



ZAŠČITA VAŠE PISARNE

Canon



Canon uniFLOW Online
Outstanding Cloud Output-Management Solution

McAfee
PROTECTED

New to the Line



KAKO VARNE SO INFORMACIJE V VAŠI PISARNI?

Podjetja se danes v veliki meri zanašajo na informacije in ustvarjajo kompleksna omrežja povezane tehnologije, procesov, ljudi in organizacij, ki segajo preko nacionalnih meja. V obdobju digitalne transformacije se pojavljajo nove, dinamične delovne prakse, ki preoblikujejo pisarno in spreminjajo način, kako ljudje ustvarjajo, delijo in uporabljajo informacije. V takem prepletenem okolju je varovanje podatkov težje zagotoviti kot kadar koli prej, pri čemer večina podjetij vlaga v sofisticirane tehnologije, kot so odporni požarni zidovi, posodobljena protivirusna zaščita, varnostna programska oprema itn. Vendar se pogosto ne zavedajo, da je takšna zaščita potrebna tudi v tiskalnikih za pisarne, in kako so brez nje ranljivi.



MISLITE NA SVOJE TISKALNIKE

Sodobni večnamenski tiskalniki so se razvili v zmogljiva orodja, ki imajo tako kot osebni računalniki operacijske sisteme, velike trde diske in povezavo z omrežjem in internetom, uporabniki pa jih medsebojno uporabljajo za obdelavo ogromnega števila poslovno pomembnih dokumentov.



KAKŠNA SO TVEGANJA?

- Nepooblašчени uporabniki dostopajo do občutljivih informacij, shranjenih v nezaščitene sodobnih večnamenskih tiskalnikih.
- Razpoložljivost vaše infrastrukture za tiskanje je ogrožena zaradi napačnega delovanja.
- Zunanji zlonamerneži pridobijo dostop do vašega omrežja prek tiskalnika in ga uporabijo za nadaljnje napade.
- Izpostavljenost zaupnih dokumentov, ki so po tiskanju ostali na izhodnem pladnju.
- Natisnjen material, ki pripada različnim uporabnikom, se pomeša.
- Dokumenti se pošljejo prek faksa ali elektronske pošte napačnim prejemnikom zaradi tipkarskih napak.
- Tiskalne ali skenirane podatke med prenosom prestrežejo hekerji.
- Podatki se izgubijo zaradi neprevidne odstranitve tiskalnikov ob koncu obdobja izposoje.

“V pisarni, kjer lahko upravljate z ogromno količino podatkov, je zelo koristno sprejeti osnovne standarde informacijske varnosti. Tiskalnik dandanes ni več neumen stroj, je strežnik, ki mimogrede tudi tiska na papir.”

(CISO, Publicis Groupe)

REŠITVE ZA VARNO TISKANJE ZA VAŠE PODJETJE

Zasnova varnosti in zasebnosti

Pri snovanju ali izbiri tehnologij, izdelkov in storitev za naše stranke upoštevamo tudi njihov verjeten vpliv na okolje naših strank z vidika informacijske varnosti. Zato so naši večnamenski tiskalniki za pisarne opremljeni z zelo raznolikimi varnostnimi funkcijami, tako standardnimi kot izbirnimi, kar podjetjem vseh velikosti omogoča zeleno raven zaščite za:



NAPRAVE



OMREŽJA



DOKUMENTE



VAŠE PODJETJE



MEDNARODNO PRIZNANI STANDARDI IN CERTIFIKATI

Naši večnamenski tiskalniki imageRUNNER ADVANCE se rutinsko preverjajo in certificirajo z metodologijo skupnih meril in v skladu z zahtevami standardov IEEE2600 za varnost tiskalnih naprav.



PREVERJANJE ZAŠČITE

Canon uporablja enega najbolj temeljitih sistemov preverjanja varnosti na področju pisarniške opreme. Tehnologije, ki jih vgradimo v naš portfelj izdelkov, so preverjene po enako visokih standardih, kot jih pričakujemo za naše lastno podjetje.

Canon kot vodilno podjetje v panogi na področju razvoja inovativnih rešitev tiskanja in upravljanja informacij za pisarne in podjetja sodeluje s strankami, da jim pomaga najti vključujoč pristop k informacijski varnosti, takšnega, ki upošteva varnostne posledice naše tehnologije za pisarne v okviru njihovega širšega informacijskega ekosistema.



