INFORMATIEBEVEILIGING IN ACTIE

HOE HOUDT UW ORGANISATIE INFORMATIE VEILIG IN EEN WERELD WAARIN CYBERDREIGINGEN STEEDS INGENIEUZER WORDEN EN HET STEEDS LASTIGER WORDT AAN REGELGEVING VOOR GEGEVENSBESCHERMING TE VOLDOEN?

Canon

INDEX

INLEIDING:
Cyberdreigingen, aanvallen van binnenuit, en het vermijden van de beveiligingsvalkuilen van de moderne werkplek.

UITDAGING 1:
De geheime strategie
Vijanden weren om uw gegevens veilig te houden.

UITDAGING 2:
Vertrouwelijke personeelsaanwerving
Behoed uw team voor onopzettelijke compliancy-schendingen.

BESCHERM UW SCHAT AAN GEGEVENS:
Ontdek hoe Canon u kan helpen.

Gegevens zijn de 'schat' van elke moderne organisatie. Ze sturen uw financiële afdeling aan, stellen uw managementteam in staat om prognoses op te stellen, en bieden uw medewerkers betere business intelligence om de bedrijfsresultaten te verbeteren.

Deze belangrijke resource moet koste wat kost worden beschermd.

Aangezien deze schat voortdurend in waarde blijft toenemen, wordt ook het aantal vijanden dat op de loer ligt om er met uw gegevens vandoor te gaan alsmaar groter: aanvallers wachten hun kans af om informatie te stelen wanneer u dat het minst verwacht. Ondertussen proberen dubbelagenten de schat voor zichzelf in te pikken.

Maar er is geen vijand voor nodig om een organisatie te doen instorten.

Een alomtegenwoordige macht waakt over het land, om erop toe te zien dat iedereen zich aan de regels voor gegevensbescherming houdt. Maar hoewel de wetten strikt zijn en de straffen streng, is het ook nog nooit zo eenvoudig geweest om een fout te maken.

Moderne organisaties zijn geen ommuurde stad; steeds vaker bevinden ze zich niet eens op één locatie. Hybride werken betekent dat medewerkers informatie opslaan en delen en samenwerken op meer locaties dan ooit tevoren.

In zo'n complexe werkomgeving kan het een onmogelijke opgave lijken om uw informatie te beveiligen en ervoor te zorgen dat uw processen aan de regels voldoen.

U hebt een betrouwbare partner nodig die uw schat kan beveiligen, u tegen schurken kan beschermen, en uw mensen kan helpen om te allen tijde aan de voorschriften te voldoen.

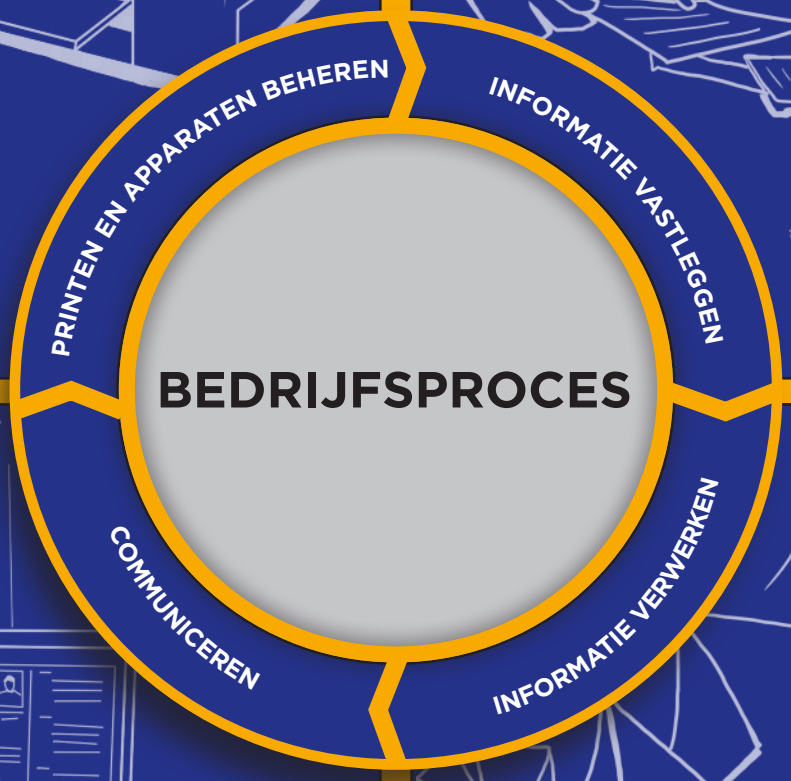
Laten we eens kijken hoe Canon en haar geheime wapens u kunnen helpen de uitdaging aan te gaan.

UITDAGINGEN IN DE DOCUMENTLEVENSCYCLUS

Tijdens hun levenscyclus worden documenten in uw organisatie gemaakt, gekopieerd, opgeslagen en gedeeld. In elk van deze stadia is het een uitdaging om te zorgen dat de gegevens beschermd blijven en voldoen aan de regelgeving.

Printen vormt een uitdaging wat betreft beveiliging en compliancy, omdat het moeilijk is volledig zicht te krijgen op gebruikers- en documentactiviteiten. Dit kan leiden tot datalekken.

Gescande documenten met gevoelige gegevens moeten hun gewenste bestemming veilig bereiken. Menselijke fouten kunnen tot gegevensverlies leiden.



Persoonlijke gegevens en gevoelige informatie van klanten en werknemers moeten veilig worden opgeslagen, verwerkt en vernietigd, in overeenstemming met de regels voor gegevensprivacy.

Uitgaande communicatie, documenten en gegevens moeten veilig worden beheerd om compliancy-problemen met informatie te voorkomen.

UITDAGING 1

DE GEHEIME STRATEGIE

Organisatie X heeft een groot geheim: het bedrijf begint aan een nieuw avontuur. Het managementteam heeft besloten te investeren in een nieuw bedrijfsonderdeel in de hoop meer macht te krijgen en ongekende rijkdommen aan te boren.

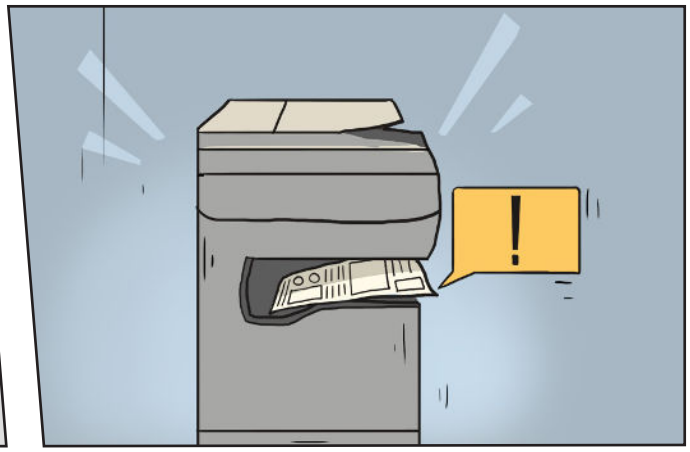
Het is van essentieel belang dat deze plannen geheim blijven totdat ze openbaar worden gemaakt. Het nieuws zou de concurrenten van Organisatie X duidelijk maken welke kant het bedrijf op gaat en ze waarschuwen dat er een nieuwe concurrent op het toneel gaat verschijnen. Ondertussen staat er voor medewerkers van Organisatie X veel op het spel. Komen er nieuwe mogelijkheden op hun afdeling? Nieuwe bedrijfsonderdelen om te verkennen? Of staan hun banen op de tocht?

Het senior managementteam moet voorzichtig te werk gaan om ervoor te zorgen dat hun plannen niet in de handen van samenzwerende medewerkers en externe vijanden vallen. Tijdens het budgetterings- en aankondigingsproces moeten ze een reeks valkuilen vermijden, van interne bedreigingen tot malware en netwerkaanvallen. Kunnen ze hun geheim stil houden?

Het communicatieteam heeft een persbericht opgesteld waarin de nieuwe strategische richting van de organisatie wordt uiteengezet. De informatie is nog steeds topgeheim en de aankondiging is geschreven en goedgekeurd door een kleine groep senior managers. Selma, de financieel directeur, heeft gevraagd om een fysieke kopie van het document te bekijken. Polina, haar assistent, staat op het punt om het voor haar te printen.

Prints vormen een groter beveiligingsrisico dan organisaties zich realiseren. Een van de typische beveiligings- en nalevingsrisico's betreft papieren documenten die uit de printer worden gepakt voordat ze door de gebruiker worden opgehaald (of die door de gebruiker volledig zijn vergeten), waardoor gevoelige of vertrouwelijke informatie bij onbevoegde personen terecht kan komen.

Door innovatie zijn er ook een reeks nieuwe beveiligingsrisico's bijgekomen. Moderne multifunctionele printers zijn net zo krachtig als een PC, met een harde schijf, geheugen en CPU, en zijn vaak verbonden met internet. Hierdoor is het mogelijk dat de printerfirmware het doelwit wordt van hackers die toegang proberen te krijgen tot het netwerk en bedrijfsgegevens.



GEHEIME WAPENS

imageRUNNER ADVANCE DX 4800

De imageRUNNER ADVANCE DX 4800 is gebouwd met standaard ingebouwde beveiliging. Polina kan het document alleen printen door zich met haar identiteitskaart bij het apparaat aan te melden. Dit betekent dat niemand anders toegang heeft tot het document dat in de printwachtrij staat en het niet in de lade van het apparaat blijft liggen.

