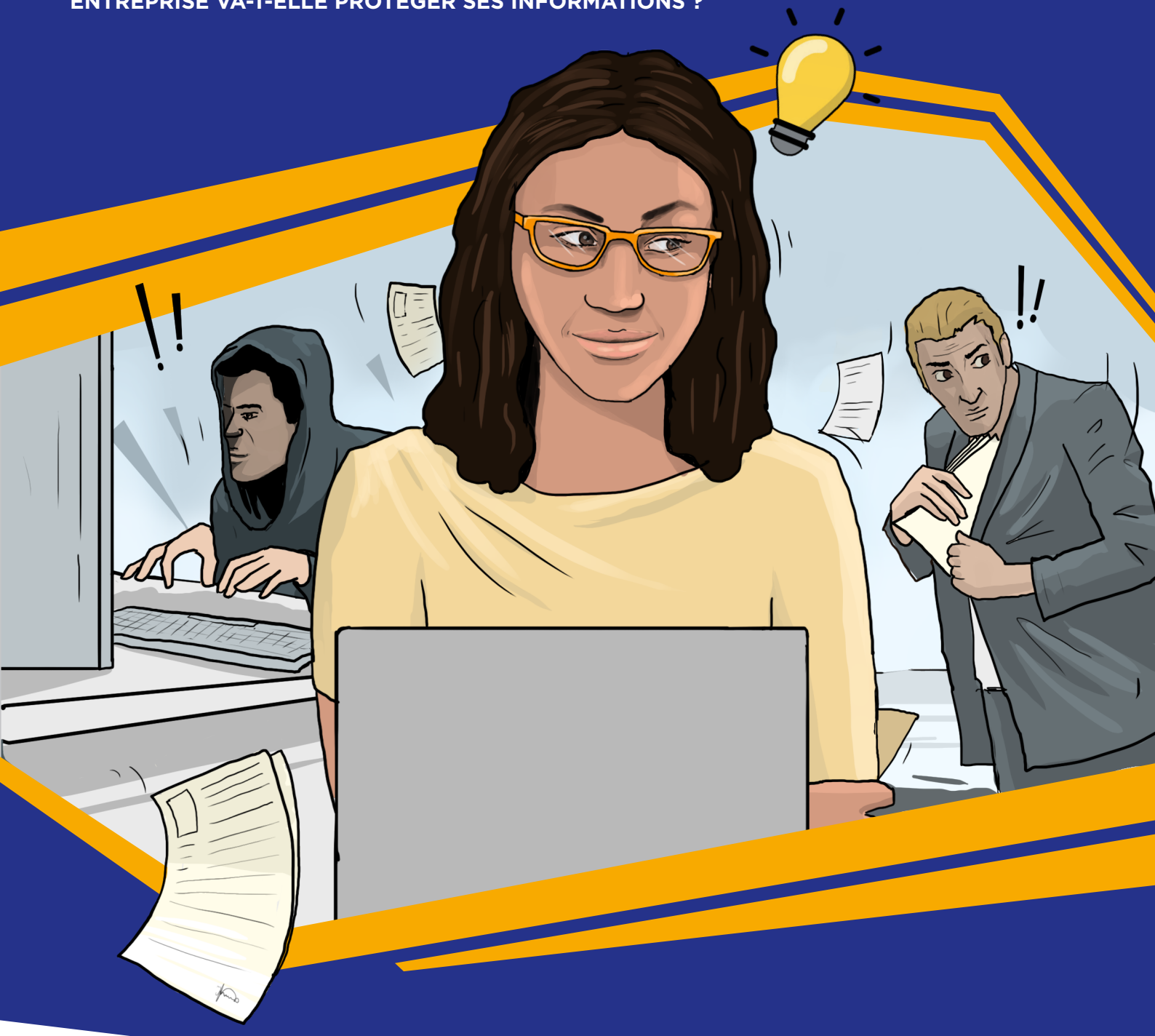
SÉCURITÉ DES INFORMATIONS
À L'ŒUVRE !

DANS UN MONDE OÙ LES CYBERMENACES DEVIENNENT DE PLUS EN PLUS INTELLIGENTES ET OÙ LA CONFORMITÉ DEVIENT DE PLUS EN PLUS COMPLEXE, COMMENT VOTRE ENTREPRISE VA-T-ELLE PROTÉGER SES INFORMATIONS ?



Canon

INDEX

Les données constituent le trésor de toute entreprise moderne. Elles dynamisent votre service financier, donnent à votre équipe de direction des pouvoirs prédictifs et fournissent à vos employés davantage d'informations stratégiques.

Cette précieuse ressource doit être protégée à tout prix.

Alors que ce trésor ne cesse de prendre de la valeur, le nombre d'ennemis qui tentent de s'en emparer augmente également : des attaquants malveillants attendent à l'extérieur pour voler des informations au moment où vous vous y attendez le moins. Dans le même temps, des agents doubles peuvent chercher à s'approprier ce trésor.

Mais un ennemi ne suffit pas pour faire tomber une entreprise.

Une grande puissance veille sur le territoire, veillant à ce que chacun respecte les règles de conformité des données. Toutefois, même si les lois sont strictes et les punitions sévères, il n'a jamais été aussi facile de faire une erreur.

Les entreprises d'aujourd'hui ne sont pas une ville fortifiée ; elles ne sont pas même situées en un seul et même endroit. Avec le travail hybride, les employés stockent, partagent et collaborent sur des informations dispersées sur plus de sites que jamais auparavant.

Dans un environnement de travail aussi complexe, assurer la sécurité de vos informations et la conformité de vos processus peut sembler un défi impossible.

Vous avez besoin d'un partenaire de confiance qui peut sécuriser votre trésor, vous protéger des pirates et aider vos collaborateurs à rester en conformité envers et contre tous.

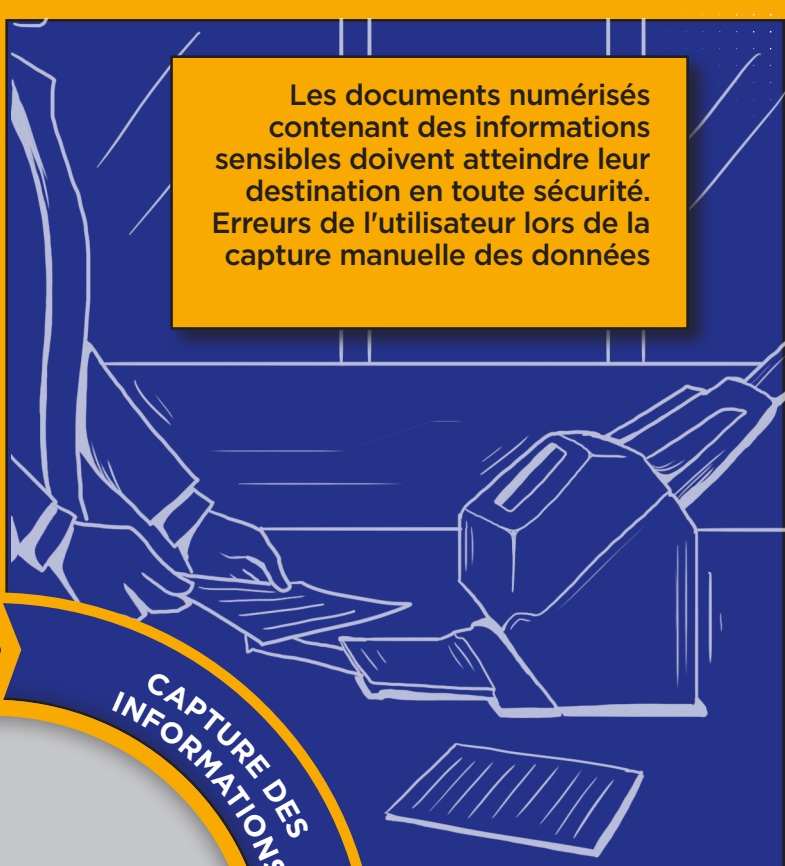
Découvrons comment Canon et nos armes secrètes peuvent vous aider à relever le défi.

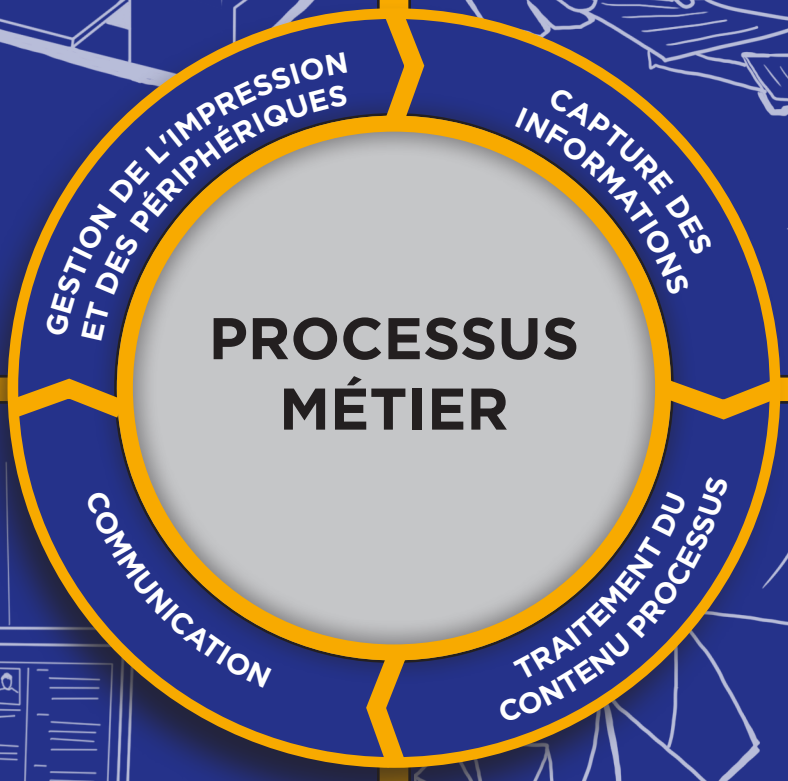
DÉFIS RENCONTRÉS AU COURS DU CYCLE DE VIE DES DOCUMENTS

Au cours de leur cycle de vie au sein de votre entreprise, des documents sont créés, copiés, stockés et partagés. Toutes ces étapes posent des difficultés pour garantir la sécurité et la conformité des données qu'ils contiennent.

