Sécurité à l'ère du travail hybride

Un guide et une liste de contrôle pour la mise en œuvre de la sécurité complète.

xerox™

Le mode de fonctionnement des entreprises et la circulation des informations ont changé

Alors que nous évoluons vers de nouvelles méthodes de travail, les périphériques, les documents et les données restent la force vitale de toute entreprise. Après les efforts déployés pour maintenir les entreprises en activité, le travail flexible est devenu la nouvelle donne. Avez-vous fait le nécessaire pour rester en sécurité quel que soit l'endroit où le travail est effectué ?

Les données dont nous dépendons pour mener nos activités exposent également nos organisations à des risques considérables. N'importe quel type de violation peut avoir des conséquences néfastes — elle peut causer le chaos et la méfiance, faire chuter le cours des actions, voire entraîner des mesures disciplinaires et de fortes amendes imposées par les autorités de réglementation.

Nous avons créé ce livre électronique afin d'aider votre entreprise à choisir judicieusement les meilleures options de protection des documents et données d'entreprise par la sécurisation de l'infrastructure d'impression qui les héberge. Il est conçu pour aider toutes les personnes et toutes les organisations, quel que soit leur rôle ou leur taille, à assimiler les procédures et les politiques nécessaires pour garantir une sécurité optimale de leur infrastructure informatique. Y sont inclus les ressources externes au-delà du pare-feu de l'entreprise.

Reportez-vous souvent à la liste de contrôle incluse dans ce livre électronique et partagez-la avec vos collaborateurs. En veillant à ce que tout le monde soit bien informé et sur la même longueur d'onde, vous pouvez être plus confiant dans vos prises de décisions en matière de sécurité et en ce qui concerne la cybersanté de votre organisation.

Votre stratégie de sécurité répond-elle aux exigences de cette nouvelle ère de travail hybride ? Pouvez-vous prouver la conformité sans l'ombre d'un doute ? Peu d'entreprises sont aussi sécurisées qu'elles le pensent.

TABLE DES MATIÈRES

La menace est réelle

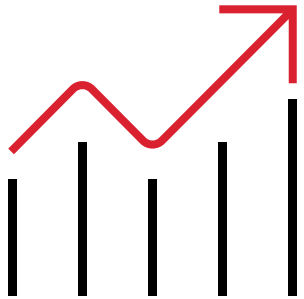
Personne ne peut se permettre d'ignorer la sécurité de son infrastructure informatique aujourd'hui. C'est une menace qui n'est pas prête de disparaître. Aujourd'hui plus que jamais, les points d'entrée potentiels se multiplient en raison de la flexibilité croissante de l'environnement de travail.

Que vous ayez adopté des pratiques de travail flexible ou que vous travailliez avec des clients qui ont adopté ce mode de travail, la nécessité d'assurer la sécurité des documents, des périphériques et du contenu est plus que jamais omniprésente.

- La propriété intellectuelle doit être protégée de la concurrence
- Les informations financières et personnelles du client doivent être à l'abri des pirates informatiques
- Les dossiers des employés et les informations personnelles identifiables sont source de préoccupation pour les ressources humaines
- Les réglementations et les exigences du secteur ajoutent à la complexité

Les grandes entreprises sont depuis longtemps des cibles, mais les PME deviennent également de plus en plus vulnérables, dans la mesure où les pirates informatiques les ciblent davantage. En outre, tout le monde est sous pression pour respecter les politiques et les exigences de sécurité internes et externes et prouver leur niveau de conformité aux partenaires, aux fournisseurs et aux clients fidèles.

Cela signifie que chacun, quels que soient son titre, son service et son secteur d'activité, joue un rôle important et doit prioriser la sécurité et la conformité.



Les violations de sécurité ont augmenté pour **61 %** des organisations au cours de l'année écoulée, atteignant **70 %** aux États-Unis et **66 %** dans les entreprises et les services professionnels.

Source : Quocirca – The Print Security Landscape, 2023 (Le paysage de la sécurité de l'impression) (États-Unis et UE)

Les coûts augmentent

Les violations de sécurité sont de plus en plus coûteuses à l'échelle mondiale, tant en termes de coûts financiers que de conséquences indirectes. Parmi ces conséquences, on peut citer le temps, les efforts et les ressources consacrés à informer les victimes et à enquêter sur l'incident, ainsi que l'impact négatif sur la réputation de l'organisation.

Aucune entreprise, aucun secteur d'activité et aucun service n'est en sécurité. Les cybercriminels lancent des attaques qui ciblent les individus, les ménages, les entreprises, les administrations, les services de police, les hôpitaux, les établissements scolaires, les banques, les réseaux électriques, les services publics, les data centers, les serveurs, les réseaux, les ordinateurs de bureau et portables, les tablettes et les téléphones intelligents.

