Solution de sécurité Ricoh

# Protégeons votre entreprise

RICOH
imagine. change.

La cybersécurité représente aujourd'hui un enjeu stratégique dans la pérennité et la réussite des entreprises modernes. Toutes les entreprises, indépendamment de leur taille, sont exposées en permanence à des attaques potentiellement dangereuses, telles que le hameçonnage, les attaques DDoS ou encore les logiciels rançonneurs. Le coût réel de ces attaques se chiffre en millions de dollars. En 2017, l'Institut Ponemon a déterminé que le coût moyen global de ces failles de sécurité s'élevait à 3,62 millions de dollars. Ce coût est appelé à s'accroître dans les prochaines années, car les réglementations gouvernementales comme le GDPR prévoient d'imposer de lourdes pénalités aux entreprises qui ne parviendraient pas à protéger leurs systèmes et leurs données de manière appropriée. Pour éviter de telles sanctions, les entreprises doivent pouvoir démontrer leur capacité à protéger leurs données.
À cet effet, il convient tout d'abord d'obtenir une vision globale de l'ensemble des vulnérabilités de l'entreprise.

La numérisation intensive des espaces de travail ainsi que l'explosion des volumes de données ne font qu'intensifier les défis à relever en matière de cybersécurité. Les flux de production sont exploités via de nombreux appareils, réseaux et sites géographiques. C'est lors de leurs transferts que les informations sont les plus exposées aux risques. Celles-ci doivent donc être constamment protégées. Au vu des risques de sécurité actuels, il est impensable que les entreprises ne soient pas équipées de systèmes sécurisés de gestion des données et des documents. Dans le même temps, les capacités des imprimantes et des multifonctions se sont multipliées par dix au cours des dernières années. Ces appareils traitent aujourd'hui d'énormes quantités de données commerciales (entrées, sorties, transferts et stockage) et constituent des facteurs de risques élevés, mais souvent sous-estimés, au sein des entreprises.

Si de nombreux acteurs proposent aujourd'hui des services de sécurité, Ricoh développe depuis plusieurs décennies des services et des solutions de sécurité conçus spécialement pour les espaces de travail. Cela fait par exemple plus de 20 ans que nos imprimantes sont dotées d'une fonction de réécriture sécurisée des disques durs.

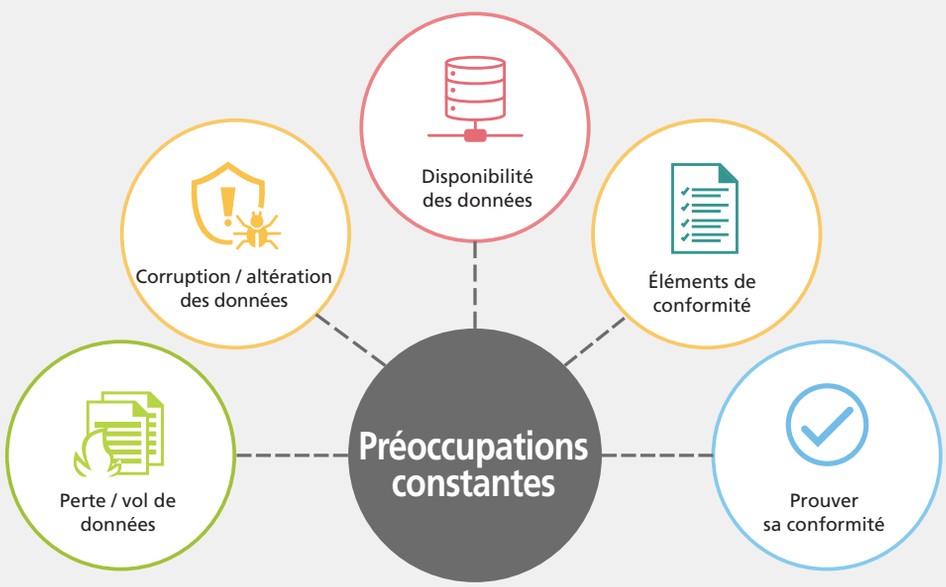
La sécurité est la marque de fabrique de notre gamme de produits dédiés aux espaces de travail numériques. Aujourd'hui, plus de 4 millions de nos produits sont en service dans le monde. Chacun des produits et services déployés en complément intègrent une sécurité renforcée. Par ailleurs, bon nombre de nos produits possèdent un système d'exploitation propre à Ricoh. Il s'agit d'un élément essentiel de défense apportant tout le contrôle et la protection nécessaires pour échapper aux attaques dont la plupart des systèmes d'exploitation sont victimes.

Ricoh propose à ses clients, à l'échelle internationale, une structure cohérente d'assistance et de services pour s'assurer que les informations relatives aux menaces sont partagées efficacement et utilisées à bon escient. Nos appareils d'impression sont conformes à la norme IEEE 2600. Par ailleurs, Ricoh compte parmi les membres et contributeurs essentiels de l'association de normalisation IEEE. Ricoh est également certifié ISO 27001 et s'engage à maintenir sa conformité avec ce système de gestion sécurisée des informations. Nous développons nos produits en fonction des besoins commerciaux de nos clients internationaux et de leurs intérêts, à travers un ensemble de programmes novateurs.

