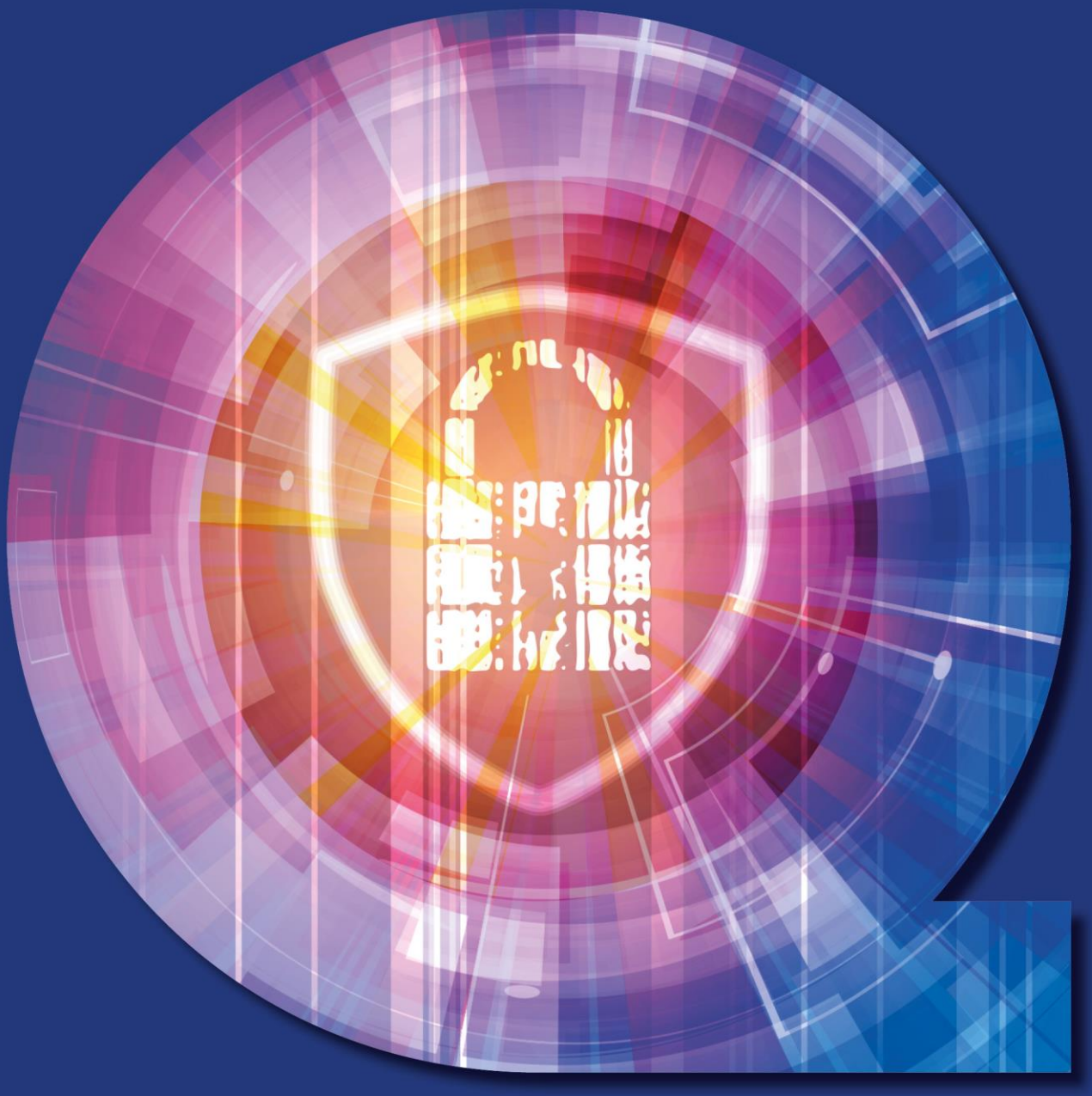
État des lieux de la sécurité d'impression en 2023

Sécuriser l'infrastructure d'impression dans un contexte de menaces grandissantes



Tendances en matière de sécurité d'impression aux États-Unis et en Europe
Extrait du rapport : Xerox
Mai 2023

QUOCIRCA

Résumé

Le rapport *Global Print Security Landscape 2023* de Quocirca révèle que les organisations sont confrontées à des défis permanents en matière de sécurisation de l'infrastructure d'impression. La question de la sécurité de l'impression à domicile reste une source de préoccupation, d'autant plus que les achats parallèles des salariés rendent plus difficile le contrôle de la sécurité des documents (Shadow IT). Les violations de données liées à l'impression restent fréquentes : 61 % des personnes interrogées ont signalé au moins une perte de données au cours des 12 derniers mois, ce chiffre passant à 67 % pour les entreprises de taille intermédiaire. Cette situation entraîne une baisse de confiance vis-à-vis de la sécurité de l'infrastructure d'impression, en particulier chez les PME.

L'étude révèle notamment un décalage marqué entre les perceptions et les comportements en matière de sécurité d'impression parmi les directeurs des systèmes d'information (DSI) et les responsables de la sécurité des systèmes d'information (RSSI). Ces derniers montrent des attentes semblables par rapport à la croissance des dépenses de sécurité au cours des 12 prochains mois : 84 % des DSI et 81 % des RSSI prévoient une augmentation de ce poste de dépense. Seuls 28 % des RSSI estiment qu'il est devenu plus difficile de relever les défis de la sécurité d'impression, contre 50 % des DSI. De la même manière, seuls 45 % des RSSI sont très ou assez préoccupés par les risques liés aux imprimantes non sécurisées, contre 72 % des DSI. La divergence de perspective entre ces deux responsables de la sécurité technique globale de l'environnement d'impression de l'entreprise a des conséquences pour l'entreprise elle-même.

