



ZAŠTITA VAŠEG UREDA

Canon



Canon uniFLOW Online
Outstanding Cloud Output-Management Solution

McAfee
PROTECTED



New to the Line



KOLIKO SU SIGURNE INFORMACIJE U VAŠEM UREDU?

Današnje tvrtke uvelike se oslanjaju na informacije, stvaranje složenih mreža povezanih tehnologija, postupaka, osoba i organizacija koje nadilaze nacionalne granice. U doba digitalne transformacije pojavljuju se nove i brze radne prakse koje mijenjaju ured i način na koji ljudi stvaraju, dijele i upotrebljavaju informacije. Osiguravanje podataka u ovom složenom okruženju zahtjevnije je nego ikada prije, stoga većina tvrtki ulaže u sofisticirane tehnologije poput robusnih vatrozidova, ažurnu antivirusnu zaštitu, sigurnosni softver i drugo. Međutim, često ne prepoznaju potrebu da tu zaštitu prošire na uredske pisane i tako ostaju ranjiviji no što shvaćaju.



RAZMISLITE O SVOJIM PISAČIMA

Moderni višefunkcijski pisači (multifunctional printer, MFP) razvili su se u moćne alate koji su, poput osobnih računala i poslužitelja, opremljeni operativnim sustavima, velikim tvrdim diskovima, povezuju se na mrežu i internet te ih dijele korisnici za dnevnu obradu velikog broja dokumenata važnih za tvrtku.



KOJI SU RIZICI?

- Neovlašteni korisnici mogu vidjeti osjetljive informacije spremljene na nezaštićenim višefunkcijskim pisačima
- Ugroženost dostupnosti infrastrukture za ispisivanje zbog pogrešne upotrebe
- Zlonamjerni vanjski pristupnici putem pisača mogu ostvariti pristup vašoj mreži i iskoristiti ga za dodatne napade
- Izlaganje povjerljivih dokumenata zaboravljenih u izlaznom odlagaču nakon ispisivanja
- Miješanje ispisanih materijala koji pripadaju različitim korisnicima
- Dokumenti se faksiraju ili šalju e-poštom pogrešnim primateljima zbog pogreške pri upisivanju
- Hakeri mogu u prolazu presresti podatke za ispisivanje ili skeniranje
- Gubitak podataka zbog neopreznog zbrinjavanja pisača na završetku najma.

“Primjena osnovnih standarda za sigurnost informacija isplativa je u uredu u kojem se potencijalno obrađuju velike količine podataka. Pisač danas više nije glup stroj, to je poslužitelj koji i ispisuje na papir”.

(CISO, Publicis Groupe)

RJEŠENJA ZA SIGURNO ISPISIVANJE U VAŠOJ TVRTKI

Dizajnirana sigurnost i privatnost

Kada za naše klijente dizajniramo ili odabiremo tehnologije, proizvode ili usluge, u obzir uzimamo vjerojatni utjecaj na sigurnost informacija u okruženju klijenata. Zato su naši uredski višefunkcijski pisači opremljeni raznim sigurnosnim značajkama, standardnim i dodatnim, koje tvrtkama svih veličina omogućuju ostvariti željenu razinu zaštite za:



UREĐAJE

MREŽE

DOKUMENTE

VAŠU TVRTKU



MEĐUNARODNO PRIZNATI STANDARDI I CERTIFIKACIJE

Naši višefunkcijski pisači imageRUNNER ADVANCE često se procjenjuju i certificiraju sukladno metodologiji Common Criteria i u skladu sa zahtjevima standarda IEEE2600 za sigurnost uređaja za ispisivanje.



TESTIRANJE SIGURNOSTI

Canon primjenjuje jedan od najstrožih sustava za ispitivanje sigurnosti u industriji uredske opreme. Tehnologije zastupljene u našem portfelju proizvoda podložne su visokim standardima ispitivanja koje primjenjujemo i na našu tvrtku.

Kao industrijski predvodnik razvoja inovativnih rješenja za ispisivanje i upravljanje podacima u uredu i tvrtki, Canon surađuje s klijentima kako bi im pomogao prihvatiti sveobuhvatan pristup sigurnosti informacija, pristup koji sigurnosne implikacije naše uredske tehnologije razmatra kao dio šireg informacijskog ekosustava.



