

2

Analyse de fichiers et outils de classification

La mise en place d'un programme de gestion des dossiers et de l'information (RIM, records information management) garantit que les organisations respectent les exigences réglementaires et juridiques en plus d'améliorer l'efficacité de l'accès à l'information. Les pratiques adéquates de gestion des dossiers et de l'information, appuyées par une plateforme sécurisée, contribuent à la protection de l'information grâce à un stockage sécurisé, à un contrôle des accès, à des pistes de chiffrement et d'audits ainsi qu'à la réduction des risques de sécurité et de confidentialité.

Il est essentiel d'établir des politiques de gouvernance, élaborées en collaboration avec des spécialistes certifiés de la gestion des dossiers, qui englobent l'information de toute l'organisation, qui sont soutenues par des pratiques et des technologies qui favorisent la gouvernance tout au long du cycle de vie des renseignements, de leur collecte à leur élimination, en passant par leur stockage. Ce faisant, les organisations peuvent se protéger contre les brèches et maintenir l'intégrité et la confidentialité des données critiques, tout en rehaussant la confiance et la fiabilité.

3

Politique et mise en œuvre alimentées par des spécialistes

L'établissement d'une politique de gouvernance de l'information approuvée par la direction offre un cadre de travail et des mesures de contrôle qui permettent de gérer efficacement le traitement de l'information. La gouvernance contribue à l'atténuation des risques organisationnels et garantit que les technologies et les comportements respectent les exigences réglementaires et juridiques. Lorsque les politiques et les directives sont mises en place, les procédures efficaces de protection des données peuvent être inculquées au personnel et intégrées aux procédures et aux technologies.

[1] IDC. "High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises," July 2022.

Les politiques devraient aborder la gestion des dossiers et de l'information, les mesures de contrôle de la confidentialité ainsi que la sécurité des données. Des directives organisationnelles expliqueront les procédures, les flux de travaux et les protections dans des communications et des guides opérationnels. Les rôles et les responsabilités y seront également clairement définis. Des formations régulières sont également nécessaires à mesure que les activités et les réglementations évoluent. Des technologies peuvent être mises en place pour activer les mesures de contrôle, automatiser les procédures ainsi que pour mesurer les résultats, en faire le suivi et produire des rapports à leur égard.

4

Politiques et procédures de gestion du cycle de vie des données
L'objectif de cette pratique exemplaire en matière de sécurité est de limiter le risque auquel une organisation est exposée grâce à la gestion des données, y compris les données confidentielles et l'information précieuse, pendant toute leur durée de vie. Les équipes de services professionnels et de services gérés de Ricoh peuvent vous aider à toutes les étapes de cette procédure.

Les politiques et les procédures portant sur la rétention et l'élimination établissent le cycle de vie des données et le traitement réservé aux différentes catégories de données. Les politiques de rétention peuvent établir le moment et la façon dont vos données sont déplacées de vos répertoires actifs à vos archives ou à un répertoire en nuage hors site ou dont elles sont purgées de vos systèmes conformément aux politiques. Les services d'élimination en fin de vie regroupent les données à nettoyer des appareils multifonctions afin d'assurer que la mémoire non volatile (NVRAM) et les lecteurs des appareils retirés des clients soient complètement nettoyés avant d'être éliminés.

Automatisation des procédures d'affaires

Alors que les façons dont nous communiquons, collaborons et créons évoluent, le besoin de solutions simples, sécuritaires et durables se manifeste de plus en plus. Nos activités principales — obtenir, créer, saisir et gérer de l'information — sont essentielles à notre succès et doivent, par conséquent, être protégées contre les menaces.

L'automatisation a créé de nouvelles méthodes d'apprentissage lié au travail en rehaussant l'efficacité, en offrant aux employés plus de temps pour se concentrer sur les tâches de haute valeur, en fournissant des analyses holistiques qui accélèrent la prise de décision et en intégrant des flux de travaux qui harmonisent l'expérience.

L'automatisation permet également une surveillance intelligente complète, un suivi des anomalies et des menaces ainsi qu'une réponse rapide à leur égard, l'atténuation des risques et l'amélioration de la conformité.

La mise en place d'une technologie alimentée par l'IA peut rehausser encore davantage la résilience tout en maintenant l'efficacité et la productivité. En analysant les données historiques, qui lui permettent de reconnaître les tendances de l'information et les comportements des utilisateurs, l'IA peut prévoir les risques de sécurité. L'IA joue également un rôle dans le chiffrement de l'information qui circule au sein de l'organisation, en utilisant des techniques de masquage des données qui protègent les données contre les interceptions.

L'automatisation robotisée des processus (ARP) fournit aux organisations une main-d'œuvre virtuelle ou des robots qui s'attaquent aux tâches répétitives dans le but d'accélérer les méthodes de travail. Les outils d'ARP possèdent leurs propres normes de sécurité comportant des mesures de chiffrement pour entreprise, l'accès fondé sur des rôles et des permissions, l'authentification au moyen d'Active Directory, le chiffrement des bases de données et bien plus encore.

Circulation de l'information :
saisie, connexion et sécurisation de l'information entrant dans votre organisation, en sortant et y circulant

Information entrante

L'information entrante, comme les courriels, le courrier, les formulaires soumis virtuellement, les documents numérisés et les données issues du commerce électronique, doit être reçue et traitée de manière sécuritaire dans le cadre de toute initiative d'automatisation des procédures d'affaires. En intégrant cette information aux flux de travaux automatisés et sécurisés, vous pouvez garantir que vos données sont en sécurité et contribuer à la conformité et à la gouvernance de l'information.

Les données numérisées exigent une protection particulière dès leur naissance et pendant toute leur durée de vie. Les documents numériques et les documents numérisés, les formulaires, les télécopies, les images saisies et toutes les autres données entrent dans les systèmes de votre organisation par différents moyens, vous devez donc choisir judicieusement la façon dont vous protégez ces précieux renseignements.

L'automatisation de la saisie, de la classification, de l'extraction et de l'exportation des données peut accélérer le flux d'information et, ainsi, faciliter leur accès pour les personnes en ayant besoin. Le contrôle et la gouvernance des accès à l'information, en particulier pour l'information confidentielle au format numérique, exigent de redoutables capacités de sécurité sur de multiples points de contact.

Les données confidentielles, comme les renseignements d'identification personnelle, l'information de propriété intellectuelle et les renseignements fiduciaires, peuvent entraîner de lourdes amendes si elles ne sont pas protégées. Toutefois, pour que de telles données non structurées puissent être protégées, elles doivent être transformées en données structurées exploitables. Voyons ensemble comment les éléments suivants peuvent contribuer à la protection de vos précieuses données.

1 **Procédure de saisie intelligente de document**

Les solutions de saisie intelligente convertissent les documents dans un format sécurisé et structuré afin que les données puissent être exportées dans toute application ou tout flux de travaux ou répertoire, comme les systèmes de planification des ressources d'entreprise (PRE), de gestion de contenu d'entreprise (GCE), de gestion des relations avec les clients (CRM, Customer Relationship Management), d'automatisation robotisée des processus (ARP), d'analyse ou de secteur d'activités ou encore des plateformes d'intégration en tant que service (iPaaS).

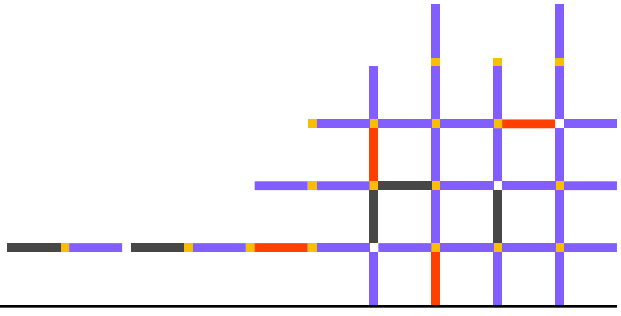
Les documents doivent d'abord être numérisés ou convertis au format numérique. Au cours du processus de numérisation, des méthodes d'authentification veillent à ce que les utilisateurs et les administrateurs puissent verrouiller l'accès à certaines procédures et même limiter ce que les utilisateurs peuvent voir, dans le but d'empêcher l'utilisation inappropriée. Il est également possible de protéger les fichiers convertis au moyen de paramètres, de permissions et de mesures de contrôle des mots de passe.

La majorité des solutions de saisie intelligente ne stockent pas les données, elles acheminent simplement les données transformées numériquement à d'autres applications ou répertoires. Puisque l'information peut être compromise si elle est interceptée, des mesures de sécurité sont mises en place dans le but de la protéger. Des services en nuage font également appel à des mesures de chiffrement, de déchiffrement et d'authentification intégrées ainsi qu'au protocole de sécurité de la couche de transport (TLS) dans le cadre des transmissions.

2 **Formulaires électroniques sécurisés**

Les formulaires électroniques sont une manière cohérente de soumettre de l'information dans un système et peuvent être une solution de rechange aux approches faisant appel au courriel ou au papier. Toutefois, des formulaires électroniques mal codés ou mal protégés peuvent entraîner des risques en matière de sécurité.