L'impression représente un défi en termes de sécurité et de conformité, car il est difficile d'avoir une visibilité complète sur l'activité d'un utilisateur ou d'un document, ce qui peut entraîner des violations de données

Les documents numérisés contenant des informations sensibles doivent atteindre leur destination en toute sécurité. Erreurs de l'utilisateur lors de la capture manuelle des données





Les données personnelles et les informations sensibles des clients et des employés doivent être stockées, traitées et détruites en toute sécurité, conformément aux règles de confidentialité des données

Les communications, données et documents sortants doivent être gérés en toute sécurité pour éviter les problèmes de conformité des informations

DÉFI 1

LA STRATÉGIE SECRÈTE

L'entreprise X a un grand secret : elle est prête à se lancer dans une nouvelle aventure. L'équipe de direction a décidé d'investir dans un nouveau domaine d'activité dans l'espoir d'acquérir un nouveau pouvoir et de découvrir des richesses incalculables.

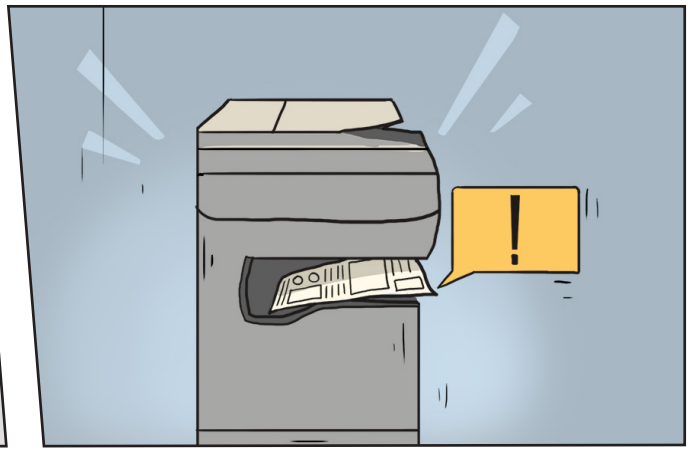
Il est primordial que ces plans restent secrets jusqu'à ce qu'ils soient rendus publics. La nouvelle dévoilerait l'intention de l'entreprise X à ses rivaux, les avertissant qu'il y a un nouveau concurrent à l'horizon. Par ailleurs, l'enjeu pour les employés de l'entreprise X est de taille : pourrait-il y avoir de nouvelles opportunités dans leur département ? De nouveaux secteurs d'activité à explorer ? Ou leurs emplois sont-ils menacés ?

L'équipe de direction doit procéder avec prudence si elle veut s'assurer que ses plans restent hors de portée des employés conspirateurs et des ennemis externes. Tout au long du processus de budgétisation et d'annonce, ils doivent éviter une série de pièges, des menaces internes aux logiciels malveillants en passant par les attaques réseau. Sont-ils capables de garder leur secret en sécurité ?

L'équipe de communication a rédigé un communiqué de presse reflétant la nouvelle orientation stratégique de l'entreprise. L'information est toujours confidentielle et l'annonce est en cours de rédaction et d'approbation par un petit groupe de cadres supérieurs. Selma, la directrice financière, a demandé d'examiner une copie physique du document. Polina, son assistante est prête à l'imprimer pour elle.

L'impression représente une réelle menace pour la sécurité et les entreprises n'en ont pas conscience. Les risques types de sécurité et de conformité incluent les documents papier retirés de l'imprimante avant qu'ils ne soient collectés par la personne qui les a imprimés, ou ceux oubliés : dans les deux cas, des informations sensibles ou confidentielles sont susceptibles d'être consultées par des personnes non autorisées.

L'innovation a également ouvert la voie à une série de nouvelles menaces de sécurité. Les imprimantes multifonctions modernes sont aussi puissantes qu'un PC, équipées d'un disque dur, d'une mémoire et d'une unité centrale de traitement (CPU), et sont souvent connectées à Internet. Par conséquent, il est possible que le micrologiciel de l'imprimante soit ciblé par des pirates qui tentent d'accéder au réseau et aux données de l'entreprise.



ARMES SECRÈTES

imageRUNNER ADVANCE DX C5800

L'imageRUNNER ADVANCE DX C5800 est conçue avec une sécurité intégrée de série. Polina ne peut imprimer le document qu'en se connectant au périphérique à l'aide de sa carte d'identification. Par conséquent, personne d'autre ne peut accéder au document en attente d'impression et il ne pourra donc pas être oublié dans le bac du périphérique.

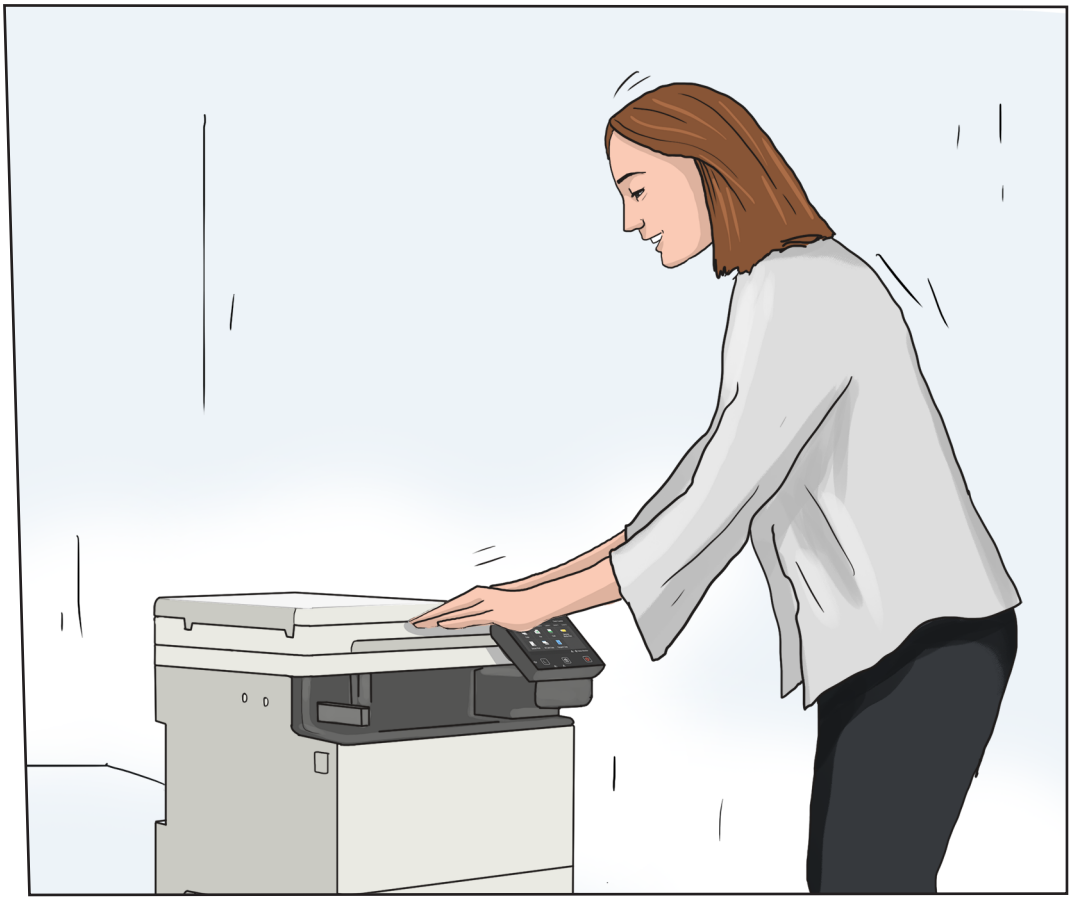
Le logiciel McAfee Embedded Control, proposé par Trellix, est également installé sur l'imprimante. Ce dernier protège contre les attaques de type « zero-day » et les menaces persistantes avancées (APT) en bloquant l'exécution d'applications non autorisées grâce à une liste blanche intelligente. Pour empêcher un pirate d'obtenir le communiqué de presse via une attaque réseau, McAfee Embedded Control protège contre le piratage du programme.

Enfin, l'imageRUNNER ADVANCE DX C5800 prend en charge l'intégration de la gestion des événements et des informations de sécurité (SIEM), ce qui permet aux entreprises d'inclure plus facilement des imprimantes dans leurs systèmes de surveillance de sécurité existants (Syslog, par exemple). Ces systèmes peuvent reconnaître et signaler les événements de sécurité sur une flotte de périphériques en temps réel, alertant l'entreprise de tout problème ou menace au fur et à mesure qu'ils surviennent.

Service de renforcement des appareils
Avec Canon, la sécurité commence avant même que vous n'ayez acheté un périphérique. Nous configurons les multifonctions imageRUNNER ADVANCE afin de renforcer leur sécurité, notamment grâce au renforcement des contrôles de sécurité intégrés et au blocage des fonctions non essentielles et des ports non sécurisés. Le périphérique configuré est contrôlé et vérifié avant d'être expédié.

