INFORMATIONSSÄKERHET I PRAKTIKEN!

HUR SKYDDAR DU VERKSAMHETENS INFORMATION I EN VÄRLD DÄR CYBERHOTEN BLIR ALLT SMARTARE OCH EFTERLEVNADEN ALLT TUFFARE?

Canon

INNEHÅLL

Data är skatten i alla moderna organisationer. De maximerar din ekonomiavdelning, ger din ledningsgrupp förmågan att förutspå utvecklingar och ger dina medarbetare högre affärsintelligens.

Den här värdefulla resursen måste skyddas till varje pris.

I takt med att värdet på den här skatten fortsätter att öka, ökar även antalet fiender som försöker ta den: illasinnade angripare väntar på att stjäla information när du minst förväntar dig det. Samtidigt kan dubbelagenter försöka ta skatten själva.

Men det krävs mer än en fiende för att få en organisation på fall.

En stor kraft vakar över landet, så att alla följer reglerna för dataefterlevnad. Men även om lagarna är stränga och påföljderna är allvarliga, är det också enklare än någonsin att begå ett misstag.

Moderna företag är inte en stad omgärdad av en mur – i de flesta fall finns de inte ens på en och samma plats. Hybridarbete innebär att medarbetare lagrar, delar och samarbetar med information på fler platser än någonsin tidigare.

I en sådan komplicerad arbetsmiljö kan det verka som en omöjlig utmaning att skydda informationen och se till att processerna följer reglerna.

Du behöver en tillförlitlig partner som kan hålla skatten säker, skydda dig mot skurkar och hjälpa dina medarbetare att följa reglerna mot alla odds.

Låt oss utforska hur Canon och våra nycklar till framgång kan hjälpa dig att anta utmaningen.

UTMANINGAR I DOKUMENTETS LIVSCYKEL

Dokument skapas, kopieras, lagras och delas i organisationen under dess livscykel. Alla dessa steg utgör en utmaning när det gäller skydd och efterlevnad för data.

Utskrift är en utmaning när det kommer till säkerhet och efterlevnad, eftersom det är svårt att uppnå fullständig insyn i användar- eller dokumentaktiviteter, vilket kan leda till dataintrång

Scannade dokument som innehåller känslig information bör nå önskad destination på ett säkert sätt. Användarfel vid manuell datainsamling

Personuppgifter och känslig information om kunder och anställda måste lagras, behandlas och förstöras på ett säkert sätt, i enlighet med reglerna för datasekretess

Utgående kommunikation, dokument och data måste hanteras på ett säkert sätt för att undvika problem med informationsefterlevnad

UTMANING 1

DEN HEMLIGA STRATEGIN

Organisation X har en stor hemlighet: det är dags att ge sig ut på ett nytt äventyr. Ledningsgruppen har beslutat att investera i ett nytt affärsområde i hopp om att få ny kraft och upptäcka dolda rikedomar.

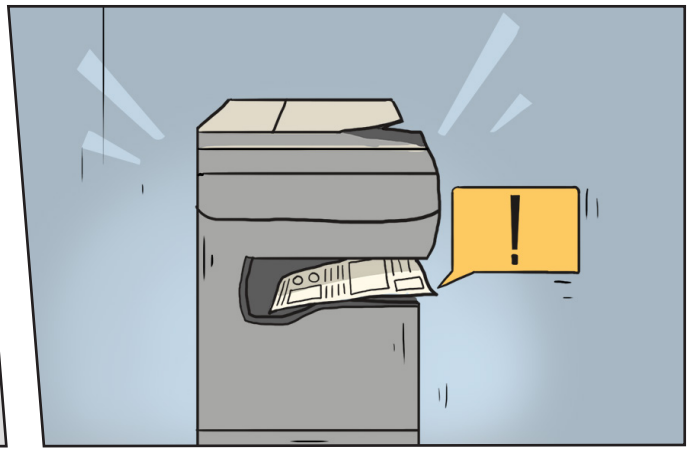
Det är viktigt att de här planerna förblir hemliga tills de offentliggörs. Nyheten skulle avslöja organisation X planer för konkurrenterna och förvarna dem om att det finns en ny konkurrent i sikte. Samtidigt står mycket på spel för medarbetarna hos organisation X – kan det finnas nya möjligheter på deras avdelning? Nya affärsområden att utforska? Eller är deras jobb hotade?

Ledningsgruppen måste gå försiktigt till väga så att deras planer inte hamnar i händerna på konspirerande medarbetare och externa fiender. Under budgeteringen och tillkännagivandet måste de undvika en rad fällor – från interna hot till skadlig programvara och nätverksattacker. Kan de skydda sin hemlighet?

Kommunikationsteamet har tagit fram ett pressmeddelande som återspeglar organisationens nya strategiska inriktning. Informationen är fortfarande topphemlig och tillkännagivandet håller på att skrivas och godkännas av en liten grupp högre chefer. Ekonomichefen Selma har bett om att få granska en fysisk kopia av dokumentet. Hennes assistent Polina är redo att skriva ut den åt henne.

Utskrift innebär ett större säkerhetshot än vad organisationer inser. Typiska risker med säkerhet och efterlevnad omfattar pappersdokument som tas från skrivaren innan de hämtas av användaren, eller glöms bort helt och hållet, vilket exponerar känslig eller konfidentiell information för obehöriga personer.

Innovation har också öppnat dörrarna för en mängd nya säkerhetshot. Moderna multifunktionsskrivare är lika kraftfulla som en dator, med hårddisk, minne och processor (CPU) och är ofta anslutna till internet. Hackare kan därför rikta in sig på skrivares fasta programvara för att få åtkomst till nätverket och företagsdata.



NYCKLAR TILL FRAMGÅNG

imageRUNNER ADVANCE DX C5800

imageRUNNER ADVANCE DX C5800 är byggd med inbyggd säkerhet som standard. Polina kan bara skriva ut dokumentet om hon loggar in på enheten med sitt ID-kort, vilket innebär att ingen annan kan komma åt dokumentet som står i kö för att skrivas ut och det lämnas inte kvar i enhetsfacket.

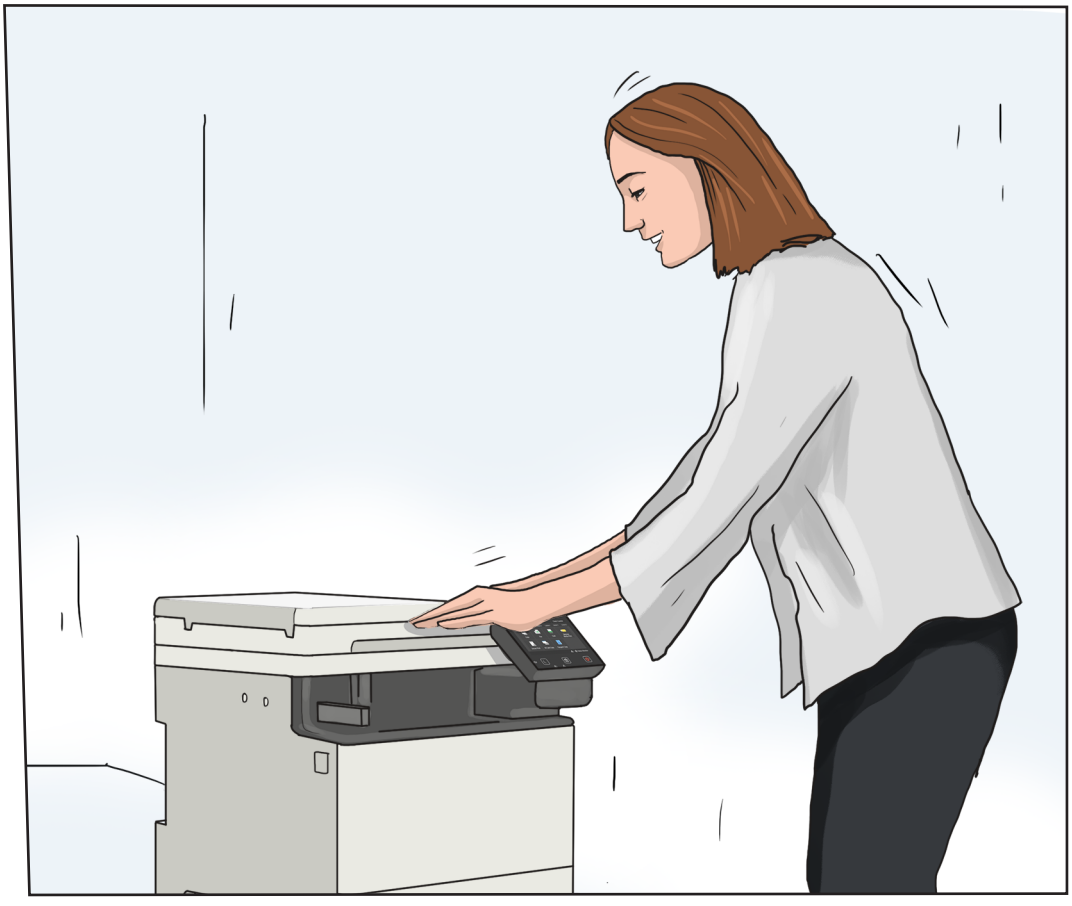
Enheten erbjuder även Trellix McAfee Embedded Control, som skyddar mot dagnollattacker och attacker med avancerade beständiga hot (APT) genom att blockera körning av obehöriga program genom intelligent vitlistning. För att förhindra att en angripare får tag på pressmeddelandet via en nätverksattack skyddar McAfee Embedded Control mot programmanipulering.

