SICUREZZA DELLE INFORMAZIONI ALL'OPERA!

IN UN MONDO IN CUI LE MINACCE INFORMATICHE DIVENTANO SEMPRE PIÙ INTELLIGENTI E LA CONFORMITÀ SEMPRE PIÙ COMPLESSA, IN CHE MODO LA TUA AZIENDA INTENDE PROTEGGERE I DATI?

Canon

INDICE

I dati sono il tesoro di ogni organizzazione moderna. Potenziano il reparto finanziario, forniscono all'amministrazione poteri predittivi e conferiscono ai dipendenti una maggiore Business Intelligence.

Questa preziosa risorsa deve essere protetta a qualsiasi costo.

Più il valore di questo tesoro aumenta, maggiore è il numero di nemici che tenta di rubarlo: gli hacker malintenzionati sono sempre in agguato per sottrarre le tue informazioni quando meno te lo aspetti. Nel frattempo, gli infiltrati potrebbero cercare di impadronirsi del tesoro da soli.

Ma un nemico non basta per abbattere un'organizzazione.

Una grande forza monitora la situazione, assicurandosi che tutti seguano le regole di conformità dei dati. Ma anche se le leggi sono rigorose e le punizioni severe, non è mai stato così facile commettere un errore.

Le aziende moderne non sono una fortezza; sempre più spesso, non sono nemmeno ubicate in una singola sede. Come mai prima d'ora, Il lavoro ibrido fa sì che i dipendenti archivino le informazioni, le condividano e ci collaborino in più luoghi.

In un ambiente di lavoro così complesso, proteggere i dati e rispettare la conformità dei processi può sembrare una sfida impossibile.

Ciò di cui hai bisogno è un partner fidato, in grado di proteggere il tuo tesoro dai nemici e aiutare i tuoi dipendenti a rispettare la conformità, nonostante le avversità.

Vediamo in che modo Canon, grazie alle sue armi segrete, può aiutarti a vincere la sfida.

SFIDE NEL CICLO DI VITA DEI DOCUMENTI

I documenti vengono creati, copiati, memorizzati e condivisi durante il loro ciclo di vita all'interno dell'azienda; tutte queste fasi presentano delle sfide per mantenere i dati al loro interno sicuri e conformi.

La stampa è complicata per la sicurezza e la conformità, poiché è difficile avere una visibilità completa dell'attività degli utenti o dei documenti, il che può comportare una violazione dei dati

I documenti scansionati contenenti dettagli sensibili devono raggiungere la destinazione desiderata in modo sicuro. Gli errori dell'utente potrebbero inoltre causare perdite di dati

I dati personali e le informazioni sensibili di clienti e dipendenti devono essere archiviati, trattati e distrutti in modo sicuro, in conformità alle norme sulla privacy dei dati

Le comunicazioni, i documenti e i dati in uscita devono essere gestiti in modo sicuro per evitare problemi di conformità delle informazioni

SFIDA 1

LA STRATEGIA SEGRETA

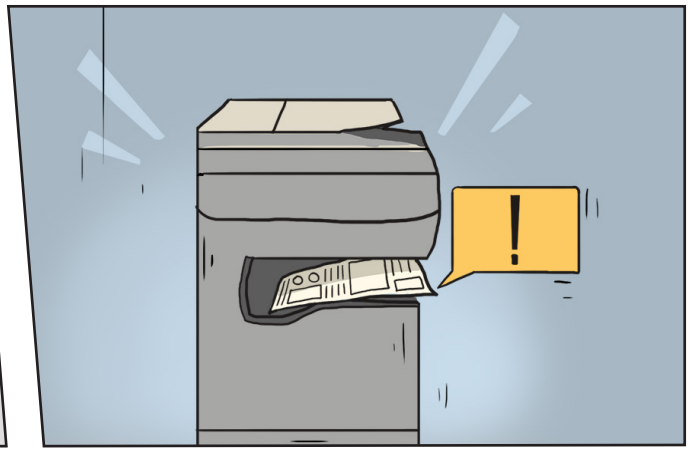
L'organizzazione X ha un gran segreto: è pronta a intraprendere una nuova avventura. L'amministrazione ha deciso di investire in una nuova area di business nella speranza di acquisire nuovi poteri e accedere a innumerevoli ricchezze.

È essenziale che questi piani restino nascosti, fino a quando non saranno resi pubblici. La notizia rivelerebbe le intenzioni dell'organizzazione X ai suoi rivali, preannunciando l'arrivo di un nuovo competitor. Nel frattempo, I dipendenti dell'organizzazione X si fanno molte domande: potrebbero esserci nuove opportunità nel loro reparto? Nuove aree di business da esplorare? O il loro ruolo è a rischio?

I dirigenti di più alto livello devono procedere con attenzione, se vogliono essere sicuri che i loro piani non finiscano nelle mani di dipendenti complottisti e avversari esterni. Durante l'intero processo di budgeting e annuncio, devono evitare una serie di trappole, dalle minacce interne ai malware e agli attacchi alla rete. Saranno in grado di proteggere i loro segreti?

L'ufficio Comunicazione ha elaborato un comunicato stampa che riflette la nuova direzione strategica dell'organizzazione. Le informazioni sono ancora top secret e l'annuncio è scritto e approvato da un piccolo gruppo di dirigenti senior. Selma, Finance Director, ha chiesto di esaminare una copia fisica del documento. La sua assistente Polina è pronta a stamparlo per lei.

La stampa rappresenta una delle maggiori minacce alla sicurezza, anche se le organizzazioni non se ne rendono conto. Tra i rischi più comuni per la sicurezza e la conformità, spesso i documenti cartacei vengono prelevati dalla stampante prima di essere ritirati dall'utente interessato o dimenticati del tutto, esponendo informazioni sensibili o riservate a persone non autorizzate. L'innovazione ha aperto le porte a una serie di nuove minacce alla sicurezza. Le moderne stampanti multifunzione sono potenti quanto un PC, dotate di disco rigido, memoria e unità centrale di elaborazione (CPU, Central Processing Unit) e spesso collegate a Internet. Di conseguenza, è possibile che il firmware della stampante venga preso di mira da hacker che tentano di accedere alla rete e ai dati aziendali.



ARMI SEGRETE

imageRUNNER ADVANCE DX C5800

imageRUNNER ADVANCE DX C5800 offre una sicurezza integrata di serie. Polina può stampare il documento solo accedendo al dispositivo tramite tessera identificativa: significa che nessun altro potrà accedere al documento in coda per la stampa e che tale documento non rimarrà nel vassoio del dispositivo in attesa di essere raccolto.

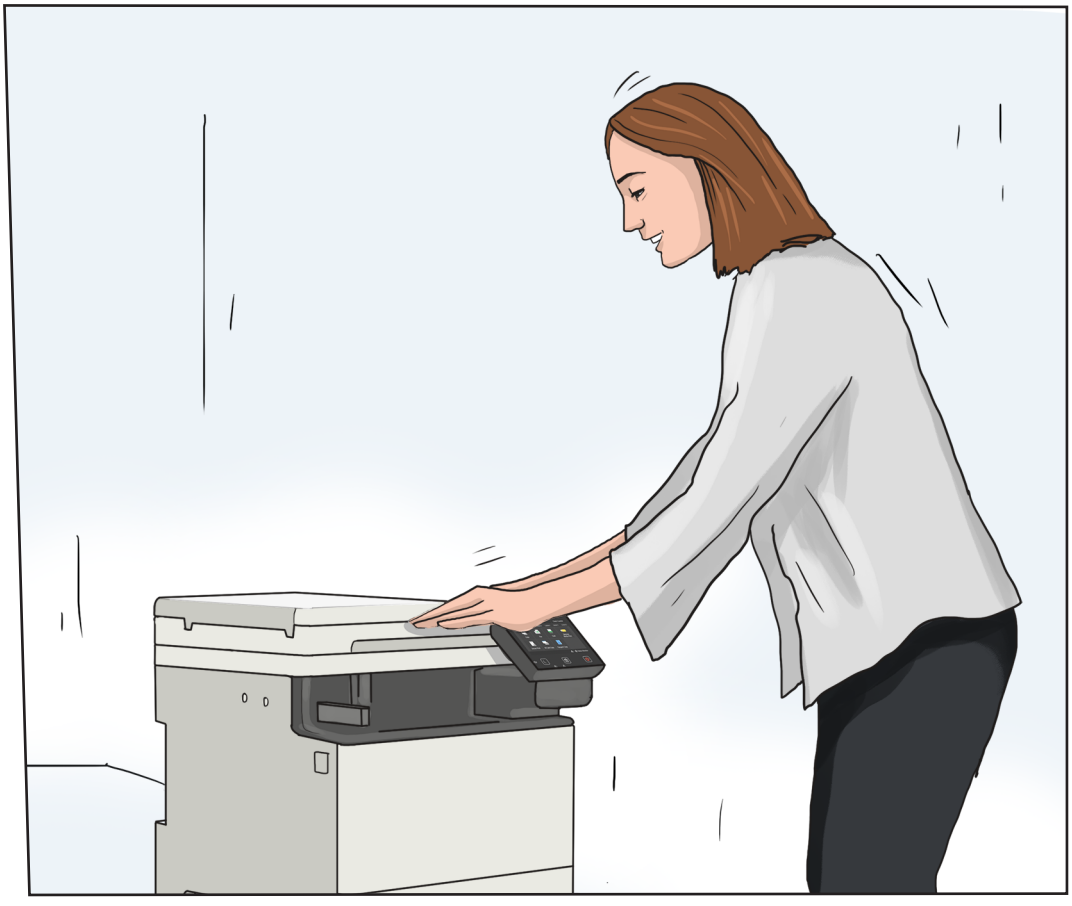
Inoltre il dispositivo include il software McAfee Embedded Control di Trellix, che protegge dagli attacchi zero-day e dalle minacce persistenti avanzate (APT, Advanced Persistent Threat) bloccando l'esecuzione di applicazioni non autorizzate tramite whitelisting intelligente. Per evitare che un hacker si appropri del comunicato stampa attraverso un attacco di rete, McAfee Embedded Control protegge il dispositivo dalla manomissione del programma.