En effet, un formulaire n'ayant pas été proprement sécurisé peut servir de passerelle à de l'information falsifiée ou faciliter les tentatives d'introduction de code malveillant. Des logiciels de création de formulaires intelligents peuvent accomplir le travail difficile à votre place et en arrière-plan, notamment la création de formulaires adéquats incluant des fonctions comme des champs de signature électronique, des services de location, des contrôles d'accès, la gestion des pièces jointes et, plus particulièrement, la gestion des flux de travaux. Surveillez et analysez vos flux de travaux basés sur les formulaires en obtenant un suivi complet des procédures essentielles en plus d'approuver ou de rejeter les soumissions de formulaire avant qu'elles poursuivent leur chemin.



Information sortante

Gérer de manière sécuritaire de grands volumes de données tout en respectant les audits et les contrôles réglementaires peut sembler difficile. Pourtant, un système de données qui gère votre information de manière sécuritaire, qui automatise vos flux de travaux de manière fluide et qui permet l'accès à distance est essentiel à l'optimisation des procédures de votre milieu de travail hybride.

Comment pouvez-vous y arriver tout en vous assurant que vos données sont protégées contre les menaces externes, les brèches de sécurité internes (accidentelles ou délibérées), les pertes de données ou les violations de conformité?

1 **Contrôle de la production d'impression**
Les imprimantes multifonctions favorisent la production efficace pour de multiples utilisateurs en plus de leur permettre de protéger l'information imprimée. Que la tâche d'impression soit transmise depuis un ordinateur ou un appareil mobile, l'impression d'information confidentielle est contrôlée par une personne autorisée. De plus, la facturation et le suivi complet des coûts permettent un contrôle exhaustif des comportements des utilisateurs et offrent une manière d'identifier les tendances inhabituelles et les abus.

2 **Relâchement sécuritaire de documents**
L'intégration du relâchement sécuritaire de documents permet d'empêcher que l'information confidentielle envoyée sur des serveurs d'impression centraux ou des services en nuage soit récupérée par erreur ou par des personnes cherchant à la voler. Plutôt que d'être transmises directement à un appareil, les tâches d'impression sont chiffrées et conservées dans la file d'attente d'impression d'où elles proviennent, dans un serveur ou dans le nuage.

Ainsi, l'utilisateur peut uniquement relâcher l'impression lorsqu'il se trouve devant l'appareil de son choix et après s'être authentifié. La file d'attente d'impression peut être sur le site ou en nuage, et les données d'impression peuvent être transmises au moyen d'une connexion Web et être chiffrées tout au long de leur transit.

3 **Impression mobile**
Compte tenu de l'évolution des comportements de la main-d'œuvre, la capacité d'imprimer à partir d'un appareil mobile est maintenant essentielle dans de nombreuses organisations. Cette capacité exige de réfléchir à la fois aux procédures et aux infrastructures technologiques. L'une des procédures pouvant être mises en place, le relâchement des impressions par authentification, permet aux utilisateurs d'empêcher que les renseignements confidentiels soient laissés sans surveillance dans une imprimante en exigeant qu'ils s'authentifient au moyen d'un appareil mobile.

L'imprimante est sélectionnée sur l'appareil mobile, et l'impression est produite lorsqu'une personne est présente pour la relâcher et pour récupérer l'information de manière sécuritaire. Pour ce qui est de l'infrastructure, il est possible de protéger le flux des données d'impression et de gérer les procédures d'impression mobile en choisissant parmi diverses méthodes de déploiement selon les politiques de sécurité. Ces méthodes peuvent impliquer des serveurs d'impression mobile sur site ou des plateformes d'impression mobile en nuage. Les activités menées à partir d'appareils mobiles peuvent faire l'objet d'un suivi et de rapports détaillés sur les utilisateurs, de plus, les appareils d'impression traditionnelle permettent de faire un suivi des impressions. Il est également possible de gérer les appareils mobiles.

4 **Impression à base de règles**
Les règles d'impression peuvent limiter le nombre de pages pouvant être imprimées sur un appareil, restreindre l'utilisation de la couleur, imposer l'option recto verso, limiter l'accès à certains paramètres et bien plus encore. Des limites de comptes budgétaires pour les copies et les impressions peuvent être établies par les utilisateurs et elles comprennent le suivi des activités effectuées directement sur une imprimante multifonction.

La prévention de la mauvaise utilisation des ressources réduit les coûts d'exploitation, restreint l'activité des utilisateurs dans le but de renforcer leur imputabilité et fournit des renseignements, au moyen d'analyses, pour repérer les irrégularités.

Puisque les utilisateurs doivent s'authentifier pour imprimer, les règles d'impression que vous établissez sont automatiquement appliquées et l'activité est réattribuée à l'utilisateur. Les utilisateurs peuvent lier l'impression, la numérisation et la télécopie de certains documents à un client, un projet ou un cas précis aux fins de facturation, ce qui permet d'obtenir des rapports d'activités détaillés à l'égard d'un projet ou d'un sujet confidentiel.

5

Solutions d'impression sécurisée en nuage

Compte tenu de la popularité grandissante du travail hybride, l'impression dans le nuage est désormais essentielle pour veiller à la sécurité dans le partage d'information, pour réduire les coûts ainsi que pour maintenir la productivité des employés, peu importe l'endroit où ils travaillent. Dans le cas de l'impression en nuage, il convient de faire appel à une combinaison des trois fonctionnalités de sécurité suivantes :

- Vérification systématique
- Authentification
- Chiffrement
- Suivi à distance

6

Envoi de télécopies dans le nuage

Vous pouvez réduire les risques associés aux télécopieurs autonomes et remplacer l'acheminement manuel par une procédure de livraison automatisée. Pour veiller à ce que les télécopies soient uniquement transmises aux destinataires voulus, il convient généralement de tirer parti de l'authentification sécurisée, de protocoles de chiffrement, du chiffrement des données au repos et de règles d'acheminement. L'automatisation élimine le traitement du papier et réduit le risque que des documents soient récupérés par des personnes non autorisées.

Vous pouvez respecter les exigences en matière de conformité et de politique en imposant un contrôle administratif à votre environnement de télécopie au moyen de la transmission et de la réception vérifiables des documents, de pistes de vérification complètes des activités et de l'accès aux télécopies archivées de toutes les transactions de télécopies reçues et envoyées.

3e niveau – Sécurité des appareils

Les menaces en matière de cybersécurité ne se limitent plus seulement aux ordinateurs personnels, aux serveurs ou aux réseaux. Les appareils — y compris les imprimantes réseau de base — nécessitent des contre-mesures face à un vaste éventail de menaces. Compte tenu de l'évolution des fonctionnalités des imprimantes multifonctions, ces dernières sont devenues d'importants actifs TI. Alors que la capacité informatique de la catégorie d'appareils « imprimantes et copieurs » a connu une croissance, les menaces se sont multipliées, notamment les suivantes :

- Accès malveillant par l'entremise des réseaux
- Espionnage et altération de l'information contenue sur les réseaux
- Infractions aux politiques de sécurité causées par inadvertance
- Accès non autorisé par l'entremise du panneau de commande d'un appareil
- Accès inapproprié au moyen de lignes de télécopieurs
- Fuite d'information au moyen de documents imprimés
- Fuite d'information à partir d'une unité de stockage

Espérer simplement que vous ne serez pas touché n'est pas une solution. Les technologies, la diligence et les connaissances supérieures sont essentielles. Elles exigent une compréhension approfondie des façons d'aborder les problèmes de sécurité dus aux vulnérabilités de vos appareils, des données qu'ils traitent et des réseaux auxquels ils se connectent.

Authentification des appareils

Il est essentiel de contrôler les accès au moyen de l'authentification basée sur vos politiques de sécurité. Les appareils sains et sécurisés offrent un autre niveau essentiel de sécurité, y compris la surveillance à distance de la configuration des appareils, des alertes liées à la consommation et aux fournitures, des alertes de services critiques et des avertissements quant aux enjeux de services à venir.

1 **Authentification des utilisateurs aux appareils**
La possibilité de faire un suivi et de contrôler l'utilisation ainsi que d'empêcher les accès non autorisés repose sur l'obligation pour les utilisateurs de s'authentifier avant de pouvoir imprimer, numériser, télécopier, etc. Après s'être authentifiés, les utilisateurs ne voient que les fonctionnalités qu'ils sont autorisés à utiliser sur l'appareil. Diverses options d'authentification vous donnent également la possibilité de contrôler les niveaux d'autorisation accordés à chaque utilisateur ou groupe d'utilisateurs. Il peut s'agir de restreindre la possibilité de modifier les paramètres de l'appareil et de visualiser les entrées du carnet d'adresses ou de donner accès à des flux de travaux de numérisation, à des serveurs de documents et à d'autres fonctions. De plus, la fonction de verrouillage des utilisateurs, qui se déclenche en cas de détection d'une fréquence élevée de tentatives de connexion réussies ou échouées, aide à se prémunir contre les attaques par déni de service et les déchiffrages de mots de passe par force.

