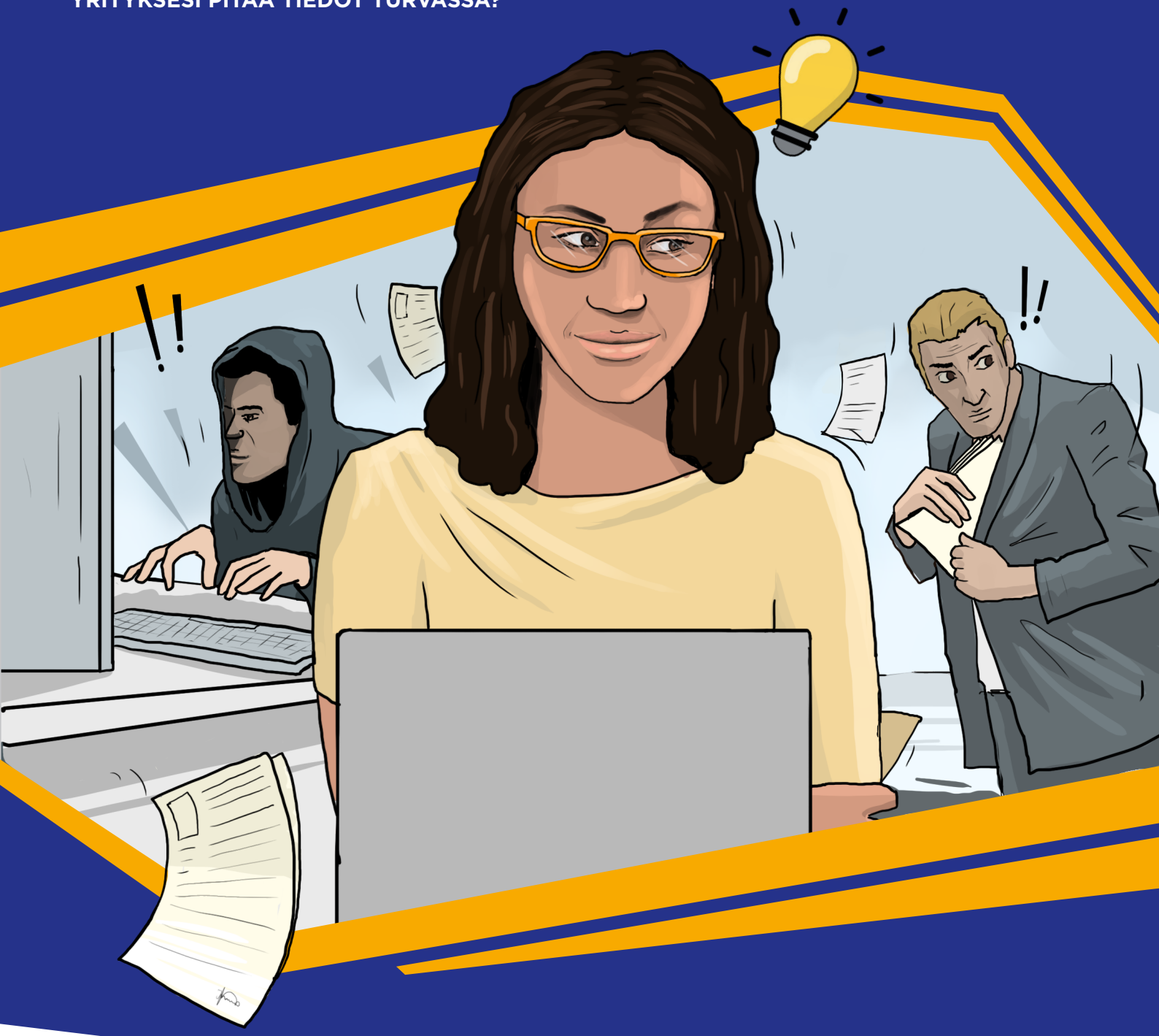
TIETOTURVA KÄYTÄNNÖSSÄ!

MAAILMASSA, JOSSA KYBERUHAT OVAT YHÄ ÄLYKKÄÄMPIÄ JA VAATIMUSTEN NOUDATTAMINEN ENTISTÄ VAIKEAMPAA, MITEN YRITYKSESI PITÄÄ TIEDOT TURVASSA?



Canon

SISÄLTÖ

Tieto on jokaisen nykypäivän organisaation aarre. Se tehostaa talousosastoa, antaa johtoryhmälle ennakointikykyjä ja tarjoaa työntekijöille paremman käsityksen liiketoiminnasta.

Arvokas materiaali on pidettävä turvassa hinnalla millä hyvänsä.

Kun aarteen arvo kasvaa, samalla kasvaa sitä tavoittelevien vihollisten määrä: he vaanivat ulkopuolella päästäkseen varastamaan tietoja silloin, kun sitä vähiten odotat. Samaan aikaan kaksoisagentit voivat yrittää ottaa aarteen haltuunsa.

Organisaatiota vavisuttava taho ei välttämättä ole vihollinen.

Suuri mahti valvoo kaikkea ja varmistaa, että jokainen noudattaa tietojen vaatimustenmukaisuutta. Vaikka lait ovat tiukkoja ja rangaistukset ankaria, myös virheiden tekeminen on helpompaa kuin koskaan.

Nykypäivän yritykset eivät ole muurien ympäröimiä, eivätkä välttämättä edes yhdessä paikassa. Hybridityöskentelyn myötä työntekijät säilyttävät, jakavat ja yhteiskäyttävät tietoja useammissa paikoissa kuin koskaan aiemmin.

Näin monimutkaisessa työympäristössä tietojen suojaaminen ja prosessien pitäminen vaatimustenmukaisina voi vaikuttaa mahdottomalta haasteelta.

Tarvitset luotettavan kumppanin, joka voi turvata aarteesi, suojata yritystäsi roistoilta ja auttaa työntekijöitä noudattamaan vaatimuksia kaikissa tilanteissa.

Katsotaanpa, miten Canon ja sen salaiset aseet voivat auttaa yritystäsi vastaamaan haasteeseen.

HAASTEENA DOKUMENTIN ELINKAARI

Dokumentteja luodaan, kopioidaan, säilytetään ja jaetaan organisaatiossa koko niiden elinkaaren ajan, ja kaikissa vaiheissa on omat haasteensa. Dokumenttien sisältämät tiedot on suojattava ja pidettävä vaatimustenmukaisina.

Tulosteet ovat haastavia tietoturvan ja vaatimustenmukaisuuden kannalta, koska kaikkea käyttäjään tai asiakirjaan liittyvää toimintaa ei nähdä, ja tästä voi aiheutua tietoturvarikkomuksia.

Skannattujen asiakirjojen, jotka sisältävät arkaluonteisia tietoja, on päästävä kohteeseensa turvallisesti. Käyttäjän virheet tietojen manuaalisen skannauksen aikana.

Henkilötiedot ja arkaluonteiset tiedot, jotka koskevat asiakkaita ja työntekijöitä, on säilytettävä, käsiteltävä ja hävitettävä tietosuojasäännösten mukaisesti

Lähteviä viestejä, dokumentteja ja tietoja on suojattava, jotta vältetään tietojen vaatimustenmukaisuuteen liittyvät ongelmat

HAASTE 1

SALAINEN STRATEGIA

Organisaatiolla X on suuri salaisuus: se on valmiina uuteen seikkailuun. Johtoryhmä on päättänyt investoida uuteen liiketoiminta-alueeseen saadakseen lisää valtaa ja ennennäkemättömiä liikevoittoja markkinoilla.

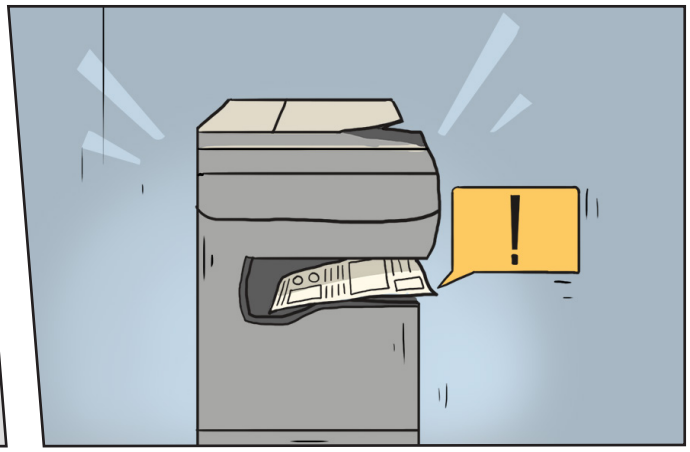
On erittäin tärkeää, että nämä suunnitelmat pysyvät salassa julkaisuun saakka. Uutinen paljastaisi Organisaatio X:n aikeet sen kilpailijoille ja varoittaisi niitä uudesta haastajasta. Samaan aikaan Organisaatio X:n työntekijöillä on paljon pelissä – voisiko heidän osastollaan olla uusia mahdollisuuksia? Entä uusia liiketoiminta-alueita? Vai uhkaako tämä heidän työpaikkojaan?

Johdon on edettävä varoen, jos halutaan varmistaa, että suunnitelmat eivät päädy juonittelevien työntekijöiden ja ulkoisten vihollisten käsiin. Budjetointi- ja tiedottamisvaiheissa johdon on vältettävä sisäisten uhkien, haittaohjelmien ja verkkohyökkäysten ansat. Pystyykö johto säilyttämään salaisuuden?