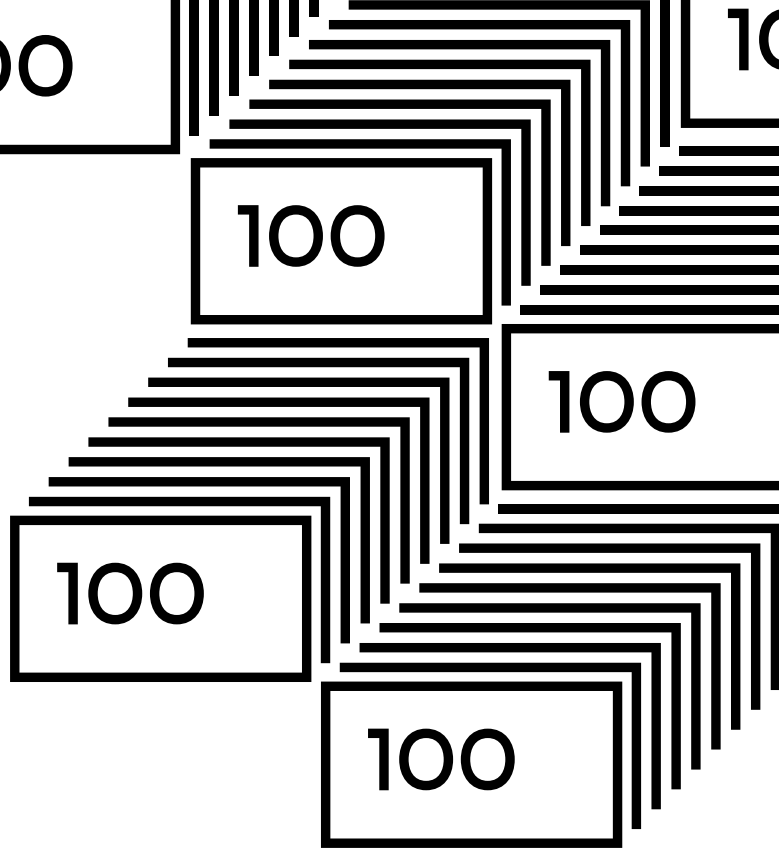
Atteignant son niveau le plus élevé, le coût d'une violation de données s'est élevé en moyenne à 4,35 millions de dollars américains en 2022.

Les cinq pays et régions où le coût moyen d'une violation de données est le plus élevé sont les États-Unis (9,44 millions USD), le Moyen-Orient (7,46 millions USD), le Canada (5,64 millions USD), le Royaume-Uni (5,05 millions USD) et l'Allemagne (4,85 millions USD).[1] Les coûts mondiaux de cybercriminalité devraient augmenter de 15 % par an au cours des trois prochaines années, pour atteindre 10 500 milliards USD par an d'ici 2025.[2]

La fréquence des attaques par ransomware contre les gouvernements, les entreprises, les consommateurs et les périphériques continuera d'augmenter au cours des cinq prochaines années, pour atteindre une attaque toutes les deux secondes.[2]

Mais plus rapidement une violation de données peut être identifiée et contenue, moins les coûts sont élevés.

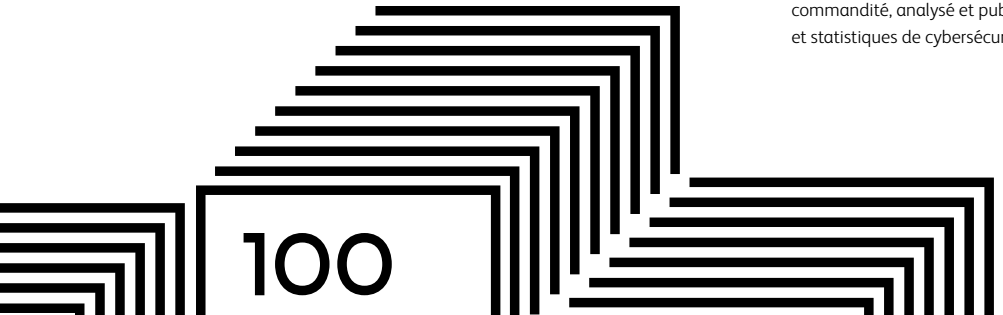
1. Rapport « Coût d'une violation de données » 2022 – Ponemon Institute, commandité, analysé et publié par IBM Security® (WW) 2. « Top 10 des prévisions et statistiques de cybersécurité pour 2023 » – Cybercrime Ventures (WW)



935 000 USD,

coût moyen estimé d'une violation de données.

Source : Quocirca – The Print Security Landscape, 2023 (Le paysage de la sécurité de l'impression) (États-Unis et UE)