2 **Authentification des utilisateurs réseau**
Les appareils Ricoh permettent l'authentification des utilisateurs réseau afin de bloquer l'accès des utilisateurs non autorisés. Par exemple, la fonction d'authentification Windows® vérifie l'identité de l'utilisateur à partir de l'appareil multifonction grâce à la comparaison des identifiants (nom d'utilisateur et mot de passe, badge d'identification avec ou sans NIP ou une combinaison des deux) avec les informations sur les utilisateurs autorisés contenues dans la base de données du serveur réseau Windows. Pour ce qui est de l'accès au carnet d'adresses principal, l'authentification LDAP (Light-weight Directory Access Protocol) valide l'identité de l'utilisateur selon le serveur LDAP, ce qui permet d'assurer que seuls les utilisateurs ayant un nom d'utilisateur et un mot de passe valide puissent avoir accès aux adresses courriel contenues sur le serveur LDAP.

Ricoh offre des solutions pour permettre aux clients ayant recours à l'authentification par carte à puce, y compris l'authentification par carte d'accès commun (CAC, Common Access Card) du Department of Defense des États-Unis ou par vérification d'identité personnelle (PIV, Personal Identity Verification), d'utiliser ce type d'outils.

Les logiciels comme Streamline NX de Ricoh, une suite modulaire prenant en charge les processus de numérisation, de télécopie, d'impression, de gestion des appareils, de sécurité et de comptabilité, fournissent des options d'authentification supplémentaires. Il s'agit notamment de l'authentification LDAP, Kerberos et SDK avec possibilité d'intégrations personnalisées.

3 **Authentification des appareils réseau**
Bon nombre d'appareils Ricoh sont compatibles avec le protocole d'authentification IEEE/802.1X, qui est souvent intégré aux mises en place de réseau doté d'une architecture à vérification systématique. Ce contrôle des accès aux réseaux faisant appel à un port permet à l'administrateur du réseau de limiter l'utilisation de ce dernier tant que l'appareil n'a pas été adéquatement authentifié. Cela garantit la sécurité des communications entre les appareils authentifiés et autorisés.

Protection des appareils

Le mauvais fonctionnement des appareils entraîne des temps d'arrêt qui engendrent des coûts, mais qui poussent également les utilisateurs à modifier leur comportement, notamment en ayant recours à des solutions de contournement peu recommandées.

Les mises à jour des micrologiciels des appareils peuvent être réalisées à distance, en lots, et être planifiées dans votre horaire.

1 **Gestion des micrologiciels et des pilotes**
Les organisations peuvent maintenir une ligne de défense en s'assurant de garder les micrologiciels de leurs appareils à jour grâce à la gestion proactive à distance, réalisée en collaboration avec leur fournisseur de service. Vous pouvez empêcher la désuétude de vos appareils d'impression en utilisant un portail en nuage à distance. La vérification du micrologiciel est réalisée à distance et la mise à jour peut être lancée automatiquement. Les mises à jour peuvent également être réalisées automatiquement selon un horaire précis.

Il est possible de mettre à jour les micrologiciels d'un vaste ensemble d'appareils ou d'un parc d'appareils entier par lot en peu de temps. Les pilotes peuvent également être préconfigurés et transmis aux appareils à distance. Vous pouvez configurer des ensembles de pilotes en établissant les paramètres par défaut appropriés selon vos politiques de sécurité et d'impression, ainsi que contrôler qui a accès à ces ensembles.

2 **Applications et micrologiciels ayant obtenu une signature numérique**
Si le logiciel intégré d'un appareil multifonction ou d'une imprimante — également connu sous le nom de micrologiciel — est modifié ou compromis, l'appareil auquel il est intégré peut alors être utilisé comme méthode d'intrusion dans le réseau de l'entreprise, servir de moyen pour endommager l'appareil ou constituer une plateforme ouvrant la porte à d'autres fins malveillantes. Bon nombre d'appareils conçus par Ricoh sont dotés du module de plateforme sécurisée (TPM, Trusted Platform Module), un module de sécurité matérielle qui valide les logiciels de base du contrôleur, le système d'exploitation, le BIOS, le chargeur de démarrage et les applications de micrologiciels.

Les appareils multifonctions et les imprimantes de Ricoh utilisent les signatures numériques pour déterminer la validité des micrologiciels et des applications. La clé publique utilisée pour cette vérification est stockée dans un secteur antiécrasement non volatil du TPM. Une clé de cryptage racine et des fonctions cryptographiques sont également contenues dans le TPM et ne peuvent pas être modifiées de l'extérieur. Ricoh utilise la procédure d'amorçage validé (Trusted Boot) comprenant deux méthodes de vérification de la validité des logiciels/micrologiciels :

- Détection des altérations
- Validation des signatures numériques

Les programmes et les micrologiciels ne peuvent pas être installés, puisque les ensembles n'étant pas dotés d'une signature numérique vérifiée ne peuvent pas être déployés. Puisqu'il couvre une gamme de logiciels, comme les programmes d'amorçage ainsi que les fonctions et applications finales, le processus d'amorçage validé procure une sécurité complète qui repose sur le TPM. Lorsque des applications ou des micrologiciels à jour sont téléchargés sur un appareil Ricoh, une procédure de vérification similaire recherche une signature numérique valide. Si la signature n'est pas validée, les mises à jour sont annulées et le fichier de mise à jour est supprimé. À ce moment, l'appareil redémarre automatiquement et le micrologiciel précédent reprendra sa place initiale. Si un micrologiciel est modifié, de toute autre façon, l'appareil de Ricoh empêchera l'exécution du micrologiciel malveillant en freinant le processus de démarrage et en affichant un code d'appel de service.

3 **Désactivation des protocoles et des services inutilisés**

En vue de faciliter l'ajout d'appareils réseau, les systèmes réseau de nombreux fournisseurs sont régulièrement expédiés au client avec tous les services et les protocoles réseau réglés sur « activé » ou « actif ». Toutefois, les services non utilisés sur les appareils réseau posent un risque de sécurité. Les ports compromis peuvent mener à diverses menaces, y compris la destruction ou la falsification des données stockées, les attaques par déni de service (DoS, Denial of Service) et les virus ou les logiciels malveillants entrant sur le réseau.

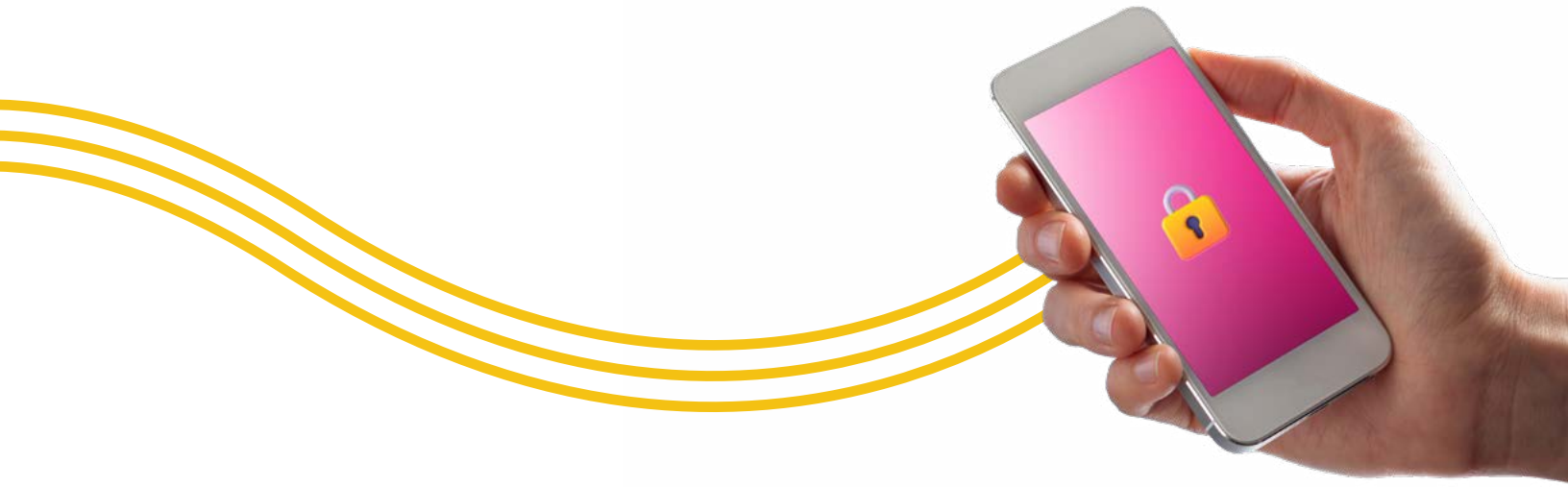
Il existe une solution simple, quoique souvent négligée, en ce qui concerne cette source de risque particulière : la désactivation de tous les services inutilisés. Les administrateurs des appareils Ricoh peuvent facilement verrouiller les services inutilisés, ce qui contribue à rendre les appareils moins susceptibles au piratage. De plus, des protocoles spécifiques, tels que SNMP ou FTP, peuvent être complètement désactivés afin d'éviter qu'ils ne soient exploités.