Heureusement, les responsables de la sécurité d'impression réduisent les risques. Comme le montre l'indice Quocirca de maturité de la sécurité d'impression, les organisations classées comme « leaders », qui ont déjà mis en place des mesures technologiques et politiques d'impression, constatent une diminution des pertes de données et ont davantage confiance dans la sécurité de leur infrastructure d'impression. Pour les fabricants d'imprimantes, les fournisseurs de services de gestion déléguée des impressions (MPS) et le reste de la chaîne d'impression, il est indispensable de combler le fossé entre ces deux camps en matière de sécurité. Toutefois, cette démarche ne saurait être simple. Elle nécessite une double approche visant à rassembler les deux parties et à faire en sorte que l'entreprise elle-même soit plus consciente des problèmes de sécurité liés à l'impression.

Par conséquent, les fabricants d'imprimantes et leurs partenaires doivent renforcer leurs propositions de sécurité pour les organisations de toutes tailles, afin d'aider les clients à réduire les risques dans la nouvelle ère du travail hybride. Il est primordial de se positionner en tant que conseiller de confiance et fournisseur de solutions de sécurité d'impression qui s'intègrent à l'environnement de sécurité existant d'une organisation. Assurer la circulation des données et de l'information, ainsi que la sécurité des appareils et des documents produits, créera de nouvelles possibilités de revenus pour le secteur de l'impression.

L'étude *Global Print Security Landscape 2023* est basée sur les opinions de 507 décideurs informatiques (ITDM) implantés aux États-Unis et en Europe. Parmi les personnes interrogées, 20 % viennent du Royaume-Uni, 20 % de France, 20 % d'Allemagne et 40 % des États-Unis. En termes de taille d'organisation, 24 % représentent des petites et moyennes entreprises (PME) (250 à 499 salariés), 26 % des organisations de taille intermédiaire (500 à 999 salariés) et 50 % des grandes entreprises (plus de 1 000 salariés). Les personnes interrogées sont issues de différents secteurs verticaux, notamment les services aux entreprises et professionnels, la finance, l'industrie, le secteur public et le commerce de détail.

L'étude comporte également un panorama des fournisseurs de solutions de sécurité d'impression, qui présente l'évaluation par Quocirca des offres de services des principaux fabricants d'imprimantes.

Les fournisseurs suivants ont participé à cette étude : Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh et Xerox.

Conclusions principales

- **Les incidents liés à la cybersécurité ne cessent d'augmenter.** Dans l'ensemble, 42 % des organisations ont signalé une violation de la sécurité informatique au cours de l'année écoulée, ce chiffre passant à 55 % dans les organisations de taille intermédiaire et tombant à 36 % dans les grandes entreprises, ainsi que 51 % dans le secteur financier et 32 % dans le secteur public. Les logiciels malveillants sont les plus répandus dans toutes les organisations, le phishing étant le plus répandu dans les organisations de taille intermédiaire. Les failles de sécurité ont augmenté pour 61 % des organisations au cours de l'année écoulée, atteignant 70 % aux États-Unis et 66 % dans le secteur des services aux entreprises et professionnels. En moyenne, 27 % des incidents de sécurité informatique sont liés à des documents papier.
- **Les entreprises ont besoin d'impressions et donc, de solutions de sécurité efficaces.** Malgré la numérisation rapide au cours de la pandémie, 70 % des entreprises dépendent encore aujourd'hui de l'impression, et ce chiffre atteint 72 % dans les grandes organisations. Une majorité (80 %) a modifié la composition de son parc d'imprimantes au cours des deux dernières années, pour atteindre 88 % parmi les entreprises de taille intermédiaire. Dans l'ensemble des pays étudiés, 79 % des entreprises prévoient d'augmenter leurs dépenses en matière de sécurité d'impression au cours de l'année prochaine, contre 86 % aux États-Unis et 85 % dans les secteurs des services aux entreprises et professionnels et du commerce de détail.
- **La sécurité d'impression figure moins haut dans les priorités de sécurité que d'autres éléments de l'infrastructure informatique.** Les plateformes d'applications cloud ou hybrides, le courrier électronique, les réseaux publics et les terminaux traditionnels sont considérés comme les principaux risques de sécurité. Les imprimantes à domicile appartenant à l'employeur se classent au septième rang des risques de sécurité (21 %), devant l'environnement d'impression des bureaux (20 %). Il existe une disparité notable entre les DSI et les RSSI : seuls 18 % des DSI considèrent l'impression au bureau comme un risque majeur pour la sécurité, contre 30 % des RSSI.
- **Les organisations adoptent différentes approches pour gérer la sécurité de leur infrastructure d'impression.** Tandis que 31 % affirment utiliser un fournisseur de services de gestion déléguée des impressions (MPS), plus de la moitié (54 %) indique recourir à un fournisseur de services de sécurité gérés (MSSP) pour gérer à la fois la sécurité d'impression et la sécurité informatique. Cette proportion atteint 58 % dans les plus petites organisations (249-499 salariés).
- **Les entreprises ont de plus en plus de mal à répondre aux exigences en matière de sécurité d'impression.** Globalement, 39 % des personnes interrogées estiment que la tâche est de plus en plus ardue, un chiffre qui passe à 50 % dans les organisations de taille intermédiaire (de 500 à 999 salariés). Le principal défi consiste à maintenir les logiciels de gestion d'impression à jour (35 %), à éviter que les documents sensibles et confidentiels soient imprimés (34 %) et à sécuriser l'impression dans l'environnement à domicile/à distance (31 %). La sécurité du matériel constitue une préoccupation majeure pour les PME (29 %), et elle est la plus importante dans les secteurs de la finance et de l'industrie (31 %) ainsi que pour les RSSI interrogés (38 %).
- **Les organisations qui utilisent des MPS ou qui sont classées comme « leaders » en matière de sécurité d'impression sont plus confiantes dans la sécurité de leur infrastructure d'impression.** La visibilité et le contrôle offerts par un MPS semblent alléger le problème de la sécurité pour les utilisateurs. Si globalement, seulement 19 % des personnes interrogées ont pleinement confiance dans la sécurité de leur infrastructure d'impression, ce chiffre passe à 26 % dans les organisations qui utilisent un MPS. Au total, 50 % des personnes interrogées se disent plutôt confiantes. Ce constat reflète la complexité et les défis croissants associés à la sécurisation des appareils et des documents dans le cadre d'un environnement de travail hybride.
- **Au cours des 12 derniers mois, 61 % des organisations ont subi des pertes de données dues à des pratiques d'impression non sécurisées.** Ce chiffre est en baisse par rapport aux 68 % de notre étude de 2022. Les organisations de taille intermédiaire sont plus susceptibles de signaler une ou plusieurs pertes de données (67 %) que les grandes organisations (57 %) et que le secteur public (49 %). En moyenne, le coût d'une violation de données liées à l'impression s'élève à 743 000 livres sterling. Au-delà de la perte financière, le principal impact d'une violation de données est le temps perdu pour y remédier et l'impact sur la continuité de l'activité (30 %). Les points de vulnérabilité liés à l'impression à domicile, causés notamment par les employés travaillant chez eux qui n'éliminent pas les informations confidentielles de manière sécurisée, ont été cités comme l'un des principaux facteurs contribuant à la perte de données.

