RICOH
imagine. change.

Guides des bases de la sécurité de Ricoh

La sécurité multicouche pour les milieux de travail numériques modernes

Les besoins du travail hybride et des opérations au sein d'un environnement axé sur le numérique ont accéléré le changement transformationnel chez les entreprises modernisant leurs capacités à l'échelle de leur organisation. Alors que les organisations s'affairent à moderniser leurs milieux de travail, le paysage souvent fragmenté d'outils et de technologies qui en découle crée des lacunes dans la sécurité, la confidentialité et les opérations.

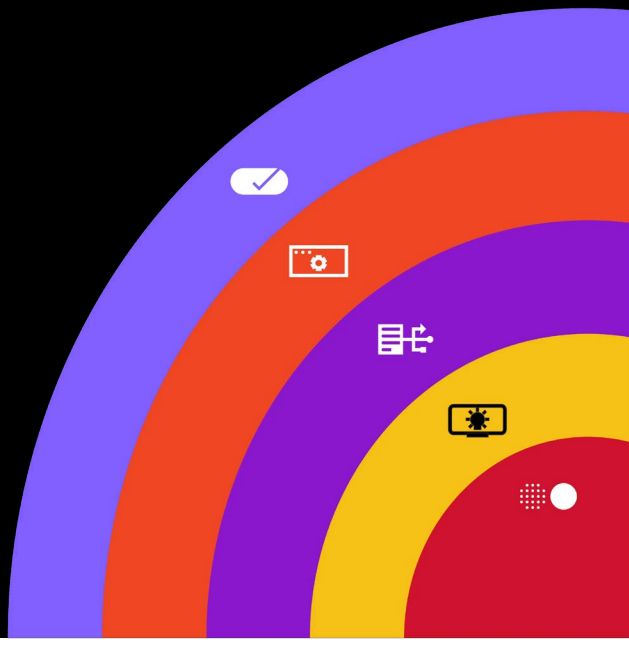
Le maintien de la sécurité, rendu possible par la protection des procédures, des systèmes, des applications et des appareils contre les brèches de données, est une lutte constante et inquiétante qui pèse lourd dans l'esprit des dirigeants. En effet, en plus de coûter cher aux organisations, chaque attaque met l'entièreté de l'organisation à risque.

Plus les risques augmentent, plus les organisations doivent sécuriser leurs investissements numériques, tout en tenant compte de la demande grandissante venant de leurs partenaires et de leur clientèle ainsi que des autorités imposant des exigences de sécurité. Ricoh offre les outils et les conseils d'experts dont ont besoin les organisations d'aujourd'hui pour protéger leur information et leurs principaux investissements ainsi que pour bâtir une image de marque de confiance. Nous le faisons en adoptant une approche stratégique multicouche qui assure une protection contre les vulnérabilités et les menaces 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 couches 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.

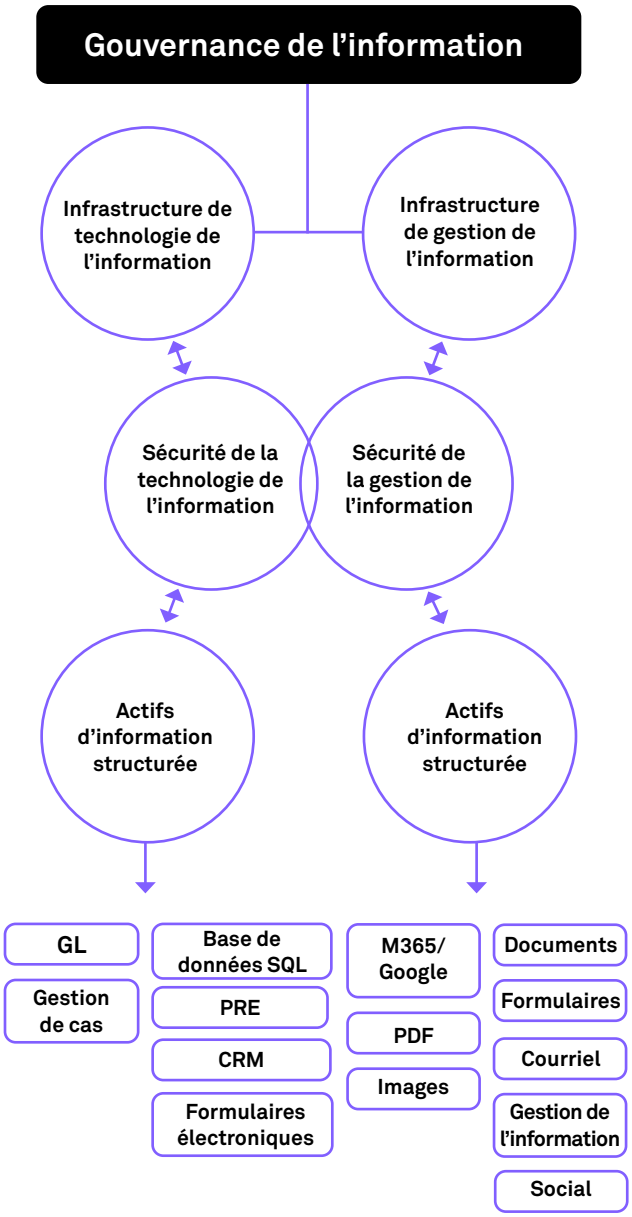
Dans ce document, vous découvrirez comment l'approche de sécurité multicouche utilisée dans le portefeuille robuste de services, de solutions et d'appareils de Ricoh aide à protéger votre entreprise et comment elle vous permet de croître en toute confiance.

1. Sécurité de l'information et des procédures
2. Sécurité des systèmes
3. Sécurité des applications
4. Sécurité des appareils
5. Sécurité des données



1re couche — Sécurité de l'information et des procédures

La transformation numérique exige l'intégration de technologies numériques dans tous les secteurs de votre entreprise, La transformation numérique exige l'intégration de technologies numériques dans tous les secteurs de votre entreprise, laquelle change radicalement la façon dont vous créez de la valeur et dont vous l'offrez à vos clients. Cette transformation entraîne également un changement de culture qui demande aux employés de s'adapter à des milieux de travail plus dispersés ainsi que d'adopter de nouvelles procédures qui peuvent leur permettre d'être plus productifs, lorsqu'ils travaillent au bureau ou à la maison. Les dirigeants d'entreprise doivent s'adapter et bien connaître les risques à l'égard de la sécurité des procédures et des données.



Gouvernance de l'information

De mauvaises pratiques en matière de gestion de l'information peuvent exposer une entreprise à de multiples risques qui peuvent mener à d'importantes pénalités financières et porter atteinte à sa réputation. Comprendre quels renseignements et quelles données vous devez conserver et la façon dont vous pouvez améliorer leur gestion réduit ces risques et vous prépare aux vérifications minutieuses.

Les services de sécurité liés à la gouvernance de l'information soutiennent l'établissement et le maintien constant de la confidentialité, de l'intégrité et de la disponibilité de l'information. Ces services ciblés 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 numérique entre une entreprise et un client laisse une trace de données. Alors que certaines données sont hautement confidentielles et nécessitent des mesures de sécurité, de confidentialité et de contrôle de la découverte, d'autres, que l'on nomme les données redondantes, obsolètes ou insignifiantes (ROT), n'ont aucune valeur et occupent 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.

Connaître l'information que vous possédez et l'endroit où elle se trouve est la première étape essentielle à la sécurité de l'information. Assurer la protection des données confidentielles, comme l'information personnelle et les renseignements de l'industrie de carte de paiement (PCI) est essentiel pour limiter les risques.

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 en matière de gestion des données et de gouvernance de l'information :

1. **Solutions de découverte de données**

   Les solutions de découverte de données automatisée sont une façon sécuritaire et efficace d'identifier et de localiser les propriétés et les permissions associées aux données confidentielles sur une quantité illimitée de terminaux. Vous pouvez protéger votre organisation en réduisant les actifs de données ROT, en gérant de manière proactive le cycle de vie de vos données et en veillant au respect des réglementations de confidentialité. La découverte des données répare également les données en les chiffrant, en les archivant ou en les censurant, en contrôlant leur accès ou en les déplaçant vers des emplacements sécurisés.

2. **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.

3. **Analyse de fichiers**

   La nature de vos données est aussi variée que celle de votre entreprise. Le manque de connaissance à l'égard des données que vous possédez nuit à votre responsabilité à l'égard de leur protection et vous empêche de profiter des avantages qu'elles pourraient vous apporter. En analysant automatiquement vos répertoires de fichiers et vos systèmes de courriel, vous pouvez identifier les données précieuses et confidentielles et, ainsi, prendre les mesures nécessaires. Une analyse de fichiers rigoureuse n'est pas que ponctuelle, afin de respecter les pratiques exemplaires, elle doit être incorporée aux flux de travaux en permanence.