ZAŠTITITE SVOJ UREĐAJ

Opsežna zaštita fizičke imovine



RJEŠENJA ZA AUTORIZACIJU KORISNIKA

Zaštitite svoj uređaj od neovlaštene upotrebe kontrolirajući pristup korisnika autorizacijom. Uz povećanje odgovornosti i kontrole, dodatna prednost za korisnike osiguranje je bržeg pristupa njihovim preferiranim postavkama i zadacima ispisa. Naši pisari za odjele opremljeni su fleksibilnim rješenjem za prijavu uniFLOW Online Express koje omogućuje autorizaciju korisnika putem baze podataka stvorene na uređaju i autorizaciju domene putem poslužitelja Active Directory ili uniFLOW. To tvrtkama osigurava kontrolu pristupa uređaju uz pravilnu ravnotežu između praktičnosti za korisnike i sigurnosti.



ZAŠTITA PODATAKA NA TVRDOM DISKU

Višefunkcijski pisar u bilo kojem trenutku sadrži veliku količinu podataka koju treba zaštititi – od zadataka ispisivanja koji čekaju na ispisivanje do primljenih faksova, skeniranih podataka, adresara, zapisnika aktivnosti i povijesti zadataka. Uređaji Canon pružaju niz mjera za zaštitu podataka u svakoj fazi vijeka trajanja uređaja i osiguranje povjerljivosti, cjelovitosti i dostupnosti podataka.



SUSTAV ZA UPRAVLJANJE PRISTUPOM

Ova značajka omogućuje zrnastu kontrolu pristupa funkcijama uređaja. Administratori mogu upotrijebiti standardne dostupne uloge ili stvoriti prilagođene sa željenom razinom privilegija za pristup. Na primjer, pojedinim korisnicima može se onemogućiti kopiranje dokumenata ili upotreba funkcije za slanje.



POSTAVLJANJE PRAVILA SIGURNOSTI

Najnoviji uređaji imageRUNNER ADVANCE DX također su opremljeni funkcijom za pravila sigurnosti koja administratoru omogućuje pristup i uređivanje svih postavki sigurnosti na jednom izborniku prije primjene na stroju. Nakon primjene, upotreba uređaja i promjene postavki moraju biti u skladu s pravilima. Pravila sigurnosti moguće je zaštititi posebnom lozinkom kako bi se pristup tom području ograničio na odgovorne stručnjake za IT sigurnost, čime se dodaje dodatna razina kontrole i sigurnosti.



ADMINISTRATIVNA KONTROLA UREĐAJA

Konfiguracija uređaja poput mrežnih postavki i drugih kontrolnih mogućnosti dostupna je samo korisnicima koji imaju administrativne ovlasti, čime se sprječavaju namjerne ili slučajne promjene.



PREVENTIVNA SIGURNOST

Proizvodi imageRUNNER ADVANCE DX donose niz postavki za sigurnost koje omogućuju zaštitu pisara od napada. Funkcija provjere sustava pri pokretanju osigurava integritet uređaja po pokretanju stroja, a ugrađeni kontrolni softver McAfee osigurava integritet kroz vijek trajanja uređaja sprečavajući neovlaštene izmjene programa ili izvedbu neovlaštenih programa tijekom vremena izvođenja. Osim toga, podaci Syslog u stvarnom vremenu prikazuju stanje sigurnosti uređaja i mogućnosti nadzora (podaci se mogu očitati odgovarajućim sustavom SIEM treće strane).



KOLIKO SU SIGURNI VAŠI UREĐAJI?

1

Dijelite li svoje uređaje i jesu li postavljeni u javne prostore?

2

Mogu li korisnici ostvariti nezaštićen pristup uređajima?

3

Jeste li poduzeli mjere za zaštitu informacija na tvrdom disku uređaja?

4

Mogu li neovlašteni korisnici promijeniti postavke uređaja?

5

Jeste li razmišljali o vijeku trajanja uređaja i njegovom sigurnom zbrinjavanju?