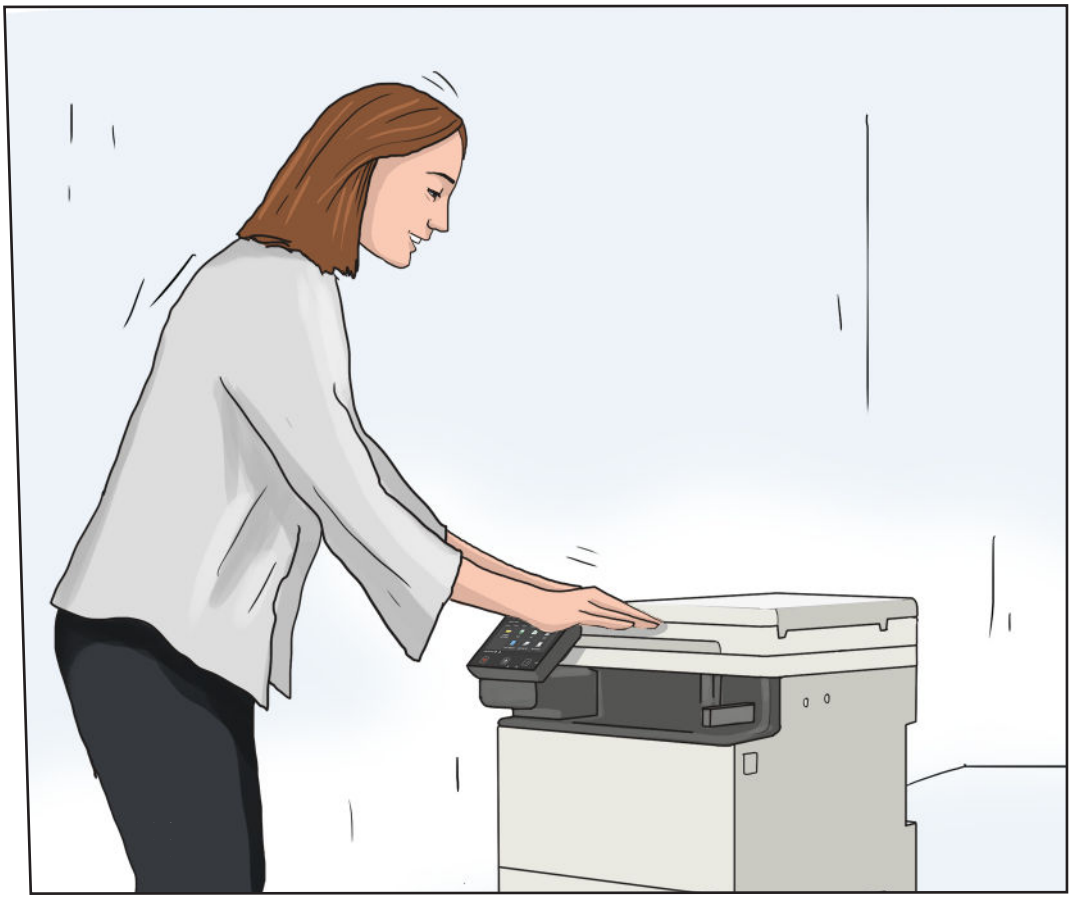
Het apparaat beschikt ook over Trellix McAfee Embedded Control, dat beschermt tegen zero-day- en APT-aanvallen (Advanced Persistent Threat) door de uitvoering van niet-geautoriseerde applicaties te blokkeren via intelligente whitelists. McAfee Embedded Control beschermt tegen ongeoorloofde manipulatie van het programma om te voorkomen dat een aanvaller het persbericht via een netwerkaanval in handen krijgt.

Ten slotte ondersteunt de imageRUNNER ADVANCE DX 4800 SIEM-integratie (Security Information Event Management). Hierdoor wordt het voor organisaties eenvoudiger om printers op te nemen in hun bestaande beveiligingssystemen (bijvoorbeeld Syslog). Deze systemen kunnen beveiligingsgebeurtenissen in een groep apparaten in realtime herkennen en markeren, zodat het bedrijf wordt gewaarschuwd bij problemen of bedreigingen zodra deze zich voordoen.

Device Hardening Service
Met Canon begint de beveiliging nog voordat u het apparaat hebt gekocht. Canon configureert haar multifunctionele imageRUNNER ADVANCE-apparaten om hun veiligheid te verbeteren, inclusief versterking van ingebouwde beveiligingscontroles en blokkering van niet-essentiële functies en onbeveiligde poorten. Het geconfigureerde apparaat wordt gecontroleerd en geverifieerd voordat het wordt verzonden.

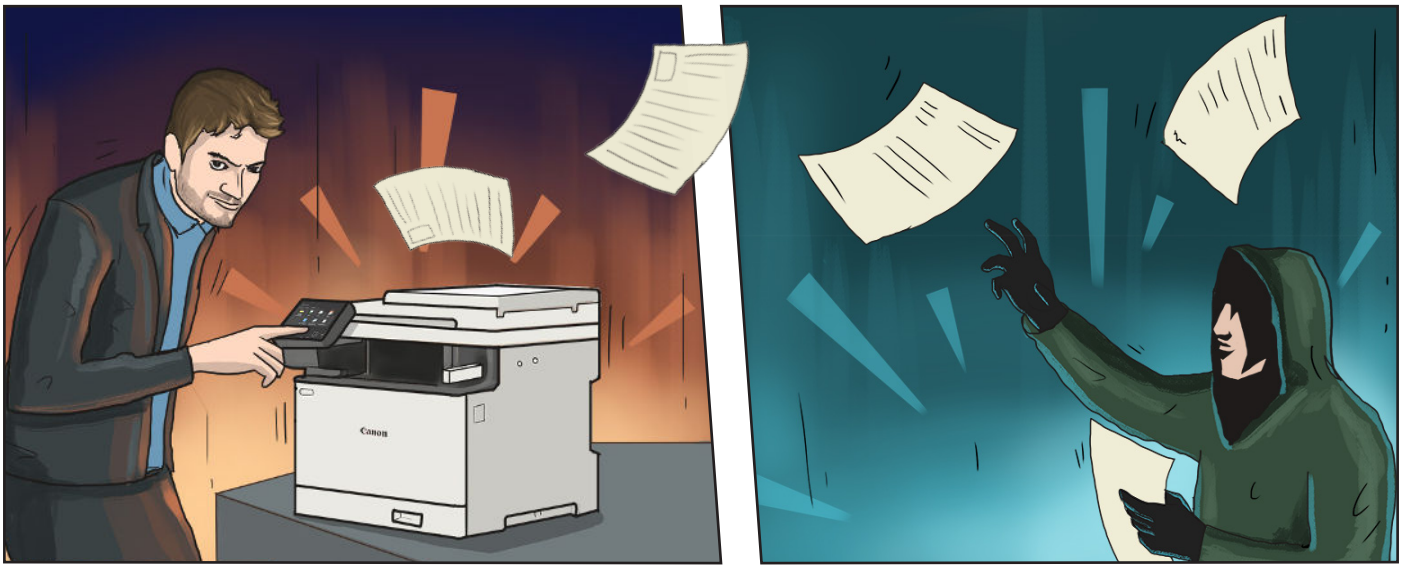
imageWARE Secure Audit Manager Express
Deze beveiligingsoplossing voor netwerkapparaten geeft Organisatie X inzicht in hun documentgerelateerde activiteiten. De oplossing kan de activiteiten op Canon-apparaten vastleggen, archiveren en controleren. Wanneer Polina het persbericht print, stuurt imageWARE Secure Audit Manager Express een e-mailwaarschuwing naar de IT-afdeling waarin staat dat er een document met een hoog risico wordt geprint. Zo kan Organisatie X onbevoegde medewerkers of partijen die proberen gevoelige informatie te kopiëren of te printen de pas afsnijden.

Selma heeft het persbericht nagekeken en voorzien van een aantal opmerkingen. Polina moet de feedback delen met Pierre, de PR-manager die verantwoordelijk is voor de aankondiging. Omdat Pierre vanuit huis werkt, moet Polina een digitale kopie maken en naar hem opsturen. Wanneer documenten worden gescand en rechtstreeks vanaf het apparaat worden gemaild, kan een aanvaller mogelijk de documenten onderscheppen.



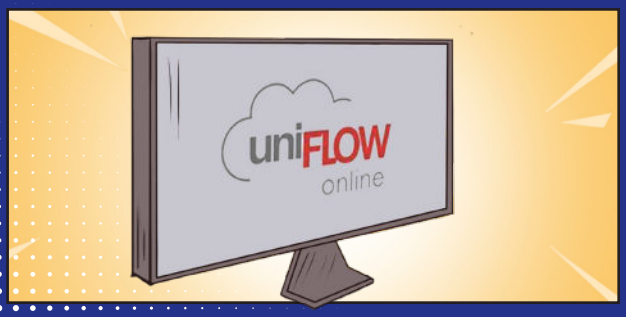
Scanners zijn tegenwoordig vaak verbonden met internet, waardoor gebruikers documenten rechtstreeks naar een ontvanger kunnen mailen of in de cloud kunnen opslaan. Als gevolg hiervan loopt digitale informatie vaker risico. Daarom is het dus van cruciaal belang dat scanners beschikken over robuuste beveiligingsfuncties. Zonder beveiligingsfuncties is een scanner kwetsbaar voor sabotage. Een interne gebruiker kan de e-mailrouteringswachtrijen wijzigen om bijvoorbeeld een e-mailtaak door te sturen naar een onbevoegde gebruiker. Zonder versleuteling kan een document bovendien eenvoudig worden geopend, bewerkt of geprint.

