BEVEILIG UW KANTOOROMGEVING

McAfee PROTECTED

COPIER MFP LINE OF THE YEAR 2018 BLI BUYERS LAB LINE OF THE YEAR

COPIER MFP LINE OF THE YEAR 2020 BLI BUYERS LAB LINE OF THE YEAR
New to the Line

BLI BUYERS LAB 2019 PICK
Canon uniFLOW Online
Outstanding Cloud Output Management Solution

Canon

See the bigger picture

HOE VEILIG IS INFORMATIE IN UW ORGANISATIE?

Vandaag de dag zijn organisaties sterk aangewezen op informatie. Informatie die rondgaat in complexe netwerken van connected technologie, processen, mensen en systemen die verder reiken dan de nationale grenzen. Het beveiligen van gegevens in deze complexe omgeving is - meer dan ooit - een enorme uitdaging. De meeste organisaties investeren dan ook fors in geavanceerde technologieën zoals robuuste firewalls en de nieuwste antivirus- en beveiligingssoftware. Bedrijven zien echter vaak niet in dat ze die beveiliging óók moeten toepassen op hun kantoorprinters en dat brengt risico's met zich mee. Wat doet ú om uw kostbare informatie te beschermen?

DENK AAN UW PRINTERS

Moderne multifunctionele printers (MFP's) zijn uitgegroeid tot krachtige hulpmiddelen die net als pc's en servers beschikken over besturingssystemen en grote harde schijven, verbonden zijn met het netwerk en internet, en dagelijks door gebruikers worden gedeeld voor het verwerken van enorme aantallen bedrijfskritische documenten.

WAT ZIJN DE RISICO'S?

- Onbevoegde gebruikers hebben toegang tot gevoelige informatie die is opgeslagen op niet-beveiligde MFP's.
- De beschikbaarheid van uw printinfrastructuur wordt in gevaar gebracht door onjuist gebruik.
- Buitenstaanders met slechte bedoelingen krijgen toegang tot uw netwerk via de printer en kunnen die gebruiken voor verdere aanvallen.
- Uitlekken van vertrouwelijke documenten die na het printen in de uitvoerlade zijn blijven liggen.
- Geprinte documenten van verschillende gebruikers raken door elkaar.
- Documenten die per fax of e-mail worden verzonden, komen vanwege typefouten bij de verkeerde personen terecht.
- Print- of scangegevens worden tijdens het verzenden onderschept door hackers.
- Gegevens die verloren gaan vanwege de onvoorzichtige verwijdering van printers nadat het contract ervan is verlopen.

"Het toepassen van basisstandaarden voor gegevensbeveiliging is de moeite zeker waard voor kantoren waar mogelijk enorme hoeveelheden gegevens worden verwerkt. Een printer is tegenwoordig geen domme machine meer, maar een server die toevallig ook nog op papier kan printen."

(CISO, Publicis Groupe)

VEILIGE PRINTOPLOSSINGEN VOOR UW ORGANISATIE

ONTWORPEN MET HET OOG OP BEVEILIGING EN PRIVACY

Wanneer we technologieën, producten en services voor onze klanten ontwerpen of kiezen, denken we na over de mogelijke gegevensbeveiligingsimpact hiervan op de omgeving van onze klant. Onze multifunctionele kantoorprinters beschikken daarom over een groot aantal standaard en optionele beveiligingsfuncties waarmee organisaties van elke omvang beschikken over de gewenste mate van beveiliging voor:

APPARATEN | NETWERKEN | DOCUMENTEN | UW ORGANISATIE

INTERNATIONAAL ERKENDE STANDAARDEN EN CERTIFICERINGEN

Onze multifunctionele printers uit de imageRUNNER ADVANCE-serie worden regelmatig geëvalueerd en gecertificeerd op basis van de Common Criteria methodologie en conform de vereisten van de IEEE2600-standaard voor de beveiliging van printapparatuur.