4 **Contrôle des accès**

L'administrateur peut limiter les appareils ou les protocoles pouvant être connectés aux appareils pour empêcher les accès indésirables. De plus, il peut établir un niveau de sécurité qui permet d'activer ou de désactiver un protocole et de configurer le statut du port. Il peut bloquer l'accès à un appareil, puis le permettre uniquement depuis ou vers l'adresse IP définie dans les filtres de réception et de transmission. Un maximum de cinq ensembles de filtres, comprenant une adresse IP, un numéro de port et un protocole peut être configuré pour la réception et la transmission.

5 **Sécurité des lignes de télécopie**

L'activation de la fonction de télécopie d'un appareil peut exiger de le connecter via une ligne téléphonique, ce qui signifie qu'il est essentiel de bloquer l'accès non autorisé potentiel via la ligne de télécopie. Le logiciel intégré Ricoh est conçu pour ne traiter que les types de données appropriées (c'est-à-dire les données de relatives aux télécopies) et envoyer ces données directement aux fonctions appropriées de l'appareil. Étant donné que seules les données de télécopie peuvent être reçues à partir de la ligne téléphonique, le risque d'accès non autorisé à partir de la ligne, du réseau ou des logiciels intégrés de l'appareil est éliminé.



L'unité de contrôle de télécopie (FCU, Facsimile Control Unit), dont sont dotés les appareils de Ricoh comprenant la fonction de télécopie, est compatible avec les protocoles de télécopie G3. Par conséquent, même si une connexion initiale est établie avec un terminal qui n'utilise pas ces protocoles, l'appareil multifonction considérera que la communication a échoué et mettra fin à la connexion. Cela empêche l'accès aux réseaux internes par les lignes de télécommunications et fait en sorte qu'aucune donnée illicite ne soit introduite par ces lignes.

6 **Simplification de la gestion des appareils**

Comme la gestion des appareils peut prendre beaucoup de temps, des failles de sécurité peuvent apparaître involontairement lorsque des aspects essentiels de la gestion des appareils ne sont pas adéquatement surveillés. Les logiciels de gestion des appareils de Ricoh, comme Streamline NX, offrent aux directeurs des TI un point de contrôle central pour surveiller leur parc d'appareils d'impression connectés à un réseau, peu importe si ceux-ci sont répartis sur plusieurs serveurs ou dans diverses régions géographiques, depuis une unique console de gestion.

Comment Ricoh procède :

- Communications entre les appareils et les serveurs chiffrées par le protocole SNMPv3
- Contrôles centralisés permettant aux administrateurs de contrôler les accès, de surveiller les paramètres de sécurité et de gérer les certificats des appareils
- Mises à jour automatisées des micrologiciels réduisant l'exposition potentielle des micrologiciels obsolètes
- Déploiement des versions des micrologiciels approuvées par le client ou des plus récentes versions offertes par Ricoh
- Fonctionnalité d'analyste de sécurité de la solution Streamline NX offrant un tableau de bord servant à l'évaluation de la conformité à la politique de sécurité des appareils et offrant une liste de vérification des pratiques exemplaires liées au respect des politiques par les appareils

7 **Compteurs et alertes**

Les avertissements hâtifs permettent aux équipes de résoudre les problèmes avant qu'un temps d'arrêt ne soit causé et, ainsi, réduisent les risques que des utilisateurs adoptent des comportements imprévus, notamment en faisant appel à des solutions de contournement non autorisées. En effet, lorsque les appareils ne fonctionnent pas comme prévu, les utilisateurs ont tendance à choisir d'autres plans d'action qui ne sont pas toujours sécuritaires. Par exemple, ils peuvent effectuer une impression ou une numérisation sur un appareil local sans pouvoir vérifier l'activité ou protéger les données.

Le recours à des logiciels de surveillance et de gestion de vos appareils vous permet de recueillir de l'information et de maintenir le bon fonctionnement de vos appareils par l'envoi d'alertes en temps opportun. Cela comprend la collecte automatique des données des compteurs, basée sur votre horaire établi, des alertes de niveau faible ou épuisé de toner, des alertes de services critiques ainsi que des avertissements à l'égard des enjeux de services à venir.

8 **@Remote.NET**

Les améliorations que le connecteur @Remote Connector NX de Ricoh apporte à la solution Streamline NX permettent de recueillir les alertes de services critiques à venir et les transmettent directement à votre fournisseur de service. Ce dernier est donc en mesure de planifier les mises à jour des micrologiciels à distance et de les mettre en œuvre immédiatement. Le connecteur @Remote collecte aussi les lectures de l'appareil et les rend disponibles selon un horaire préétabli, de pair avec les alertes de niveaux de consommables, afin de maintenir le temps de fonctionnement et de diminuer le fardeau administratif. Les données recueillies peuvent être consultées dans le portail Web @Remote.NET.

9 **Sécurité des ports physiques**

Les ports physiques (USB, carte SD, etc.) des appareils Ricoh peuvent être contrôlés par l'administrateur de l'appareil. Ainsi, ils peuvent empêcher les utilisateurs de stocker des éléments sur des dispositifs de mémoire externe ou d'imprimer depuis ce type de dispositif.

Type de chiffrement

1 **Chiffrement du disque dur et de la mémoire (données au repos)**
Même si le disque dur est physiquement retiré d'un appareil Ricoh, les données chiffrées ne peuvent pas être lues. Lorsqu'elle est activée, la fonctionnalité de chiffrement du disque dur peut contribuer à la protection de ce dernier ainsi que de la mémoire RAM non volatile contre le vol de données, tout en aidant les organisations à respecter leurs politiques de sécurité. Le chiffrement comprend les données stockées dans le carnet d'adresses d'un système, ce qui réduit le risque que les employés, les clients ou les fournisseurs d'une organisation voient leurs informations détournées et potentiellement ciblées.

Voici les autres types de données (qui sont stockées dans la mémoire non volatile ou sur le disque dur des imprimantes multifonctions) pouvant être chiffrées :

- Carnet d'adresses
- Données sur l'authentification des utilisateurs
- Documents stockés de manière temporaire ou permanente
- Registres
- Configurations de l'interface réseau
- Information sur la configuration

2 **Chiffrement des appareils réseau (données en transit)**
Il est possible pour un pirate informatique connaisseur d'intercepter des flux de données brutes, des fichiers et des mots de passe pendant que l'information circule au sein du réseau. Sans la protection adéquate, l'information non chiffrée peut être volée, altérée, falsifiée et réintégrée dans le réseau à des fins malveillantes. Pour prévenir ces problèmes, Ricoh utilise le chiffrement et des protocoles de sécurité réseau robustes qui peuvent être configurés en fonction des besoins du client. À titre d'exemple, le protocole de sécurité de la couche de transport (TLS) est utilisé afin de maintenir la confidentialité et l'intégrité des données transmises d'un terminal à un autre. Bon nombre d'appareils Ricoh sont compatibles avec la plus récente version du protocole TLS, soit la version 1.3.

3 **Chiffrement du flux d'impression**
Les données contenues dans un flux d'impression peuvent être interceptées et exploitées si elles ne sont pas chiffrées. Ricoh peut permettre le chiffrement des données d'impression au moyen des protocoles de chiffrement SSL et TLS via le protocole d'impression Internet (IPP), ce qui sécurise les données entre les postes de travail et les imprimantes et appareils multifonctions du réseau. Comme il s'agit d'un protocole qui aide à maintenir la confidentialité des données, une personne tentant d'intercepter les flux de données d'impression chiffrées en transit n'obtiendrait que des données indéchiffrables. Les données transmises aux imprimantes sans être chiffrées peuvent faire l'objet d'une attaque ou d'une utilisation malveillante.

4 **Chiffrement complet par pilote**
Les inquiétudes liées aux attaques malveillantes touchant les données d'impression peuvent être dissipées grâce au pilote d'impression universel de Ricoh qui permet le chiffrement complet des données circulant entre le système de l'utilisateur et l'appareil multifonction Ricoh. Le chiffrement complet peut être activé dans la fenêtre de dialogue d'impression qui permettra à l'utilisateur d'établir un mot de passe pour le chiffrement. S'il souhaite relâcher une tâche d'impression, l'utilisateur doit entrer le mot de passe de chiffrement dans l'appareil Ricoh, qui peut ensuite déchiffrer les données et lancer l'impression. Cette méthode de chiffrement des données d'impression fait appel au protocole AES-256.

5 **Communications IPsec**
Les imprimantes multifonctions de Ricoh peuvent faire appel au protocole IPsec pour chiffrer les communications. Ce protocole permet aux communications de circuler en ensemble sécurisé au niveau du protocole IP. Même si aucune méthode de chiffrement n'est utilisée par un protocole supérieur ou une application, le protocole IPsec rehausse la sécurité et empêche l'accès au contenu des communications ou sa modification.