Externe aanvallers kunnen ook toegang krijgen via het netwerk en wijzigingen aanbrengen in e-mailmappen, zodat een document kan worden verzonden naar ontvangers buiten de organisatie. Of ze kunnen een via HTTPS verzonden document onderscheppen als het document en de bijbehorende gegevens niet zijn versleuteld.



GEHEIME WAPENS

i-SENSYS X C1333iF
Selma staat op het punt om het document te scannen met de i-SENSYS X C1333iF. Dit multifunctionele apparaat (met print- en scanfuncties) biedt functies voor veilig scannen om informatie te beschermen. Op het moment dat het apparaat wordt ingeschakeld, controleert de systeemverificatie bij het opstarten of er pogingen zijn gedaan om het apparaat te manipuleren en waarschuwt het Selma als er met het apparaat is geknoeid. Selma moet zich vervolgens aanmelden met een identificatiekaart, zodat er wordt vastgelegd wie informatie kopieert of deelt. Ten slotte biedt de IEEE802.1X-ondersteuning van de i-SENSYS X C1333iF een verificatiemechanisme. Wanneer het apparaat verbinding maakt met het LAN of WLAN van de organisatie, vindt automatisch verificatie van het apparaat op het netwerk plaats.



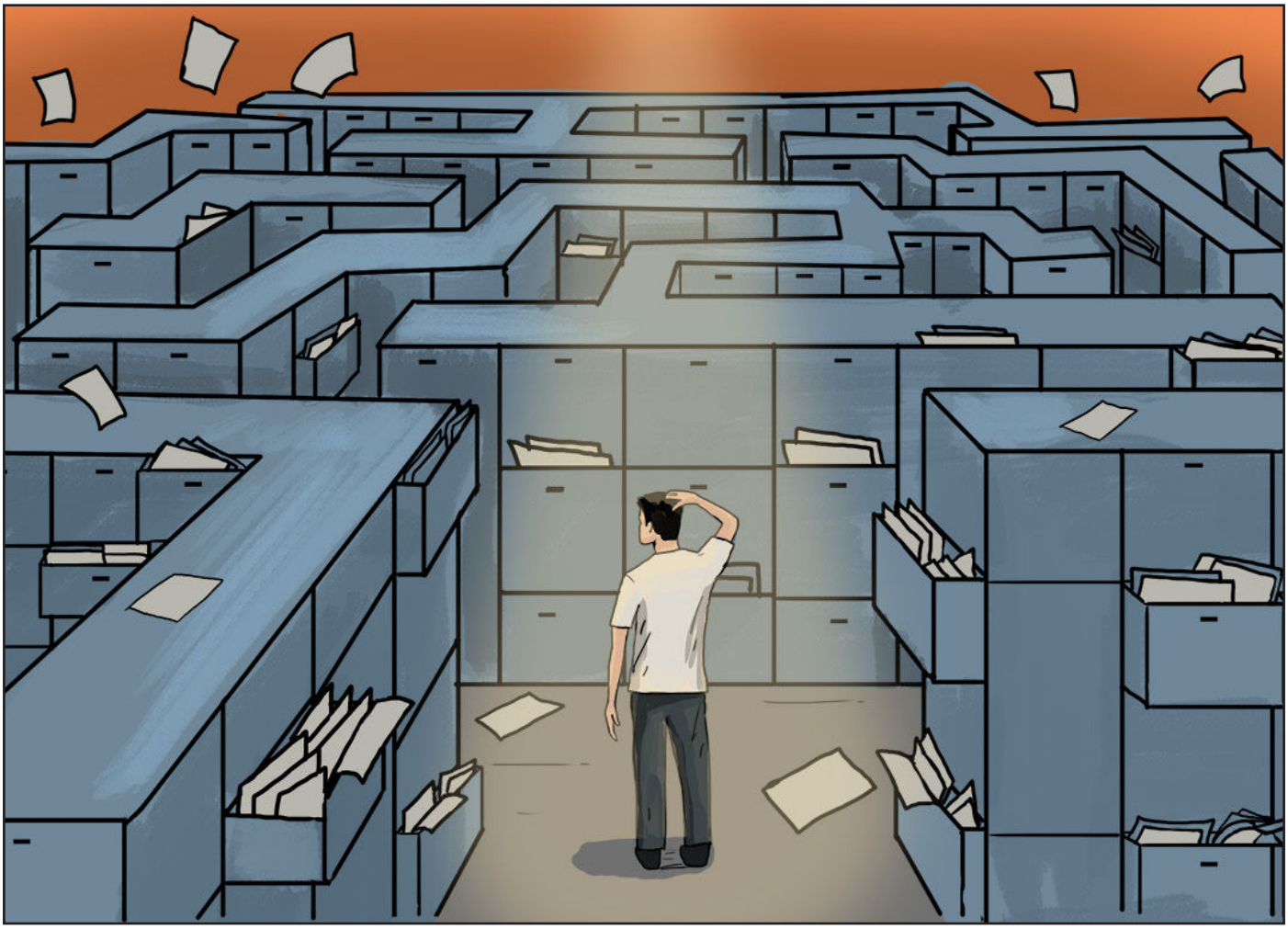
uniFLOW Online
Wanneer Selma het document scant, maakt uniFLOW Online een versleutelde PDF en biedt het optionele wachtwoordbeveiliging. Hiermee wordt voorkomen dat onbevoegde gebruikers het document kunnen bekijken, bewerken of printen, waardoor de informatie niet kan worden onderschept.

Tobias heeft gehoord dat de organisatie mogelijk een nieuwe richting op gaat. Als hoofd van een van de teams die het moeilijk heeft onder de huidige strategie, weet hij dat dit kan leiden tot een aanzienlijke inperking van zijn budget voor dit jaar, of zelfs tot het verlies van banen.

Tobias is gefrustreerd door het nieuws, dus hij neemt zich voor om te kijken of de geruchten kloppen en waar mogelijk collega's te waarschuwen. Hij denkt te weten waar het senior management de financiële documenten opslaat, en begint een geheime zoektocht naar alles wat mogelijk verband houdt met de nieuwe plannen.

Organisaties maken en bewaren elk jaar steeds meer informatie. Nu veel ook een hybride model gebruiken, wordt deze informatie over een toenemend aantal locaties verspreid, zowel fysieke als virtuele. Als gevolg daarvan worstelen organisaties vaak met lukrake opslagstrategieën, waarbij medewerkers van alles gebruiken om interne bedrijfsgegevens op te slaan, van archiefkasten tot persoonlijke cloudopslagservices zoals Dropbox.

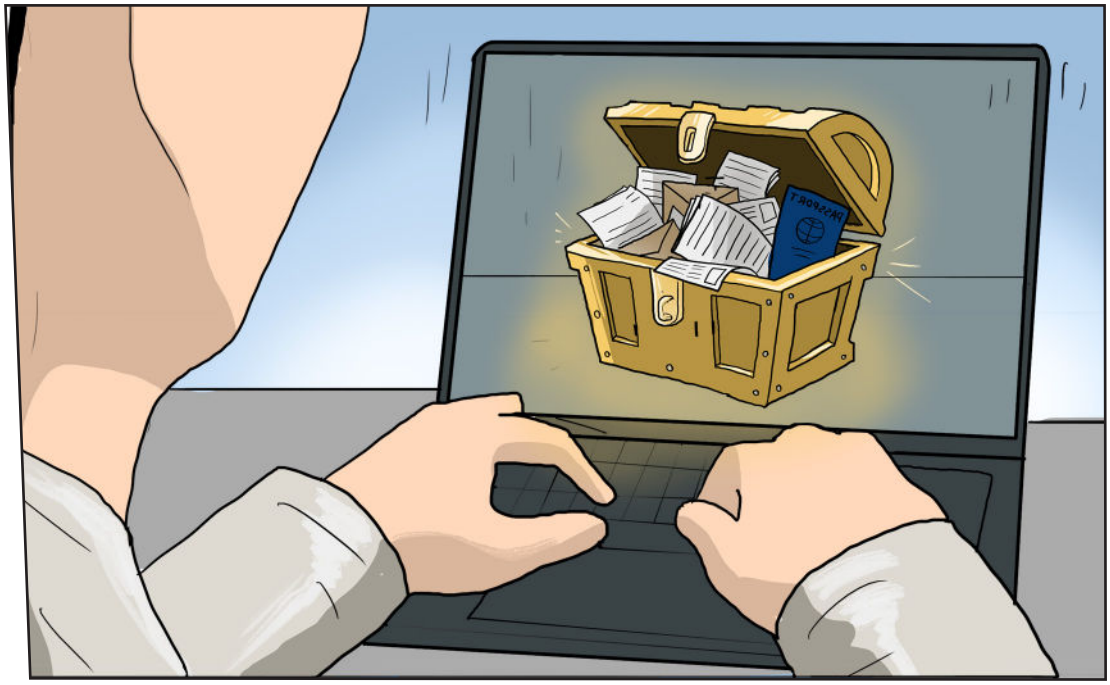
Bovendien verwerken medewerkers vaak gevoelige informatie zoals contracten, bankgegevens van het personeel, en financiële resultaten van het bedrijf. Het is voor IT-teams bijna onmogelijk om ervoor te zorgen dat best practices voor informatiemanagement worden toegepast wanneer documenten op een dergelijke manier worden opgeslagen, zelfs voor zulke kritieke gegevens.



