Paysage de la sécurité de l’impression, 2024

Atténuer l’impact de l’infrastructure d’impression en tant que vecteur de menaces

Tendances à l’égard de la sécurité de l’impression aux États-Unis et en Europe
Extrait du rapport d’un fournisseur : Ricoh

Juillet 2024

QUOCIRCA

Sommaire exécutif

L'essor du travail hybride a brouillé les limites de la sécurité des infrastructures d'impression traditionnelle. Les réseaux publics et les environnements peu contrôlés sont désormais répandus, et ils exigent l'adoption d'une approche plus robuste en matière de sécurité de l'impression. De plus, la progression de l'intelligence artificielle (IA) impose de nouveaux défis de sécurité, notamment en rehaussant le risque que les appareils vulnérables deviennent des cibles faciles et qu'ils soient compromis, en raison de la faiblesse des protocoles de sécurité. Les fabricants d'appareils d'impression et les partenaires au sein du réseau doivent s'adapter à cette nouvelle réalité en offrant des solutions de sécurité sophistiquée qui s'intègrent aisément aux infrastructures TI existantes. Ce changement engendre d'importantes occasions. En assumant le rôle de conseillers de confiance, les membres du réseau de l'impression peuvent orienter les organisations vers des solutions complètes qui abordent la sécurité des appareils, des données et des documents. Il est possible de protéger son entreprise, mais aussi d'acquérir de nouvelles sources de revenus au sein du secteur de l'impression en s'assurant que l'infrastructure d'impression soit un élément essentiel de la sécurité de l'information dans son ensemble.

L'étude du paysage de la sécurité de l'impression de 2024 de Quocirca révèle que les organisations sont continuellement confrontées à des défis liés à la sécurité de leur infrastructure d'impression. Les imprimantes qui se trouvent chez les employés représentent l'une des principales préoccupations liées à la sécurité pour 33 % des organisations. Cela témoigne de la difficulté de contrôler l'impression à la maison, à la fois au niveau de l'appareil et à celui des documents, puisque les documents sont exposés à des utilisateurs non autorisés. Malgré la sensibilisation grandissante à l'égard des faiblesses de la sécurité de l'impression, les organisations peinent à passer à l'action.

Les brèches de données entraînées par l'impression demeurent une menace importante. En effet, 67 % des participants à l'étude ont admis avoir subi un incident ayant entraîné une perte de données dans la dernière année (comparativement à 61 % en 2023). Au sein des organisations du marché intermédiaire, ce chiffre atteint 74 %. Cette réalité affaiblit la confiance que les organisations, en particulier les petites et les moyennes entreprises (PME), portent à l'égard de la sécurité globale de leur infrastructure d'impression.

On note surtout que les organisations qui possèdent un parc standard sont moins susceptibles d'être victime d'une ou de plusieurs pertes de données (59 %) que celles qui ont un parc formé d'appareils de différents fournisseurs (70 %). Ces données reflètent le défi que représente le maintien de la sécurité des parcs mixtes, en comparaison à l'utilisation de plateformes de sécurité exclusives intégrées dans les parcs standard. Ces solutions de gestion de l'impression de tierce partie peuvent contribuer à rehausser la sécurité de l'impression au sein des parcs mixtes. Toutefois, la charge de travail supplémentaire qu'impose la gestion d'un parc mixte sur les équipes TI ainsi que les difficultés et les frais liés à l'approvisionnement de multiples pilotes, de multiples systèmes d'intégration et de multiples systèmes de surveillance et de production de rapports, rendent les parcs mixtes moins attrayants que les parcs standard.

Cette plus récente étude révèle une inquiétante lacune à l'égard de la perception de la sécurité de l'impression chez les dirigeants principaux de l'information (DPI) et des officiers principaux de la sécurité de l'information (OPSI). Bien que ces deux types de dirigeants prévoient une hausse de leurs dépenses en matière de sécurité (77 % des DPI et 78 % des OPSI), les OPSI sont beaucoup moins confiants à l'égard de leurs mesures de sécurité de l'impression actuelles que les DPI. Cet écart se creuse encore plus, puisque les OPSI sont plus nombreux que les DPI (41 % contre 34 %) à trouver que les défis liés à la gestion de la sécurité de l'impression sont complexes. Il est intéressant de noter que les DPI sont plus préoccupés par les imprimantes non sécurisées dans les domiciles des employés que les OPSI (52 % contre 32 %). Cette donnée illustre un possible angle mort.