Viestintätiimi on laatinut lehdistötiedotteen, jossa kuvataan organisaation uusi strateginen suunta. Tiedot ovat edelleen erittäin salaisia, ja tiedotteen kirjoittaa ja hyväksyy pieni ryhmä ylimmän johdon jäseniä. Talousjohtaja Selmaa on pyydetty tarkistamaan paperikopio asiakirjasta. Hän assistenttinsa Polina on valmiina tulostamaan sen hänelle.

Tulostus on suurempi tietoturvauhka kuin mitä organisaatioissa uskotaan. Tietoturva- ja vaatimustenmukaisuusriskejä ilmenee, kun asiakirjat viedään tulostimesta ennen kuin käyttäjä ehtii hakea ne, tai kun unohdetuista asiakirjoista paljastuu luottamuksellisia tietoja valtuuttamattomille henkilölle.

Innovaatiot ovat myös avanneet ovia uusille tietoturvauhille. Modernit monitoimilaitteet ovat yhtä tehokkaita kuin tietokone ja niissä on kiintolevy, muistia ja suoritin sekä usein internetyhteys. Siksi hakkerit, jotka haluavat päästä sisälle verkkoon ja käsiksi yrityksen tietoihin, voivat kohdistaa hyökkäyksen tulostimen laiteohjelmistoon.



SALAISET ASEET

imageRUNNER ADVANCE DX C5800

imageRUNNER ADVANCE DX C5800 sisältää vakiona tietoturvaominaisuudet. Polina voi tulostaa asiakirjan vain kirjautumalla laitteeseen henkilökortilla, joten kukaan muu ei pääse käsiksi tulostusjonossa olevaan asiakirjaan, eikä se jää odottamaan laitteen lokeroon.

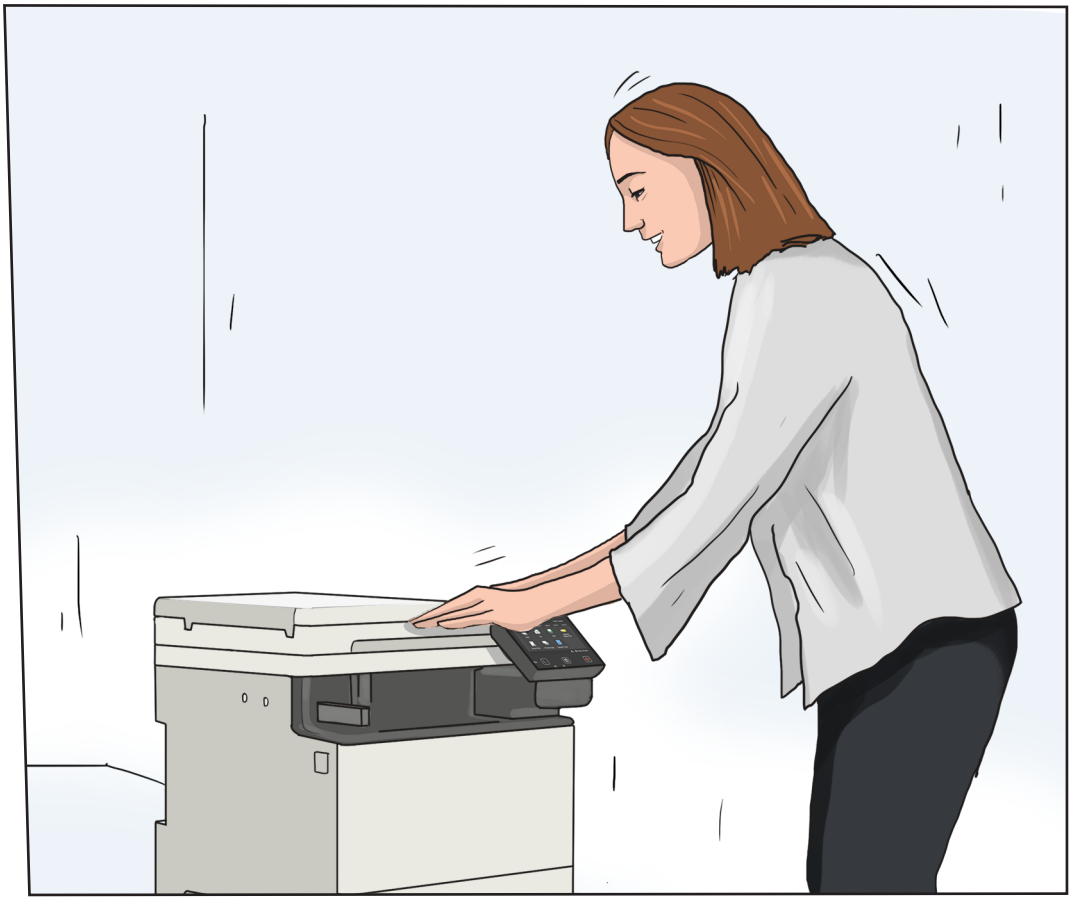
Laitteessa on myös Trellix McAfee Embedded Control, joka suojaa nollapäivä- ja APT-hyökkäyksiltä estämällä luvattomien sovellusten suorittamisen älykkään sallittujen sovellusten luettelon avulla. Hyökkääjä ei saa lehdistötiedotetta verkkohyökkäyksen avulla, sillä McAfee Embedded Control suojaa ohjelmaa peukaloinnilta.

Lisäksi imageRUNNER ADVANCE DX C5800 tukee Security Information Event Management (SIEM) -integrointia, jonka ansiosta organisaatiot voivat lisätä helposti tulostinlaitteita nykyisiin valvontajärjestelmiinsä (esim. Syslog). Nämä järjestelmät voivat tunnistaa ja ilmoittaa suojaustapahtumat reaaliaikaisesti koko laitteistossa ja varoittaa näin yritystä ongelmista tai uhista.

Laitteiden suojauspalvelu
Canonilla tietoturva on huomioitu jo ennen laitteen ostamista. Määritämme imageRUNNER ADVANCE -monitoimilaitteet tietoturvallisemmiksi vahvistamalla niiden sisäisiä suojaustoimintoja ja estämällä vähemmän tärkeät toiminnot ja suojaamattomat portit. Konfiguroitu laite tarkistetaan ennen toimitusta.

imageWARE Secure Audit Manager Express
Tämä verkkolaitteiden suojausratkaisu antaa Organisaatiolle X mahdollisuuden valvoa asiakirjoihin liittyviä toimiaan. Se voi tallentaa, arkistoida ja auditoida Canon-laitteilla suoritetut toimet. Kun Polina tulostaa lehdistötiedotteen, imageWARE Secure Audit Manager Express lähettää IT-osastolle sähköposti-ilmoituksen riskialttiin asiakirjan tulostamisesta. Näin Organisaatio X tietää, ovatko valtuuttamattomat työntekijät tai muut tahot yrittäneet tulostaa arkaluonteisia tietoja.

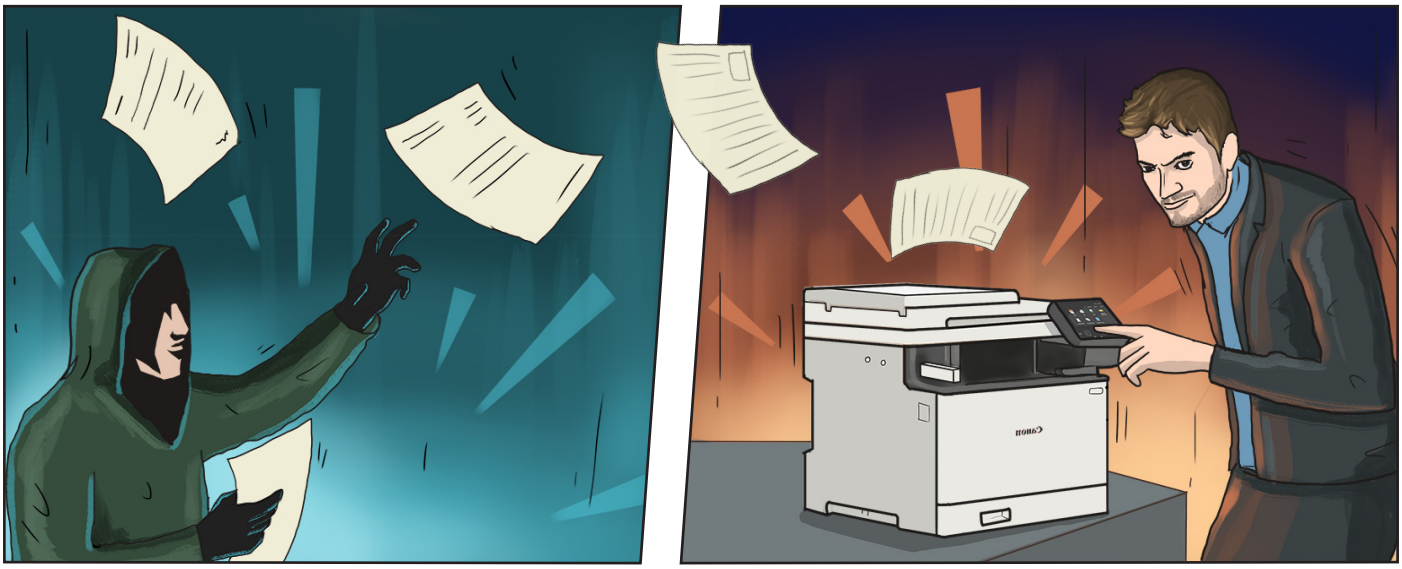
Selma on tarkistanut lehdistötiedotteen ja kirjoittanut siihen kommentteja. Polinan on toimitettava palaute vastaavalle PR-johtaja Pierrelle. Koska Pierre työskentelee kotona, Polinan on luotava lähettämistä varten digitaalinen kopio. Jos asiakirja skannataan ja lähetetään sähköpostitse suoraan laitteesta, hyökkääjä saa mahdollisuuden siepata asiakirjan.