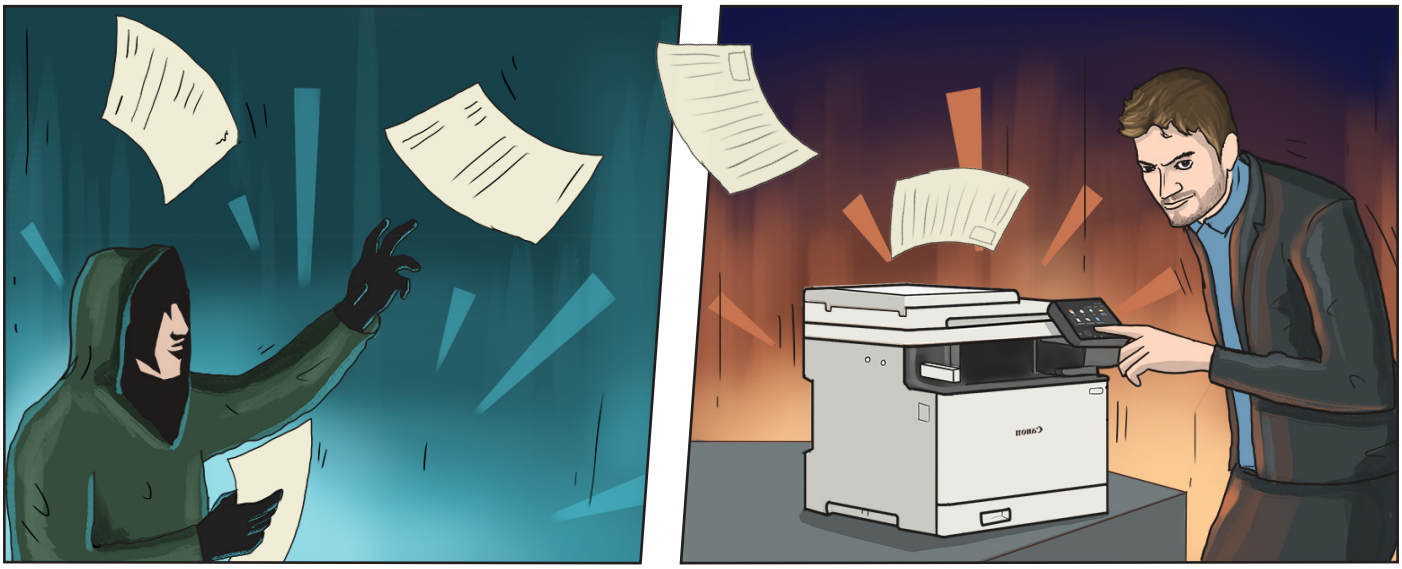
imageWARE Secure Audit Manager Express
Cette solution de sécurité des périphériques réseau permet à l'entreprise X de surveiller ses activités liées aux documents. Elle permet de capturer, d'archiver et d'auditer les activités qui se produisent sur les périphériques Canon. Lorsque Polina imprime le communiqué de presse, imageWARE Secure Audit Manager Express envoie une alerte par e-mail au service informatique indiquant qu'un document à haut risque est en cours d'impression. Cela permet à l'entreprise X de savoir si un employé ou une personne non autorisée tente de copier ou d'imprimer des informations sensibles.

Selma a examiné le communiqué de presse et fourni quelques commentaires écrits. Polina doit faire part de ses commentaires à Pierre, le responsable des relations publiques en charge de l'annonce. Comme Pierre travaille depuis son domicile, Polina devra créer une copie numérique pour la lui envoyer. La numérisation de documents et leur envoi par e-mail directement depuis le périphérique créent une opportunité pour le pirate d'intercepter le document.



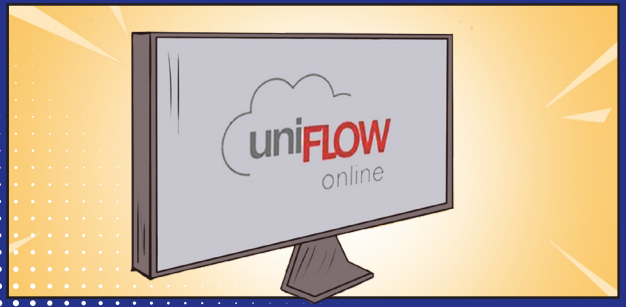
Les périphériques de numérisation actuels sont souvent connectés à Internet, ce qui permet aux utilisateurs d'envoyer des documents par e-mail directement à un destinataire ou de les enregistrer dans des destinations cloud. Par conséquent, les informations numériques sont de plus en plus menacées. Il est donc crucial que les périphériques de numérisation disposent de fonctions de sécurité robustes. Sans fonctions sécurisées, un scanner est susceptible d'être piraté - un utilisateur interne pourrait modifier les files d'attente de routage des e-mails pour diriger un travail d'e-mail vers un utilisateur non autorisé, par exemple. Ou, sans cryptage, un document peut simplement être ouvert, modifié ou imprimé.

De l'extérieur, un pirate pourrait également accéder au scanner via le réseau et apporter des modifications aux répertoires de messagerie, permettant l'envoi d'un document à des destinataires extérieurs à l'entreprise. Ou il pourrait également intercepter un document transmis via HTTPS si celui-ci et ses données ne sont pas cryptés.



ARMES SECRÈTES

i-SENSYS X C1333iF
Selma est prête à numériser le document à l'aide de l'i-SENSYS X C1333iF. Ce périphérique multifonction (combinant les fonctionnalités d'impression et de numérisation) offre des fonctions de numérisation sécurisées qui contribuent à la sécurité des informations. Dès qu'il est mis sous tension, sa fonction de vérification du système au démarrage vérifie s'il y a eu des tentatives de compromettre l'intégrité du périphérique et peut alerter Selma s'il a été piraté. Selma doit ensuite se connecter à l'aide d'une carte d'identification. Cette dernière permet de s'assurer qu'un enregistrement de la personne qui copie ou partage des informations existe bel et bien. Enfin, la prise en charge IEEE802.1X de l'i-SENSYS X C1333iF fournit un mécanisme d'authentification. Ainsi, lorsqu'il se connecte au LAN ou au WLAN de l'entreprise, il fournit une confirmation de son authenticité.



uniFLOW Online
Lorsque Selma numérise le contrat, uniFLOW Online crée un PDF crypté et propose une protection par mot de passe en option. Cela empêche les utilisateurs non autorisés de visualiser, modifier ou imprimer le document, et protège ainsi les informations de toute personne qui tenterait de les intercepter.

Tobias a entendu dire que l'entreprise pourrait prendre une nouvelle direction. En tant que chef de l'une des équipes en difficulté dans le cadre de la stratégie actuelle, il sait que cela pourrait impliquer de sérieuses coupes dans son budget cette année, voire une menace pour l'emploi.

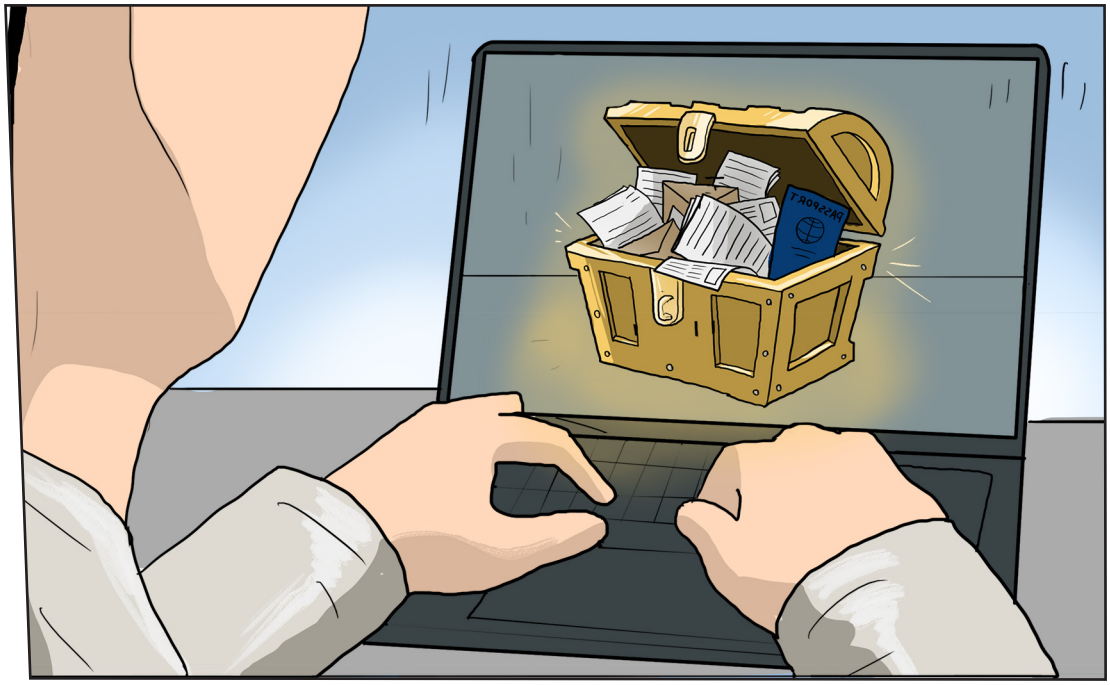
Tobias est frustré par la nouvelle. Il décide donc de chercher des informations lui permettant de confirmer la véracité des rumeurs et pourrait éventuellement avertir ses collègues. Comme il pense savoir où les hauts dirigeants stockent leurs documents financiers, il commence secrètement à chercher toutes les informations qui pourraient avoir un lien avec les nouveaux plans.