- **L'indice Quocirca de maturité de la sécurité d'impression révèle que seulement 27 % des organisations étudiées peuvent être considérées comme des « leaders » de la sécurité d'impression**, ce qui signifie qu'elles ont mis en œuvre six mesures de sécurité ou plus. Le nombre de leaders atteint 31 % aux États-Unis et tombe à 18 % en Allemagne, qui compte également le plus grand nombre de retardataires (29 %). Les leaders de la sécurité d'impression sont susceptibles de dépenser plus pour la sécurité d'impression, de subir moins de pertes de données et d'afficher des niveaux de confiance plus élevés vis-à-vis de la sécurité de leur environnement d'impression. En comparaison verticale, les services aux entreprises et professionnels comptent le plus grand pourcentage de « leaders » (37 %) ; le secteur public est celui qui en compte le moins (18 %).
- **Moins d'un tiers (32 %) sont très satisfaites des capacités de sécurité de leur fournisseur d'impression.** Cette proportion atteint 50 % dans les organisations américaines et tombe à 17 % en Allemagne. Les personnes qui utilisent un MPS sont beaucoup plus satisfaites (39 % sont très satisfaites) que celles qui n'utilisent pas actuellement un MPS ou qui n'envisagent pas d'en utiliser un (23 %). Les « leaders » en matière de sécurité d'impression, qui ont adopté diverses mesures comprenant notamment des évaluations de sécurité, l'impression par badge et des politiques strictes de sécurité d'impression, sont le plus susceptibles de faire état de niveaux de satisfaction plus élevés : 53 % des « leaders » sont très satisfaits, contre 27 % des « suiveurs » et seulement 15 % des « retardataires ».

Table des matières

Résumé **2**
Conclusions principales 3
Introduction **6**
Panorama des fournisseurs **7**
Profil du fournisseur : Xerox **9**
Recommandations **12**
Recommandations aux fournisseurs 12
Recommandations aux acheteurs 13
À propos de Quocirca **14**

Introduction

À mesure que les organisations s'adaptent à la gestion des équipes hybrides et à distance, qu'elles soutiennent la transformation numérique et qu'elles naviguent dans une économie mondiale incertaine et volatile, elles sont confrontées à des points de vulnérabilité et à des risques toujours croissants. L'étude de Quocirca révèle que 42 % des organisations ont subi un incident de cybersécurité au cours de l'année écoulée, ce chiffre passant à 51 % dans le secteur financier et à 55 % dans les organisations de taille intermédiaire. Le volume des incidents de sécurité a augmenté au cours de l'année écoulée pour 61 % des organisations.

Les perturbations de la chaîne d'approvisionnement et les situations géopolitiques, telles que la guerre entre la Russie et l'Ukraine, ont encore intensifié le contexte de menace. En raison de la prévalence croissante des ransomwares, des dénis de service par ransomware (RDoS), des dénis de service distribués (DDoS), de l'ingénierie sociale et des attaques de la chaîne d'approvisionnement, la cybersécurité et la résilience des fonctions critiques des entreprises suscitent de plus en plus d'inquiétudes.