Slutligen stöder imageRUNNER ADVANCE DX C5800 integrering med Security Information Event Management (SIEM), vilket gör det enklare för organisationer att inkludera skrivare i sina befintliga säkerhetsövervakningssystem (till exempel Syslog). Dessa system kan identifiera och flagga säkerhetshändelser för enheter i realtid och varna företaget om eventuella problem eller hot när de inträffar.

Enhetsskyddstjänst
Med Canon börjar säkerheten innan du ens har köpt en enhet. Vi konfigurerar imageRUNNER ADVANCE multifunktionsenheter för att stärka deras säkerhet, bland annat förstärkning av inbyggda säkerhetskontroller och blockering av icke-väsentliga funktioner och osäkra portar. Den konfigurerade enheten kontrolleras och verifieras innan den levereras.

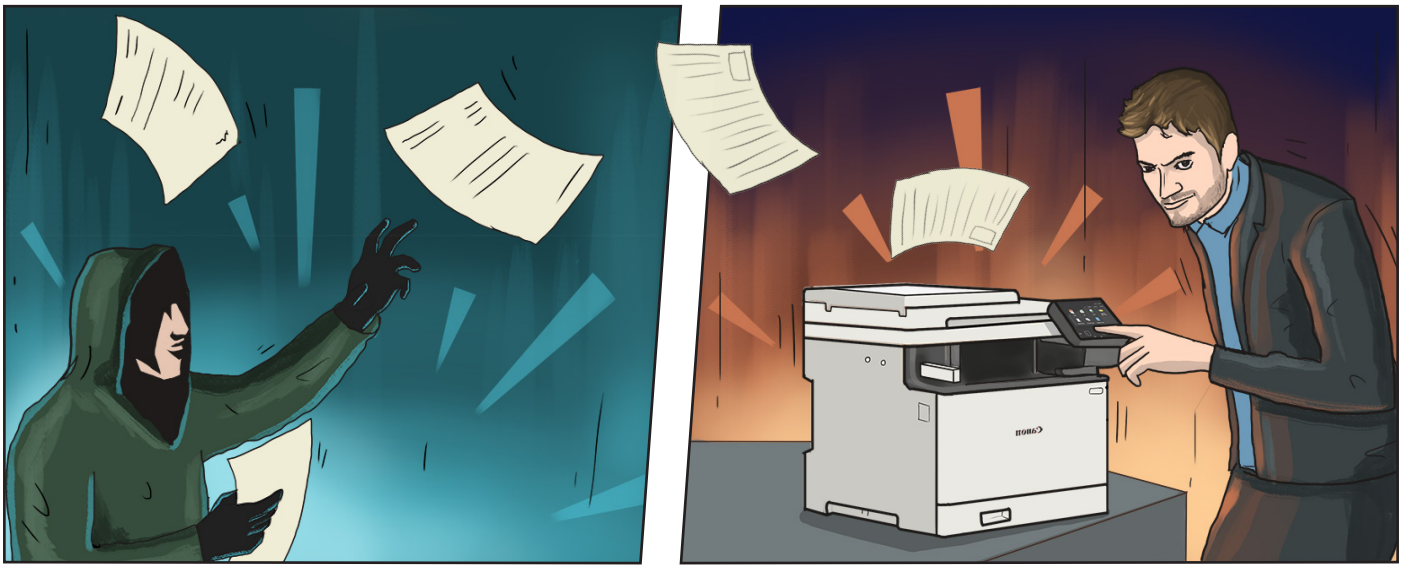
imageWARE Secure Audit Manager Express
Den här säkerhetslösningen för nätverksenheter ger företaget X en översikt över sina dokumentrelaterade aktiviteter. Den kan registrera, arkivera och granska de aktiviteter som sker på Canon-enheter. När Polina skriver ut pressmeddelandet utlöser imageWARE Secure Audit Manager Express en e-postvarning om att ett högriskdokument skrivs ut. Det hjälper organisation X att hålla sig informerad om obehöriga medarbetare eller parter som försöker kopiera eller skriva ut känslig information.

Selma har granskat pressmeddelandet och lämnat några skriftliga kommentarer. Polina måste dela med sig av återkopplingen till Pierre, PR-ansvarig, som ansvarar för tillkännagivandet. Eftersom Pierre arbetar hemifrån måste Polina skapa en digital kopia för att skicka det till honom. Att scanna dokument och skicka dem via e-post direkt från enheten skapar en möjlighet för angriparen att fånga upp dokumentet.



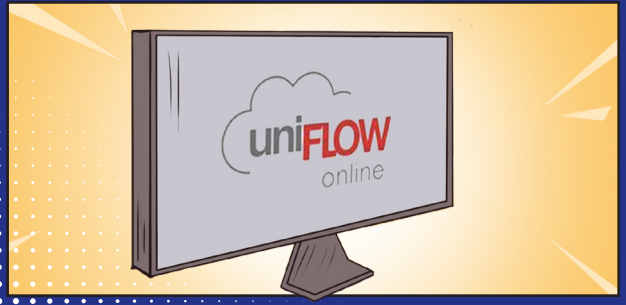
Dagens scanningsenheter är ofta anslutna till internet, vilket gör att användare kan skicka dokument direkt till en mottagare eller spara dem på molndestinationer. Det innebär att det finns fler sätt att utsätta digital information för risker, så det är viktigt att scanningsenheter har robusta säkerhetsfunktioner. Utan säkra funktioner är en scanner sårbar för manipulering – en intern användare kan till exempel ändra e-postflödesköer för att skicka ett e-postjobb till en obehörig användare. Utan kryptering kan ett dokument helt enkelt öppnas, redigeras eller skrivas ut.

Ur ett externt perspektiv kan en angripare även få åtkomst via nätverket och göra ändringar i e-postkataloger, vilket gör att ett dokument kan skickas till mottagare utanför organisationen. De kan även fånga upp ett dokument som överförs via HTTPS om det och dess data inte är krypterade.



NYCKLAR TILL FRAMGÅNG

i-SENSYS X C1333iF
Selma är redo att scanna dokumentet med i-SENSYS X C1333iF. Den här multifunktionsenheten (med både utskrifts- och scanningsfunktioner) har säkra scanningsfunktioner som hjälper till att skydda informationen. Från ögonblicket den startas kontrollerar funktionen systemverifiering vid start om det har gjorts några försök att äventyra enhetens integritet och kan varna Selma om den har manipulerats. Selma måste sedan logga in med ett ID-kort och se till att det finns ett register över vem som kopierar eller delar information. Slutligen tillhandahåller stödet för i-SENSYS X C1333iF:s IEEE802.1X en autentiseringsmekanism, så när den ansluts till företagets LAN eller WLAN bekräftar den dess äkthet.



uniFLOW Online
När Selma scannar avtalet skapar uniFLOW Online en krypterad PDF-fil och erbjuder valfritt lösenordsskydd. Det förhindrar att obehöriga användare ser, redigerar eller skriver ut dokumentet, och skyddar informationen från alla som försöker komma åt den.