Autres fonctionnalités de sécurité

1 **Impression verrouillée**
Les documents imprimés laissés sur les bacs de sortie ou oubliés peuvent être récupérés par n'importe qui. Cela constitue un risque relativement à la sécurité de l'information, d'autant plus lors de l'impression de documents confidentiels. Les capacités d'impression verrouillée de Ricoh permettent de retenir les documents cryptés sur le disque dur de l'appareil jusqu'à ce que l'utilisateur se présente devant l'appareil et entre le bon numéro d'identification personnel ou les bonnes données d'authentification réseau. Pour encore plus de capacités, des logiciels comme Streamline NX peuvent assurer le relâchement de documents entièrement sécurisé en offrant aux utilisateurs des options liées aux flux d'impressions tout en conférant un certain contrôle à l'administrateur.

2 **Sécurité des données de copie**
Ricoh offre des fonctions visant à empêcher les copies non autorisées de documents papier afin de contribuer à prévenir les fuites d'information. Cette fonction de copie protégée permet d'imprimer et de copier des documents avec des masques invisibles spéciaux intégrés au fond. Si le document imprimé ou copié tente d'être photocopié de nouveau, le masque intégré deviendra visible sur les copies.
La fonction de contrôle de copie non autorisée protège de deux façons. L'option « Masque pour copie » intègre un motif de masquage et un message à l'intérieur de l'impression originale pour protéger l'information. Si des copies non autorisées sont faites, le message intégré apparaît sur la copie. Il peut s'agir du nom de l'auteur du document ou d'un message d'avertissement. Lorsque l'appareil Ricoh détecte le motif de masquage, les données imprimées sont masquées par une boîte grise qui couvre toute la page sur laquelle le motif de masquage est détecté, à l'exception d'une marge de 4 mm de chaque côté.

3 **Tampon de sécurité obligatoire**
Identifiez les documents avec des renseignements clés pour une responsabilisation accrue et un plus grand contrôle sur la gestion. La fonction d'impression obligatoire des renseignements sur la sécurité intègre obligatoirement des renseignements sur le document imprimé, dont le nom de la personne ayant imprimé le document, à quel moment et à partir de quel appareil. Cette fonctionnalité peut être configurée pour les copies, les impressions, les télécopies et les fonctions de serveur de documents.

Les administrateurs peuvent choisir à quel endroit les informations obligatoires seront imprimées et quels types de renseignements seront inclus. Ces renseignements peuvent comprendre :

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

4 **Retrait temporaire des données**
Lorsqu'un document est numérisé ou lorsque de l'information est reçue à partir d'un ordinateur, certaines données peuvent être temporairement stockées sur le disque dur ou sur le périphérique de mémoire de l'appareil. Cela peut inclure la numérisation, l'impression et la copie des fichiers d'image, les données saisies par l'utilisateur et les configurations de l'appareil. Ces données temporaires représentent une brèche potentielle de la sécurité.

Le système de sécurité par écrasement des données (DOSS, Data Overwrite Security System), intégré à la plupart des appareils Ricoh, referme cette brèche de sécurité en détruisant les données temporaires stockées sur le disque dur du MFP en les écrasant avec des séquences aléatoires de « 1 » et de « 0 ». Les données temporaires sont activement écrasées et ainsi effacées chaque fois qu'une nouvelle tâche est exécutée. Le DOSS peut également :

- Inclure des options pour les recommandations du Service canadien du renseignement de sécurité (SCRS) et du ministère de la Défense nationale (MDN) à l'égard du traitement de l'information classifiée.
- Rendre pratiquement impossible l'accès aux données latentes des tâches de copie, d'impression, de numérisation et de télécopie une fois que le processus d'écrasement est terminé (le processus d'écrasement peut être réalisé entre 1 et 9 fois).
- Aider les clients à respecter les normes de la Health Insurance Portability and Accountability Act (HIPPA), de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), de la Loi sur la protection des renseignements personnels sur la santé (LPRPS), de la Gramm-Leach-Bliley Act (GLBA) et de la Family Education Rights Privacy Act (FERPA) ainsi que de bien d'autres réglementations.
- Fournir une rétroaction visuelle du processus d'écrasement (c.-à-d. processus terminé ou en cours) à l'aide d'une simple icône.

5 **Confirmation du numéro de télécopieur**
Il est facile de commettre des erreurs lorsque l'on inscrit un numéro de télécopieur directement sur un clavier. Nos spécialistes peuvent configurer les appareils de manière à ce que le numéro doive être inscrit 2 fois, ou plus, aux fins de confirmation. Si des numéros différents sont inscrits, la transmission ne sera pas lancée. Cette fonctionnalité réduit le risque de transmettre de l'information à la mauvaise destination.

Normes et certifications de sécurité indépendante

Les Critères communs pour l'évaluation de sécurité de la technologie de l'information sont utilisés à l'échelle internationale. Ils servent à définir si les fonctionnalités de sécurité sont adéquatement conçues pour les produits TI. La certification des Critères communs est reconnue par plus de 25 pays partout dans le monde. Les fournisseurs de copieurs multifonctions nationaux et étrangers souhaitent tous obtenir l'authentification pour leurs copieurs numériques multifonctions.

La procédure de certification liée aux Critères communs vérifie la protection offerte par les multiples technologies de sécurité contre les diverses menaces de sécurité. La certification aborde notamment la vérification de la validité du système au démarrage, le contrôle des accès et les connexions, la protection des données par chiffrement ainsi que la suppression des données au moment du retrait d'un appareil. Ainsi, elle contribue à protéger nos produits contre les diverses menaces, notamment les modifications des logiciels, les accès invalides et les fuites d'information

1 **Profil de protection pour les appareils (PP_HCD_V1.0)**
Le profil PP_HCD_V1.0 est un profil de protection approuvé par le gouvernement des États-Unis pour les appareils comme les appareils multifonctions numériques. Ce profil a été créé par la communauté technique des appareils multifonctions, formée notamment de représentants du secteur (dont Ricoh), d'organismes gouvernementaux des États-Unis et du Japon, de laboratoires d'essais des Critères communs ainsi que des schémas internationaux des Critères communs. L'objectif du profil de protection est de simplifier l'achat efficace d'appareils commerciaux sur étagère (COTS, Commercial Off-The-Shelf) en faisant appel à la méthodologie des Critères communs pour évaluer la sécurité des technologies de l'information.

Les aspects suivants, qui ont été identifiés comme représentant les plus importantes protections de sécurité, sont certifiés dans plusieurs des appareils Ricoh conformément à la norme PP_HCD_V1 et peuvent être activés :

- Systèmes d'identification et d'authentification des utilisateurs
- Technologies de chiffrement des données compatibles avec les imprimantes multifonctions
- Fonction de validation des micrologiciels du système
- Séparation de la ligne de télécopie analogue et du contrôleur de copie, d'impression et de numérisation
- Validation des algorithmes de chiffrement des données
- Protection des données

La gamme de produits de Ricoh est continuellement améliorée pour respecter les exigences en évolution des clients et des organismes de réglementation.

Veuillez visiter ce site Web pour obtenir la liste complète des appareils Ricoh dotés des certifications ISO/IEC 15408.

2 **IEEE 2600.2**

La norme de sécurité IEEE 2600.2 concerne les appareils utilisés dans des environnements commerciaux de traitement de l'information devant détenir des niveaux précis de sécurité des documents et des réseaux ainsi que d'assurance de la sécurité. Cette norme établit une référence commune quant aux attentes en matière de sécurité pour les appareils multifonctions. Afin de s'assurer qu'un appareil est conforme à la norme établie, des laboratoires indépendants effectuent des essais et vérifient les fonctions de sécurité du fabricant. Ricoh offre une vaste gamme d'appareils multifonctions certifiés comme étant conformes à la norme de sécurité IEEE 2600.2.

3 **FIPS 140-2/3**

La Federal Information Processing Standard (FIPS) 140-2/3 est une norme de sécurité du gouvernement des États-Unis qui sert à la validation des modules cryptographiques dans le cadre du Cryptographic Module Validation Program (CMVP) du National Institute of Standards and Technology (NIST). De nombreux modules cryptographiques des appareils Ricoh font appel aux algorithmes recommandés ou approuvés par le Cryptographic Algorithm Validation Program (CAVP) du NIST. L'approbation du CAVP est un prérequis de l'approbation du CMVP.

Les clients peuvent mettre à niveau certains appareils pour obtenir un pilote validé par le CMVP* ou mettre à niveau le micrologiciel d'un appareil multifonction pour intégrer les modules approuvés par le CMVP dans d'autres éléments de l'appareil multifonction**. Les appareils dont le micrologiciel est mis à niveau mettront en place certaines mesures de renforcement des appareils, y compris la désactivation des ports et des protocoles moins sécurisés ainsi que la restriction de l'utilisation de certaines applications. Lorsqu'un appareil est retourné au fabricant à la fin de sa location ou de son cycle de vie, la fonctionnalité de suppression complète de la mémoire peut être utilisée pour éliminer toutes les données stockées à divers emplacements dans l'appareil.