4. **Classification des données**

   La classification des données fait appel à une technologie automatisée fondée sur l'intelligence artificielle pour catégoriser ou indexer vos documents dans le but de faciliter l'extraction, l'exportation et la protection des données ainsi que l'accès à ces dernières. La mise en œuvre d'un système de classification des données renforce la sécurité et contribue au respect des politiques. Un tel système peut également transformer les données générées depuis divers flux de travaux physiques et numériques en information permettant de prendre de meilleures décisions, d'offrir un service à la clientèle plus réceptif et de mener des activités efficaces. Puisque les spécialistes de la sécurité et des procédures de Ricoh ont une compréhension approfondie de l'information générée par les flux de travaux numériques et par les flux d'impression ainsi que de l'archivage et de la sécurité des courriels, il est possible d'adopter l'approche appropriée dans la classification de vos données.

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

Automatisation des transactions et des procédures

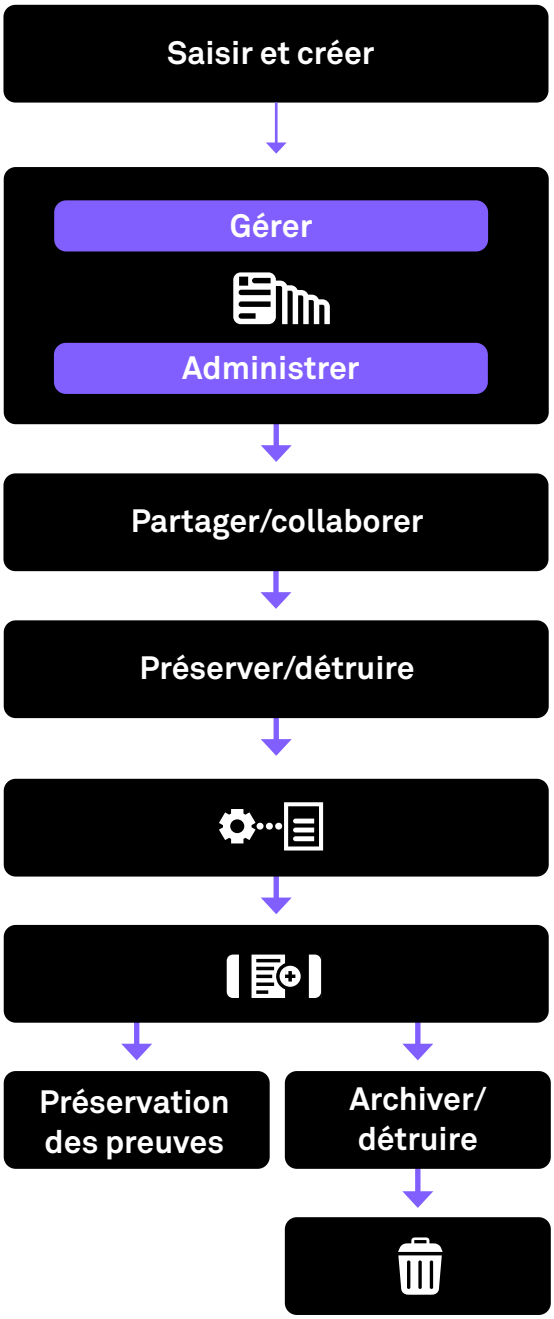
La plupart des transactions et des processus d'affaires suivent essentiellement le même chemin. Nous recueillons ou saisissons l'information, nous la stockons, la gérons et la partageons, ou nous collaborons grâce à elle, pour ensuite l'archiver ou la détruire.

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.

Les solutions de procédures d'affaires automatisées rationalisent la façon dont l'information se déplace et circule dans votre entreprise, ce qui est particulièrement important au sein des milieux de travail hybrides et pour les travailleurs à distance qui ont besoin d'un accès sécurisé partout.

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.

L'information entrante, comme les courriels, le courrier, les formulaires soumis virtuellement, les numérisations de document et les données issues du commerce électronique, doit être reçue et traitée de manière sécuritaire. 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.



Voici certaines des procédures communes où les plateformes commerciales intelligentes comme les applications de saisie de données ou de flux de travaux peuvent être utiles :

- Traitement des factures
- Traitement des prêts
- Gestion des réclamations
- Orientation des ressources humaines
- Formulaires et dossiers de patients
- Dossiers et relevés de notes d'étudiants
- Demande d'entretien et de ventes

L'information sortante est soumise aux mêmes exigences en matière de sécurité et de confidentialité. Les organisations sont responsables de déterminer si l'information qu'elles produisent et distribuent doit être chiffrée ou suivie ou encore si son accès doit être limité par une authentification utilisateur.

Les dirigeants d'entreprise doivent tenir compte des procédures suivantes :

- Comptes créditeurs
- Signatures électroniques sécurisées
- Procédures de courrier
- Communications destinées aux clients

L'automatisation des procédures ouvre de nouvelles possibilités quant à la façon dont les gens travaillent et offrent de nombreux avantages, mais les données numérisées exigent une protection particulière dès leur naissance et pendant toute leur durée de vie. Les documents papier numérisés, 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.

Saisie sécuritaire et documents numérisés

L'automatisation, la classification, l'extraction et l'exportation des données peuvent accélérer le flux d'information et, ainsi, faciliter leur accès aux 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 manquements en matière de protection des données confidentielles, comme l'information personnelle, l'information exclusive, les propriétés intellectuelles ou les renseignements fiduciaires, peuvent mener à de lourdes amendes. Toutefois, pour que de telles données non structurées puissent être protégées, elles doivent être transformées en données structurées exploitables. Découvrons comment la saisie intelligente et les solutions de formulaires électroniques sécurisés peuvent protéger 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), 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 passer 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 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.

Gestion et administration sécurisée

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. **Solutions et services de gestion de documents**

   Les solutions de gestion de documents offrent bien plus qu'un espace de stockage sécurisé. Les contrôles d'accès restreignent l'utilisation aux personnes en ayant l'autorisation et contrôlent les permissions des personnes pouvant afficher, partager ou mettre à jour certains documents. Le suivi des activités des documents vous permet de savoir qui consulte et utilise vos données.

   Les pistes de vérification fournissent un registre des activités et assurent la préservation jusqu'au niveau du document. Grâce à des politiques portant sur la rétention et le versionnage, vous pouvez veiller à ce que les documents soient gérés conformément aux exigences financières ou légales ou à d'autres types d'exigences. Que la solution de gestion des documents soit offerte en tant que service (comme DocuWare) ou déployée sur un site, les fichiers stockés sont protégés lorsqu'ils sont au repos, en transmission ou au moment où quelqu'un y accède. Le tout est accompli grâce au chiffrement, à la transmission sécurisée et à diverses options de contrôle des fichiers.

2. **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.

3. **Relâchement sécuritaire de documents**

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

   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.

4 **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.

5 **Authentification et utilisation**

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.

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.

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. Vous pouvez lier l'impression, la numérisation et la télécopie de certains documents à un client 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.

Collaboration et partage sécurisés

Le partage et la collaboration peuvent inclure l'envoi et la réception d'information. Ces activités peuvent dépendre de plusieurs systèmes de validation de l'information ou de processus impliquant une interaction humaine comme ceux mentionnés ci-dessus. L'information peut servir à l'interne, à l'externe, ou les deux, et peut également être intégrée au sein d'un système collaboratif comme Microsoft Teams. Les points clés à tenir en compte comprennent la façon dont les systèmes collaboratifs utilisent l'information ainsi que l'état final de l'information traitée dans le cadre du processus.

1 **Numérisation avancée**

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.

Conversation et élimination sécurisées

Il est si facile de perdre de vue la quantité d'information confidentielle stockée, l'emplacement où elle se trouve et les personnes pouvant y accéder. Les risques augmentent lorsque vous n'avez pas une visibilité complète des données confidentielles détenues par votre organisation, et cette lacune peut vous empêcher de respecter les exigences de base en matière de sécurité.

1 **Rétention et élimination**

Les politiques portant sur l'information 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.

2e couche — Sécurité des systèmes

À mesure que les organisations numérisent leurs procédures, il est attendu que les professionnels des TI offrent une expérience de travail fluide au bureau et à l'extérieur, soutiennent tous les secteurs d'affaires et veillent à ce que les données et les systèmes soient protégés.

Désormais, de nombreux clients nécessitent un environnement de travail entièrement virtuel. Que ce soit pour le stockage des fichiers, les applications, l'identification des utilisateurs, la sécurité, les serveurs ou les courriels, tout ce qui se trouve dans l'environnement de travail doit être accessible à distance, de manière sécuritaire, au moyen du nuage.