BEVEILIGINGSTESTEN

Canon hanteert een van de strengste regimes voor beveiligingstesten in de kantoormachine-industrie. De technologieën die worden gebruikt in ons productportfolio, worden getest volgens dezelfde hoge standaarden die we verwachten voor ons eigen bedrijf.

Als marktleider op het gebied van de ontwikkeling van innovatieve oplossingen voor print en informatiebeheer voor kantoren en bedrijven, werkt Canon samen met klanten om hen te helpen een inclusieve benadering van gegevensbeveiliging te hanteren. Deze aanpak houdt rekening met de beveiligingsconsequenties van onze technologie als onderdeel van hun bredere informatie-ecosysteem.

BESCHERM UW SYSTEMEN

UITGEBREIDE BESCHERMING VAN FYSIEKE MIDDELEN

OPLOSSINGEN VOOR GEBRUIKERSAUTHENTICATIE

Bescherm uw apparatuur tegen onbevoegd gebruik door gebruikerstoegang te beheren via authenticatie. Een bijkomend voordeel hiervan is dat gebruikers sneller toegang hebben tot hun voorkeursinstellingen en printopdrachten, terwijl registratie en controle beter zijn. Onze afdelingsprinters zijn voorzien van uniFLOW Online Express, een flexibele oplossing waarmee gebruikersauthenticatie plaatsvindt op basis van een gebruikersdatabase die op het apparaat is gemaakt, en domeinauthenticatie via een Active Directory- of uniFLOW-server. Op die manier kunnen organisaties de toegang tot apparaten beheren en de juiste balans vinden tussen gebruiksgemak en beveiliging.

MANAGEN VAN CONFIGURATIES

Configureren van apparaten, zoals netwerkinstellingen en andere beheeropties, kan alleen worden uitgevoerd door gebruikers die beschikken over beheerdersbevoegdheden, zodat opzettelijke of onbedoelde wijzigingen worden voorkomen.

MANAGEN VAN TOEGANG

Deze functionaliteit biedt gedetailleerde controle over de toegang tot apparaatfuncties. Beheerders kunnen gebruikmaken van de profielen die standaard beschikbaar zijn of specifieke profielen instellen, met het gewenste niveau aan toegangsrechten. Zo kan worden ingesteld dat bepaalde gebruikers geen kopieën kunnen maken van documenten of de verzendfunctie niet kunnen gebruiken.

DOORVOEREN BEVEILIGINGSBELEID

De nieuwste imageRUNNER ADVANCE DX-apparaten beschikken eveneens over een beveiligingsbeleidsfunctie, waarmee de beheerder in één menu toegang heeft tot alle beveiligingsfuncties en deze kan bewerken alvorens ze af te dwingen op het apparaat. Na de ingebruikname moeten het gebruik van het apparaat en wijzigingen in de instellingen voldoen aan het beleid. De instellingen kunnen worden beschermd met een apart wachtwoord, zodat toegang tot dit gebied beperkt is tot de verantwoordelijke IT-beveiligingsmedewerker waarmee een extra beheer- en veiligheidslaag wordt toegevoegd.

BESCHERMING VAN GEGEVENS OP DE HARDE SCHIJF

Multifunctionele printers kunnen grote hoeveelheden gegevens bevatten die beschermd moeten worden, van printopdrachten in de wachtrij tot ontvangen faxberichten, en van gescande gegevens, adresboeken en activiteitenlogboeken tot opdrachtengeschiedenis. De apparaten van Canon bieden verschillende functies waarmee uw gegevens in elke fase van de levensduur van het apparaat worden beschermd, en de vertrouwelijkheid, integriteit en beschikbaarheid ervan worden gewaarborgd.