* Un pilote respectant la norme FIPS 140-2 du CMVP (validé) est disponible pour plusieurs de nos produits.
** Une mise à niveau de micrologiciel est disponible pour les appareils sélectionnés.

4e niveau — Sécurité des réseaux

Dans le paysage numérique au rythme effréné d'aujourd'hui, les professionnels des TI sont submergés par de plus en plus de responsabilités : ils doivent offrir des expériences de travail fluide, de partout, tout en soutenant toutes les unités d'affaires, en offrant des formations et en effectuant des dépannages auprès des utilisateurs ainsi qu'en veillant à ce que les données, les systèmes et les réseaux soient protégés. Tout ce qui se trouve dans l'environnement de travail doit être accessible, intégré, efficace, fluide et sécurisé. Cela comprend les communications, le stockage des fichiers, les applications, les identités des utilisateurs, les réseaux, les serveurs, les courriels et bien d'autres éléments.

À mesure que les menaces évoluent et que les surfaces d'attaques s'élargissent, on observe une croissance de la marge d'erreur. La mise en place d'une cybersécurité robuste et proactive est plus essentielle que jamais. Ricoh offre un vaste éventail de services et de solutions TI qui permettent la numérisation simple et sécuritaire dans tous les secteurs de votre entreprise. Explorons les options.

Vérification systématique

Les environnements de travail modernes, où le télétravail est fréquent et dont les données et les systèmes sont bien souvent à l'extérieur des espaces de bureau physique, ont brouillé les limites de ce qui se trouve à l'intérieur ou à l'extérieur des réseaux. L'approche de vérification systématique présume que les menaces peuvent provenir de l'intérieur ou de l'extérieur d'un réseau et, ainsi, qu'elle fait appel à des vérifications et au contrôle des accès pour tous les utilisateurs et tous les appareils du réseau.

1. **Authentification multifacteur**
   Pendant de nombreuses années, les organisations ont fait appel aux données d'authentification (code d'utilisateur et mot de passe) pour authentifier les utilisateurs et leur donner un accès. Toutefois, les cybercriminels ont appris à voler les données d'authentification en lançant des attaques ciblées, comme des attaques d'hameçonnage ou d'espionnage. En faisant appel à la technologie de l'IA, ils peuvent déchiffrer les mots de passe les plus complexes en seulement quelques minutes. L'ajout de couches d'authentification additionnelles (l'authentification multifacteur [MFA, multi-factor authentication]) complique l'accès pour les attaquants.

2. **Gestion des identités et des authentifications**
   Le transfert d'un réseau vers une plateforme unifiée, comme Microsoft 365, simplifie l'adoption d'une approche à vérification systématique, puisque ces plateformes offrent des fonctionnalités puissantes comme la gestion centralisée des identités, qui permet la mise en place de politiques d'authentification uniformisées dans l'ensemble des services et des applications. Il est également possible d'adopter des politiques d'accès granulaire en créant des politiques conditionnelles basées sur des facteurs précis comme l'emplacement, l'utilisateur, l'appareil et le niveau de risque.

Évaluations de la sécurité

Puisque les organisations continuent de passer au travail hybride et de permettre aux utilisateurs de se connecter régulièrement à leur réseau depuis l'extérieur du bureau ou depuis un appareil non sécurisé, le besoin d'obtenir un accès sécurisé aux réseaux a connu une croissance. La numérisation accrue des procédures signifie qu'un plus grand volume de données est au repos, en circulation ou en utilisation au sein des organisations, ce qui accentue leur exposition aux risques. C'est là que les évaluations des vulnérabilités et de la sécurité interviennent.

1. **Évaluations de la vulnérabilité**
   L'évaluation des vulnérabilités comprend deux éléments :

   • Analyse de vulnérabilité et production de rapports à son égard
   • Analyse et planification de la correction

   Les spécialistes de la sécurité de Ricoh évaluent les actifs accessibles depuis l'extérieur et recherchent les vulnérabilités, notamment les correctifs manquants, les versions logicielles obsolètes, les ports ouverts et les services de système d'exploitation. Ensuite, ils produisent des rapports sur leurs découvertes et élaborent un plan de correction personnalisé selon le client. Les évaluations des vulnérabilités peuvent être réalisées de manière régulière ou ponctuelle.

2 **Test d'intrusion**
Dans quelle mesure vos données sont-elles sécurisées? La seule façon d'en avoir le cœur net est de tester votre sécurité actuelle en essayant de la contourner de l'extérieur, comme le ferait un pirate informatique. Ce type d'essai relève les forces de votre réseau, mais aussi les zones qui exigent une protection plus approfondie.

Les évaluations et les tests d'intrusion repèrent les faiblesses de vos réseaux, de vos applications et de vos contrôles de sécurité. Ils peuvent également confirmer l'efficacité des différentes politiques, procédures et technologies de sécurité que vous avez mises en place.

Détection des intrusions

Aujourd'hui, les cybermenaces sont en constante évolution et elles utilisent de nouvelles méthodes pour pénétrer des réseaux et causer des ravages. Les maliciels, les rançongiciels et les attaques par déni de service sont les attaques dont les entreprises de toute taille sont les plus souvent victimes.

La détection des intrusions ressemble au jeu du chat et de la souris. C'est une bataille constante et énergique entre les attaquants et les défenseurs. En suivant l'évolution de la technologie, les deux parties s'adaptent et élaborent de nouvelles techniques pour se montrer plus habiles que leurs adversaires. Plus les attaquants innovent, plus les défenseurs réagissent. Les défenseurs repèrent, alors que les attaquants s'enfuient.

1 **Pare-feux**
Les pare-feux sont conçus pour protéger l'infrastructure de vos réseaux et pour rehausser la connectivité entre les différents sites. Aujourd'hui, les pare-feux les plus sophistiqués présentent des capacités améliorées permettant de se protéger en temps réel contre les maliciels, les vulnérabilités et les attaques visant les réseaux. Les analyses intelligentes permettent de combiner l'apprentissage humain et l'apprentissage automatique pour appliquer des règles qui laissent circuler le trafic ou l'empêchent.

2 **Logiciel antivirus**
Les logiciels antivirus sont divisés en trois catégories principales : la vérification basée sur la signature numérique, sur les comportements ou sur l'apprentissage automatique.

- **Signature numérique :** la méthode basée sur la signature numérique compare le code d'un fichier suspect à ceux des maliciels connus inscrits dans une base de données. Si une correspondance est trouvée, le fichier est automatiquement signalé et bloqué, isolé ou supprimé.
- **Comportement :** les logiciels utilisant cette méthode analysent les comportements d'un fichier (p. ex. : un chiffrement rapide) pour être en mesure de repérer les nouveaux maliciels auxquels ils n'ont pas encore été confrontés.
- Puisque les cybercriminels évoluent sans cesse et créent constamment de nouvelles souches de maliciels, cette méthode offre une bien meilleure protection que celle basée sur la signature numérique.
- **Intelligence artificielle :** les logiciels faisant appel à l'apprentissage automatique sont le plus récent et le plus robuste type de protection antivirus. Ils utilisent des algorithmes et des ensembles de données pour repérer les tendances des maliciels dans les appareils individuels et les réseaux vastes.

3 **Confinement des rançongiciels**
L'époque où l'on pouvait installer un logiciel antivirus et l'oublier est révolue. En effet, l'arrivée des attaques malveillantes et sophistiquées, comme les rançongiciels, exige une combinaison de mesures de prévention et d'atténuation. Les solutions de prévention repèrent les signatures et les comportements des rançongiciels et les empêchent de pénétrer le périmètre. Toutefois, compte tenu des tactiques de plus en plus sophistiquées utilisées par les cybercriminels, il est essentiel de mettre en place une seconde ligne de défense.

Les mesures de confinement des rançongiciels freinent le chiffrement malveillant à la source, l'isolent et le confinent afin de l'empêcher de se propager. Le confinement des rançongiciels est la dernière ligne de défense de l'infrastructure de sécurité des organisations. Cette mesure comble les dangereuses lacunes de sécurité entre les appareils et les fonctions de partage de fichiers, où la protection est souvent négligée par les entreprises.

Gestion des terminaux

Les terminaux sont les points d'entrée les plus communs des maliciels, des rançongiciels, des hypertrucages et des attaques par piratage psychologique. Lorsqu'un cybercriminel obtient l'accès à l'un de vos terminaux, il peut trouver comment fouiller dans votre réseau pour accéder à des données confidentielles ou déployer des attaques de grande ampleur.

1. **Filtrage Web**
   Assurer la protection de la sécurité et le filtrage du contenu limite les risques et optimise la sécurité, puisqu'il s'agit d'un important élément de la défense. Le filtrage est utilisé couramment pour les outils liés au courriel, on y réfère souvent à titre d'antipourriel, de sécurité des courriels ou de filtrage des courriels. Bien que détenir une protection des courriels soit important, cela n'est qu'une partie de la solution de filtrage.