Les systèmes et les données des entreprises existent désormais dans un monde du travail sans frontières. Alors que les employés accèdent aux réseaux et aux applications depuis différents endroits et sur différents appareils, les angles d'attaque se multiplient, tandis que des menaces telles que les rançongiciels, elles, sont à la hausse. Même une toute petite faille dans les dispositifs de défense d'un réseau risque d'entraîner des conséquences sérieuses pour l'entreprise en question.

Ricoh offre un éventail de services et de solutions solides qui permettent la numérisation simple et sécuritaire dans tous les secteurs de votre entreprise. Explorons les nombreuses options offertes:

Paramètre de sécurité

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 et, par conséquent, ont introduit de nouvelles vulnérabilités complexifiant la gestion de la sécurité.

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 automatique pour appliquer des règles à des fonctions permettant de laisser circuler le trafic ou de l'empêcher.

2. **Gestion de l'identité et de l'authentification**

   L'utilisation d'un seul mot de passe pour authentifier les utilisateurs rend les organisations vulnérables aux menaces externes. Si un mot de passe est faible, les attaques par force brute peuvent le déjouer en quelques secondes; et si ce même mot de passe vulnérable est utilisé ailleurs, vous donnez en réalité aux cybercriminels les clés pour accéder à votre réseau. L'introduction de couches supplémentaires d'authentification (authentification multifacteur ou AMF) rend l'accès plus difficile pour les cyberattaquants. Les authentificateurs de mot de passe vérifient l'identité de l'utilisateur en comparant les identifiants saisis aux données d'un serveur d'authentification. Si une correspondance est trouvée, le système accordera l'accès.

   Lorsque les données sont partagées entre des solutions technologiques disparates, il est très difficile de surveiller l'identité des utilisateurs. C'est pourquoi de nombreuses organisations intègrent l'ensemble de l'environnement de travail dans un seul environnement infonuagique où les identités, les applications, les fichiers et les appareils sont tous gérés de manière centralisée. Microsoft Azure Active Directory est une plateforme de pointe qui offre des fonctionnalités approfondies d'authentification et de contrôle d'accès. À titre d'exemple, la plateforme permet de limiter l'accès à une région spécifique ou d'utiliser des fonctions avancées d'autorisation des utilisateurs afin de créer un lieu de travail plus sécuritaire.

3 **Test d'intrusion**

Dans quelle mesure vos données sont-elles sécurisées? La seule façon d'en avoir le cœur net est de tester vos mesures de sécurité actuelles en essayant de les contourner de l'extérieur, comme le ferait un cybercriminel. Ce genre de test révèle les points forts de votre réseau, mais aussi les points faibles où vous avez besoin de mesures de sécurité plus approfondies.

Les tests d'intrusion et les évaluations de leurs résultats dévoileront les faiblesses dans vos réseaux, vos applications et vos contrôles de sécurité. Ils peuvent aussi confirmer l'efficacité de diverses politiques, procédures et technologies de sécurité.

Les tests devraient se concentrer sur l'analyse des logiciels malveillants, l'ingénierie inverse et la cryptographie; ils devraient intégrer le développement et les mesures de sécurité offensive et défensive; et ils devraient fournir des informations claires et exploitables avec les prochaines étapes pour une correction efficace.

Sécurité du réseau

Dans un contexte où les organisations adoptent de plus en plus des régimes de travail hybrides, permettant aux utilisateurs de se connecter régulièrement au réseau depuis l'extérieur du bureau ou sur des appareils non sécurisés, il est de plus en plus important de sécuriser l'accès au réseau. Une numérisation accrue des processus signifie un plus grand volume de données stockées, transférées ou utilisées, exposant les organisations à des risques. C'est là que les évaluations de vulnérabilité entrent en jeu.

Une évaluation de la vulnérabilité comprend deux éléments :

- Analyse et signalement des vulnérabilités
- Planification de l'analyse et des mesures correctives

Les spécialistes en sécurité de Ricoh analysent les systèmes accessibles aux utilisateurs externes pour détecter les vulnérabilités telles que les correctifs manquants, les versions de logiciels obsolètes, les ports ouverts et les services de système d'exploitation.

À partir de là, nous rendons compte des résultats et élaborons un plan adapté au client afin de corriger les failles de sécurité. Les évaluations de vulnérabilité peuvent être effectuées de façon récurrente ou à titre de service ponctuel.

Sécurité des terminaux

Les terminaux sont les points d'entrée les plus courants pour les logiciels malveillants, les rançongiciels et les tentatives d'ingénierie sociale. Si un cybercriminel accède à l'un de vos terminaux, il peut potentiellement trouver des moyens d'accéder à des zones critiques du réseau pour accéder aux données sensibles ou lancer de grandes attaques.

Il ne suffit pas d'acheter un logiciel antivirus, de le configurer et de l'oublier. Une sécurité robuste des terminaux vous permet de protéger vos systèmes chaque fois que les employés accèdent au réseau à l'aide d'appareils tels que des téléphones intelligents, des ordinateurs portables ou des tablettes.

Nous pouvons également fournir le personnel, le temps et les connaissances nécessaires pour aider à la création et au déploiement de politiques, de normes et de paramètres de sécurité des appareils d'impression dans l'ensemble des appareils d'un client, y compris les appareils de Ricoh et d'autres fournisseurs.

1 **Logiciel antivirus**

Les logiciels antivirus peuvent être regroupés dans trois catégories principales : ceux qui sont basés sur la reconnaissance des signatures, ceux qui analysent le comportement des fichiers, et ceux qui exploitent l'apprentissage automatique.

- **Reconnaissance des signatures :** La méthode basée sur la reconnaissance des signatures compare le code d'un fichier suspect à une base de données de signatures de logiciels malveillants connus. S'il y a une correspondance, le fichier est immédiatement signalé et bloqué, mis en quarantaine ou supprimé**.**
- **Analyse du comportement :** Ce logiciel analyse les comportements d'un fichier (comme le chiffrement rapide), ce qui lui permet de découvrir de nouveaux logiciels malveillants qu'il n'a jamais vus auparavant. Puisque les cybercriminels évoluent constamment et développent de nouvelles souches de logiciels malveillants, cela offre une protection beaucoup plus forte que les solutions basées sur la signature.
- **Apprentissage automatique à base d'intelligence artificielle:** Cette méthode basée sur l'apprentissage automatique est le type de protection antivirus le plus récent et le plus robuste, appliquant des algorithmes et des ensembles de données pour détecter les comportements associés aux logiciels malveillants sur des appareils individuels et sur de grands réseaux.

2 **Filtrage Web**

La combinaison de mesures défensives de sécurité et d'un filtrage du contenu Web minimise les risques et maximise la sécurité en tant que composante essentielle de la défense. Le filtrage est couramment utilisé pour les courriels, que ce soit pour bloquer les pourriels, pour assurer la sécurité des courriels entrants ou pour filtrer leur contenu. Bien que la protection des courriels soit importante, elle ne représente que la moitié de la solution de filtrage.

Le filtrage Web géré est conçu pour bloquer les domaines malveillants qui pourraient héberger du contenu nuisible comme des rançongiciels, des logiciels malveillants, des virus et des tentatives d'hameçonnage de données. En option, certains types de contenu peuvent être bloqués en fonction des besoins individuels de l'entreprise afin d'empêcher l'accès à des domaines qui peuvent contenir du contenu pour adultes, des jeux de hasard, des plateformes de minage de cryptomonnaie, des sites de rencontres ou d'autres contenus interdits.

3 **Gestion des appareils mobiles**

Les applications de gestion d'appareils mobiles comme Microsoft Intune peuvent être utilisées pour déployer la gestion d'applications lors de la sécurisation d'applications sur l'appareil mobile d'un utilisateur afin de contrôler le transfert de données. Cette méthode peut être utilisée lors de la sécurisation globale d'un appareil mobile, en protégeant également contre les logiciels malveillants et en permettant la suppression complète des données de l'entreprise en cas de menace ou de départ d'un employé.

Gestion experte de la cybersécurité

Une bonne préparation commence par l'intégration de services et de solutions de cybersécurité intelligents dans vos processus d'affaires de base et par l'assurance d'une gestion rigoureuse par des experts en cybersécurité des TI.

L'évolution constante des menaces impose la nécessité d'une gestion sans compromis et ciblée des systèmes, des appareils et des environnements. Les équipes des TI subissent plus de pression que jamais pour maintenir les opérations, appuyer les secteurs d'activité et offrir du soutien aux utilisateurs. En confiant votre cyberprotection à une équipe d'experts en la matière, vous libérerez votre service TI pour qu'il se concentre sur les capacités de base sans distraction. Une équipe des TI distraite et débordée mène invariablement à des lacunes dans la protection de la sécurité, avec des résultats potentiellement désastreux.