GEHEIME WAPENS

Therefore Online
Dankzij de robuuste ingebouwde beveiliging stelt Therefore Online organisaties in staat om automatisch beleid in te stellen voor wie toegang heeft tot documenten en hoe informatie wordt opgeslagen, gedeeld of bewerkt. Toegangsfuncties voorkomen dat onbevoegde medewerkers zoals Tobias persoonlijke of gevoelige documenten zoals het persbericht kunnen openen.

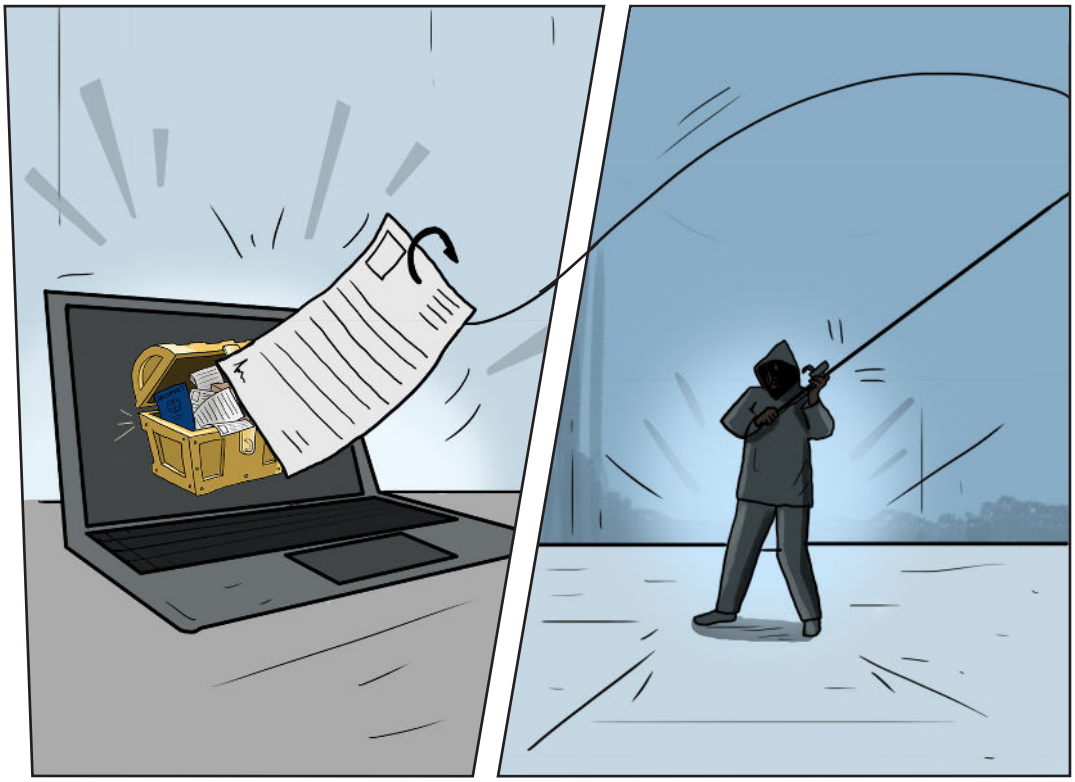
Therefore Online is cloudgebaseerd, zodat de locatie van de gebruiker geen invloed heeft op de toegankelijkheid. Geautoriseerde gebruikers die thuis werken of onderweg, hebben zo nog steeds toegang tot essentiële documenten. Elke interactie met een document wordt bijgehouden, zodat informatie strak wordt beheerd en van begin tot eind zichtbaar is, waardoor een digitale audittrail kan worden geboden.



Pierre wil de aankondiging onder embargo versturen naar verschillende ontvangers, waaronder belangrijke aandeelhouders en bepaalde journalisten. Het is van essentieel belang dat het document alleen naar deze contactpersonen wordt verstuurd; het mag niet in verkeerde handen terechtkomen.

Ondertussen moet hij voorzichtig zijn met de aanvullende informatie die Organisatie X geheim houdt. De bedrijfsdatabase bevat talloze parels: gevoelige gegevens over de ontvangers, waaronder hun e-mailadressen, telefoonnummers en, in het geval van de journalisten, paspoortgegevens van eerdere persreizen.

Deze gegevens zijn aantrekkelijk voor dieven, die deze gegevens kunnen gebruiken om de aankondiging vroegtijdig te laten uitlekken of met de gegevens van personen in de database identiteitsdiefstal of phishing-aanvallen te plegen.



Organisaties bewaren vaak zeer persoonlijke en vertrouwelijke informatie over hun klanten, partners en andere partijen waarmee ze nauw samenwerken. Deze informatie bevindt zich niet alleen op bedrijfsservers, maar ook in uitgaande communicatie zoals bankafschriften, facturen en correspondentie met deze partijen.
Het bewaren van deze informatie vormt een risico voor de organisatie, want als de informatie kwijtraakt of gestolen wordt door aanvallers, loopt de organisatie risico op aanzienlijke boetes en reputatieschade. Wanneer een organisatie met deze contacten communiceert, is het van cruciaal belang dat persoonlijke informatie in deze communicatie alleen de beoogde ontvanger bereikt.

GEHEIME WAPENS

Office Health Check
Office Health Check helpt organisaties hun IT-omgeving te controleren, om er vanaf het begin zeker van te zijn dat deze veilig is. De NCC Group, met wereldwijde experts in cybersecurity, voert hierbij een externe analyse uit van de interne en externe IT-infrastructuur van de organisatie, inclusief communicatiekanalen en poorten, om eventuele kwetsbaarheden aan het licht te brengen. Door eventuele problemen te identificeren, kan de organisatie voorkomen dat ze slachtoffer worden van een potentiële aanvaller, dat bijvoorbeeld de communicatie van Pierre wordt onderschept of dat gegevens van journalisten of aandeelhouders worden gestolen uit de databases van Organisatie X.

uniFLOW sysHUB
uniFLOW sysHUB biedt gebruikers strakke controle over en nauwkeurig toezicht op hun communicatie met de klant, waardoor Pierre er zeker van kan zijn dat de communicatie naar de juiste ontvangers gaat. Deze oplossing consolideert interne communicatieprocessen en -toepassingen in één workflow, die wordt beheerd vanuit één centrale locatie. uniFLOW sysHUB automatiseert deze workflow vervolgens om deze efficiënter te maken en het risico op fouten te verkleinen. Elke stap van de workflow wordt geregistreerd en opgeslagen in een sysHUB-bibliotheek voor latere controle en ter ondersteuning van audittrails, waardoor het voor een personeelslid moeilijk is om een document opzettelijk te lekken zonder dat dit wordt geregistreerd. Tevens kan Pierre de aflevering controleren om er zeker van te zijn dat de communicatie de juiste persoon heeft bereikt.

UITDAGING 2

VERTROUWELIJKE PERSONEELSAANWERVING

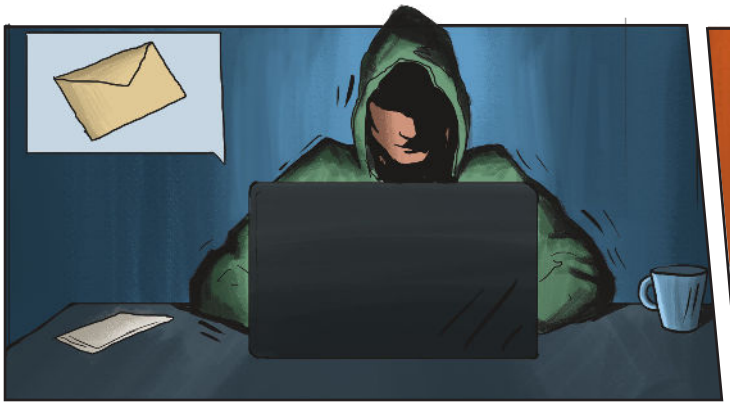
Organisatie Y wordt steeds groter en moet daarom nieuwe medewerkers aantrekken. Het personeel werkte vroeger op één locatie, maar door de opkomst van hybride werken, bevinden de medewerkers zich verspreid over het land. Het drukke HR-team heeft zich razendsnel moeten aanpassen aan de nieuwe situatie. Nieuwe medewerkers worden nu geregistreerd via virtuele wervings- en inwerkprocessen. Het HR-team moet op een tig aantal zaken letten, en over grote afstanden communiceren om vertrouwelijke documenten met betrekking tot nieuwe medewerkers te delen.

Het HR-team heeft veel macht en dus ook een grote verantwoordelijkheid. Het team heeft een berg waardevolle en gevoelige informatie in zijn bezit, van salarisgegevens van medewerkers tot gezondheids- en prestatierecords. De teamleden weten dat het aan hen is om deze informatie veilig te houden en te voldoen aan alle regelgeving. Auditors kunnen op elk moment opduiken en de HR-teamleden weten dat van hen wordt verwacht dat zij kunnen laten zien hoe informatie wordt opgeslagen en gedeeld. Dat is niet eenvoudig. Hoewel de medewerkers van het HR-team hard werken, hebben ze geen superkrachten. Het team kan door onopzettelijke fouten gemakkelijk in de problemen komen.

Zonder de juiste technologische oplossingen, kan dit problemen opleveren voor Organisatie Y.