ZAŠČITITE SVOJO NAPRAVO

Celovita zaščita za materialna sredstva



REŠITVE ZA PREVERJANJE PRISTNOSTI UPORABNIKA

Zaščitite svojo napravo pred nepooblaščenno uporabo, tako da nadzorujete uporabniške dostope s preverjanjem pristnosti. To vam nudi tudi dodano vrednost, saj uporabnikom zagotavlja hitrejši dostop do lastnih nastavitev in tiskarskih opravil, hkrati pa povečuje odgovornost in nadzor. Naši oddelčni tiskalniki so opremljeni s sistemom uniFLOW Online Express, ki je prožna rešitev za prijave in omogoča preverjanje pristnosti uporabnika na podlagi uporabniške zbirke podatkov, ustvarjene v napravi, ter preverjanje pristnosti domene prek sistema Active Directory ali strežnika uniFLOW. Tako lahko podjetja nadzorujejo dostop do naprav, hkrati pa je doseženo ustrezno ravnoesje med prilagojenostjo uporabniku in varnostjo.



ZAŠČITA PODATKOV NA TRDEM DISKU

Večnamenski tiskalnik vedno vsebuje veliko količino podatkov, ki jih je treba zaščititi: od opravil tiskanja, ki čakajo na izvedbo, do prejetih faksov, skeniranih podatkov, imenikov, dnevnikov dejavnosti in zgodovine opravil. Canonove naprave nudijo številne ukrepe za zaščito vaših podatkov na vseh stopnjah življenjske dobe naprave in zagotavljajo zaupnost, celovitost in razpoložljivost podatkov.



SISTEM ZA NADZOR DOSTOPA

Ta funkcija omogoča natančen nadzor dostopa do funkcij naprave. Skrbniki lahko uporabljajo standardne, že pripravljene vloge ali ustvarijo prilagojene vloge z želeno ravno skrbniških pravic. Nekaterim uporabnikom bo na primer prepovedano kopiranje dokumentov ali uporaba funkcije pošiljanja.



NASTAVITEV VARNOSTNE POLITIKE

Najnovejše naprave imageRUNNER ADVANCE DX so opremljene tudi s funkcijo varnostne politike, ki skrbniku omogoča dostop do vseh nastavitev v zvezi z varnostjo v enem meniju ter njihovo spreminjanje, preden jih določi v napravi. Ko se določijo, se mora naprava uporabljati v skladu s to politiko, enako pa velja tudi za spremembe nastavitev. Varnostna politika se lahko zaščiti z ločenim geslom, da je dostop do tega področja omejen na odgovornega strokovnjaka za varnost informacijske tehnologije, kar še dodatno poveča raven nadzora in zanesljivosti.



SKRBNIŠKO UPRAVLJANJE NAPRAVE

Konfiguracijsko upravljanje naprave, kot so omrežne nastavitve in druge možnosti upravljanja, je dostopno le uporabnikom, ki imajo skrbniške pravice, s čimer se prepreči namerno ali nenamerno spreminjanje.



PREVENTIVNA VARNOST

Izdelki imageRUNNER ADVANCE DX nudijo številne varnostne nastavitve, ki omogočajo zaščito tiskalnikov pred vdori. Funkcija sistema za preverjanje ob zagonu zagotavlja integriteto naprave med zagonom, medtem ko programska oprema McAfee Embedded Control integriteto zagotavlja med celotno življenjsko dobo naprave, tako da preprečuje spreminjanje programov ali zagon nepooblaščenih programov med delovanjem. Podatki Syslog pa dodatno zagotavljajo informacije o delovanju zaščite v realnem času in nudijo možnost nadzora (do podatkov je mogoče dostopati z ustreznim sistemom SIEM drugega ponudnika).



KAKO VARNE SO VAŠE NAPRAVE?

1

Ali so vaše naprave v skupni rabi in nameščene na javnih mestih?

2

Ali uporabniki lahko pridobijo nezaščiten dostop do naprav?

3

Ali ste sprejeli ukrepe za zaščito informacij na trdem disku naprave?

4

Ali lahko nepooblašчени uporabniki spremenijo nastavitve naprave?

5

Ali ste pomislili na življenjsko dobo naprave in njeno varno odstranitev?