Pour répondre de manière efficace et concrète à leurs demandes, nous avons placé la sécurité au cœur de la conception de nos produits et services. Il est essentiel de disposer d'une vue d'ensemble des points faibles des entreprises pour assurer leur survie.

# LA SÉCURITÉ DE NOS CLIENTS, UN ENJEU DE TAILLE

**TENDANCES :** Avec l'augmentation des volumes des données, les points sensibles, attaques et sanctions se multiplient.




## Sécurisation et renforcement des espaces de travail numériques

Ricoh cherche à renforcer et à sécuriser les activités numériques développées par les collaborateurs. À l'ère de l'économie numérique, cela se traduit par l'apport d'une valeur ajoutée allant au-delà des espaces de travail traditionnels. Le travail à distance constitue un véritable gain de productivité et de flexibilité pour les entreprises dans la réalisation de leurs activités quotidiennes. Il permet aux entreprises de mieux répondre aux attentes et aux exigences de leurs clients en termes de services.

Cependant, les activités impliquant une connexion réseau mettent souvent à mal la sécurité des entreprises. Les appareils et données manipulés par les travailleurs mobiles doivent être sécurisés de manière appropriée. Dans leurs activités, les employés utilisent souvent plusieurs réseaux, à différents emplacements, ce qui complexifie cette tâche. Les règlementations gouvernementales, telles que le GDPR, demandent aux entreprises de sécuriser les données exploitées sur l'ensemble de leur cycle de vie et d'apporter la preuve des mesures prises, sous peine d'être pénalisées financièrement. Avec l'évolution des espaces de travail et l'adoption de flux de production numériques, le cycle de vie des données commerciales gagne graduellement en complexité. Examinons ce phénomène étape par étape.

La première étape concerne la saisie des données et les appareils de capture, composants essentiels de la stratégie Ricoh en matière de sécurité. Les données doivent ensuite être transportées sur plusieurs réseaux et stockées de manière sécurisée. À cette étape, il est indispensable de préserver l'intégrité des données. Les systèmes Ricoh restreignent l'accès utilisateur aux fonctionnalités des appareils et des réseaux afin que les données ne puissent être manipulées à aucun moment. Ces services comprennent le contrôle d'accès, le chiffrement et la protection contre les copies non autorisées. C'est que nous appelons le Contrôle.

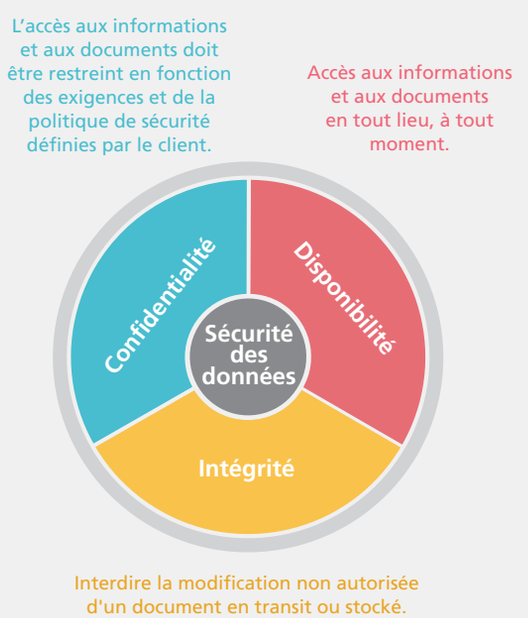
Une fois stockés, les documents doivent pour autant rester accessibles aux employés qui en ont besoin. L'extraction et la visualisation des informations à la demande dépendent de leur disponibilité. L'analyse des données est un composant vital des espaces de travail habilités. Elle fournit un aperçu pertinent de chaque élément de l'entreprise, du département des ventes aux RH. Les outils infrastructurels d'autorisation apportent un accès rapide et sécurisé, indépendamment de l'emplacement ou de l'appareil

utilisé. Les protocoles de sécurité ne doivent en aucun cas être un frein à l'innovation et aux différentes fonctionnalités et les employés ne doivent pas être paralysés par des enjeux liés à la sécurité. C'est que nous appelons la Préservation.

Ces données doivent enfin être stockées de manière sécurisée et contrôlable. Cette étape est essentielle pour être conforme aux exigences réglementaires, et réduit les risques de vol ou de perte. Dans les faits, ce processus s'applique sur toute la durée de vie des documents, jusqu'à leur suppression. Tout fichier imprimé laisse une image latente sur le disque dur des imprimantes multifonctions (MFP), qui doit être effacée complètement pour empêcher tout accès non autorisé. Nos services de suppression des données comprennent le nettoyage en profondeur des disques durs et de la mémoire, la suppression des fichiers non imprimés ainsi qu'une fonction de suppression après déconnexion pour éviter qu'une personne malintentionnée ne recueille des données sensibles à partir des traces laissées par les documents. C'est que nous appelons la Destruction.

