



# BESKYTTE KONTORET

**Canon**

---



# HVOR SIKKER ER INFORMASJONEN PÅ KONTORET DITT?

Dagens bedrifter er svært avhengige av informasjon. Derfor er det viktig å kunne opprette komplekse nettverk av tilkoblede teknologier, prosesser, mennesker og organisasjoner på tvers av landegrenser. Nye og smidige arbeidsmetoder trer frem, gjør om kontoret og måten folk skaper, deler og forbruker informasjon på. I slike sammensatte miljøer er det mer utfordrende enn noen gang å sørge for god datasikkerhet. De fleste bedrifter investerer i avansert teknologi som blant annet solide brannmurer, oppdatert antivirusbeskyttelse og sikkerhetsprogrammer. Bedriftene ser imidlertid ofte ikke behovet for å utvide beskyttelsen til å dekke kontorskriverne sine, og derfor blir de mer sårbare enn de tror.



## TENK PÅ SKRIVERNE DINE

Moderne flerfunksjonsskrivere (MFP-er) har blitt utviklet til kraftige verktøy, som på lik linje med PC-er og servere har operativsystemer, store harddisker, kan koble til nettverk og Internett samt deles av brukere for å behandle store antall forretningskritiske dokumenter hver dag.



## HVA ER RISIKOENE?

- Uautoriserte brukere kan se sensitiv informasjon lagret på ubeskyttede MFP-er.
- Tilgjengeligheten til utskriftsinfrastrukturen reduseres på grunn av feil betjening.
- Uvedkommende kan få tilgang til nettverket via skriveren og bruke det til angrep.
- Konfidensielle dokumenter som er glemt på utmatingsbrettet etter utskrift, eksponeres.
- Utskrifter som tilhører ulike brukere, forveksles.
- Dokumenter som faxes eller sendes per e-post, ender opp hos feil mottaker som følge av skrivefeil.
- Utskrifts- eller skannedata som sendes, fanges opp av hackere.
- Tap av data på grunn av uforsiktig avhending av skrivere når leieavtalene avsluttes.

«Det er vel verdt å ta i bruk grunnleggende standarder for informasjonssikkerhet på kontoret, der du muligens håndterer store mengder data. En skriver er i dag ikke lenger en simpel maskin, det er en server som også kan skrive ut papir.»

(CISO, Publicis Groupe)

# SIKRE UTSKRIFTSLØSNINGER FOR BEDRIFTEN DIN

## Tilpasset sikkerhet og personvern

Når vi utformer eller velger teknologi, produkter og tjenester for kundene våre, vurderer vi hvordan disse kan påvirke informasjonssikkerheten i kundenes miljøer. Derfor er de flerfunksjonelle kontorskriverne våre utstyrt med en rekke sikkerhetsfunksjoner, både som standard og tilleggsutstyr, som gjør det mulig for bedrifter i alle størrelser å oppnå ønsket beskyttelsesnivå for



## ENHETER | NETTVERK | DOKUMENTER | BEDRIFTEN DIN



### INTERNASJONALT ANERKJENTE STANDARDER OG SERTIFISERINGER

De multifunksjonelle imageRUNNER ADVANCE-enhetene våre er rutinemessig evaluert og sertifisert ved hjelp av Common Criteria-metoden og i samsvar med krav til Standard Beskyttelse for Harddiskenheter (HCD\_PP) eller IEE P2600.2.



### SIKKERHETSTESTING

Canon benytter en av de mest omfattende rutinene for sikkerhetstesting i kontorutstysbransjen. Teknologier som er tatt i bruk i produktporteføljen vår, gjennomgår de samme høye standardene for testing som vi forventer i vår egen virksomhet.

Som bransjeleder innen utvikling av innovative løsninger for utskrift og informasjonsstyring for kontor og bedrifter, samarbeider Canon med kunder for å hjelpe dem med å ta i bruk en felles tilnærming til informasjonssikkerhet – en tilnærming som regner sikkerhetsimplikasjonene til kontorteknologien vår som en del av det større informasjonssystemet.



