



BESKYTTELSE AF JERES KONTOR

Canon



HVOR SIKRE ER OPLYSNINGERNE PÅ JERES KONTOR?

Virksomheder er i dag i høj grad afhængige af information. De skaber komplekse netværk af tilsluttede teknologier, processer, medarbejdere og virksomheder, som strækker sig ud over landegrænser. Nye og fleksible arbejdsmetoder bliver mere og mere populære, hvilket ændrer kontoret og måden, som medarbejdere opretter, deler og bruger information på. Det er blevet en stor udfordring at sikre data i dette indviklede miljø, og de fleste virksomheder investerer i sofistikerede teknologier som for eksempel effektive firewalls, den nyeste antivirusbeskyttelse, sikkerhedssoftware m.m. Men ofte glemmer de, at deres kontorprintere også bør omfattes af denne beskyttelse, hvilket gør dem mere sårbare, end de selv er klar over.



HAR I KONTROL OVER JERES PRINTERE?

Moderne multifunktionsprintere er blevet effektive værktøjer, der lige som computere og servere har operativsystemer, store harddiske, er tilsluttet netværket og internettet, og som deles af brugere til at håndtere den store mængde af vigtige dokumenter hver dag.



HVAD ER RISICIENE?

- Uautoriserede brugere kan se følsom information, der er gemt på ikke-beskyttede multifunktionsprintere
- Forkert betjening kan gå ud over jeres printinfrastrukturs tilgængelighed
- Ondsindede outsiders kan få adgang til jeres netværk via printeren og bruge den til yderligere angreb
- Fortrolige dokumenter, der er glemt i printerens udbakke efter print, ligger frit tilgængelige
- Sammenblanding af printet materiale, som tilhører forskellige brugere
- Dokumenter, der faxes eller e-mailer til forkerte modtagere som følge af tastefejl
- Printet eller scannet data bliver opsnappet af hackere på vej til modtageren
- Datatab som følge af ubetænksom bortskaffelse af printere, når leasingaftalen er udløbet

"På et kontor, hvor man potentielt skal håndtere enorme mængder af data, kan det virkelig betale sig at indføre grundlæggende standarder for informationssikkerhed. En moderne printer er ikke længere blot en simpel maskine - den er en server, der tilfældigvis også kan printe papir."

(CISO, Publicis Groupe)

SIKRE PRINTLØSNINGER TIL JERES VIRKSOMHED

Designet til sikkerhed og fortrolighed

Når vi designer eller udvælger teknologier, produkter og services for vores kunder, tager vi også den sandsynlige indvirkning på vores kunders informationssikkerhed i betragtning. Derfor er vores multifunktionsprintere til kontoret udstyret med en bred vifte af sikkerhedsfunktioner, både som standard og som tilvalg, så enhver virksomhed – uanset størrelse – kan opnå det ønskede beskyttelsesniveau til:



ENHEDER | NETVÆRK | DOKUMENTER | JERES VIRKSOMHED



INTERNATIONALT ANERKENDTE STANDARDER OG CERTIFIKATER

Vores imageRUNNER ADVANCE-multifunktionsprintere evalueres og certificeres rutinemæssigt ved hjælp af metoden Common Criteria og i overensstemmelse med Hard Copy Device Protection Profile (HCD_PP) eller IEE P2600.2 Protection Profile.



SIKKERHEDSTEST

Canon anvender et af de strengeste sikkerhedstestsystemer i branchen. Teknologierne i vores produktportefølje gennemgår de samme høje teststandarder, som vi kræver i vores egen forretning.

Som brancheførende virksomhed inden for udvikling af innovative print- og Information Management-løsninger til kontorer og virksomheder arbejder Canon tæt sammen med vores kunder for at hjælpe dem med at have en åben tilgang til informationssikkerhed. Denne tilgang tager hensyn til de forskellige sikkerhedspåvirkninger på vores kontorteknologi, der er en del af et større informationsøkosystem.



BESKYT JERES ENHED

Omfattende beskyttelse af jeres fysiske aktiver



BRUGERGODKENDELSE

Beskyt jeres enheder mod uautoriseret brug ved at implementere adgangskontrol gennem brugergodkendelse. Dette giver også den ekstra fordel, at man kan give brugere hurtigere adgang til deres foretrukne indstillinger og printjob, samtidig med at I får et bedre overblik og mere kontrol over printerbrug. Vores afdelingsprintere er udstyret med Universal Login Manager, en fleksibel login-løsning, der muliggør brugergodkendelse mod en brugerdatabase, som findes på enheden, domænegodkendelse vha. Active Directory eller en uniFLOW-server. Dermed kan virksomheder kontrollere adgang til enheden, samtidig med at de får den rette balance mellem brugervenlighed og sikkerhed.