Tobias har hört att företaget är på väg att ta en ny riktning. Som chef för ett av de team som kämpar med den aktuella strategin vet han att det kan innebära allvarliga nedskärningar av budgeten i år eller till och med utgöra ett hot mot jobb.

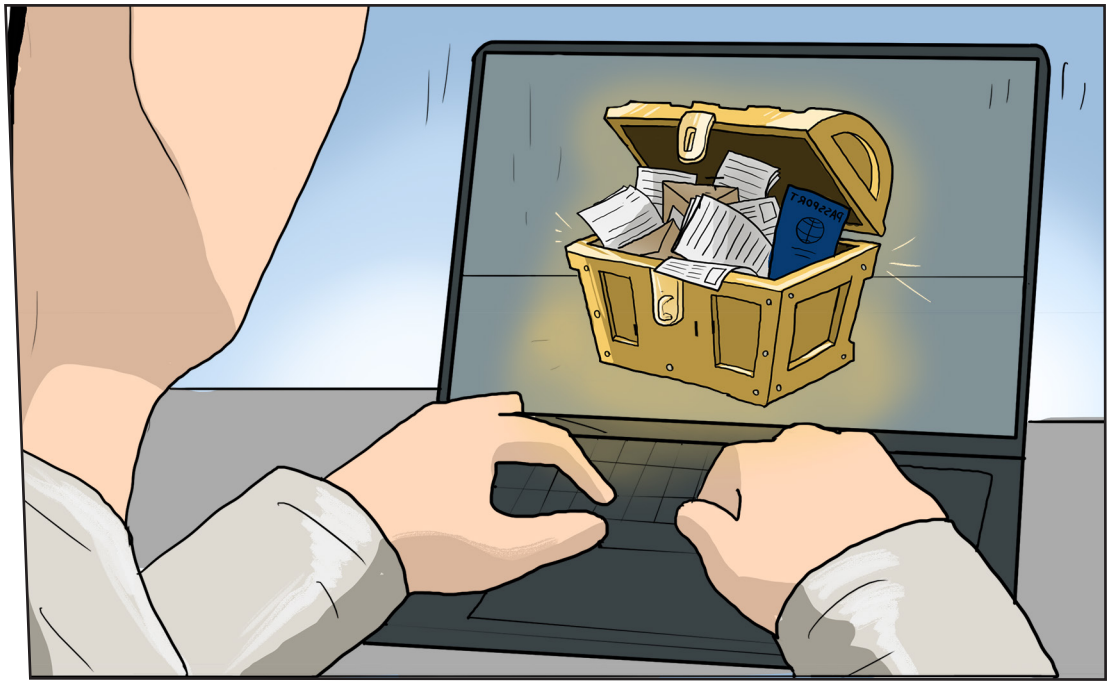
Tobias är frustrerad över nyheterna, så han försöker bekräfta ryktena och eventuellt varnar kollegor. Eftersom han tror att han vet var ledningen skulle lagra sina finansiella dokument börjar han en hemlig sökning efter allt som kan vara kopplat till de nya planerna.

Organisationer skapar och lagrar allt mer information varje år. I och med att många nu även använder hybridmodeller sprids den här informationen över allt fler platser, både fysiskt och virtuellt. Därför är det vanligt att organisationer kämpar med slumpmässiga lagringsstrategier, med medarbetare som använder allt från arkivskåp till personliga molnlagringstjänster, till exempel Dropbox, till företagsdata.
Dessutom hanterar medarbetare ofta känslig information som avtal, personalens bankuppgifter och företagets ekonomiska resultat. Även med viktiga data som dessa är det nästan omöjligt för IT-team att säkerställa informationshantering med bästa praxis när dokument lagras på ett sådant sätt.

NYCKLAR TILL FRAMGÅNG

Therefore Online
Tack vare robust inbyggd säkerhet ger Therefore Online organisationer möjlighet att upprätta automatiska policyer avseende vem som har åtkomst till dokument, hur uppgifter lagras, delas eller redigeras. Åtkomstkontroller förhindrar att obehöriga medarbetare som Tobias öppnar privata eller känsliga dokument som pressmeddelandet.

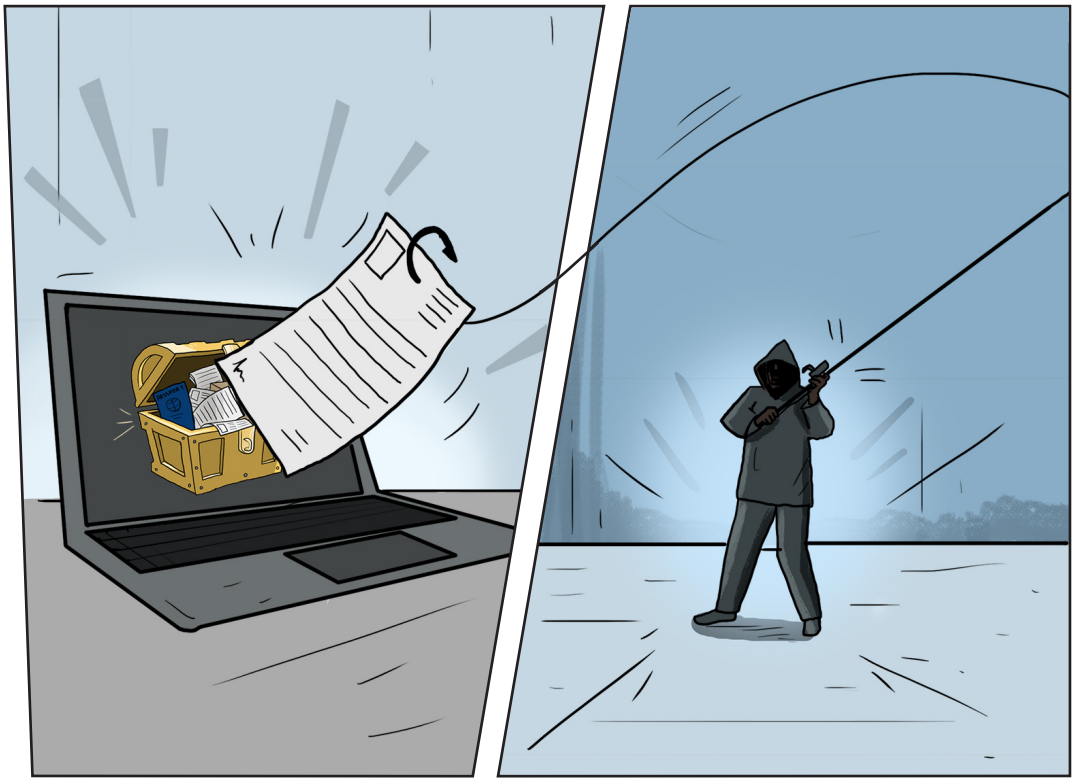
Therefore Online är molnbaserat, vilket säkerställer att en användares plats inte påverkar tillgängligheten. Behöriga användare som arbetar hemifrån eller på resande fot har fortfarande åtkomst till viktiga dokument. All interaktion med ett dokument spåras, vilket säkerställer att informationen hanteras säkert och är synlig från början till slut, vilket ger en digital verifieringskedja.



Pierre förbereder sig för att skicka ut tillkännagivandet under embargo till mottagare, bland annat viktiga aktieägare och utvalda journalister. Det är viktigt att dokumentet endast skickas till de här kontakterna. Han kan inte riskera att det hamnar i fel händer.

Samtidigt måste han vara försiktig med den extra information som organisation X håller hemlig. Företagsdatabasen innehåller otaliga juveler: känsliga uppgifter om mottagarna, däribland deras e-postadresser, telefonnummer och, vad gäller journalister, passinformation från tidigare pressresor.

Dessa data är en potentiell guldgruva för tjuvar som kan använda dessa uppgifter för att läcka tillkännagivandet för tidigt eller använda information om personer i databasen för att utföra identitetsstöld eller nätfiskeattacker.