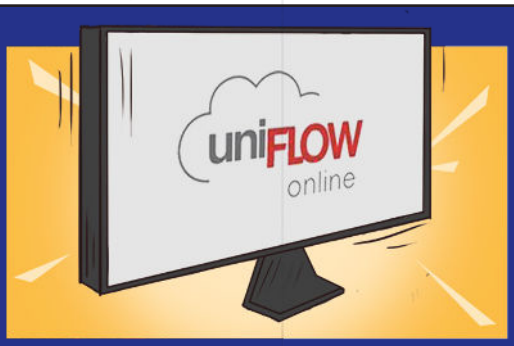
Na een succesvolle sollicitatie besluit Organisatie Y een nieuwe medewerker aan te nemen. De kandidaat heeft het hoofdkantoor bezocht om diens paspoort te verstrekken en zijn contract te ondertekenen bij Fatima, de wervingsmanager. Fatima wil kopieën van de documenten maken voor haar eigen administratie en deze delen met het hoofd HR dat thuis werkt. Fatima kan gemakkelijk per ongeluk de verkeerde ontvanger invoeren of het document opslaan op een locatie die voor iedereen toegankelijk is. Als de verkeerde persoon het document ontvangt, kan deze het zo openen en de informatie bekijken.

Organisaties zijn ervoor verantwoordelijk dat gescande documenten alleen kunnen worden bekeken door personen die daartoe bevoegd zijn. Een kleine fout kan leiden tot mogelijk gegevensverlies of -inbreuk, wat ernstige consequenties kan hebben voor de nalevingsintegriteit. Als de organisatie zich niet realiseert dat er sprake is geweest van een ernstig veiligheidsincident en verzuimt de inbreuk te melden, kan de toezichthouder voor gegevensbescherming de organisatie een boete van maximaal 4% van haar wereldwijde omzet opleggen.



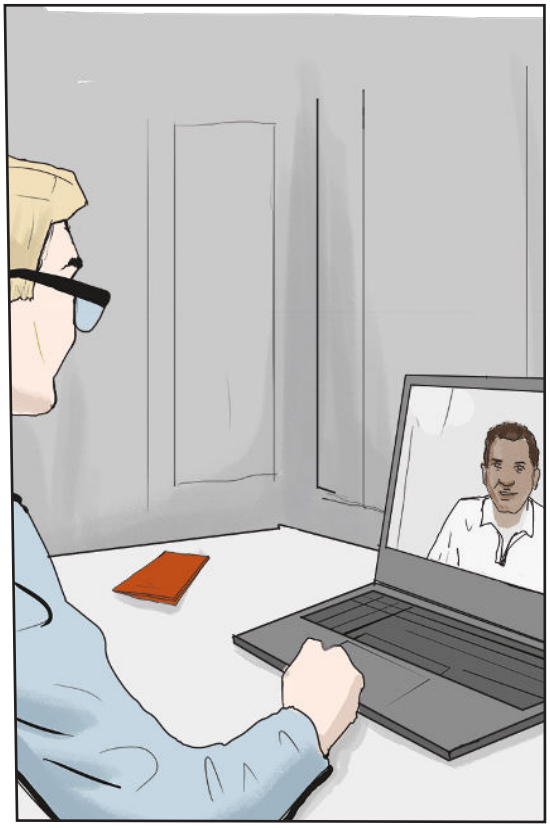
GEHEIME WAPENS

uniFLOW Online
uniFLOW Online biedt ingebouwde Secure Scan Workflows waarmee Organisatie Y specifieke scanworkflows voor elke gebruiker vooraf kan configureren. Documentworkflows zoals HR Onboarding zijn al vooraf gedefinieerd, waardoor Fatima de documentscan van een nieuwe medewerker niet op een onjuiste locatie kan opslaan.



imageFORMULA DR-S150
Fatima gaat het document scannen met de imageFORMULA DR-S150. Deze scanner biedt veiligheidsfuncties die de informatie veilig houden. Elke gebruiker moet zich aanmelden met een identificatiekaart, zodat alleen Fatima toegang heeft tot het vastgelegde document. Ook wordt automatisch versleuteling toegepast op de gedigitaliseerde versie, waardoor alleen een ontvanger met een wachtwoord het document kan lezen, bewerken en printen. imageFORMULA DR-S150 apparaten bieden ook opties voor het verzenden van documenten via beveiligde protocollen, zoals scannen naar FTPS, SFTP en SMTPS.

IRISPowerscan
De organisatie beschikt ook over IRISPowerscan, waarmee documenten bij het digitaliseren automatisch worden geïdentificeerd als een paspoort of contract. De software corrigeert scanfouten, zoals scheefstand, en gebruikt Optical Character Recognition om belangrijke details te herkennen, zoals de naam en het paspoortnummer van de medewerker. Deze informatie wordt aan de indexering toegevoegd, waardoor het voor de organisatie gemakkelijker wordt om deze informatie in de toekomst terug te vinden. Bovendien stuurt IRISPowerscan automatisch de contract- en paspoortscans naar de juiste veilige opslaglocatie in het bedrijfssysteem.



Tijdens het wervingsproces waren verschillende medewerkers, waaronder Fatima en haar collega Nick, betrokken bij het ondervragen van de sollicitanten en het beoordelen van cv's. Beide medewerkers werken online vanaf verschillende locaties in Europa. Zowel Fatima als Nick hebben kopieën van de cv's van de kandidaten en aantekeningen over hun sollicitaties opgeslagen op hun persoonlijke laptops en op gedeelde Dropbox-locaties. Zodra de nieuwe kandidaat de functie krijgt aangeboden, kunnen Fatima en Nick gemakkelijk vergeten om deze documenten te verwijderen.

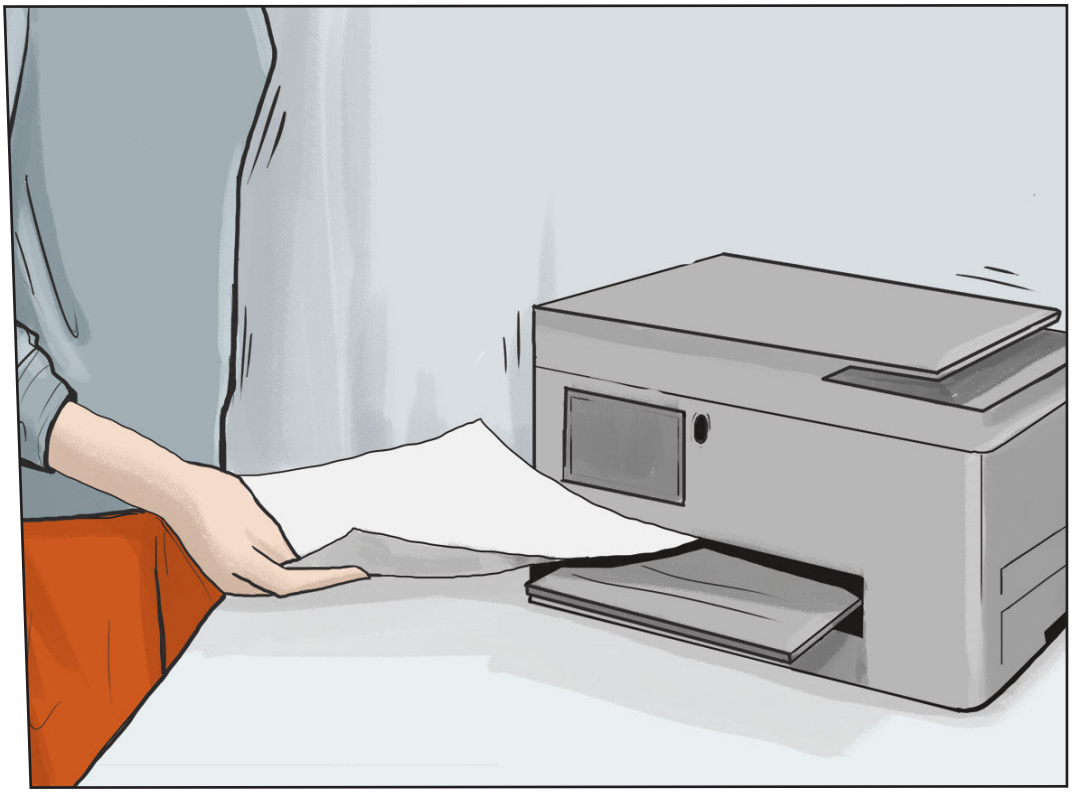
Recent aangescherpte wetgeving betekent dat naleving nog nooit zo belangrijk is geweest. Met wetgeving zoals de AVG zijn specifieke regels ingevoerd die bepalen hoe informatie moet worden opgeslagen. Organisaties mogen bijvoorbeeld persoonlijk identificeerbare informatie niet langer bewaren dan strikt vereist is. Veel organisaties worstelen echter nog steeds met lukrake opslagstrategieën, zonder officiële locaties om documenten op te slaan of de mogelijkheid om documenten te vinden die op hun eigen servers zijn opgeslagen.
Als een ex-medewerker of voormalig sollicitant een verzoek tot toegang tot diens opgeslagen informatie zou indienen, zou het voor de organisatie erg moeilijk zijn om aan te geven welke informatie het van die persoon in bezit heeft. Bovendien zou de organisatie moeite hebben om bij audits aan te tonen dat ze controle hebben over waar persoonlijk identificeerbare informatie wordt opgeslagen.

GEHEIME WAPENS

Therefore Online
Dankzij de robuuste ingebouwde beveiliging stelt Therefore Online organisaties in staat om automatisch beleid in te stellen voor wie toegang heeft tot documenten en hoe informatie wordt opgeslagen, gedeeld of bewerkt. Het houdt elke interactie met een document bij, zodat informatie strak wordt beheerd en van begin tot eind zichtbaar is, wat het auditproces veel eenvoudiger maakt.