ŠIFRIRANJE TRDEGA DISKA

Naše naprave imageRUNNER ADVANCE DX šifrirajo vse podatke na trdem disku, s čimer povečujejo varnost. Ta varnostni čip, ki je odgovoren za šifriranje podatkov, je skladen z varnostnim standardom FIPS 140-2 ravni 2, ki ga je določila ameriška vlada in je certificiran v okviru programa Cryptographic Module Validation Program (CMVP), ki so ga določile ZDA in Kanada, ter tudi v okviru japonskega programa Japan Cryptographic Module Validation Program (JCMVP).

BRISANJE TRDEGA DISKA

Nekateri podatki, kot so podatki o kopirani ali skenirani sliki in tudi podatki dokumenta, natisnjenega z računalnika, so na trdem disku shranjeni le začasno in se po dokončanem opraviu izbrišejo. Za zagotovitev, da se odvečni podatki ne ohranijo, naše naprave, ki imajo trdi disk, nudijo možnost rutinskega izbrisa odvečnih podatkov v sklopu obdelave opravila.

PONASTAVITE VSE PODATKE IN NASTAVITVE

Če želite preprečiti izgubo podatkov med zamenjavo ali odstranjevanjem trdega diska, lahko prepišete vse dokumente in podatke na trdi disk ter ponastavite nastavitve naprave na privzete.

ZRCALJENJE TRDEGA DISKA*

Podjetja imajo možnost, da podatke na trdem disku svoje naprave varnostno kopirajo v dodaten izbirni trdi disk. Med izvajanjem zrcaljenja se podatki na obeh trdih diskih v celoti šifrirajo.

*Izbirno za izbrane modele. Za podrobne informacije o razpoložljivosti funkcij in možnosti po celotnem portfelju pisarniškega tiskanja se obrnite na svojega predstavnika družbe Canon.



ZAVARUJTE SVOJE OMREŽJE



ALI LAHKO TISKALNIK OGROŽA VAŠE OMREŽJE?

- Ali puščate omrežna vrata odprta in s tem tvegate vdor?
- Ali lahko gostje tiskajo in skenirajo, ne da bi s tem vaše omrežje izpostavili tveganjem?
- Ali je vaša politika prinašanja lastnih naprav na delovno mesto varna in podporna?
- Ali se podatki tiskanja med pretakanjem iz računalnika do izhodne naprave šifrirajo?
- Ali so podatki, ki se tiskajo in skenirajo, med prenosom zavarovani?

Canon nudi vrsto varnostnih rešitev, da bodo vaše omrežje in podatki varni pred notranjimi in zunanji vdori.

FILTRIRANJE NASLOVOV IP IN MAC

Zaščitite svoje omrežje pred nepooblaščenim dostopom tretjih oseb tako, da dovolite komunikacijo le z napravami, ki imajo določen naslov IP ali MAC, tako za izhodno kot vhodno komunikacijo.

KONFIGURACIJA POSREDNIŠKEGA STREŽNIKA

Namesto svoje naprave za upravljanje komunikacije nastavite posredniški strežnik in ga uporabite med povezovanjem z napravami zunaj omrežja.

PREVERJANJE PRISTNOSTI IEEE 802.1X

Nepooblaščen dostop do omrežja blokira stikalo LAN, ki pravico do dostopa odobri le napravam strank s pooblastilom strežnika za preverjanje pristnosti.

KOMUNIKACIJA IPSEC

Komunikacija IPsec preprečuje tretjim osebam, da bi prestregle pakete IP, ki se prenašajo prek omrežja IP, ali posegale vanje.

S šifrirano komunikacijo TLS preprečite razkrivanje, imitacijo in spreminjanje podatkov, ki se izmenjajo med strojno napravo in drugimi napravami, npr. računalniki.

NADZOR VRAT

Vrata konfigurirajte kot del nastavitve svoje varnostne politike.

SAMODEJEN VPIS POTRDILO

S to funkcijo je vzdrževanje varnostnih certifikatov neprimerno lažje. Skrbnik sistema lahko s priznano tehnologijo samodejno posodobi in izdaja certifikate, da zagotovi stalno skladnost z varnostnimi politikami.

SPREMLJANJE Z DNEVNIKI

Z različnimi dnevniki lahko spremljate dejavnost v okolici svoje naprave, vključno z blokiranimi zahtevami za komunikacijo.

WI-FI DIRECT

Omogočite povezavo med enakovrednimi napravami za mobilno tiskanje, ne da bi mobilna naprava potrebovala dostop do vašega omrežja.