PREVENTIEVE BEVEILIGING

imageRUNNER ADVANCE DX-apparaten bieden een aantal beveiligingsinstellingen waarmee printers tegen aanvallen kunnen worden beveiligd. De functie Beveiligd opstarten zorgt voor integriteit van het apparaat terwijl Mc Afee Embedded Control de integriteit garandeert gedurende de levensduur van het apparaat. Dit voorkomt dat programma's worden gemanipuleerd of dat er niet-geautoriseerde programma's worden uitgevoerd tijdens runtime. Daarnaast bieden Syslog-gegevens realtime beveiliging van het apparaat (gegevens kunnen gelezen worden door een geschikt SIEM-systeem van derden).

HOE VEILIG ZIJN UW APPARATEN?

1	2	3	4	5
Worden uw systemen gedeeld en bevinden ze zich in openbare ruimten?	Kunnen gebruikers onbeveiligde toegang tot apparaten krijgen?	Hebt u maatregelen geïmplementeerd om de informatie op de harde schijf van het apparaat te beschermen?	Kunnen onbevoegde gebruikers wijzigingen aanbrengen in apparaat-instellingen?	Hebt u nagedacht over de levenscyclus en veilige verwijdering van uw apparaat?

VERSLEUTELING VAN DE HARDE SCHIJF

Onze imageRUNNER ADVANCE DX-apparaten versleutelen alle gegevens op de harde schijf en verbeteren daarmee de beveiliging. De beveiligings-chip die verantwoordelijk is voor gegevensversleuteling voldoet aan de FIPS 140-2 Level 2-beveiligingsnorm van de Amerikaanss overheid en is gecertificeerd in het kader van het Cryptographic Module Validation Program (CMVP) dat is opgezet door de V.S. en Canada en het Japan Cryptographic Module Validation Program (JCMVP).

GEGEVENS VAN DE HARDE SCHIJF VERWIJDEREN

Bepaalde gegevens, zoals gekopieerde of gescande afbeeldingsgegevens en documentgegevens die zijn geprint vanaf een computer, worden alleen tijdelijk op de harde schijf opgeslagen en worden verwijderd wanneer de bewerking is voltooid. Om te voorkomen dat er overbodige gegevens behouden blijven, beschikken onze apparaten over een functie waarmee routinematig de overbodige gegevens van de harde schijf worden verwijderd als onderdeel van de verwerking van opdrachten.

ALLE GEGEVENS EN INSTELLINGEN INITIALISEREN

U kunt gegevensverlies bij het vervangen of weggooien van de harde schijf voorkomen door alle documenten en gegevens op de harde schijf te overschrijven en de fabrieksinstellingen van het apparaat te herstellen.

HARDE SCHIJF SPIEGELEN*

Organisaties kunnen een back-up maken van de gegevens op de harde schijf van hun apparaat met behulp van een extra, optionele harde schijf. Tijdens het kopiëren worden de gegevens op beide harde schijven volledig versleuteld.

REMOVABLE HDD*

Met deze optie kunt u de harde schijf uit het apparaat halen en deze veilig opbergen als het apparaat niet in gebruik is.

*Optioneel. Voor nadere informatie over de beschikbaarheid van de functies en opties in het volledige portfolio van kantoorsystemen neemt u contact op met uw Canon-vertegenwoordiger.

BEVEILIG UW NETWERK

BRENGT UW PRINTER UW NETWERK IN GEVAAR?

- Zijn netwerkpoorten kwetsbaar voor aanvallen?
- Kunnen gastgebruikers printen en scannen zonder dat ze uw netwerk blootstellen aan risico's?
- Is uw Bring Your Own Device-beleid veilig en beheersbaar?
- Zijn printgegevens versleuteld van pc tot uitvoerapparaat?
- Zijn print- en scangegevens beveiligd tijdens het verzenden?

CANON BIEDT EEN REEKS BEVEILIGINGSOPLOSSINGEN WAARMEE U UW NETWERK EN GEGEVENS BESCHERMT TEGEN INTERNE EN EXTERNE AANVALLEN.