Organisatie Y kan ook een automatisch gegevensretentiebeleid instellen om ervoor te zorgen dat oude documenten die gevoelige informatie bevatten, worden verwijderd na een conforme bewaarperiode, zodat automatisch aan de voorschriften wordt voldaan. Aangezien Therefore Online cloudgebaseerd is, kunnen teams ook wanneer ze op afstand werken, documenten uploaden en er zeker van zijn dat ze worden beschermd.

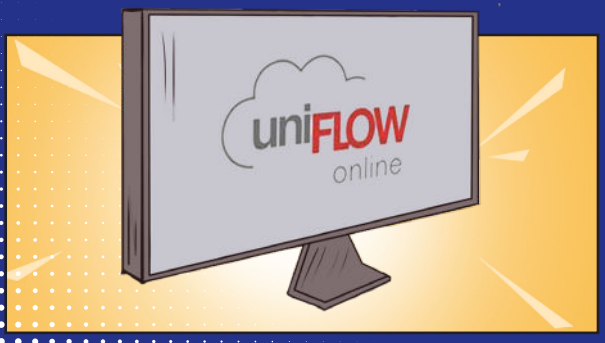
Ingrid, de nieuwe lijnmanager van de medewerker, werkt vanuit huis en bereidt een introductiegesprek voor dat de volgende dag op kantoor zal plaatsvinden. Ze wil hiervoor de brief waarin het salaris van de nieuwe medewerker wordt bevestigd samen met een aantal andere formulieren printen, om deze tijdens het gesprek te delen. Ingrid werkt pas sinds kort vanuit huis en heeft nog geen speciale werkprinter ontvangen, dus gebruikt ze haar eigen persoonlijke apparaat.



Het is voor organisaties gemakkelijk te vergeten dat printers een grote rol spelen in de beveiliging en conformiteit van workflows. Op deze apparaten staan namelijk waardevolle gegevens en documenten. Als onderdeel van hun wettelijke nalevingsverplichtingen, wordt van organisaties verwacht dat ze audittrails kunnen verstrekken waarmee wordt aangegeven hoe gevoelige informatie wordt gebruikt. Hiervoor dienen zij goed inzicht te hebben in de interactie tussen documenten en apparaten en zijn ze verplicht deze interactie nauwkeurig bij te houden. Omdat Ingrid echter haar eigen persoonlijke printer gebruikt, – die niet is verbonden met het bedrijfsnetwerk –, is er geen traceerbaarheid, geen registratie van de gegevens die op het apparaat zijn opgeslagen, en geen garantie dat deze veilig zijn.

GEHEIME WAPENS

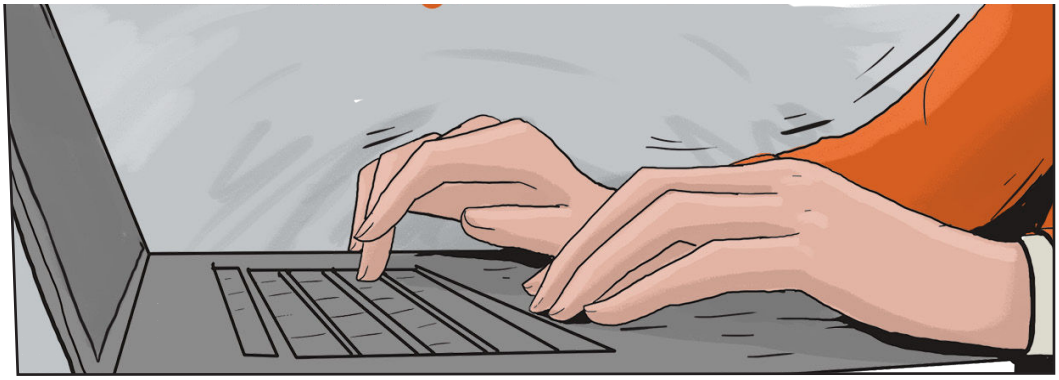
MAXIFY GX6050
Deze efficiënte desktopprinter produceert hoogwaardige prints voor thuiswerkers, maar zorgt er ook voor dat documenten veilig blijven en wordt voldaan aan de voorschriften dankzij de geïntegreerde integratie met uniFLOW Online. Dankzij de functie Scan to Myself kan Ingrid documenten alleen naar haar eigen e-mailadres of persoonlijke map verzenden. Zo wordt voorkomen dat ze per ongeluk zakelijke documenten naar persoonlijke contactpersonen verzendt. De functie voor het veilig vrijgeven van printopdrachten houdt in dat Ingrid alleen documenten print wanneer ze klaar is, zodat gevoelige zakelijke documenten niet op het apparaat achterblijven.



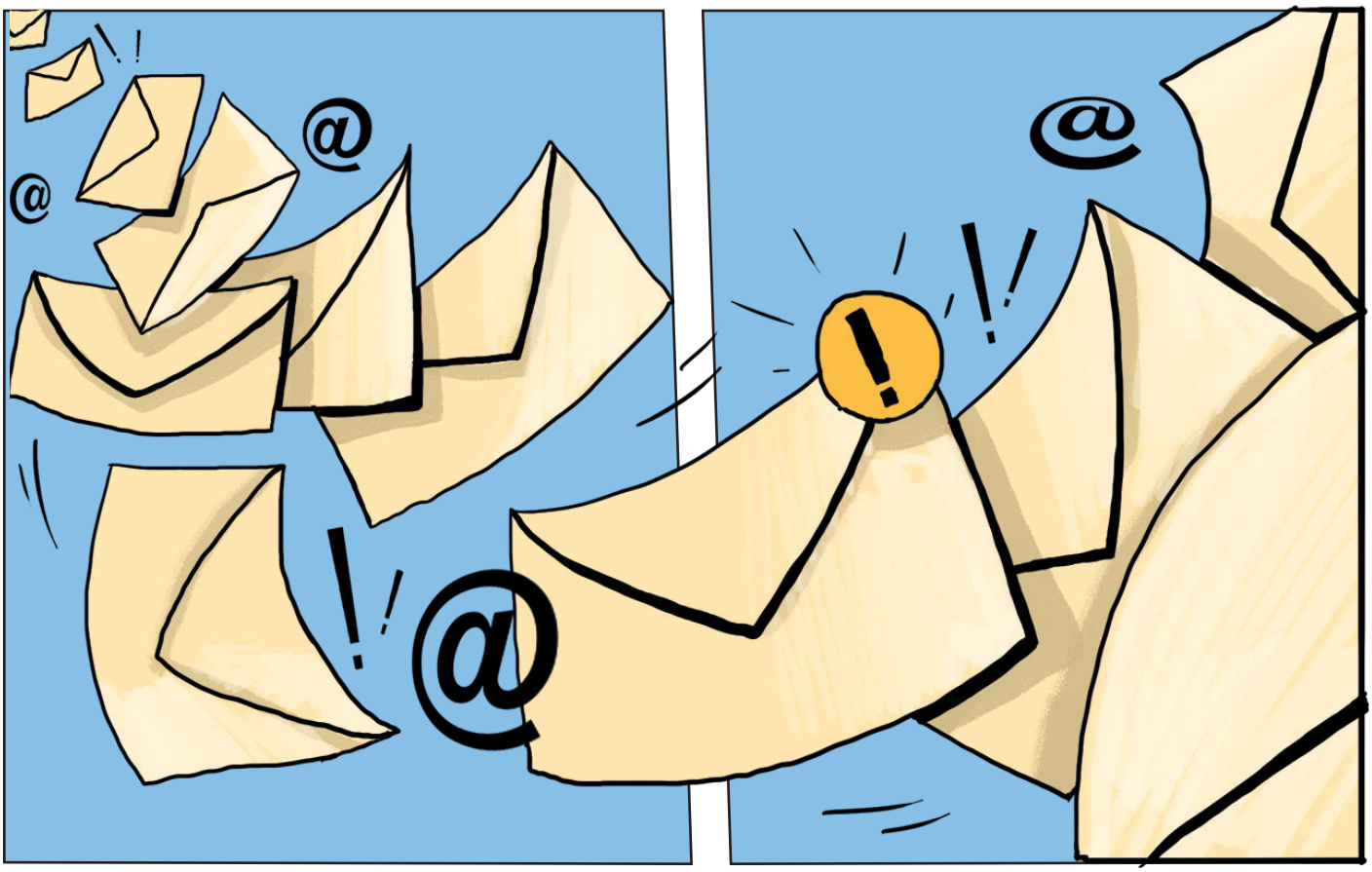
uniFLOW Online
Deze geïntegreerde software integreert de MAXIFY GX6050 met de omgeving van de organisatie, waardoor het IT-team van Organisatie Y de printactiviteiten van Ingrid kan volgen en nauwkeurig kan rapporteren hoe gevoelige informatie wordt gebruikt, zelfs wanneer ze thuis werkt.

Bij de indiensttreding bij het bedrijf kiest de nieuwe medewerker ervoor om enkele details over diens medische achtergrond bekend te maken. De medewerker wil graag dat zijn lijnmanager op de hoogte is van deze informatie om zijn ontwikkeling beter te kunnen ondersteunen. Fatima van HR stelt snel een e-mail op om deze naar Ingrid te versturen, de nieuwe lijnmanager. Er zijn echter twee medewerkers in de organisatie die Ingrid heten, en ze stuurt de e-mail per ongeluk naar de verkeerde contactpersoon.