Les points d'entrée sont nombreux et se multiplient

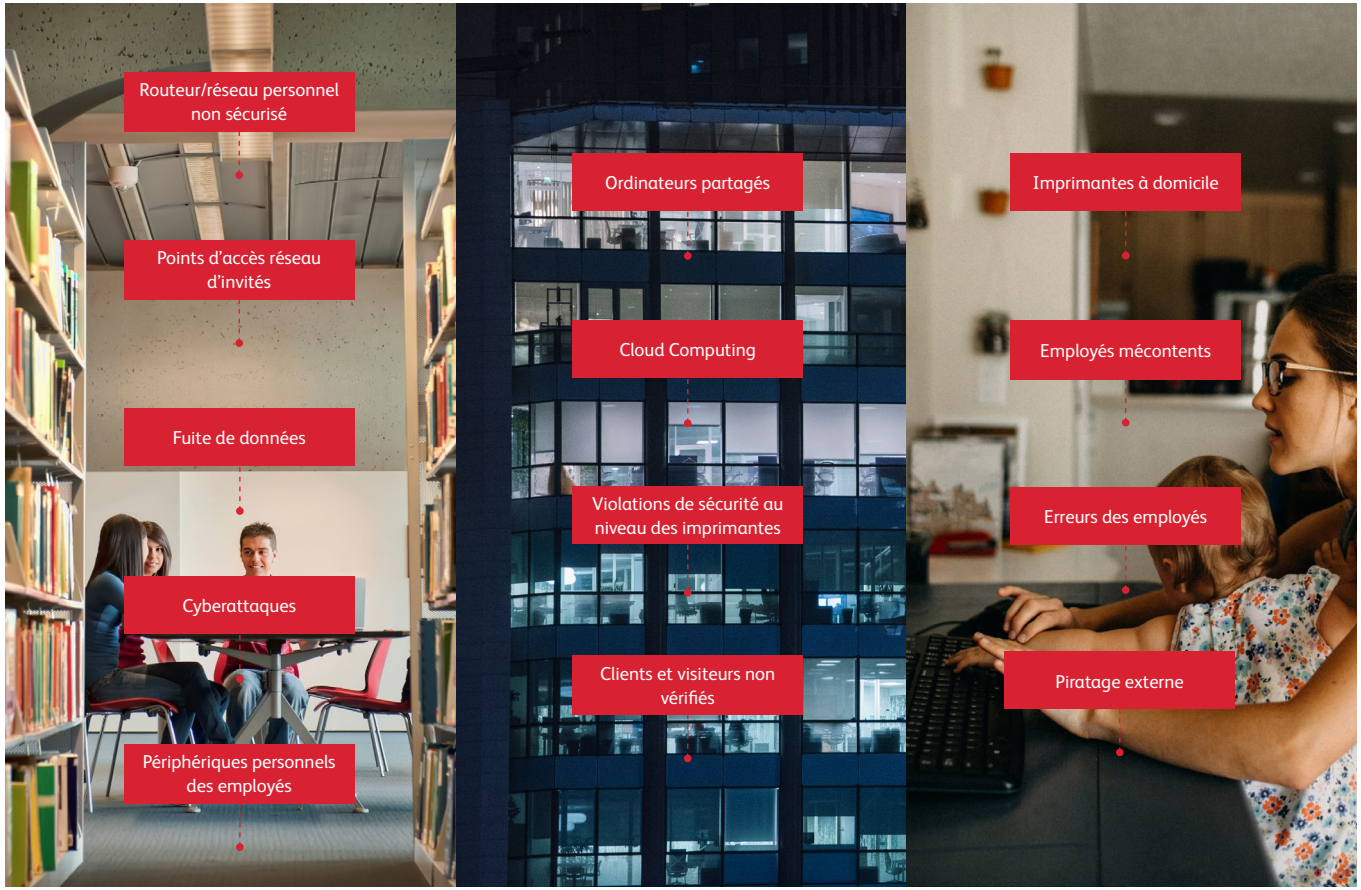
Les menaces proviennent de l'ensemble de votre infrastructure IT ainsi que des personnes qui y accèdent, en interne ou depuis l'extérieur. Vous devez également tenir compte des employés ou des clients qui travaillent à domicile ou ou dans des emplacements distants moins sécurisés, voire qui utilisent un inventaire non contrôlé par les politiques informatiques.

En moyenne, **25 %** des effectifs travaillent à distance en permanence, **33 %** sont des travailleurs hybrides et **42 %** travaillent au bureau en permanence.

Source : Quocirca – The Print Security Landscape, 2023 (Le paysage de la sécurité de l'impression) (États-Unis et UE)

Plus de **7 %** des périphériques de bureau Windows exécutent des versions non prises en charge

La part de marché de la version Windows de bureau dans le monde – février 2023



Les imprimantes ne sont pas à l'abri d'une violation de sécurité

Pour les pirates informatiques qui cherchent un moyen d'accéder à un réseau d'entreprise ou personnel, les déploiements IoT non sécurisés comme les imprimantes constituent le point d'entrée idéal. En adoptant quelques mesures simples, vous pouvez atténuer les risques et stopper les cybercriminels dans leur élan.

COMMENT PROCÉDER ? ALLOUEZ DES RESSOURCES ADÉQUATES OU ASSOCIEZ-VOUS AUX RESSOURCES NÉCESSAIRES POUR UNE STRATÉGIE DE SÉCURITÉ ET UNE MISE EN ŒUVRE COMPLÈTES.

Pour garantir que vos périphériques d'impression sont aussi sûrs que vous l'espérez, vous avez besoin d'une stratégie globale qui couvre plusieurs niveaux — des données et documents aux personnes et périphériques, en passant par les règles et réglementations générales qui régissent votre entreprise.

Les organisations, grandes ou petites, mettent en place des politiques et des procédures de sécurité pour empêcher les logiciels malveillants, les attaques, les fuites de données et les risques associés à l'informatique en nuage ; elles définissent également des politiques à l'intention des employés. Mais nombreuses sont celles qui n'ont encore rien fait pour protéger leur infrastructure d'impression.

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 taux atteignant **67 %** pour les organisations de taille moyenne.