ŠIFRIRANJE TVRDOG DISKA

Naši uređaji imageRUNNER ADVANCE DX šifriraju sve podatke na tvrdom disku i tako povećavaju sigurnost. Sigurnosni čip odgovoran za šifriranje podataka ispunjava 2. razinu sigurnosnog standarda FIPS 140-2 kojeg je uspostavila vlada SAD-a i koji nosi certifikaciju programa za provjeru valjanosti modula za šifriranje (Cryptographic Module Validation Program, CMVP) SAD-a i Kanade, kao i japanskog programa za provjeru valjanosti modula za šifriranje (Japan Cryptographic Module Validation Program, JCMVP).

BRISANJE TVRDOG DISKA

Neki podaci, poput podataka kopiranih ili skeniranih slika, kao i podaci dokumenta ispisanog s računala, privremeno se spremaju na tvrdi disk te brišu nakon dovršetka radnje. Kako bismo osigurali da nema preostalih podataka, naši uređaji opremljeni tvrdim diskom pružaju mogućnost rutinskog brisanja preostalih podataka u sklopu obrade zadatka.

POSTAVLJANJE SVIH PODATAKA I POSTAVKI NA POČETNU VRIJEDNOST

Izbrišite sve dokumente i podatke na tvrdom disku te vratite stroj na zadane postavke kako pri zamjeni ili odlaganju tvrdog diska ne bi došlo do gubitka podataka.

ZRCALJENJE TVRDOG DISKA*

Tvrtke podatke s tvrdog diska svojeg uređaja mogu sigurnosno kopirati na dodatni tvrdi disk. Pri zrcaljenju podaci na oba tvrda diska potpuno se šifriraju.

*Opcionalno za odabrane modele. Za detaljne informacije o dostupnosti značajki i opcija u portfelju za uredsko ispisivanje obratite se predstavniku tvrtke Canon.



ZAŠTITITE SVOJU MREŽU



UGROŽAVA LI PISAČ VAŠU MREŽU?

- Jesu li vaši mrežni priključci nezaštićeni od napada?
- Mogu li gosti ispisivati i skenirati bez izlaganja mreže opasnostima?
- Jesu li vaša pravila o donošenju vlastitih uređaja na posao sigurna i održiva?
- Jesu li šifrirani protoci podataka za ispisivanje između osobnog računala i izlaznog uređaja?
- Jesu li podaci za ispisivanje i skenirani podaci sigurni u prijenosu?

Canon nudi niz sigurnosnih rješenja za zaštitu mreže i podataka od unutarnjih i vanjskih napada.

FILTRIRANJE IP I MAC ADRESE

Zaštitite mrežu od neovlaštenog pristupa trećih strana omogućujući komunikaciju s uređajima samo putem posebnih IP ili MAC adresa za izlaznu i ulaznu komunikaciju.

KONFIGURACIJA PROXY POSLUŽITELJA

Za upravljanje komunikacijom postavite proxy umjesto stroja i upotrebljavajte ga za povezivanje uređaja koji su izvan mreže.

IEEE 802.1X PROVJERA AUTENTIČNOSTI

LAN prespojnik blokira neovlašten pristup mreži i dopušta ga samo klijentskim uređajima s ovlaštenjem poslužitelja za provjeru autentičnosti.

IPSEC KOMUNIKACIJA

IPSec komunikacija trećim stranama onemogućuje presretanje ili neovlašteno mijenjanje IP paketa koji se prenose IP mrežom.

Upotrijebite TLS šifriranu komunikaciju kako biste spriječili otkrivanje sadržaja, krivotvorenje i neovlašteno mijenjanje podataka koji se izmjenjuju između stroja i drugih uređaja, primjerice računala.

KONTROLA PRIKLJUČAKA

Priključke konfigurirajte tijekom postavljanja pravila sigurnosti.

AUTOMATSKO UVRŠTAVANJE CERTIFIKACIJE

Ova značajka znatno smanjuje problem održavanja sigurnosnih certifikata. Primjenom u industriji priznate tehnologije administrator sustava može automatski ažurirati i otpuštati certifikate te tako održavati ispunjenost sigurnosnih pravila.

NADZOR POMOĆU ZAPISNIKA

Različiti zapisnici omogućuju nadzor aktivnosti oko uređaja, uključujući blokirane zahtjeve za komunikaciju.