Les services et les solutions de cybersécurité des experts de Ricoh peuvent vous aider à bâtir une infrastructure informatique plus résiliente, à comprendre et à gérer vos vulnérabilités et à vous permettre de croître en toute confiance.

3e couche – Sécurité des applications

Bien que les logiciels soient conçus pour accélérer l'efficacité et la productivité, ils peuvent également poser des risques. Les applications intégrées, les applications installées et les logiciels fonctionnant comme services infonuagiques peuvent être des cibles potentielles d'intrusions. Par conséquent, vos données doivent être protégées.

Tout comme pour sécuriser vos appareils, votre organisation doit également sécuriser vos applications logicielles et les données générées par ces applications. La gestion sécuritaire de toutes ces données est un défi pour de nombreuses organisations aujourd'hui.

1 Des solutions conçues pour la sécurité

Ricoh fournit divers logiciels et solutions intégrées pour les systèmes informatiques, la gestion des processus d'affaires et les appareils et imprimantes multifonctions. Par conséquent, les micrologiciels et les applications qui s'exécutent sur des appareils Ricoh font l'objet d'un examen rigoureux et doivent être certifiés en matière de compatibilité et signés numériquement par Ricoh, en plus de nombreux autres facteurs de sécurité.

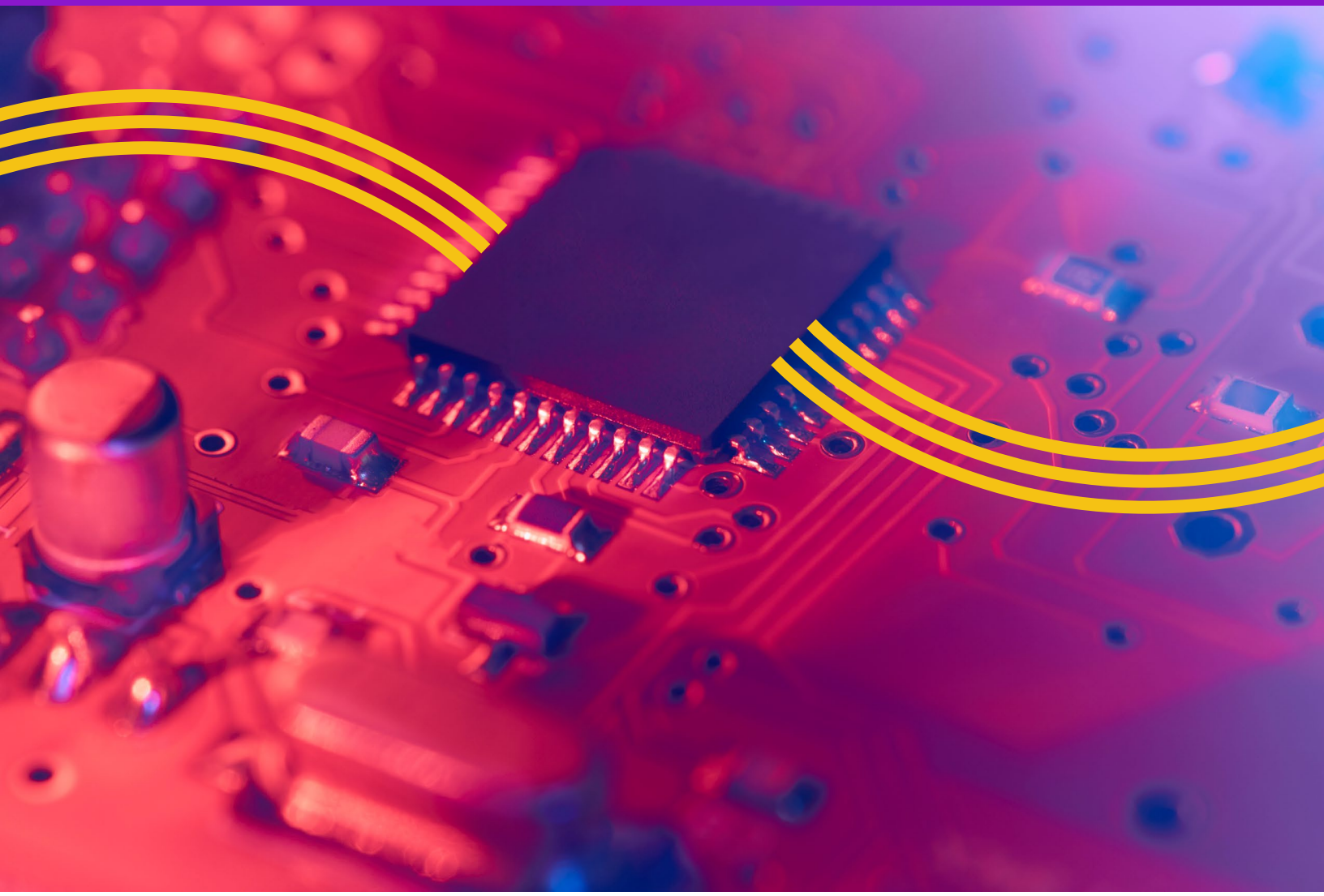
Lors de l'utilisation de ces produits, nous fournissons des fonctions de sécurité pour nous assurer que les données sensibles des clients sont protégées contre diverses menaces. Cela comprend l'atténuation des vulnérabilités persistantes des photocopieurs et des imprimantes multifonctions.

Les menaces liées à la sécurité deviennent de plus en plus avancées et sophistiquées. Ricoh continue de protéger les actifs informationnels des clients et de fournir des produits qui peuvent être adaptés à la fois à l'environnement de bureau du client et à ses politiques de sécurité, garantissant que ces produits peuvent être utilisés en toute confiance.

2 Meilleures pratiques en matière de sécurité des applications

Pour se protéger contre les dommages résultant de tiers malveillants, les administrateurs de système doivent tenir compte de ce qui suit :

1. Lisez l'intégralité du contrat de licence pour chaque logiciel et chaque solution intégrée. Pour poursuivre l'utilisation de ces services et produits, vous devez accepter les conditions.
2. Confirmez que votre système d'exploitation ou le micrologiciel de votre appareil sont à la version la plus récente avant l'installation et le fonctionnement. Installez et exploitez des logiciels et des solutions intégrées sur un réseau protégé par un pare-feu. Pour éviter les risques inhérents, il est suggéré de ne pas connecter de logiciels et de solutions intégrées directement à Internet.
3. Limitez l'accès aux logiciels et aux produits de solution intégrés aux utilisateurs autorisés seulement et limitez l'accès aux logiciels et aux produits de solution intégrés par le contrôle d'accès, en n'autorisant que les plages d'adresses IP approuvées.
4. Pour empêcher l'accès non autorisé par des tiers malveillants, modifiez le mot de passe administrateur par défaut pour le logiciel et les produits de solution intégrés et le système d'exploitation.
5. Confirmez que le logiciel, le système d'exploitation du logiciel, les solutions intégrées et l'imprimante multifonctions ou l'imprimante de base sont configurés correctement pour correspondre à votre flux de travail souhaité et respecter les politiques de sécurité de votre entreprise.



6. Les paramètres de sécurité de l'imprimante multifonctions et de l'imprimante de base doivent être réglés de manière appropriée conformément aux détails décrits dans le manuel d'utilisation du photocopieur multifonctions ou de l'imprimante dans la section « Précautions de sécurité ».
7. Utilisez le chiffrement pour toutes les données en transit. De plus, les certificats devraient être signés par une autorité de certification hébergée par l'entreprise ou par une autorité tierce publique. Des risques inhérents existent si des certificats autosignés sont utilisés.
8. Des instructions et une formation devraient être offertes aux personnes qui utilisent le logiciel et les solutions intégrées.
9. Pour atténuer les menaces extérieures, assurez-vous que les fonctions de sécurité du navigateur sont activées sur les ordinateurs utilisés pour gérer les logiciels et les solutions intégrées. De plus, n'utilisez pas le même navigateur ou la même session du navigateur pour gérer/accéder aux logiciels et aux solutions intégrées tout en accédant aux ressources réseau extérieures en même temps. Déconnectez-vous complètement de tout logiciel et de toute solution intégrée avant d'accéder aux ressources réseau externes.
10. Pour les logiciels et les solutions intégrées qui ne sont plus pris en charge, désinstallez le logiciel et supprimez toute donnée personnelle ou sensible utilisée dans les flux de travail précédents. Cela évitera la fuite des renseignements sensibles du client qui pourraient encore se trouver dans les données de ces applications.