Infine, imageRUNNER ADVANCE DX C5800 supporta l'integrazione Security Information Event Management (SIEM) che semplifica l'inclusione delle stampanti nei sistemi di monitoraggio della sicurezza esistenti (ad esempio, Syslog). Questi sistemi sono in grado di rilevare e contrassegnare gli eventi di sicurezza di un parco di dispositivi in tempo reale, avvisando l'azienda di eventuali problemi o minacce non appena si verificano.

Servizio di configurazione sicura dei dispositivi
Con Canon, la sicurezza inizia prima di acquistare un dispositivo. Configuriamo i dispositivi multifunzione imageRUNNER ADVANCE per potenziarne la sicurezza, rafforzando i controlli di sicurezza integrati e bloccando le funzioni non essenziali e le porte non protette. Il dispositivo configurato è controllato e verificato prima della spedizione.

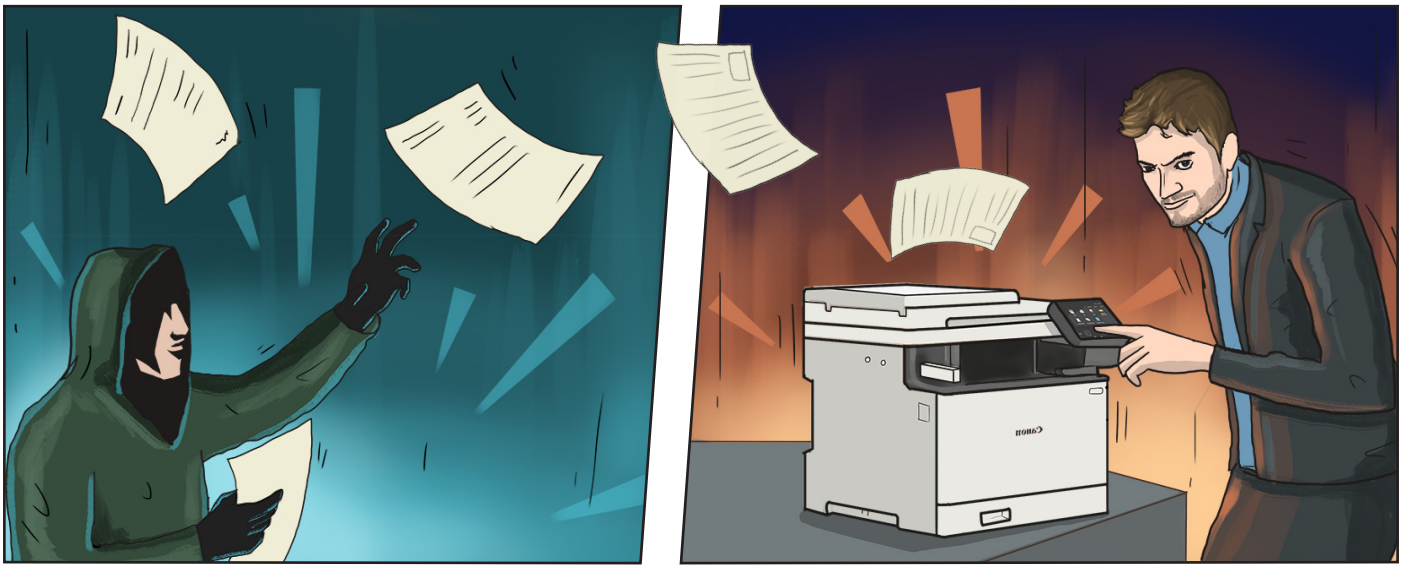
imageWARE Secure Audit Manager Express
Questa soluzione per la sicurezza dei dispositivi di rete fornisce all'organizzazione X la supervisione delle attività correlate ai documenti. È in grado di acquisire, memorizzare e controllare le attività che si verificano sui dispositivi Canon. Quando Polina stampa il comunicato, imageWARE Secure Audit Manager Express attiva un avviso via e-mail all'IT che segnala la stampa di un documento ad alto rischio. In questo modo, l'organizzazione X è in grado di tenere sotto controllo eventuali dipendenti o persone non autorizzate che cercano di copiare o stampare informazioni sensibili.

Selma ha esaminato il comunicato stampa e ha fornito alcuni commenti scritti. Polina deve condividere il feedback con Pierre, il PR Manager responsabile dell'annuncio. Poiché Pierre lavora da casa, Polina dovrà creare una copia digitale da inviargli. La scansione e l'invio di e-mail direttamente dal dispositivo favoriscono l'intercettazione del documento da parte di hacker.



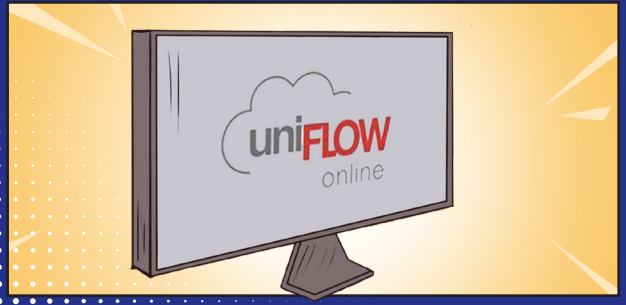
I dispositivi di scansione moderni sono spesso connessi a Internet, consentendo agli utenti di inviare documenti via e-mail a un destinatario o di salvarli in destinazioni cloud. Di conseguenza, le informazioni digitali sono più a rischio. È quindi fondamentale che i dispositivi di scansione dispongano di funzioni di sicurezza avanzate. In assenza di funzioni sicure, uno scanner è vulnerabile alla manomissione: per esempio, un utente interno potrebbe modificare il routing di posta elettronica per indirizzare una e-mail a un utente non autorizzato. Oppure, senza crittografia, un documento può essere semplicemente aperto, modificato o stampato.

Esternamente, un hacker potrebbe accedere alla rete e apportare modifiche alle directory di posta elettronica, consentendo l'invio di un documento a destinatari esterni all'organizzazione. Oppure, potrebbe intercettare un documento trasmesso tramite HTTPS se tale documento e i suoi dati non sono crittografati.



ARMI SEGRETE

i-SENSYS X C1333iF
Selma è pronta per eseguire la scansione del documento con i-SENSYS X C1333iF. Questo dispositivo multifunzione (ovvero, che combina le funzionalità di stampa e scansione) offre funzioni di scansione sicure che contribuiscono a proteggere le informazioni. Al momento dell'accensione, la funzione di verifica del sistema all'avvio accerta la presenza di tentativi di compromissione dell'integrità del dispositivo e avvisa Selma in caso di manomissione. A questo punto, Selma deve effettuare l'accesso con una tessera identificativa, assicurandosi che vi sia un registro con i dettagli di coloro con i quali sta copiando o condividendo le informazioni. Infine, EEE802.1X di i-SENSYS X C1333iF fornisce un meccanismo di autenticazione: quando si connette alla LAN o alla WLAN aziendale, fornisce la conferma della sua autenticità.



uniFLOW Online
Quando Selma esegue la scansione del documento, uniFLOW Online crea un PDF crittografato e offre una protezione opzionale tramite password. In questo modo, evita che gli utenti non autorizzati visualizzino, modifichino o stampino il documento, proteggendo le informazioni da chiunque tenti di intercettarle.