# BESKYTT ENHETEN

## Omfattende beskyttelse for de fysiske ressursene dine



### LØSNINGER FOR BRUKERGODKJENNING

Beskytt enheten mot uautorisert bruk ved å implementere kontroll av brukertilgang med godkjenning. Du får også en ekstra fordel siden brukerne får raskere tilgang til de foretrukne innstillingene og utskriftsjobbene sine, samtidig som løsningen gir økt ansvarlighet og kontroll. Avdelingsskriverne våre er utstyrt med Universal Login Manager, en fleksibel påloggingsløsning som muliggjør brukergodkjenning mot en brukerdatabase som er opprettet på enheten, domenegodkjenning via Active Directory eller uniFLOW-server. Dette gir bedrifter muligheten til å kontrollere tilgangen til enheter, samtidig som de oppnår riktig balanse mellom brukervennlighet og sikkerhet.



### KONTROLL FOR ENHETSSTYRING

Enhetskonfigurasjon, for eksempel nettverksinnstillinger og andre kontrollalternativer, er bare tilgjengelige for brukere som har administratorrettigheter som hindrer tilsiktede eller utilsiktede endringer.



### FOREBYGGENDE SIKKERHET

Med imageRUNNER ADVANCE-produkter får du en rekke sikkerhetsinnstillinger som kan beskytte skriverne mot angrep. Sikker oppstartfunksjonalitet gir enhetsintegritet, mens Syslog-data viser enhetens sikkerhetstilstand i sanntid (data kan leses av et passende tredjeparts SIEM-system).



### SYSTEM FOR TILGANGSADMINISTRERING

Denne funksjonen gir detaljert kontroll over tilgangen til enhetsfunksjonene. Administratorer kan bruke tilgjengelige standardroller eller opprette skreddersydde roller med et ønsket tilgangsnivå. Enkelte brukere kan for eksempel begrenses fra å kopiere dokumenter eller bruke send-funksjonen.



### INNSTILLING AV SIKKERHETSBESTEMMELSER

De nyeste imageRUNNER ADVANCE-enheterne er også utstyrt med en funksjon for sikkerhetsbestemmelser, som gjør det mulig for administratoren å få tilgang til alle sikkerhetsrelaterte innstillinger fra én meny og redigere dem før de trer i kraft på maskinen.

Når endringene trer i kraft, må bruken av endringene til enheten og innstillingene samsvare med bestemmelsene. Sikkerhetsbestemmelsene kan beskyttes med et eget passord, slik at tilgangen til dette området begrenses til den IT-sikkerhetsansvarlige, noe som gir ytterligere kontroll og sikkerhet.



### BESKYTTELSE AV DATA PÅ ENHETENS LAGRINGSMEDIER

Flerfunksjonsskriveren inneholder til enhver tid store mengder data som bør beskyttes – fra utskriftsjobber som venter på å bli skrevet ut til mottatte fakser, skannedata, adressebøker, aktivitetslogger og jobbhistorikk. Canon-enheter tilbyr en rekke tiltak for å beskytte dataene dine på hvert steg av enhetens levetid og kan sikre at dataene forblir konfidensielle og tilgjengelige samt bevarer integriteten.

Avhengig av enhetsmodellen brukes enten en HDD (hard disc drive) eller SSD (solid-state drive). Siden en HDD bruker en spinnende plate som registrerer data, kreves det en rekke overskrivninger, vanligvis tre, for å sikre at dataene overskrives på en effektiv måte. I motsetning til en HDD flytter SSD data rundt den tilgjengelige minneplassen for å sikre at det er jevn elektrisk slitasje på minnecellene. Hver celle har bare et begrenset antall skrivinger, og TRIM-prosessen maksimerer SSD-levetiden samtidig som den overskriver logisk slettede data.

imageRUNNER ADVANCE har flere ulike konfigurasjonsalternativer som kan konfigureres til å angi punktet der en overskriving utføres, og metoden for hvordan overskriving skal utføres.