4e couche – Sécurité des appareils

Les menaces en matière de cybersécurité ne se limitent plus seulement aux ordinateurs personnels, aux serveurs ou aux réseaux. Tous les appareils — y compris les imprimantes réseau de base — nécessitent des contre-mesures face à un vaste éventail de menaces. Au fur et à mesure que la fonctionnalité des imprimantes multifonctions (MFP) a évolué, elles sont devenues des actifs informatiques de base. Les capacités informatiques de ce qui était traditionnellement considéré comme des « imprimantes/copieurs » se sont accrues, tout comme les menaces potentielles, dont :

- L'accès malveillant par l'entremise des réseaux
- L'espionnage et l'altération des informations contenues sur les réseaux
- La fuite d'information à partir d'unités de stockage
- L'accès non autorisé par l'entremise du panneau de commande d'un appareil
- L'accès inapproprié au moyen de lignes de télécopieurs
- La fuite d'informations par l'entremise des sorties imprimées
- Les infractions aux politiques de sécurité causées par l'inadvertance

Espérer simplement que vous ne serez pas touché n'est pas une solution. Il est nécessaire de déployer des technologies, une diligence et des connaissances supérieures, ce qui exige une compréhension approfondie de la façon de résoudre les problèmes potentiels causés par les vulnérabilités de vos appareils, les données qu'ils traitent et les réseaux auxquels ils se connectent.

Authentification des appareils

Il est nécessaire de contrôler l'accès grâce à des méthodes d'authentification, conformément à vos politiques de sécurité. Des appareils sains et sécurisés peuvent offrir un autre niveau de sécurité critique, y compris un aperçu à distance de la configuration des appareils, des alertes liées à l'utilisation et aux fournitures, des alertes d'entretien critiques et des avertissements pour les problèmes d'entretien à venir.

1 **Authentification des utilisateurs des appareils**

La capacité de suivre, de contrôler l'utilisation et d'empêcher l'accès non autorisé est fondée sur l'exigence que les utilisateurs s'authentifient avant qu'ils puissent imprimer, numériser, télécopier, etc. Une fois la session ouverte, les utilisateurs ne verront que les fonctions et les options de l'appareil qu'ils sont autorisés à utiliser. Une multitude d'options d'authentification vous donne 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 tentatives de craquer les mots de passe par la force brute.

2 **Authentification des utilisateurs réseau**

Les appareils Ricoh permettent l'authentification des utilisateurs réseau afin de restreindre l'accès aux 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, mot de passe, badge d'identification avec ou sans code PIN, 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.
Pour les clients qui utilisent des cartes à puce pour l'authentification, comme les cartes d'accès communes (CAC) émises par le gouvernement ou les cartes de vérification d'identité personnelle, Ricoh offre des solutions pour activer ce type d'authentification.

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. Ces options comprennent notamment l'authentification LDAP, Kerberos et SDK avec possibilité d'intégrations personnalisées.

3 **Authentification du réseau de l'appareil**

De nombreux dispositifs Ricoh prennent en charge le protocole d'authentification IEEE 802.1X, qui fait souvent partie des mises en œuvre de réseaux à vérification systématique. Ce contrôle d'accès au réseau basé sur les ports permet à un administrateur de réseau de restreindre l'utilisation d'un réseau jusqu'à ce qu'un dispositif ait été correctement authentifié. Cela garantit une communication sécurisée entre les appareils authentifiés et autorisés.

Protection de l'appareil

Lorsque des appareils ne fonctionnent pas comme prévu, il y a non seulement des coûts associés aux temps d'arrêt, mais cela peut avoir un impact négatif sur le comportement d'autres utilisateurs, ce qui peut inclure des solutions de rechange plus ou moins désirables.

La mise à jour des micrologiciels des appareils peut être effectuée à distance et par lots, et les mises à jour peuvent être configurées selon votre horaire

1 **Gestion des micrologiciels et des pilotes**

En travaillant avec leur fournisseur de services, les organisations peuvent maintenir une ligne de défense en assurant un micrologiciel à jour sur vos appareils grâce à une gestion proactive à distance. Vous pouvez empêcher le micrologiciel de l'imprimante de devenir désuet grâce à un portail infonuagique distant. Le micrologiciel d'un appareil peut être vérifié à distance et une mise à jour peut être immédiatement lancée. Ou, les mises à jour peuvent être effectuées automatiquement selon un calendrier planifié.

L'actualisation des micrologiciels pour un grand nombre d'appareils ou pour l'ensemble d'un parc peut être traitée comme une mise à niveau par lots en quelques instants. Les pilotes peuvent également être préconfigurés et installés à distance sur les appareils. Vous pouvez configurer les pilotes avec les valeurs par défaut appropriées selon vos politiques d'impression et de sécurité, et contrôler qui a accès à différentes configurations de pilotes

2 **Validation des micrologiciels par signature numérique**

Si le logiciel intégré d'une imprimante multifonction ou d'une imprimante traditionnelle — également connu sous le nom de micrologiciel — est modifié ou compromis, celui-ci peut alors être utilisé comme méthode d'intrusion dans le réseau de l'entreprise pour endommager l'appareil ou pour constituer une plateforme ouvrant la porte à d'autres fins malveillantes. Les appareils conçus par Ricoh sont construits à l'aide d'un module de plateforme sécurisée (TPM) et sont conçus pour ne pas démarrer si un micrologiciel a été compromis. Le TPM de Ricoh est 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 imprimantes multifonctions et les imprimantes de base Ricoh utilisent une signature numérique pour juger de la validité du micrologiciel. La clé publique utilisée pour cette vérification est stockée dans une région non volatile et protégée contre l'écrasement du module 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 appareils Ricoh sont conçus pour ne pas démarrer à moins que leur micrologiciel et leurs applications ne soient vérifiés comme étant authentiques et sécuritaires pour les utilisateurs.

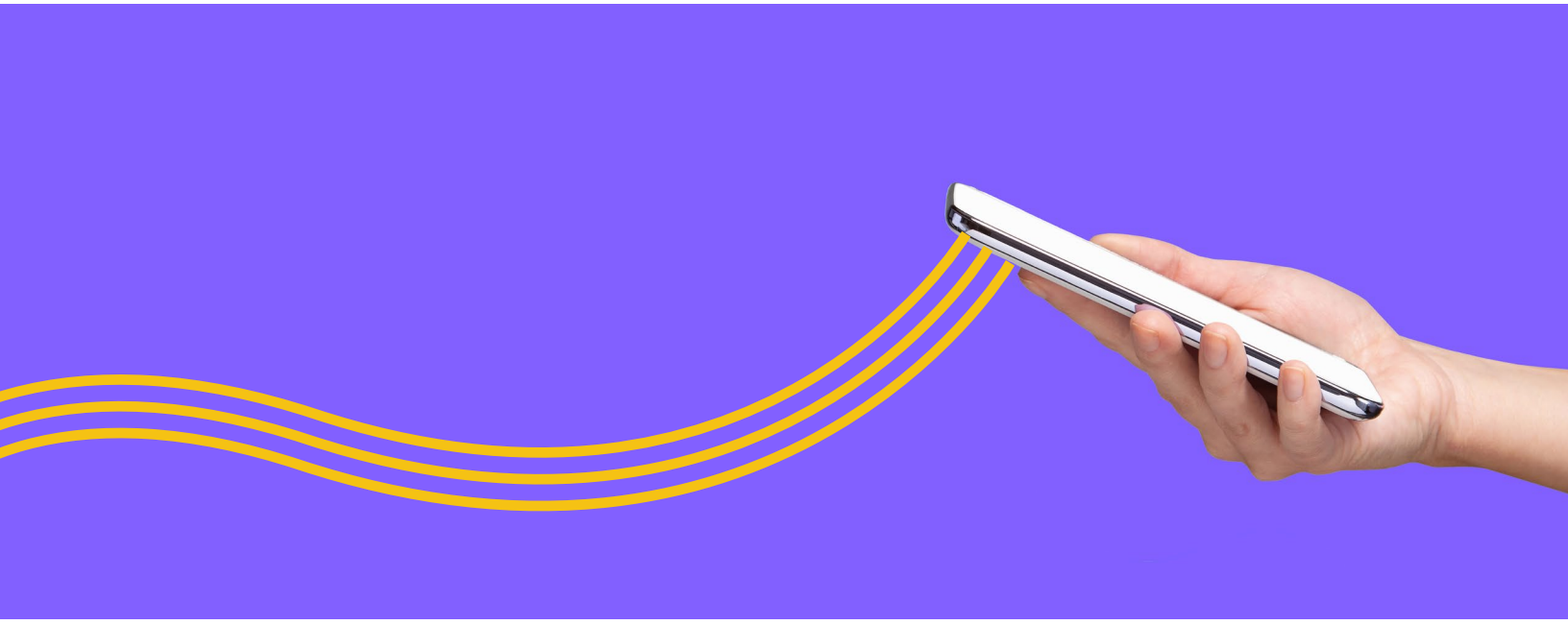
3 Désactiver les protocoles et services inutilisés

Pour faciliter l'ajout d'appareils au réseau, les systèmes réseau de nombreux fournisseurs sont systématiquement expédiés au client avec tous les protocoles et services réseau réglés à « activés ou actifs », mais les services inutilisés sur les appareils réseau posent un risque pour la 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 et l'irruption de virus ou de logiciels malveillants sur le réseau.