IP- EN MAC-ADRES FILTERING
Bescherm uw netwerk tegen onbevoegde toegang door derden door alleen communicatie toe te staan met apparaten met een specifiek IP- of MAC-adres voor inkomende en uitgaande communicatie.

CONFIGURATIE VAN PROXYSERVER
Stel een proxy in die in plaats van uw apparaat communiceert en gebruik deze bij het maken van verbinding met apparaten buiten het netwerk.

IEEE 802.1X-AUTHENTICATIE
Onbevoegde netwerktoegang wordt geblokkeerd door een LAN-schakelaar die alleen toegangsrechten verleent aan clientapparaten die zijn geautoriseerd door de verificatieserver

IPSEC-COMMUNICATIE
IPSec-communicatie voorkomt dat derden IP-pakketten die via een IP-netwerk worden verzonden, onderscheppen of manipuleren.
Gebruik TLS versleutelde communicatie ter preventie van sniffing, spoofing en tampering, met gegevens die worden uitgewisseld tussen het apparaat en andere apparaten, zoals computers.

BEHEER VAN POORTEN
Configureer poorten als onderdeel van uw beveiligingsbeleid.

AUTOMATISCHE INSCHRIJVING CERTIFICEREN
Met deze functie wordt het lastige onderhoud van beveiligingscertificaten drastisch verminderd. Met behulp van erkende technologie kan een systeembeheerder certificaten automatisch bijwerken en vrijgeven, zodat er altijd aan het beveiligingsbeleid wordt voldaan.

MONITORING VAN ACTIVITEITEN
U kunt verschillende logboeken gebruiken om activiteit rond uw apparaat te volgen, met inbegrip van geblokkeerde communicatie-aanvragen.

WI-FI DIRECT
Maak peer-to-peer-verbinding mogelijk voor mobiel printen zonder dat het mobiele apparaat toegang tot het netwerk hoeft te hebben.

VERSLEUTELING VAN GEGEVENS TIJDENS VERZENDING NAAR EN VANAF HET APPARAAT
Met deze optie worden printopdrachten versleuteld tijdens het verzenden van de pc van de gebruiker naar de multifunctionele printer. Door de universal send security feature set in te schakelen, kunt u scangegevens in PDF-formaat eveneens laten versleutelen.

MOBIEL PRINTEN DOOR GASTGEBRUIKERS
Onze software voor veilig netwerkprinten en -scannen houdt rekening met voorkomende beveiligingsrisico's op het gebied van mobiel printen en printen door gastgebruikers. De software maakt het mogelijk om externe printopdrachten via e-mail, internet en mobiele apps aan te bieden. Hiermee worden aanvalsvectoren tot het minimum beperkt door het MFD te koppelen aan een veilige bron.

*Beschikbaarheid verschilt per regio/land. Neem voor meer informatie contact op met uw Canon-vertegenwoordiger.

BESCHERM UW DOCUMENTEN

Iedere organisatie heeft te maken met gevoelige documenten zoals contracten, salarisgegevens, klantgegevens, research- en ontwikkelingsplannen enz. Wanneer documenten in verkeerde handen vallen kunnen de gevolgen uiteenlopen van imagoschade tot hoge boetes en zelfs rechtszaken.

Canon biedt een reeks beveiligingsoplossingen waarmee u uw gevoelige documenten gedurende hun volledige levenscyclus kunt beschermen.

VERTROUWELIJKHEID VAN GEPRINTE DOCUMENTEN

Beveiligd printen
De gebruiker kan een pincode instellen voor printen, zodat het document pas kan worden geprint nadat de juiste pincode is ingevoerd op het apparaat. Op die manier kunnen medewerkers de documenten beveiligen die zij als vertrouwelijk beschouwen.