Pour sécuriser de manière efficace les données professionnelles tout au long de leur cycle de vie, Ricoh utilise le même mode opératoire que la CIA en matière de confidentialité et de sécurité : Confidentialité, Disponibilité et Intégrité. Nous utilisons ces trois grands principes pour concevoir des produits et des solutions conformes aux normes et réglementations en vigueur. Cette approche laisse libre cours à l'innovation et à la croissance dans les espaces de travail, tout en garantissant l'efficacité et la sécurité des processus.

# LA SÉCURITÉ VUE PAR RICOH




**Nous reprenons les principes de la CIA en matière de sécurité : confidentialité, intégrité et disponibilité.**


**La sécurité est notre marque de fabrique. Tous les produits et services Ricoh ont été conçus en intégrant plusieurs fonctions de sécurité.**

Ricoh propose une suite complète de produits et de services permettant de sécuriser l'intégralité du processus de création des documents.

Analysons à présent chaque étape clé : contrôle, préservation, destruction et support.

# QUATRE ÉTAPES DE SÉCURITÉ POUR LES ESPACES DE TRAVAIL NUMÉRIQUES

## 1 CONTRÔLE

Un contrôle efficace des données est primordial pour en assurer la confidentialité et l'intégrité. Les informations commerciales sont des ressources de premier ordre qui doivent impérativement être protégées. Les appareils physiques sont aujourd'hui des terminaux d'informations susceptibles de laisser s'échapper des informations commerciales. C'est pourquoi Ricoh emploie plusieurs outils d'authentification utilisateurs et d'administration des appareils pour contrôler et sécuriser les données commerciales. Ils se retrouvent dans les paramètres de nos appareils qui autorisent ou interdisent l'accès à certaines fonctionnalités et données. Limiter l'accès des employés aux informations transitant par un MFP est une bonne pratique essentielle pour assurer la sécurité des documents. La phase de contrôle comprend également une protection contre les programmes malveillants, qui se fait par la mise en place d'un système de sécurité de nos firmwares sur trois niveaux.

### Contrôle des tentatives de copies non autorisées

Pour empêcher toute tentative de copie non autorisée, Ricoh propose une solution astucieuse pour assurer la sécurité des documents papier. Notre système de protection contre les copies imprime ou copie les documents en y intégrant des motifs invisibles en arrière-plan. Si le document imprimé ou copié est photocopié et/ou numérisé, les motifs apparaîtront sur les copies. Le module de protection contre les copies non autorisées permet aux MFP de détecter les motifs intégrés et remplace l'image photocopiée par une image grise pour éviter les fuites d'informations. Cette fonction est très utile lors de l'impression d'informations confidentielles. Restreindre la duplication d'informations confidentielles évite ce type d'inconvénients.

### Impression sécurisée

Un document reçu d'un ordinateur peut être stocké sur le disque dur du MFP. Avec la fonction de verrouillage d'impression de Ricoh, un mot de passe est créé lors de l'envoi d'un document. L'utilisateur doit ensuite saisir ce mot de passe sur le MFP pour lancer l'impression. Le document ne pouvant pas être imprimé avant d'arriver sur l'appareil, l'impression verrouillée permet au propriétaire d'en garder le contrôle à tout moment.

### Capture avancée

Les solutions de capture avancée proposées par Ricoh offrent plusieurs niveaux de chiffrement et de déchiffrement à chaque étape du processus de capture. Les administrateurs peuvent autoriser un ou plusieurs utilisateurs à accéder aux files d'attente de traitement par le biais d'informations d'authentification. Les niveaux de sécurité supplémentaires comprennent le SAML (Security Assertion Markup Language) pour une structure SSO (Single Sign On, authentification unique), PIV (Personal Identity Verification, vérification personnelle d'identité) et le chiffrement PKI (Public Key Infrastructure, infrastructure à clés publiques).

### Contrôles d'authentification intégrée

La gestion des protocoles d'accès et d'authentification des produits Ricoh peut s'effectuer de manière centralisée. Plusieurs méthodes d'authentification sont disponibles, telles que l'authentification par carte d'identité, code PIN, la connexion réseau ou à facteurs multiples, ou encore une combinaison de ces méthodes. L'authentification à facteurs multiples renforce la sécurité mais suppose un ralentissement des processus pour les utilisateurs. L'authentification unique (SSO) est utile à cet égard, car elle permet aux utilisateurs d'accéder à plusieurs appareils en toute simplicité. De plus, le logiciel Quick Authentication de Ricoh (mécanisme d'authentification à carte) est préinstallé sur nos appareils pour permettre aux utilisateurs d'accéder facilement à leurs documents. Un dispositif de lecture/écriture NFC simplifie grandement la connexion de l'utilisateur tout en garantissant un accès sécurisé et contrôlé au MFP. Cette forme d'accès fonctionne également en complément des paramètres d'autorisation habituels du MFP pour restreindre l'accès utilisateur aux fonctions de l'appareil, comme déterminé par le client.