   Les solutions gérées de filtrage Web sont conçues pour bloquer les domaines malveillants qui pourraient comprendre du contenu nuisible comme un rançongiciel, un maliciel, un virus ou une fraude d'hameçonnage. Il est également possible de bloquer certains types de contenu, selon les besoins, afin d'empêcher l'accès à des domaines pouvant comprendre du contenu pour adultes, du contenu lié au jeu, à la cryptomonnaie, aux sites de rencontre ou tout autre contenu interdit.

2. **Gestion des appareils mobile**
   Les applications de gestion des appareils mobiles, comme Intune de Microsoft, permettent le déploiement rapide et la gestion des applications depuis des appareils mobiles, ce qui limite la migration de données. Ces applications peuvent servir lors de la sécurisation de l'entièreté d'un appareil mobile. Elles permettent de le protéger contre les maliciels et permettent le retrait complet de toutes les données de l'entreprise dans l'éventualité d'une menace ou du départ d'un employé.

Services experts de gestion de la cybersécurité

Pour être prêt, il faut commencer par intégrer des solutions et des services de cybersécurité intelligente aux principales procédures d'affaires et veiller à ce que la gestion rigoureuse soit assumée par des spécialistes de la cybersécurité.

Les menaces en constante évolution exigent une gestion rigoureuse et sans compromis des systèmes, des appareils et des environnements. Les équipes TI subissent plus de pression que jamais à l'égard du maintien des activités, de l'aide aux unités d'affaires et du soutien des utilisateurs. En impartissant la cyberprotection à une équipe de spécialistes dévoués, vous pouvez libérer votre équipe TI et lui permettre de se concentrer sur ses capacités principales, sans être dérangée. Les équipes TI distraites et surchargées causent inévitablement des lacunes en matière de sécurité qui, elles, peuvent entraîner des conséquences désastreuses.

Les solutions et les services de Ricoh offerts par des spécialistes de la cybersécurité peuvent vous aider à bâtir une infrastructure TI plus résiliente, à comprendre et gérer vos vulnérabilités ainsi que vous permettre de croître en toute confiance.

5e niveau – Sécurité des applications

Même si les logiciels sont conçus pour rehausser l'efficacité et la productivité, ils peuvent également entraîner des risques. Les applications logicielles intégrées, les applications installées et les logiciels hébergés dans le nuage peuvent être des cibles d'attaques à distance. C'est pourquoi vos données doivent être protégées.

Bon nombre d'attaques lancées par des cybercriminels exploitent les vulnérabilités des logiciels. Ces vulnérabilités sont généralement causées par des erreurs ou des omissions commises lors de la programmation ou de la conception et qui exposent les applications, les serveurs ou les sites Web.

Voici comment assurer la sécurité des applications :

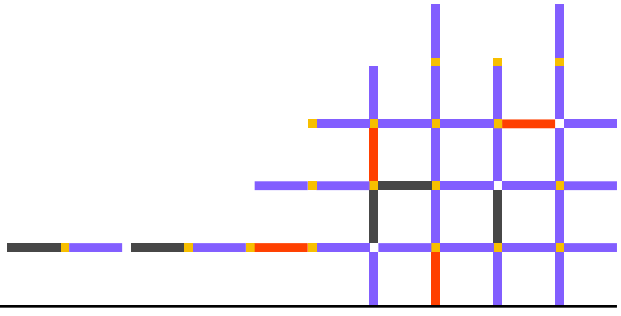
1 **Sécurité par défaut**
Les applications devraient faire appel à la sécurité par défaut, une approche de conception qui vise la protection contre les cyberattaques. Lors de l'installation d'une nouvelle application, il est important d'effectuer des recherches à l'égard du respect, par le développeur, des normes internationales comme la norme ISO 27034.

Les pratiques de sécurité par défaut de Ricoh sont basées sur la norme ISO/IEC 27034-1:2011 (« Sécurité des applications — Partie 1 : Aperçu général et concepts »), qui tiennent compte de la sécurité tout au long du cycle de vie des produits et de services, des étapes de planification à celles de la conception. Nous offrons plusieurs solutions et logiciels intégrés pour les systèmes TI, pour la gestion des procédures d'affaires ainsi que pour les imprimantes et les appareils multifonctions.

2 **Intégrations sécurisées**
Les interfaces de programmation d'applications (API) sécurisées font partie intégrante de l'infrastructure TI d'une organisation. Elles permettent la communication fluide entre les applications et les systèmes. Les API se trouvent entre les applications de tierce partie et les données et les systèmes de votre organisation. Elles facilitent le mouvement des données entre ces destinations. La mauvaise gestion de la sécurité ouvre essentiellement la voie aux diverses cybermenaces.

Il est essentiel de veiller à ce que le flux soit chiffré, de régulièrement effectuer des évaluations des vulnérabilités ainsi qu'apporter des mises à jour et des correctifs en plus de s'assurer que toutes les données soient chiffrées à tous les niveaux.

3 **Sécurité des données**
Lorsque vous collaborez avec un fournisseur de logiciels comme service (SaaS), il est important de comprendre où seront hébergées vos données, qui y aura accès et quelles mesures de contrôle les protégeront. Il faut se demander, surtout si l'application stockera des données confidentielles, si le fournisseur détient des certifications de sécurité ou s'il a mis en place des normes et des mesures de contrôle.



4

Pratiques exemplaires en matière de cybersécurité

Pour se protéger contre les dommages causés par de tierces parties malveillantes, les administrateurs de système devraient poser les gestes suivants :

1. Lire l'entièreté de l'entente de licence de chaque solution et logiciel intégré. Afin de poursuivre l'utilisation, il faut accepter les conditions.

2. Vérifier que le système d'exploitation ou le micrologiciel d'un appareil corresponde à la plus récente version avant l'installation et l'utilisation. Installer et utiliser les solutions et les logiciels intégrés sur un réseau protégé par un pare-feu. Afin d'éviter les risques inhérents, il est conseillé de ne pas connecter les solutions et les logiciels intégrés directement à Internet.

3. Limiter l'accès aux solutions et aux logiciels intégrés uniquement aux utilisateurs autorisés, notamment au moyen de mesures de contrôle des accès ainsi qu'en n'autorisant que les plages d'adresses IP approuvées.

4. Modifier le mot de passe administrateur établi par défaut des solutions et des logiciels intégrés aux produits et aux systèmes d'exploitation pour empêcher l'accès non autorisé par de tierces parties malveillantes.

5. Vérifier que les solutions intégrées, les imprimantes, multifonctions ou non, les logiciels et les systèmes d'exploitation soient configurés adéquatement pour répondre aux flux de travaux dont vous avez besoin et pour respecter la politique de sécurité de votre entreprise.

6. Établir les paramètres de sécurité des imprimantes et des imprimantes multifonction selon les renseignements fournis dans le guide d'instruction de l'appareil ou dans la politique du client.

7. Utiliser le chiffrement pour toutes les données en circulation. De plus, les certifications devraient être approuvées par une autorité de certification tierce publique ou privée. Les certifications autosignées posent des risques.

8. Offrir des instructions et de la formation aux utilisateurs des solutions et des logiciels intégrés.

9. Veiller à ce que la sécurité des navigateurs soit activée sur les ordinateurs servant à la gestion des solutions et des logiciels intégrés pour limiter les menaces externes. De plus, il convient de ne jamais utiliser le même navigateur ou la même fenêtre pour gérer une solution ou un logiciel intégré ou y accéder tout en consultant les ressources externes. Fermer toutes les sessions des solutions et des logiciels intégrés avant d'accéder à des ressources externes.

10. Désinstaller les solutions et les logiciels désuets et toute donnée confidentielle ou personnelle auparavant utilisée dans les flux de travaux. Cela empêchera la fuite d'information confidentielle des clients qui pourrait y demeurer.