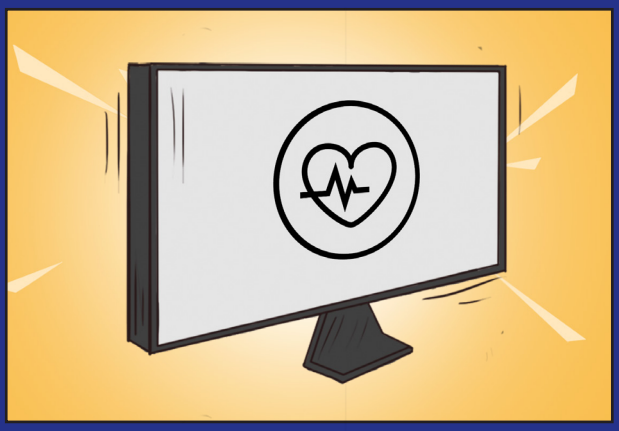


Företag har ofta mycket personlig och konfidentiell information om sina kunder, partner och andra parter som de har ett nära samarbete med. Den här informationen finns inte bara på företagets servrar utan ingår i utgående kommunikation som kontoutdrag, fakturor och korrespondens med dessa parter.

Det medför även en risk för företaget att inneha den här informationen eftersom det kan innebära att företaget får stora böter och ett skadat anseende om den försvinner eller stjäls av angripare. Om en organisation kommunicerar med dessa kontakter är det mycket viktigt att personuppgifter i dessa meddelanden endast når mottagaren.

NYCKLAR TILL FRAMGÅNG

Säkerhetskontroll på kontoret
Säkerhetskontroll på kontoret hjälper organisationer att granska sin IT-miljö för att säkerställa att den är säker från början. Den globala cybersäkerhetsexperten NCC Group utför en fjärranalys av organisationens interna och externa IT-infrastruktur, bland annat kommunikationskanaler och portar, för att avslöja eventuella sårbarheter. Genom att identifiera eventuella problem kan organisationen undvika att de utnyttjas av en potentiell angripare, vilket förhindrar att Pierres meddelanden fångas upp eller att journalisters eller intressenters data stjäls från organisationen X databaser.



uniFLOW sysHub
uniFLOW sysHUB ger användare god kontroll och översikt över sin kundkommunikation, vilket gör det enklare för Pierre att säkerställa att meddelandet når rätt destination. Den här lösningen samlar processer för intern kommunikation och program i ett arbetsflöde som hanteras från en och samma plats. uniFLOW sysHUB automatiserar sedan det här arbetsflödet för att göra det mer effektivt och minska risken för fel. Varje steg i arbetsflödet loggas och lagras i ett sysHUB-bibliotek för senare granskning och för att stödja verifieringskedjor, vilket gör det svårt för någon i personalen att avsiktligt läcka ett dokument utan att det registreras. Samtidigt kan Pierre kontrollera leveransbekräftelsen för att säkerställa att meddelandet har nått rätt person.

UTMANING 2

DEN KONFIDENTIELLA ANSTÄLLNINGEN

Organisation Y måste locka nya medarbetare för att driva sitt växande kungarike. Personalen brukade befinna sig på en enda plats, men i och med hybridarbete har de orädda medarbetarna spritt ut sig över hela landet. Det upptagna HR-teamet har behövt anpassa sig snabbt. Nya medarbetare registreras nu via virtuella anställnings- och introduktionsprocesser. HR-teamet måste ha ögon överallt och kommunicera över stora avstånd för att kunna dela konfidentiella dokument med nykomlingar.

HR-teamets stora kraft medför ett stort ansvar: de besitter ett berg av värdefull och känslig information, från medarbetarnas löneuppgifter till deras hälsostatus och prestationsregister. De vet att det ligger på dem att skydda den här informationen och följa gällande lagstiftning. Granskarna är aldrig långt borta och HR-teamet vet att de förväntas visa hur information lagras och delas. Det är inte enkelt. Trots att HR-teamet arbetar hårt har de inga superkrafter. Det är lätt hänt att olyckor och fel försätter teamet i trubbel.

Utan rätt tekniska lösningar för att rädda dagen kan detta innebära problem för organisation Y.

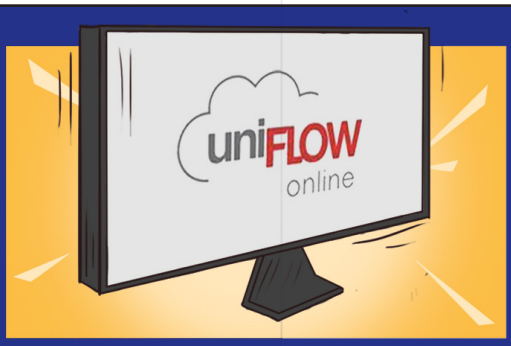
Efter en lyckad intervjuprocess har organisation Y beslutat att anställa en ny medarbetare. Kandidaten har besökt huvudkontoret för att tillhandahålla sitt pass och underteckna avtalet med rekryteringschefen Fatima. Fatima vill kopiera dokumenten till sina egna register och dela dem med HR-chefen som arbetar hemifrån. Det är lätt hänt att Fatima råkar ange fel mottagare eller spara dokumentet på en plats som är tillgänglig för alla. Om fel person fick det kan den öppna de inlästa dokumenten för att komma åt informationen.

Organisationer har ett ansvar att se till att alla scannade dokument endast ses av de som har behörighet att se dem. Ett enkelt fel kan leda till potentiell dataförlust eller överträdelse, vilket kan ha en allvarlig inverkan på efterlevnaden.

Om organisationen inte inser att den har begått en allvarligt överträdelse och inte rapporterar det kan dataskyddsregulatorn utfärda en böter på upp till 4 % av organisationens globala omsättning.

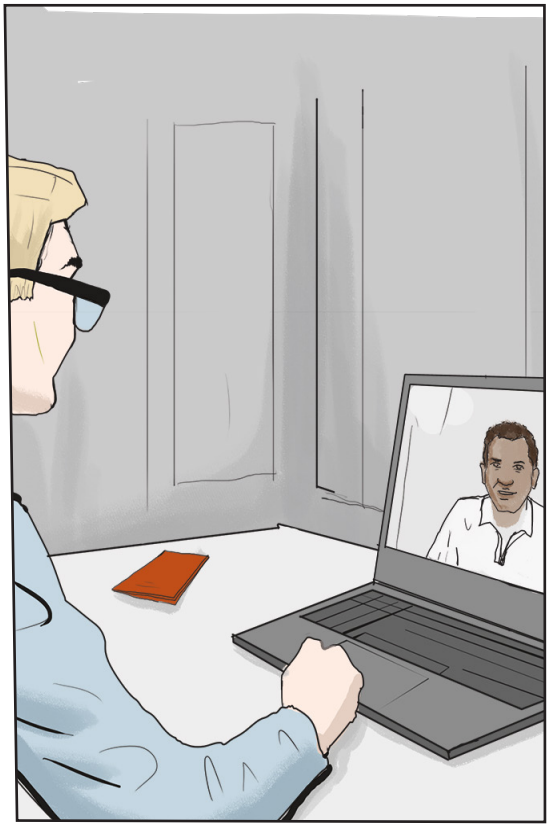
NYCKLAR TILL FRAMGÅNG

uniFLOW Online
uniFLOW Online erbjuder inbyggda arbetsflöden för säker scanning som gör det möjligt för organisation Y att förkonfigurera specifika scanningsarbetsflöden för varje användare. Dokumentarbetsflöden som HR-onboarding är redan fördefinierade, vilket förhindrar Fatima från att spara scanningen om en ny medarbetare på en felaktig destination.



imageFORMULA DR-S150
Fatima är redo att scanna dokumentet med imageFORMULA DR-S150. Den här scannern har säkra funktioner som hjälper till att skydda informationen: alla användare måste logga in med ett ID-kort, vilket säkerställer att endast Fatima kan komma åt dokumentet som har lästs in. Den tillämpar även automatiskt kryptering på den digitaliserade versionen, vilket innebär att endast en mottagare med ett lösenord kan läsa, redigera och skriva ut den. imageFORMULA DR-S150-enheter erbjuder även alternativ för att skicka dokument via säkra protokoll, till exempel scanning till FTPS, SFTP och SMTPS.