ŠIFRIRANJE PODATKOV MED PRENOSOM V NAPRAVO IN IZ NJE

Ta možnost šifrira opravila tiskanja med prenosom iz uporabnikovega računalnika v večnamenski tiskalnik. Če omogočite komplet za univerzalne varnostne funkcije, se lahko šifrirajo tudi skenirani podatki v obliki PDF.

TISKANJE IZ GOSTUJOČIH MOBILNIH NAPRAV

Naša programska oprema za varno upravljanje tiskanja in skeniranja v omrežju pogosta varnostna tveganja za mobilno in gostujoče tiskanje preprečuje tako, da zagotavlja zunanje poti pošiljanja opravil prek e-pošte, spleta in mobilne aplikacije. S tem se možnost napada vektorjev zmanjša na minimum, ker se večnamenska naprava zaklene na varen vir.

DVOJNO OMREŽJE

Najnovejša tehnologija ima sedaj dvojno omrežno zmogljivost: medtem ko je primarno omrežje vedno žično, ima lahko sekundarna linija sedaj brezžično povezavo oz. žično povezavo za strožje varnostno ločevanje omrežij.



ZAŠČITITE SVOJE DOKUMENTE

Vsa podjetja delajo z občutljivimi dokumenti, kot so pogodbeni sporazumi, podatki o plačah zaposlenih, podatki o strankah, načrti o raziskavah in razvoju itn. Če pridejo taki dokumenti v napačne roke, so posledice lahko okrnjen ogled, visoke denarne kazni ali celo sodni ukrep.

Canon nudi vrsto varnostnih rešitev za zaščito vaših občutljivih dokumentov skozi njihov celoten življenjski cikel.



ZAUPNOST ZA NATISNJEN DOKUMENT

Varno tiskanje

Uporabnik lahko za tiskanje nastavi PIN-kodo, da naprava dokument natisne le, če je bila vnesena pravilna PIN-koda. Tako lahko posamezniki zaščitijo dokumente, ki jih želijo ohraniti zaupne.

Zadržanje vseh opravil tiskanja

Skrbnik lahko v napravi imageRUNNER ADVANCE DX izvede zadržanje vseh oddanih opravil tiskanja, tako da se morajo uporabniki pred izvedbo tiskanja prijaviti, da se zagotovi zaupnost vsega natisnjenega materiala.



ODVRAČANJE OD PODVAJANJA DOKUMENTOV ALI NJEGOVO PREPREČEVANJE

Tiskanje z vidnimi vodnimi žigi

Gonilniki lahko natisnejo vidne žige na vrhu strani ali za vsebino dokumenta. To ima odvrčalen učinek od kopiranja, ker ozavešča uporabnika o zaupnosti dokumenta.

Tiskanje/kopiranje z nevidnimi vodnimi žigi

Če je ta možnost omogočena, se dokumenti lahko natisnejo ali kopirajo z vdelanim skritim besedilom v ozadju, tako da se pri podvajanju besedilo pojavi na dokumentu in deluje odvrčalno.

Poštni nabiralniki

Opravila tiskanja ali skenirani dokumenti se lahko shranijo v poštni nabiralnik z možnostjo poznejšega dostopa. Poštni nabiralniki so lahko zaščiteni s PIN-kodo za zagotovitev, da lahko njihovo vsebino vidijo le njihovi dodeljeni lastniki. Ta varen prostor v napravi je primeren za hrambo dokumentov, ki jih je treba pogosto tiskati (na primer obrazci), vendar zahtevajo previdno ravnanje.

Varno tiskanje uniFLOW*

Uporabniki z varnim tiskanjem uniFLOW MyPrintAnywhere oddajo opravila tiskanja prek univerzalnega gonilnika in gradivo natisnejo prek katerega koli tiskalnika v omrežju.

Preprečevanje izgube podatkov na korporativni ravni

Nadgradite osnovne zmožnosti preprečevanja izgube podatkov na iW SAM Express v kombinaciji z uniFLOW. Ta rešitev v strežniku vam omogoča zajetje in arhiviranje dokumentov, poslanih iz tiskalnika in v njega, ter analiziranje in interpretiranje besedila ali atributov, njena najpomembnejša naloga pa je reakcija na varnostne grožnje.

Sledenje izvoru dokumenta*

Prek vdelane kode se lahko izvoru dokumenta sledi do vira.