Nykyaikaiset skannerit on usein yhdistetty internetiin, jotta käyttäjät voivat lähettää asiakirjat sähköpostitse suoraan vastaanottajalle tai tallentaa ne pilveen. Digitaalisiin tietoihin kohdistuu siis useampia riskejä, joten on erittäin tärkeää, että skannereissa on tehokkaat tietoturvaominaisuudet. Ilman suojausta skanneri on altis väärinkäytölle: sisäinen käyttäjä voi muuttaa sähköpostin reititysjonoja ja ohjata sähköpostiin lähetettävän työn valtuuttamattomalle käyttäjälle.

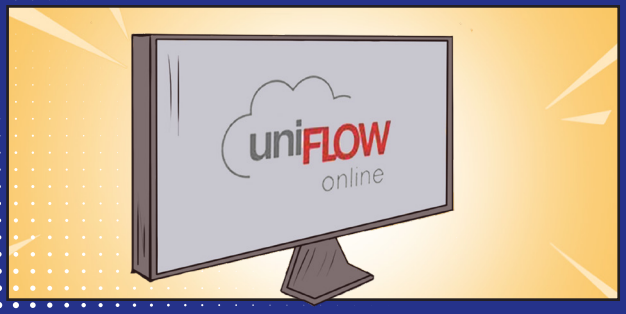
Salaamattoman asiakirjan voi avata tai tulostaa tai sitä voi muokata.

Ulkopuolelta katsottuna hyökkääjä voisi myös päästä sisään verkon kautta ja tehdä muutoksia sähköpostihakemistoihin, jotta asiakirjan voi lähettää organisaation ulkopuolisille vastaanottajille. Hän voi myös siepata HTTPS:n kautta lähetetyn asiakirjan, jos sitä ja sen sisältöä ei ole salattu.



SALAISET ASEET

i-SENSYS X C1333iF
Selma on valmis skannaamaan asiakirjan i-SENSYS X C1333iF -laitteella. Tämä monitoimilaite (jossa on tulostus- ja skannaustoiminnot) tarjoaa turvalliset skannausominaisuudet, joiden avulla tiedot pysyvät turvassa. Kun laite käynnistetään, sen suojattu käynnistys tarkistaa, onko laitetta yritetty peukaloida, ja laite voi ilmoittaa Selmalle, jos näin on tapahtunut. Tämän jälkeen Selman on kirjauduttava henkilökortilla, jotta järjestelmään tallentuu tieto siitä, kuka kopioi tai jakaa tietoja. i-SENSYS X C1333iF -laitteen IEEE802.1X-tuki tarjoaa tunnistusmekanismin, ja kun laite muodostaa yhteyden yrityksen LAN- tai WLAN-verkkoon, tämä vahvistaa sen aitouden.



uniFLOW Online
Kun Selma skannaa asiakirjan, uniFLOW Online luo salatun PDF-tiedoston ja mahdollisuuden salasanasuojaukseen. Nämä ominaisuudet estävät valtuuttamattomia käyttäjiä tarkastelemasta, muokkaamasta tai tulostamasta asiakirjaa ja suojaavat tietoja sieppaajilta.

Tobias on kuullut, että yritys saattaa muuttaa strategian suuntaa. Koska hänen johtamallaan tiimillä on vaikeuksia nykyisen strategian kanssa, hän tietää, että tämä voi tarkoittaa leikkauksia tämän vuoden budjettiin tai jopa työpaikkoihin.

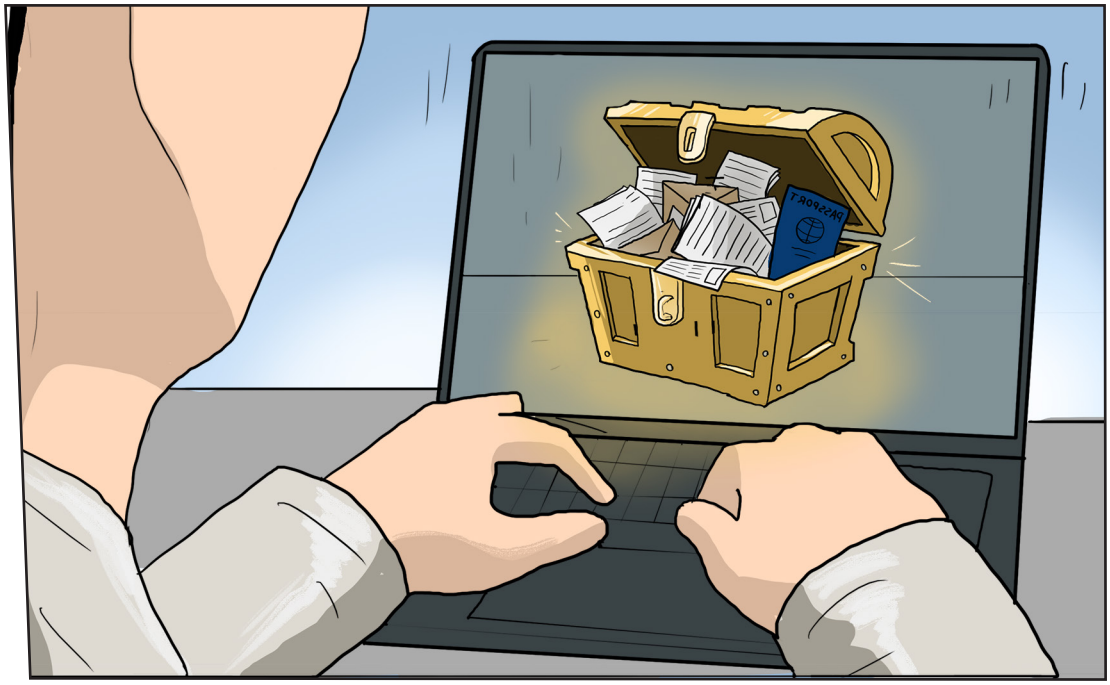
Tobias turhautuu uutisesta, joten hän haluaa selvittää huhujen todenperäisyyden ja ehkä varoittaa kollegoitaan. Hän luulee tietävänsä, missä ylin johto säilyttää talousdokumentteja ja alkaa etsiä salaa tietoja, jotka saattaisivat liittyä uusiin suunnitelmiin.

Organisaatiot luovat ja säilyttävät vuosi vuodelta enemmän tietoja. Monilla on nyt myös käytössä hybridimalli, joten tiedot ovat pirstaloituneet yhä useampaan paikkaan sekä fyysisesti että virtuaalisesti. Jos organisaatioiden arkistointistrategia on sattumanvaraista, työntekijät saattavat käyttää yritystietojen säilyttämiseen mm. arkistokaappeja tai Dropboxin kaltaisia henkilökohtaisia pilvipalveluja.
Lisäksi työntekijät käsittelevät usein arkaluonteisia tietoja, kuten sopimuksia, henkilöstön pankkitietoja ja yrityksen tulostietoja. Vaikka kyseessä ovat näinkin tärkeät tiedot, IT-tiimien on lähes mahdotonta varmistaa tiedonhallinnan parhaat käytännöt, kun asiakirjoja säilytetään tällä tavoin.

SALAISET ASEET

Therefore Online
Therefore Onlinen vahvan suojauksen ansiosta organisaatiot voivat määrittää automaattiset asetukset dokumentteihin pääsylle sekä tietojen säilytykselle, jaolle ja muokkaukselle. Käyttäjävalvonta estää luvattomia työntekijöitä, kuten Tobiasta, avaamasta arkaluonteisia asiakirjoja, kuten lehdistötiedotetta.