## Streamline NX (SLNX)

Le module de gestion d'appareils de la plateforme Streamline NX de Ricoh est un logiciel d'administration et de surveillance des appareils présents sur un réseau. Le logiciel permet aux administrateurs d'afficher ou de configurer les paramètres de sécurité des appareils à l'aide de modèles prédéfinis et de paramètres personnalisés. Les paramètres de sécurité essentiels comprennent l'activation / la désactivation des protocoles, les paramètres d'adressage IP, les mots de passe administrateurs, les alertes par e-mail, les paramètres de chiffrement et bien plus encore. SLNX peut également signaler les imprimantes non conformes à la politique du client.

## Protection contre les programmes malveillants

Ricoh utilise trois niveaux de sécurité pour protéger ses appareils des programmes malveillants. Tout d'abord, les appareils Ricoh peuvent uniquement fonctionner avec un langage ou un système d'exploitation Ricoh. Puis, pour éviter toute altération malveillante par un logiciel, les mises à jour du microprogramme doivent être écrites et approuvées exclusivement à l'aide du langage Ricoh. Enfin, chaque mise à jour firmware doit être signée numériquement par Ricoh. Grâce à ces trois étapes, aucun microprogramme non approuvé ne pourra s'installer sur des appareils Ricoh : les programmes malveillants/espions et les virus sont donc efficacement écartés.

## Sécurisation des documents papier

Les meilleurs pratiques en matière de sécurité ne sont pas forcément complexes. Les espaces de travail sont des lieux à forte activité pour lesquels les documents papier constituent un risque majeur (vol et négligence des employés). Ricoh propose des options supplémentaires afin de renforcer la sécurité physique des documents papier et d'en empêcher l'accès non autorisé. Verrouiller des tiroirs papiers évite par exemple les vols de supports papier sensibles, tels que les modèles d'ordonnances dans le domaine médical. Les obturateurs de câbles écartent également le risque de toute manipulation en interne. Une solution sécurisée d'impression des documents (Print-to-me) garantit leur impression uniquement en présence de leur propriétaire, afin d'éviter les risques liés à l'oubli de documents imprimés.

# 2 PRÉSERVATION

Pour répondre aux nombreuses exigences réglementaires, les entreprises doivent sans cesse garantir la confidentialité et l'intégrité de leurs informations afin d'en éviter la perte, le vol ou toute manipulation indésirable. Pour y parvenir, elles doivent restreindre l'accès aux documents sensibles. Toute modification non autorisée ou falsification devient alors impossible. L'objectif est également de se protéger des menaces ciblées ou opportunistes en interne.

Le travail mobile est un défi supplémentaire à relever. Des mesures de sécurité supplémentaires doivent être mises en place pour permettre le partage de fichiers, sans restriction géographique. Ces fichiers doivent être sécurisés pendant leur transfert sur les réseaux, entre les appareils, mais également lorsqu'ils sont stockés. Une technologie de chiffrement forte permet de suivre et de protéger efficacement les données sur l'ensemble de leur cycle de vie. Elle s'applique bien sûr aux documents, mais également à certains éléments clés de sécurité, comme les mots de passe, les paramètres et les carnets d'adresses stockés sur l'appareil. Une fois le chiffrement mis en place, les personnes malintentionnées qui parviendraient à accéder à votre réseau auraient beaucoup de mal à en extraire des informations exploitables. L'intégrité des données est donc préservée en cas de brèche.

Pouvoir compter sur un temps de disponibilité ininterrompu revêt une importance capitale pour de nombreuses industries. Les événements imprévisibles, comme les catastrophes naturelles, constituent donc un risque direct pour les entreprises. Les documents papier sont particulièrement vulnérables dans de tels cas. L'utilisation d'un référentiel sécurisé et basé sur le cloud pour les documents numérisés apporte la flexibilité essentielle et nécessaire pour se protéger contre tous types d'accidents. Toutefois, plusieurs étapes de sécurité doivent être appliquées pour préserver au mieux ces données numériques.

## Chiffrement des données confidentielles

Pour protéger les informations, un chiffrement peut être appliqué aux données envoyées vers ou stockées sur le disque dur d'un MFP Ricoh. Des options intégrées appliquent un chiffrement complet aux fichiers imprimés et numérisés, via la clé PKI de l'utilisateur. Ce mécanisme protège le client des attaques par interception au sein de son environnement informatique.

Pour une sécurité renforcée, les données d'impression sont continuellement effacées par le système DOSS (Data Overwrite Security System, Système d'écrasement sécurisé des données) de Ricoh, qui sera abordé plus en détail dans la phase Destruction du cycle de vie des données.