Cette vision fracturée entraîne un important obstacle. Il est crucial d'harmoniser les perspectives des DPI et des OPSI à l'égard de la sécurité pour favoriser la solidité de la sécurité de l'information. Combler ce fossé n'est plus une option, il s'agit d'une nécessité. Heureusement, les chefs de file du domaine de la sécurité de l'impression, définis selon l'index de maturité à l'égard de la sécurité de l'impression de Quocirca, s'affairent à limiter les risques. En effet, les chefs de file sont des organisations qui ont mis en place davantage de mesures de sécurité que les « aspirants » et les « retardataires », définis par Quocirca. Les chefs de file signalent moins de perte de données et ont une plus grande confiance en la sécurité de leur infrastructure d'impression.

Cette réalité offre aux fournisseurs l'occasion de se positionner à titre de partenaires stratégiques, mais aussi de solidifier leurs propositions liées à la sécurité pour aider les clients à limiter les risques entraînés par l'impression non sécuritaire à la fois dans les bureaux et dans les domiciles. En identifiant et en adoptant les pratiques exemplaires exploitées par les chefs de file, les fournisseurs de l'écosystème d'impression peuvent jouer un rôle crucial dans l'amélioration de la posture de sécurité des « aspirants » et des « retardataires ».

Principales conclusions

- **Les fabricants d'imprimantes et d'appareils multifonctions continuent d'améliorer et d'approfondir leur approche de sécurité.** L'entreprise HP a obtenu une meilleure position, grâce à l'innovation continue dont elle fait preuve au sein de son portefeuille, à l'établissement d'une architecture d'impression à vérification systématique ainsi qu'à la meilleure harmonisation de sa solution HP Wolf Security dans l'ensemble de son offre liée à l'impression et aux ordinateurs. L'entreprise Xerox offre des mesures de sécurité complète pour l'ensemble de son équipement et de ses solutions, surtout au sein de son portefeuille de sécurité des flux de travaux et du contenu. L'offre de sécurité de l'organisation Canon est globalement uniforme et elle est soutenue par sa plateforme mature uniFLOW. Les autres fournisseurs de la catégorie des chefs de file sont Lexmark, qui adopte une approche mature de sécurité par défaut dans tout son équipement, Ricoh, qui se démarque grâce à ses services de cybersécurité, ainsi que Konica Minolta, qui offre la gamme sécuritaire bizHUB. L'organisation Sharp a réalisé d'importants investissements en matière de sécurité dans la dernière année, notamment en adoptant une approche de sécurité à plusieurs niveaux et en s'associant à Bitdefender. Les importants joueurs comprennent Epson, Brother, Kyocera et Toshiba.
- **La sécurité de l'impression occupe une place plus importante qu'en 2023.** Si les réseaux publics sont considérés comme le plus important risque en matière de sécurité des TI (35 %), les risques associés aux imprimantes situées dans les domiciles des employés les suivent de près (33 % comparativement à 21 % en 2023). Cette statistique peut traduire la croissance de « l'impression de l'ombre » entraînée par le télétravail et l'utilisation d'imprimantes en dehors du contrôle des entreprises. L'impression au bureau occupe la troisième position (29 %), alors qu'elle occupait la huitième position en 2023 (20 %).