Cette situation est encore aggravée par une série de défis technologiques. À mesure que les organisations migrent plus d'applications et de services vers le cloud pour soutenir les initiatives de transformation numérique, de nouveaux défis en matière de sécurité apparaissent. La quantité croissante de données critiques hébergées dans le cloud devient vulnérable aux attaques et à la compromission.

Ce risque est accentué par la possibilité pour les travailleurs à distance d'accéder à des données à partir de réseaux domestiques potentiellement non sécurisés. Les menaces de sécurité incluent des points d'accès mal configurés, des mots de passe faibles, l'absence de gestion des identités et des accès (IAM) et la non-utilisation de l'authentification multifactorielle. Les équipes de sécurité peinent à suivre le rythme en raison d'une approche fragmentée de la détection et de la surveillance des menaces.

L'infrastructure d'impression n'est pas à l'abri des risques de sécurité : en moyenne, les documents papier représentent 27 % des incidents de sécurité informatique. Les imprimantes multifonctions (MFP) intelligentes d'aujourd'hui présentent non seulement le risque que les documents papier tombent entre de mauvaises mains, que ce soit par accident ou par malveillance, mais elles peuvent également servir de passerelles vers le réseau de l'entreprise. Les imprimantes domestiques présentent un risque supplémentaire, en particulier celles qui ont été achetées par les salariés. Ces achats parallèles impliquent que les imprimantes domestiques ne répondent pas forcément aux normes de sécurité de l'entreprise ou ne sont pas surveillées via des outils de sécurité centralisés.

Bien que l'impression ne figure pas parmi les priorités en matière de sécurité informatique, les entreprises signalent toujours des pertes de données liées à l'impression. Dans notre étude de 2023, 61 % des personnes interrogées font état d'une violation de données liées à l'impression, avec un coût moyen estimé à 743 000 livres sterling pour chaque événement. L'impact d'un incident de sécurité en termes financiers et de réputation est considérable ; c'est pourquoi les organisations ne peuvent pas se permettre de relâcher leur vigilance.

Ces risques pourraient être atténués par l'adoption d'une approche de sécurité de type « confiance zéro ». Le cryptage des données et du réseau, le contrôle de la sécurité, les mesures correctives, ainsi que la micro-segmentation, peuvent réduire la surface d'attaque, améliorer la maîtrise des menaces et renforcer la conformité aux réglementations.

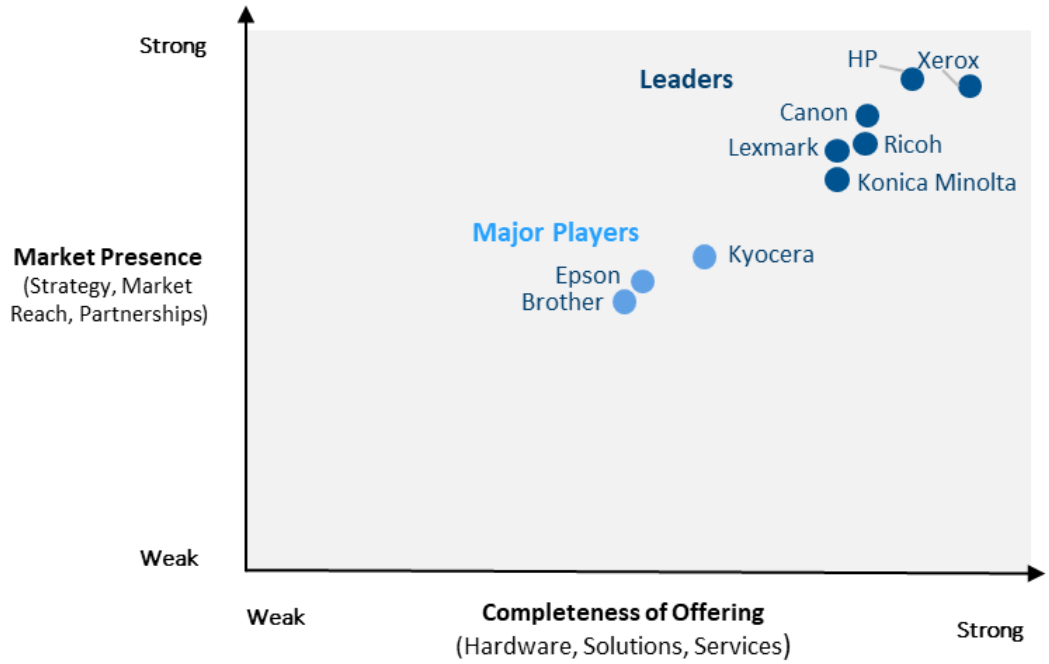
Ce rapport met en évidence les risques et les défis associés à la sécurisation de l'infrastructure d'impression pour l'environnement de travail hybride. Il y est question des niveaux de confiance en matière de sécurité, de l'adoption de mesures de sécurité d'impression, et du décalage qui sépare les DSI et les RSSI, qui doit être résolu. Il comprend également une analyse des produits, services et solutions de sécurité proposés par les principaux fabricants d'imprimantes du marché.

Panorama des fournisseurs

Quocirca a dressé un panorama du positionnement des fournisseurs sur le marché mondial de la sécurité d'impression (figure 14). Veuillez noter qu'en raison de la diversité des services offerts par chaque fournisseur et des différences régionales, ces informations ne sont données qu'à titre indicatif.