Il existe une solution simple, quoique souvent négligée, en ce qui concerne cette source de risque particulière : désactiver tous les services non requis. Les administrateurs d'appareils Ricoh peuvent facilement bloquer les services inutiles, ce qui contribue à rendre les appareils moins vulnérables 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 Sécurité des lignes de télécopieur

L'activation de la fonction de télécopieur d'un appareil peut exiger de le connecter à une ligne téléphonique, ce qui signifie qu'il est essentiel de bloquer l'accès non autorisé potentiel via la ligne de télécopieur. Le logiciel intégré Ricoh est conçu pour ne traiter que les types de données appropriées (c'est-à-dire les données 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 au réseau ou aux logiciels intégrés de l'appareil est éliminé.



L'unité de contrôle de télécopieur (FCU) de Ricoh prend en charge uniquement les protocoles de télécopie G3. Par conséquent, même si une connexion initiale est établie avec un terminal qui n'utilise pas ces protocoles, l'imprimante multifonction considérera que la communication a échoué et terminera la connexion. Cela empêche l'accès aux réseaux internes via les lignes de télécommunication et garantit qu'aucune donnée illégale ne peut être introduite via ces lignes.

5 Simplifier la gestion des appareils

La gestion des appareils peut prendre beaucoup de temps, et 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, tels que Streamline NX, offrent aux directeurs des TI un point de contrôle central pour surveiller et gérer 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 – et ce, à partir d'une seule console de commande.

Voici comment Ricoh s'y prend :

- Des communications SNMPv3-encrypted entre les appareils et les serveurs sont mises en place.
- Les fonctions de commande centralisées permettent aux administrateurs de contrôler l'accès, de surveiller les paramètres de sécurité et de gérer les certificats des appareils.
- Les tâches automatisées de mise à jour des micrologiciels peuvent également réduire les risques associés aux micrologiciels obsolètes.
- Des versions de micrologiciel approuvées par le client sont déployées ou la plus récente version de micrologiciel disponible auprès de Ricoh est utilisée.
- Le plugiciel Security Analyst pour Streamline NX fournit un tableau de bord en un coup d'œil pour évaluer la conformité aux politiques de sécurité des appareils et offre une liste de vérification des pratiques exemplaires pour savoir si les appareils respectent les politiques.

6 Compteurs et alertes

Lorsqu'un avertissement précoce permet aux équipes de résoudre un problème avant qu'il ne cause des temps d'arrêt, les utilisateurs risquent moins de réagir avec des comportements inattendus, comme en adoptant des solutions de rechange non autorisées. Si les appareils ne fonctionnent pas comme prévu, les utilisateurs peuvent réagir en adoptant des plans d'action imprévus et non sécurisés. Ils peuvent imprimer ou numériser à partir d'un appareil local sans pouvoir vérifier l'activité ou protéger les données transférées.

L'utilisation d'un logiciel de surveillance et de gestion des appareils vous permet de recueillir des renseignements et de garder votre appareil sain grâce à des alertes en temps opportun. Cette surveillance comprend la collecte automatique des données de compteur en fonction de l'horaire établi, des alertes de toner épuisé/à remplacer, les alertes d'entretien critiques et des alertes de tâches d'entretien critiques à venir.

7 @Remote.NET

Le plugiciel @Remote Connector NX de Ricoh améliore les fonctionnalités de Streamline NX en collectant les alertes d'entretien imminentes et en les transmettant directement à votre fournisseur de service. Votre fournisseur est donc en mesure de planifier les mises à jour des micrologiciels à distance et de mettre en œuvre les mises à jour critiques immédiatement. Le plugiciel @Remote Collector recueille aussi les données des compteurs des appareils et les rend disponibles selon un horaire préétabli, de pair avec les alertes de niveaux de fournitures consommables, afin de maximiser le temps de fonctionnement et de diminuer le fardeau administratif. Les données recueillies sont disponibles sur le portail Web @Remote.NET.

Types de chiffrement

1 Chiffrement du disque

Si le disque dur est physiquement retiré d'un appareil Ricoh, les données chiffrées ne peuvent pas être lues. Une fois activée, la fonction de chiffrage du disque dur peut aider à protéger le disque dur d'une imprimante multifonctions contre le vol de données tout en aidant les entreprises à se conformer aux politiques de sécurité en vigueur. Le chiffrement comprend les données stockées dans le carnet d'adresses d'un système, ce qui réduit le risque de détournement des données des employés, des clients ou des fournisseurs d'une organisation.

Les types de données suivants, qui sont stockés dans la mémoire NVRAM ou sur le disque dur des imprimantes multifonctions, peuvent être chiffrés :

- Carnet d'adresses
- Données sur l'authentification des utilisateurs
- Documents stockés
- Fichiers éphémères
- Journaux
- Configurations de l'interface réseau
- Informations sur les configurations

2 Chiffrement des données en transit de l'appareil

Il est possible pour un cybercriminel avisé d'intercepter des trains de données brutes, des fichiers et des mots de passe lorsque les informations circulent au sein du réseau. Sans une protection adéquate, les informations non chiffrées peuvent être volées, altérées, falsifiées et réintégrées dans le réseau à des fins malveillantes. Pour combattre cette menace, 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 point à l'autre.

3 Chiffrement des flux d'impression

Les données envoyées dans un flux d'impression peuvent être exploitées si elles ne sont pas cryptées et être interceptées en cours de route. Ricoh permet le cryptage des données d'impression au moyen des protocoles de cryptage 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 cryptées en transit n'obtiendrait que des données indéchiffrables. Les données envoyées aux imprimantes pourraient être mal utilisées ou attaquées si elles ne sont pas chiffrées.

4 Chiffrement de bout en bout basé sur les pilotes

Les risques d'attaque malveillante sur les données des tâches d'impression peuvent être atténués à l'aide du pilote d'impression universel Ricoh pour le chiffrement de bout en bout des données d'impression entre le système de l'utilisateur et l'imprimante multifonctions Ricoh. Le chiffrement de bout en bout peut être activé dans la boîte de dialogue d'impression afin qu'un utilisateur puisse définir un mot de passe de chiffrement. Pour lancer la tâche d'impression, l'utilisateur entre le mot de passe de chiffrement sur le dispositif Ricoh, qui déchiffre ensuite les données et imprime la tâche. Cette méthode de chiffrement des données d'impression utilise le chiffrement AES-256.

5 Tâches d'impression verrouillées

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 chiffrés 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 bons authentifiants du réseau. Pour encore plus de capacités, des logiciels comme SLNX de Ricoh (voir photo) peuvent assurer le relâchement de documents entièrement sécurisé en offrant aux utilisateurs des options relativement aux flux d'impressions tout en préservant le contrôle des administrateurs.

6 Sécurité des données photocopiées

Ricoh offre des fonctions visant à empêcher les copies non autorisées de documents papier afin de contribuer à prévenir les fuites d'informations. 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 est 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, protégeant 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.

7 Impression obligatoire des renseignements sur la sécurité

Identifier les documents avec des informations clés permet d'améliorer la responsabilisation et le contrôle de la gestion des documents. 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 ou le numéro de série de l'appareil utilisé

8 Suppression des données temporaires

Lorsqu'un document est numérisé ou lorsque des informations sont reçues à partir d'un ordinateur, certaines données peuvent être temporairement stockées sur le disque dur ou 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. Ces données temporaires représentent une vulnérabilité potentielle pour la sécurité.

Le système de sécurité par écrasement des données (DOSS) qui est 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 tâche est terminée avec succès. Le système de sécurité DOSS peut également :

- Inclure des options conformes aux recommandations du Service canadien du renseignement de sécurité (SCRS) et du ministère de la Défense nationale (MDN) concernant le traitement des renseignements classifiés
- Rendre virtuellement impossible l'accès aux données latentes des tâches de copie, d'impression et de numérisation 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 se conformer aux lois et règlements comme le HIPPA, la LPRPDE, le GLBA, le FERPA et autres
- Fournir une rétroaction visuelle relativement au processus d'écrasement (c.-à-d. processus terminé, processus en cours) à l'aide d'une simple icône

Normes et certifications de sécurité indépendantes

Les Critères communs sont utilisés à l'échelle internationale pour l'évaluation de la sécurité des technologies de l'information. Ces critères servent à évaluer si les fonctions de sécurité sont développées de manière appropriée pour les produits informatiques. La certification des Critères communs est une norme reconnue par plus de 25 nations du monde. Les fournisseurs de photocopieurs multifonctions nationaux et internationaux s'efforcent d'obtenir l'authentification pour les photocopieurs multifonctions numériques.