## HVOR SIKRE ER ENHETENE DINE?

**1**

Deles enhetene av flere personer, og er de plassert på offentlige områder?

**2**

Kan brukere få usikret tilgang til enhetene?

**3**

Har du iverksatt tiltak for å beskytte informasjonen på enhetens harddisk?

**4**

Kan uautoriserte brukere endre på enhetsinnstillingene?

**5**

Har du vurdert livssyklusen til og sikker avhending av enheten?

## DISKKRYPTERING

imageRUNNER ADVANCE-enhetene våre krypterer alle data på harddisken, noe som øker sikkerheten. Sikkerhetsbrikken som sikrer datakryptering, overholder sikkerhetsstandarden FIPS 140-2 nivå 2, fastsatt av amerikanske myndigheter og er sertifisert under Cryptographic Module Validation Program (CMVP), som er etablert av USA og Canada samt Japan Cryptographic Module Validation Program (JCMVP).

## SLETNING AV DATALAGRING

Enkelte data, for eksempel kopierte eller skannede billedata samt dokumentdata som skrives ut fra en datamaskin, lagres bare midlertidig på HDD eller SSD og slettes etter at operasjonen er fullført. Enhetene våre er utstyrt med en funksjon for tidvis å slette restdata som en del av jobbbehandling. Dette sikrer at restdata ikke oppbevares.

## INITIALISER ALLE DATA OG INNSTILLINGER

Du kan overskrive alle dokumenter og data på harddisken og gjenopprette maskininnstillingene til fabrikkinnstillingene for å unngå tap av data når du erstatter eller avhender harddisken.

## SPEILING AV HARDDISK\*

Bedrifter har muligheten til å sikkerhetskopiere dataene på enhetsharddisken ved å benytte en ekstra valgfri harddisk. Når speiling utføres, er data på begge harddisker fullstendig kryptert.

\*Tilleggsutstyr. Hvis du vil ha detaljert informasjon om tilgjengeligheten til funksjonene og alternativene i hele porteføljen for kontorutskrift, kan du ta kontakt med Canon-representanten din.



# SIKRE NETTVERKET DITT



## KAN SKRIVEREN UTSETTE NETTVERKET DITT FOR RISIKO?

- Er nettverksportene åpne for angrep?
- Kan gjester skrive ut og skanne uten å utsette nettverket for risiko?
- Er det trygt og praktisk at de ansatte kan ta med seg sine egne enheter på jobb?
- Er utskriftsdatastrømmene kryptert fra PC-er til utdataenheten?
- Er utskrift- og skannedata sikret under sending?

# Canon tilbyr en rekke sikkerhetsløsninger som beskytter nettverket ditt og dataene dine mot interne og eksterne angrep.

## FILTRERING AV IP- OG MAC-ADRESSER

Beskytt nettverket mot uautorisert tilgang fra tredjeparter ved å bare tillate kommunikasjon med enheter som har en bestemt IP- eller MAC-adresse, for både utgående og inngående kommunikasjon.

## KONFIGURASJON AV PROXY-SERVER

Angi en proxy som skal håndtere kommunikasjonen i stedet for maskinen din, og bruk den når du kobler til enheter utenfor nettverket.

## IEEE 802.1X-GODKJENNING

Uautorisert nettverkstilgang blokkeres av en LAN-bryter som bare gir tilgangsrettigheter til klientenheter som er godkjent av godkjenningsserveren.

## IPSEC-KOMMUNIKASJON

IPSec-kommunikasjon hindrer tredjeparter i å avskjære eller tukle med IP-pakker som sendes over IP-nettverket.

Bruk TLS-kryptert kommunikasjon for å hindre at data som utveksles mellom maskinen og andre enheter (som datamaskiner), kan spores, forfalskes og tukles med.