## Protection du système d'exploitation et du BIOS

Les MFP Ricoh emploient un TPM (Trusted Platform Module, Module de plateforme de confiance), un module de sécurité matériel anti-piratage. Le TPM permet de chiffrer et de stocker de manière sécurisée les données cryptographiques. Ricoh utilise le TPM pour stocker la clé de chiffrement racine qui protège la clé de chiffrement des données du disque dur et le certificat numérique des MFP. De la même manière, les administrateurs peuvent initialiser l'appareil de façon sécurisée afin de valider l'authenticité du firmware du MFP avant d'en autoriser l'utilisation.

## Validation du firmware

La clé racine et les fonctions de chiffrement sont toujours contenues dans le TPM et ne peuvent pas être modifiées hors du pare-feu, évitant ainsi l'utilisation malintentionnée ou le piratage de nos produits. Ce processus fournit une validation de haut niveau du firmware du MFP et assure l'identification de l'appareil et la sécurité du disque dur. La sécurité est ainsi au cœur de la conception de nos produits.

## Gestion des mots de passe

Les appareils Ricoh peuvent être configurés avec plusieurs utilisateurs administrateurs, chacun avec des rôles et des mots de passe différents. Les mots de passe utilisateurs peuvent être configurés à distance à l'aide d'outils d'administration Web et vérifiés à intervalles réguliers. Cette séparation des fonctions est de fait une exigence présente dans de nombreuses réglementations d'entreprise.

## Restriction de l'accès utilisateur

Notre outil de gestion des utilisateurs permet aux administrateurs système de contrôler les droits d'accès des utilisateurs. Par exemple, l'administrateur peut définir des droits permettant à certains utilisateurs d'accéder au carnet d'adresses d'un MFP. Ce mécanisme permet de bloquer tout accès non autorisé aux informations personnelles stockées sur les appareils de l'entreprise.

## Verrouillage des utilisateurs

Lorsqu'un utilisateur saisit plusieurs fois un mot de passe de connexion incorrect, les MFP Ricoh peuvent déterminer si cette personne cherche à casser le mot de passe. Cette situation peut déclencher la fonction de verrouillage et ainsi bloquer l'utilisateur. L'utilisateur verrouillé ne peut pas s'authentifier, même s'il saisit ensuite un mot de passe correct. Le verrouillage ne peut être levé qu'après une certaine durée ou par un administrateur, repoussant ainsi de manière efficace les pirates informatiques.

# 3 DESTRUCTION

Tout bon système de cybersécurité se doit de proposer un mécanisme de suppression sécurisée des données. Il serait trop simple de penser que les responsabilités d'une entreprise prennent fin lorsque les données sortent de l'organisation. En effet, de nombreuses réglementations stipulent que la destruction des données est une procédure obligatoire pour éviter les risques potentiels de vol ou d'utilisation frauduleuse. Les obligations des entreprises concernant les données qu'elles détenaient ne se terminent jamais avant qu'elles ne soient en mesure de le prouver.

Les appareils professionnels en fin de vie ou renvoyés pour réparation constituent souvent un risque sous-estimé pour les informations commerciales. Ricoh propose un service certifié et contrôlable de suppression des données sur ces imprimantes en fin de vie. Cette suppression porte sur des éléments souvent négligés, comme les paramètres réseau, les données des utilisateurs, des disques durs ou même les autocollants figurant sur l'appareil. Tout manquement à cet égard induit des risques de divulgation involontaire de données confidentielles et personnelles. De plus, pour répondre aux exigences réglementaires, ce processus doit se produire tout au long du cycle de vie des appareils. Les entreprises sont ainsi certaines de garder le contrôle des données dont elles sont responsables.

## Écrasement des images : Système d'écrasement sécurisé des données (DOSS)

Les disques durs des MFP, pour fonctionner efficacement, stockent en mémoire des images latentes lors du traitement d'un document. Notre solution d'écrasement sécurisée des données garantit l'écrasement des données avant le début de l'impression suivante. Ainsi, si une personne malintentionnée parvient à accéder au disque dur, elle ne pourrait retrouver aucune trace des données générées par les impressions précédentes. Chez Ricoh, nous sommes fiers de proposer ce service de sécurité exceptionnel depuis plus de 20 ans.

## Service de nettoyage en fin de vie

Ricoh propose un service de nettoyage complet des données pour les MFP et imprimantes en fin de vie : tous les modules de mémoire et les ressources de stockage des appareils sont effacés définitivement, sans récupération possible, à l'aide de solutions de sécurité certifiées. Les services informatiques de Ricoh proposent également un service d'élimination des équipements, comprenant plusieurs niveaux de services certifiés de suppression des données.

## Remplacement des disques durs et stockage amovible

Ricoh propose également un service permettant aux clients de conserver leurs disques durs, en les remplaçant par un nouveau disque dur vierge lorsqu'ils renvoient leur équipement en fin de contrat. Les entreprises possèdent ainsi le contrôle total sur leur environnement de données.