Chaque année, les entreprises créent et stockent de plus en plus d'informations. En raison des nombreux modèles hybrides actuels, ces informations sont réparties sur un nombre croissant de sites, à la fois physiquement et virtuellement. Par conséquent, les entreprises sont confrontées à des stratégies de stockage aléatoires, avec des employés qui utilisent différents systèmes, des classeurs aux services de stockage cloud personnels tels que Dropbox pour héberger les données de l'entreprise.
De plus, les employés traitent fréquemment des informations sensibles telles que les contrats, les coordonnées bancaires du personnel et les résultats financiers de l'entreprise. Même avec des données critiques comme celles-ci, il est presque impossible pour les équipes informatiques d'assurer une gestion des informations conforme aux meilleures pratiques lorsque les documents sont stockés de cette manière.

ARMES SECRÈTES

Therefore Online
La sécurité intégrée robuste de la solution Therefore Online permet aux entreprises de définir des politiques automatisées concernant les personnes pouvant accéder aux documents et la manière dont les informations sont stockées, partagées ou modifiées. Les contrôles d'accès empêchent les employés non autorisés tels que Tobias d'ouvrir des documents privés ou sensibles comme le communiqué de presse.

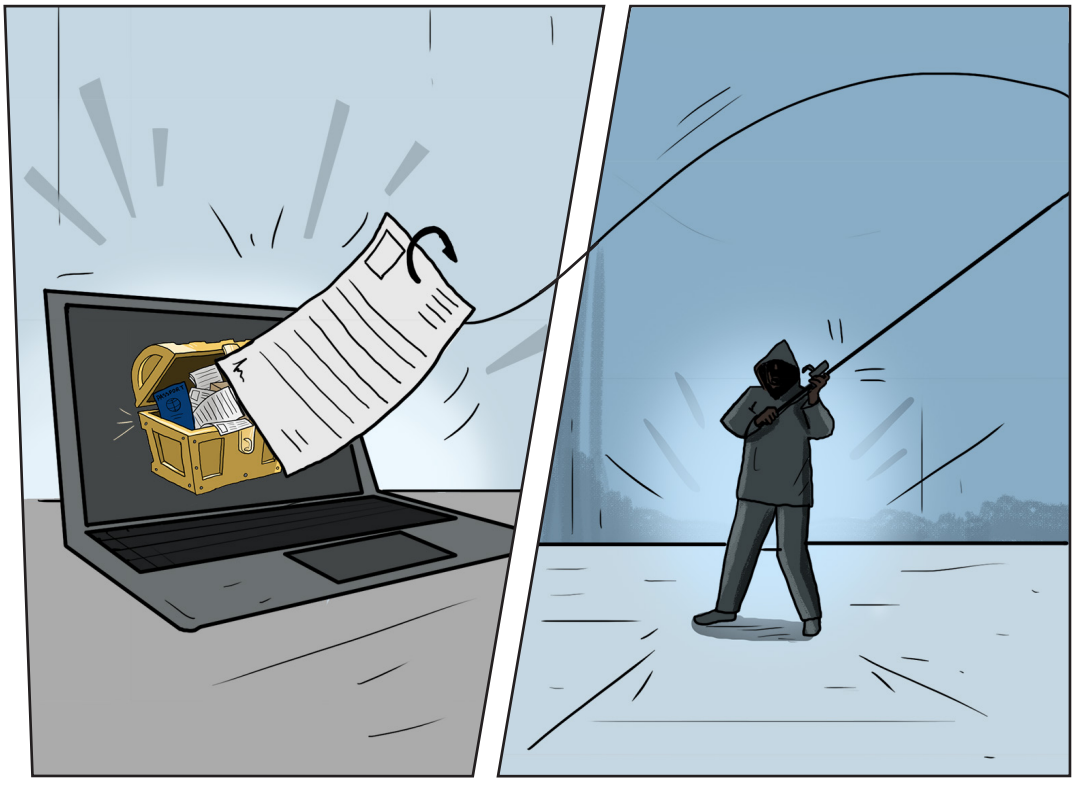
La solution Therefore Online est basée sur le cloud, et garantit que l'emplacement d'un utilisateur n'a pas d'impact sur l'accessibilité ; les utilisateurs autorisés qui travaillent à domicile ou sont en déplacement peuvent toujours accéder aux documents critiques. Toute interaction avec un document fait l'objet d'un suivi ; ce dernier offre la garantie que les informations sont étroitement gérées et visibles de bout en bout, et fournit une piste d'audit numérique.



Pierre se prépare à envoyer l'annonce sous embargo aux destinataires, y compris les actionnaires clés et les journalistes sélectionnés. Il est primordial que le document ne soit envoyé qu'à ces contacts ; il ne peut pas risquer qu'il finisse entre de mauvaises mains.

En attendant, il doit faire attention aux informations supplémentaires que l'entreprise X garde confidentielles. La base de données de l'entreprise contient d'innombrables trésors : des données sensibles sur les destinataires, notamment leurs adresses électroniques, numéros de téléphone et, dans le cas des journalistes, les données de leurs passeports utilisés lors de précédents voyages.

Ces données constituent un butin potentiel pour les pirates qui pourraient utiliser ces informations d'identification pour divulguer l'annonce plus tôt ou, s'ils le souhaitaient, utiliser les coordonnées des individus dans la base de données pour effectuer un vol d'identité ou orchestrer des attaques de phishing.

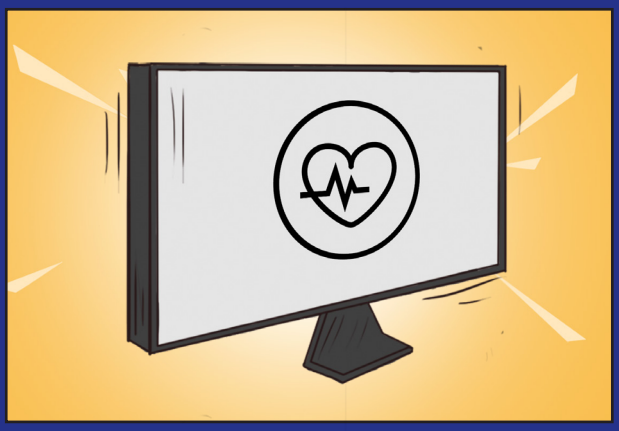


Les entreprises détiennent souvent des informations hautement personnelles et confidentielles sur leurs clients, partenaires et autres parties avec lesquelles elles travaillent en étroite collaboration. Ces informations ne sont pas seulement contenues sur les serveurs de l'entreprise, mais sont incluses dans les communications sortantes telles que les relevés bancaires, les factures et la correspondance avec ces parties.

La détention de ces informations représente un risque pour l'entreprise, car si elles étaient perdues ou volées par des pirates, cela l'exposerait à des amendes importantes et constituerait une atteinte à sa réputation. Dans l'intervalle, si une entreprise communique avec ces contacts, il est crucial que les informations personnelles contenues dans ces communications n'atteignent que le destinataire.

ARMES SECRÈTES

Vérification de l'intégrité du réseau
La vérification de l'intégrité du réseau aide les entreprises à examiner leur environnement informatique pour s'assurer qu'il est sécurisé dès le départ. L'expert mondial en cybersécurité NCC Group effectuera une analyse à distance de l'infrastructure informatique interne et externe de l'entreprise, notamment les canaux de communication et les ports, afin de mettre en lumière tout type de vulnérabilité. En identifiant les problèmes, l'entreprise peut éviter qu'ils ne soient exploités par un pirate potentiel, et empêcher l'interception des communications de Pierre, ou le vol de données des journalistes ou des parties prenantes dans les bases de données de l'entreprise X.



uniFLOW sysHUB
uniFLOW sysHUB offre aux utilisateurs un contrôle et une surveillance stricts de leurs communications avec les clients, ce qui permet à Pierre de s'assurer plus facilement que la communication atteint la bonne destination. Cette solution consolide les processus de communications internes et les applications en un seul workflow, géré à partir d'un point d'opération unique. uniFLOW sysHUB automatise ensuite ce workflow pour le rendre plus efficace et réduire le risque d'erreur. Chaque étape du workflow est enregistrée et stockée dans une bibliothèque sysHUB pour un examen ultérieur et pour prendre en charge les pistes d'audit, ce qui rend difficile pour un membre du personnel de divulguer délibérément un document sans qu'il soit enregistré. Par ailleurs, Pierre peut vérifier la preuve de livraison pour s'assurer que la communication est parvenue à la bonne personne.

DÉFI 2

L'EMBAUCHE CONFIDENTIELLE

L'entreprise Y doit attirer de nouveaux collaborateurs pour développer son royaume en pleine expansion. Auparavant, sa main-d'œuvre était basée sur un seul site, mais grâce au travail hybride, ses collaborateurs intrépides errent à travers le pays. L'équipe RH toujours très sollicitée a dû s'adapter rapidement. Les nouvelles recrues sont désormais inscrites via des processus d'embauche et d'intégration virtuels. L'équipe RH doit avoir des yeux partout, communiquer sur de grandes distances pour partager des documents confidentiels liés aux nouveaux arrivants.

Le pouvoir non négligeable de l'équipe RH s'accompagne d'une grande responsabilité : elle a en sa possession une montagne d'informations précieuses et sensibles, des données salariales, à l'état de santé des salariés en passant par leurs dossiers de performance. L'équipe RH sait qu'il lui incombe de conserver ces informations en toute sécurité et conformément à la législation en matière de conformité. Les auditeurs sont toujours à l'horizon et l'équipe RH sait qu'elle devra démontrer comment les informations sont stockées et partagées. La tâche est complexe. Bien que l'équipe RH travaille d'arrache-pied, elle n'est pas dotée de superpouvoirs. Les accidents et les erreurs peuvent être vraiment problématiques pour l'équipe.

Sans de bonnes solutions technologiques en place pour sauver la situation, cela pourrait causer des problèmes à l'entreprise Y.