Tobias ha sentito che l'organizzazione potrebbe intraprendere una nuova direzione. In qualità di responsabile di uno dei team messi in difficoltà dalla strategia attuale, sa che questo potrebbe comportare seri tagli al budget di quest'anno o addirittura rappresentare una minaccia per i posti di lavoro.

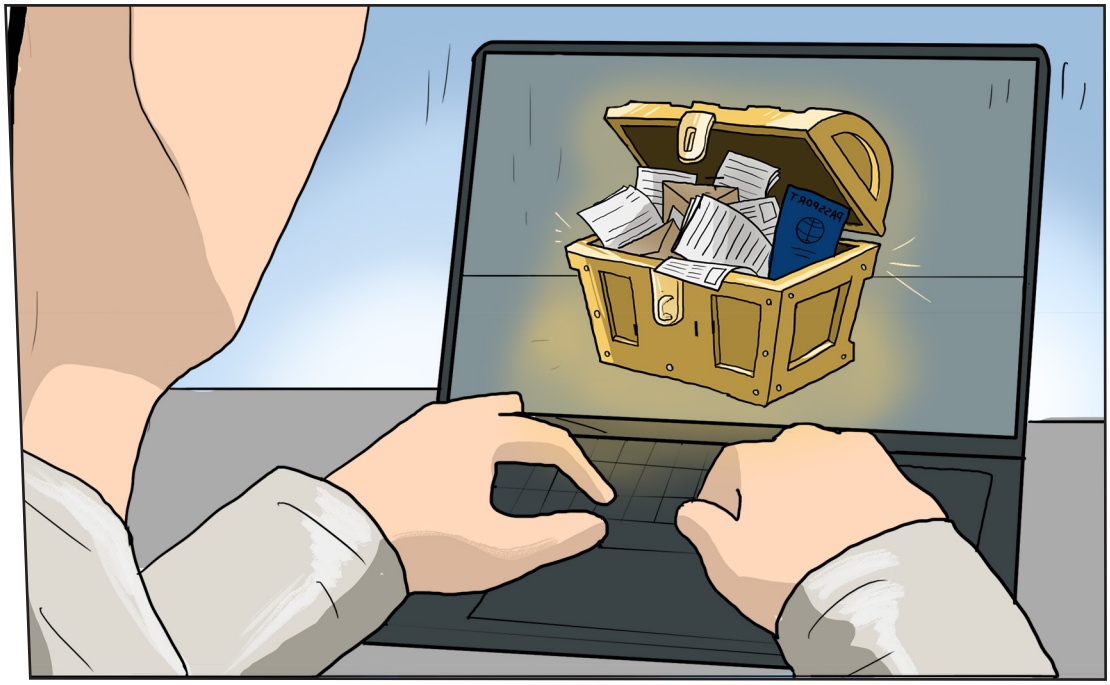
Tobias è turbato da tale notizia, perciò intende confermare la veridicità delle voci ed eventualmente avvisare i colleghi. Dal momento che pensa di sapere dove i dirigenti di più alto livello archivieranno i documenti finanziari, intraprende una ricerca segreta su tutto ciò che potrebbe essere associato ai nuovi piani.

Ogni anno le organizzazioni creano e archiviano sempre più informazioni. Con molti modelli operativi ibridi, queste informazioni vengono distribuite in un numero sempre crescente di sedi, sia fisiche che virtuali. Di conseguenza, molte organizzazioni ricorrono a strategie di conservazione dei dati aziendali improvvisate, che vedono i dipendenti utilizzare qualsiasi metodo, dagli archivi fisici a servizi di storage cloud personali come Dropbox.
Inoltre, i dipendenti trattano spesso informazioni sensibili come contratti, dati bancari del personale e risultati finanziari aziendali. Se i documenti vengono conservati in questo modo, è quasi impossibile per i team IT garantire la best practice nella gestione delle informazioni, perfino nel caso di dati critici come questi.

ARMI SEGRETE

Therefore Online
Grazie a una robusta sicurezza integrata, Therefore Online consente alle organizzazioni di impostare policy automatizzate su chi può accedere ai documenti e su come le informazioni vengono archiviate, condivise o modificate. I controlli relativi agli accessi impediscono ai dipendenti non autorizzati, come Tobias, di aprire documenti privati o riservati, come il comunicato stampa.

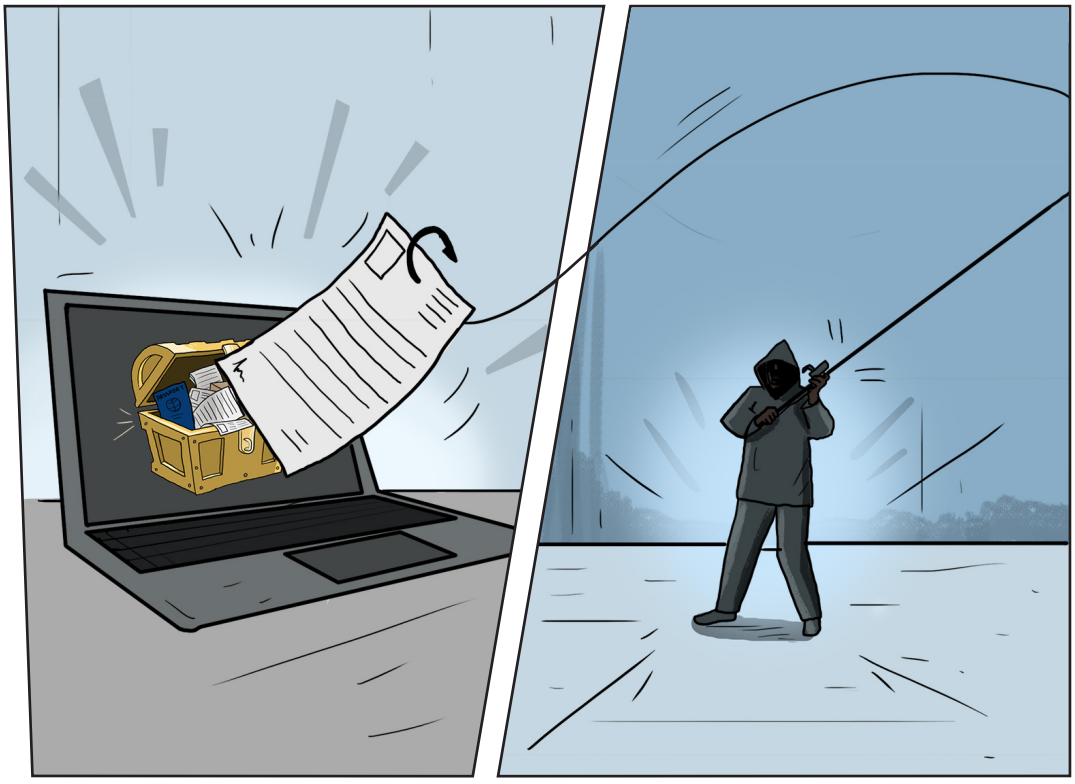
Therefore Online è basato su cloud, per garantire che la posizione di un utente non influisca sull'accessibilità; gli utenti autorizzati che lavorano da casa o in viaggio possono accedere ai documenti essenziali. Tutte le interazioni con un documento vengono monitorate, assicurando che le informazioni siano rigorosamente gestite e visibili end-to-end, fornendo una traccia di controllo digitale.



Pierre si sta preparando a inviare l'annuncio sotto embargo ai destinatari, tra cui i principali azionisti e giornalisti selezionati. È essenziale che il documento venga inviato solo a questi contatti; non può rischiare che finisca nelle mani sbagliate.

Nel frattempo, deve prestare attenzione alle informazioni aggiuntive che l'organizzazione X sta tenendo segrete. Il database aziendale contiene innumerevoli dati sensibili e preziosi sui destinatari, inclusi indirizzi e-mail, numeri di telefono e, nel caso dei giornalisti, i dettagli dei passaporti utilizzati precedentemente per i viaggi stampa.