Vasthouden van printopdrachten
Met imageRUNNER ADVANCE kan de beheerder alle verzonden printopdrachten in een wachtrij plaatsen, zodat gebruikers zich moeten aanmelden voordat ze hun opdrachten kunnen printen en de vertrouwelijkheid van al het geprinte materiaal wordt gewaarborgd.

Mailbox printen & scannen
Printopdrachten of gescande documenten kunnen worden opgeslagen in een mailbox zodat hier later toegang toe kan worden verkregen. Mailboxen kunnen worden beveiligd met een pincode om ervoor te zorgen dat alleen de eigenaar aan wie de pincode is toegekend de inhoud van het postvak kan bekijken. Deze veilige omgeving op het apparaat is eveneens geschikt voor het opslaan van documenten die vaak moeten worden geprint (zoals formulieren), maar waarmee voorzichtig moet worden omgegaan.

Beveiligd printen met uniFLOW*
Met beveiligd printen met uniFLOW MyPrintAnywhere kunnen gebruikers printopdrachten indienen via het universele stuurprogramma en ze bij elke printer in het netwerk ophalen.

ONTMOEDIG EN VOORKOM HET DUPLICEREN VAN DOCUMENTEN

Print met zichtbare watermerken
De stuurprogramma's kunnen zichtbare markeringen op de pagina's printen, over de inhoud van het document heen of erachter. Hiermee wordt het kopiëren van het document ontmoedigd omdat de gebruiker bewust wordt gemaakt van de vertrouwelijkheid van het document.

Print/kopieer met onzichtbare watermerken
Als deze optie is ingeschakeld, kunnen documenten worden geprint of gekopieerd met ingesloten verborgen tekst op de achtergrond. Als het document vervolgens wordt gekopieerd, verschijnt de tekst in het document. Dit heeft een ontmoedigend effect.

Preventie van gegevensverlies op bedrijfsniveau*
Upgrade uw basismogelijkheden voor het voorkomen van gegevensverlies naar iW SAM Express in combinatie met uniFLOW. Met deze server-gebaseerde oplossing kunt u documenten die naar en van de printer zijn verzonden, vastleggen en archiveren, analyseren en interpreteren met behulp van tekst of attributen, met als uiteindelijke doel om bedreigingen van de beveiliging aan te pakken.

Achterhalen van de oorsprong van documenten*
Via ingesloten code kan de oorsprong van een document worden getraceerd naar de bron.

*Optioneel. Voor nadere informatie over de beschikbaarheid van de functies en opties in het volledige portfolio voor kantoorprinters neemt u contact op met uw Canon-vertegenwoordiger.

HOE VEILIG ZIJN UW DOCUMENTEN?

1	2	3	4	5
Wordt voorkomen dat onbevoegde gebruikers toegang krijgen tot gevoelige documenten op de printer?	Kunt u de vertrouwelijkheid waarborgen van alle documenten van alle gebruikers die via het gedeelde apparaat worden verwerkt?	Kunt u de oorsprong van geprinte documenten traceren?	Kan iemand gevoelige documenten van uw printer meenemen?	Kunt u veel gemaakte fouten bij het verzenden van documenten vanaf het apparaat voorkomen?

KRIJG GRIP OP HET VERZENDEN EN FAXEN VAN DOCUMENTEN

Beperk bestemmingen voor verzending
Beheerders kunnen het risico van informatielekken verminderen door de beschikbare verzendbestemmingen te beperken tot die in het adresboek of op de LDAP-server, het adres van de aangemelde gebruiker of bepaalde domeinen.

Schakel automatisch aanvullen van adressen uit
Voorkom dat documenten naar verkeerde bestemmingen worden verzonden door het automatisch aanvullen van e-mailadressen uit te schakelen.

Adresboekbeveiliging
Stel een pincode in om het adresboek op het apparaat te beschermen tegen onbevoegde bewerking door gebruikers.

Faxnummer-bevestiging
Voorkom dat documenten naar onbedoelde ontvangers worden verzonden door in te stellen dat gebruikers het faxnummer ter bevestiging een tweede keer moeten invoeren voordat ze documenten kunnen verzenden.