## PORTKONTROLL

Konfigurer portene som en del av innstillingene dine for sikkerhetsbestemmelser.

## AUTOMATISK REGISTRERING AV SERTIFIKAT

Med denne funksjonen reduseres arbeidet med å opprettholde sikkerhetssertifikater betraktelig. Ved bruk av bransjeanerkjent teknologi kan en systemadministrator automatisk oppdatere og utgi sertifikater og sørge for at sikkerhetsbestemmelser overholdes til enhver tid.

## LOGGOVERVÅKING

Ulike logger tillater at du kan overvåke aktiviteten rundt enheten din, inkludert blokkerte kommunikasjonsforespørslers.

## WI-FI DIRECT

Aktiver node-til-node-tilkobling for mobil utskrift uten at mobilenheten trenger tilgang til nettverket.

## KRYPTERING AV DATA UNDER SENDING TIL OG FRA ENHETEN

Dette alternativet krypterer utskriftsjobber under sending fra brukerdatablader til flerfunksjonskriveren. Ved å aktivere det universelle sikkerhetsfunksjonssettet kan skannede data i PDF-format også krypteres.

## MOBIL GJESTEUTSKRIFT

Vår sikre programvare for nettverksutskrifts- og skanneadministrering håndterer vanlige sikkerhetsrisikoer for mobil- og gjesteutskrift, ved å tilby eksterne jobbsendingsbaner via e-post, nett og mobilapp. Dette minimerer angrepsvektorer ved å låse flerfunksjonsenheter til en sikker kilde.



# BESKYTT DOKUMENTENE DINE

Alle bedrifter håndterer sensitive dokumenter som kontraktsmessige avtaler, lønningsinformasjon for ansatte, kundedata, forsknings- og utviklingsplaner med mer. Dersom dokumenter havner i feil hender, kan konsekvensene være alt fra store bøter og omdømmetap til juridiske tiltak.

**Canon tilbyr en rekke sikkerhetsløsninger som beskytter de sensitive dokumentene gjennom hele livssyklusen.**



## KONFIDENSIALITET FOR DE UTSKREVNE DOKUMENTENE

### Sikker utskrift

Brukeren kan angi en PIN-kode for utskrift, slik at dokumentet bare kan skrives ut etter at riktig PIN-kode er angitt på maskinen. Dette gjør det mulig for enkeltpersoner å sikre de dokumentene de regner som konfidensielle.

### Holde tilbake alle utskriftsjobber

På imageRUNNER ADVANCE kan administratoren holde tilbake alle innsendte utskriftsjobber, slik at brukerne må logge seg på før jobbene kan skrives ut. Dette beskytter konfidensialiteten til alle utskrevne dokumenter.

### Postbokser

Utskriftsjobber eller skannede dokumenter kan lagres i en postboks for tilgang senere. Postbokser kan beskyttes med en PIN-kode for å sikre at bare den tilordnede eieren kan se innholdet som er lagret i den. Denne sikre plassen på maskinen er egnet for å oppbevare dokumenter som ofte må skrives ut (for eksempel skjemaer), men som krever nøye håndtering.

### uniFLOW og sikker utskrift\*

Med sikker uniFLOW MyPrintAnywhere-utskrift sender brukerne utskriftsjobber via den universale driveren og henter dem fra hvilken som helst skriver på nettverket.



## MOTARBEIDE ELLER HINDRE DUPLISERING AV DOKUMENTER

### Utskrift med synlige vanmerker

Driveren kan skrive ut synlige merker på siden, som overlegg eller bak på dokumentinnholdet. Dette motvirker kopiering ved å øke brukernes bevissthet rundt dokumentenes konfidensialitet.

### Skriv ut / kopier med usynlige vanmerker

Når dette alternativet er aktivert, kan dokumenter skrives ut eller kopieres med innebygd skjult tekst i bakgrunnen, slik at teksten vises på dokumentet når teksten dupliseres, og fungerer preventivt.