Source : Quocirca – The Print Security Landscape, 2023 (Le paysage de la sécurité de l'impression) (États-Unis et UE)

Le facteur humain

Lorsque des violations de sécurité ou de données se produisent, il est naturel de se tourner vers les services informatiques. Cependant, ce sont bien souvent les erreurs ou les actions des utilisateurs ne respectant pas les les directives en matière de comportement recommandées par les services informatiques qui causent des problèmes. Vos plus grandes cybermenaces ne sont pas des acteurs malveillants. Ce sont vos employés : ils commettent des erreurs involontaires. Ils utilisent des raccourcis non approuvés. Ils s'efforcent de faire plus avec moins. Par conséquent, ils peuvent prendre des décisions qui mettent votre entreprise en danger.

Cliquez ici pour regarder la vidéo

COMMENT PROCÉDER ?

Commencez par exploiter les données analytiques pour découvrir comment vos utilisateurs travaillent avec les documents et les périphériques. Deuxièmement, cherchez à mettre en œuvre un environnement de travail Confiance zéro, de vérification systématique de la sécurité.

Une analyse sur les utilisateurs peut répondre aux questions suivantes :

- Qui effectue des impressions en dehors des heures de bureau, lorsque d'employés sont présents ?
- Une personne importante a démissionné. Qu'a-t-elle imprimé récemment ?
- Un employé a-t-il numérisé ou envoyé du contenu par courrier électronique vers un emplacement non autorisé comme un cloud public ?

Mise en œuvre du modèle Confiance zéro :

- Aide à limiter le facteur humain
- Permet l'authentification, de sorte que seuls les utilisateurs autorisés peuvent accéder à ce qui leur est destiné exclusivement
- Provoque des changements de comportement conscients

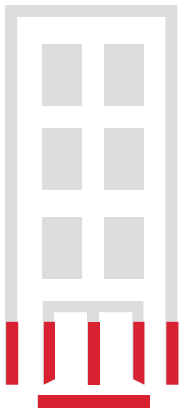
L'analyse des utilisateurs et la mise en œuvre de la sécurité Confiance zéro peuvent vous orienter vers d'autres services et solutions qui favorisent la durabilité, la productivité et la conformité.

> **95 %** des violations de cybersécurité sont dues à des erreurs humaines.
>
> Source : Rapport « Risques à l'échelle mondiale » 2022 – World Economic Forum

Dans une enquête récente, la moitié des personnes interrogées ont déclaré inclure l'impression dans leur stratégie Confiance zéro, et 39 % supplémentaires prévoyant de le faire au cours des 12 prochains mois.[1]

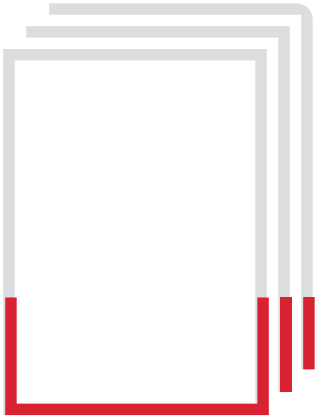
1. Étude « Tendances de Sécurité Confiance zéro de 2022 » de Quocirca. (États-Unis et Royaume-Uni)

Les mesures de sécurité sont à la traîne



19 %

des personnes interrogées sont tout à fait convaincues que leur infrastructure d'impression est sécurisée.



En moyenne,

27 %

des incidents de sécurité informatique étaient liés à des documents papier.

Pour

34 %

des personnes interrogées, le principal défi consiste à empêcher l'impression de documents confidentiels et sensibles.

Source : Quocirca – The Print Security Landscape, 2023 (Le paysage de la sécurité de l'impression) (États-Unis et UE)

La sécurité est une préoccupation grandissante, mais la mise en place de mesures de sécurité est à la traîne. Où en est votre organisation ? La sécurité de votre infrastructure informatique et de vos documents, de vos imprimantes, de votre contenu et des données qui y sont stockées vous préoccupe-t-elle ? Que pourriez-vous ou devriez-vous faire que vous ne faites pas ?

Dépasser la gestion de l'impression

L'Internet des objets (IoT) ne se compose plus uniquement d'ordinateurs et de téléphones. L'information n'est plus contenue dans des environnements contrôlés et fiables. Le cloud a changé la façon dont les entreprises fonctionnent, permettant essentiellement l'accès aux données, aux applications, aux plateformes et aux services n'importe où, à tout moment.

À mesure que votre milieu de travail s'étend au-delà du confinement de vos quatre murs et devient plus connecté, le nombre de périphériques intelligents et IoT dans vos environnements de travail augmentera, et le besoin d'aller au-delà des services de gestion d'impression traditionnels augmentera également.

Une approche de la sécurité axée sur les données, qui utilise l'analytique pour identifier les possibilités d'économies de coûts et de gains de productivité, est essentielle pour optimiser les interactions entre les employés et la technologie. Le résultat est un milieu de travail plus productif et plus efficace, ainsi qu'une sécurité et une conformité accrues.

VOICI SIX ÉLÉMENTS CLÉS À PRENDRE EN COMPTE AU MOMENT DE CHOISIR UN PARTENAIRE POUR VOUS AIDER À COMBLER VOS LACUNES EN MATIÈRE DE SÉCURITÉ :

1. Peut-il appliquer sa solution aux bons périphériques au bon moment et créer des politiques faciles à appliquer et à respecter ?
2. Comprend-t-il les exigences de votre réseau ? Peut-il recommander des solutions adaptées et utiliser les données pour assurer la maintenance continue et un service et une assistance proactifs ?
3. Se concentre-t-ils sur l'inspection et la surveillance constantes de tous les périphériques et processus documentaires afin d'assurer automatiquement la conformité à tous les niveaux ?
4. Peut-il prendre des mesures correctives au niveau du parc, des imprimantes et des paramètres afin que les problèmes de non-conformité puissent être identifiés et résolus rapidement ?
5. Fournira-t-il des rapports continus et en temps réel pour montrer la conformité et/ou mettre en évidence les domaines qui doivent être corrigés ?
6. Peut-il le faire quel que soit le milieu de travail ?