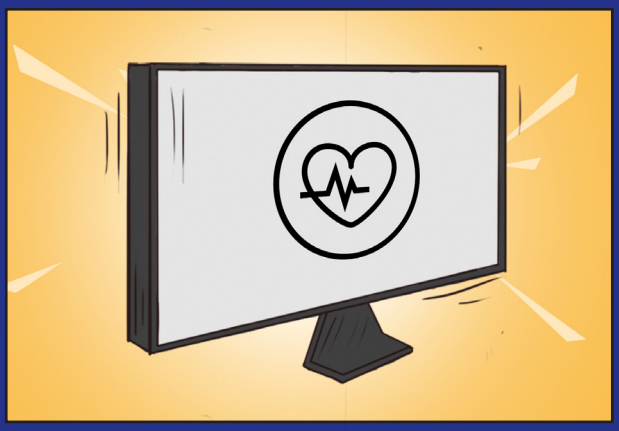
Questi dati rappresentano un potenziale honeypot per i ladri che potrebbero utilizzare queste credenziali per diffondere anticipatamente l'annuncio oppure, in certi casi, utilizzare i dati delle persone presenti nel database per eseguire furti di identità o orchestrare attacchi di phishing.



Spesso le aziende detengono informazioni altamente personali e riservate sui propri clienti, partner e altre parti con cui lavorano a stretto contatto. Queste informazioni non sono contenute solamente sui server aziendali, ma sono incluse nelle comunicazioni in uscita, quali estratti conto bancari, fatture e corrispondenza con tali parti. La conservazione di tali informazioni rappresenta un rischio per l'azienda, poiché in caso di smarrimento o furto da parte di hacker verrebbe esposta a sanzioni pecuniarie significative e a danni reputazionali. Se un'organizzazione comunica con questi contatti, è fondamentale che le informazioni personali contenute in tali comunicazioni raggiungano unicamente il destinatario.

ARMI SEGRETE

Verifica dell'integrità dell'ufficio
La Verifica dell'integrità dell'ufficio consente alle organizzazioni di esaminare il proprio ambiente IT per garantire che sia protetto fin dall'inizio. NCC Group, esperto globale in sicurezza informatica, condurrà un'analisi da remoto dell'infrastruttura IT interna ed esterna dell'organizzazione, inclusi i canali e le porte di comunicazione, per individuare le vulnerabilità. Identificando eventuali problemi, l'organizzazione è in grado di evitare che vengano sfruttati da potenziali hacker, impedendo l'intercettazione delle comunicazioni di Pierre e il furto dei dati di giornalisti e azionisti dai database dell'organizzazione X.



uniFLOW sysHub
uniFLOW sysHub controlla e supervisiona in modo rigoroso le comunicazioni con i clienti, consentendo a Pierre di assicurarsi più facilmente che le comunicazioni raggiungano la giusta destinazione. Questa soluzione consolida i processi e le applicazioni di comunicazione interna in un unico flusso di lavoro, gestito da un unico punto operativo. uniFLOW sysHub automatizza quindi questo flusso di lavoro per renderlo più efficiente e ridurre il rischio di errore. Ogni fase del flusso di lavoro viene registrata e memorizzata in una libreria sysHUB per una revisione successiva e come supporto alle tracce di controllo, rendendo difficile per un membro del personale la diffusione intenzionale di un documento, senza che questa venga registrata. Nel frattempo, Pierre può controllare la prova di consegna per assicurarsi che la comunicazione abbia raggiunto la persona giusta.

SFIDA 2

L'ASSUNZIONE RISERVATA

L'organizzazione Y deve attrarre nuovi lavoratori per potenziare il proprio regno in espansione. Un tempo la sua forza lavoro era ubicata in un'unica sede, ma grazie al lavoro ibrido, i suoi intrepidi dipendenti sono collocati su tutto il territorio. Il team HR ha dovuto adattarsi rapidamente. I nuovi dipendenti vengono ora sottoposti a processi di assunzione e onboarding virtuali. Il team HR deve avere occhi ovunque, dal momento che trasmette a grandi distanze documenti riservati relativi ai nuovi arrivati.

Dal grande potere del team HR derivano grandi responsabilità: una mole esorbitante di informazioni preziose e sensibili, dai dati relativi alle buste paga dei dipendenti a quelli sul loro stato di salute, fino ai registri delle prestazioni. Il team HR è consapevole che è necessario proteggere queste informazioni, in linea con la legislazione in materia di conformità. Gli auditor sono sempre all'orizzonte e il team HR sa che sarà tenuto a dimostrare come le informazioni vengono conservate e condivise. Non è semplice. Anche se il team HR lavora sodo, non ha superpoteri. È facile che incidenti o errori comportino dei problemi.

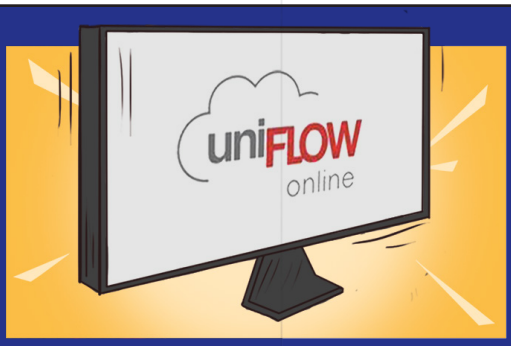
Senza le giuste soluzioni tecnologiche in grado di risolvere la situazione, l'organizzazione Y potrebbe ritrovarsi nei guai.

Dopo un colloquio di successo, l'organizzazione Y ha accettato di assumere un nuovo dipendente. Il candidato ha visitato la sede centrale per consegnare il passaporto e firmare il contratto con Fatima, Responsabile delle assunzioni. Fatima desidera eseguire delle copie dei documenti per il suo archivio e condividerle con il responsabile HR, che lavora da casa. È possibile che Fatima inserisca per errore il destinatario sbagliato o che salvi il documento in una posizione accessibile a chiunque. Se la persona sbagliata ricevesse i documenti acquisiti, potrebbe semplicemente aprirli e accedere alle informazioni contenute.

Le organizzazioni hanno la responsabilità di garantire che i documenti acquisiti tramite scansione siano visibili solo da utenti autorizzati. Un semplice errore potrebbe causare l'esposizione o la perdita di dati, nonché gravi conseguenze in termini di conformità. Se l'organizzazione non si rende conto della violazione e non inoltra la relativa segnalazione, il garante della protezione dei dati può emettere una sanzione pecuniaria fino al 4% del fatturato globale dell'organizzazione.

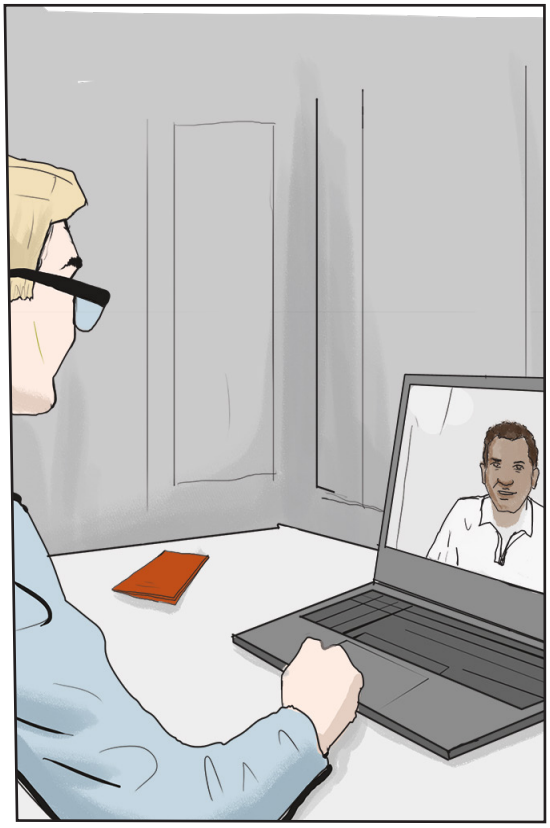
ARMI SEGRETE

uniFLOW Online
uniFLOW Online offre flussi di scansione sicuri integrati che consentono all'organizzazione Y di preconfigurare specifici flussi di scansione per ciascun utente. I flussi documentali, come nel caso dell'onboarding delle Risorse umane, sono già predefiniti, impedendo così a Fatima di salvare la scansione del nuovo dipendente in una destinazione errata.