## HVOR SIKRE ER DOKUMENTENE DINE?

- |   |  |
|---|--|
| <b>1</b><br>Forhindres uautoriserte brukere fra å få tilgang til sensitive dokumenter på skriveren? | <b>2</b><br>Kan du sikre at alle brukerdokumenter sendes gjennom den delte enheten på en konfidensiell måte? |
| <b>3</b><br>Kan noen ta med seg sensitive dokumenter fra skriveren din?                             | <b>4</b><br>Kan du forhindre vanlige feil når du sender dokumenter fra enheten?                              |



### UTØVE KONTROLL OVER DOKUMENTSENDING OG FAKSING

#### Begrense mottakere for sending

Administratorer kan begrense de tilgjengelige mottakerne til bare de som står i adresseboken eller LDAP-serveren, de påloggede brukeradressene eller enkelte domener. Dette gjøres for å redusere risikoen av informasjonslekkasje.

#### Deaktivere automatisk utfylling av adresse

Unngå å sende dokumenter til feil mottaker ved å deaktivere automatisk utfylling av e-postadresser.

#### Beskyttelse av adressebok

Angi en PIN-kode for å beskytte enhetsadresseboken mot uautorisert redigering fra brukere.

#### Bekreftelse av faksnummer

Du kan hindre at dokumenter sendes til feil mottakere ved å kreve at brukere skriver inn faksnummeret to ganger for bekreftelse, før faksen sendes.

#### Konfidensialitet for mottatt faks

Angi maskinen til å lagre dokumenter i minnet uten å skrive ut. Du kan også beskytte konfidensialiteten til mottatte faksdokumenter ved å bruke betingelser for å bestemme lagringsplasseringen for en konfidensiell innboks samt angi PIN-koder.



### VERIFISERE DOKUMENTOPPRINNELSE OG -AUTENTISITET VED BRUK AV DIGITALE SIGNATURER

#### EnhetsSignatur

Enhetssignaturen kan brukes på skannede dokumenter i PDF- eller XPS-format ved å bruke en nøkkel og sertifiseringsmekanisme slik at mottakeren kan bekrefte dokumentets opprinnelse og autentisitet.

#### Brukersignatur\*

Med dette alternativet kan brukerne sende en PDF- eller XPS-fil med en unik digital brukersignatur fra en sertifiseringsinstans. På denne måten kan mottakeren bekrefte hvilken bruker som har signert filen.

\*Tilleggsutstyr. Hvis du vil ha detaljert informasjon om tilgjengeligheten til funksjonene og alternativene i hele porteføljen for kontorutskrift, kan du ta kontakt med Canon-representanten din.



# SIKKERHET FOR BEDRIFTS- INFORMASJON

Canon kan bidra til den totale beskyttelsen av informasjon i virksomheten din.



## FULLSTENDIG KONTROLL FOR TOTALREGISTRERING OG UTSKRIFTSBEHOV

Med vår modulære programvare for utskriftsstyring får bedrifter sikker deling av nettverksenheter, slik at de kan skrive ut jobber sikkert på alle skrivere som er koblet til serveren for utskriftsstyring. Mobile brukere støttes av en sentral kontrollert tjeneste, der både interne brukere og gjestebbrukere har sikker tilgang til utskrift fra mobile enheter.

Skannemodulen for bedriftsskanning gjør at dokumenter kan skannes, komprimeres, konverteres og distribueres fra flerfunksjonsenheten til en rekke mottakere, inkludert nettskybaserte systemer. Du kan også videresende utskriftsjobber til den mest egnede skriveren på en sikker måte, slik at utskriftskostnadene for hvert dokument optimaliseres.

Løsningen vår forbedrer sikkerheten til dokumentene i hele bedriften, kombinert med fullstendig dokumentregnskap som gir fullstendig oversikt over brukeraktivitet, enhet og avdeling.