De organisatie heeft nu de vertrouwelijkheid van de nieuwe medewerker geschonden. Het is mogelijk dat deze zich niet meer op zijn gemak voelt om bij het bedrijf te komen werken, en kan de organisatie nu voor de rechtbank dagen.



Communicatie is een risicovolle fase binnen elke documentworkflow, omdat er informatie wordt gedeeld, zowel intern met medewerkers als extern met klanten, leveranciers en andere belanghebbenden. In een standaard audit wordt van organisaties verwacht dat ze kunnen aantonen hoe gevoelige informatie met andere partijen wordt gedeeld. Gezien de enorme hoeveelheid communicatie die een organisatie in een bepaalde week verwerkt, is het van essentieel belang om oplossingen te hebben die het volgen en traceren van deze processen vergemakkelijken.



GEHEIME WAPENS

uniFLOW sysHUB
uniFLOW sysHUB biedt gebruikers strakke controle over en toezicht op hun interne communicatie, waardoor het voor Fatima eenvoudiger wordt om HR-communicatie vertrouwelijk te houden. De oplossing consolideert interne communicatieprocessen en -toepassingen in één workflow, die wordt beheerd vanuit één centrale locatie. uniFLOW sysHUB automatiseert de workflow om deze efficiënter te maken en het risico op fouten te verkleinen. In dit voorbeeld zou Fatima niet per ongeluk vertrouwelijke informatie naar een contactpersoon buiten de goedgekeurde HR-workflow kunnen verzenden.

Elke stap van de workflow wordt geregistreerd en opgeslagen in een sysHUB-bibliotheek voor latere controle en ter ondersteuning van audittrails. Dit betekent dat Fatima de aflevering kan controleren om er zeker van te zijn dat haar communicatie de juiste persoon heeft bereikt.

HOE KAN CANON U HELPEN?

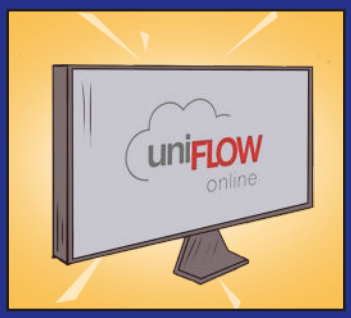
Elke organisatie wil haar informatie beschermen en aan regelgeving voldoen. Maar zoals Organisatie X en Y hebben laten zien, zijn er overal vijanden. Organisaties vechten niet alleen tegen meer schurken dan voorheen, maar strengere wetgeving betekent ook dat de gevolgen groot zijn wanneer er fouten worden gemaakt. Het lijkt misschien vechten tegen de bierkaai, maar dat hoeft niet zo te zijn. Het geheim ligt in het hebben van de juiste technologie en partner.

Canon is een leider in de IDC MarketScape voor print- en documentbeveiligingsoplossingen en -services en een leider in Quocirca's Print Security Landscape. Canon's hardware, software en services helpen uw organisatie zo efficiënt en effectief mogelijk te werken in een complexe wereld. De technologie van Canon ondersteunt elke werkomgeving, ongeacht waar uw mensen werken en hoe ver u bent met uw digitale transformatie.

Doordat Canon veiligheid vooropstelt bij haar oplossingen, wordt het voor u heel gemakkelijk uw informatie veilig te houden. De Canon-oplossingen zijn ontwikkeld om aanvallen te voorkomen, gegevens te beschermen en naleving te waarborgen, zodat u kunt profiteren van nieuwe mogelijkheden zonder uw team met extra werk op te zadelen.

APPARATEN VOOR PRINTEN EN SCANNEN
Canon's print- en scanportfolio is uitgerust met de nieuwste beveiligingsfuncties om kritieke gegevens in elke fase van de documentworkflow te beschermen. Alle Canon-producten worden tijdens de ontwerp- en ontwikkelingsfasen en voorafgaand aan de release gecontroleerd op veiligheid.

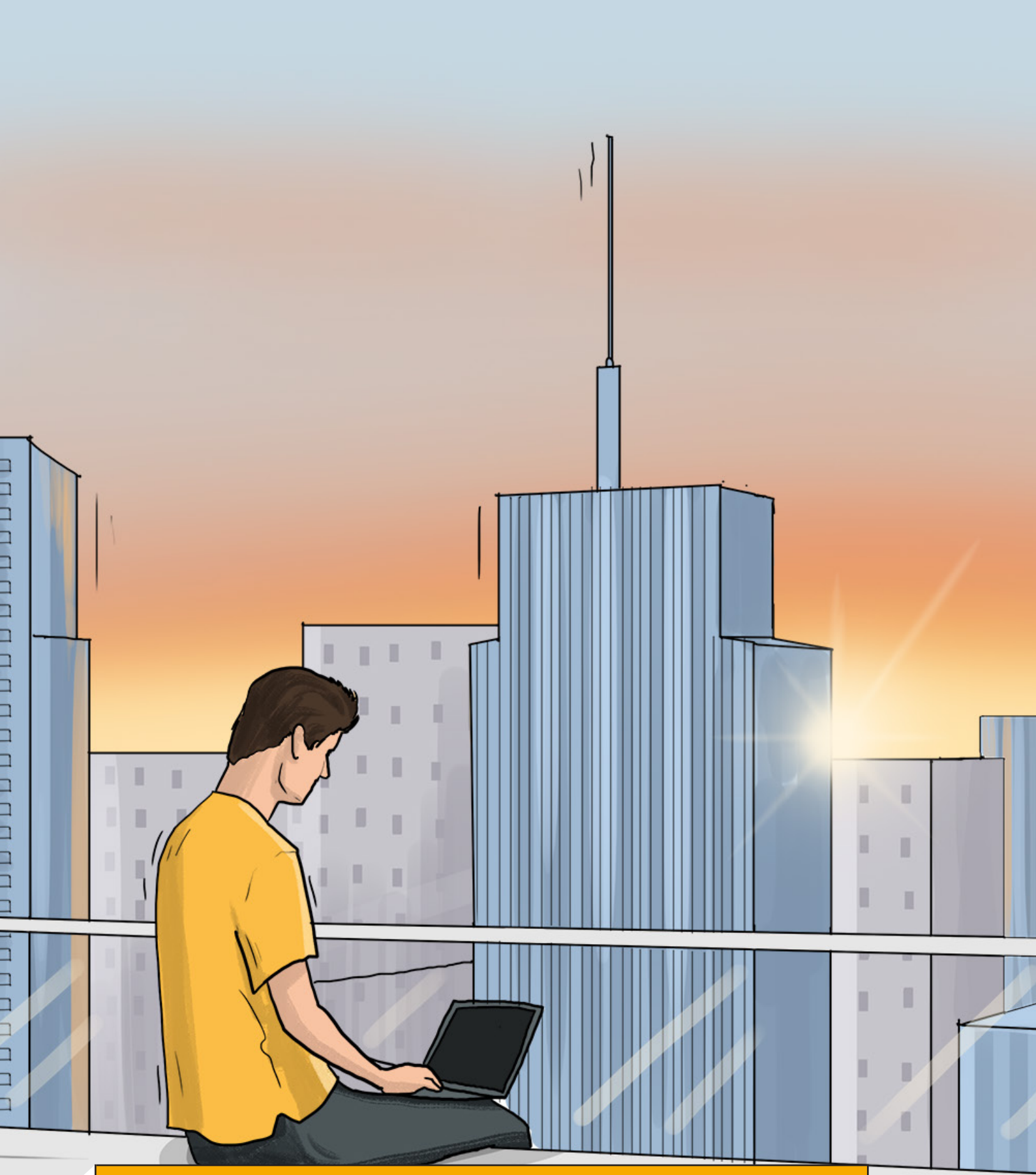
Canon blijft sterke partnerschappen aangaan met toonaangevende bedrijven in de branche, zoals Trellix en Microsoft, om de grootst mogelijke dekking en compatibiliteit te garanderen bij de beveiliging van groepen apparaten. Bovendien heeft Canon een speciaal team voor het reageren op productbeveiligingsincidenten.



SOFTWARE
Canon begrijpt dat informatie niet gebonden is aan locatie. Daarom biedt zij software die gegevens beschermt, waar die zich ook bevinden. Daarnaast werkt Canon samen met andere organisaties, zoals IOActive, om penetratietests uit te voeren in de releasefase en voor belangrijke software-updates.

SERVICES
De beveiligingsservices van Canon helpen u de regelgeving omtrent gegevensbescherming te blijven naleven en uw gevoelige gegevens te beschermen gedurende de levensduur van uw print- en scaninfrastructuur.

PASSPORT



Wilt u een effectieve oplossing voor uw beveiligings- en nalevingsproblemen? Bekijk de technologieën van Canon in actie in onze showroom of boek een demonstratie bij het deskundige Canon-verkoopteam om te zien wat de oplossingen van Canon voor uw organisatie kunnen betekenen.

Wilt u meer weten over de geheime wapens van Canon? Ga naar onze Digital Transformation Services-website voor meer informatie.

INFORMATIE OVER CANON

Canon maakt het verschil. Canon gebruikt haar kennis en jarenlange ervaring om verandering mogelijk te maken. Verandering bij Canon's klanten, bij een digitale transformatie en werken op nieuwe manieren. Bredere maatschappelijke veranderingen met voortdurende aandacht voor duurzaamheid als onderdeel van Canon's impact en cultuur.