- **Les organisations abordent de mieux en mieux les défis liés à la sécurité de l'impression.** Dans l'ensemble 30 % des organisations ont admis qu'il est très difficile ou assez difficile de maintenir le rythme de la demande à l'égard de la sécurité de l'impression, comparativement à 39 % en 2023. Le plus important défi de la sécurité de l'impression est d'empêcher l'impression de documents confidentiels (28 % et 34 % aux États-Unis). On note que les organisations dont l'environnement d'impression fait appel à plusieurs fournisseurs sont plus susceptibles de voir cet enjeu comme un défi (30 %) que celles qui font appel à un parc standard.
- **Dans les 12 derniers mois, 67 % des organisations ont été victime de pertes de données causées par des pratiques d'impression non sécuritaires (comparativement à 61 % en 2023).** Comme c'était le cas en 2023, les organisations du marché intermédiaire sont plus susceptibles d'être victimes d'une ou de plusieurs pertes de données (70 %) que les grandes entreprises (63 %). Les secteurs des entreprises et des services professionnels subissent le plus de brèches (71 %). Le secteur public se classe au second rang (70 %). En moyenne, une brèche de données liée à l'impression coûte plus de 1 million de livres, alors qu'elle coûtait 743 000 livres en 2023.
- **L'index de maturité de la sécurité de l'impression établi par Quocirca révèle que seuls 20 % des organisations sont classées à titre de chef de file.** Les chefs de file sont les organisations qui ont établi au moins 6 mesures de sécurité. Le pourcentage de chefs de file grimpe à 25 % aux États-Unis, et est réduit à 14 % en France. La France compte également le plus grand nombre de « retardataires » (23 %). Les chefs de file investissent davantage dans la sécurité de l'impression, sont moins souvent victimes de pertes de données et ont une plus grande confiance à l'égard de la sécurité de leur environnement d'impression.
- **L'intelligence artificielle (IA) engendre de nouvelles préoccupations en matière de risque de sécurité.** Dans l'ensemble 62 % des organisations ont admis être extrêmement ou modérément préoccupées par les risques de sécurité qu'entraîne l'IA. Dans l'ensemble, 83 % des répondants ont admis qu'il est très important (34 %) ou assez important (49 %) que les fournisseurs utilisent l'IA ou l'apprentissage automatique pour repérer les menaces liées à la sécurité de l'impression. Ces révélations offrent aux fournisseurs d'impression l'occasion de créer et de fournir des solutions novatrices qui font appel à l'IA ou à l'apprentissage automatique pour rehausser la sécurité de l'impression, qu'elles impliquent la sécurité de l'IA pour les appareils ou la surveillance à distance basée sur l'IA.
- **Plus du tiers des entreprises (36 %) sont très satisfaites par les capacités de leur fournisseur d'impression en matière de sécurité (comparativement à 32 % en 2023).** Cette donnée grimpe à 47 % chez les organisations américaines, mais passe à 19 % en Allemagne. Les organisations utilisant des appareils multifonctions sont beaucoup plus satisfaites (43 % ont indiqué être très satisfaites) que celles qui n'en utilisent pas ou qui ne prévoient pas de le faire (23 %).

Table des matières

Recommandations pour les acheteurs

Puisque de plus en plus d'entreprises délaissent les simples appareils d'impression pour adopter des appareils multifonctions intelligents, qui comportent de multiples points d'attaque, l'impression devient un maillon de plus en plus faible au sein de la sécurité des TI. Les risques que ces appareils entraînent peuvent être limités par l'adoption de diverses mesures basées sur la posture de sécurité de l'organisation.

Les acheteurs devraient envisager de poser les gestes suivants :