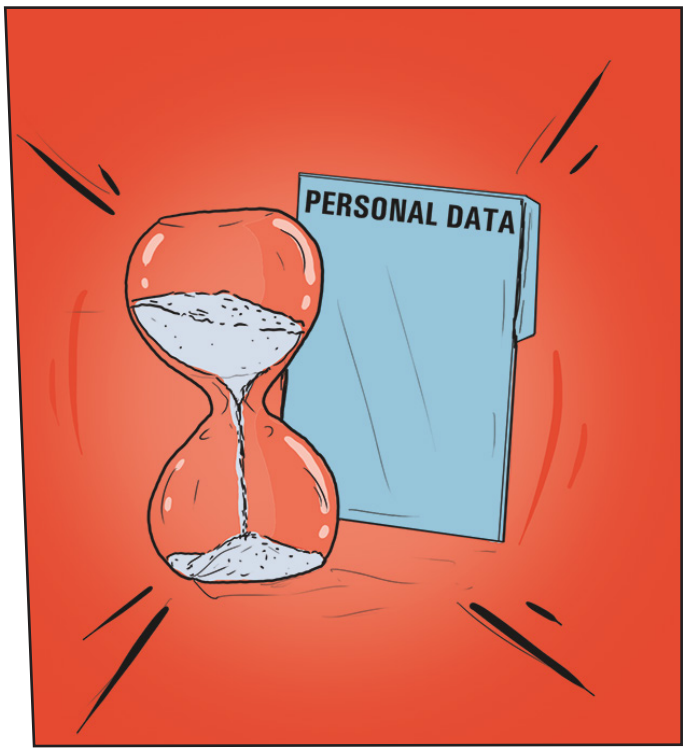
imageFORMULA DR-S150
Fatima è pronta per eseguire la scansione del documento con imageFORMULA DR-S150. Questo scanner offre funzioni di sicurezza che contribuiscono a proteggere le informazioni: per effettuare l'accesso è richiesta una tessera identificativa, garantendo così che solo Fatima possa accedere al documento acquisito. Inoltre, esegue automaticamente la crittografia della versione digitalizzata; in questo modo, solo i destinatari che conoscono la password possono leggerla, modificarla e stamparla. Infine, i dispositivi imageFORMULA DR-S150 offrono opzioni per inviare documenti tramite protocolli sicuri, quali la scansione a FTPS, SFTP e SMTPS.

IRISPowerscan
L'azienda dispone anche di IRISPowerscan: una volta digitalizzati i documenti, questi vengono automaticamente identificati come passaporto e contratto. Il software corregge eventuali errori di scansione, come le inclinazioni del foglio, e utilizza il riconoscimento ottico dei caratteri per riconoscere informazioni chiave come il nome e il numero di passaporto del dipendente. Tali informazioni vengono aggiunte all'indicizzazione, così da rendere più facile la loro ricerca in futuro. Inoltre, IRISPowerscan indirizza automaticamente le scansioni del contratto e del passaporto nella corretta posizione di archiviazione sicura sul sistema aziendale.



Durante il processo di reclutamento, diversi dipendenti, tra cui Fatima e il suo collega Nick, sono stati coinvolti nei colloqui con i candidati e nella revisione dei CV. Entrambi i dipendenti hanno sede virtuale e lavorano in diversi luoghi in Europa. Sia Fatima che Nick hanno archiviato le copie dei CV dei candidati e gli appunti relativi ai colloqui sul proprio laptop e su cartelle Dropbox condivise. Una volta offerta la posizione al candidato selezionato, è possibile che Fatima e Nick si dimentichino di eliminare questi documenti.

Con la normativa più severa di oggi, la conformità non è mai stata così importante. Leggi come il GDPR ha introdotto regole specifiche che disciplinano le modalità di conservazione delle informazioni; ad esempio, le organizzazioni non devono conservare i dati personali per un periodo di tempo superiore a quello strettamente necessario. Tuttavia, molte organizzazioni ricorrono ancora a strategie di conservazione dei dati improvvisate e non dispongono di posizioni ufficiali per l'archiviazione dei documenti né hanno la possibilità di individuare i documenti salvati sui propri server.
Se un ex dipendente o un candidato precedente presentasse una richiesta di accesso soggetto all'organizzazione, sarebbe difficile per l'azienda dichiarare quali informazioni sono in suo possesso. Inoltre, in caso di audit, l'organizzazione farebbe fatica a dimostrare di avere il controllo sulle posizioni di conservazione delle informazioni personali identificabili.

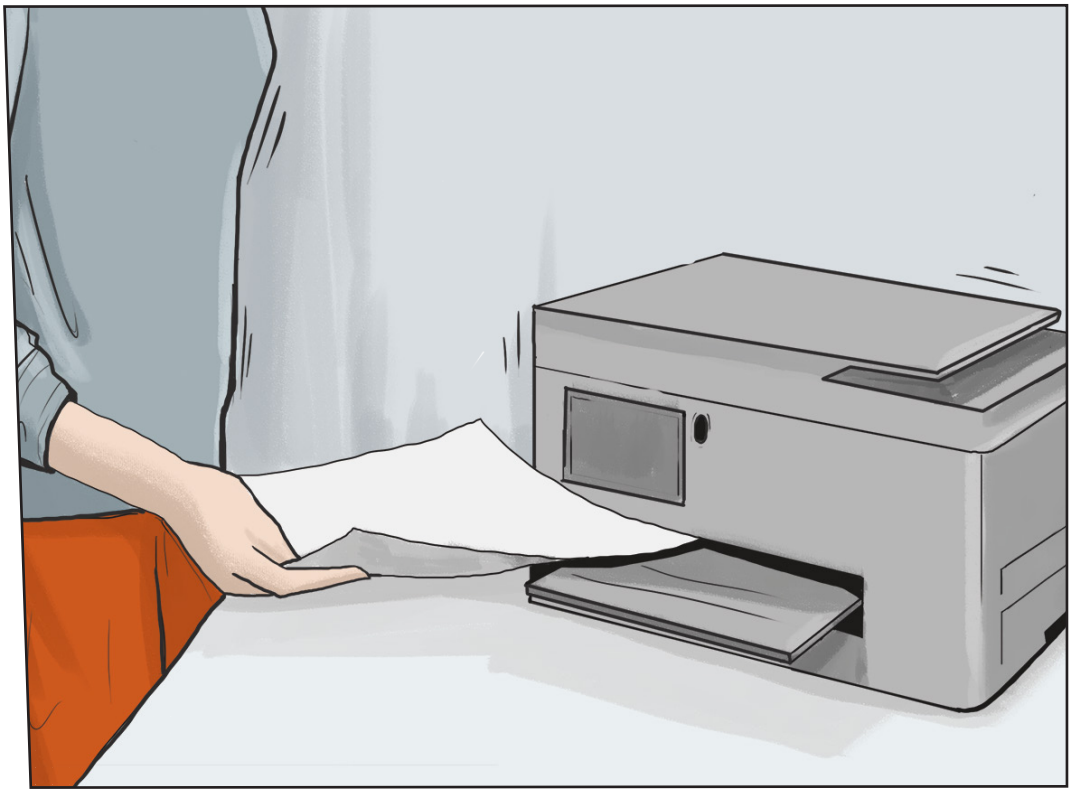


ARMI SEGRETE

Therefore Online
Grazie a una robusta sicurezza integrata, Therefore Online consente alle organizzazioni di impostare policy automatizzate su chi può accedere ai documenti e su come le informazioni vengono archiviate, condivise o modificate. Monitora tutte le interazioni con un documento, assicurando che le informazioni siano rigorosamente gestite e visibili end-to-end, il che rende il processo di audit molto più semplice.

L'organizzazione Y può anche impostare criteri di conservazione automatici per garantire che i vecchi documenti contenenti informazioni sensibili vengano eliminati dopo un periodo di conservazione appropriato, garantendo la conformità. Dal momento che Therefore Online è basato su cloud, i team possono caricare documenti in tutta sicurezza anche quando non si trovano in sede.

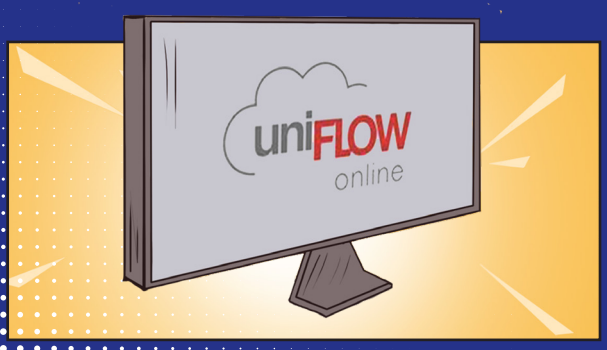
Ingrid, nuova line manager del dipendente, sta lavorando da casa e si prepara a condurre un colloquio introduttivo in ufficio il giorno successivo. Desidera stampare una copia della lettera di conferma dello stipendio del nuovo assunto, oltre ad altri moduli, da condividere durante il colloquio. Ingrid ha iniziato a lavorare solo di recente da casa e non ha ricevuto una stampante aziendale, perciò utilizza il suo dispositivo personale.