ENHEDSADMINISTRATION

Enhedskonfiguration, som for eksempel netværksindstillinger, er kun tilgængelig for brugere med administratorrettigheder. Dette forhindrer både tilsigtede og utilsigtede ændringer.



FOREBYGGENDE SIKKERHED

imageRUNNER ADVANCE-produkter tilbyder en række sikkerhedsindstillinger, som gør det muligt at beskytte printere mod angreb. Secure Boot-funktionen giver enhedsintegritet, mens Syslog-data viser sikkerhedsstatus for enheden i realtid (data kan læses af et relevant tredjeparts-SIEM-system).



ACCESS MANAGEMENT SYSTEM

Denne løsning giver omfattende kontrol over adgang til enhedens funktioner. Administratorer kan anvende de tilgængelige standardroller eller selv oprette skræddersyede roller med det ønskede niveau af adgangsrettigheder. For eksempel kan visse brugere forhindres i at kopiere dokumenter eller bruge Send-funktionen.



INDSTILLING AF SIKKERHEDSPOLITIK

De nyeste imageRUNNER ADVANCE-multifunktionsprintere er desuden udrustet med en sikkerhedspolitikfunktion, hvormed administratoren kan få adgang til samtlige sikkerhedsrelaterede indstillinger fra én menu og redigere dem, inden politikken bliver håndhævet på maskinen.

Når politikken er indført, skal al brug af enheden og ændringer til indstillinger stemme overens med sikkerhedspolitikken. Sikkerhedspolitikken kan beskyttes med en separat adgangskode, så adgang til dette område er forbeholdt den IT-sikkerhedsansvarlige medarbejder, hvilket giver en endnu højere grad af kontrol og sikkerhed.



BESKYTTELSE AF DATA PÅ ENHEDSLAGRINGSMEDIE

Multifunktionsprinter indeholder generelt store mængder data, der bør beskyttes - fra printjob, der venter på at blive printet, til modtagne faxdokumenter, scannet data, adressebøger, aktivitetslogger og jobhistorik. Canon-enheder har en række muligheder til at beskytte jeres data ved hvert trin i en enheds levetid og sikre datas fortrolighed, integritet og tilgængelighed.

Afhængigt af den specifikke enhedsmodel anvendes enten et harddiskdrev (HDD) eller et solid state-drev (SSD). Da et harddiskdrev anvender en fysisk roterende plade, hvorpå data optages, kræves der et antal overskrivninger, generelt tre, for at sikre, at data effektivt overskrives. I modsætning til et HDD flytter et SSD data rundt på den tilgængelige hukommelsesplads for at sikre, at der er en jævn elektrisk slitage på hukommelsescellerne. Hver celle har kun et begrænset antal skrivninger, og denne "TRIM"-proces maksimerer SSD-levetiden og overskriver samtidig "logisk slettede" data.

imageRUNNER ADVANCE indeholder flere forskellige konfigurationsindstillinger, som kan konfigureres til at angive det punkt, hvor en overskrivning udføres, og overskrivningsmetoden.



HVOR SIKRE ER JERES ENHEDER?

- 1.** Deles jeres enheder, og befinder de sig på offentligt tilgængelige steder?
- 2.** Kan brugere få fri adgang til enhederne?
- 3.** Har I taget forholdsregler for at beskytte information på enhedens harddisk?
- 4.** Kan uautoriserede brugere ændre enhedens indstillinger?
- 5.** Har I tænkt på jeres enheds livscyklus og på sikker bortskaffelse af enheden?

DISKKRYPTERING

Vores imageRUNNER ADVANCE-enheder øger sikkerheden ved at kryptere alt data på harddisken. Den sikkerhedschip, der sørger for datakrypteringen, overholder FIPS 140-2 Level 2-sikkerhedsstandard, som er fastsat af den amerikanske regering, og er certificeret under Cryptographic Module Validation Program (CMVP), der er oprettet af USA og Canada, samt Japans Cryptographic Module Validation Program (JCMVP).