- **Commencer par mener une analyse approfondie des risques et de la sécurité de l'impression.** Malgré la plus grande sensibilisation à l'égard des enjeux de sécurité de l'impression, les organisations en font peu pour combler les lacunes. Les organisations qui ne possèdent pas les compétences nécessaires à l'interne doivent faire appel à des fournisseurs qui peuvent réaliser des évaluations approfondies de leur environnement d'impression. Les vérifications de sécurité peuvent révéler des vulnérabilités à l'égard de la sécurité des appareils et des documents, en plus de permettre l'élaboration de stratégies pour les gérer. Chez les organisations dotées d'un parc mixte, une telle vérification peut également encourager le passage à un parc plus standard, qui permet l'adoption d'une approche de sécurité plus uniforme et plus complète.
- **Traiter la sécurité de l'impression comme une priorité stratégique, mais pas de manière isolée.** La sécurité de l'impression et des TI doit être intégrée et être traitée comme une importante priorité d'affaires. L'importance de la sécurité des infrastructures d'impression doit être transmise aux DPI et aux OPSI, afin qu'ils s'entendent sur les risques que courent les affaires et les plateformes des TI. Il convient de se concentrer sur les mesures qui peuvent être prises pour limiter les risques de l'impression non sécurisée ainsi que pour surveiller et gérer le flux d'information engendré par le recours croissant aux flux de travaux numériques.
- **Évaluer la sécurité de l'intelligence artificielle.** Les fournisseurs devraient chercher à adopter et à intégrer l'IA à la fois pour les appareils et pour les logiciels dans le but d'offrir d'importants avantages de sécurité. Les analyses des données des appareils en temps réel peuvent contribuer à limiter l'utilisation de ces appareils à titre de vecteurs d'attaques. Toutefois, il peut être difficile de maintenir les capacités de l'IA dans un marché évoluant si rapidement. Le recours à l'IA avec les logiciels est une bonne façon d'obtenir davantage de souplesse. Dans l'ensemble, avoir recours à une approche à plusieurs volets, à la fois au niveau de l'équipement et des logiciels, permet d'obtenir le plus de capacités.
- **Inclure les télétravailleurs à l'environnement d'impression géré.** Les imprimantes conçues pour le grand public ne respectent pas toujours les normes de sécurité des entreprises. Toutefois, les appareils multifonctions peuvent imposer des mesures de contrôle à ce type d'imprimantes dans le but de garantir la sécurité de l'information et du contenu. Des directives de sécurité concernant le droit d'utiliser ces imprimantes et la façon de le faire doivent être rédigées et imposées.
- **Bâtir une architecture de sécurité d'impression cohérente.** Les solutions de sécurité fragmentaires offrent rarement une sécurité constante et robuste, en particulier dans les environnements de travail hybride. Pensez à faire appel à une plateforme de sécurité intégrée qui offre des capacités comme l'impression « pull », la surveillance à distance ainsi que la production de rapports sur l'ensemble du parc. Prolonger la sécurité de l'impression protégeant aussi le contenu et les flux de travaux grâce à des outils de prévention de la perte de données et d'outils de sécurité du contenu au niveau des applications. Évaluez attentivement les promesses de vérification systématique des fournisseurs et veillez à ce qu'elle puisse être intégrée aux plateformes d'authentification multifacteur utilisées au sein de votre organisation. Vérifiez si les solutions de gestion de la sécurité de l'impression peuvent être exploitées dans un réseau microsegmenté.
- **Créer, normaliser et réviser sans cesse les procédures pour répondre aux incidents liés à la sécurité de l'impression.** Les organisations doivent s'assurer d'être prêtes à subir d'inévitables incidents de sécurité. Elles doivent mettre en place les procédures nécessaires pour réagir aux conséquences techniques et juridiques ainsi qu'aux atteintes à la réputation entraînées par de tels incidents. Pour ce faire, les membres de l'organisation doivent travailler ensemble pour créer un ensemble global de politiques.
- **Assurer la continuité de la surveillance, des analyses et de la production de rapports.** Lorsque la surveillance et la production de rapports comportent des lacunes, les brèches peuvent passer inaperçues. Ces brèches ont un impact à plus long terme et elles entraînent des coûts plus importants que celles qui sont repérées et traitées rapidement. Assurez-vous que les données d'impression soient intégrées aux données des appareils de sécurité existants, comme les appareils de gestion de l'information et des événements de sécurité (GIES), et qu'elles soient analysées pour démontrer les événements passés et présents, mais aussi les événements qui pourraient se produire dans le futur. Veillez à ce que ces systèmes couvrent le plus possible la plateforme globale, puis utilisez les renseignements recueillis pour combler, en continu, les lacunes de sécurité au sein de votre organisation.