WI-FI DIRECT

Omogućite vezu između ravnopravnih članova za ispisivanje s mobilnog uređaja bez pristupa mobilnog uređaja mreži.

ŠIFRIRANJE PODATAKA U PRIJENOSU NA UREĐAJ I S NJEGA

Ova opcija šifrira zadatke ispisivanja u prijenosu s osobnog računala korisnika u višefunkcijski pisač. Omogućenjem kompleta univerzalnih značajki za sigurnost podatke skenirane u formatu PDF također je moguće šifrirati.

ISPISIVANJE S MOBILNOG UREĐAJA GOSTA

Naš softver za sigurno ispisivanje s mreže i upravljanje skeniranjem suočava se s ispisivanjem s mobilnih uređaja i ispisivanja gostiju osiguravajući putove za slanje vanjskih zadataka putem e-pošte, weba i mobilne aplikacije. Na taj način napadački vektori smanjuju se na minimum zaključavanjem višefunkcijskog uređaja na siguran izvor.

DVIJE MREŽE

Najnovija tehnologija sada omogućuje rad na dvije mreže: primarna mreža uvijek je žična, a sekundarna linija sada može biti bežična ili žična za strože i sigurnije razdvajanje mreža.



ZAŠTITITE SVOJE DOKUMENTE

Sve tvrtke rade s osjetljivim dokumentima poput ugovornih sporazuma, informacija o platnom popisu zaposlenika, korisničkih podataka, planova za istraživanje i razvoj i slično. Ako dokumenti dospiju u pogrešne ruke, posljedice sežu od gubitka ugleda do velikih kazni ili čak pravnih postupaka.

Canon nudi niz sigurnosnih rješenja za zaštitu osjetljivih dokumenata kroz njihov vijek trajanja.



POVJERLJIVOST ISPISANOG DOKUMENTA

Sigurno ispisivanje

Korisnik za ispisivanje može postaviti PIN kôd kako bi ispisivanje dokumenta bilo moguće samo nakon unosa ispravnog PIN koda u stroj. Pojedinci tako mogu zaštititi dokumente koje smatraju povjerljivima.

Zadržavanje svih zadataka ispisa

Administrator pisača imageRUNNER ADVANCE DX radi zaštite povjerljivosti ispisanih materijala može prisilno zadržati sve poslane zadatke ispisivanja. Korisnici se tada moraju prijaviti prije ispisivanja zadataka.

Sandučići e-pošte

Zadatke ispisivanja ili skenirane dokumente moguće je pohraniti u sandučić e-pošte za kasniji pristup. Sandučić e-pošte moguće je zaštititi PIN kodom kako bi samo dodijeljeni vlasnik mogao pregledavati pohranjeni sadržaj. Taj sigurni prostor na uređaju prikladan je za dokumente koje treba često ispisivati (poput obrazaca), no zahtijevaju opreznost.

Sigurno ispisivanje uniFLOW*

Sa sigurnim ispisivanjem uniFLOW MyPrintAnywhere korisnici zadatke ispisivanja šalju putem univerzalnog upravljačkog programa i preuzimaju ih s bilo kojeg pisača na mreži.



DESTIMULIRAJTE ILI SPRIJEČITE KOPIRANJE DOKUMENATA

Ispisivanje s vidljivim vodenim žigovima

Upravljački programi mogu ispred ili iza sadržaja na stranici dokumenta ispisati vidljive oznake. To destimulira kopiranje pojačavajući svjesnost korisnika o povjerljivosti dokumenta.

Ispisivanje/kopiranje s vidljivim vodenim žigovima

Kada je ova opcija omogućena, dokumente je moguće ispisati ili kopirati sa tekstom sakrivenim u pozadini, tako da se tekst pri kopiranju pojavljuje na dokumentu i djeluje kao odvraćajući čimbenik.

Sprječavanje gubitaka podataka na razini tvrtke

Nadogradite osnovne mogućnosti zaštite od gubitka podataka na iW SAM Express u kombinaciji s uniFLOW. Ovo na poslužitelju utemeljeno rješenje omogućuje snimanje i arhiviranje dokumenata koji se šalju pisaču

i koje šalje pisač, te analizu u interpretaciju pomoću teksta ili karakteristika sa ciljem djelovanja u slučaju sigurnosne prijetnje.