Le graphique représente le regard de Quocirca sur le paysage concurrentiel des fournisseurs, sur la base des catégories suivantes :

1. **Leaders :** ce sont les fournisseurs qui ont une vision stratégique forte et une offre complète de produits et de services de sécurité d'impression. Les leaders ont réalisé des investissements importants dans leur matériel, leur portefeuille de solutions et de services et leur infrastructure, et font preuve d'une vision forte quant à leur stratégie future.
2. **Les acteurs majeurs :** ces fournisseurs ont des offres établies et démontrées et continuent à développer leur portefeuille de solutions et de services. Ils sont plus susceptibles d'être fortement axés sur le marché des PME avec une approche centrée sur le matériel.



Completeness of Offering (Hardware, Solutions, Services)	Exhaustivité de l'offre (matériel, solutions, services)
Market Presence (Strategy, Market Reach, Partnerships)	Présence sur le marché (stratégie, couverture du marché, partenariats)
Weak	Faible
Strong	Forte
Major Players	Acteurs majeurs
Epson	Epson
Brother	Brother
Kyocera	Kyocera
Leaders	Leaders
HP	HP
Xerox	Xerox
Canon	Canon
Ricoh	Ricoh

Lexmark	Lexmark
Konica Minolta	Konica Minolta

Figure 1. Panorama des fournisseurs de sécurité d'impression en 2023, Quocirca

Ce panorama des fournisseurs est une représentation graphique de la perception du marché par Quocirca et est basée sur la méthodologie de la fiche d'évaluation de Quocirca. Ces informations sont fournies à titre de représentation visuelle uniquement et doivent être combinées à d'autres sources pour déterminer la pertinence d'un fournisseur. Quocirca ne soutient aucun fournisseur, produit ou service. Les informations sont basées sur les meilleures ressources disponibles, et les opinions reflètent un jugement porté sur le moment. Toutes les opinions sont susceptibles d'être modifiées.

Profil du fournisseur : Xerox

Avis Quocirca

Xerox a renforcé sa position de leader dans l'évaluation du marché de la sécurité d'impression en 2023 réalisée par Quocirca. Xerox a affiné sa stratégie en matière de sécurité, renforcé ses investissements dans son portefeuille de services et amélioré sa capacité de commercialisation. Son portefeuille de technologies centrées sur la sécurité est complété par une large gamme de services et de solutions de sécurité flexibles et évolutifs, qu'elle propose aussi bien aux PME qu'aux grands clients internationaux et mondiaux dont les besoins en matière de sécurité sont très stricts. Xerox se distingue particulièrement par sa forte expérience dans le secteur de la gestion déléguée des impressions (MPS) et par son expertise dans la réalisation d'évaluations de sécurité globale. Son expérience et ses capacités en matière de sécurisation et d'optimisation des processus de traitement de documents sont parmi les plus développées du secteur.

Au cours de l'année écoulée, l'entreprise a amplifié son message global sur la sécurité, et adopté un portefeuille de sécurité multicouche conforme à une série de principes de « confiance zéro ». Xerox a notamment renforcé ses capacités en matière de sécurité des appareils, de gestion du parc informatique et de sécurité du contenu. Des progrès notables ont été réalisés dans des domaines tels que la gestion des certificats, la gestion des micrologiciels, la gestion des points de vulnérabilité, la surveillance de la sécurité et les mesures correctives automatisées.

Les produits Xerox sont conformes à un large éventail de certifications sectorielles, notamment ISO 27001, ISO 22301, SOC2, SOC3 et FedRAMP. Plus récemment, l'entreprise a lancé un programme privé de recherche de bug en partenariat avec HackerOne afin d'identifier de manière proactive les points de vulnérabilité potentiels des imprimantes Xerox de la série AltaLink 8100, et d'y remédier. La sécurité renforcée s'étend aux services cloud de Xerox tels que Workplace Cloud, qui permet une gestion sécurisée de l'impression et du parc informatique, et qui est également agréé par FedRAMP.

Grâce à ses capacités étendues en matière d'impression, de capture et de flux de travail, Xerox est un bon choix stratégique pour les organisations qui dépendent fortement de l'impression et qui cherchent à atténuer les risques de sécurité dans leurs processus documentaires.

Points forts du fournisseur

Le portefeuille de produits et de services de Xerox comprend une gamme de solutions et de services qui incluent des solutions de gestion déléguée des impressions (MPS), des services de capture et de contenu (CCS), des services d'engagement des clients (CES) et des services informatiques. Les investissements continus en R&D ont permis à Xerox de déposer plus de 600 brevets dans le domaine de la sécurité. Tous les produits développés par Xerox sont conformes à la norme Xerox Product Security Standard (XPSS), qui s'inspire de la norme NIST SP 900-53. Les analyses de vulnérabilité, les tests de pénétration et le piratage éthique sont effectués tout au long du cycle de vie du produit afin de détecter, de corriger et de valider les points de vulnérabilité.