Les entreprises investiront **15 000 milliards de dollars** en IoT d'ici 2025.*

*Source : vXchnge (WW)

Une approche globale et Confiance zéro en matière de sécurité

La protection totale des terminaux dans un monde mobile, axé sur le cloud et l'IoT requiert une approche multicouches et une vigilance constante, mais il n'est pas possible de surveiller chaque terminal manuellement. Malgré les nouveaux défis actuels, la plupart des stratégies de sécurité ne tiennent pas compte du fait que les documents, les données et le contenu qui font fonctionner les entreprises de nos jours se trouvent partout et sont disponibles 24h/24, 7j/7.

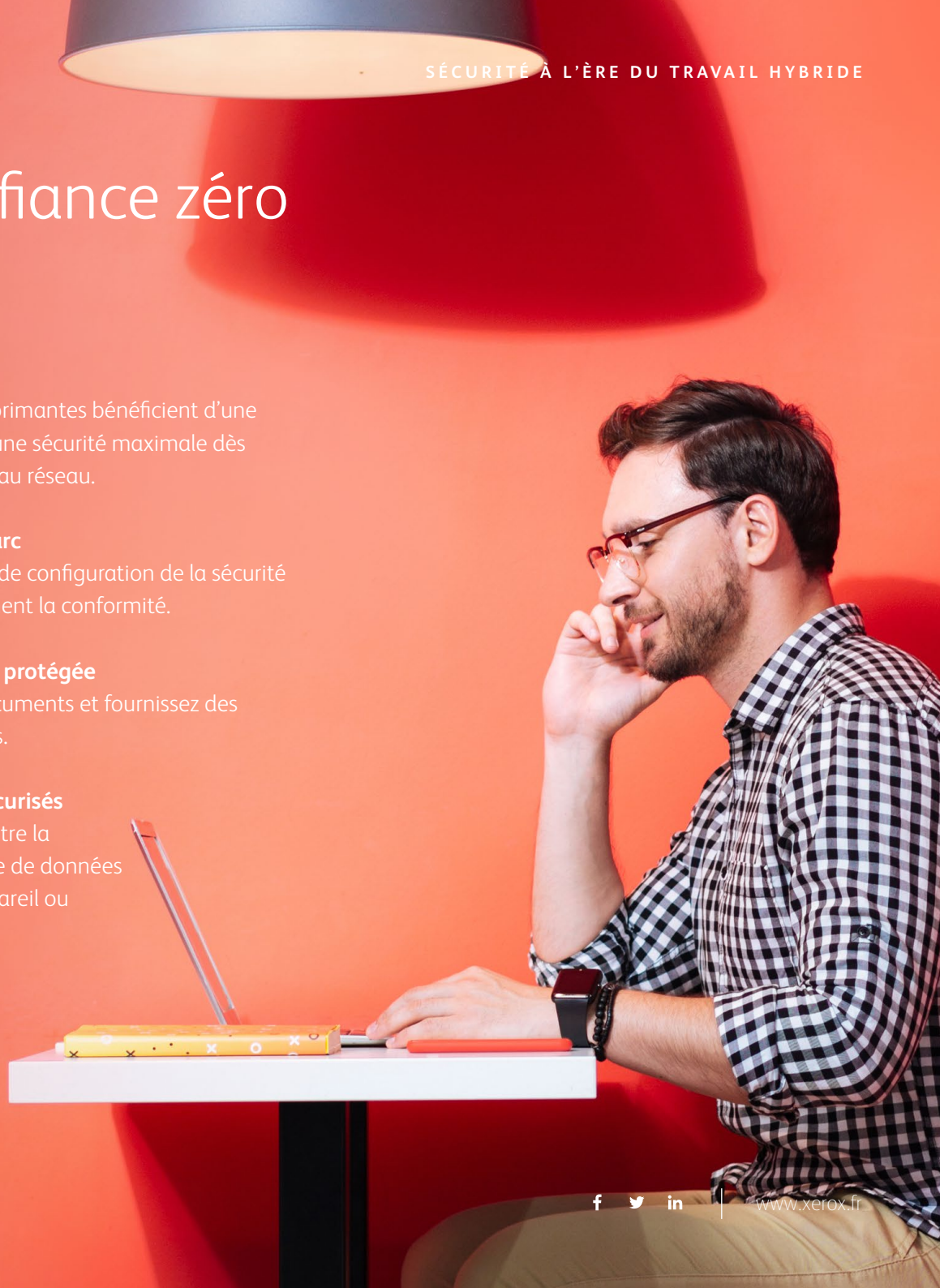
Il est essentiel que votre fournisseur de services adopte une approche globale et multicouches de la sécurité avec une intelligence proactive qui protège les périphériques, les documents, les données et le contenu. En même temps, nous complétons votre mise en œuvre de la Confiance zéro en offrant des solutions qui s'harmonisent parfaitement.