# 4 SUPPORT

À mesure que les entreprises se développent, le nombre de connexions entre les appareils et les réseaux se multiplient. Les entreprises ont besoin de stratégies garantissant que la croissance de leur infrastructure n'entraîne aucun risque. Elles doivent prendre conscience des points faibles de leur système, et appliquer les mesures nécessaires pour contrer les attaques ciblées.

Une expertise en sécurité informatique spécialisée est souvent nécessaire pour analyser l'infrastructure des entreprises et en identifier les points faibles. De nombreuses entreprises ne peuvent pas disposer en permanence d'une équipe informatique dédiée. Les coûts et le manque d'efficacité d'une telle approche obligent souvent ces entreprises à agir de manière dangereuse.

Le service de support informatique Ricoh propose aux entreprises des services de configuration, de contrôle à distance et de gestion des transitions, afin de renforcer leurs processus de cybersécurité. Disposer d'une compréhension globale des risques métier est un élément primordial de la cybersécurité. Notre équipe de réponse aux incidents de sécurité (SIRT) communique à nos clients du monde entier des informations cruciales concernant les menaces, afin de permettre la mise en place instantanée de réponses efficaces et coordonnées.

## Évaluation de la sécurité des infrastructures

Streamline NX (SLNX), un outil de gestion des appareils Ricoh, a été conçu pour réaliser un audit de la stratégie de sécurité des entreprises. SLNX fournit une fonctionnalité que les responsables informatiques activent pour répartir les différents paramètres en fonction de la stratégie de l'entreprise, puis les analyser sous forme de rapports. SLNX peut également émettre des alertes lorsqu'un appareil n'est plus conforme à la stratégie de l'entreprise.

## Optimisation de la sécurité d'impression

Ricoh propose un service complet d'optimisation de la sécurité d'impression (PSO), ainsi que des services de conseil pour identifier les failles de sécurité du parc. Cet outil Web est doté d'un assistant graphique offrant une vue d'ensemble de l'état actuel du parc et permettant à Ricoh d'émettre des recommandations précises dans le but de réduire les risques.

## Équipe de réponse aux incidents de sécurité des produits (PSIRT)

La réponse active de Ricoh aux nouvelles menaces et le développement de contre-mesures efficaces s'effectue au sein de l'équipe PSIRT de Ricoh. L'équipe PSIRT Ricoh se charge d'apporter des réponses à ses clients et de développer les contre-mesures nécessaires en cas de menace. Il s'agit d'un programme permettant de s'assurer que tous nos produits (matériels et logiciels) soient continuellement mis à jour et protégés contre les menaces identifiées. Nous sommes ainsi toujours en mesure d'assurer un niveau de service élevé, à l'échelle mondiale, et de réduire les vulnérabilités détectées sur les produits Ricoh.

## Documentation connexe

La préparation et la formation sont deux pans essentiels dans la mise en place d'un système sécurisé. La documentation de support, les guides utilisateur, les livres blancs relatifs à la sécurité et la formation constituent autant d'éléments à fournir au client. Comme pour de nombreux éléments en matière de cybersécurité, conformité et documentation jouent un rôle clé afin de sécuriser toute une entreprise.

# RICOH S'OCCUPE DE TOUT

Ricoh fournit aujourd'hui les meilleures solutions de sécurité du marché dans le secteur de l'impression et de l'informatique. Cette position unique s'explique par notre excellente compréhension de l'évolution des marchés et l'adaptation immédiate de notre offre à ces variations. Nos solutions sont conçues pour protéger toutes les informations, sur l'ensemble de leur cycle de vie, en respectant les quatre domaines de sécurité analysés dans ce rapport.

Notre équipe de spécialistes se charge d'analyser les besoins du marché, comprenant les exigences spécifiques à chaque secteur, afin de créer des solutions ou d'adapter les solutions existantes.

Nous nous engageons également à développer notre capacité interne à concevoir et déployer des solutions privilégiant la sécurité.
Pour y parvenir, nous avons mis en place des équipes spécialisées au sein de notre organisation de développement des services, qui s'attachent à créer de nouveaux services de gouvernance, de gestion des risques, de conformité et de cybersécurité.