Portefeuille de technologies centrées sur la sécurité

Les appareils dotés de la technologie Xerox ConnectKey sont certifiés selon les critères communs (ISO/ IEC 15408) et FIPS 140-2/140-3, et comprennent une gamme de fonctionnalités visant à prévenir les attaques malveillantes, les logiciels malveillants et les attaques non autorisées. Cela englobe la prévention des intrusions, la signature numérique des logiciels, l'authentification des utilisateurs, la vérification des micrologiciels (au démarrage de certains appareils ou lors de l'activation par l'utilisateur), la technologie de liste blanche Trellix et l'intégration avec le moteur de services d'identité de Cisco, qui peuvent être utilisés dans une politique de sécurité et dans le respect de la réglementation. Xerox propose également l'intégration d'un fournisseur d'identité numérique (IdP) avec Okta, Ping Identity et Microsoft Azure comme solution standard, et fournit une authentification multifactorielle. Des fonctionnalités supplémentaires de sécurité des appareils et des documents sont également prises en charge, telles que le PDF crypté, l'écrasement matériel du disque et de la mémoire, et les journaux d'audit.

Son programme de conformité offre une garantie indépendante sur ses politiques et contrôles de sécurité, renforcée par les certifications ISO 27001, SOC2, FedRAMP, PCI DSS et d'autres encore. Xerox a également été le premier à recevoir l'agrément de sécurité FedRAMP pour les services de gestion déléguée des impressions basés sur le cloud.

Structure de sécurité renforcée pour l'ensemble du matériel, des solutions et des services
La structure de sécurité de Xerox repose sur quatre éléments clés : la gestion sécurisée des appareils, la gestion du parc informatique, la gestion de l'impression et la gestion sécurisée du contenu. Au niveau de l'appareil, ces mesures impliquent une série de fonctionnalités visant à prévenir les attaques malveillantes, les logiciels malveillants et les attaques non autorisées. Cela englobe la prévention des intrusions, la signature numérique des logiciels, l'authentification des utilisateurs, la vérification des micrologiciels (au démarrage de certains appareils ou lors de l'activation par l'utilisateur), la technologie de liste blanche Trellix et l'intégration avec le moteur de services d'identité de Cisco.

La gestion sécurisée du parc informatique permet d'appliquer des politiques à l'échelle du parc dans sa globalité, et de prendre des mesures correctives automatisées afin d'assurer la conformité avec les politiques de sécurité applicables aux micrologiciels, aux mots de passe, aux paramètres de sécurité et aux certificats de l'appareil. Xerox propose également un contrôle proactif de la sécurité. Les services d'audit de sécurité des imprimantes Xerox utilisent un mécanisme de politique centralisé et un regroupement de périphériques pour rationaliser la gestion du parc.

La gestion sécurisée des données et du contenu est possible grâce à la fonction de sécurité du contenu des solutions Xerox Workplace Cloud et Workplace Suite. Cette fonction permet de détecter des contenus sensibles prédéfinis et de générer des alertes et des rapports en fonction de l'utilisation de ces données. De plus, la solution Xerox Workplace Cloud crypte le contenu en circulation et hors circulation. Le contenu stocké dans le cloud chez Xerox peut être crypté en utilisant la propre clé de cryptage du client.

Extension de l'intégration de logiciels et de la gestion des points de vulnérabilité
L'intégration de solutions de sécurité, notamment de systèmes de gestion des informations et des événements de sécurité (SIEM) de Trellix (anciennement McAfee Enterprise), LogRhythm et Splunk, simplifie la création de rapports et la gestion des événements de sécurité. Parmi les services proposés par Xerox, citons le service d'audit de sécurité des imprimantes (sur site ou via un cloud privé hébergé) et la surveillance avancée du parc informatique, qui comprend la surveillance de la sécurité et l'intégration du système SIEM.

Les derniers développements portent notamment sur le Device Certificate Management (gestion de certificats d'appareils), qui permet la configuration à distance, la surveillance et des mesures correctives automatisées des politiques de certificats numériques. Sans oublier le lancement de son programme Bug Bounty en partenariat avec HackerOne en décembre 2022.

Fonctionnalités de sécurité approfondies pour le contenu et la capture
Au-delà de sa gamme de produits ConnectKey, qui présente de multiples fonctionnalités de sécurité, Xerox se distingue particulièrement par ses solutions de contenu et de capture, qui incluent des fonctionnalités avancées de prévention de la perte de contenu et de données. Xerox, qui excelle dans le domaine de l'analyse et du reporting, fournit des évaluations approfondies et surveille en permanence le profil de risque des environnements d'impression de ses clients.

Points forts du fournisseur et opportunités

Points forts

- **Un engagement fort à améliorer le portefeuille de produits en fonction des certifications de sécurité les plus rigoureuses.** Large éventail de certifications, notamment ISO 27001, SOC2, FedRAMP et PCI DSS. Investissement important dans la R&D : plus de 600 brevets liés à la sécurité ont été déposés.
- **Une approche transparente basée sur la « confiance zéro ».** Xerox a développé une proposition transparente autour de la « confiance zéro » qui englobe l'authentification, la surveillance, les mesures correctives et l'automatisation. L'entreprise propose désormais des fonctions de sécurité matérielle avancées, telles que Trusted Boot sur certains produits, et prévoit de les étendre à une plus grande partie de son portefeuille, ainsi qu'une protection des micrologiciels et du BIOS sur tous les produits AltaLink et VersaLink. Les appareils Xerox sont ainsi bien positionnés sur le marché.
- **Capacités d'évaluation et d'analyse approfondies.** Xerox possède un savoir-faire avéré sur le marché des MPS, ainsi que des capacités approfondies en matière d'évaluation de la sécurité. Ainsi, l'entreprise

est en mesure de fournir des informations pertinentes sur les points de vulnérabilité des environnements multifournisseurs existants, et de démontrer comment un parc Xerox standardisé, soutenu par ses services et ses solutions de sécurité, peut atténuer les risques.