Vertrouwelijkheid voor ontvangen faxdocumenten
Stel het apparaat zo in dat documenten in het geheugen worden opgeslagen zonder dat ze worden afgedrukt. U kunt de vertrouwelijkheid van ontvangen faxdocumenten ook beschermen door voorwaarden te stellen aan de opslaglocatie voor een vertrouwelijk postvak en door pincodes in te stellen.

DATA REMOVAL SERVICE*

Een uitgebreide service voor het verwijderen van fysieke en digitale gegevens uit uw buiten gebruik gestelde Canon-printers en multifunctionele apparaten, waarmee het risico van potentieel gegevensverlies tot het minimum wordt beperkt.

VERIFIEER DE OORSPRONG EN ECHTHEID VAN DOCUMENTEN DOOR DIGITALE HANDTEKENINGEN

Apparaathandtekening
Een apparaathandtekening kan worden toegepast op gescande PDF- of XPS-documenten op basis van een sleutel- en certificaatmechanisme, zodat de ontvanger de oorsprong en echtheid van het document kan controleren.

Gebruikershandtekening*
Met deze optie kunnen gebruikers een PDF- of XPS-bestand verzenden met een unieke digitale handtekening die wordt verkregen via een certificeringsinstantie. Op die manier kan de ontvanger controleren van welke gebruiker de handtekening afkomstig is.

VOER BELEID UIT MET ADOBE LIVECYCLE MANAGEMENT ES-INTEGRATIE

Gebruikers kunnen PDF-bestanden beveiligen en permanente en dynamische beleidsregels toepassen om toegangs- en gebruiksrechten te managen met het oog op de bescherming van gevoelige en waardevolle informatie tegen onbedoelde of opzettelijke publicatie. Beveiligingsbeleidsregels worden onderhouden op serverniveau, zodat rechten gewijzigd kunnen worden, zelfs nadat een bestand is verspreid. De producten uit de imageRUNNER ADVANCE DX-serie kunnen worden geconfigureerd voor Adobe® ES-integratie.

*Beschikbaarheid verschilt per regio/land. Neem voor meer informatie contact op met uw Canon-vertegenwoordiger.

GEGEVENSBEVEILIGING VOOR ORGANISATIES

CANON KAN EEN BIJDRAGE LEVEREN AAN DE ALGEHELE INFORMATIEBESCHERMING IN UW ORGANISATIE.

COMPLETE CONTROLE VOOR UW END-TO-END SCAN- EN UITVOERBEHOEFTEN

Met onze modulaire scan- en outputmanagementsoftware kunnen organisaties apparaten op een veilige manier delen en opdrachten veilig printen op elke printer die is verbonden met de outputmanagement-server. Mobiele gebruikers worden ondersteund door een centraal beheerde service, waarmee zowel interne gebruikers als gastgebruikers veilig kunnen printen vanaf mobiele apparaten.

Voor de digitaliseringsbehoeften van organisaties biedt de scanmodule functies voor het scannen, comprimeren, omzetten en verspreiden van documenten vanaf het multifunctionele apparaat naar een groot aantal verschillende bestemmingen, waaronder cloudoplossingen. Daarnaast kunt u printopdrachten veilig omleiden naar de meest geschikte printer en zo de printkosten voor elk document optimaliseren.

Onze oplossing verbetert niet alleen de beveiliging van documenten in organisaties, maar zorgt ook voor een volledige registratie zodat u beschikt over een compleet overzicht van de activiteiten per gebruiker, apparaat en afdeling.

GECENTRALISEERD FLEET MANAGEMENT

Met onze Device Management software iW MC kunnen apparaatinstellingen, Security Policies, wachtwoorden, certificaten en firmware worden bijgewerkt en geïmplementeerd op alle Canon-apparaten in het netwerk.
Dit betekent dat uw IT-team kostbare tijd bespaart en dat de beveiliging van uw printinfrastructuur altijd up-to-date is.