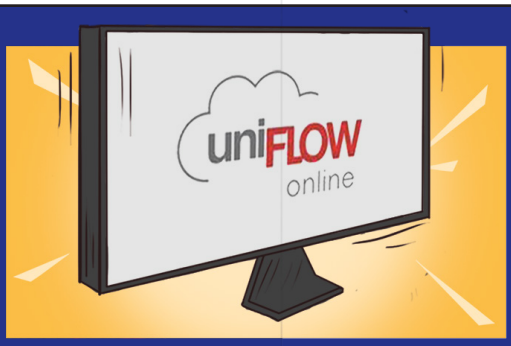
Après un processus d'entretien réussi, l'entreprise a accepté d'embaucher un nouvel employé. Le candidat s'est rendu au siège social pour remettre son passeport et signer son contrat avec Fatima, la responsable du recrutement. Fatima souhaite faire des copies des documents pour ses dossiers et les partager avec le responsable des RH qui travaille à domicile. Il est facile pour Fatima de saisir accidentellement le mauvais destinataire ou d'enregistrer le document dans un lieu accessible à tous. Si la mauvaise personne le recevait, elle pourrait simplement ouvrir le document capturé pour accéder aux informations.

Les entreprises ont la responsabilité de s'assurer que tous les documents numérisés ne sont vus que par les personnes autorisées à les consulter. Une simple erreur pourrait entraîner une perte ou une violation potentielle des données, ce qui pourrait avoir de graves répercussions sur la conformité.

Si l'entreprise ne se rend pas compte qu'elle a subi une violation grave et ne la signale pas, le régulateur de la protection des données peut imposer une amende pouvant aller jusqu'à 4 % de son chiffre d'affaires mondial.

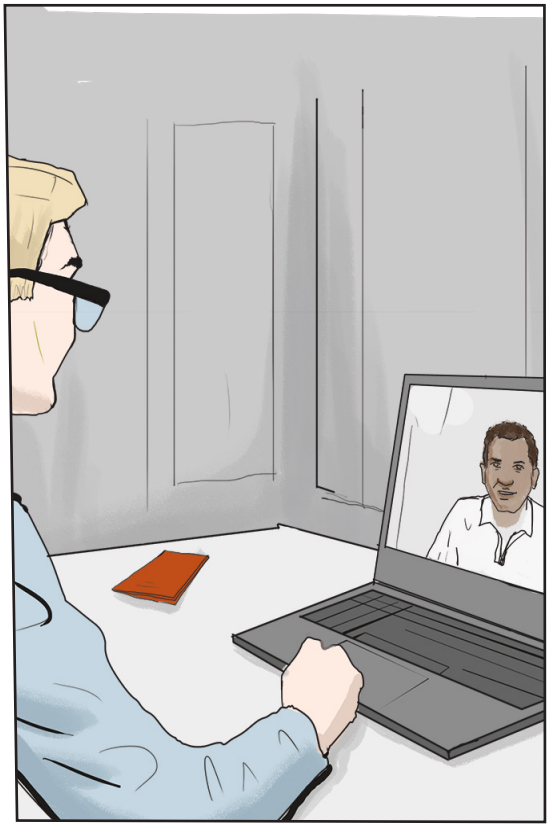
ARMES SECRÈTES

uniFLOW Online
uniFLOW Online propose des workflows de numérisation sécurisés intégrés qui permettent à l'entreprise Y de préconfigurer des workflows de numérisation spécifiques pour chaque utilisateur. Les workflows documentaires tels que l'intégration de nouvelles ressources sont déjà prédéfinis, ce qui empêche Fatima d'enregistrer le scan d'une nouvelle recrue dans une destination incorrecte.



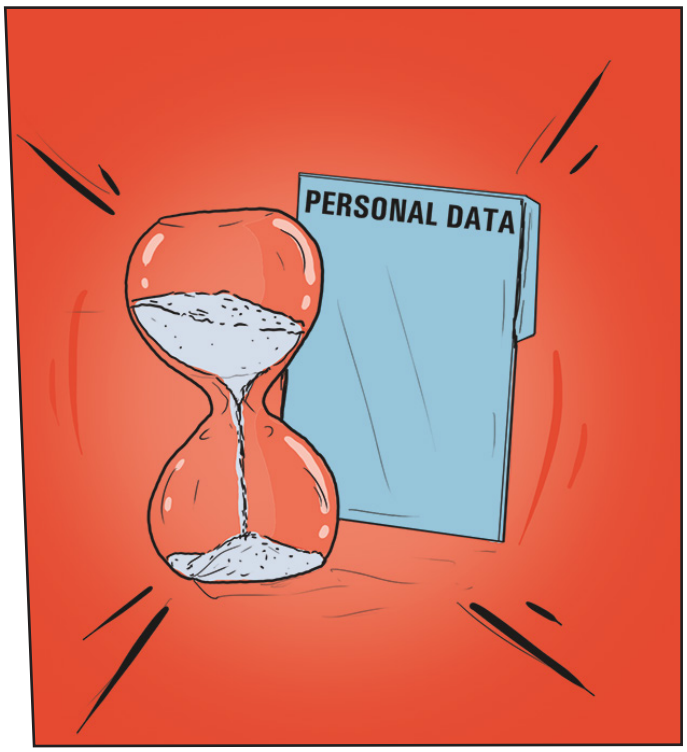
imageFORMULA DR-S150
Fatima est prête à numériser le document à l'aide de l'imageFORMULA DR-S150. Ce scanner offre des fonctionnalités sécurisées qui permettent de protéger les informations : il nécessite que tout utilisateur se connecte à l'aide d'une carte d'identification, garantissant que seule Fatima peut accéder au document qui a été capturé. Il applique également automatiquement le cryptage à la version numérisée. Ainsi, seul un destinataire disposant d'un mot de passe peut le lire, le modifier et l'imprimer. Les périphériques imageFORMULA DR-S150 offrent également des options pour envoyer des documents via des protocoles sécurisés tels que la numérisation vers FTPS, SFTP et SMTPS.

IRISPowerscan
La société dispose également d'IRISPowerscan. Par conséquent, une fois les documents numérisés, ils sont automatiquement identifiés en tant que passeport et contrat. Le logiciel corrige tous les défauts de numérisation tels que les désalignements et utilise la reconnaissance optique de caractères pour détecter les détails clés tels que le nom de l'employé et le numéro de son passeport. Ces informations sont ajoutées à l'indexation, ce qui permet à l'entreprise de les retrouver plus facilement ultérieurement. De plus, IRISPowerscan achemine automatiquement les numérisations de contrats et de passeports vers le bon emplacement de stockage sécurisé sur le système de l'entreprise.



Au cours du processus de recrutement, plusieurs employés – dont Fatima et Nick, un collègue – ont été impliqués dans les entretiens avec les candidats et l'examen des CV. Les deux employés sont basés virtuellement et travaillent sur différents sites en Europe. Fatima et Nick ont tous deux des copies des CV des candidats et des notes sur leurs entretiens stockés sur leurs ordinateurs portables personnels et dans des emplacements Dropbox partagés. Une fois que le nouveau candidat est embauché, Fatima et Nick peuvent facilement oublier de supprimer l'un de ces documents.

La législation récemment renforcée prouve que la conformité n'a jamais été aussi importante. Des lois telles que le RGPD ont introduit des règles spécifiques régissant la manière dont les informations doivent être stockées - par exemple, les entreprises ne doivent pas conserver les informations personnellement identifiables plus longtemps que le strict nécessaire. Pourtant, nombre d'entre elles doivent lutter contre des stratégies de stockage aléatoires, sans emplacements officiels pour stocker des documents ou la possibilité de localiser des documents enregistrés sur leurs propres serveurs. Si un ex-employé, voire un ancien candidat, faisait une demande d'accès à des informations personnelles auprès de l'entreprise, il serait très difficile pour cette dernière de déclarer les informations dont elle dispose. De plus, à des fins d'audit, l'entreprise aurait du mal à démontrer qu'elle contrôle l'endroit où les informations personnellement identifiables sont stockées.

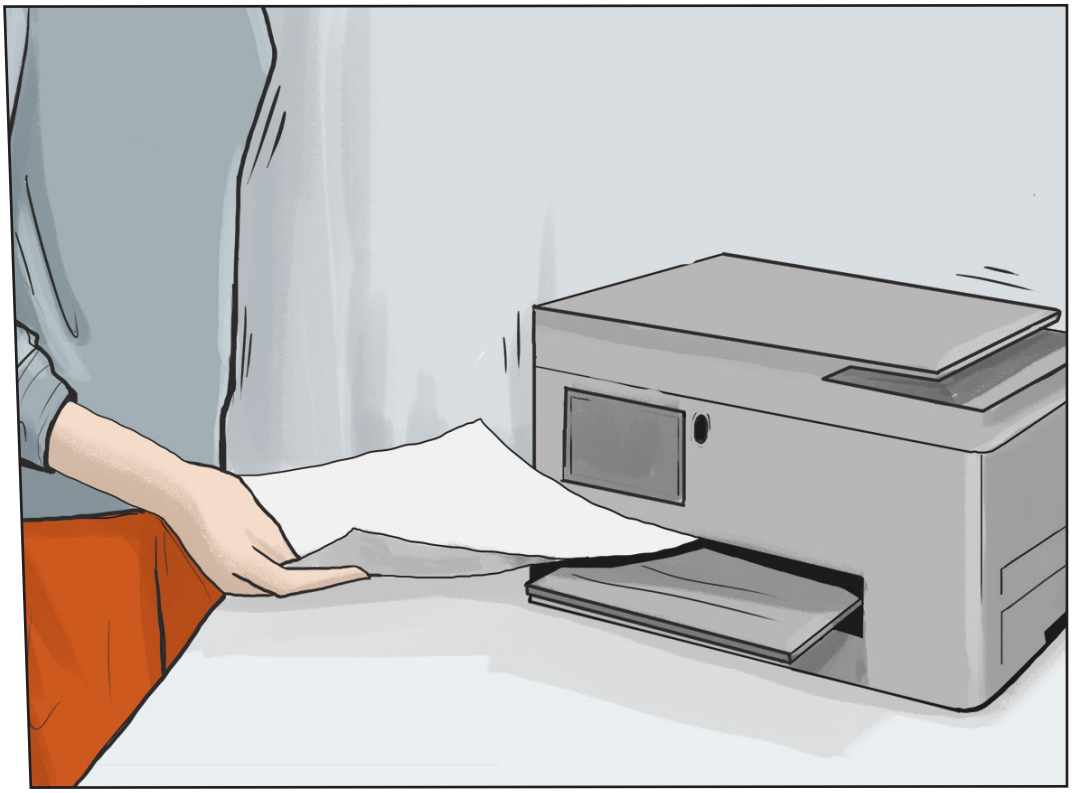


ARMES SECRÈTES

Therefore Online
La sécurité intégrée robuste de la solution Therefore Online permet aux entreprises de définir des politiques automatisées concernant les personnes pouvant accéder aux documents et la manière dont les informations sont stockées, partagées ou modifiées. La solution permet de suivre chaque interaction avec un document, en gardant les informations étroitement gérées et visibles de bout en bout, ce qui rend le processus d'audit beaucoup plus simple.