IRISPowerscan
Företaget har även IRISPowerscan, vilket innebär att när dokumenten har digitaliserats identifieras de automatiskt som pass och avtal. Programvaran korrigerar eventuella scanningsfel som skevheter och använder OCR (Optical Character Recognition) för att känna igen viktiga detaljer som medarbetarens namn och passnummer. Den här informationen läggs till i indexeringen, vilket gör det enklare för organisationen att hitta den i framtiden. Dessutom dirigerar IRISPowerscan automatiskt avtalet och passet till den rätta säkra lagringsplatsen i företagets system.



Under rekryteringsprocessen deltog flera medarbetare, bland annat Fatima och kollegan Nick, i intervjuer med kandidaterna och granskade CV:n. Båda medarbetarna är virtuellt baserade och arbetar på olika platser i Europa. Både Fatima och Nick har kopior av kandidaternas CV:n och anteckningar om intervjuerna på sina bärbara datorer och på delade Dropbox-platser. När den nya kandidaten har erbjudits jobbet är det lätt hänt att Fatima och Nick glömmer att ta bort något av dessa dokument.

Allt striktare lagar innebär att efterlevnaden aldrig har varit så viktig. Lagar som GDPR har infört specifika regler som styr hur information ska lagras – organisationer får till exempel inte behålla personligt identifierbar information längre än vad som är absolut obligatoriskt. Trots detta har många organisationer fortfarande problem med slumpmässiga lagringsstrategier, utan officiella platser för att lagra dokument eller möjlighet att hitta dokument som sparats på de egna servrarna.

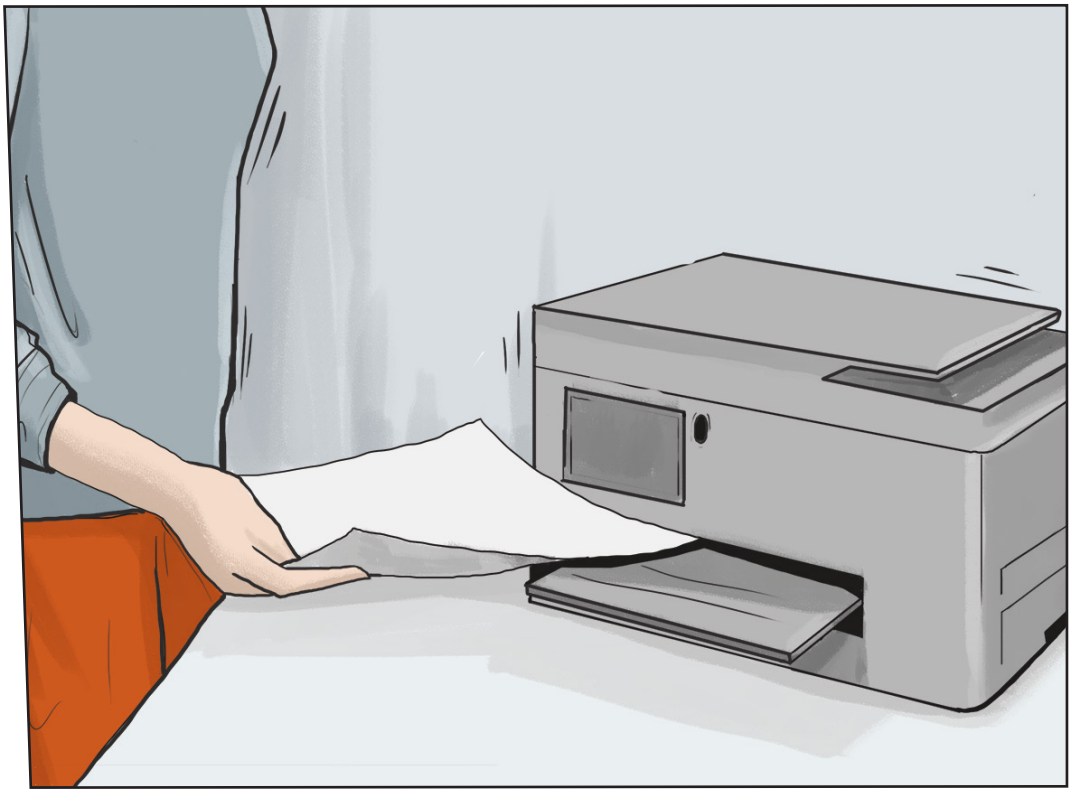
Om en före detta medarbetare eller en tidigare kandidat gör en åtkomstbegäran till organisationen, skulle det vara mycket svårt för företaget att förklara vilken information de har. Dessutom skulle organisationen ha svårt att i granskningssyfte visa att de har kontroll över var personligt identifierbar information lagras.

NYCKLAR TILL FRAMGÅNG

Therefore Online
Tack vare robust inbyggd säkerhet ger Therefore Online organisationer möjlighet att upprätta automatiska policyer avseende vem som har åtkomst till dokument, hur uppgifter lagras, delas eller redigeras. Den spårar all interaktion med ett dokument och hanterar informationen säkert och synligt från början till slut, vilket gör granskningsprocessen mycket enklare.

Organisation Y kan dessutom införa automatiska lagringspolicyer för att säkerställa att gamla dokument som innehåller känslig information tas bort efter en skälig lagringsperiod, vilket uppfyller regelefterlevnaden. Eftersom Therefore Online är molnbaserat kan team fortfarande ladda upp dokument och känna sig trygga med att de är säkra, även när teamen inte är på plats.

Medarbetarens nya linjechef Ingrid arbetar hemifrån och förbereder sig för att genomföra en introduktionsintervju på kontoret nästa dag. Hon vill skriva ut en kopia av brevet som bekräftar den nya medarbetarens lön, tillsammans med andra formulär, att dela med sig av den under processen. Ingrid har nyligen börjat arbeta hemifrån och har inte fått någon arbetsskrivare ännu, så hon använder sin privata enhet.

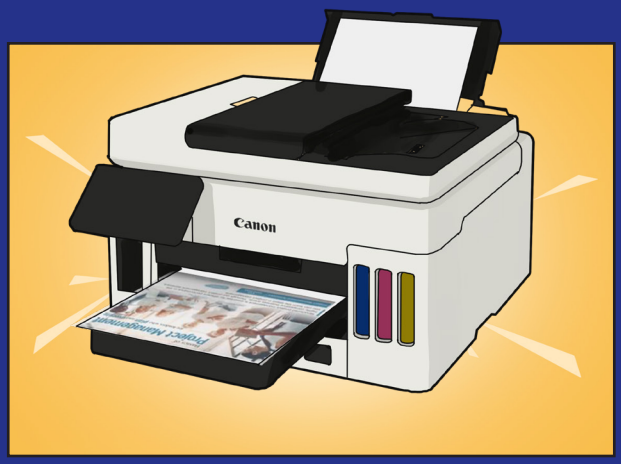


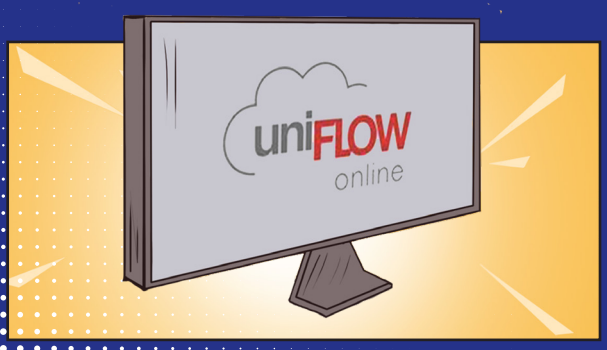
Det är enkelt för organisationer att glömma att skrivare spelar en stor roll i säkerheten och efterlevnaden av arbetsflöden då enheterna innehåller värdefulla data och dokument. Som en del av lagstadgade skyldigheter gällande efterlevnad förväntas organisationer tillhandahålla verifieringskedjor som rapporterar hur känslig information används.

Det innebär att de måste ha större insyn och spårning över hur dokument interagerar med enheter. Eftersom Ingrid använder sin privata skrivare är den dock inte ansluten till företagets nätverk – det finns alltså ingen spårbarhet, inga register över data som lagras i enheten och det finns ingen garanti för att de är säkra.