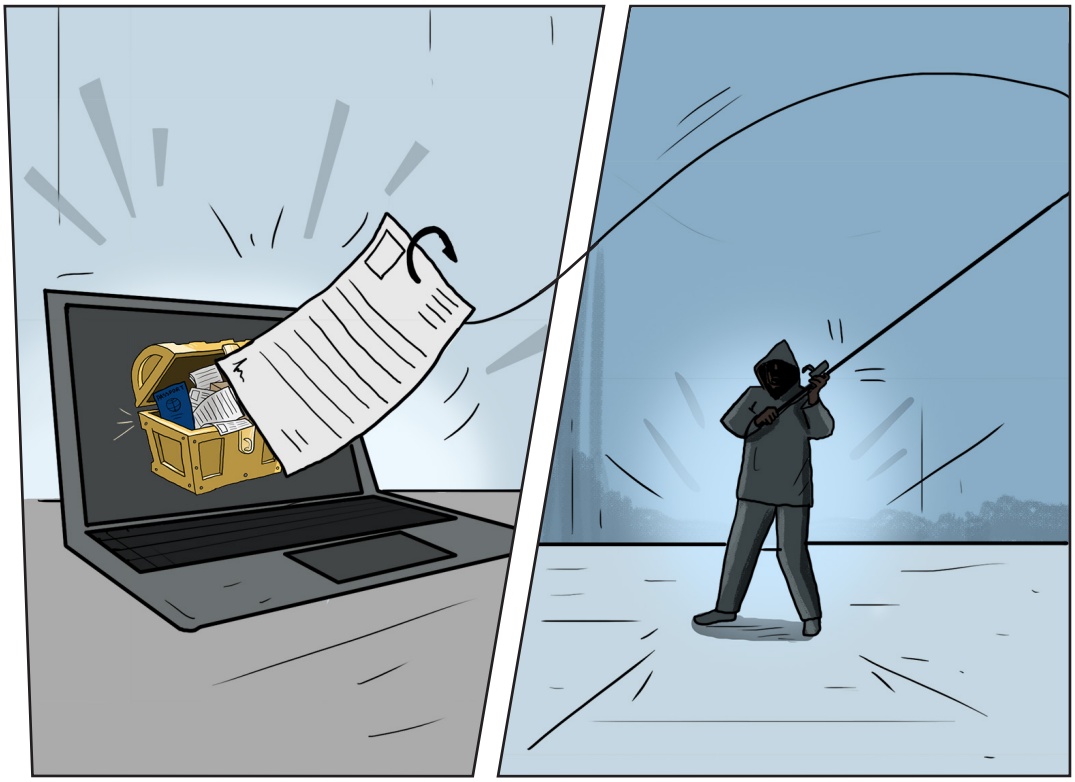
Therefore Online on pilviratkaisu, joten käyttäjän sijainti ei vaikuta tiedon saatavuuteen: valtuutetut käyttäjät, jotka työskentelevät etänä tai tien päällä, voivat silti käyttää tärkeitä dokumentteja. Asiakirjoihin liittyvää toimintaa seurataan, jotta tietoja voidaan hallita, ne nähdään kaikissa vaiheissa ja niistä saadaan digitaalinen kirjausketju.



Pierre valmistautuu lähettämään tiedotteen, jota ei vielä saa julkaista, tärkeimmille osakkaille ja valituille toimittajille. On erittäin tärkeää, että dokumentti lähetetään vain näille yhteyshenkilöille. Se ei saa joutua vääriin käsiin.

Samalla hänen on muistettava muut lisätiedot, jotka Organisaatio X haluaa pitää salassa. Yrityksen tietokannassa on lukemattomia aarteita: arkaluonteisia tietoja vastaanottajista, kuten sähköpostiosoitteet ja puhelinnumerot, ja toimittajien passitiedot aiemmilta lehdistömatkoilta.

Nämä tiedot houkuttavat varkaita, jotka voivat käyttää näitä tunnistetietoja ilmoituksen vuotamiseen etuajassa, tai käyttää tietotietokannassa olevia henkilötietoja identiteettivarkauksiin tai tiedonkalasteluhyökkäyksiin.

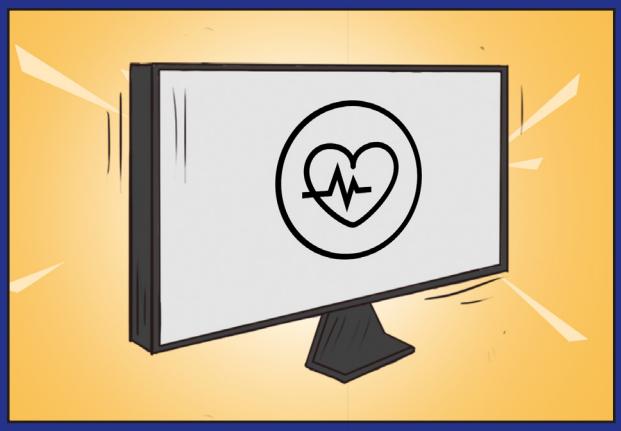


Yrityksillä on usein erittäin henkilökohtaisia ja luottamuksellisia tietoja asiakkaista, kumppaneista ja muista yhteistyötahoista. Sen lisäksi, että tiedot ovat yrityksen palvelimissa, niitä myös käytetään lähtevissä viesteissä, kuten tiliotteisissa, laskuissa ja viestinnässä eri osapuolten kanssa.

Näiden tietojen säilyttäminen on riski yritykselle, sillä jos ne katoavat tai hyökkääjät vievät ne, yritys voi saada suuret sakot tai menettää maineensa. Jos organisaatio viestii näiden yhteyshenkilöiden kanssa, on erittäin tärkeää, että kyseisten viestien sisältämät henkilötiedot päätyvät vain vastaanottajalle.

SALAISET ASEET

Kuntotarkastus
Tietoturvatarkastuksen avulla organisaatiot voivat tarkistaa IT-ympäristönsä ja varmistaa, että se on kaikilta osin turvallinen. Kyberturvallisuuden asiantuntija NCC Group analysoi etänä organisaation sisäisen ja ulkoisen IT-infrastruktuurin, kuten viestintäkanavat ja portit, ja paljastaa mahdolliset haavoittuvuudet. Etsimällä mahdolliset ongelmat organisaatio voi välttää sen, että mahdollinen hyökkääjä käyttää niitä, Pierren viestit siepataan tai toimittajien tai sidosryhmien tiedot varastetaan Organisaatio X:n tietokannoista.



uniFLOW sysHub
uniFLOW sysHUB -ohjelmiston avulla käyttäjät voivat valvoa tarkasti asiakasviestintää, joten Pierre voi varmistaa, että viestit menevät oikeaan kohteeseen. Tämä ratkaisu yhdistää sisäiset viestintäprosessit ja -sovellukset yhdeksi työnkuluksi, jota hallitaan samasta paikasta. uniFLOW sysHUB automatisoi työnkulun, jotta se toimii tehokkaammin ja pienentää virheiden riskiä. Jokainen työnkulun vaihe kirjataan lokiin ja tallennetaan sysHUB-kirjastoon tarkastelua ja kirjausketjuja varten, joten työntekijät eivät voi vuotaa asiakirjoja ilman, että tieto siitä tallentuu. Sillä aikaa Pierre voi tarkistaa toimitusvahvistuksesta, että viesti on tavoittanut oikean henkilön.

HAASTE 2

LUOTTAMUKSELLINEN REKRYTOINTI

Organisaatio Y:n on houkuteltava uusia työntekijöitä kasvavaan valtakuntaansa. Koko henkilöstö oli aiemmin samassa toimipaikassa, mutta hybridityön myötä yrityksen työntekijöitä on nyt eri puolilla maata. Kiireisen HR-tiimin on pitänyt mukautua nopeasti. Uudet työntekijät hankitaan nyt virtuaalisten rekrytointi- ja perehdytysprosessien avulla. HR-tiimin on valvottava kaikkea ja lähetettävä uusien työntekijöiden luottamuksellisia asiakirjoja pitkienkin matkojen päähän.

HR-tiimillä on paljon valtaa ja suuri vastuu: sillä on käytössään valtava määrä arvokkaita ja arkaluonteisia tietoja työntekijöiden palkkatiedoista terveyttä ja osaamista koskeviin tietoihin. Tiimi tietää, että sen on pidettävä tiedot turvassa ja noudatettava lainsäädännön vaatimuksia. Auditointeja on usein, ja HR-tiimi tietää, että sen on osoitettava miten tietoja säilytetään ja jaetaan. Se ei ole helppoa. Vaikka HR-tiimi tekee kovasti töitä, sillä ei ole supervoimia. Tiimi voi joutua vaikeuksiin vahinkojen ja virheiden takia.

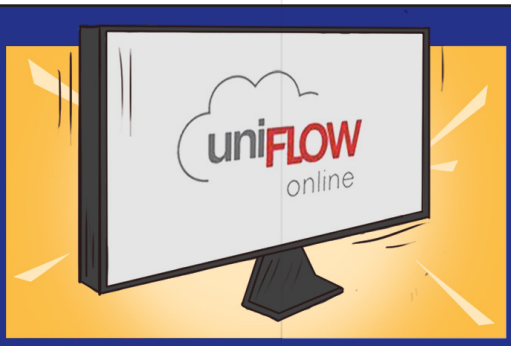
Jos tilanteeseen ei ole oikeanlaisia teknisiä ratkaisuja, tästä voi aiheutua Organisaatio Y:lle ongelmia.

Onnistuneen haastatteluprosessin jälkeen Organisaatio Y on päättänyt palkata uuden työntekijän. Hakija on vienyt passinsa pääkonttorille ja allekirjoittanut sopimuksen palkkaavan päällikön Fatiman kanssa. Fatima haluaa ottaa asiakirjoista kopiot itselleen ja HR-osaston päällikölle, joka työskentelee kotona. Fatima voi syöttää vahingossa väärän vastaanottajan tai tallentaa asiakirjan paikkaan, joka on kaikkien saatavilla. Jos väärä henkilö saa asiakirjat, hänen tarvitsee vain avata ne, jotta hän näkee tallennetut tiedot.