Per le organizzazioni è facile dimenticare che le stampanti svolgono un ruolo importante nella sicurezza e nella conformità dei flussi di lavoro, dal momento che tali dispositivi sono in grado di contenere dati e documenti importanti. Nell'ambito degli obblighi di conformità legale, le organizzazioni sono tenute a fornire tracce di controllo che riportino le modalità di utilizzo delle informazioni sensibili. Ciò richiede una maggiore visibilità e tracciabilità delle modalità di interazione dei documenti con i dispositivi. Tuttavia, poiché Ingrid utilizza la propria stampante personale, non è connessa alla rete aziendale: non esiste alcuna tracciabilità, nessun registro dei dati memorizzati sul dispositivo e nessuna garanzia di sicurezza.

ARMI SEGRETE

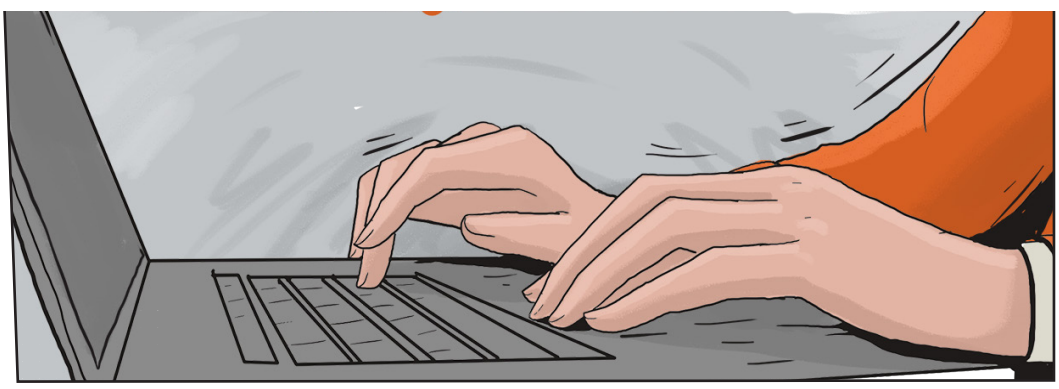
MAXIFY GX6050
Questa efficiente stampante da tavolo produce stampe di alta qualità per chi lavora da casa, ma contribuisce anche a mantenere i documenti protetti e conformi grazie all'integrazione con uniFLOW Online incorporata. La funzione Scan to Myself impedisce a Ingrid di inviare documenti a chiunque, a eccezione della propria e-mail o cartella personale, per evitare che invii accidentalmente documenti aziendali a contatti personali. La funzione Rilascio protetto lavori di stampa consente a Ingrid di stampare i documenti solo quando è pronta, per evitare che documenti aziendali sensibili vengano lasciati nel dispositivo.



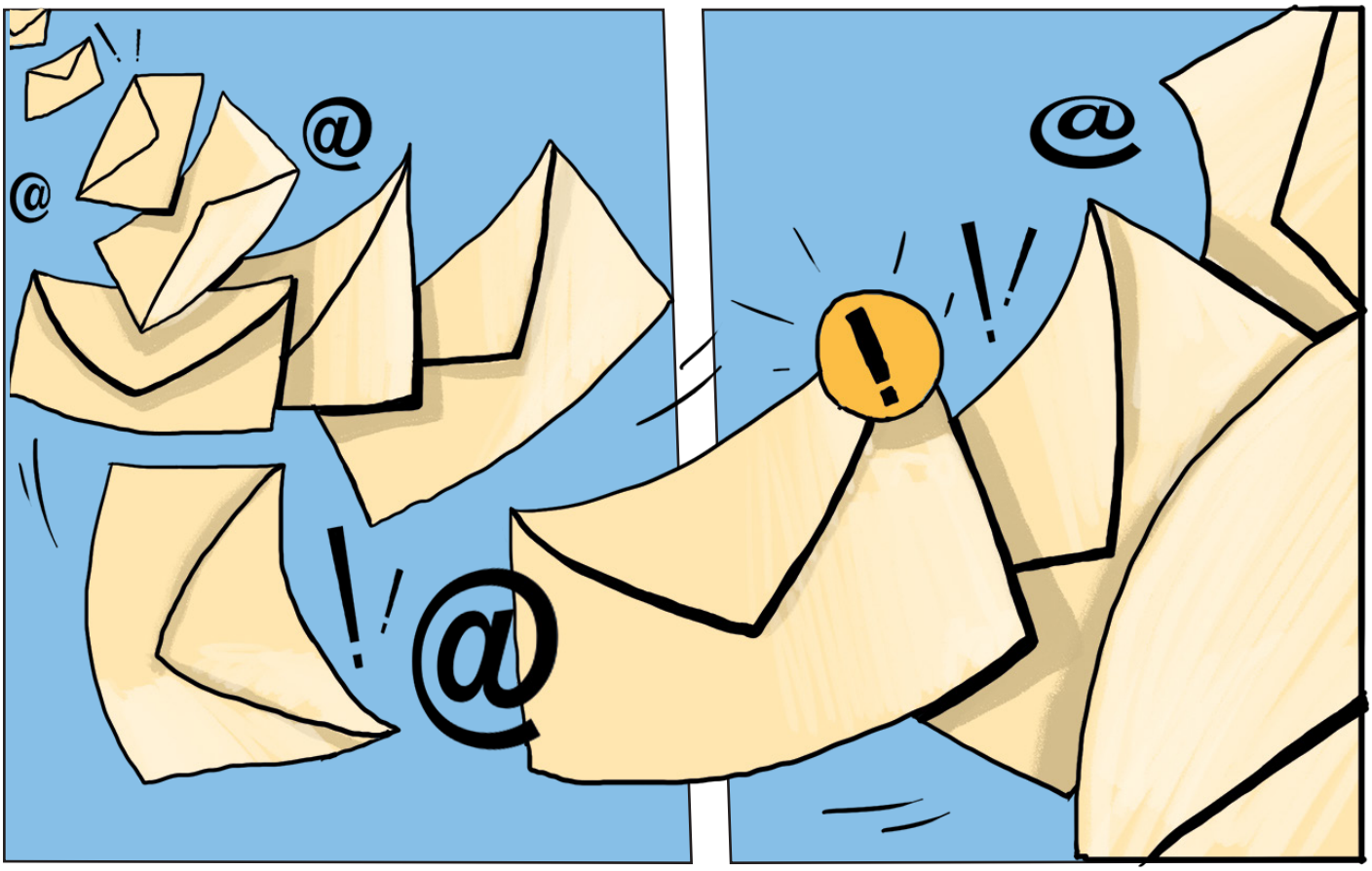
uniFLOW Online
Questo software incorporato integra MAXIFY GX6050 con l'ambiente organizzativo, consentendo al team IT dell'organizzazione Y di tenere traccia dell'attività di stampa di Ingrid e di registrare con precisione l'utilizzo delle informazioni sensibili, anche quando lavora da casa.

È la fine del primo mese del nuovo dipendente e Fatima delle risorse umane si sta preparando a inviare i cedolini. Sfortunatamente, il nuovo dipendente ha lo stesso nome di un altro membro del personale. Fatima, inviando i cedolini, inverte accidentalmente i destinatari, il che significa che entrambi sono in grado di vedere quanto viene pagato l'altro.

L'organizzazione ha violato la riservatezza dei dipendenti, i quali, tecnicamente, avrebbero i motivi per portare l'azienda a un tribunale del lavoro. Inoltre, avendo visto lo stipendio dei colleghi, il nuovo dipendente sta ora contestando il proprio stipendio con le risorse umane e potrebbe non sentirsi più a proprio agio nel ruolo.



La comunicazione è una fase ad alto rischio di qualsiasi flusso documentale, in quanto implica la condivisione di informazioni tanto internamente con i dipendenti, quanto esternamente con clienti, fornitori e altre parti interessate. In un audit standard, le organizzazioni sono tenute a dimostrare le modalità di condivisione delle informazioni sensibili con altre parti. Dato l'enorme volume di comunicazioni effettuate ogni settimana da un'organizzazione, è essenziale disporre di soluzioni in grado di eliminare il problema del monitoraggio e del tracciamento di tali processi.



ARMI SEGRETE

uniFLOW sysHub
uniFLOW sysHUB controlla e supervisiona in modo rigoroso le comunicazioni interne, consentendo a Fatima di garantire più facilmente la riservatezza delle comunicazioni HR. La soluzione consolida i processi e le applicazioni di comunicazione interna in un unico flusso di lavoro, gestito da un unico punto operativo. uniFLOW sysHub automatizza questo flusso di lavoro per renderlo più efficiente e ridurre il rischio di errore. In questo modo, Fatima non potrebbe inviare accidentalmente informazioni riservate a un altro dipendente.

Ogni fase del flusso di lavoro viene registrata e memorizzata in una libreria sysHUB per una revisione successiva e come supporto alle tracce di controllo, il che significa che Fatima può controllare la prova di consegna per assicurarsi che la comunicazione abbia raggiunto il giusto destinatario.