SLETNING AF DATALAGRING

Nogle data, for eksempel kopierede eller scannede billeddata, samt dokumentdata, der er printet fra en computer, gemmes kun midlertidigt på harddisken eller solid state-disken og slettes, når handlingen er udført. For at sikre at der ikke gemmes resterende data, er vores enheder udstyret med funktionalitet, der jævnligt sletter resterende data som en del af jobhåndteringsprocessen.

FORMATÉR ALT DATA OG ALLE INDSTILLINGER

For at undgå at miste data, når I udskifter eller bortskaffer harddisken, kan I overskrive samtlige dokumenter og alt data på harddisken og gendanne maskinen til fabriksindstillingerne.

SPEJLING AF HARDDISK*

Virksomheder kan sikkerhedskopiere data fra en enheds harddisk ved at anvende en ekstra harddisk (tilvalg). Når spejlingen er fuldført, er data på begge harddiske fuldstændigt krypteret.

* Tilvalg. Kontakt jeres Canon-repræsentant for yderligere information om tilgængeligheden af funktionerne og tilvalgene i kontorprinterporteføljen.



BESKYT JERES NETVÆRK



KUNNE JERES PRINTER BRINGE JERES NETVÆRK I FARE?

- Er jeres netværksporte åbne for angreb?
- Kan gæster printe og scanne uden at bringe jeres netværk i fare?
- Er jeres Bring-Your-Own-Device (BYOD)-politikker sikre og håndterbare?
- Bliver printdatastrømmene krypteret på vej fra PC til output-enhed?
- Er print- og scanningsdata sikret undervejs på netværket?

Canon tilbyder en række sikkerhedsløsninger, som beskytter jeres netværk og data mod interne og eksterne angreb.

IP- OG MAC-ADRESSEFILTRERING

Beskyt jeres netværk mod uautoriseret adgang af tredjeparter ved kun at tillade kommunikation med enheder, der har en specifik IP- eller MAC-adresse, for både udadgående og indkommende kommunikation.

KONFIGURATION AF PROXYSERVER

Lad en proxy håndtere al kommunikation på jeres maskines vegne, og brug den til at oprette forbindelse til enheder uden for netværket.

IEEE 802.1X-GODKENDELSE

Uautoriseret netværksadgang blokeres af en LAN-switch, der kun giver adgangsrettigheder til klientenheder, som er godkendt af godkendelsesserveren.

IPSEC-KOMMUNIKATION

IPSec-kommunikation forhindrer tredjeparter i at opfange eller manipulere IP-pakker, der transporteres over IP-netværket.

Anvend TLS-krypteret kommunikation for at forhindre sniffing, spoofing og manipulation af data, der udveksles mellem maskinen og andre enheder som for eksempel computere.

PORTKONTROL

Konfigurér porte som en del af jeres sikkerhedspolitikindstilling.

AUTOMATISK CERTIFIKATVEDLIGEHOLDELSE

Med denne funktion bliver besværet med at vedligeholde sikkerhedscertifikater væsentligt mindsket. Ved hjælp af en brancheanerkendt teknologi kan en systemadministrator automatisk opdatere og frigive certifikater, hvilket sikrer, at sikkerhedspolitikkerne altid opfyldes.

OVERVÅGNINGSLOGS

Forskellige logs giver jer mulighed for at overvåge aktiviteten på jeres enhed, herunder blokerede kommunikationsanmodninger.

WI-FI DIRECT

Aktivér P2P (peer-to-peer)-tilslutning for mobilt print, uden at den mobile enhed behøver have adgang til jeres netværk.

KRYPTERING AF DATA MELLEML ENHEDER

Denne funktion krypterer printjob på deres vej fra brugerens PC til multifunktionsprinter. Ved at aktivere Universal Security Feature Set kan scannet data i PDF-format også krypteres.

MOBILT GÆSTEPRINT

Vores administrationssoftware til sikker netværksprint og -scanning håndterer almindelige sikkerhedsrisici for mobilt og gæsteprint ved at levere eksterne jobafsendelsesstier via e-mail, web og mobil-app. Dette minimerer angrebsvektorer ved at låse multifunktionsprinter til en sikker kilde.



BESKYT JERES DOKUMENTER

Enhver virksomhed håndterer fortrolige dokumenter som kontrakter, lønsedler, kundedata, forsknings- og forretningsplaner m.m. Hvis dokumenter skulle falde i de forkerte hænder, kan det medføre alt fra et beskadiget omdømme til store bøder eller endda retssager.