On organisaatioiden vastuulla varmistaa, että vain valtuutetut henkilöt voivat nähdä skannatut asiakirjat. Pienikin virhe voi johtaa tietojen menettämiseen tai tietovuotoon, josta voi seurata vaatimustenmukaisuuden laiminlyöminen. Jos organisaatio ei huomaa vakavaa tietovuotoa eikä ilmoita siitä, tietosuojaviranomainen voi antaa sakon, joka voi olla jopa 4 % organisaation maailmanlaajuisesta liikevaihdosta.

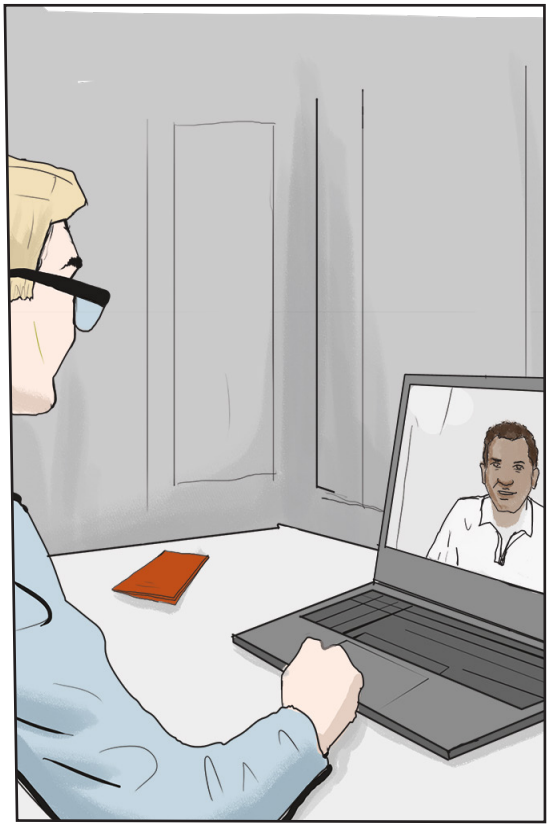
SALAISET ASEET

uniFLOW Online
uniFLOW Online tarjoaa suojatut skannaustyönkulut, joiden avulla Organisaatio Y voi määrittää ennalta kullekin käyttäjälle omat työnkulut. Asiakirjatyönkulut, kuten HR-osaston perehdytys, on esimääritetty, mikä estää Fatimaa tallentamasta uuden työntekijän skannattua asiakirjaa väärään paikkaan.



imageFORMULA DR-S150
Fatima on valmis skannaamaan dokumentin imageFORMULA DR-S150 -laitteella. Skannerissa on suojausominaisuudet, jotka auttavat pitämään tiedot turvassa: käyttäjien on kirjauduttava sisään henkilökortilla, joten vain Fatima voi käyttää skannattua dokumenttia. Skanneri myös lisää digitaaliseen versioon automaattisesti salauksen, joten vain salasanan tietävä vastaanottaja voi lukea, tulostaa ja muokata sitä. imageFORMULA DR-S150 -laitteilla voi myös lähettää dokumentteja käyttämällä skannausta ja suojattuja FTPS-, SFTP- ja SMTPS-protokollia.

IRISPowerscan
Yrityksellä on myös IRISPowerscan. Tämä tarkoittaa, että dokumentteja digitoitaessa ne tunnistetaan automaattisesti passiksi ja sopimukseksi. Ohjelmisto korjaa skannausvirheet, kuten vääristymät, ja tunnistaa optisen merkintunnistuksen (OCR) avulla tärkeät tiedot, kuten työntekijän nimen ja passin numeron. Nämä tiedot indeksoidaan, jotta ne on helpompi löytää jatkossa. Lisäksi IRISPowerscan reitittää sopimuksen ja passin skannatut versiot automaattisesti yrityksen suojattuun arkistointipaikkaan.



Rekrytointiprosessin aikana useat työntekijät, myös Fatima ja hänen kollegansa Nick, haastattelivat hakijoita ja tarkistivat ansioluetteloita. Kumpikin heistä työskentelee virtuaalisesti Euroopan alueella. Sekä Fatimalla että Nickillä on kopiot hakijoiden ansioluetteloista ja haastattelumuistiinpanoista omilla kannettavilla tietokoneillaan ja jaetuissa Dropbox-kansioissa. Kun hakijalle on tarjottu töitä, Fatima ja Nick saattavat unohtaa poistaa nämä asiakirjat.

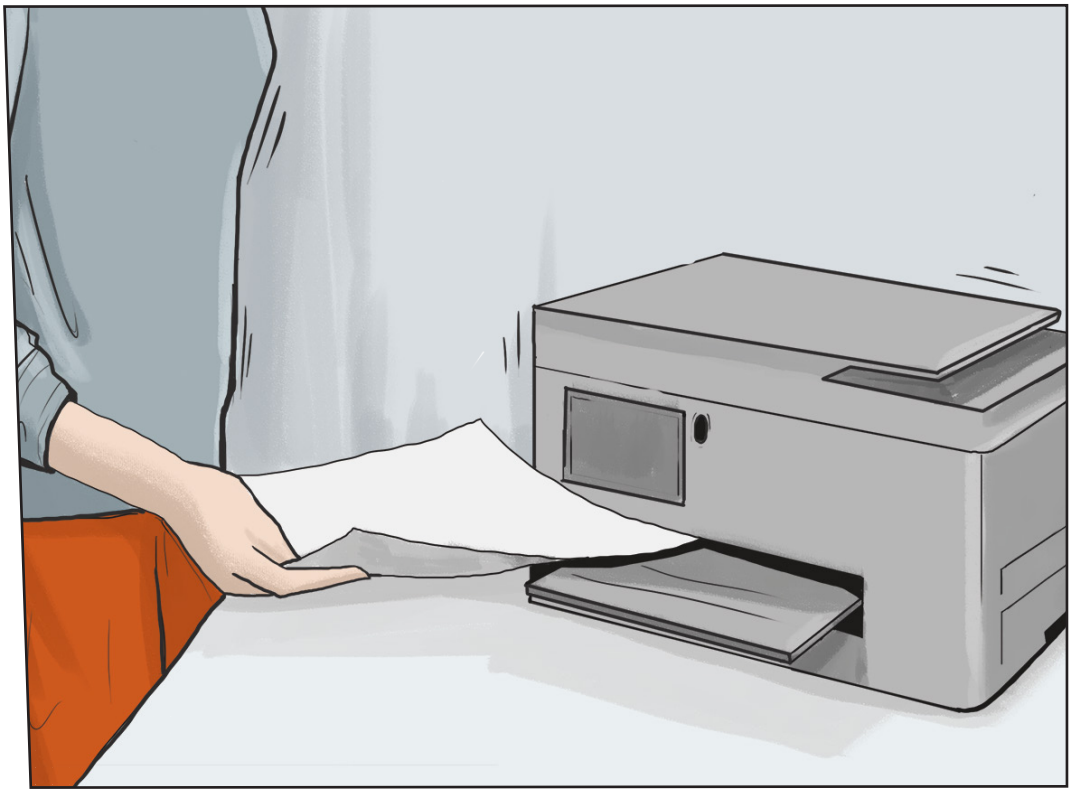
Tiukentunut lainsäädäntö tarkoittaa, että vaatimustenmukaisuus on tärkeämpää kuin koskaan. Lait, kuten yleinen tietosuoja-asetus, sisältävät säännöt tietojen käyttöön ja säilytykseen. Organisaatiot eivät esimerkiksi saa säilyttää henkilötietoja kauempaa kuin on ehdottomasti tarpeen. Silti monien organisaatioiden arkistointistrategiat ovat edelleen sattumanvaraisia: dokumenttien tallennukseen ei ole virallisia paikkoja, eikä palvelimiin tallennettuja dokumentteja pystytä löytämään.
Jos entinen työntekijä tai hakija tekisi organisaatiolle tietopyynnön, sen olisi erittäin vaikea kertoa, mitä tietoja sillä on. Lisäksi organisaation olisi vaikea osoittaa auditoinneissa, että se pystyy hallitsemaan sitä, missä henkilötietoja säilytetään.

SALAISET ASEET

Therefore Online
Therefore Onlinen vahvan suojauksen ansiosta organisaatiot voivat määrittää automaattiset asetukset dokumentteihin pääsylle sekä tietojen säilytykselle, jaolle ja muokkaukselle. Dokumentteihin liittyviä toimia seurataan, jotta tietoja voidaan hallita ja ne nähdään kaikissa vaiheissa. Tämä helpottaa auditointeja.

Organisaatio Y voi myös määrittää automaattiset arkistointikäytännöt, jotta arkaluonteisia tietoja sisältävät vanhat asiakirjat poistetaan sopivan säilytysjakson jälkeen ja vaatimuksia noudattaen. Koska Therefore Online on pilvipohjainen, myös tiimit, jotka eivät ole paikan päällä, voivat ladata asiakirjoja varmoina siitä, että ne suojataan.