COME POSSIAMO AIUTARTI?

Ogni azienda desidera garantire la sicurezza e la conformità delle proprie informazioni. Ma come dimostrato dalle organizzazioni X e Y, non è affatto semplice. Non solo le organizzazioni si trovano a combattere un numero maggiore di nemici rispetto al passato, ma di fronte a una legislazione sempre più severa, la posta in gioco è alta in caso di errori. Può sembrare una battaglia persa, ma non deve essere per forza così. Il segreto è avere al proprio fianco la giusta tecnologia e il giusto partner.

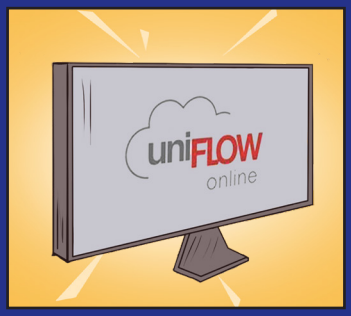
Canon è un'azienda leader nell'IDC MarketScape per le soluzioni e i servizi di sicurezza di stampa e documenti, nonché in Quocirca Print Security Landscape. I nostri hardware, software e servizi sono progettati per aiutare la tua organizzazione a operare nel modo più efficiente ed efficace possibile in un mondo tanto complesso. A prescindere dalla posizione dei dipendenti o dai propri progressi nel percorso di trasformazione digitale, la nostra tecnologia supporta ogni ambiente di lavoro.

Grazie al nostro approccio "Secure by Design", ci occupiamo di tenere al sicuro le informazioni. Le nostre soluzioni sono progettate per prevenire attacchi informatici, proteggere i dati e garantire e salvaguardare la conformità, così che tu possa sfruttare nuove funzionalità senza aumentare il carico di lavoro del tuo team.

DISPOSITIVI PER LA STAMPA E LA SCANSIONE

Il nostro portafoglio di dispositivi per la stampa e la scansione è dotato delle più recenti funzioni di sicurezza per proteggere i dati sensibili in ogni fase del flusso di lavoro documentale. Tutti i prodotti Canon sono sottoposti a controlli di sicurezza nelle fasi di progettazione e sviluppo, nonché prima del rilascio.

Continuiamo a creare solide partnership con i leader del settore, come Trellix e Microsoft, per garantire la massima copertura e compatibilità nella protezione dei parchi dispositivi. Vantiamo un team dedicato che si occupa della risposta agli incidenti di sicurezza dei prodotti.



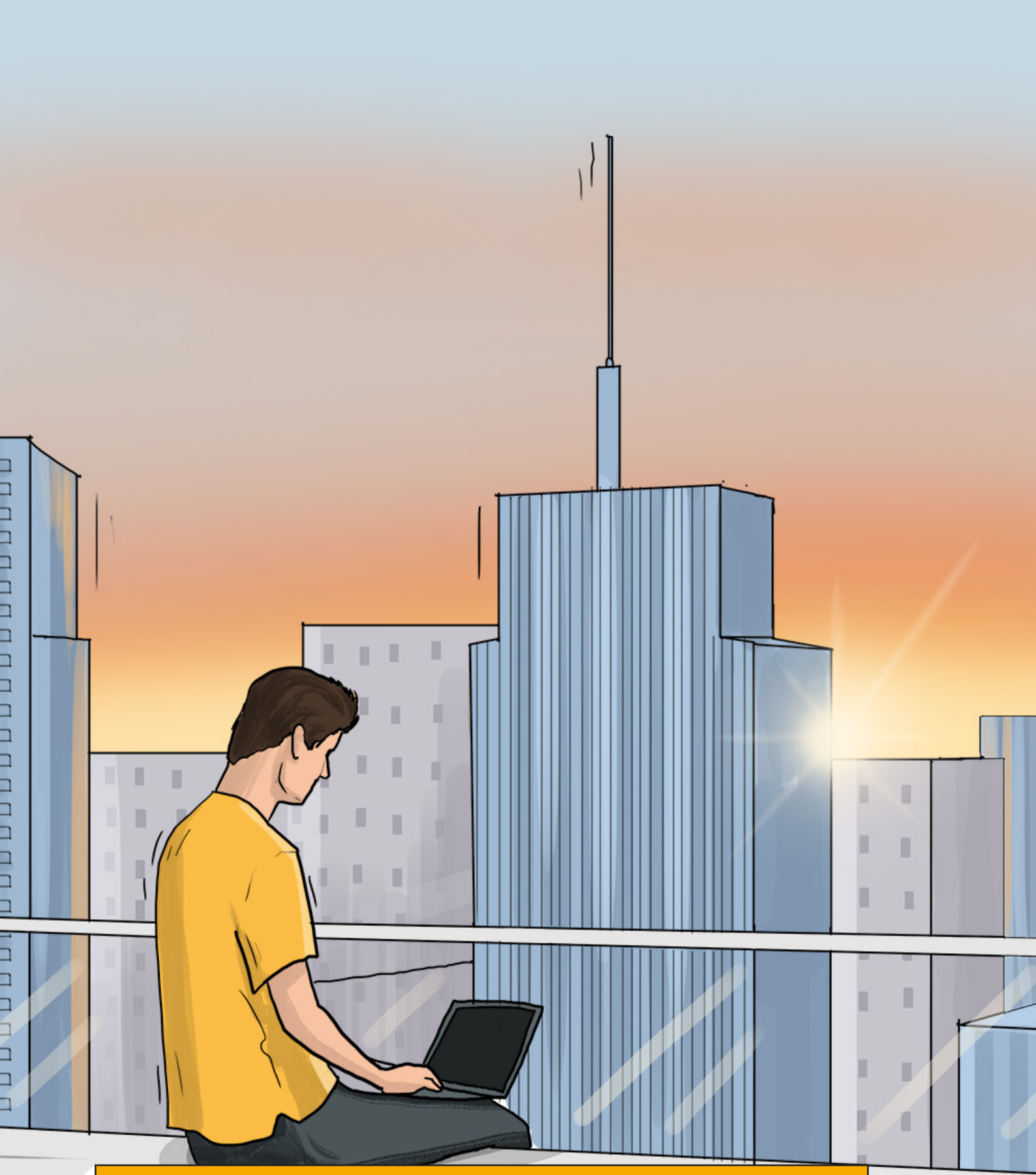
SOFTWARE

Siamo consapevoli che le informazioni non sono vincolate alla posizione, per questo offriamo software in grado di proteggere i dati ovunque si trovino. Collaboriamo con organizzazioni esterne come IOActive per condurre penetration test in fase di rilascio e per importanti aggiornamenti software.

SERVIZI

Offriamo servizi per la sicurezza pensati per aiutarti a mantenere la conformità in materia di sicurezza dei dati e a proteggere i dati sensibili per tutto il ciclo di vita dell'infrastruttura di stampa e scansione.


PASSPORT



Preparati a sconfiggere i problemi di sicurezza e conformità! Vieni a vedere le nostre tecnologie in azione nel nostro showroom o prenota una demo con il nostro team di vendite per scoprire cosa potrebbero fare le nostre soluzioni per la tua azienda.

Desideri ulteriori informazioni sulle nostre armi segrete? Visita il nostro sito sui Servizi per la trasformazione digitale.

INFORMAZIONI SU CANON

Canon è sinonimo di imaging. E noi utilizziamo l'imaging per fare la differenza e promuovere il cambiamento. Per i nostri clienti che intraprendono la trasformazione digitale e hanno cambiato il loro modo di lavorare. Per il cambiamento sociale in generale, grazie a un'attenzione continua alla sostenibilità che è parte integrante della tradizione e della cultura della nostra azienda.

Infine, stiamo cambiando il nostro modo di investire in nuovi mercati, prodotti e tecnologie al fine di continuare a lavorare ancora per molto tempo a beneficio di tutti: dei nostri clienti, dei nostri dipendenti e dell'intera società.

CANON SI BASA SU 4 VALORI DI BASE:

Innovazione

Una lunga tradizione di innovazione incentrata sulle immagini, che ci permette di realizzare tecnologie all'avanguardia da più di 80 anni. Nel nostro settore siamo sempre i primi a sperimentare le nuove soluzioni e ci impegniamo al massimo per lo sviluppo futuro della tecnologia.

Supporto

Offriamo un portafoglio di servizi diversificato per garantire la massima qualità, assicurando la soddisfazione dei clienti. I nostri esperti interni fanno tutto il possibile per migliorare l'efficienza e aiutare i clienti a esprimere il loro potenziale.