### Autorisation et authentification des utilisateurs

- Impression verrouillée
- Logiciels d'authentification intégrés en standard
- Authentification utilisateur / restriction d'accès
- Authentification unique
- Plusieurs rôles d'administrateur
- Protection par mot de passe des PDF (mot de passe pour documents numérisés)
- Protection contre la copie non autorisée
- Contrôle d'accès par plages d'adresses IP
- Gestion sécurisée de l'impression et du parc
- Prise en charge PKI (Infrastructure à clés publiques) / SmartCard
- Impression sécurisée (print2me / impression verrouillée)

### Protection contre les programmes malveillants

- Serveurs
- Exposition réduite aux logiciels malveillants
- Panneau de commande intelligent – version renforcée d'Android
- Système d'exploitation Ricoh (langage de contrôle appareil) pour MFP
- 3 niveaux de sécurité : signature numérique, téléchargement via l'outil Ricoh, écriture dans un langage de contrôle spécifique

### Élimination des disques durs

- Élimination des disques durs, écrasement des images
- Service de nettoyage complet des données
- Service en fin de vie : destruction des données dans les modules de mémoire et ressources de stockage

### Gestion des appareils

- Quotas / limite de compte
- DMNX : audit de sécurité unique, gestion des mots de passe, contrôles, alertes

### Protection du système d'exploitation et du BIOS

- Initialisation sécurisée via TPM

### Écrasement des images et supports de stockages amovibles

- Système d'écrasement sécurisé des disques (DOSS)
- Disque dur amovible

### Chiffrement des données

- Chiffrement du disque dur via TPM
- Clés de chiffrement via TPM
- Chiffrement intégral des fichiers d'impression/ numérisation à l'aide d'une clé PKI
- Disques durs certifiés FIPS (normes de traitement des informations fédérales)
- Chiffrement intégral de l'impression
- Chiffrement intégral de la numérisation

### Mises à jour firmware et gestion des mots de passe

- Audit à distance des mots de passe
- Fonction de verrouillage des utilisateurs
- Validation du firmware via TPM

### Conformité avec les normes industrielles

- Certification ISO 27001
- Certification IEEE 2600.2 pour certains produits
- Certification ISO 15408 pour certains produits
- Formation et documentation de sécurité

# PLUSIEURS NIVEAUX DE SÉCURITÉ POUR LES APPAREILS RICOH

Le rôle du fournisseur de MFP a énormément évolué. Il ne s'agit plus simplement de vendre du matériel, mais également de proposer des solutions de gestion des données. Nos MFP possèdent de nombreuses fonctionnalités, notamment la capture d'informations à partir de sources multiples, la classification des données capturées et l'intégration des flux de production, ou encore le stockage sécurisé et l'analyse des données. En réponse aux contraintes soulevées par les réglementations et les exigences de conservation, ainsi qu'aux menaces internes et externes mettant en danger les données (perte, destruction, piratage), nous avons choisi une approche de sécurité sur plusieurs niveaux, pour vous assurer que votre MFP et les systèmes qu'il relie vous offrent la meilleure protection possible.

## 1. L'appareil

L'appareil est au cœur de tout. Que ce soit lors de sa conception, sa fabrication ou sa mise en place, la sécurité est toujours notre priorité. Le système d'exploitation Ricoh n'est en rien concerné par les vulnérabilités des systèmes d'exploitation grand public et nos appareils sont certifiés IEEE2600.2 en standard. Le chiffrement du disque dur et la fonction d'écrasement assurent la confidentialité des données traitées.

## 2. Le panneau de commande intelligent (Smart Operation Panel) constitue l'interface utilisateur

À la façon d'un MFP, le panneau de commande intelligent utilise un système d'exploitation propre à Ricoh. Aucun composant superflu n'est installé et l'accès racine n'est pas disponible. Ricoh a travaillé dur afin de s'assurer que le panneau de commande n'affaiblisse en rien la sécurité de l'appareil.