## SENTRALISERT SKRIVERADMINISTRASJON

Med IW MC-programvaren vår for enhetsadministrasjon kan enhetsinnstillinger, sikkerhetsbestemmelser, passord og sertifikater samt fastvare oppdateres og sendes ut til Canon-enheterne i hele nettverket. På denne måten sparer IT-teamet verdifull tid og holder sikkerheten i utskriftsinfrastrukturen oppdatert.



## ADMINISTRERTE UTSKRIFTSTJENESTER

Canon MPS kombinerer nyskapende teknologi og programvare med de rette tjenestene, slik at du får den ønskede utskrifts- og dokumentopplevelsen uten å skape bry for IT-teamene dine. Gjennom proaktiv administrering og kontinuerlig optimalisering av utskriftsinfrastrukturen og dokumentarbeidsflytene kan vi hjelpe deg med å nå sikkerhetsmålene dine samtidig som du reduserer kostnadene og øker produktiviteten i hele bedriften.

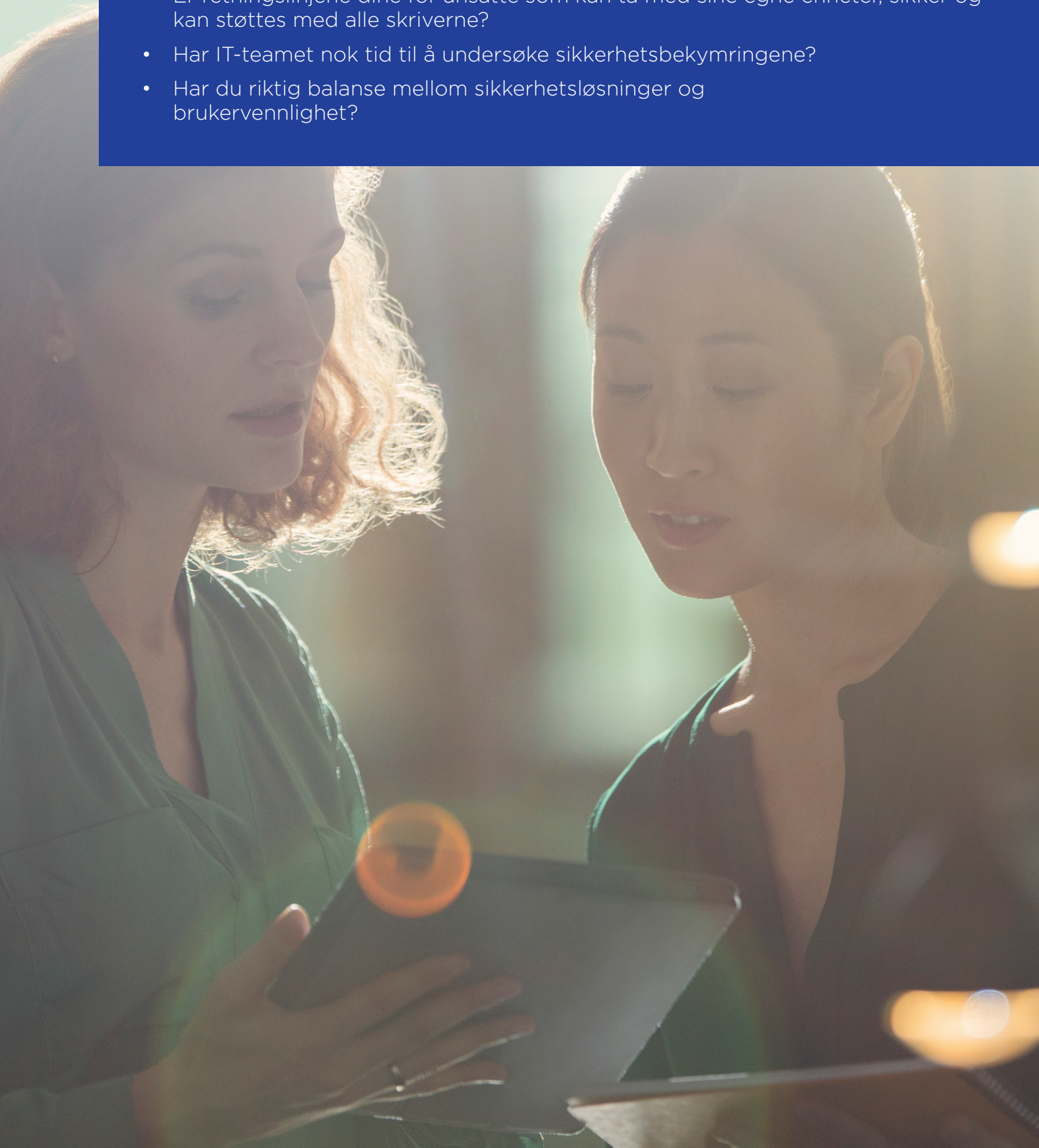


## TILPASSET UTVIKLING

Vi har et team av Canon-ansatte utviklere som kan foreslå og utvikle en tilpasset løsning som passer din spesifikke situasjon eller unike krav.

## HVOR OMFATTENDE ER BEDRIFTENS SIKKERHETSTILNÆRMING?

- Gjelder sikkerhetsbestemmelsene dine også for multifunksjonsenhetene dine?
- Hvordan sikrer du at utskriftsinfrastrukturen er oppdatert, og at forbedringene og feilrettinger implementeres raskt og effektivt?
- Kan gjester skrive ut og skanne uten å utsette nettverket for risiko?
- Er retningslinjene dine for ansatte som kan ta med sine egne enheter, sikker og kan støttes med alle skriverne?
- Har IT-teamet nok tid til å undersøke sikkerhetsbekymringene?
- Har du riktig balanse mellom sikkerhetsløsninger og brukervennlighet?