Canon tilbyder en række sikkerhedsløsninger, som beskytter jeres følsomme dokumenter igennem hele deres livscyklus.



BESKYTTELSE AF PRINTEDE DOKUMENTER

Sikkert print

Brugeren kan angive en pinkode til print, så dokumentet først kan printes, når den korrekte pinkode er indtastet på maskinen. Dermed kan enkelte brugere sikre de dokumenter, som de betragter som fortrolige.

Tilbagehold alle printjob

For at beskytte fortroligheden af alt printet materiale kan administratorer gennemtvinge en tilbageholdelse af samtlige afsendte printjob på imageRUNNER ADVANCE-enheder, så brugere først skal logge ind, før de kan printe deres printjob.

Mailbokse

Printjob eller scannede dokumenter kan gemmes i en mailboks, så de kan hentes på et senere tidspunkt. Mailbokse kan beskyttes med en pinkode for at sikre, at kun den specifikke ejer kan se indholdet, der er gemt i mailboksen. Denne sikrede plads på maskinen er velegnet til at gemme dokumenter, der skal printes/scannes ofte (som for eksempel formularer), men som kræver varsom håndtering.

uniFLOW sikkert print*

Med uniFLOW MyPrintAnywhere sikkert print kan brugere sende printjob via den almindelige driver og hente dem fra hvilken som helst printer på netværket.



FRARÅD ELLER FORHINDR KOPIERING AF DOKUMENTER

Print med synlige vandmærker

Driverne kan printe synlige mærker på en side, enten lagt hen over eller bag om dokumentets indhold. Dette forhindrer kopiering, eftersom brugeren bliver gjort opmærksom på et dokumentets fortrolighed.

Print/kopiér med usynlige vandmærker

Når denne funktion er aktiveret, kan dokumenter printes eller kopieres med indlejret skjult tekst i baggrunden. Når dokumentet duplikeres, bliver teksten synlig, hvilket virker som et afskrækkelsesmiddel.

HVOR SIKRE ER JERES DOKUMENTER?

- 1.** Bliver uautoriserede brugere forhindret i at få adgang til følsomme dokumenter ved printeren?
- 2.** Kan I sikre fortroligheden af samtlige brugeres dokumenter, der kommer forbi den delte enhed?
- 3.** Kunne nogen bare gå forbi en af jeres printere og samle fortrolige dokumenter op?
- 4.** Kan I forhindre almindelige fejl, når I sender dokumenter fra enheden?



UDØV KONTROL OVER AFSENDELSE OG FAX AF DOKUMENTER

Begræns antallet af modtagere

For at mindske risikoen for informationslæk kan administratorer begrænse antallet af tilgængelige modtagere til kun at omfatte dem, der er gemt i adressebogen eller på LDAP-serveren, til den indloggede brugers adresse eller til bestemte domæner.

Deaktiver automatisk udfyldelse af adresser

Undgå at dokumenter bliver sendt til de forkerte modtagere ved at slå automatisk fuldførelse af e-mailadresser fra.

Beskyttelse af adressebog

Angiv en pinkode for at beskytte enhedens adressebog mod ikke-godkendte ændringer af brugere.

Bekræftelse af faxnummer

Sørg for, at dokumenter ikke bliver sendt til forkerte modtagere ved at kræve, at brugere bekræfter faxnummeret, inden de sender dokumenterne.

Fortrolighed for modtagne faxdokumenter

Indstil maskinen til at gemme dokumenter i hukommelsen, uden at de bliver printet. I kan også beskytte modtagne faxdokumenter ved at angive, om et faxdokument skal gemmes i en fortrolig indbakke eller ved at angive pinkoder.



BEKRÆFT DOKUMENTERS OPRINDELSE OG ÆGTHED MED DIGITALE SIGNATURER

EnhedsSignatur

EnhedsSignaturer kan anvendes på scannede dokumenter i PDF- eller XPS-format ved hjælp af en nøgle- og certifikatmekanisme, så modtageren kan bekræfte både dokumentets oprindelse og ægthed.

Brugersignatur*

Denne funktion sætter brugere i stand til at sende en PDF- eller XPS-fil med en unik, digital brugersignatur, der er udstedt af en certifikatmyndighed. På den måde kan modtageren kontrollere, hvilken bruger der har signeret filen.

* Tilvalg. Kontakt jeres Canon-repræsentant for yderligere information om tilgængeligheden af funktionerne og tilvalgene i kontorprinterporteføljen.