Tot slot veranderingen bij Canon zelf, met de investering in nieuwe markten, producten en technologieën. Canon staat voor iedereen klaar: klanten, medewerkers en de samenleving in het algemeen.

CANON IS GEBOUWD OP VIER KERNWAARDEN:

Innovatie

Meer dan 80 jaar innovatie op het gebied van imaging met geavanceerde technologie als resultaat. Pionierswerk in de industrie en een sterke betrokkenheid bij toekomstige technologische ontwikkelingen.

Support

Een divers servicepakket om de hoogste kwaliteit te garanderen, voor optimale klanttevredenheid. Experts in huis die werken aan het verbeteren van efficiëntie en zich inzetten om Canon's klanten optimaal te ondersteunen.

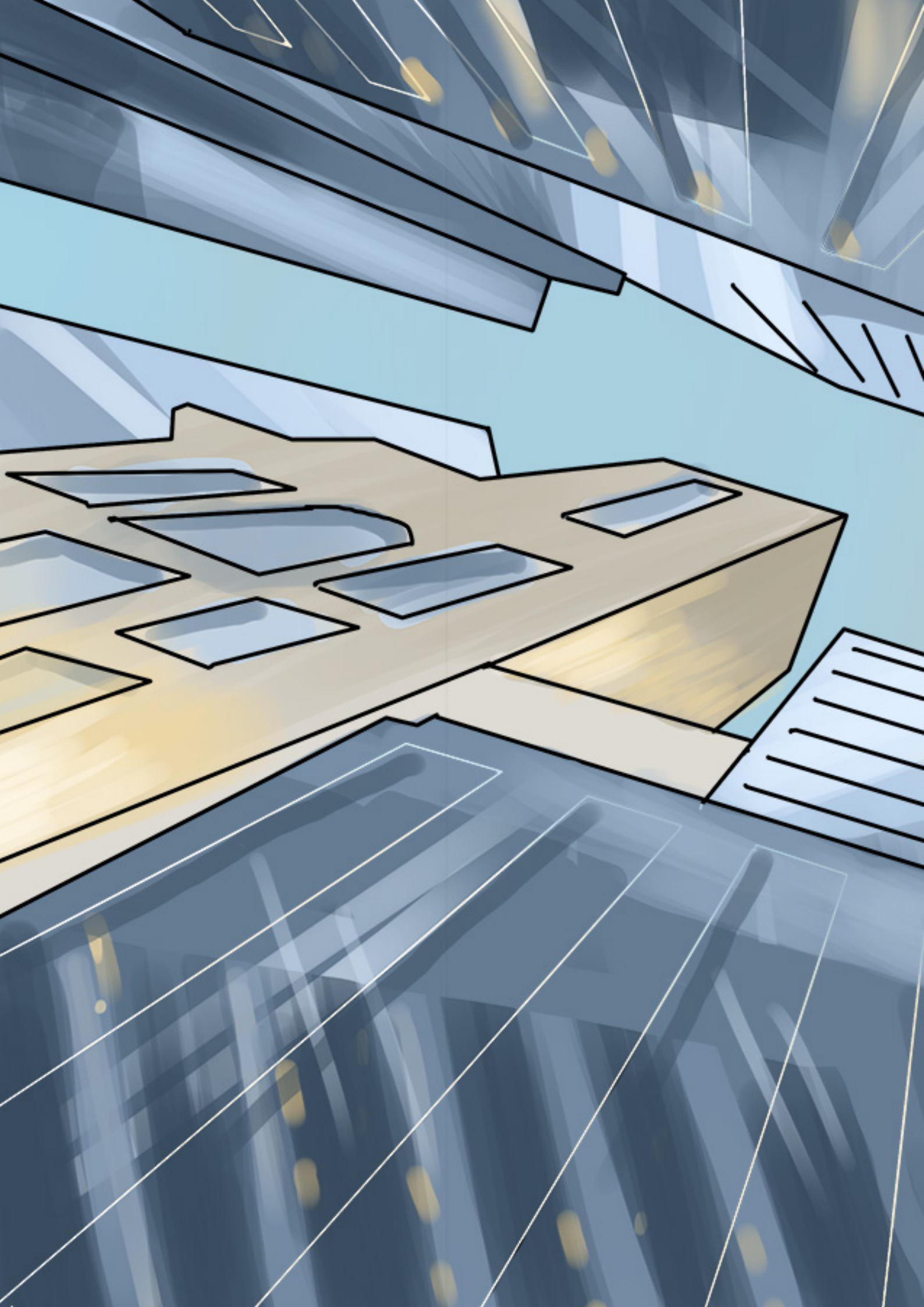
Beveiliging

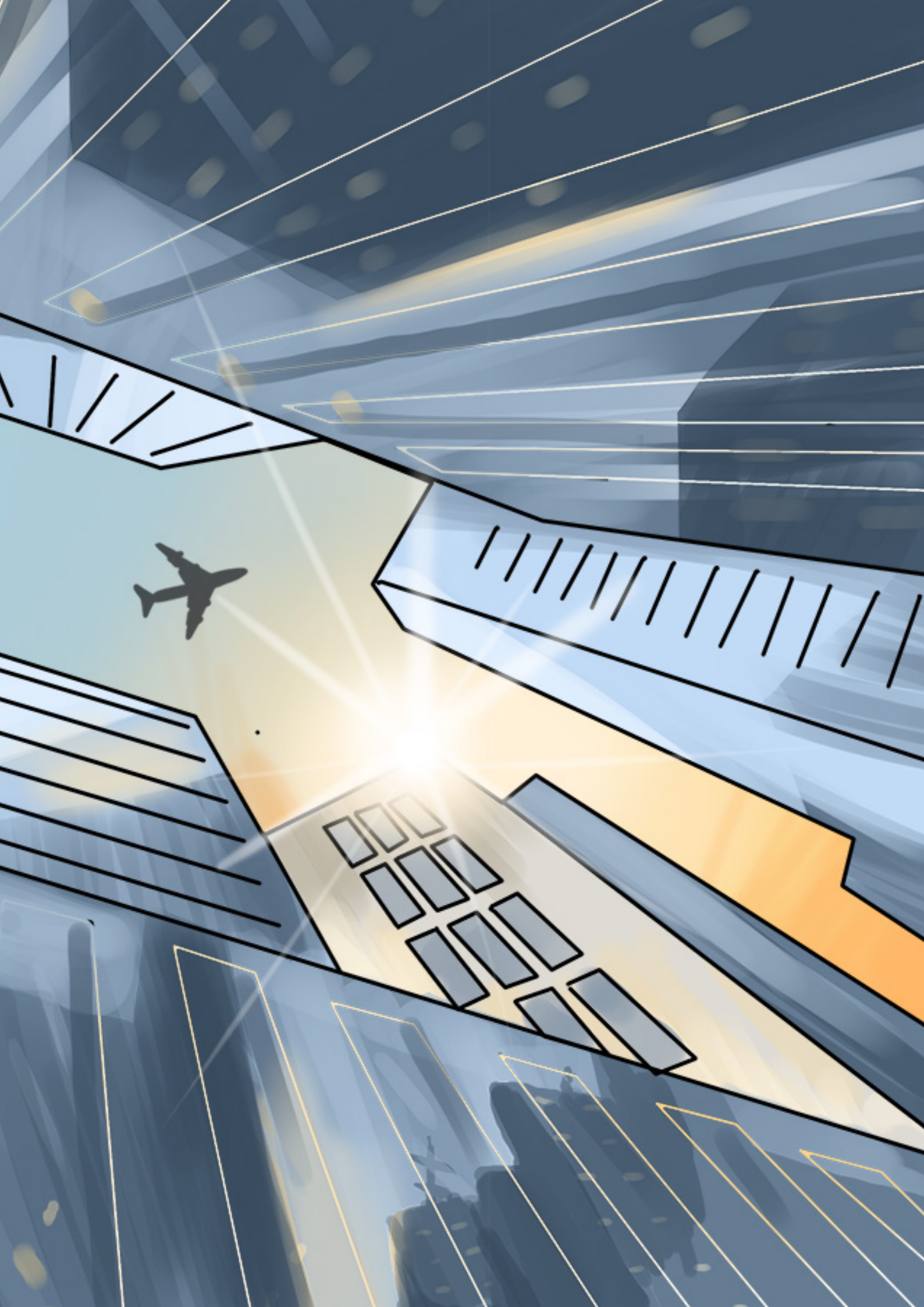
Canon's oplossingen en services helpen alle documenten en gevoelige gegevens te beveiligen, zowel op papier als digitaal, gedurende de hele documentlevenscyclus. Apparaten, oplossingen en services ontworpen vanuit het oogpunt van beveiliging.

Duurzaamheid

Canon's duurzaamheidsbeleid ligt op één lijn met de Duurzame Ontwikkelingsdoelstellingen van de VN, waaronder toezeggingen voor verlaging van de CO2-uitstoot tijdens de gehele levenscyclus van het product, door minder verpakking en consolidatie van distributiecentra.

AL DEZE EIGENSCHAPPEN SAMEN MAKEN CANON TOT DE JUISTE PARTNER.





Canon Inc.
Canon.com

Canon Nederland / Canon België
canon.nl / nl.canon.be
Dutch edition
© Canon Europa N.V., 2022

Canon Nederland N.V.
Brabantlaan 2
5216 TV 's-Hertogenbosch
Telefoon: (073) 6 815 815
canon.nl
b2b@canon.nl

Canon Belgium NV
Berkenlaan 3
1831 Diegem
Telefoon: 02 722 04 11
canon.be
contact@canon.be