Périphériques sécurisés
Assurez-vous que vos imprimantes bénéficient d'une protection intégrée et d'une sécurité maximale dès qu'elles sont connectées au réseau.

Gestion sécurisée du parc
Définissez des politiques de configuration de la sécurité et validez automatiquement la conformité.

Gestion de l'impression protégée
Contrôlez l'accès aux documents et fournissez des informations exploitables.

Données et contenu sécurisés
Verrouillez la sécurité contre la divulgation non autorisée de données et de contenus (sur l'appareil ou dans le cloud).



68 %

des entreprises ont subi une ou plusieurs attaques au niveau des terminaux.

Source : Ponemon Institute, 2020 Étude sur l'État du risque de sécurité des points de terminaison

Prochaines étapes : Identifier les lacunes, gagner en confiance

Comment pouvez-vous être sûr que vos périphériques, vos documents et vos données sont sécurisés; quels aspects de la sécurité avez-vous envisagés et ce faisant, quelles mesures avez-vous prises ? Il est important que vous soyez informé des discussions et des décisions prises en matière de sécurité au sein de votre organisation, et que vous soyez au courant des lacunes existantes afin de savoir si vous allez dans la bonne direction pour votre entreprise.

LES ÉTAPES SUIVANTES

1. Comprendre les politiques de sécurité de votre entreprise pour les périphériques, les documents et les données.

2. Identifier et engager les principales parties prenantes, évaluer votre niveau de risque.

3. Isoler les vulnérabilités des périphériques ou des processus, ainsi que les points faibles, et prendre des mesures pour s'assurer qu'ils sont corrigés.

4. Utilisez la liste de contrôle suivante pour discuter des besoins et des lacunes avec votre équipe.

Les services de gestion d'impression de Xerox® offrent un processus simplifié et sécurisé pour accélérer la transformation numérique et améliorer la façon dont les gens interagissent avec la technologie.

Nous assurons une surveillance interactive de la sécurité et la conformité à partir d'un tableau de bord visuel et intuitif, et intégrons les technologies de sécurité des imprimantes avec les plateformes Trellix[3] DXL et Cisco® pxGrid, permettant ainsi une réponse instantanée et automatique aux menaces.

En outre, nous sommes le seul fournisseur de services d'impression à avoir obtenu des autorisations de sécurité de la FedRAMP pour nos services de gestion d'impression basés sur le cloud, l'un des composantes de l'offre Service de gestion d'impression Xerox®. Nous sommes placés en haut du classement des rapports sur la sécurité d'IDC Marketscape et de Quocirca (Paysage de la sécurité de l'impression) en raison de l'importance que nous accordons à la sécurité et à l'autonomisation des services informatiques et des utilisateurs finaux. Ensemble, nous pouvons créer un environnement plus sûr.

Pour en savoir plus, consultez le site **www.xerox.fr/fr-fr/qui-sommes-nous/solutions-de-securite**

3. Trellix : anciennement une société de McAfee®.

Liste de contrôle complète : Périphériques, documents et données

Que vous souhaitiez le mettre en œuvre vous-même ou que vous choisissiez de travailler avec des partenaires de confiance, nous vous présentons votre guide de travail pour une approche globale de la sécurité Confiance zéro.

Qualifications et bonnes pratiques des partenaires de sécurité

Éléments à prendre en compte pour garantir une sécurité complète des périphériques, des documents et des données.

ANALYSE DE LA SÉCURITÉ ET CRÉATION DE RAPPORTS

- ☐ Le partenaire travaille-t-il avec vous pour évaluer les besoins en matière de sécurité et identifier où se trouvent vos informations, comment elles sont transférées et quels sont les domaines où les risques sont les plus élevés ?
- ☐ Le partenaire propose-t-il un plan/une stratégie de sécurité global(e) qui englobe les périphériques, les documents et les données ?
- ☐ Le partenaire vous aide-t-il à définir des politiques de sécurité, à valider la conformité, à contrôler l'accès et à verrouiller la divulgation non autorisée de documents et de données sensibles ?
- ☐ Le partenaire a-t-il des directives claires pour les stratégies à mettre en place en vue de soutenir vos initiatives de sécurité Confiance zéro ?
- ☐ Le partenaire dispose-t-il de technologies robustes qu'il peut utiliser pour garantir la qualité et la précision des données ?
- ☐ Le partenaire vous rencontre-t-il de manière proactive pour discuter de la sécurité et d'autres problèmes ?
- ☐ Les rapports fournis par le partenaire de sécurité apportent-ils des informations et perspectives sur la mise en œuvre des politiques de sécurité et sur les périphériques à risque ?

RECOMMANDATIONS POUR LES PÉRIPHÉRIQUES, LE POSITIONNEMENT ET L'OPTIMISATION

- ☐ Le partenaire de sécurité vous aidera-t-il à sélectionner les meilleurs périphériques pour en assurer la sécurité ? Les imprimantes les plus sécurisées disposent de plusieurs niveaux de fonctions de sécurité et sont capables de s'intégrer à des programmes centralisés de gestion de la sécurité tels que Trellix[3] ePolicy Orchestrator et Cisco ISE.
- ☐ Le partenaire peut-il utiliser l'analytique pour avoir une compréhension approfondie des périphériques dont vous disposez aujourd'hui et identifier les domaines pour une réduction ou une optimisation ?