Profil de fournisseur : Ricoh

Opinion de Quocirca

Quocirca a classé Ricoh parmi les chefs de file dans son évaluation du marché de la sécurité de l'impression de 2024. Ricoh offre un vaste portefeuille de produits et de services axés sur la sécurité, notamment la sécurité des appareils, des données et des documents. Ricoh ne se contente pas d'intégrer des fonctionnalités de sécurité à son équipement, l'entreprise a également développé une grande expertise en cybersécurité. En effet, selon les différentes régions, Ricoh offre des services de cybersécurité personnalisés qui comprennent des analyses des risques et de la préparation et qui aident les clients à repérer, à surveiller et à répondre aux incidents de sécurité.

Approche de sécurité à multiples niveaux

Ricoh fait appel à des fonctionnalités intégrées aux appareils ainsi qu'à une vaste gamme de solutions et de services pour s'attaquer aux trois principales facettes de l'infrastructure de documents et d'impression : la sécurité des produits et des applications, la sécurité de l'infrastructure ainsi que la conformité aux normes de l'industrie, comme les Critères communs, les normes du *National Institute of Standards and Technology* (NIST) et la norme FIPS 140-2. Ricoh a rehaussé la sécurité de ses solutions et de ses services en ayant recours au chiffrement complet (avec ICP), aux modules TPM2.0 et TLS1.3, à l'algorithme de chiffrement AES 256 ainsi qu'à de robustes normes de chiffrement.

Pour cette organisation, les principes de sécurité à vérification systématique sont également une priorité. Ses solutions de gestion des documents et de l'impression comprennent des fonctionnalités visant notamment l'authentification fiable, l'application des politiques de sécurités, la microsegmentation, l'automatisation, la classification des données ainsi que la protection. Cette approche exhaustive garantit que les clients profitent d'une stratégie de défense robuste.

Surveillance des appareils en temps réel

Au début de l'année 2024, Ricoh USA a lancé le centre de commande IDO (Internet des objets), une plateforme tout-en-un indépendante qui permet la détection et la résolution en temps réel des problèmes ainsi que l'extraction de renseignements exploitables depuis les appareils connectés. Les fonctionnalités et les capacités clés incluent la surveillance de l'état des appareils et la production de rapports à son égard ainsi que la configuration et le contrôle à distance des appareils.

Vaste offre de services TI

L'offre de Ricoh comprend une vaste gamme de solutions et de services TI, notamment des pare-feux, des tests d'intrusion et des solutions de gestion des identités, qui sont conçus pour simplifier et sécuriser la numérisation. L'entreprise offre également des services gérés et des services de consultation qui complètent les niveaux de protection de ses appareils et de ses solutions dans le but d'optimiser la sécurité des documents, des données, des appareils ainsi que de l'information. À titre d'exemple, au Royaume-Uni, les services de gestion de la cybersécurité de Ricoh comprennent des services d'évaluation de sécurité non liée aux fournisseurs, de vérification de la conformité, de vérification des rançongiciels ainsi que de test de pénétration pour permettre aux clients de comprendre et de gérer leurs vulnérabilités en matière de sécurité. Aux États-Unis, Ricoh offre également des services de gestion de la sécurité, qui aident les clients à surveiller les menaces de sécurité, à se protéger contre elles ainsi qu'à y répondre.

Dans les trois dernières années, Ricoh a fait l'acquisition de 20 entreprises offrant des services TI et des services de cybersécurité. Ces acquisitions lui ont permis de grandement rehausser son expertise à l'égard de la cybersécurité et de la sécurité des données. Ces facteurs, combinés à de solides partenariats avec des leaders du secteur comme CISCO, BullWall, Microsoft, Trend Micro, VEEAM, Carbonite et SentinelOne, placent l'entreprise dans une excellente position pour répondre aux divers besoins du marché.