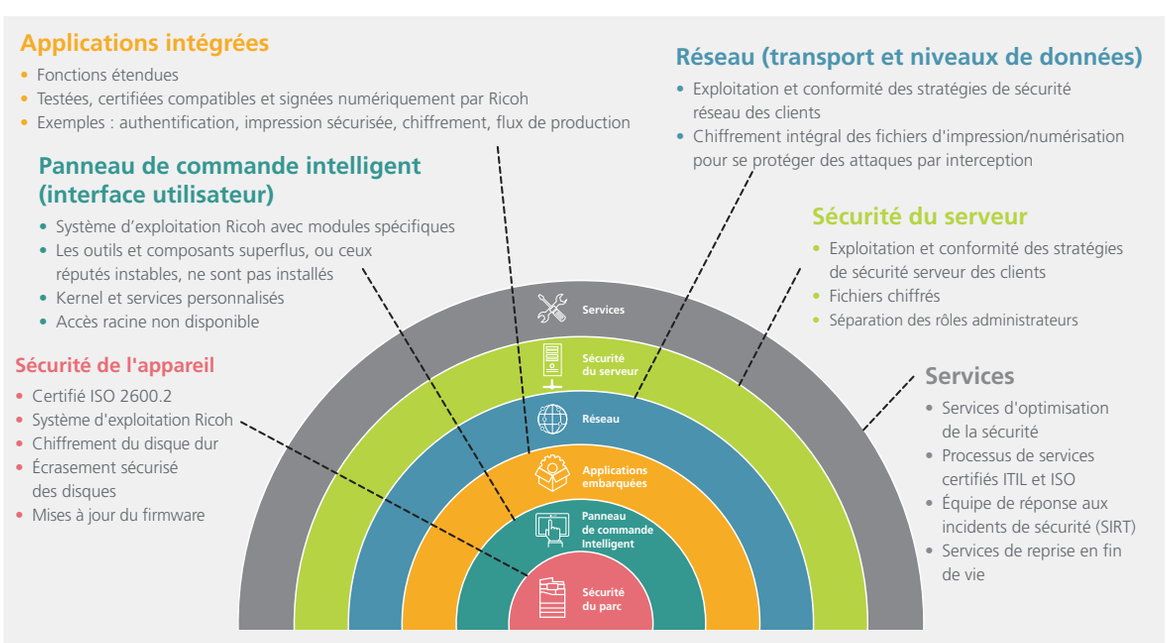
## 3. Applications intelligentes

Elles peuvent être intégrées au panneau de commande pour apporter des fonctions supplémentaires à l'utilisateur, notamment la capture des données et les flux de production. Certaines applications fournissent des fonctions de sécurité essentielles. Parmi elles, on retrouve l'impression sécurisée, l'accès par carte et le chiffrement. Les applications sont développées par Ricoh ou des membres du programme de développement Ricoh et toutes les applications doivent réussir notre test de compatibilité et être signées numériquement avant de pouvoir être installées sur le panneau de commande.

## 4. Réseaux et serveurs

Indépendamment du responsable de l'infrastructure, nous garantissons que nos produits et services sont conformes aux stratégies de sécurité réseau de votre entreprise. Le chiffrement intégral des fichiers d'impression et de numérisation, le chiffrement des données sur les serveurs et la séparation des fonctions d'administration sont des techniques utilisées pour se protéger des attaques par interception.

Une gamme complète de services de sécurité se retrouve sur l'ensemble de notre offre. Parmi eux, des services de gestion et de conseil pour aider les clients à surveiller, optimiser et gérer la sécurité de leurs documents et informations. Nous disposons également de nombreux services de fin de vie supprimant entièrement les données présentes dans la mémoire RAM et les disques durs des appareils mis au rebut par les clients.



# PROTÉGER VOTRE ENVIRONNEMENT DE TRAVAIL

Nos clients possèdent de nombreuses exigences en matière de sécurité, conscients que l'augmentation des volumes des données multiplie les vulnérabilités, attaques et sanctions potentielles. Pour assurer la confidentialité, la sécurité et l'inviolabilité des données, il est nécessaire de déployer des efforts en continu. À titre d'exemple, Ricoh repoussent environ 8 milliards d'attaques mensuelles à l'encontre de pare-feu. Il existe des dizaines de milliers de réglementations relatives aux données aux niveaux national et international, et les entreprises doivent être en mesure de prouver continuellement leur conformité avec chacune d'elles. Les organisations de toutes tailles recherchent des partenaires de confiance, capables de leur fournir des produits et des services sécurisés pour l'ensemble de leurs environnements de travail.

Ricoh a développé une large gamme de solutions permettant de réduire les différents risques encourus par les entreprises. Avec la rapide évolution des menaces liées à la sécurité des données, Ricoh propose à ses clients des programmes sur mesure pour améliorer le développement de ses services.

Nos centres de conseil clients constituent un atout majeur. Nous les utilisons pour mieux comprendre les tendances, les vecteurs et les priorités de nos clients. Des conférences consultatives sur les technologies apportent aux décisionnaires des informations cruciales. Les équipes d'ingénierie et de R&D Ricoh utilisent ces conférences pour recueillir l'opinion de ses clients sur différentes idées, concepts et prototypes. Enfin, Ricoh collabore avec des clients particuliers afin de développer de nouvelles fonctions de sécurité avancées pour les clients des marchés généraux et verticaux. Cette approche orientée clients nous aide à valider le développement de nos produits et permet à nos clients de profiter d'un réseau mondial de services et d'assistance.

L'espace de travail numérique moderne doit se montrer aussi dynamique que les menaces auxquelles il est confronté et aussi flexible que les pratiques de travail qui la composent. C'est pourquoi nous pensons que la cybersécurité doit opérer en toute transparence sur l'ensemble des technologies que nos clients choisissent pour leur environnement de travail. Notre engagement envers les certifications ISO 27001 et IEEE 2600 sur l'ensemble de nos produits, ainsi que notre système d'exploitation Ricoh, sont la preuve que nous avons mis en place d'excellents systèmes de contrôle, eux-mêmes issus des meilleures pratiques et correspondant au mieux à la structure et au développement de votre activité.

Les menaces de sécurité, les exigences législatives et la complexité des normes industrielles constituent autant de risques potentiels capables de nuire à la réputation ou à la capacité financière de votre entreprise. Il est aujourd'hui temps de travailler avec un partenaire de confiance, capable de vous aider à sécuriser vos actifs les plus vulnérables, afin de protéger et d'encourager vos ambitions.

RICOH
imagine. change.

www.ricoh.fr