Pour garantir la conformité, l'entreprise Y peut également définir des politiques de conservation automatiques pour s'assurer que les anciens documents contenant des informations sensibles sont supprimés après une période de conservation appropriée. La solution Therefore Online étant basée sur le cloud, même lorsque les équipes ne sont pas sur site, elles peuvent toujours télécharger des documents et être assurées qu'ils sont sûrs et sécurisés.

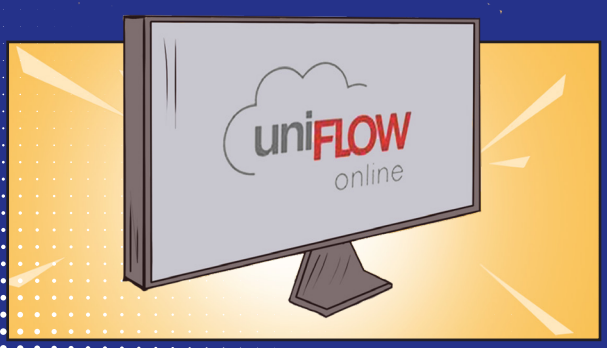
Ingrid, la nouvelle responsable hiérarchique de l'employé, travaille à domicile et se prépare à organiser un entretien d'intégration au bureau le lendemain. Elle souhaite imprimer une copie de la lettre confirmant le salaire de la nouvelle recrue, ainsi que d'autres formulaires, à partager avec elle au cours de ce processus. Ingrid n'a commencé à travailler à domicile que récemment et n'a pas reçu d'imprimante de la part de son employeur, elle utilise donc son imprimante personnelle.



Les entreprises oublient facilement que les imprimantes jouent un rôle important dans la sécurité et la conformité des workflows, car ces périphériques contiennent des données et des documents précieux. Dans le cadre des obligations légales de conformité, les entreprises doivent fournir des pistes d'audit qui indiquent la manière dont les informations sensibles sont utilisées. Cela les oblige à avoir une plus grande visibilité et un meilleur suivi de la façon dont les documents interagissent avec les périphériques. Cependant, comme Ingrid utilise son imprimante personnelle, celle-ci n'est pas connectée au réseau de l'entreprise – il n'y a donc aucune traçabilité, aucun enregistrement des données stockées sur le périphérique et aucune garantie quant à sa sécurité.

ARMES SECRÈTES

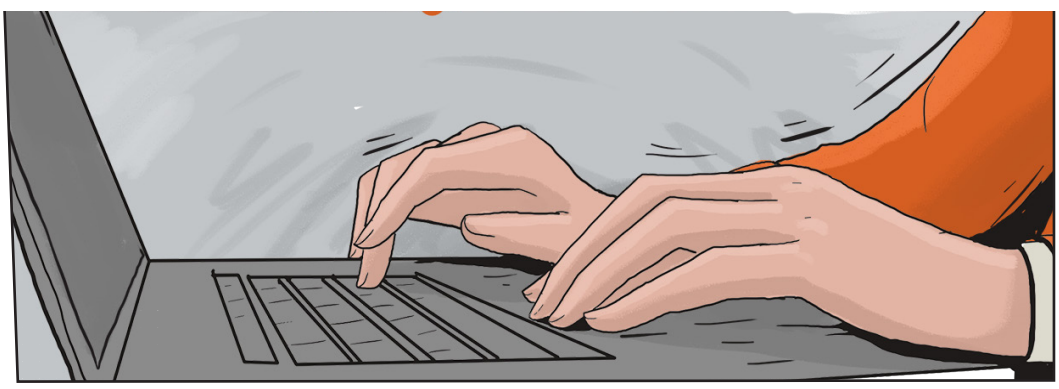
MAXIFY GX6050
Cette imprimante de bureau efficace produit des impressions de haute qualité pour les travailleurs à domicile, mais elle contribue également à la sécurité et à la conformité des documents grâce à son intégration embarquée à uniFLOW Online. La fonction « Scan to Myself » empêche Ingrid d'envoyer des documents à qui que ce soit d'autre qu'à son adresse électronique ou à son dossier personnel, afin d'éviter qu'elle n'envoie accidentellement des documents professionnels à des contacts personnels. Grâce à la fonction d'envoi sécurisé des travaux d'impression, Ingrid imprime les documents uniquement lorsqu'elle est prête. Cela permet d'éviter que les documents professionnels sensibles soient oubliés sur le périphérique.



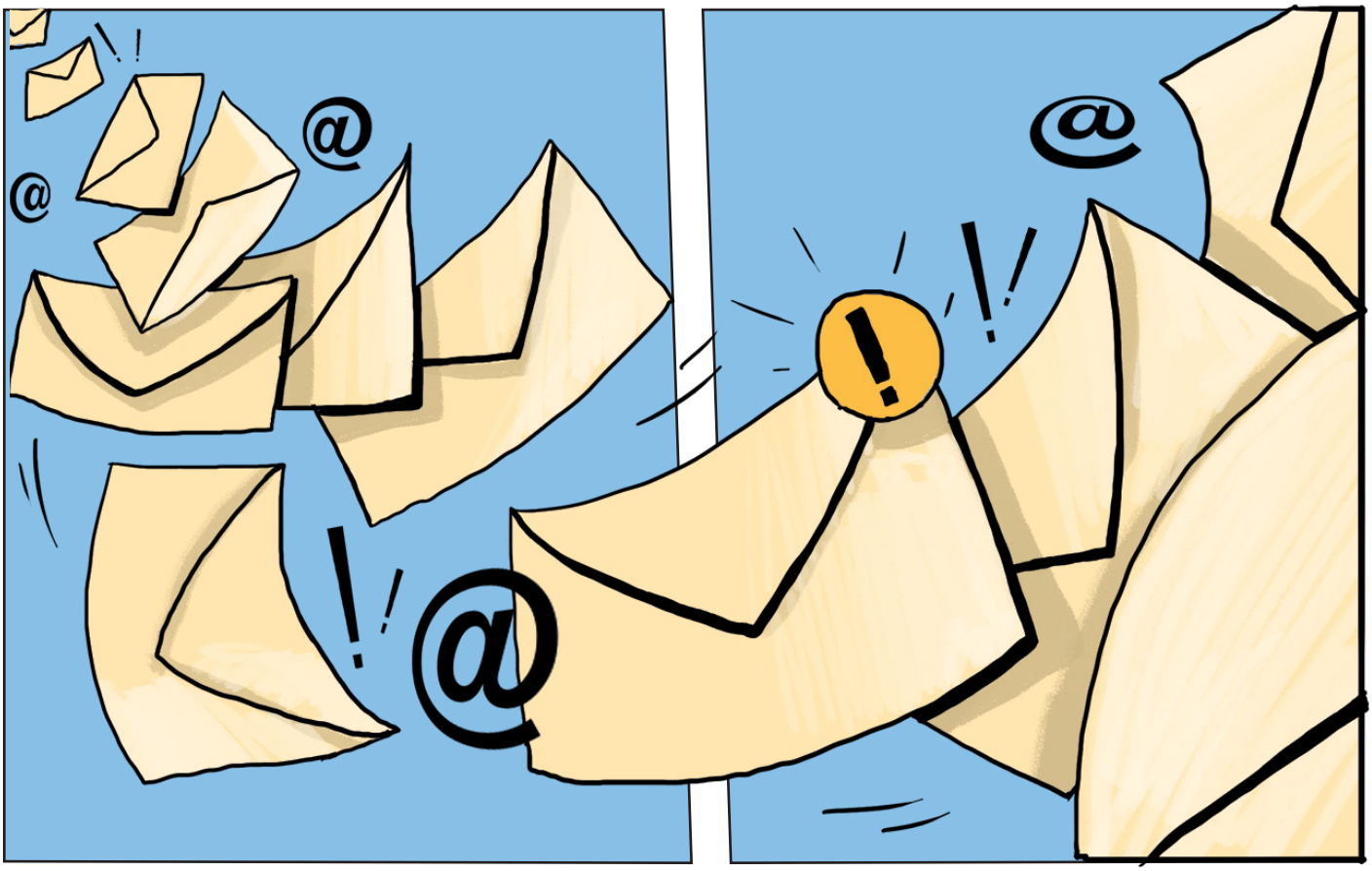
uniFLOW Online
Ce logiciel embarqué intègre la MAXIFY GX6050 à l'environnement de l'entreprise, permettant à l'équipe informatique de l'entreprise Y de suivre l'activité d'impression d'Ingrid et de rendre compte avec précision de la manière dont les informations sensibles sont utilisées, même lorsqu'elle travaille à domicile.