UITGEBREIDE AUDIT MOGELIJKHEDEN

Onze oplossingen kunnen worden uitgebreid met apart te bestellen opties voor het vastleggen van complete records (d.w.z. scan- en opdrachtmetagegevens) van ieder document dat via imageRUNNER ADVANCE DX-apparaten worden verwerkt.

DATA LOSS PREVENTION-INTEGRATIE*

Met Canon kunt u niet alleen uw Data Loss Prevention-strategie uitbreiden naar uw printnetwerk, maar beschikt u ook over cruciale registratie van alle print-, kopieer- en scangegevens.

MANAGED PRINT SERVICES

Canon MPS combineert innovatieve technologie en software met de juiste services, zodat u de gewenste print- en documentdienstverlening heeft zonder rompslomp voor uw IT-teams. Dankzij proactief beheer en voortdurende optimalisatie van uw print-infrastructuur en documentworkflows, kunnen wij u helpen uw beveiligingsdoelstellingen te bereiken en tegelijkertijd de kosten te beheersen en de productiviteit te verhogen in uw hele bedrijf.

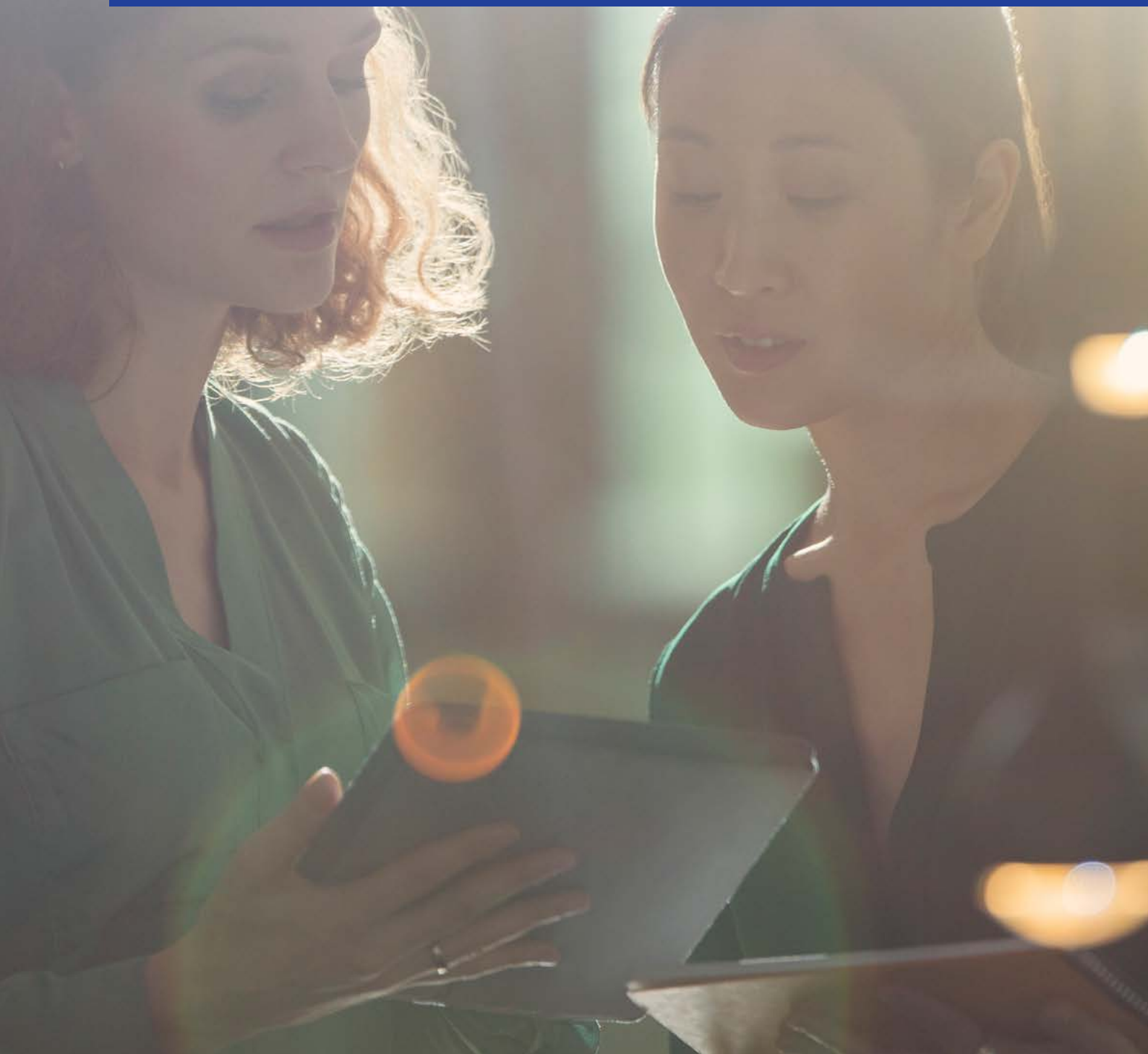
MAATWERKOPLOSSINGEN

Ons team van interne ontwikkelaars kan een op maat gemaakte oplossing ontwerpen en ontwikkelen die precies aansluit op uw specifieke situatie of unieke behoeften.

*Beschikbaarheid verschilt per regio/land. Neem voor meer informatie contact op met uw Canon-vertegenwoordiger.

HOE INCLUSIEF IS DE BEVEILIGINGSAANPAK VAN UW ORGANISATIE?

- Is uw beveiligingsbeleid ook van toepassing op uw multifunctionele apparaten?
- Hoe zorgt u ervoor dat uw print-infrastructuur up-to-date is en dat aanpassingen en bug fixes tijdig en efficiënt worden geïmplementeerd?