Praćenje porijekla dokumenta*

Zahvaljujući ugrađenom kodu moguće je pratiti porijeklo dokumenta do izvora.

KOLIKO SU SIGURNI VAŠI DOKUMENTI?

1

Je li neovlaštenim korisnicima onemogućen pristup osjetljivim dokumentima na pisaču?

2

Možete li zajamčiti povjerljivost svih dokumenata korisnika koji prolaze kroz dijeljeni uređaj?

3

Možete li utvrditi porijeklo ispisanih dokumenata?

4

Može li netko preuzeti osjetljive dokumente s vašeg pisača?

5

Možete li spriječiti uobičajene pogreške pri slanju dokumenata s uređaja?



PROVODITE NADZOR NAD SLANJEM I FAKSIRANJEM DOKUMENATA

Ograničite odredišta za slanje

Kako bi smanjili opasnost od curenja informacija, administratori mogu ograničiti dostupna odredišta za slanje na one iz adresara ili s LDAP poslužitelja, adrese prijavljenog korisnika ili određene domene.

Onemogućite automatsko dovršavanje adrese

Spriječite slanje dokumenata na pogrešna odredišta onemogućavanjem automatskog dovršenja adresa e-pošte.

Zaštita adresara

Postavite PIN kod za zaštitu adresara od neovlaštenih korisnika.

Potvrda broja faksa

Zahtijevajući od korisnika da prije slanja za potvrdu dva puta unesu broj faksa spriječite slanje dokumenata pogrešnim primateljima.

Povjerljivost primljenih faksova

Postavite stroj na spremanje dokumenata u memoriju bez ispisivanja. Povjerljive dokumente primljene faksom također možete zaštititi primjenom uvjeta prema kojima se za lokaciju za pohranu određuje poštanski pretinac za povjerljive materijale, kao i postavljanjem PIN kodova.



POMOĆU DIGITALNIH POTPISA PROVJERITE PORIJEKLO I AUTENTIČNOST DOKUMENTA

Potpis uređaja

Potpis uređaja moguće je primijeniti na dokumente skenirane u formatu PDF ili XPS mehanizmom ključa i certifikacije, tako da primatelj može provjeriti porijeklo i autentičnost dokumenta.

Potpis korisnika*

Ova opcija omogućuje korisnicima slanje datoteke PDF ili XPS s jedinstvenim digitalnim potpisom korisnika kojeg izdaje ustanova za certifikate. Tako primatelj može provjeriti koji ga je korisnik potpisao.



PRIMIENITE PRAVILA INTEGRACIJOM S POSLUŽITELJEM ADOBE LIFECYCLE MANAGEMENT ES

Korisnici mogu osigurati datoteke PDF i primijeniti dosljedna i dinamična pravila za kontrolu pristupa i prava upotrebe kako bi osjetljive i vrlo vrijedne informacije zaštitili od slučajnog ili zlonamjernog objavljivanja.

Sigurnosna pravila održavaju se na razini poslužitelja pa se prava mogu mijenjati čak i nakon distribucije datoteke. Seriju imageRUNNER ADVANCE DX moguće je konfigurirati za integraciju s poslužiteljem Adobe® ES.

*Opcionalno. Za detaljne informacije o dostupnosti značajki i opcija u portfelju za uredsko ispisivanje obratite se predstavniku tvrtke Canon.



SIGURNOST INFORMACIJA O TVRTKI

Canon može pridonijeti ukupnoj zaštiti svih informacija u vašoj organizaciji.

POTPUNA KONTROLA ZA CJELOVITO SNIMANJE I POTREBE ISPISIVANJA

Zahvaljujući našem modularnom softveru za upravljanje ispisivanjem tvrtke mogu sigurno dijeliti mrežne uređaje, što im omogućuje sigurno ispisivanje zadataka na bilo kojem pisaču povezanom s poslužiteljem za upravljanje ispisivanjem. Mobilne korisnike podržava središnje upravljana usluga koja internim korisnicima i gostima osigurava siguran pristup za ispisivanje s mobilnih uređaja.