NYCKLAR TILL FRAMGÅNG

MAXIFY GX6050
Den här effektiva skrivbordsskrivaren producerar utskrifter av hög kvalitet för hemmakontor, men den hjälper även till att hålla dokument säkra och kompatibla tack vare den inbyggda integreringen med uniFLOW Online. Funktionen Scanna till mig själv förhindrar att Ingrid skickar dokument till någon annan än sin egen e-post eller personliga mapp, för att undvika att hon av misstag skickar affärsdokument till privata kontakter. Funktionen för säker frisläppning av utskriftsjobb innebär att Ingrid bara skriver ut dokument när hon är redo, vilket innebär att känsliga affärsdokument inte lämnas kvar på enheten.

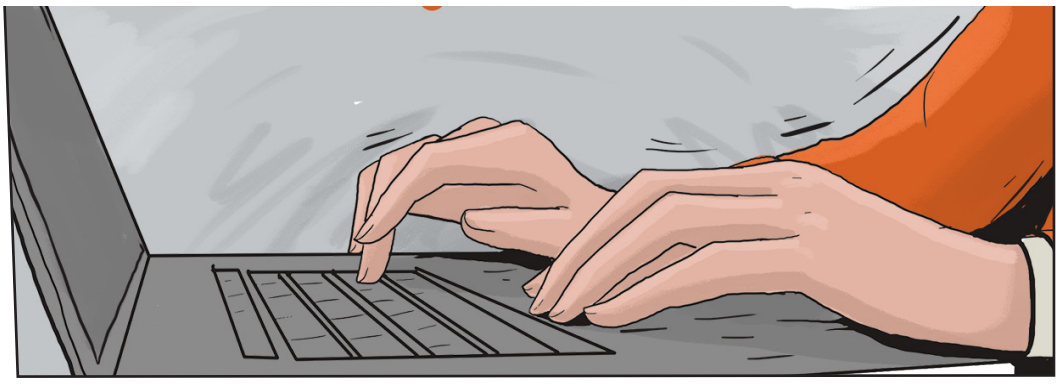




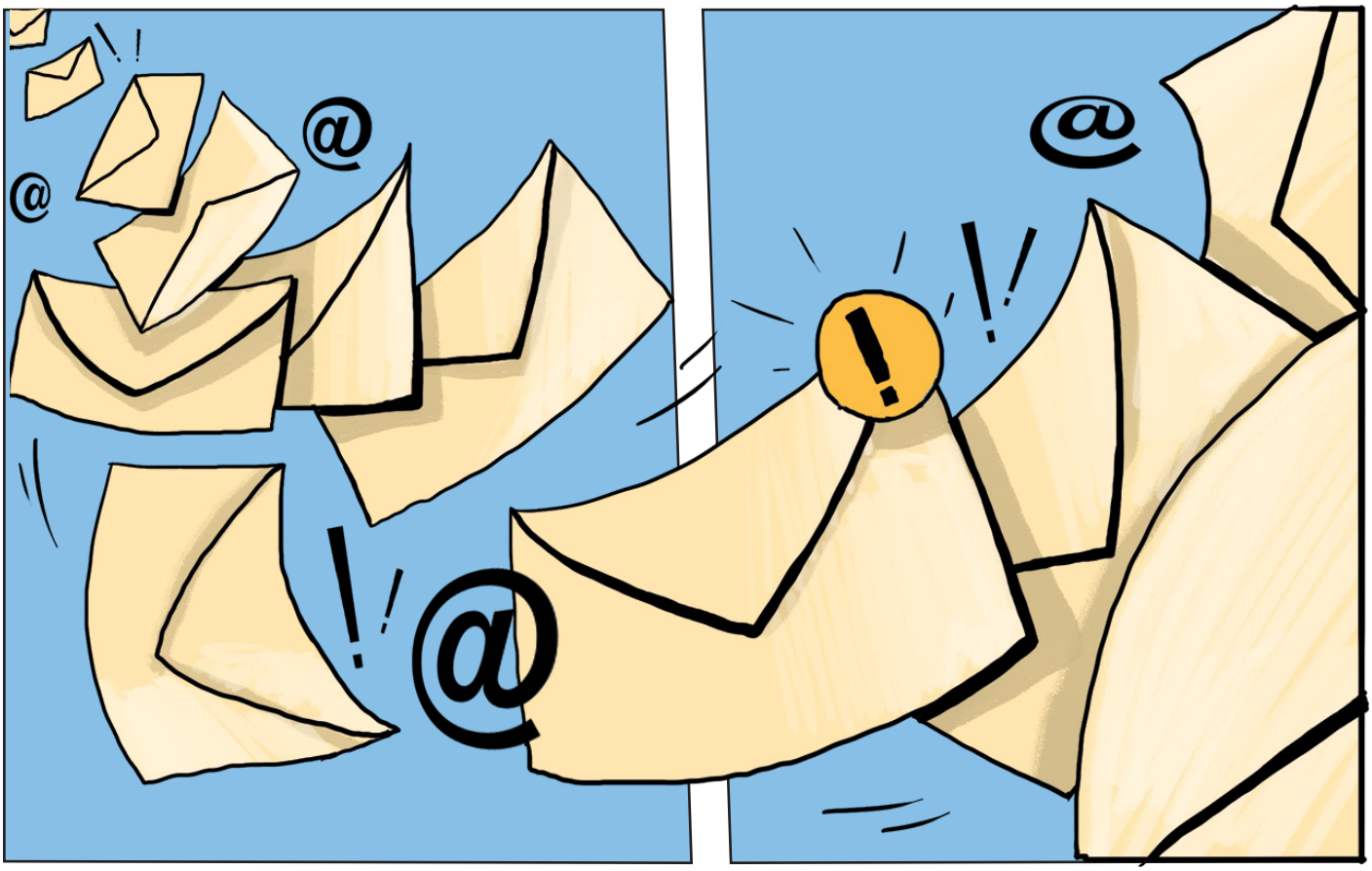
uniFLOW Online
Den här inbyggda programvaran integrerar MAXIFY GX6050 med organisationens miljö, vilket gör att IT-teamet på organisation Y kan spåra Ingrids utskriftsaktivitet och rapportera exakt hur känslig information används, även när hon arbetar hemifrån.

Det är slutet på den nya medarbetarens första månad och Fatima från HR förbereder sig för att skicka ut lönebesked. Tyvärr har den nya medarbetaren samma förnamn som en annan medarbetare. Fatima råkar skicka de två lönebeskeden till fel mottagare, vilket innebär att båda kan se hur mycket den andra tjänar.

Organisationen har brutit mot medarbetarnas sekretess, vilket innebär att det tekniskt sett finns skäl till att ställa företaget inför en arbetsdomstol. När den nya medarbetaren har sett sin kollegas lönebesked kanske medarbetaren dessutom ifrågasätter sin egen lön hos HR och inte längre känner sig bekväm med att stanna kvar i sin roll.



Kommunikation medför en stor risk i ett dokumentarbetsflöde eftersom det innebär att dela information, oavsett om det är internt med medarbetare eller externt med kunder, leverantörer och andra intressenter. Vid en standardgranskning förväntas organisationer visa hur känslig information delas med andra parter. Med tanke på den enorma mängd meddelanden som en organisation skickar under en vecka är det viktigt att det finns lösningar som gör det enkelt att spåra dessa processer.



NYCKLAR TILL FRAMGÅNG

uniFLOW sysHub
Med uniFLOW sysHUB får användare god kontroll och översikt över sin interna kommunikation, vilket gör det enklare för Fatima att hålla HR-kommunikation konfidentiell. Lösningen samlar processer för intern kommunikation och program i ett arbetsflöde som hanteras från en och samma plats. uniFLOW sysHUB automatiserar det här arbetsflödet för att göra det mer effektivt och minska risken för fel. I det här exemplet skulle Fatima inte kunna råka skicka konfidentiell information till en annan medarbetare.

Varje steg i arbetsflödet loggas och lagras i ett sysHUB-bibliotek för senare granskning och för att stödja verifieringskedjor, vilket innebär att Fatima kan kontrollera leveransbekräftelsen för att säkerställa att hennes meddelande har nått rätt person.

HUR KAN VI HJÄLPA TILL?

