



# MEGVÉDJÜK IRODÁJÁT

**Canon**



**McAfee**  
PROTECTED

Canon uniFLOW Online  
Outstanding Cloud Output-Management Solution



# MENNYIRE VANNAK BIZTONSÁGBAN IRODÁJÁBAN AZ INFORMÁCIÓK?

Napjaink vállalatai nagyban támaszkodnak a különböző információkra, és hálózati technológiák, folyamatok, emberek és szervezetek határokra átívelő, összetett hálózatát hozzák létre. A digitális átalakulás korában új és rugalmas munkahelyi gyakorlatok nyernek teret, amelyek átalakítják az irodát és az információ keletkezésének, megosztásának és fogyasztásának a folyamatát. Az összetett munkakörnyezetekben az adatvédelem minden eddiginél nehezebb feladattá vált. A cégek többsége kifinomult tűzfalakba, naprakész vírusirtókba, biztonsági szoftverekbe és más technológiákba fektet be. Ugyanakkor gyakran nem ismerik fel, hogy e védelmet az irodai nyomtatókra is ki kell terjeszteni, ezért sebezhetőbbek maradnak, mint gondolnák.



## GONDOLJON NYOMTATÓIRA

A modern, többfunkciós nyomtatók (MFP-k) olyan nagy teljesítményű eszközökké váltak, amelyek a számítógépekhez és szerverekhez hasonlóan operációs rendszerekkel, nagy merevlemezekkel, illetve hálózati és internetkapcsolattal rendelkeznek, és amelyeket naponta több felhasználó használ hatalmas mennyiségű, üzleti szempontból kritikus jelentőségű dokumentumok feldolgozására.



## MIK A KOCCÁZATOK?

- Jogosulatlan felhasználók juthatnak a védtelen MFP-ken tárolt bizalmas információkhoz
- Nyomtatási infrastruktúrájának elérhetősége a nem megfelelő működtetés nyomán veszélybe kerülhet
- Kártékony, jogosulatlan személyek szerezhetnek hozzáférést hálózatához és hajthatnak végre további támadásokat a nyomtatón keresztül
- A nyomtatást követően a kimeneti tálcán felejtett bizalmas dokumentumokhoz mások is hozzáférhetnek
- Összekeveredhetnek a különböző felhasználókhöz tartozó nyomtatott anyagok
- Gépelési hiba miatt rossz címzethez kerülhetnek a faxolt vagy e-mailen elküldött dokumentumok
- Hekkerek foghatják el a nyomtatási vagy szkennelési célra elküldött adatokat
- A nyomtatók hanyag kezelése miatt adatok veszhetnek el azok lízingidőszakának lejártakor.

„A nagy mennyiségű adatot kezelő irodáknak érdemes átvenni az információvédelem terén felállított alapvető mércéket. A nyomtató ma már nem egy egyszerű készülék, hanem egy olyan szerver, amely történetesen nyomtat is.”

(CISO, Publicis Groupe)

# BIZTOSÍTSA VÁLLALATA NYOMTATÁSI MEGOLDÁSAIT

## Biztonság és adatvédelem a tervezésnek köszönhetően

Amikor ügyfeleink számára technológiákat, termékeket és szolgáltatásokat tervezünk vagy választunk, azok ügyfeleink környezetére gyakorolt potenciális adatvédelmi hatásokat is figyelembe vesszük. Ezért többfunkciós irodai nyomtatóinkat számos különböző alapvető és választható biztonsági funkcióval látjuk el, így ezek a vállalat méretétől függetlenül garantáltan megfelelő szintű biztonságot nyújtanak a következők tekintetében:



KÉSZÜLÉKEK

HÁLÓZATOK

DOKUMENTUMOK

AZ ÖN VÁLLALATA



### NEMZETKÖZILEG ELISMERT SZABVÁNYOK ÉS TANÚSÍTVÁNYOK

ImageRUNNER ADVANCE többfunkciós nyomtatóinkat rutinszerű ellenőrzéseknek vetjük alá, és az IEEE2600 papíralapú eszközök biztonságára vonatkozó szabványok előírásainak megfelelő, közös szempontrendszer módszert alkalmazva hitelesítjük azokat.



### BIZTONSÁGI VIZSGÁLAT

A Canon vállalaté az egyik legszigorúbb vizsgálati rendszer az irodai eszközök ágazatában. A termékportfóliónkba választott technológiákat olyan magas szintű vizsgálatoknak vetjük alá, amelyeket saját fejlesztéseinkkel szemben is megkövetelnénk.