INFORMATIONSSIKKERHED I VIRKSOMHEDEN

Canon kan bidrage til den overordnede beskyttelse af informationen i jeres virksomhed.



FULD KONTROL OVER ALLE CAPTURE- OG OUTPUTBEHOV

Ved hjælp af vores modulopbyggede output management-software kan virksomheder få glæde af sikker deling af netværksenheder. Dermed kan de printe sikkert fra en hvilken som helst printer, der er tilsluttet output management-serveren. Mobile brugere understøttes af en centralt styret service, hvor både interne brugere og gæsteburgere kan printe sikkert fra mobile enheder. Scanningsmodulet giver virksomheder mulighed for at registrere, komprimere, konvertere og distribuere dokumenter fra multifunktionsprinteren til en lang række destinationer, herunder cloud-baserede systemer. I kan også omdirigere printjob til den mest passende printer, hvilket er med til at optimere printomkostningerne for hvert dokument.

Vores løsning forbedrer dokumentetsikkerheden på tværs af jeres virksomhed, og sammen med et komplet dokumentregnskab får I fuldt overblik over aktivitet pr. bruger, enhed og afdeling.



CENTRALISERET FLÅDEADMINISTRATION

Vores enhedsadministrationssoftware IW MC giver jer ikke alene mulighed for at håndtere enhedsindstillinger, sikkerhedspolitikker, adgangskoder og certifikater, men også for at opdatere firmware og implementere det på samtlige Canon-enheder på netværket. Dette sparer jeres IT-team for dyrebar tid og er med til at holde sikkerheden af jeres printinfrastruktur opdateret.



MANAGED PRINT SERVICES

Canon MPS kombinerer innovativ teknologi og software med de rette services for at give jer den ønskede print- og dokumentoplevelse uden det dermed forbundne besvær for jeres IT-team. Gennem proaktiv håndtering og løbende optimering af jeres printinfrastruktur og dokumentworkflows kan vi hjælpe jer med at opnå jeres sikkerhedsmål, samtidig med at omkostningerne optimeres og produktiviteten øges i hele virksomheden.