# HVORFOR CANON?

Canon er bilder. Vi prøver å gjøre en forskjell og skape mulighet for endring. For kundene våre når de gjør digitale endringer og arbeider på nye måter. For større samfunnsmessige endringer med vårt kontinuerlige fokus på bærekraft som en del av vår bedriftskultur.

Vi er i endring ved å investere i nye markeder, produkter og teknologier, så vi har et langsiktig perspektiv til fordel for alle: kundene våre, medarbeiderne våre og samfunnet generelt.

## Canon er bygd på fire hovedpilarer:



### SIKKERHET

Canons løsninger og tjenester bidrar til å sikre alle dokumenter og sensitive data, enten de er på papir eller i digitalt format, gjennom hele dokumentlivssyklusen. Sikker utforming: Løsningene og tjenestene er utviklet med sikkerhet i tankene.



### BÆREKRAFT

Canon har innrettet sin praksis for bærekraft etter FNs bærekraftsmål, som forpliktelser om å redusere CO2-utslipp i hele produktets levetid ved å redusere emballasjemengden og konsolidere distribusjonssentre.

**Alt dette gjør Canon til den rette partneren for deg.**



### SUPPORT

Et variert utvalg av tjenester som sikrer topp kvalitet og tilfredse kunder. Interne eksperter arbeider for å øke effektiviteten og er fokusert på å utnytte potensialet til kundene våre.



### INNOVASJON

En lang historie med innovasjon drevet av bildebehandling, som har levert nyskapende teknologi i over 80 år. Banebrytende ideer for bransjen og et sterkt engasjement for teknologiske nyvinninger.



New to the Line



Canon uniFLOW Online  
Outstanding Cloud Output Management Solution

**Canon Norge AS**  
Hallagerbakken 110  
Postboks 33 Holmlia  
1201 OSLO  
Tlf. +47 2262 9200  
canon.no

**Canon Inc.**  
Canon.com

**Canon Europe**  
canon-europe.com

Norwegian edition 1.0  
© Canon Europa N.V., 2021