Irodai és üzleti felhasználású innovatív nyomtatási és információkezelési megoldások fejlesztése terén piacvezető vállalként a Canon ügyfeleivel együttműködve segít egy olyan átfogó információvédelmi megoldás elsajátításában, amely a szélesebb információs környezet részeként az irodai technológiánk alkalmazásának biztonsági következményeit is figyelembe veszi.



# VÉDJE MEG ESZKÖZEIT

## Átfogó védelem tárgyi eszközeinek



### FELHASZNÁLÓHITELESÍTÉSI MEGOLDÁSOK

Védje meg eszközeit a jogosulatlan hozzáféréstől a felhasználóhitelesítés általi hozzáférés-szabályozással. Ezzel azt is elérheti, hogy a felhasználók gyorsabban hozzáférjenek az általuk preferált beállításokhoz és nyomtatási feladatokhoz, miközben növeli az elszámoltathatóságot és az ellenőrzést. Hivatali nyomtatóinkat egy rugalmas beléptetőrendszerrel, a uniFLOW Online Express megoldással szereljük fel, amelynek használatával az eszközön létrehozott felhasználói adatbázis használatával felhasználói hitelesítés, míg az Active Directory vagy a uniFLOW szerveren tárolt adatok alapján tartományhitelesítés végezhető el. Ennek köszönhetően vállalata felügyelni tudja az eszközhozzáféréseket, miközben megfelelő egyensúlyt valósít meg a felhasználói kényelem és a biztonság között.



### ADATVÉDELEM A MEREVLEMEZEN

A többfunkciós nyomtatón tárolt nagy mennyiségű adat számára folyamatos védelmet kell biztosítani – a nyomtatásra váró feladatoktól a szkennelt adatokon és a címjegyzéken keresztül a naplózott aktivitásokig és a feladatelőzményekig. A Canon eszközei többféle lehetőséget is kínálnak adatai védelmére az eszköz élettartamának különböző szakaszaiban, ezzel biztosítva az adatok titkosságának megőrzését, sértetlenségét és elérhetőségét.



### HOZZÁFÉRÉS-KEZELŐ RENDSZER

Ez a szolgáltatás az eszközfunkciókhoz való hozzáférés részletes szabályozását teszi lehetővé. A rendszergazdák használhatják a standard szerepköröket, vagy egyedi szerepeket is létrehozhatnak, amelyekhez a kívánt hozzáférési jogosultságokat állíthatják be. Bizonyos felhasználóktól például megvonható a dokumentumok másolásának vagy elküldésének a lehetősége.



### BIZTONSÁGI SZABÁLYZAT BEÁLLÍTÁSA

A legújabb imageRUNNER ADVANCE DX eszközök „biztonsági szabályzat” funkcióval is rendelkeznek, amely révén a rendszergazdák minden biztonsággal kapcsolatos beállítást egy menüben érhetnek el és szerkeszthetnek, mielőtt még a készüléken alkalmaznák azokat. Az alkalmazást követően az eszköz használata, valamint a beállítások módosítása kizárólag a szabályzatnak megfelelően történhet. Ha a biztonsági szabályzatot külön jelszóval védi, ahhoz kizárólag a felelős IT biztonságtechnikai szakértő férhet hozzá, ami magasabb szintű ellenőrzés és megbízhatóság elérését teszi lehetővé.



### ESZKÖZADMINISZTRÁCIÓS ELLENŐRZÉS

Az olyan eszközkonfigurációk, mint a hálózati beállítások és más szabályozási lehetőségek, csak azon felhasználók számára érhetők el, akik rendszergazdai jogosultságokkal rendelkeznek, ezzel elkerülve a szándékos vagy véletlen módosítások kockázatát.



### MEGELŐZŐ BIZTONSÁG

Az imageRUNNER ADVANCE DX termékek számos olyan biztonsági beállítást kínálnak, amelyekkel megóvhatja nyomtatóit a támadásoktól. Az indításkori rendszerellenőrzés biztosítja a készülék sérthetlenségét a rendszer betöltését követően, miközben a McAfee Embedded Control a készülék teljes élettartama alatt biztosítja annak sérthetlenségét, megakadályozva, hogy a programokon illetéktelen módosításokat végezzenek vagy jogosulatlan programokat futtassanak annak futási ideje alatt. A Syslog-adatok ezen kívül valós idejű biztonsági állapotadatokat szolgáltatnak az eszközről, valamint felügyeleti funkciókat (az adatok megfelelő, külső féltől származó SIEM-rendszer által olvashatók).