Le processus de certification des Critères communs vérifie la protection offerte par plusieurs technologies de sécurité contre diverses menaces à la sécurité. La certification couvre, par exemple, la vérification de la validité du système au démarrage, le contrôle et l'enregistrement de l'accès, la protection des données par chiffrement et la suppression des données lors de la mise hors service de l'appareil. Par conséquent, elle aide à protéger nos produits contre diverses menaces, comme l'altération de logiciels, l'accès non valide et la fuite d'informations.

1 **Profil de protection pour les dispositifs d'impression sur papier (PP_HCD_V10)**

Le profil PP_HCD_V10 est un profil de protection approuvé par le gouvernement des États-Unis pour les dispositifs d'impression sur papier tels que les imprimantes multifonctions numériques. Il a été développé par l'association Multifunction Printers Technical Community avec des représentants de l'industrie (y compris Ricoh), des agences gouvernementales américaines et japonaises, des laboratoires d'essais des Critères communs et des organismes internationaux chargés d'appliquer les Critères communs. L'objectif de ce profil de protection (PP) est de faciliter l'approvisionnement efficace en dispositifs d'impression sur papier commerciaux prêts à l'emploi en utilisant la méthodologie des Critères communs pour l'évaluation de la sécurité des technologies de l'information.

Les domaines suivants, qui ont été identifiés comme étant parmi les plus importants pour les protections de sécurité, ont été validés dans la plupart des appareils Ricoh selon la norme PP_HCD_V10 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

Plus de 50 produits répondant aux critères communs (ISO/IEC15408)

Chez Ricoh, nous améliorons constamment notre gamme de produits pour répondre aux exigences changeantes de nos clients et des organismes de réglementation.

2 IEEE 2600.2

La norme de sécurité IEEE 2600.2 concerne les dispositifs d'impression sur papier fonctionnant dans un environnement de traitement de l'information commerciale, avec les niveaux requis de sécurité des documents, de sécurité du réseau et d'assurance de la sécurité. Elle établit une base commune des attentes en matière de sécurité pour les appareils multifonctions. Afin de s'assurer qu'un appareil est conforme à la norme établie, des tests réalisés par un laboratoire indépendant confirment le bon fonctionnement des fonctions de sécurité du fabricant. Ricoh offre une vaste gamme d'appareils multifonctions certifiés conformément à la norme de sécurité IEEE 2600.2.

3 FIPS 140-2/3

Parmi les 200 meilleurs sous-traitants du gouvernement fédéral

La Federal Information Processing Standard (FIPS) 140-2/3 est une norme de sécurité du gouvernement américain pour la validation des modules cryptographiques par le biais du programme de validation des modules cryptographiques (CMVP) du National Institute of Standards and Technology (NIST). De nombreux modules cryptographiques dans les appareils Ricoh utilisent des algorithmes recommandés ou approuvés par le NIST, y compris des algorithmes validés dans le cadre du programme de validation de l'algorithme cryptographique (CAVP) du NIST. La validation CAVP est une condition préalable à la validation CMVP.

Les clients peuvent mettre à niveau certains appareils vers un lecteur certifié CMVP* et installer une mise à niveau des micrologiciels d'appareils multifonctions qui sera bientôt disponible pour intégrer des modules validés CMVP aux autres systèmes d'appareils multifonctions**. Les appareils dont les micrologiciels ont été mis à jour mettront en œuvre certaines mesures de renforcement de la sécurité, y compris la désactivation des ports et des protocoles moins sécurisés, ainsi que la limitation de l'utilisation de certaines applications.

* Des disques durs certifiés FIPS 140-2 CMVP sont maintenant disponibles en quantité limitée pour bon nombre de nos produits.
** La mise à niveau du micrologiciel est prévue pour une prochaine version. Peut ne pas convenir à tous les appareils.

5e couche – Sécurité des données

Les données sont la devise la plus précieuse de votre organisation, et avec la quantité et la diversité des menaces pour les données auxquelles nous sommes tous confrontés, les dirigeants d'entreprise doivent prioriser la protection des données et structurer la gouvernance de façon à soutenir ces efforts.

Les menaces proviennent de diverses sources externes et internes, y compris les cyberattaques, les attaques de rançongiciels, les menaces internes, les défaillances technologiques, les catastrophes naturelles, l'hameçonnage et les erreurs humaines. Une organisation résiliente exige des stratégies de protection qui servent à prévenir les brèches de données ainsi que des stratégies pour atténuer les dommages en cas d'attaque.

1 **Chiffrement**

Comme mentionné dans les sections précédentes de ce document, le chiffrement des données doit être appliqué aux documents, fichiers, messages ou toute autre forme de communication sur un réseau. Ricoh s'assure que tous ses appareils, logiciels et solutions de stockage offrent un chiffrement de bout en bout.

La sécurité des données devrait être une priorité absolue pour tous les membres du personnel, mais vous ne pouvez pas toujours vous fier à eux pour savoir quand et comment les données doivent être chiffrées. Lors de l'élaboration de la politique de chiffrement de votre organisation, vous devez d'abord obtenir une image précise de l'endroit où se trouvent toutes vos données, de leur confidentialité ou de leur valeur (une cible potentielle pour les acteurs malveillants) et des risques qu'elles présentent pour votre organisation. Le nettoyage des données non structurées et la réalisation d'une évaluation de l'impact sur la protection des données vous permettront d'élaborer une stratégie complète de sécurité des données.

2 **Hébergement en nuage**

L'intégration de vos données et de votre infrastructure distribuées dans un seul environnement infonuagique permet une surveillance et une gestion holistiques de bout en bout, le comblement des lacunes en matière de sécurité et la mise en place d'une gestion plus rigoureuse et centralisée. Les modèles de nuage public, privé et hybride permettent différents niveaux de sécurité adaptés aux besoins de votre organisation.

Microsoft 365 et Azure sont des plateformes infonuagiques publiques de premier plan en raison des nombreuses couches de fonctionnalités de sécurité, d'ajouts et d'intégrations de Microsoft, allant de la gouvernance unifiée des données au partage sécurisé des fichiers, en passant par l'authentification des utilisateurs et la gestion de l'identité.

3 **Sécurité contre les rançongiciels**

Il existe deux couches essentielles à la sécurité des rançongiciels : la prévention et l'atténuation. Les solutions préventives détectent les signatures et les comportements des rançongiciels, les empêchant de dépasser le périmètre, tandis que le confinement des rançongiciels arrête les éclosions de chiffrement malveillant s'il traverse les mesures de protection. Le logiciel met l'accent sur le résultat d'un rançongiciel, un chiffrement illégitime rapide. Il arrête le chiffrement au niveau du fichier source ou racine, l'isolant et le contenant pour empêcher toute propagation ultérieure.

Le confinement des rançongiciels est une dernière ligne de défense critique pour l'infrastructure de sécurité d'une organisation, surveillant les interactions dangereuses entre les dispositifs et les fichiers partagés, un domaine où les organisations manquent souvent de défenses essentielles.

4 Sauvegarde et récupération sécurisées des données

Prévoir l'imprévisible est un élément essentiel de la sécurité des données, qu'il s'agisse d'une cyberattaque ou d'un dysfonctionnement du système, pour maintenir les opérations dont vous avez besoin pour savoir que vos données peuvent être restaurées de manière fiable et rapide.