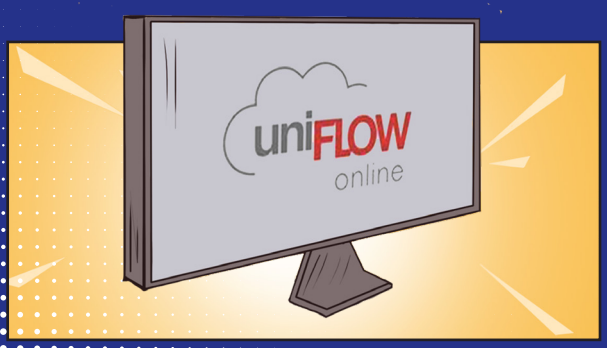
Työntekijän uusi linjapäällikkö Ingrid työskentelee kotona ja valmistelee toimistolla seuraavana päivänä pidettävää perehdytyshaastattelua. Hän haluaa tulostaa kirjeen, jossa vahvistetaan uuden työntekijän palkka, sekä muut lomakkeet, jotka hän luovuttaa prosessin aikana. Ingrid on vasta aloittanut kotona työskentelyn eikä ole saanut työtulostinta, joten hän käyttää omaa laitettaan.



Organisaatioissa on helppo unohtaa, että tulostimet ovat tärkeä osa työnkulkujen turvallisuutta ja vaatimustenmukaisuutta, koska laitteiden kautta kulkee arvokkaita tietoja ja asiakirjoja. Organisaatioilla on oltava lain vaatimusten mukainen kirjausketju, josta ilmenee, miten arkaluonteisia tietoja käytetään. Tämä edellyttää parempaa näkyvyyttä ja seurantaa sille, miten asiakirjoja ja laitteita käytetään yhdessä. Koska Ingrid käyttää omaa tulostintaan, se ei ole yhteydessä yrityksen verkkoon. Laitetta ei siis voi jäljittää, laitteeseen tallennetuista tiedoista ei ole kirjausta eikä laitteen tietoturvaa voi taata.

SALAISET ASEET

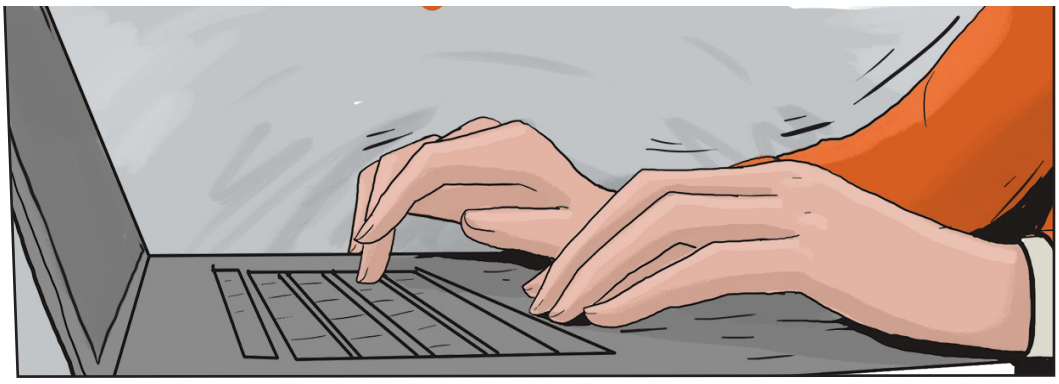
MAXIFY GX6050
Tämä tehokas pöytätulostin tuottaa laadukkaita tulosteita kotona työskenteleville, ja auttaa myös pitämään asiakirjat suojattuina ja vaatimustenmukaisina uniFLOW Online -integroinnin ansiosta. Skannaus itselle -toiminto estää Ingridiä lähettämästä asiakirjoja kenellekään muulle kuin omaan sähköpostiinsa tai omaan kansioonsa, jotta hän ei lähetä asiakirjoja vahingossa omille yhteyshenkilöilleen. Turvatulostuksen vapautustoiminnon ansiosta Ingrid tulostaa asiakirjat vasta sitten, kun hän on valmis, jotta arkaluonteiset asiakirjat eivät jää laitteeseen.



uniFLOW Online
Tämä sisäinen ohjelmisto integroi MAXIFY GX6050 -tulostimen organisaation ympäristöön, jotta Organisaatio Y:n IT-tiimi voi seurata Ingridin tulostustoimia ja raportoida tarkasti, miten arkaluonteisia tietoja käytetään, vaikka hän työskentelisi kotoa käsin.

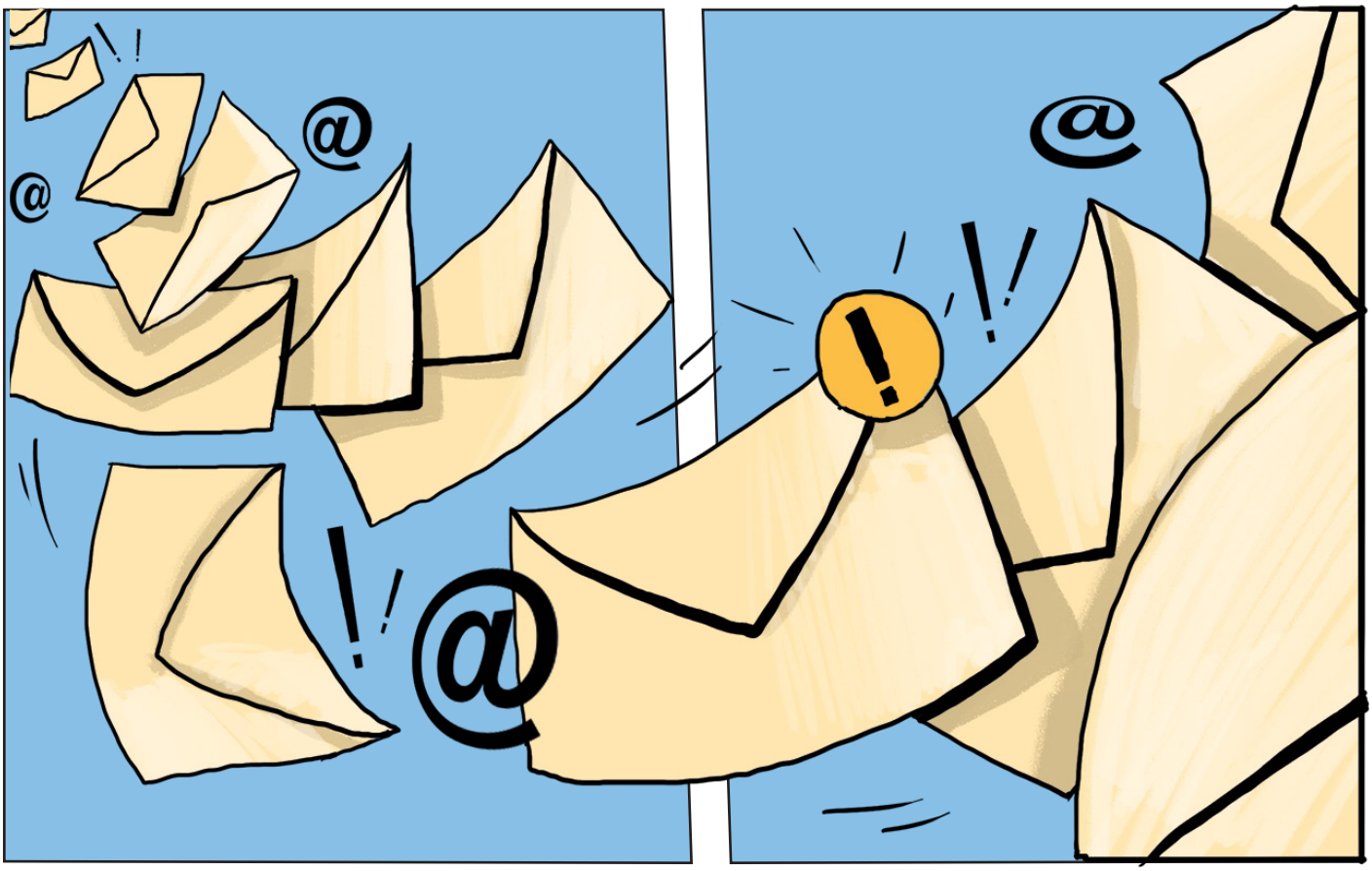
Uuden työntekijän ensimmäinen kuukausi päättyy, ja henkilöstöhallinnon Fatima valmistautuu lähettämään palkkalaskelman. Valitettavasti uudella työntekijällä on sama etunimi kuin toisella työntekijällä. Fatima lähettää vahingossa palkkalaskelman väärälle henkilölle, mikä tarkoittaa, että tämä näkee kuinka paljon toiselle työntekijälle maksetaan.

Yritys on rikkonut työntekijän tietojen luottamuksellisuutta – jopa niin pahasti, että asia voi päätyä työtuomioistuimeen. Lisäksi uusi työntekijä on nähnyt kollegansa palkkalaskelman, joten hän pyytää nyt henkilöstöhallintoa tarkistamaan oman palkkansa eikä ehkä enää tunne oloaan mukavaksi nykyisessä tehtävässään.



Viestintä on aina dokumenttien työnkulun riskialtis vaihe, koska siinä jaetaan tietoja sisäisesti työntekijöille tai ulkoisesti asiakkaille, toimittajille ja muille sidosryhmille. Tavallisessa auditoinnissa organisaatioiden odotetaan osoittavan, miten arkaluonteisia tietoja jaetaan muille osapuolille.

Koska organisaation viikoittainen viestimäärä on suuri, on oleellisen tärkeää, että käytössä on ratkaisuja, jotka helpottavat näiden prosessien seurantaa ja jäljitystä.