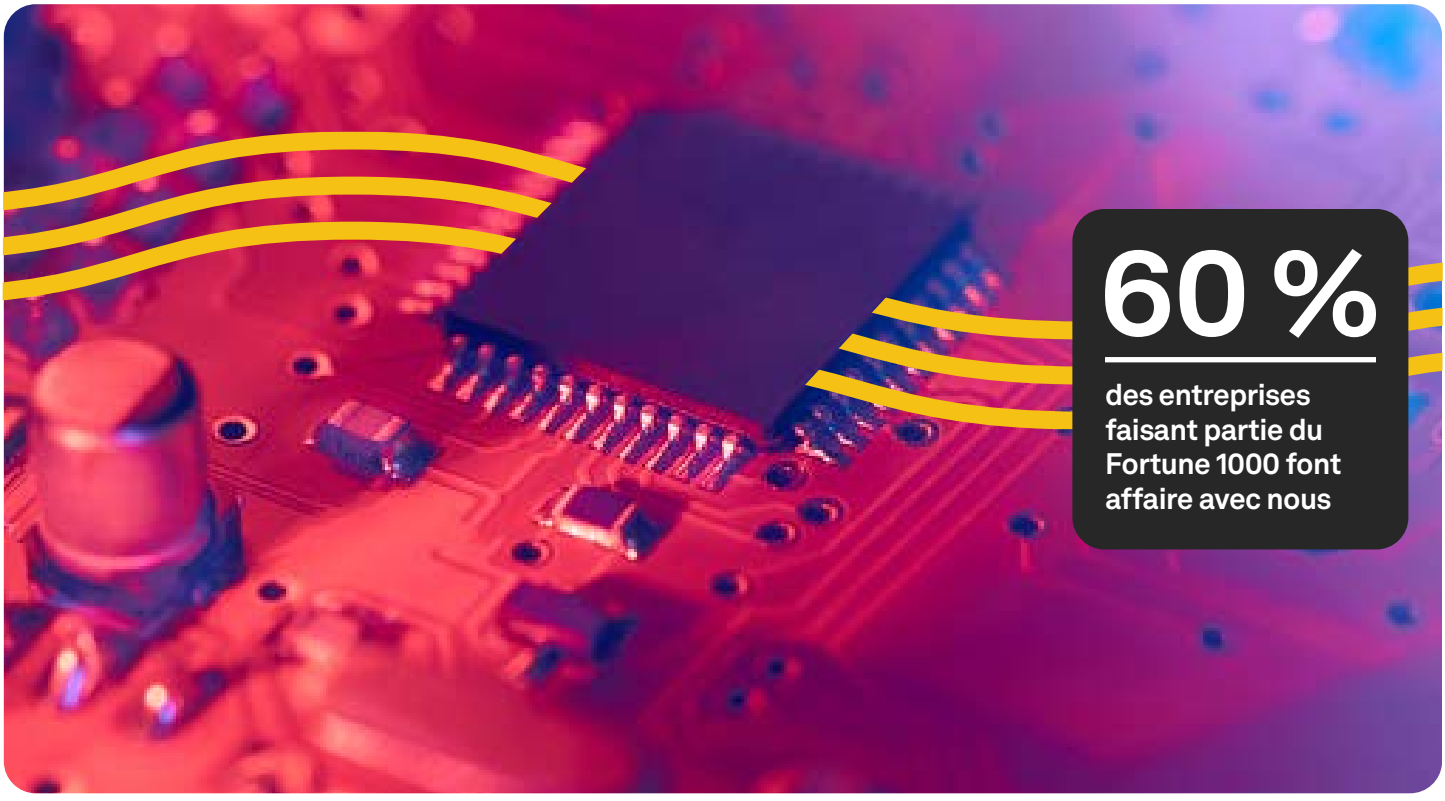
Soutien et orientation stratégiques

Consultations en sécurité
Faites que votre stratégie TI qui se contente de soutenir les activités quotidiennes devienne une stratégie qui fait partie intégrante de la mise sur pied et de l'appui d'initiatives d'affaires stratégiques.

Les conseillers en technologies virtuelles et les spécialistes en sécurité de Ricoh sont en mesure de vous aider à concevoir un plan de reprise général qui est évalué, testé, puis testé de nouveau avant qu'un désastre s'abatte sur vous. Notre approche, fondée sur les meilleures pratiques de gouvernance, de gestion du risque et de conformité, repère rapidement les vulnérabilités pouvant se solder par des infractions à la sécurité, les vides pouvant entraîner des cyberattaques et les autres angles d'exposition de votre technologie à l'interne avant que votre entreprise ne soit touchée.

Consultation en matière de gouvernance de l'information
Plusieurs aspects de la gestion de l'information donnent du fil à retordre à de nombreuses organisations, notamment la sécurité et la protection, la rétention et l'élimination, la conformité légale ou réglementaire, la fiabilité et l'authenticité. Les conseillers de Ricoh aident les organisations à aborder ces aspects en les aidant à supprimer les cloisonnements et à mettre en place des programmes durables à long terme. Nous considérons l'information comme étant à la fois le problème et la solution. Nous adoptons une approche proactive pour surmonter les défis liés à l'information et plaçons votre organisation sur la voie du succès en lui permettant de prendre des décisions d'affaires éclairées.

Soutien technique à l'échelle nationale et internationale
Ricoh a mis en place des centres de technologies dans chaque région afin de fournir du soutien technique et de répondre rapidement et efficacement aux besoins de ses clients partout à travers le monde. L'équipe des services mondiaux de Ricoh fournit des solutions uniformes, normalisées et complètes. Couvrant approximativement 200 pays et territoires autour du globe, Ricoh emploie plus de 9 000 spécialistes de la prestation de service. Notre réseau de partenaires détaillants de vente et de soutien se démarque par sa capacité de faire affaire avec 60 % des entreprises faisant partie du Fortune 1000, ce qui signifie que vous pouvez compter sur un seul partenaire pour l'ensemble de vos besoins. Grâce à nos bureaux et à nos professionnels de la prestation de service situés dans un si grand nombre de pays, nous sommes en mesure de répondre rapidement aux demandes des clients.



Documentation d'appui sur la sécurité
Ricoh fournit de la documentation technique afin d'appuyer ses clients relativement aux exigences de sécurité en matière d'information, notamment les certificats et les rapports de validation des Critères communs pour certaines offres de produit. Cette documentation comprend la validation d'un tiers relativement aux réclamations en matière de sécurité et peut être fournie sur demande. De plus, des livres blancs sur la sécurité relative aux appareils et aux réseaux ainsi que des guides d'administrateur pour la sécurité des appareils, lesquels sont exigés par les Critères communs, sont disponibles pour les clients. Ces guides fournissent des renseignements détaillés sur la manière dont l'équipement de Ricoh transmet les données de l'appareil et sur la façon dont celui-ci interagit avec le réseau. Cliquez ici pour consulter plus de documentation.

Formation des administrateurs et des utilisateurs
Maintenir un niveau de vigilance élevé et adhérer à des pratiques exemplaires en matière de sécurité impliquent bien plus que la simple technologie — cela concerne aussi les gens. Ricoh offre des formations à propos de ses appareils, et ceux de ses fournisseurs tiers, à l'intention des administrateurs et des utilisateurs directs. Équipés des bonnes connaissances, les membres de votre personnel seront en mesure de comprendre les capacités de sécurité à leur disposition et apprendre comment en faire un usage approprié afin de contribuer à protéger l'information de votre organisation et à respecter les réglementations.

Engagement continu de Ricoh en matière de sécurité
La sécurité est ancrée dans nos valeurs, auxquelles nous sommes extrêmement dévoués. Que vous soyez pris dans un déluge de données, que vous travailliez dans un secteur hautement réglementé, que vous manquiez de ressources ou d'expérience ou que vous souhaitiez obtenir la confiance liée à l'utilisation de services et de logiciels hautement sécurisés, nous aspirons à gagner votre confiance en répondant aux normes les plus sévères du secteur. Notre objectif est de garder une longueur d'avance sur les cybercriminels, mais, s'ils parviennent tout de même à pénétrer dans nos systèmes, d'avoir un plan et des systèmes en place pour limiter les dégâts causés par une brèche.

La promesse que nous faisons à tous nos clients est de respecter les normes et les directives de sécurité actuelle dans tous nos produits et tous nos services, de travailler sans relâche pour protéger leurs données et de permettre à nos clients de se protéger eux-mêmes. Nous sommes engagés à toujours évaluer, apprendre et innover dans le cadre de toutes nos initiatives en imaginant le meilleur avenir possible pour nos clients et nos partenaires.

Les menaces planant sur la sécurité de l'information deviennent plus sophistiquées et furtives chaque jour. Ricoh s'est engagé à offrir des produits sécuritaires qui protègent vos actifs d'information et qui s'harmonisent à votre environnement de bureau et à vos politiques en matière de sécurité. Pour veiller à la sécurité, il faut s'assurer d'établir les bons paramètres et de faire les mises en œuvre appropriées pour votre environnement spécifique.

Notre vaste expérience et notre approche à plusieurs niveaux peuvent être utiles à l'ensemble de votre organisation, que ce soit en matière de stratégie, d'appareils, de logiciels, de services, de soutien, de formation et bien plus encore. Laissez-nous vous aider dans vos parcours de services d'information numérique.

RICOH
imagine. change.

Ricoh, un partenaire de choix

Chez Ricoh, nous habilitons nos clients à répondre à notre monde en évolution au moyen de renseignements exploitables. Nous croyons que l'accès à la bonne information se traduit par une plus grande agilité opérationnelle, des expériences plus humaines et la capacité à prospérer en cette époque actuelle de travail hybride et sans frontières. Grâce à notre personnel, à notre expérience et à nos solutions, nous créons chaque jour un avantage concurrentiel pour plus de 1,4 million d'entreprises dans le monde. Pour nous, il n'y a jamais trop d'information.

Vous avez des questions? Visitez le site Web ricoh.ca ou communiquez avec un spécialiste de la sécurité de Ricoh dès aujourd'hui.

Ricoh Canada Inc., 400-5560 Explorer Drive, Mississauga, Ontario, L4W 5M3 | 1 800 63-RICOH

RICOH
imagine. change.