Za potrebe snimanja u tvrtki modul za skeniranje omogućuje snimanje, komprimiranje, pretvorbu i distribuciju dokumenata s višefunkcijskog uređaja na brojna odredišta, uključujući i sustave informatičkih oblaka. Također možete sigurno preusmjeriti zadatke ispisivanja na najprikladniji pisač i optimirati troškove ispisivanja svakog dokumenta.

Naše rješenje povećava sigurnost dokumenata u vašem poslovanju te osigurava cjelovito računovodstvo koje daje potpun pregled aktivnosti po korisniku, uređaju i odjelu.

CENTRALIZIRANO UPRAVLJANJE SKUPINOM UREĐAJA

Naš softver za upravljanje uređajima IW MC omogućuje ažuriranje i prosljeđivanje postavki uređaja, pravila sigurnosti, lozinki i certifikata te programskih datoteka skupini uređaja Canon diljem mreže. Tako vašem IT timu omogućuje uštedu dragocjenog vremena i pomaže sigurnost infrastrukture pisača održati ažuriranom.

OPSEŽNA REVIZIJA DOKUMENTA

Arhitekturu naših usluga za uredske dokumente moguće je unaprijediti naručivim opcijama za snimanje cjelovitog zapisa (tj. skeniranje i metapodaci zadatka) svih dokumenata obrađenih uređajima imageRUNNER ADVANCE DX.

USLUGE UPRAVLJANJA ISPISIVANJEM

Usluga upravljanja ispisivanjem tvrtke Canon kombinira inovativnu tehnologiju i softver s odgovarajućim uslugama kako biste dobili željeno iskustvo ispisivanja i rada s dokumentima bez povezanog uznemiravanja IT timova. Proaktivnim upravljanjem i kontinuiranim optimiranjem infrastrukture za ispisivanje i tijeka rada s dokumentima možemo vam pomoći u postizanju sigurnosnih ciljeva, uz optimiranje troškova i povećanje produktivnosti cijele tvrtke.

PRILAGOĐENI RAZVOJ

Imamo interni razvojni tim koji može predložiti i razviti prilagođeno rješenje za posebnu situaciju i jedinstvene zahtjeve.

KOLIKO JE SVEOBUH VATAN VAŠ PRISTUP SIGURNOSTI TVRTKE?

- Obuhvaćaju li vaša sigurnosna pravila i skupinu višefunkcijskih uređaja?
- Kako postižete pravovremeno i učinkovito ažuriranje infrastrukture za ispisivanje te primjenu poboljšanja i zakrpa za otklanjanje pogrešaka?
- Mogu li gosti ispisivati i skenirati bez izlaganja mreže opasnosti?
- Jesu li vaša pravila o donošenju vlastitih uređaja na posao sigurna i održiva u cijeloj skupini za ispisivanje?
- Ima li vaš IT tim dovoljno vremena za istraživanje sigurnosnih problema?
- Jeste li pravilno uravnotežili mjere sigurnosti i praktičnost za korisnike?



ZAŠTO CANON?



STRUČNOST

Integracija hardvera i softvera smanjuje potencijal za povrede sustava.



PARTNERSTVO

Klijentima pomažemo bolje poslovati jer znaju kako ćemo se **proaktivno suočiti** sa sigurnosnim prijetnjama.



USLUGA

Tim za sigurnost informacija klijenata također upravlja našom unutarnjom IT sigurnošću.

Razmatramo sve potencijalne prijetnje unutar i izvan vatrozida tvrtke.



INOVACIJE

Naši proizvodi i usluge **obuhvaćaju pametnije načine** za smanjenje vjerojatnih narušavanja sigurnosti informacija na minimum.



"Visoka preporuka"

u kategoriji za najbolji sigurnosni tim na natjecanju **SCA Awards Europe u 2017.** kojom se nagrađuje stručnost u kibernetičkoj sigurnosti.

Tvrtka Canon U.S.A. primila je dvije nagrade na **BLI PaceSetter Awards u 2017.** (sigurnost obrade slika u dokumentima i ispisivanje s mobilnih uređaja).

Canon Inc.

Canon.com

Canon Europe

canon-europe.com

Croatian edition

© Canon Europa N.V., 2019

Canon d.o.o.

Kovinska 4a

10090 Zagreb

Hrvatska

Tel: + 385 1 5579 843

Fax: + 385 1 5579 856

canon.hr