SALAISET ASEET

uniFLOW sysHub
uniFLOW sysHUB -ohjelmiston avulla käyttäjät voivat valvoa tarkasti sisäistä viestintää, joten Fatiman on helppo pitää HR-osaston viestintä luottamuksellisena. Tämä ratkaisu yhdistää sisäiset viestintäprosessit ja -sovellukset yhdeksi työnkuluksi, jota hallitaan samasta paikasta. uniFLOW sysHUB automatisoi työnkulun, jotta se toimii tehokkaammin ja pienentää virheiden riskiä. Tässä esimerkissä Fatima ei voi vahingossa lähettää luottamuksellisia tietoja toiselle työntekijälle.

Jokainen työnkulun vaihe kirjataan lokiin ja tallennetaan sysHUB-kirjastoon tarkastelua ja kirjausketjuja varten. Fatima voi tarkistaa toimitusvahvistuksesta, että viesti on tavoittanut oikean henkilön.

KUINKA VOIMME AUTTAA?

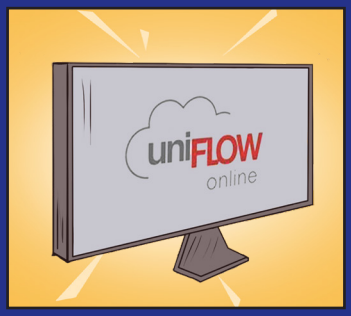
Jokainen yritys haluaa pitää tietonsa turvassa ja vaatimustenmukaisina. Organisaatiot Y ja X ovat kuitenkin osoittaneet, että ympäristössä on arvaamattomia uhkia. Yrityksillä on vastassaan entistä enemmän rikollisia, ja virheiden tapahtuessa tiukentunut lainsäädäntö tekee tilanteesta vakavan. Voi näyttää siltä, että peli on menetetty, mutta niin ei tarvitse olla. Salaisuus piilee oikeanlaisen tekniikan ja kumppanin valinnassa.

Canon on johtava tulostuksen ja dokumenttien tietoturvaratkaisujen ja -palvelujen tarjoaja IDC MarketScapen ja Quocirca Print Security Landscape -raportin mukaan. Laitteistomme, ohjelmistomme ja palvelumme on suunniteltu auttamaan organisaatiotasi toimimaan mahdollisimman tehokkaasti monimutkaisessa maailmassa. Teknologiamme tukee kaikenlaisia työympäristöjä - riippumatta siitä, missä työntekijät työskentelevät tai missä vaiheessa digitalisaatiota yritys on.

Koska tuotteemme on suunniteltu turvallisiksi, tietojen suojaaminen on helppoa. Ratkaisumme on suunniteltu torjumaan hyökkäykset, suojaamaan tietoja sekä ylläpitämään ja suojaamaan vaatimustenmukaisuutta, jotta voit hyödyntää uusia ominaisuuksia ilman lisätyötä.

TULOSTUS- JA SKANNAUSLAITTEET
Tulostus- ja skannauslaitevalikoimassamme on uusimmat tietoturvaominaisuudet, jotka suojaavat tärkeitä tietoja dokumenttien työnkulun jokaisessa vaiheessa. Kaikkien Canon-tuotteiden turvallisuus tarkastetaan suunnittelu- ja kehitysvaiheissa sekä ennen julkaisua.

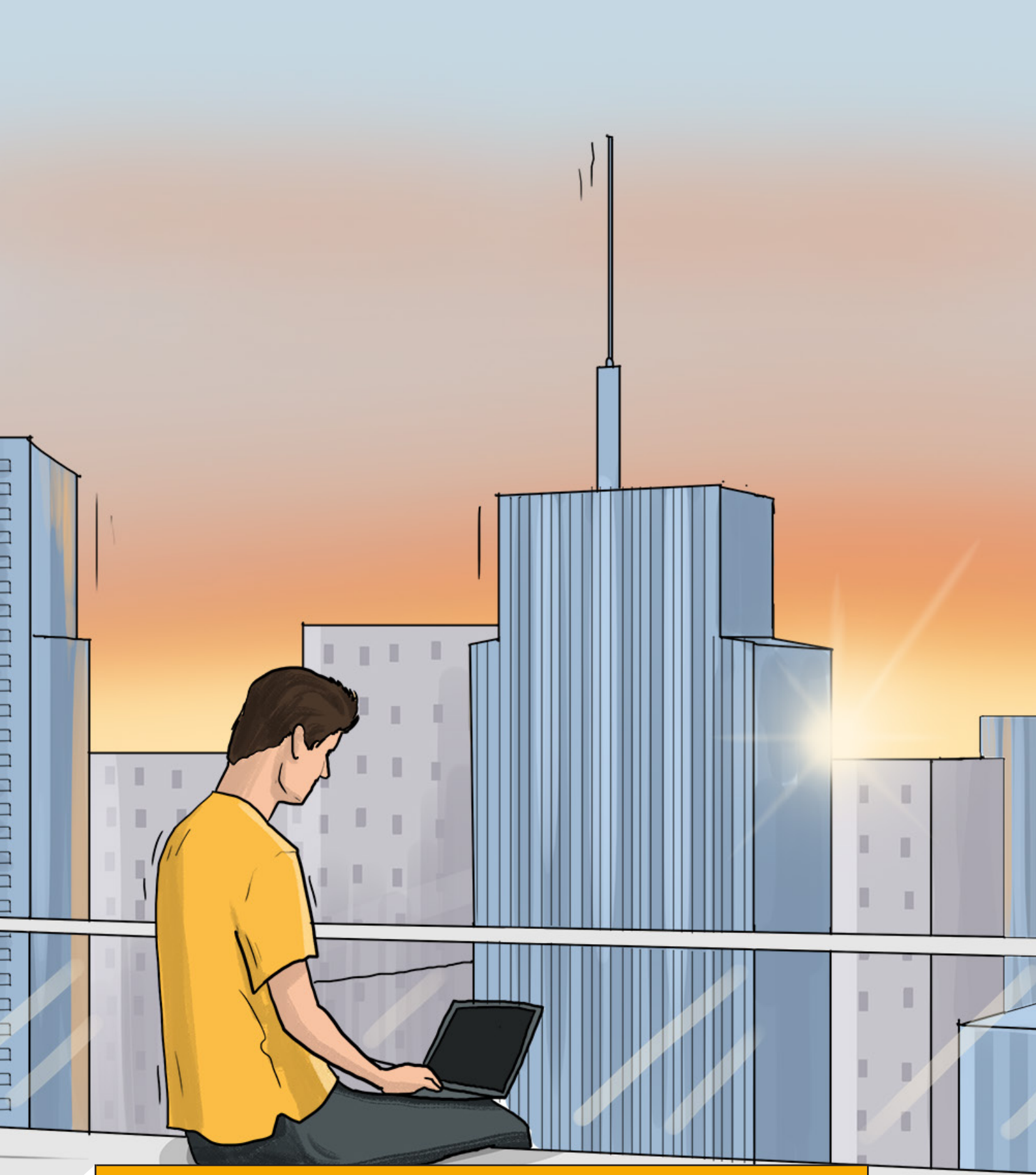
Luomme vahvoja kumppanuuksia Trellixin ja Microsoftin kaltaisten alan johtavien toimijoiden kanssa, jotta laitteet voidaan suojata mahdollisimman kattavasti ja yhteensopivasti. Lisäksi meillä on erillinen tuotteiden tietoturvasta vastaava tiimi.



OHJELMISTOT
Ymmärrämme, että tiedot eivät ole sidoksissa sijaintiin. Siksi tarjoamme ohjelmistoja, jotka suojaavat tietoja kaikkialla. Teemme yhteistyötä IOActiven kaltaisten riippumattomien organisaatioiden kanssa, kun teemme penetraatiotestejä julkaisuvaiheessa ja tärkeiden ohjelmistopäivitysten yhteydessä.

PALVELUT
Tietoturvapalvelujemme avulla voit varmistaa tietojen suojauksen vaatimustenmukaisuuden ja suojata arkaluonteisia tietoja tulostus- ja skannausympäristön koko elinkaaren ajan.


PASSPORT



Valmiina kukistamaan tietoturvan ja vaatimustenmukaisuuden haasteet? Varaa Canon yhteyshenkilöltäsi esittely teknologiastamme ja sen mahdollisuuksista, niin näet, miten ratkaisumme voivat auttaa yritystäsi.

Haluatko lisätietoja salaisista aseistamme? Tutustu aiheeseen Canonin Tiedonhallinnan palvelujen sivustolla.

TIETOJA CANONISTA

Canon on kuvantamisen edelläkävijä. Käytämme kuvantamista saadaksemme aikaan muutosta. Haluamme auttaa asiakkaitamme edistämään digitalisaatiota ja työskentelemään uusilla tavoilla. Haluamme osoittaa sosiaalisen vastuumme nostamalla kestävän kehityksen yrityskulttuurimme ytimeen.

Haluamme panostaa uusiin markkinoihin, tuotteisiin ja teknologioihin, jotka tarjoavat pitkällä aikavälillä hyötyjä asiakkaillemme, työntekijöillemme ja koko yhteiskunnalle.