Centres d'excellence

Ricoh a également créé davantage de centres d'excellence en Europe, au Moyen-Orient et en Afrique (EMEA). Les équipes de ces centres créent de nouvelles technologies liées notamment à l'IDO, à la cybersécurité et aux chaînes de blocs. De plus, la capacité d'intelligence artificielle pour les opérations informatiques (*AIOps*) de la protection continue des données, qui peut repérer les cybermenaces et y répondre, qu'elles touchent un seul appareil ou tout le réseau, et qui comprend des capacités avancées de sécurité, comme les empreintes digitales des appareils et la chasse aux menaces, permet à l'entreprise de se démarquer.

Aux États-Unis, Ricoh a préparé et formé ses équipes de l'ingénierie et du développement de logiciels à adopter les pratiques de la méthodologie *DevSecOps*, et s'assure qu'elles la respectent, dans le but de rehausser la collaboration, d'accélérer la création de logiciels sécurisés et d'uniformiser les pratiques de programmation sécuritaire pour améliorer la qualité des logiciels, pour accélérer leur livraison et pour réduire les coûts connexes.

Ricoh est un partenaire de choix pour les organisations qui souhaitent protéger l'information tout au long du cycle de vie des documents, ainsi que pour celles qui cherchent à s'associer à un seul fournisseur qui peut gérer la sécurité à l'échelle de l'infrastructure TI et de l'infrastructure d'impression. Puisque l'offre de Ricoh est quelque peu fragmentée selon les régions et les réseaux, les organisations devraient évaluer les services de cybersécurité et de sécurité de l'impression offerts par Ricoh dans leur région précise.

Offres de sécurité

Sécurité robuste de l'équipement

Les appareils de Ricoh sont conçus et fabriqués pour comprendre une protection complète ainsi que les plus récentes fonctionnalités de sécurité, comme un système amélioré de contrôle des comptes privilégiés, le plus récent protocole de sécurité de la couche de transport (TLS1.3), la compatibilité avec la plus récente norme relative aux puces de sécurité TPM (TPM2.0), l'authentification multifacteur ainsi que l'intégration aux solutions d'identité de multiples fournisseurs.

Solutions nuagicielles sécuritaires

Les solutions exclusives de Ricoh et les offres de ses partenaires permettent aux clients de profiter du caractère agile et novateur de la technologie du nuage, tout en maintenant la sécurité robuste de leur environnement d'impression et de documents. De plus, Ricoh offre des options d'acheminement sécuritaire des impressions, notamment l'impression directe hors ligne, l'impression sécuritaire en nuage, l'impression sécuritaire sur PC ainsi que l'impression périphérique comprenant une passerelle d'intégration, qui rehaussent la sécurité et la souplesse de la gestion de l'impression.

Analyses au moyen de l'IA et de l'apprentissage automatique dans le centre de commande IDO de Ricoh

Ce service offre la surveillance des appareils, la surveillance autonome, des analyses du trafic de donnée, des analyses au moyen de l'IA et de l'apprentissage automatique (analyse prédictive et détection des anomalies) comprenant la résolution automatique, la surveillance complète de la sécurité, la vérification automatisée de la conformité ainsi que le suivi des changements.

Vulnérabilités de la sécurité de l'impression et résolution

Ricoh a une offre, indépendante des fournisseurs, qui aborde les vulnérabilités de la sécurité de l'impression et qui les résout. Ses spécialistes de la sécurité aident les clients à établir une stratégie de sécurité complète qui est analysée, évaluée et testée plusieurs fois avant qu'une catastrophe ne survienne. Par exemple, les services de sécurité de l'impression de Ricoh sont offerts par des ressources dévouées et hautement formées plutôt que par des organisations offrant des services partagés. Son approche, fondée sur les meilleures pratiques de gouvernance, de gestion du risque et de conformité, repère rapidement les vulnérabilités pouvant se solder par des infractions à la sécurité, les vides pouvant entraîner des cyberattaques et les autres angles d'exposition de la technologie des clients à l'interne avant que ces éléments n'affectent leur entreprise.

Services de sécurité

Les services de sécurité de Ricoh comprennent la formation et la sensibilisation des employés, la sécurité du nuage, le filtrage de sécurité, la protection des terminaux, la détection des brèches et la réponse à leur égard ainsi que des solutions de sauvegarde.