KAKO VARNI SO VAŠI DOKUMENTI?

1

Ali je nepooblaščenim uporabnikom preprečen dostop do občutljivih dokumentov v tiskalniku?

2

Ali lahko zagotovite zaupnost vseh dokumentov uporabnikov, ki gredo skozi napravo v skupni rabi?

3

Ali lahko sledite izvorom natisnjenih dokumentov?

4

Ali lahko pride do odtujitve občutljivih dokumentov iz vašega tiskalnika?

5

Ali lahko preprečite pogoste napake pri pošiljanju dokumentov iz naprave?



IZVAJAJTE NADZOR NAD POŠILJANJEM DOKUMENTOV IN FAKSOM

Omejite prejemnike za pošiljanje

Da bi zmanjšali tveganje za odtekanje informacij, lahko skrbniki omejijo razpoložljive prejemnike, ki se jim lahko pošiljajo podatki, na zgolj tiste, ki so v imeniku ali strežniku LDAP, prijavljeni v uporabnikov naslov ali v določenih domenah.

Onemogočitev samodejnega dokončanja naslova

Preprečite pošiljanje dokumentov napačnim prejemnikom, tako da onemogočite samodejno dokončanje e-poštnega naslova.

Zaščita imenika

Z nastavitvijo PIN-kode zaščitite imenik naprave pred spreminjanjem nepooblaščenih uporabnikov.

Potrditev številke faksa

Preprečite pošiljanje dokumentov neželenim prejemnikom, tako da morajo uporabniki pred pošiljanjem za potrditev dvakrat vnesti številko faksa.

Zaupnost za prejeti faks

Nastavite napravo tako, da bo shranjevala dokumente v spomin, ne da bi jih natisnila. Zaupnost prejetih faksiranih dokumentov lahko zaščitite tudi z določitvijo pogojev za določanje lokacije shranjevanja v zaupnem nabiralniku ali z nastavitvijo PIN-kod.



PREVERJANJE IZVORA IN PRISTNOSTI DOKUMENTOV Z DIGITALNIMI PODPISI

Podpis naprave

Podpis naprave se lahko uporabi v skeniranih dokumentih v obliki PDF ali XPS, in sicer z mehanizmom ključa in potrdila, da lahko prejemnik preveri izvor in tudi pristnost dokumenta.

Podpis uporabnika*

Možnost omogoča uporabnikom pošiljanje datoteke PDF ali XPS z edinstvenim digitalnim podpisom uporabnika, pridobljenega pri overitelju potrdil. Tako lahko prejemnik preveri, kateri uporabnik je podpisan.



UPORABA POLITIK Z INTEGRACIJO S PROGRAMSKO OPREMO ADOBE LIFECYCLE MANAGEMENT ES

Uporabniki lahko občutljive podatke in informacije visoke vrednosti zaščitijo pred nenamernim ali zlonamernim razkritjem tako, da zavarujejo datoteke PDF in uporabijo stalne in dinamične politike za nadzor nad dostopom in uporabniškimi pravicami. Varnostne politike

se hranijo na ravni strežnika, tako da se pravice lahko spremenijo tudi po distribuciji datoteke. Družino imageRUNNER ADVANCE DX je mogoče konfigurirati za integracijo z Adobe® ES.

*Izbirno. Za podrobne informacije o razpoložljivosti funkcij in možnosti po celotnem portfelju pisarniškega tiskanja se obrnite na svojega predstavnika družbe Canon.



VARNOST PODJETNIŠKIH INFORMACIJ

Canon lahko prispeva k celostni zaščiti informacij v vaši organizaciji.

POPOLN NADZOR ZA VAŠE POTREBE CELOVITEGA ZAJEMANJA IN TISKANJA

Z našo modularno programsko opremo za upravljanje tiskanja imajo podjetja zagotovljeno varno skupno rabo omrežnih naprav, kar jim omogoča varna opravila tiskanja na vseh tiskalnikih, povezanih v strežnik za upravljanje tiskanja. Mobilne uporabnike podpira centralno upravljana storitev, v kateri imajo tako notranji uporabniki kot gostje varen dostop do tiskanja iz mobilnih naprav.

Za potrebe zajema v podjetju modul za tiskanje zagotavlja zajem, stiskanje, pretvorbo in distribucijo dokumentov iz večnamenske naprave v zelo različne destinacije, vključno s sistemi, ki temeljijo na oblaku. Opravila tiskanja lahko tudi varno preusmerite v najprimernejši tiskalnik ter tako optimizirate strošek tiskanja posameznih dokumentov.