Un nouvel employé vient de terminer son premier mois de travail et Fatima des RH se prépare à envoyer les bulletins de salaire. Malheureusement, ce nouvel employé porte le même prénom qu'un autre membre du personnel. Fatima intervertit accidentellement les bulletins de salaire lors de l'envoi, ce qui signifie qu'ils peuvent tous les deux voir le salaire de l'autre.

L'organisation a enfreint la confidentialité des employés, qui ont techniquement des raisons de porter l'entreprise devant un tribunal compétent. De plus, après avoir vu le bulletin de salaire de son collègue, le nouvel employé remet en question son propre salaire auprès des RH et ne se sent peut-être plus à l'aise à son poste.



La communication est une étape à haut risque de tout workflow documentaire, car elle implique le partage d'informations, que ce soit en interne avec les employés ou en externe avec les clients, les fournisseurs et les autres parties prenantes. Dans le cadre d'un audit standard, les entreprises devront démontrer comment les informations sensibles sont partagées avec d'autres parties. Étant donné l'important volume de communications qu'une entreprise effectue au cours d'une semaine donnée, il est impératif de mettre en place des solutions qui simplifient le suivi et la traçabilité de ces processus.



ARMES SECRÈTES

uniFLOW sysHUB
uniFLOW sysHUB offre aux utilisateurs un contrôle et une surveillance stricts de leurs communications internes, ce qui permet à Fatima de préserver plus facilement la confidentialité des communications RH. La solution consolide les processus et les applications de communication interne en un seul workflow, géré à partir d'un point d'opération unique. uniFLOW sysHUB automatise ce workflow pour le rendre plus efficace et réduire le risque d'erreur. Dans cet exemple, Fatima n'aurait pas pu envoyer accidentellement des informations confidentielles à un autre employé.

Chaque étape du workflow est consignée et stockée dans une bibliothèque sysHUB pour une consultation ultérieure et pour prendre en charge les pistes d'audit. Ainsi, Fatima peut vérifier la preuve de livraison pour s'assurer que sa communication a bien été établie avec la bonne personne.

COMMENT POUVONS-NOUS AIDER ?

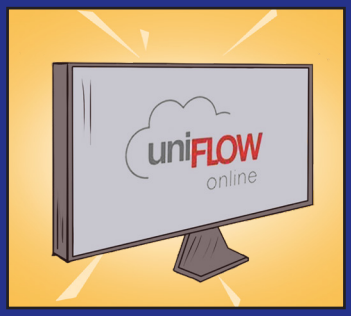
Chaque entreprise souhaite que ses informations soient sécurisées et conformes. Toutefois, comme l'ont montré les entreprises X et Y, l'environnement est plutôt hostile. Les entreprises doivent désormais faire face à davantage de pirates, et une législation plus stricte signifie que les enjeux sont élevés lorsque des erreurs sont commises. La bataille peut sembler perdue d'avance, mais ce n'est pas forcément le cas. Le secret : disposer de la technologie et du partenaire adaptés à vos besoins.

Canon est l'un des leaders reconnus par IDC MarketScape en matière de solutions et de services de sécurité d'impression et de documents, ainsi que par l'enquête Quocirca Print Security Landscape. Notre matériel, nos logiciels et nos services sont conçus pour aider votre entreprise à fonctionner aussi efficacement que possible dans un monde complexe. Peu importe la localisation de vos employés ou le stade de votre parcours de transformation numérique, notre technologie prend en charge tous les environnements de travail.

Grâce à notre approche de « sécurité dès la conception », nous nous efforçons de préserver la sécurité des informations. Nos solutions sont conçues pour empêcher les attaques, protéger les données et maintenir et préserver la conformité, afin que vous puissiez tirer parti des nouvelles fonctionnalités sans effort supplémentaire pour votre équipe.

PÉRIPHÉRIQUES D'IMPRESSION ET DE NUMÉRISATION
Notre gamme d'impression et de numérisation est dotée des dernières fonctionnalités en matière de sécurité pour protéger les données essentielles à chaque étape du workflow documentaire. Tous les produits Canon font l'objet d'un contrôle de sécurité lors des phases de conception et de développement, ainsi qu'avant leur lancement.

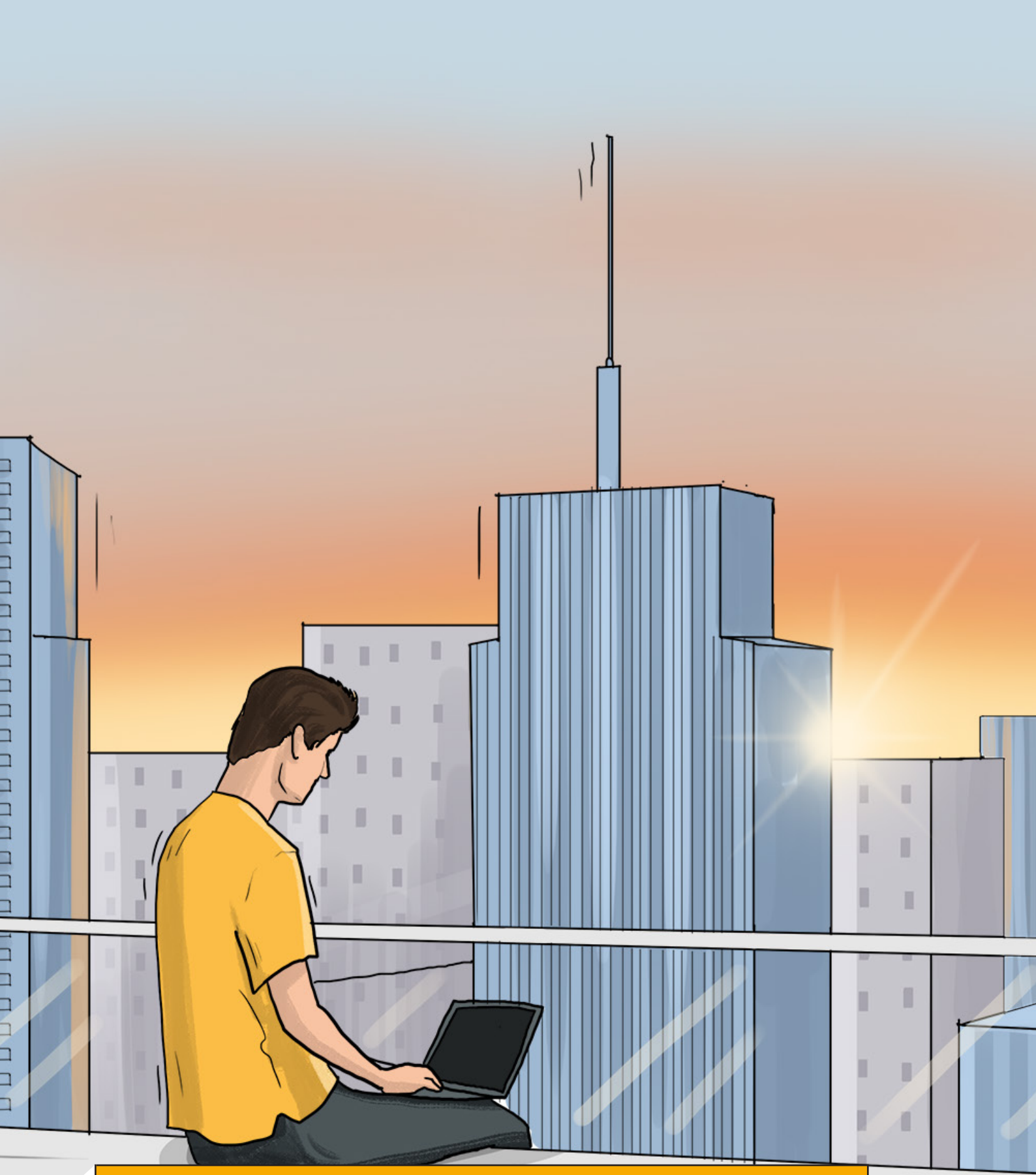
Nous continuons à établir des partenariats solides avec des leaders du secteur, tels que Trellix et Microsoft, afin d'assurer la couverture et la compatibilité les plus larges possibles lors de la sécurisation des flottes de périphériques. De plus, nous disposons d'une équipe dédiée à la réponse aux incidents de sécurité des produits.



LOGICIEL
Nous comprenons que les informations ne sont pas liées à l'emplacement, c'est pourquoi nous proposons un logiciel qui protège les données où qu'elles se trouvent. Nous travaillons également avec des entreprises externes comme IOActive pour effectuer des tests de pénétration lors de l'étape de lancement et pour les mises à jour logicielles majeures.

SERVICES
Nous proposons des services de sécurité conçus pour vous aider à maintenir la protection des données et protéger vos données sensibles tout au long de la durée de vie de votre infrastructure d'impression et de numérisation.


PASSPORT



Prêt à éliminer les problèmes de sécurité et de conformité ? Venez découvrir nos technologies à l'œuvre dans notre salle d'exposition, ou réservez une démonstration avec notre équipe commerciale d'experts pour voir ce que nos solutions pourraient faire pour votre entreprise.

Vous voulez en savoir plus sur nos armes secrètes ? Visitez notre site de services de transformation numérique pour en savoir plus.

À PROPOS DE CANON

La marque Canon est associée aux technologies d'imagerie. Nous utilisons ces technologies pour faire la différence et favoriser le changement. Pour nos clients qui engagent leur transformation numérique et adoptent de nouveaux modes de travail. Pour des changements sociétaux plus vastes grâce à notre objectif de développement durable dans le cadre de notre héritage et de notre culture d'entreprise.