- Kunnen gastgebruikers printen en scannen zonder dat ze uw netwerk blootstellen aan risico's?
- Is uw 'Bring Your Own Device'-beleid veilig en wordt het ondersteund door uw print-infrastructuur?
- Heeft uw IT-team voldoende tijd om beveiligingskwesties te onderzoeken?
- Heeft uw organisatie de juiste balans tussen beveiliging en gebruiksgemak?



WAAROM CANON?

EXPERTISE
De integratie van hardware en software verlaagt het risico van systeeminbreuken.

PARTNERSCHAP
Wij helpen klanten betere prestaties te leveren in de wetenschap dat we proactief bedreigingen op het gebied van gegevensbeveiliging aanpakken.

SERVICE
Het team dat zorgdraagt voor de beveiliging van onze klanten, zorgt ook voor onze eigen IT-beveiliging. We houden rekening met elke mogelijke bedreiging, van binnen en buiten de firewall van de organisatie.

INNOVATIE
Onze producten en services bevatten slimmere manieren om potentiële risico's op het gebied van gegevensbeveiliging te minimaliseren.

SC 2017 awards EUROPE

BLI PACESETTER MOBILE Print 2017-2018

'Highly commended' in de categorie voor het beste beveiligingsteam tijdens de **2017 SC Awards Europe**, die worden uitgereikt voor expertise op het gebied van cybersecurity.

Canon U.S.A. ontving twee **BLI PaceSetter Awards 2017** (Document Imaging Security en Mobile Print).

Canon Inc.
canon.com
Canon Europe
canon-europe.com

Canon Nederland N.V.
Brabantlaan 2
5216 TV 's-Hertogenbosch
Telefoon: 073 681 58 15
canon.nl

/company/canon-nederland-n-v-
/CanonProPrintNL en /CanonBusinessNL
/CanonBusinessNL
/CanonNL

Canon

See the bigger picture