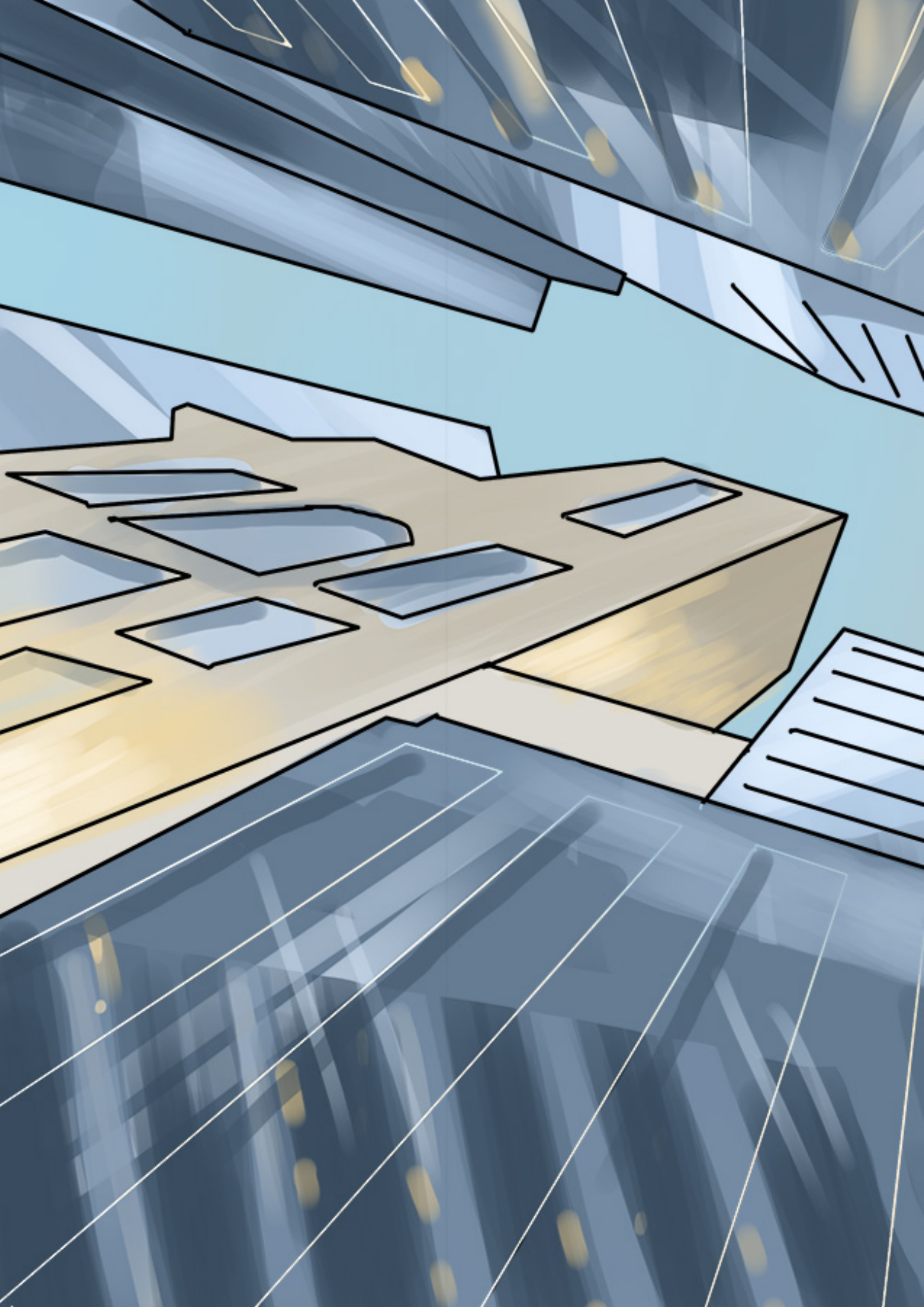
Sicurezza

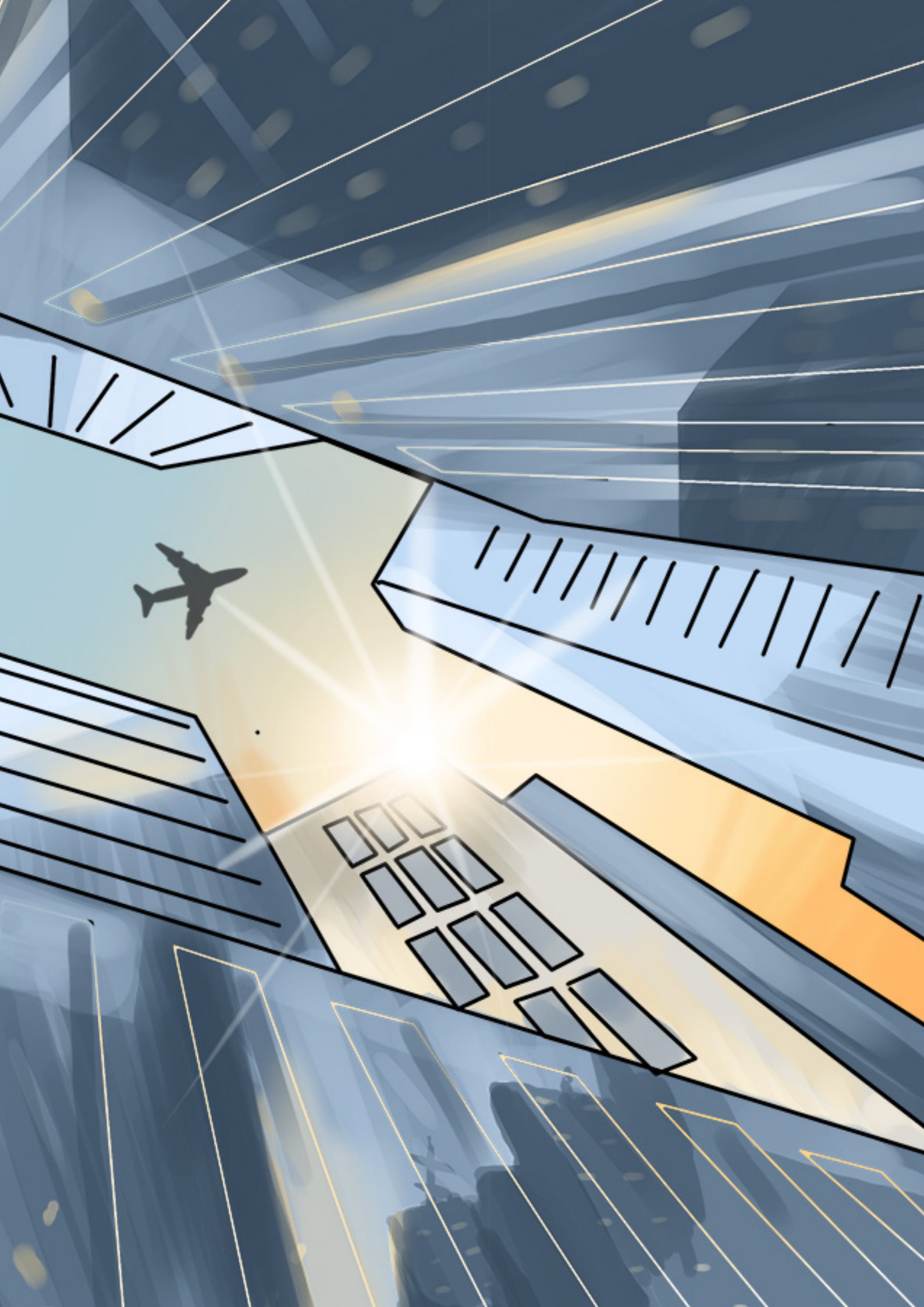
Le soluzioni e i servizi Canon consentono di proteggere tutti i documenti e i dati sensibili, in formato digitale o cartaceo, per l'intero ciclo di vita dei documenti. I nostri dispositivi, servizi e soluzioni sono sicuri by-design, perché vengono concepiti pensando alla sicurezza.

Sostenibilità

Canon ha allineato le sue procedure per la sostenibilità agli Obiettivi di sviluppo sostenibile delle Nazioni Unite, come l'impegno a ridurre le emissioni di CO_2 nell'intero ciclo di vita dei prodotti, riducendo le dimensioni degli imballaggi e consolidando i centri di distribuzione.

TUTTI INSIEME, QUESTI ELEMENTI FANNO DI CANON IL PARTNER IDEALE PER LA TUA AZIENDA.





Canon Inc.
Canon.com

Canon Europe
canon-europe.com
Italian edition/canon.it

Canon Italia Spa
Strada Padana Superiore, 2/B
20063 Cernusco sul Naviglio MI
Tel 02 82481
Fax 02 82484600
Pronto Canon 848800519
canon.it

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