Naša rešitev omogoča večjo varnost dokumentov na ravni vašega podjetja in skupaj s celovitim sledenjem dokumentom zagotavlja popolno preglednost nad dejavnostmi posameznega uporabnika, naprave in oddelka.

CENTRALIZIRANO UPRAVLJANJE SKUPINE NAPRAV

Naša programska oprema za upravljanje naprav IW MC omogoča, da se varnostne politike, gesla in certifikati, pa tudi strojna programska oprema posodobijo in namestijo v celotno omrežje vaše skupine Canonovih naprav, kar vaši ekipi za IT prihrani dragoceni čas, poskrbljeno pa je tudi za posodobljeno varnost vaše infrastrukture za tiskanje.

IZČRPNNO PREGLEDOVANJE DOKUMENTOV

Našo arhitekturo storitev za pisarniške dokumente lahko okrepite z naročilom možnosti za zajem celotnega zapisa (meta podatki skeniranja in opravil) vseh dokumentov, ki se obdelajo z napravami imageRUNNER ADVANCE DX.

UPRAVLJANE STORITVE TISKANJA

Canonove upravljane storitve tiskanja združujejo inovativno tehnologijo in programsko opremo z ustreznimi storitvami, da bo vaša izkušnja tiskanja in upravljanja dokumentov v skladu z vašimi željami, ne da bi vaša ekipa za IT morala za to vložiti ogromno truda. S proaktivnim upravljanjem in nenehno optimizacijo vaše infrastrukture za tiskanje ter potekov dela z dokumenti vam lahko pomagamo doseči vaše varnostne cilje ob hkratni optimizaciji stroškov in povečanju produktivnosti v vašem podjetju.

RAZVOJ PO MERI

Imamo ekipo notranjih razvijalcev, ki lahko predlagajo in razvijejo rešitev po meri za vaše specifične okoliščine ali posebne zahteve.

KAKO VKLJUČUJOČ JE PRISTOP VAŠEGA PODJETJA K VARNOSTI?

- Ali vaša varnostna politika vključuje tudi vašo skupino večnamenskih naprav?
- Kako zagotavljate, da je vaša infrastruktura za tiskanje posodobljena ter da se pravočasno in učinkovito izvajajo izboljšave ter odpravljajo napake?
- Ali lahko gostje tiskajo in skenirajo, ne da bi bilo zato vaše omrežje izpostavljeno tveganju?
- Ali je vaša politika prinašanja lastnih naprav varna in podporna na ravni vaše skupine naprav?
- Ali ima vaša ekipa za IT dovolj časa za preučevanje varnostnih vprašanj?
- Ali je ravnovesje med zagotavljanjem varnosti in prilagojenostjo uporabniku ustrezno?



ZAKAJ CANON?



STROKOVNO ZNANJE

Integracija strojne in programske opreme zmanjša možnost kršitev v sistemu.



SERVIS

Za **stranke skrbi ista ekipa za informacijsko varnost** kot za našo lastno notranjo varnost IT.

Upoštevamo vse potencialne grožnje, tako znotraj požarnega zidu podjetja kot zunaj njega.



PARTNERSTVO

Z našo pomočjo lahko stranke poslujejo bolje, saj vedo, da bomo **proaktivno obravnavali tveganja za varnost podatkov**.



INOVATIVNOST

Naši izdelki in storitve **vključujejo pametnejše načine** za zmanjšanje verjetnih tveganj za informacijsko varnost na minimum.



"Zelo pohvaljeno" v kategoriji najboljših ekip za varnost na podelitvi nagrad **SCA Awards Europe** za leto 2017 v okviru podeljevanja priznanj za strokovno znanje na področju kibernetične varnosti.

Canon U.S.A. je prejel dve nagradi **BLI PaceSetter Awards za leto 2017** (kategoriji varnost pri obdelavi slik v dokumentih in mobilno tiskanje).

Canon Inc.

Canon.com

Canon Europe

canon-europe.com

Slovenian edition

© Canon Europa N.V., 2019

Canon Adria d.o.o.

Dunajska 128a

1000 Ljubljana

Slovenija

Tel: +386 1 5308 710

Fax: +386 1 5380 745

canon.si