- **Aide à la vente cohérente à l'échelle mondiale.** Au cours de l'année écoulée, Xerox a investi dans la formation et les ressources pour soutenir ses canaux directs et indirects. L'entreprise a mené une campagne de marketing efficace qui contribue à démystifier la complexité de la sécurité, ce qui renforce sa position non seulement auprès des utilisateurs finaux, mais aussi des membres du réseau qui ont besoin de construire ou d'améliorer leur offre de services de sécurité.

Opportunités

- **Poursuivre le développement de l'offre de services informatiques sur le marché des PME.** Xerox a réussi à s'imposer dans le secteur des services informatiques et peut tirer parti de ses partenariats pour proposer des offres de services de sécurité packagées à ses partenaires de distribution, tant dans le secteur des technologies informatiques que dans celui de l'impression traditionnelle.
- **Améliorer l'utilisation du ML (machine learning) et de l'IA pour faciliter la détection des anomalies.** Cette avancée pourrait étendre les capacités de Xerox au-delà de la protection contre les intrusions, afin de mieux détecter et remédier aux menaces nouvelles et sophistiquées.
- **Établir des relations avec les MSSP.** Bien que Xerox soit tout à fait en mesure de proposer ses propres services de gestion déléguée des impressions, de nombreux clients cherchent à travailler avec ce type de fournisseurs pour tous les aspects de leur sécurité, incluant l'impression. Xerox doit s'assurer de nouer les bonnes relations avec les principaux fournisseurs dans ce domaine.

Recommandations

Les dépenses liées à la sécurité d'impression continueront probablement à augmenter au cours des 12 prochains mois, ce qui créera des opportunités pour les fabricants d'imprimantes, les fournisseurs de services de gestion déléguée des impressions et les partenaires du réseau de distribution. De toute évidence, les organisations qui utilisent des MPS et celles qui ont adopté diverses mesures de sécurité pour l'impression ont une longueur d'avance. Si les fournisseurs démontrent comment les MPS peuvent améliorer la sécurité de l'infrastructure d'impression, ils pourront adapter leurs propositions aux environnements d'impression de bureau et domestiques.

Recommandations aux fournisseurs

Quocirca recommande aux fournisseurs d'aborder les domaines suivants.

- **Réduire le décalage entre les DSI et les RSSI.** Dans les grandes entreprises, la responsabilité de la sécurité d'impression se trouve souvent fragmentée entre les différents intervenants des services informatiques et métiers. Tandis que les DSI ont une vision stratégique de l'ensemble de l'infrastructure informatique, les RSSI se concentrent entièrement sur la sécurité. Compte tenu du manque de sensibilisation de ces décideurs, les fournisseurs devraient élever le positionnement et le message de la sécurité d'impression à un niveau stratégique. Cette approche permettra d'aligner les priorités en matière de sécurité d'impression, à mesure que les DSI et les RSSI développeront une relation de collaboration plus étroite.
- **Assurer une sécurité cohérente au sein de l'environnement hybride.** Beaucoup d'imprimantes à domicile achetées par les salariés ne sont pas conformes aux exigences de sécurité de l'entreprise. Il faut veiller à ce que les offres MPS axées sur la sécurité contribuent à résoudre le problème de l'achat parallèle, soit par une surveillance à distance centralisée, soit par la mise à disposition d'appareils autorisés pour l'utilisation à domicile. Bien que les environnements standardisés présentent généralement un niveau de sécurité matérielle plus élevé que les environnements dont le parc informatique est mixte, de nombreuses organisations utilisent une variété de marques d'appareils au bureau et à domicile. Cette situation crée un besoin de plateformes tierces intégrées de gestion de l'impression, capables de gérer la sécurité des documents de manière cohérente au sein d'un parc hétérogène. Cependant, cela offre aux fournisseurs MPS la possibilité de diriger leurs clients vers un environnement uniformisé afin de renforcer la sécurité de leur infrastructure d'impression.
- **Clarifier les offres basées sur la « confiance zéro ».** Il n'existe pas de solution unique pour atteindre cette « confiance zéro ». Il convient d'expliquer clairement le fonctionnement des dispositifs existants, et d'éviter l'utilisation abusive du terme « confiance zéro », afin de donner un sentiment de sécurité renforcée. La meilleure façon d'obtenir un niveau de « confiance zéro » dans le domaine de l'impression est de procéder à une micro-segmentation et à une intégration avec des plateformes d'authentification multifactorielle et de gestion des identités et des accès (IAM). Démontrer ses compétences et son savoir-faire dans ce domaine en se concentrant sur les principes stratégiques et les partenariats, ce qui permettra également d'instaurer un climat de confiance avec les clients qui ont besoin de passer en toute sécurité à une infrastructure d'impression basée sur l'informatique dans le cloud.
- **Exploiter le MPS pour renforcer la sécurité.** Les organisations qui utilisent des MPS ainsi que diverses mesures de sécurité (évaluations régulières de la sécurité, audits et solutions) ont une longueur d'avance sur la courbe de la sécurité de l'impression, aussi bien du point de vue de la confiance que de la réduction des pertes de données. Les services et solutions de sécurité évolutifs et flexibles intéresseront les plus petites organisations, qui ne sont pas à l'abri des risques de sécurité mais qui ne disposent pas non plus du budget nécessaire pour mettre en œuvre des mesures de sécurité avancées en matière d'impression. Proposer des évaluations régulières de la sécurité en fonction de l'évolution des besoins de l'entreprise est également essentiel pour améliorer les niveaux de satisfaction en matière de sécurité d'impression.