Enfin, nous évoluons à mesure que nous investissons dans de nouveaux marchés, produits et technologies. Nous serons donc présents sur le long terme pour servir les intérêts de nos clients, de nos collaborateurs et de la société dans son ensemble.

LES 4 PILIERS DE CANON :

Innovation

Longue tradition d'innovation reposant sur l'image et la technologie de pointe depuis plus de 80 ans. Pionnier du secteur et véritable engagement à faire évoluer la technologie.

Support

Portefeuille de services diversifié pour garantir une qualité optimale et la satisfaction des clients. Expertise interne visant à renforcer l'efficacité et à libérer le potentiel de nos clients.

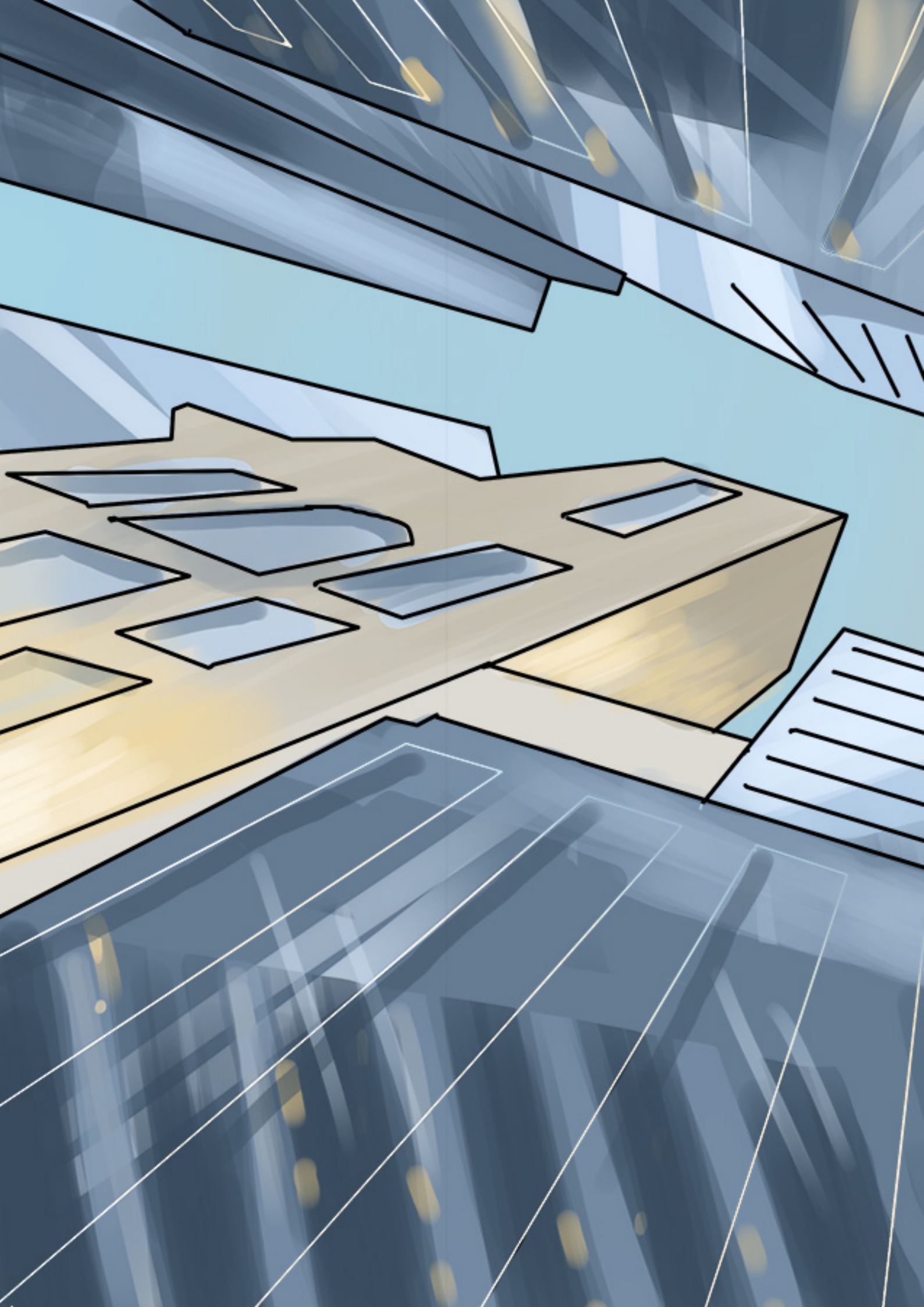
Sécurité

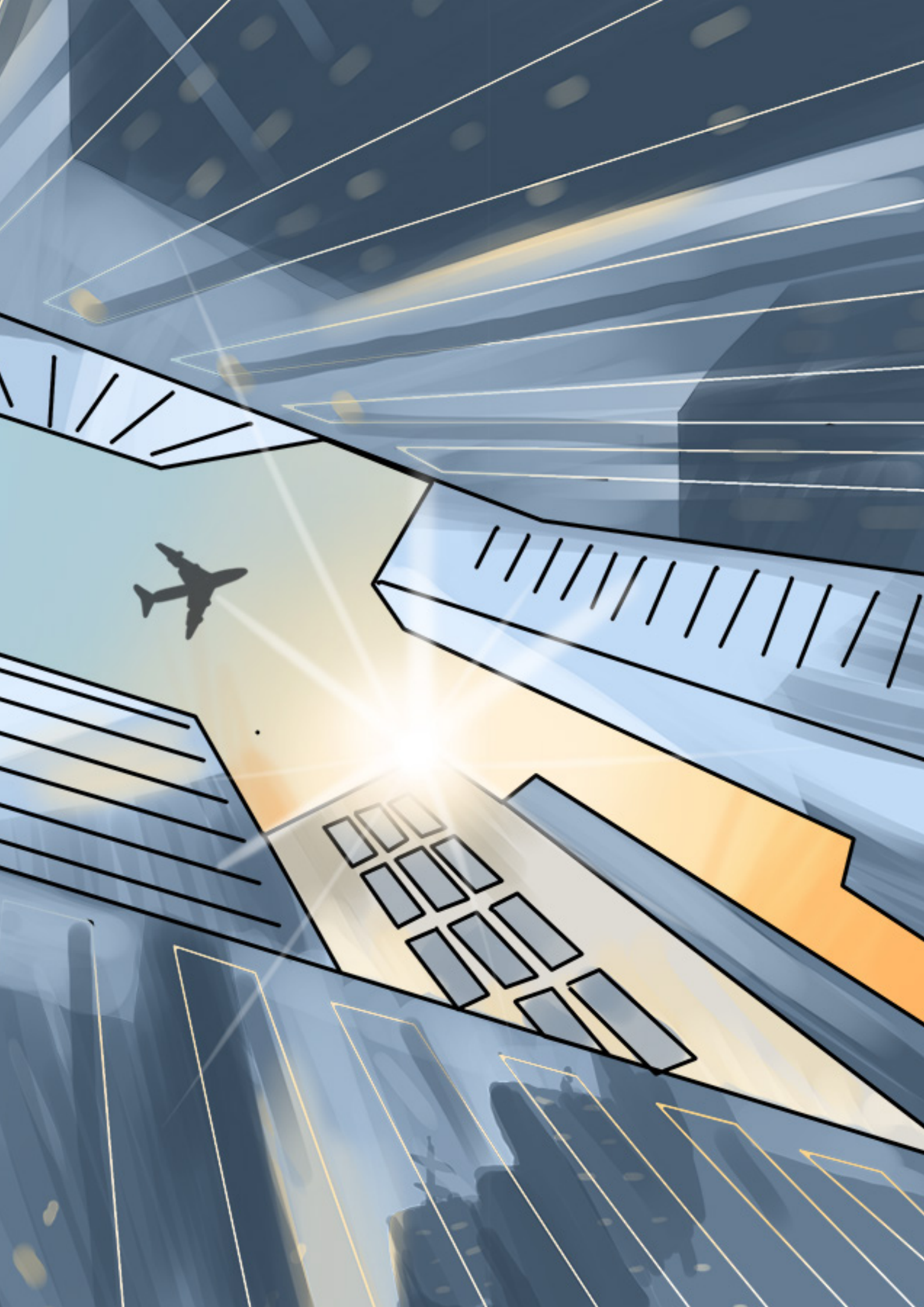
Les solutions et services de Canon permettent de sécuriser tous les documents et les données sensibles, au format papier ou numérique, tout au long du cycle de vie des documents. Sécurisés dès la conception, les périphériques, solutions et services sont conçus pour répondre aux exigences de sécurité.

Politique environnementale

Canon a aligné ses pratiques en matière de politique environnementale sur les objectifs de développement durable de l'ONU, notamment en s'engageant à réduire les émissions de CO2 tout au long du cycle de vie des produits, en réduisant les emballages et en consolidant les centres de distribution.

C'EST POUR TOUTES CES RAISONS QUE CANON EST LE PARTENAIRE IDÉAL POUR VOTRE ENTREPRISE.





Canon Inc.
Canon.com

Canon Europe
canon-europe.com
French edition canon.fr
© Canon Europa N.V., 2022

Canon France SAS
14 Rue Emile Borel
CS 28646
75809 PARIS CEDEX 17
Tél : 01 85 14 40 00
canon.fr

Canon Belgium NV/SA
Berkenlaan 3
1831 Diegem
Tel. 02-722 04 11
Fax 02-721 32 74
canon.be

Canon Luxembourg SA
WestSide Village Complex
Building E
Rue Pafebruch 89E
L-8308 Capellen
Luxembourg
Tél: +352 48 47 961
Fax: +352 48 47 96 235
Site Web: www.canon.lu

Canon (Suisse) SA
Richtistrasse 9
CH-8304 Wallisellen
Tel. +41 (0) 848 833 835
canon.ch