ENGAGEMENT EN FAVEUR DE L'INNOVATION EN MATIÈRE DE SÉCURITÉ

- ☐ Le partenaire travaille-t-il avec des fournisseurs qui investissent dans la recherche, le développement et l'ingénierie en matière de sécurité ? Xerox, par exemple, consacre un pourcentage de son chiffre d'affaires à la sécurité et à d'autres projets critiques portant sur la recherche, le développement et l'ingénierie.
- ☐ Le fournisseur de services de sécurité fait-il recours à des personnes, des processus et des technologies pour répondre aux normes les plus strictes en matière de conformité à la sécurité ?

PROGRAMME DE CONFORMITÉ À LA SÉCURITÉ

- ☐ Ces fournisseurs obtiennent-ils des accréditations, réalisent-ils des audits stricts et reçoivent-ils de nombreuses certifications pour leurs solutions matérielles et logicielles ?

LOGICIEL DE SÉCURITÉ DES SERVICES DE GESTION D'IMPRESSION

- ☐ Le partenaire travaille-t-il avec des fournisseurs de services de gestion d'impression dont le back-office a été certifié conforme à norme ISO 27001 en tant qu'installation sécurisée ?
- ☐ Le logiciel du partenaire peut-il interroger l'imprimante multifonctions ou le parc d'imprimantes pour déterminer les niveaux des micrologiciels des périphériques et déterminer s'ils correspondent à vos politiques de sécurité ?
- ☐ Les configurations de sécurité peuvent-elles être facilement configurées et surveillées ? Les périphériques non conformes peuvent-ils être mis aux normes sans effort manuel supplémentaire ?
- ☐ Pouvez-vous consulter des documents confidentiels imprimés, copiés ou numérisés qui ne sont pas approuvés et être notifié d'un tel comportement ?
- ☐ Le partenaire peut-il fournir en temps réel une génération d'états continue par le biais d'un tableau de bord interactif afin d'indiquer des problèmes de conformité ou cas spécifiques à résoudre ?
- ☐ Les données sensibles sont-elles sécurisées via un contrôle d'accès basé sur les utilisateurs ou groupes d'utilisateurs, avec une protection par mot de passe, un chiffrement du contenu, et une rétention et mise au rebut automatisées du contenu ?

3. Trellix : anciennement une société de McAfee®.

TECHNOLOGIE BASÉE SUR LES NORMES

La sécurité des terminaux peut avoir un impact sur votre capacité à vous conformer aux exigences réglementaires et sectorielles.

- ☐ Les produits que les partenaires fournissent sont-ils conçus pour répondre aux normes et réglementations telles que l'HIPAA, la loi Sarbanes-Oxley, le Gramm-Leach-Bliley Act (GLBA), la directive américaine FDA 21 CFR Partie 11 et le RGPD ?
- ☐ Le partenaire travaille-t-il avec des fournisseurs qui recherchent une validation tierce de la sécurité des périphériques en participant au programme international des Critères Communs (ISO/IEC 15408) ?
- ☐ Ces fournisseurs soumettent-ils le périphérique entier à l'évaluation et pas seulement un kit de sécurité ? Cet aspect est important pour les entreprises de haute sécurité, comme les agences gouvernementales qui achètent des multifonctions avec des disques de stockage. Cela garantit qu'une protection supplémentaire est intégrée au périphérique.

Prise en charge d'un modèle Confiance zéro

AUTHENTIFICATION RÉSEAU

La sécurité s'améliore lorsque les administrateurs limitent l'accès aux utilisateurs en fonction de leur rôle/fonction.

- ☐ Les utilisateurs autorisés sont-ils obligés de se connecter à l'aide d'un mot de passe ou une carte d'identité pour accéder en toute sécurité aux fonctions du périphérique ?
- ☐ Ces sessions d'authentification et d'autorisation peuvent-elles être vérifiées ?
- ☐ Une Authentification unique (SSO) et une authentification multifacteur (MFA) ont-ils été mises en œuvre pour renforcer la sécurité ?

ACCÈS AUX INFORMATIONS

- ☐ L'utilisation du contenu confidentiel peut-elle être signalée et surveillée ?
- ☐ Est-il possible d'envoyer une notification d'un tel accès non autorisé ?
- ☐ Pouvez-vous limiter et suivre les personnes qui ont accès à des informations confidentielles ?
- ☐ Des contrôles sont-ils en place pour gérer ces informations sur les périphériques de sortie ?

POLITIQUE DE SÉCURITÉ DES PÉRIPHÉRIQUES

Envisagez l'accès aux ressources réseau, pas seulement aux informations.

- ☐ Avez-vous créé une politique de sécurité pour l'accès aux ressources réseau et l'impression depuis ces ressources ?
- ☐ Les données entrant et sortant des imprimantes multifonctions, sont-elles sécurisées via un chiffrement avancé ?

DIRECTIVES À L'INTENTION DES EMPLOYÉS

- ☐ Des mesures ont-elles été mises en place pour s'assurer que les employés comprennent et respectent les directives en matière de sécurité ?
- ☐ L'activité des employés qui ne respectent pas ces directives de sécurité est-elle suivie ?
- ☐ Disposez-vous d'une politique et d'un processus d'approbation des micrologiciels des périphériques avant leur déploiement ?
- ☐ Existe-t-il un processus pour déterminer la crédibilité des mises à niveau logicielles et pour valider les signatures numériques ?