La solution @Remote favorise la connexion sécuritaire des appareils pour permettre l'affichage de l'état des appareils et des alertes de service, qui sert à la surveillance des appareils dans le cadre de la prestation des services gérés de Ricoh. Les services de vérification des vulnérabilités de Ricoh analysent les appareils connectés à la solution @Remote et les solutions installées sur les serveurs pour fournir des rapports détaillés à l'égard des risques ainsi que pour prévenir les risques au sein de l'environnement. Ricoh fait également appel à des outils de gestion complète du parc, comme Streamline NX et CloudStream, pour surveiller les appareils et produire des rapports à leur sujet, ce qui inclut des services comme les mises à jour automatiques, la surveillance et la production avancée de rapports, l'application des politiques ainsi que la résolution.

Forces et occasions

Forces

- **Portée mondiale.** L'équipe des services mondiaux de Ricoh offre des solutions complètes, uniformes et standard dans environ 200 pays et territoires partout dans le monde.
- **Offres complètes axées sur la sécurité dans l'ensemble du portefeuille de solutions et d'équipement.** Ricoh détient une grande expérience en matière de gestion et d'optimisation des parcs mixtes au sein des organisations où les exigences de

sécurité sont rigoureuses. Ses capacités en matière de services TI et de services professionnels lui permettent d'offrir des services personnalisés et robustes qui sont conçus selon les divers besoins de sécurité des clients.

- **Offres de services TI matures et expertise favorisée par des acquisitions.** Les acquisitions de Ricoh lui ont permis d'approfondir son expertise en matière de cybersécurité, ce qui lui donne la possibilité de se démarquer de ses concurrents sur le marché.

Occasion

- **Création d'une offre de services de sécurité cohérente.** Actuellement, les offres de Ricoh sont fragmentées au sein de différents groupes, ce qui entraîne des incohérences dans son approche régionale. Partout dans le monde, les clients devraient évaluer les capacités à l'échelle locale, puisqu'elles diffèrent selon les régions.
- **Création d'un programme solide de sécurité axé sur les canaux.** Ricoh se fie à son réseau solide pour offrir des produits et des services aux petites et aux moyennes entreprises (PME). Offrir son soutien aux partenaires du réseau en leur offrant des outils de sécurité axés sur les TI, comme les audits et les évaluations, permettrait à ces partenaires de grandement se démarquer sur le marché.

À propos de Quocirca

Quocirca est une société de recherche et d'étude de marché se spécialisant dans la convergence de l'impression et des technologies numériques dans l'avenir des milieux de travail.

Depuis 2006, Quocirca joue un rôle important dans les conseils offerts aux clients sur les évolutions majeures du marché. Ses recherches et sa consultation occupent une place importante au sein du marché des solutions et des services d'impression évoluant rapidement. Les clients cherchant de nouvelles stratégies pour aborder les technologies perturbatrices font confiance à cette société.

La société Quocirca est une pionnière de la recherche dans bon nombre de secteurs émergents du marché. Il y a plus de 10 ans, elle était la première à analyser le paysage du marché mondial des services de gestion de l'impression. Elle a ensuite mené la première évaluation de la concurrence du marché de la sécurité de l'impression à l'échelle mondiale. Plus récemment, Quocirca a solidifié son approche unique au sein du marché en publiant la première étude portant sur l'avenir intelligent et connecté de l'impression dans les milieux de travail numériques. Cette étude (*Global Print 2025 Study*) fournit des renseignements hors pair sur l'impact de la perturbation numérique du point de vue des dirigeants du secteur, mais aussi de celui du consommateur.

Pour obtenir plus d'information, rendez-vous sur la page suivante : www.quocirca.com.

Droits d'utilisation

Toute citation d'une information contenue dans ce rapport doit obtenir une autorisation. Veuillez consulter la politique de citation de Quocirca pour connaître tous les détails.

****Ce document est une traduction, réalisée par Ricoh, du rapport original publié en anglais par Quocirca. Toute erreur ou tout écart par rapport à l'information contenue dans le rapport original relève de la responsabilité de Ricoh.****