CANONIN TOIMINTA PERUSTUU NELJÄÄN KESKEISEEN PILARIIN:

Innovointi

Canon on kehittänyt markkinoiden johtavia kuvantamisteknologioita jo yli 80 vuoden ajan. Alan edelläkävijänä olemme vahvasti sitoutuneet teknologian kehittämiseen.

Tukipalvelut

Laaja palveluvalikoimamme takaa huippulaadun ja asiakastyytyväisyyden. Asiantuntijamme auttavat asiakkaitamme parantamaan tuotteidemme ja ratkaisujemme tehokkuutta ja hyödyntämään niiden täyden potentiaalin.

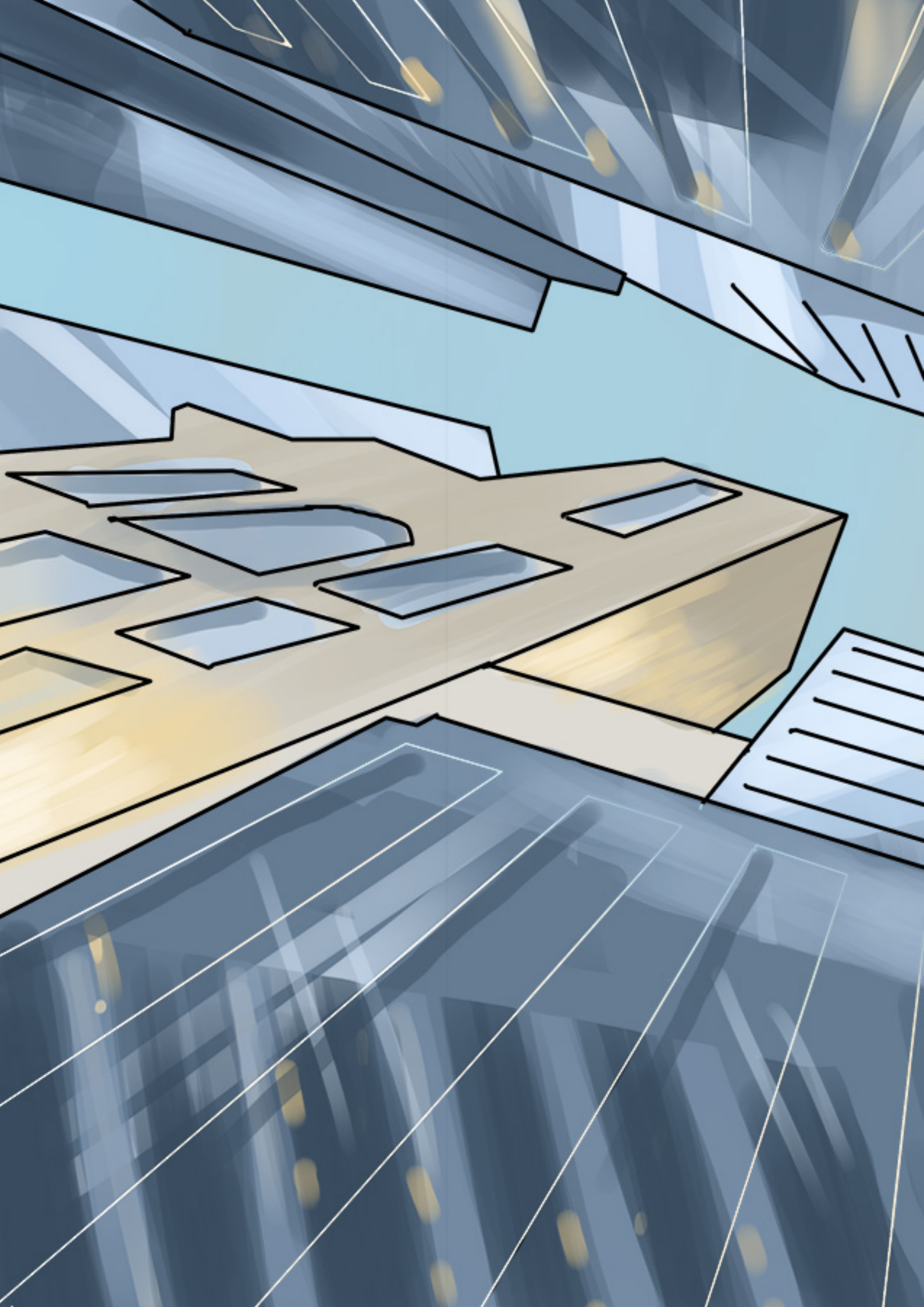
Tietoturva

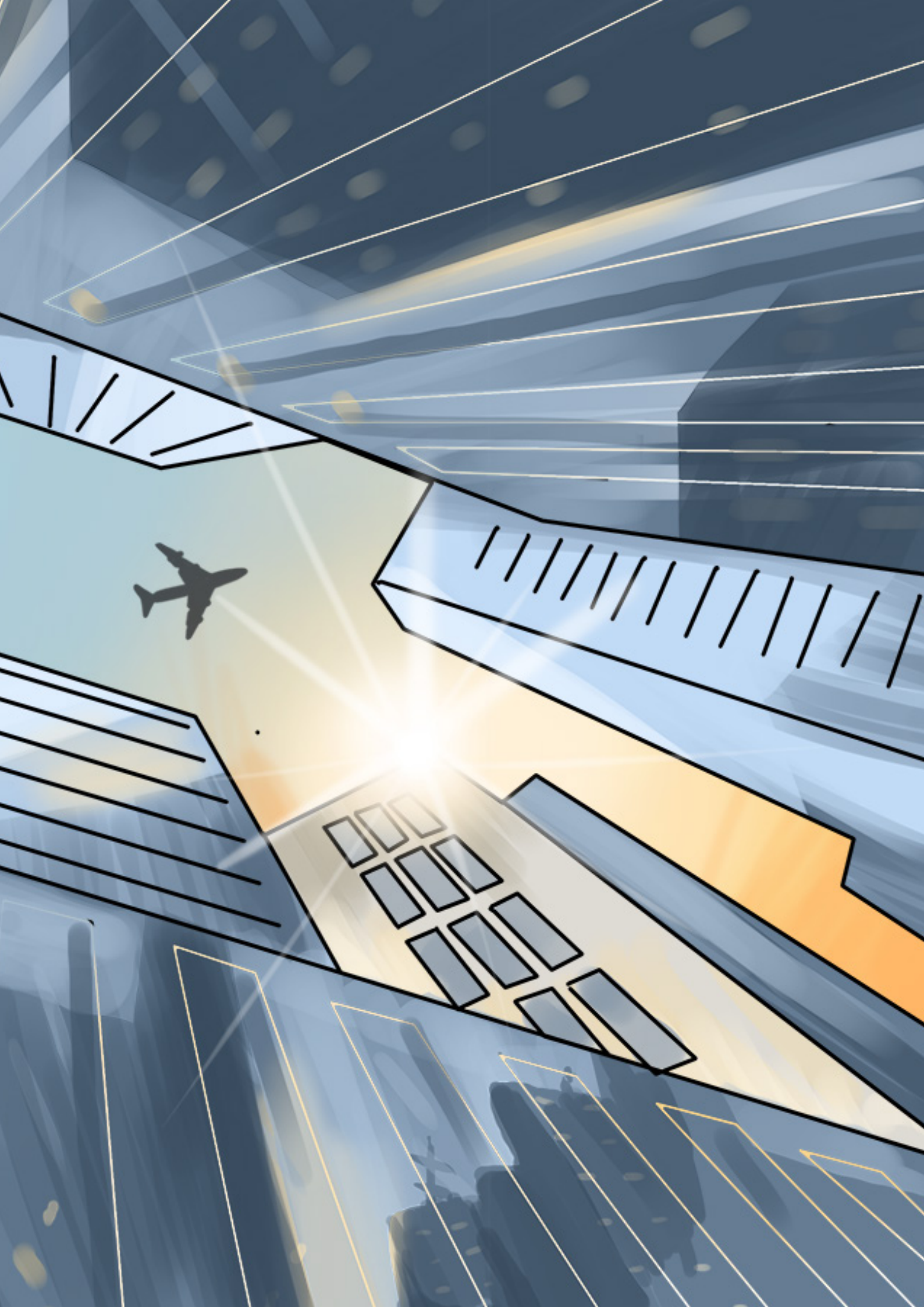
Canonin ratkaisut ja palvelut auttavat turvaamaan kaikki dokumentit ja arkaluontoiset tiedot niin paperiversioina kuin digitaalisessakin muodossa koko dokumenttien elinkaaren ajan. Laitteemme, ratkaisumme ja palvelumme on suunniteltu alusta lähtien tietoturvallisiksi.

Vastuullisuus

Canon on yhdenmukaistanut kestävän kehityksen käytäntönsä YK:n asettamien kestävän kehityksen tavoitteiden mukaisesti. Canon on sitoutunut vähentämään hiilidioksidipäästöjä tuotteiden elinkaaren aikana pienentämällä pakkausmateriaalien käyttöä ja keskittämällä jakelukeskuksia.

NÄIDEN PILARIEN ANSIOSTA CANON ON PARAS KUMPPANI YRITYKSELLESI.





Canon Inc.
Canon.com

Canon Europe / Canon Oy
canon-europe.com / canon.fi
Finnish edition

Canon Oy
Huopalahdentie 24, PL 1
00351 Helsinki
puhelin 010 544 20
canon.fi