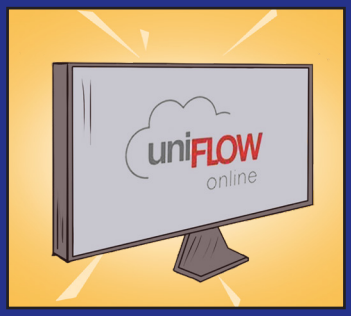
Alla företag vill skydda sin information och upprätthålla efterlevnaden. Men som organisation X och Y har visat är det ett fientligt landskap där ute. Organisationer kämpar inte bara mot fler skurkar än tidigare, utan tuffare lagstiftning innebär att mer står på spel när misstag begås. Det kan verka som ett förlorat slag, men det behöver det inte vara. Hemligheten är att ha rätt teknik och partner på din sida.

Canon är ledande inom IDC MarketScape för utskrifts- och dokumentsäkerhetslösningar och -tjänster, samt inom Quocirca Print Security Landscape. Våra maskinvaror, programvaror och tjänster är utformade för att hjälpa din organisation att arbeta så effektivt som möjligt i en komplicerad värld. Oavsett var dina medarbetare sitter, eller var du befinner dig på din resa mot digitala transformation, stöder vår teknik alla arbetsmiljöer.

Med vår säkra konstruktion gör vi det enkelt att skydda information. Våra lösningar är byggda för att förhindra attacker, skydda data och upprätthålla och skydda efterlevnaden, så att du kan dra nytta av nya funktioner utan att öka arbetsbördan för ditt team.

UTSKRIFTS- OCH SCANNINGSENHETER
Vårt utbud för utskrift och scanning innehåller de senaste säkerhetsfunktionerna för att skydda viktiga data i varje steg av dokumentarbetsflödet. Alla Canon-produkter säkerhetskontrolleras under design- och utvecklingsfaserna, samt före lanseringen.

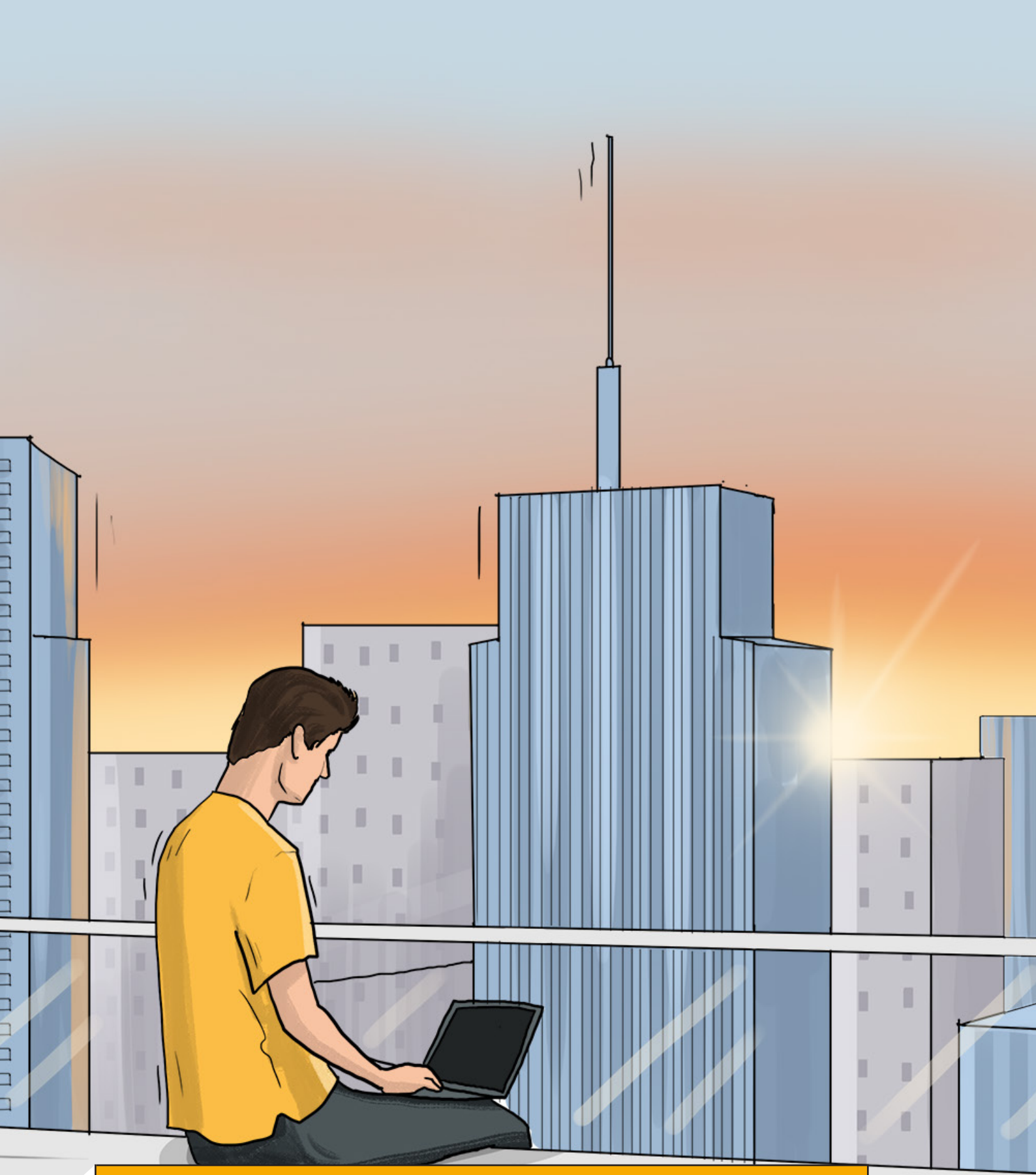
Vi fortsätter att bygga starka partnerskap med branschledare, som Trellix och Microsoft, för att säkerställa största möjliga täckning och kompatibilitet när vi säkrar enheter. Dessutom har vi ett särskilt produktteam som ansvarar för säkerhetsincidenter.



PROGRAMVARA
Vi förstår att information inte är bunden till en viss plats, vilket är anledningen till att vi erbjuder programvaror som skyddar data var de än finns. Vi arbetar även med externa organisationer som IOActive för att utföra intrångstester vid lanseringen och för större programvaruuppdateringar.

TJÄNSTER
Vi erbjuder säkerhetstjänster som är utformade för att hjälpa dig att upprätthålla dataskyddsefterlevnad och skydda dina känsliga data under hela livscykeln för din utskrifts- och scanningsinfrastruktur.


PASSPORT



Är du redo att besegra fienderna som äventyrar säkerheten och efterlevnaden? Se vår teknik i praktiken i vårt showroom eller boka en demonstration hos vårt expertteam för att se vad våra lösningar kan göra för din verksamhet.

Vill du veta mer om våra hemligheter? Besök vår webbplats för tjänster för digital transformation för att ta reda på mer.

OM CANON

Vi på Canon står för bild. Vi använder bild för att göra skillnad och skapa förändring. För våra kunder när de tar steget mot digital transformation och att arbeta på nya sätt. För en bredare samhällsförändring med vårt pågående hållbarhetsfokus som en del av vårt företags arv och kultur.

Slutligen undergår vi en förändring när vi investerar i nya marknader, produkter och teknik. Vi är här med våra långsiktiga mål, vilka är till allas fördel: våra kunder, medarbetare och samhället i stort.

CANON VILAR PÅ FYRA HUVUDPELARE:

Innovation

En lång historia av bildstyrd innovation där vi levererat den senaste tekniken i över 80 år. Pionjärer inom branschen med ett starkt engagemang för den framtida tekniska utvecklingen.

Support

En mångsidig tjänsteportfölj för att säkerställa högsta kvalitet och nöjda kunder. Intern expertis som arbetar mot ökad effektivitet och strävar efter att frigöra potential för våra kunder.