Recommandations aux acheteurs

Pour répondre aux nouveaux modes de travail hybrides, le champ des menaces en matière de sécurité de l'impression s'est élargi pour englober désormais toute une série d'appareils à domicile et professionnels. En tant qu'appareils intelligents connectés en réseau, les multifonctions constituent un maillon faible de la sécurité informatique. Ce problème pourrait être atténué par une série de mesures basées sur le positionnement de l'organisation en matière de sécurité.

Les acheteurs devraient envisager les mesures suivantes.

- **Faire de la sécurité d'impression une priorité stratégique.** La sécurité d'impression et la sécurité informatique doivent être intégrées et considérées comme une priorité de premier ordre. Souligner l'importance de la sécurisation de l'infrastructure d'impression auprès des DSI et des RSSI, afin qu'ils comprennent les risques liés à l'impression non sécurisée et les mesures qui peuvent être mises en œuvre pour les atténuer.
- **Procéder à des évaluations approfondies de la sécurité et des risques liés à l'impression.** Les organisations devraient se tourner vers des fournisseurs capables d'offrir des évaluations approfondies de l'environnement d'impression. Les audits de sécurité permettent de révéler des failles potentielles dans la sécurité des appareils et des documents. Pour les organisations qui exploitent un parc mixte, cette démarche permet de mieux comprendre les possibilités d'optimisation des appareils au moyen d'un parc unique doté de fonctions de sécurité matérielle homogènes.
- **Garantir la sécurité d'impression pour les salariés à distance et à domicile.** Veiller à ce que les imprimantes soient conformes aux normes de sécurité de l'entreprise et, dans le cas où les salariés ont acheté leurs propres imprimantes, élaborer des lignes directrices en matière de sécurité pour déterminer si et comment ces imprimantes peuvent être utilisées. Évaluer les plateformes de gestion de l'impression pour la prise en charge et le contrôle de la sécurité d'impression à domicile.
- **Construire une architecture de sécurité d'impression efficace.** Les solutions de sécurité fragmentaires offrent rarement une sécurité efficace et fiable, en particulier dans un environnement de travail hybride. Il convient d'envisager une plateforme de sécurité intégrée capable de prendre en charge des fonctions telles que l'impression pull (par badge), la surveillance à distance et la création de rapports pour l'ensemble du parc informatique. Étendre la sécurité d'impression au contenu et aux flux de travail en utilisant des outils de sécurité du contenu et de prévention de la perte de données (DLP) au niveau de l'application. Évaluer soigneusement les déclarations de « confiance zéro » des fournisseurs et veiller à l'intégration avec les plateformes d'authentification multifactorielle déjà utilisées dans l'entreprise. Déterminer si les solutions de gestion sécurisée des impressions peuvent fonctionner dans un réseau micro-segmenté.
- **Formaliser les processus de réponse aux incidents liés à la sécurité d'impression.** Les organisations doivent s'assurer qu'elles sont préparées à cette éventualité et qu'elles ont mis en place les processus adéquats pour faire face aux retombées techniques, juridiques et de réputation d'une telle violation. Pour ce faire, l'organisation doit collaborer à la mise en place d'un ensemble de politiques globales.
- **Contrôler, analyser et établir des rapports en permanence.** Garantir la collecte et l'analyse des données provenant des dispositifs de sécurité existants, tels que les systèmes de gestion des informations et des événements de sécurité (SIEM), afin de déterminer les événements passés, présents et futurs. Veiller à ce que ces systèmes couvrent autant que possible l'ensemble de la plateforme et utiliser les connaissances acquises pour combler les vulnérabilités de l'organisation en matière de sécurité.

À propos de Quocirca

Quocirca est un cabinet de recherche et d'analyse du marché mondial spécialisé dans la convergence des technologies de l'impression et du numérique dans l'environnement de travail de demain.

Depuis 2006, Quocirca exerce une grande influence en conseillant ses clients sur les évolutions majeures du marché. Nos services de conseil et de recherche sont à la pointe de l'évolution rapide du marché des services et des solutions d'impression, et sont reconnus par les clients à la recherche de nouvelles stratégies pour faire face aux bouleversements technologiques.

Quocirca a mené des recherches pionnières dans de nombreux domaines des marchés émergents. Après avoir analysé pour la première fois, il y a plus de dix ans, le paysage concurrentiel mondial des services de gestion déléguée des impressions (MPS), nous avons procédé à la première analyse concurrentielle mondiale du marché de la sécurité d'impression. Plus récemment, Quocirca a renforcé son approche avant-gardiste et unique sur le marché en publiant la première étude sur l'avenir intelligent et connecté de l'impression dans l'environnement de travail numérique. L'étude Global Print 2025 offre un aperçu inégalé de l'impact des bouleversements numériques, tant du point de vue des dirigeants de l'industrie que de celui des utilisateurs finaux.

Pour plus d'informations, rendez-vous sur www.quocirca.com.

Droits d'utilisation
Toute citation d'une information contenue dans ce rapport est soumise à autorisation. Veuillez consulter la politique de citation de Quocirca pour plus de détails.