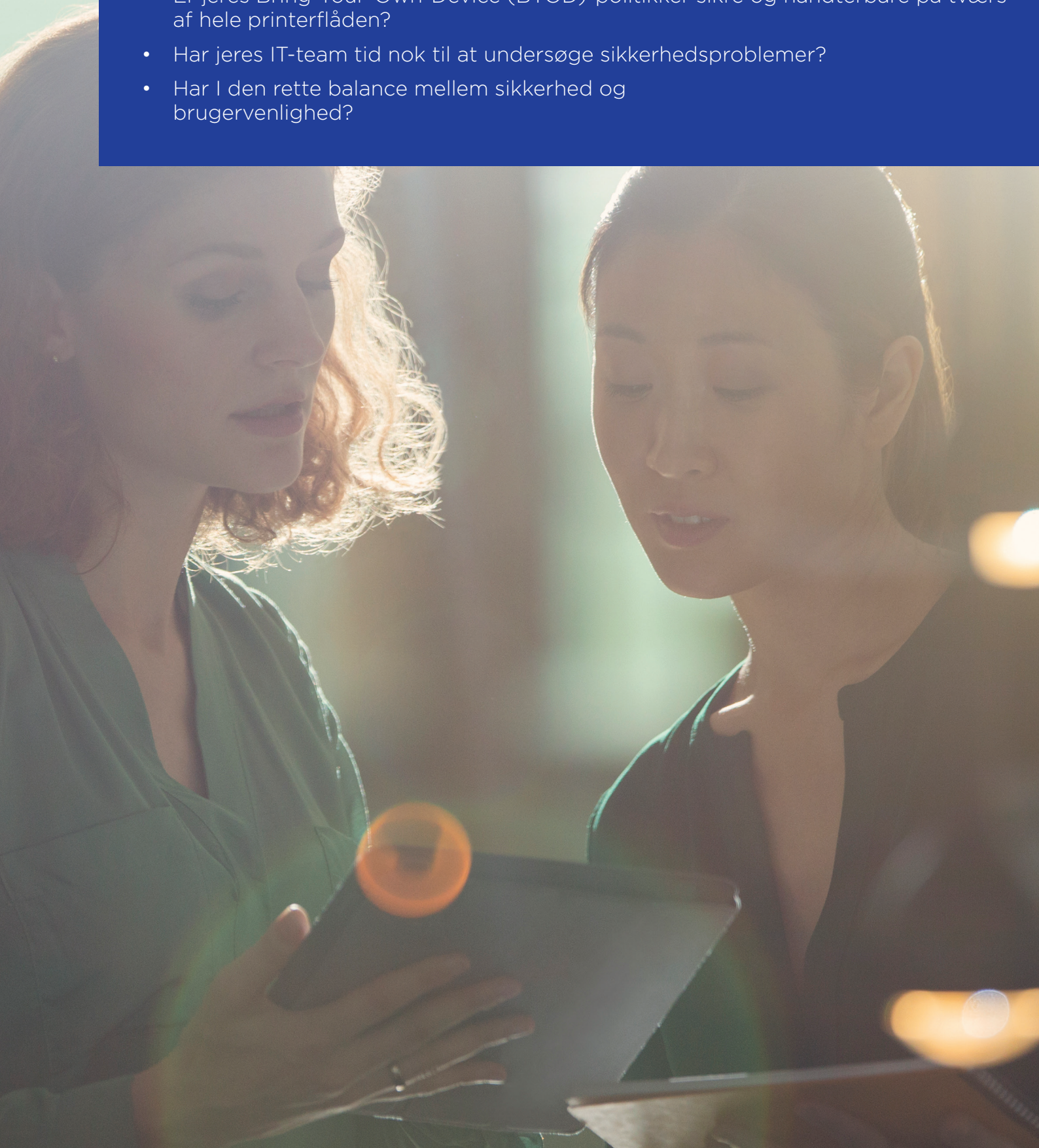


BRUGERTILPASSET DESIGN

Vi har et team af interne programmører, som kan foreslå og udvikle en brugertilpasset løsning, der passer til jeres specifikke situation eller unikke behov.

HVAD DÆKKER SIKKERHEDEN I JERES VIRKSOMHED OVER?

- Er jeres flåde af multifunktionsprintere også omfattet af jeres sikkerhedspolitik?
- Hvordan sikrer I, at jeres printinfrastruktur er opdateret, og at opgraderinger og fejlretninger implementeres rettidigt og effektivt?
- Kan gæster printe og scanne uden at bringe jeres netværk i fare?
- Er jeres Bring-Your-Own-Device (BYOD)-politikker sikre og håndterbare på tværs af hele printerflåden?
- Har jeres IT-team tid nok til at undersøge sikkerhedsproblemer?
- Har I den rette balance mellem sikkerhed og brugervenlighed?



HVORFOR CANON?

Canon er imaging. Vi bruger imaging-teknologier til at gøre en forskel og skabe ændringer.

Dette er til stor fordel for vores kunder, når de gennemfører den digitale transformation og arbejder på nye måder. Vi ønsker at skabe store samfundsmæssige forandringer ved løbende at fokusere på bæredygtighed som en del af vores virksomhedsarv og -kultur.

Derudover forandrer vi os, efterhånden som vi investerer i nye markeder, produkter og teknologier. Vi kommer til at være her på den lange bane til gavn for alle – vores kunder, vores medarbejdere og samfundet i bred forstand.

Canon er bygget på 4 grundpiller:



SIKKERHED

Canons løsninger og services hjælper med at sikre alle dokumenter og følsomme data i hele dokumentets levetid, uanset om de er i papirformat eller digitalt format. Løsningerne og servicerne er sikre gennem design, og de er udviklet med udgangspunkt i sikkerhed.



BÆREDYGTIGHED

Canon har tilpasset sin praksis for bæredygtighed til FN's mål for bæredygtig udvikling (SDG'er), f.eks. tilsagn om at reducere CO2-udledninger i hele produktets livscyklus ved at reducere mængden af emballage og konsolidere distributionscentre.

Alle disse elementer gør Canon til den rigtige partner for jer.



SUPPORT

En mangfoldig portefølje af services, der sikrer høj kvalitet og resulterer i kundetilfredshed. Intern ekspertise, der arbejder på at øge effektiviteten og frigøre potentialet for vores kunder.



INNOVATION

En lang historie med billedstyret innovation og levering af banebrydende teknologi i mere end 80 år. Førende i branchen med et stærkt engagement i den fremtidige udvikling inden for teknologi.



New to the Line



Canon uniFLOW Online
Outstanding Cloud Output Management Solution

Canon Danmark
Knud Højgaards Vej 1
2860 Søborg
Tlf.: 70 15 50 05
canon.dk

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

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