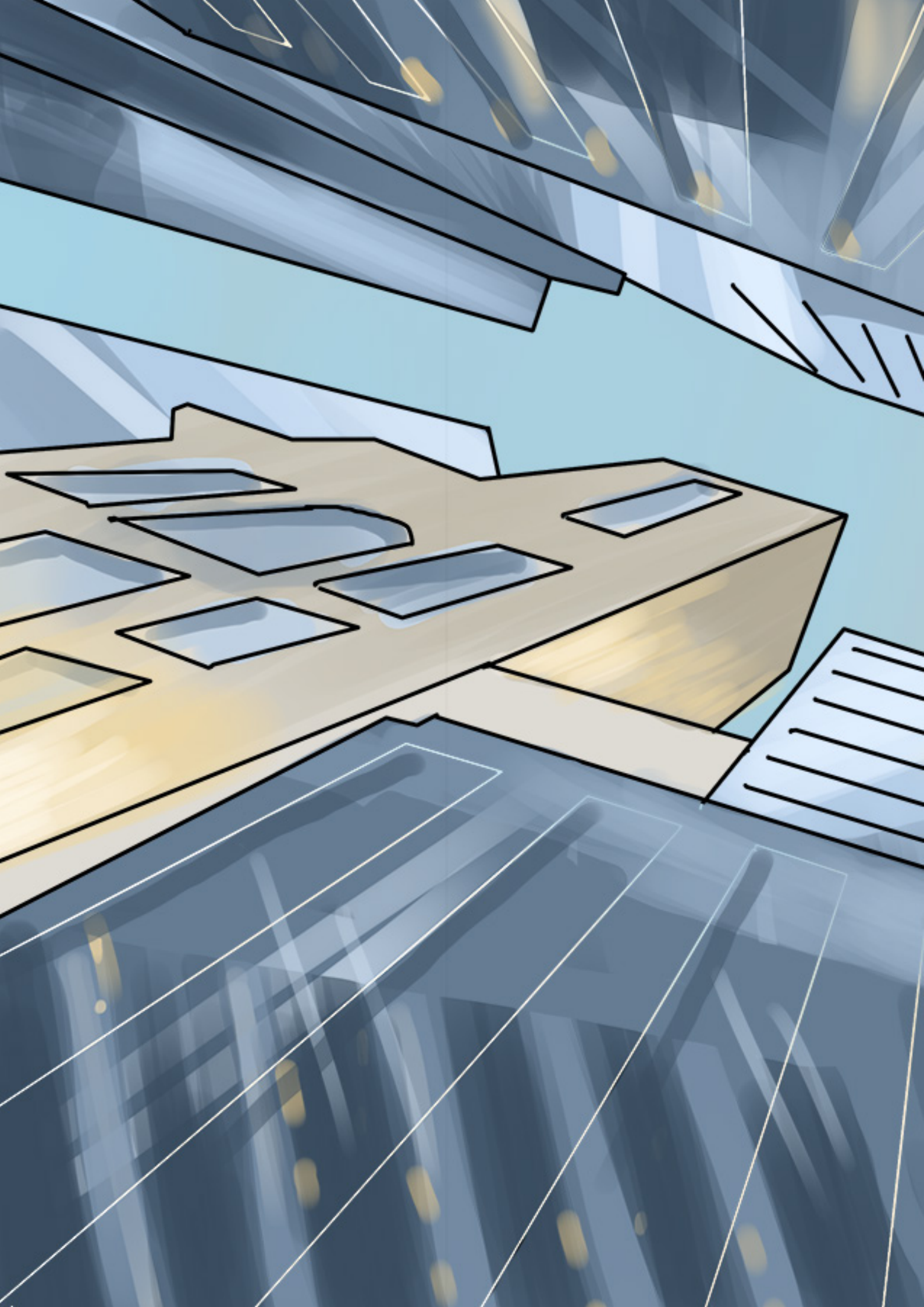
Säkerhet

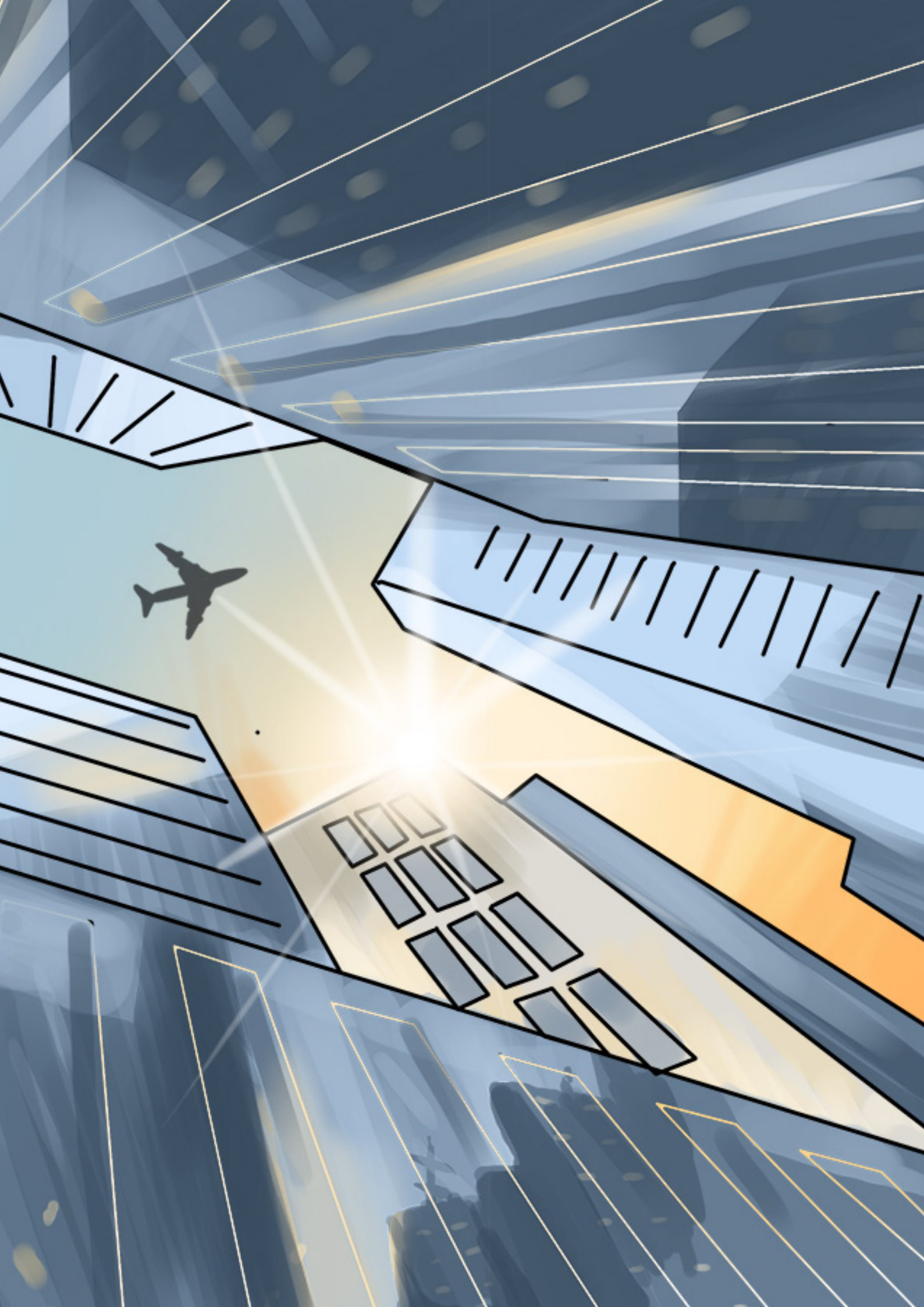
Canons lösningar och tjänster bidrar till att säkra alla dokument och känslig data – oavsett om det är i digitalt eller pappersformat – under hela dokumentets livscykel. Säker konstruktion – enheterna, lösningarna och tjänsterna är byggda med fokus på säkerheten.

Hållbarhet

Canon har anpassat sitt hållbarhetsarbete efter FN:s mål för hållbar utveckling, t.ex. åtagande om att minska koldioxidutsläpp över hela produktens livscykel genom att skära ned på förpackningar och konsolidera distributionsanläggningar.

TILLSAMMANS GÖR DESSA FAKTORER CANON TILL DEN RÄTTA PARTNERN FÖR DIG.





Canon Inc.
Canon.com

Canon Europe
canon-europe.com
Swedish edition

Canon Svenska AB
Björnstigen 85
170 73 Solna
Tel. +46 8 744 85 00
canon.se