Les solutions de sauvegarde les plus fiables et les plus sécuritaires impliquent une combinaison de technologies infonuagiques avancées et de gestion experte, c'est pourquoi de nombreuses organisations externalisent à un fournisseur de services de confiance. De la mise en œuvre à la configuration, en passant par les tests réguliers et la récupération, vous pouvez être assuré que vos données sont protégées et accessibles dans n'importe quel scénario

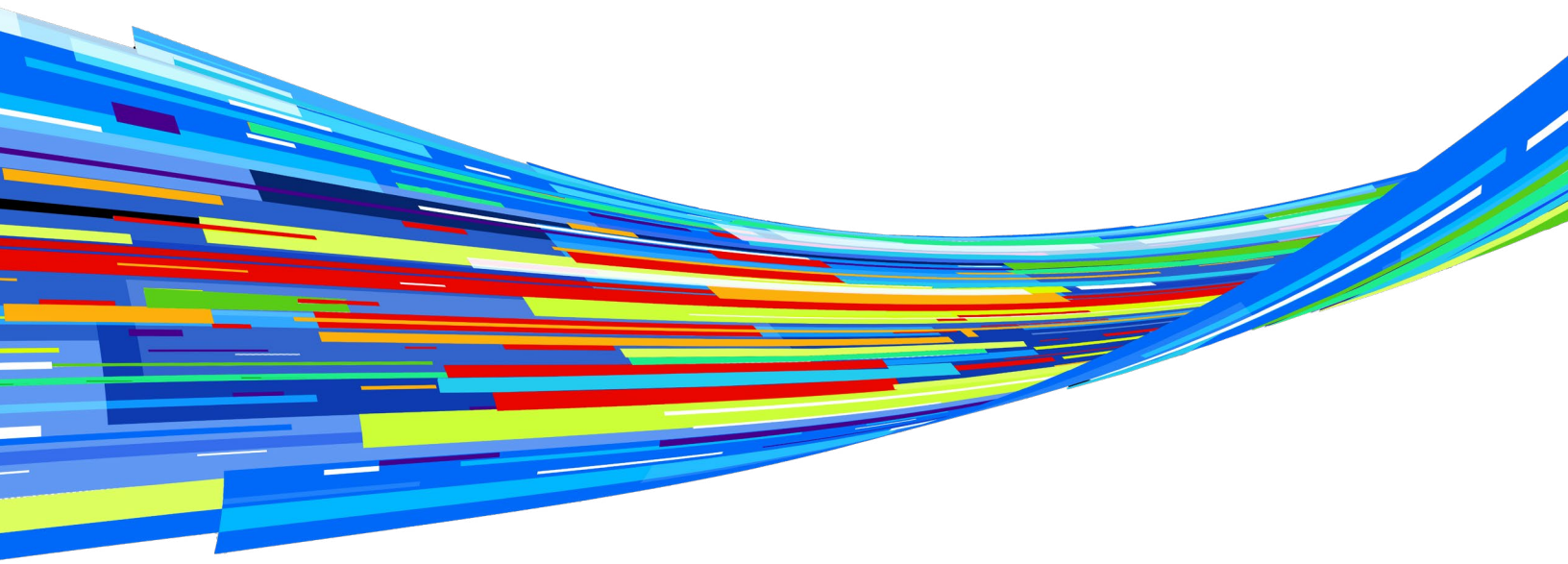
5 Évaluations de la conformité

Les organisations assujetties aux normes, lois et règlements PCI DSS, PII, LPRPDE, HIPAA, FINRA, FERPA, RGPD, CCPA, ou qui doivent répondre aux exigences de conformité des assureurs, des clients ou d'autres politiques de sécurité de l'entreprise doivent envisager des services professionnels axés sur la conformité.

Ces services ciblés aident les clients à se conformer à une variété de règlements fédéraux, provinciaux et industriels, y compris la Loi sur la protection des renseignements personnels et les documents électroniques, le PIPA et la Loi sur la protection des renseignements personnels dans le secteur privé.

Les mesures axées sur la conformité comprennent :

- Saisie, marquage et archivage automatisés de tous les courriels et pièces jointes
- Préservation du format de courriel original
- Suppression automatisée des utilisateurs
- Gestion des appareils mobiles
- Isolation des systèmes pour les informations sensibles
- Droits d'accès liés et vérification des identités des utilisateurs
- Réponse réglementaire à la suite de violations



Conseils et soutien stratégiques

Consultations en sécurité

Faites passer votre stratégie informatique d'une stratégie de simple soutien des activités quotidiennes à une stratégie qui fait partie intégrante de la mise en place et du soutien d'initiatives commerciales sûres et stratégiques.

Les directeurs des systèmes d'information virtuels et les spécialistes en technologie de Ricoh sont en mesure de vous aider à concevoir une stratégie de sécurité globale qui est évaluée, testée, puis testée 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 lacunes pouvant entraîner des cyberattaques et les autres angles d'exposition de votre technologie à l'interne avant que votre entreprise ne soit touchée.

Services de conseil en matière de gouvernance de l'information

De nombreuses organisations éprouvent des difficultés avec plusieurs aspects de la gestion de l'information, comme la sécurité et la protection, la conservation et l'élimination, la conformité juridique et réglementaire, la fiabilité et l'authenticité.

Les consultants en gouvernance de l'information de Ricoh sont des spécialistes de ces enjeux, aidant les organisations à supprimer les cloisonnements et à mettre en place des programmes durables à long terme. Nous considérons l'information à la fois comme un problème et comme une solution et nous adoptons une approche proactive pour relever vos défis en matière d'information afin de permettre à votre organisation de prendre des décisions commerciales judicieuses.

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. Avec des activités dans approximativement 200 pays et territoires à l'échelle mondiale, Ricoh emploie plus de 9 000 techniciens et spécialistes de la prestation de service. Notre réseau de partenaires détaillants de vente et de soutien se démarque par sa capacité de traiter avec 60 % des entreprises 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.

60%

des entreprises Fortune 1000 font affaire avec nous

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 des rapports et des certificats de validation des Critères communs pour certaines offres de produits. 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 relativement aux appareils et aux réseaux ainsi que des guides sur l'administration sécuritaire des appareils exigés en vertu des Critères communs sont également disponibles pour les clients. Ces guides fournissent des informations détaillées sur la manière dont l'équipement de Ricoh transmet les données de l'appareil et dans quelle mesure celui-ci interagit avec le réseau. Cliquez ici pour consulter plus en détail la documentation.

Formation des administrateurs et des utilisateurs finaux

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 propose des formations sur ses appareils – et ceux de ses partenaires – à l'intention des utilisateurs finaux et des administrateurs. Armés 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 les informations de votre organisation et à respecter la réglementation en vigueur.

L'engagement de Ricoh en matière de sécurité

La sécurité fait partie intégrante de nos valeurs, et nous ne prenons pas cet engagement à la légère. 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 l'assurance d'utiliser des services, des logiciels et des appareils hautement sécurisés, nous visons à gagner votre confiance en ayant les normes de sécurité les plus élevées de l'industrie. Notre objectif est de garder une longueur d'avance sur les cybercriminels, et s'ils empiètent sur nos systèmes, nous avons un plan et des systèmes en place pour atténuer les intrusions.

Notre engagement envers chaque client est de respecter les normes et les directives de sécurité actuelles dans nos produits et services, de travailler avec diligence pour protéger les données de nos clients et de leur permettre de se protéger. Nous nous engageons à toujours évaluer, apprendre et innover avec chaque initiative, en cherchant à atteindre les meilleurs résultats pour nos clients et nos partenaires.

Les menaces à la sécurité de l'information deviennent de plus en plus avancées et difficiles à repérer. Ricoh s'engage à offrir des produits sécurisés qui protègent vos actifs informationnels et s'harmonisent avec votre environnement de bureau et vos politiques de sécurité. Assurer la sécurité exige des paramètres bien configurés et une mise en œuvre adéquate dans votre environnement spécifique.

Notre expérience approfondie et notre approche multicouche peuvent être mises à profit dans l'ensemble de votre organisation, qu'il s'agisse de la stratégie, des appareils, des logiciels, des services, du soutien, de la formation et plus encore. Laissez-nous vous aider dans votre évolution vers de meilleurs services d'information numérique.

RICOH
imagine. change.

Ricoh, un partenaire de confiance

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 meilleure agilité opérationnelle, davantage d'expériences humaines et la capacité à prospérer en cette époque 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. Chez Ricoh, nous n'avons jamais trop d'information.

Avez-vous des questions?
Visitez Ricoh.ca ou communiquez avec un expert en sécurité de Ricoh dès aujourd'hui.

Ricoh Canada, Inc. 100-5560 Explorer Drive, Mississauga (Ontario) L4W 5M3, 1-888-742-6417 ©2023 Ricoh Canada Inc. Tous droits réservés. Ricoh® et le logo Ricoh sont des marques de commerce enregistrées de Ricoh Company Ltd. Toutes les autres marques appartiennent à leur propriétaire respectif. Le contenu de ce document, de même que l'apparence, les fonctions et les caractéristiques des produits et services de Ricoh peuvent changer de temps à autre sans préavis. Les produits illustrés comportent des options. Même après avoir pris toutes les précautions possibles pour assurer l'exactitude de l'information, Ricoh ne fait aucune déclaration ni ne garantit l'exactitude de l'information contenue dans le présent document et n'accepte aucune responsabilité à l'égard de toute erreur ou omission dans ledit texte. Les résultats réels peuvent varier selon l'utilisation faite des produits et des services, ainsi que les conditions et les facteurs pouvant altérer la performance. Les seules garanties relatives aux produits et services de Ricoh sont exposées dans les énoncés de garantie formelle s'y rattachant.

RICOH
imagine. change.