Facteurs importants sur la sécurité des périphériques

VULNÉRABILITÉ DES PÉRIPHÉRIQUES

- ☐ Les périphériques sont-ils équipés d'un pare-feu réseau pour empêcher tout accès externe non autorisé à vos systèmes via une connexion réseau ?
- ☐ Existe-t-il des vulnérabilités susceptibles d'exposer vos périphériques à une attaque ?

- ☐ Des contrôles sont-ils en place pour protéger l'intégrité du micrologiciel du périphérique, tels que la signature numérique, le chiffrement et la vérification ?
- ☐ Les périphériques ont-ils une protection intégrée contre les logiciels malveillants ?
- ☐ Disposez-vous d'un moyen cohérent de vous assurer que les appareils sont conformes aux politiques relatives aux ressources réseau ?
- ☐ Disposez-vous d'un processus permettant d'accepter uniquement les comportements prévus au niveau des périphériques ?
- ☐ La gestion automatisée des certificats est-elle disponible ?
- ☐ Êtes-vous en mesure de sécuriser la communication entre vos périphériques et votre réseau ou les périphériques de vos employés ?

ASSURANCE DE CORRECTION

- ☐ Que se passe-t-il si un périphérique n'est plus conforme à la politique de sécurité ; êtes-vous averti lorsque cela se produit ?
- ☐ Existe-t-il des étapes spécifiques pour rétablir la conformité ?
- ☐ Disposez-vous d'une politique de correction ?
- ☐ Avez-vous un moyen de vérifier que la politique est en place ?
- ☐ Si une ressource réseau n'est plus conforme, pouvez-vous capturer les données nécessaires à l'établissement de rapports ?
- ☐ Existe-t-il une piste d'audit ?
- ☐ À partir des périphériques, est-il possible de transférer le journal d'audit vers un serveur SIEM ou vers un serveur de journaux d'audit ?

Facteurs de vulnérabilité des informations basées sur des documents

SÉPARATION TÉLÉCOPIE/RÉSEAU

- ☐ Les connexions de télécopie non protégées constituent une porte d'entrée potentielle dans votre réseau. Existe-t-il une séparation complète entre les lignes téléphoniques et les connexions de télécopie en réseau ?

ÉCRASEMENT D'IMAGE

- ☐ Les périphériques peuvent-ils être configurés pour écraser automatiquement les fichiers stockés sur les disques de stockage ?
- ☐ Avez-vous une politique documentée sur la façon dont vous purgez ou détruisez les disques de stockage des machines mises hors service ?

Sécurité tout au long du cycle de vie du périphérique

PROGRAMME DE CORRECTIFS DE SÉCURITÉ ET COMMUNICATIONS S'Y RAPPORTANT

- ☐ Disposez-vous d'un fournisseur de solutions de sécurité qui propose un programme actif de correctifs de sécurité ? À ce titre, il surveille la survenue de nouvelles vulnérabilités sur les périphériques, tout comme les développeurs de logiciels OS surveillent la survenue de nouveaux virus qui ciblent les logiciels.
- ☐ Votre fournisseur de solutions de sécurité publie-t-il des bulletins de sécurité lorsque des correctifs sont apportés aux vulnérabilités des produits/logiciels ?
- ☐ Pouvez-vous vous inscrire aux flux RSS et recevoir des alertes immédiates lorsque de nouveaux bulletins et correctifs sont publiés ?
- ☐ Le fournisseur a-t-il mis en place un programme Bug Bounty pour aider à détecter les vulnérabilités potentielles ?

RETRAIT DU DISQUE DE STOCKAGE

- ☐ Avez-vous d'un partenaire du Service de gestion d'impression (MPS) qui formule des recommandations sur la manière la plus efficace d'éliminer les données dans les disques de stockage ?
- ☐ Votre méthodologie pour purger/détruire les disques de stockage des machines mises hors service est-elle conforme à la norme NIST SP 800-88r1 ?
- ☐ Les reprises et les retours qui seront remis à neuf sont-ils réécrits ou reformatés ?

Si vous n'avez pas coché tous les éléments de cette liste, vous aurez peut-être besoin d'un partenaire pour vous aider à y parvenir. Pour en savoir plus sur les solutions de sécurité complètes et de premier ordre que nous proposons, consultez la page **www.xerox.fr/fr-fr/qui-sommes-nous/solutions-de-securite**

Pour planifier une évaluation complète de l'environnement de travail, rendez-vous sur **www.xerox.fr/fr-fr/services/formulaire-evaluation-digitale**

À propos de Xerox

À l'ère du travail hybride, nous ne faisons pas que réfléchir à l'avenir, nous le façonnons. Xerox Corporation est un leader technologique axé sur la convergence des mondes physique et numérique. Nous utilisons l'automatisation et la personnalisation de nouvelle génération pour redéfinir la productivité, stimuler la croissance et rendre le monde plus sûr. Chaque jour, nos technologies innovantes et nos solutions de travail intelligentes Optimisés par Xerox® aident le monde à mieux communiquer et mieux travailler. Pour en savoir plus, consultez le site **www.xerox.fr** et suivez-nous sur Twitter **@Xerox**.

xerox™