## MENNYIRE VANNAK BIZTONSÁGBAN AZ ESZKÖZEI?

**1**

Eszközei meg vannak osztva és nyilvános helyen vannak elhelyezve?

**2**

Hozzáférhetnek a felhasználók nem biztonságos módon az eszközhöz?

**3**

Érvényben vannak az eszköz merevlemezen tárolt információk megővésére szolgáló intézkedések?

**4**

Az eszköz beállításait jogosulatlan felhasználók is módosíthatják?

**5**

Belegondolt már eszköze életciklusába és biztonságos lecserélésébe?

### A MEREVLEMEZ TITKOSÍTÁSA

ImageRUNNER ADVANCE DX eszközeink a merevlemezen található valamennyi adatot titkosítják, ezzel javítva azok biztonságát. Az adattitkosításért felelős biztonsági chip megfelel az Egyesült Államok által megfogalmazott FIPS 140-2 2-es szintű biztonsági szabvány által támasztott követelményeknek, továbbá az Egyesült Államok és Kanada által létrehozott Cryptographic Module Validation Program (CMVP), valamint a japán Japan Cryptographic Module Validation Program (JCMVP) szerinti tanúsítvánnyal is rendelkezik.

### A MEREVLEMEZ TÖRLÉSE

Egyes adatok, mint például a másolt vagy szkennelt képek vagy a számítógépről nyomtatott dokumentumok adatai, csak átmenetileg vannak jelen a merevlemezen, a művelet elvégzése után törlődnek. Annak érdekében, hogy biztosan ne maradjon semmilyen adat az eszközön, olyan

merevlemezzel szereljük fel őket, amely a munkafolyamat részeként lehetőséget ad ezen adatok rutinszerű törlésére.

### VALAMENNYI ADAT ÉS BEÁLLÍTÁS INICIALIZÁLÁSA

A merevlemez cseréjekor vagy eltávolításakor bekövetkező adatvesztés elkerülése érdekében felülírhatja a merevlemezen található dokumentumokat és adatokat, és visszaállíthatja a készülék beállításait az alapértelmezett értékekre.

### MEREVLEMEZ TÜKRÖZÉSE\*

A vállalatoknak lehetőségük van az eszközök merevlemezen tárolt adatokat biztonsági mentés segítségével egy másik merevlemezre menteni. A tükrözés végeztével az adatok mindkét merevlemezen teljesen titkosítva lesznek.

\*Opcionális a kiválasztott modell esetén. Az irodai nyomtatási portfólió funkcióira és beállításaira vonatkozó további információkért vegye fel a kapcsolatot a Canon képviselőjével.



# BIZTOSÍTSA HÁLÓZATÁT



## NYOMTATÓJA VESZÉLYBE SODORHATJA HÁLÓZATÁT?

- Hálózati csatlakozói megtámadhatók?
- Tudnak a vendégek anélkül nyomtatni és szkennelni, hogy veszélybe sodornák a hálózatot?
- A saját eszközök használatára vonatkozó irányelvek biztonságosak és fenntarthatóak?
- A számítógép és a kimeneti eszköz közötti nyomtatási adatfolyamok titkosítottak?
- Biztonságban vannak az úton lévő nyomtatási és szkennelési adatok?

# A Canon biztonsági megoldások egész sorát kínálja, amelyekkel megvédheti hálózatát és adatait a belső vagy külső támadásoktól.

## IP- ÉS MAC-CÍM SZŰRÉSE

Védje hálózatát a jogosulatlan hozzáférésektől: csak adott IP-címmel vagy MAC-címmel rendelkező eszközök esetén engedélyezze a bejövő és kimenő kommunikációt.

## PROXY SZERVER KONFIGURÁCIÓJA

Állítson be proxy-kiszolgálót a kommunikáció kezelésére és a hálózaton kívüli eszközökkel való kapcsolattartásra.

## IEEE 802.1X HITELESÍTÉS

A jogosulatlan hálózati hozzáférés egy LAN-switch segítségével blokkolható, amely csak olyan kliensz eszközöknek enged hozzáférést, amelyek a hitelesítő szerver szerint jogosultak.

## IPSEC KOMMUNIKÁCIÓ

Az IPsec kommunikáció megakadályozza, hogy harmadik felek elfogják vagy manipulálják az IP-hálózaton keresztül továbbított IP-csomagokat.

Használjon titkosított TLS kommunikációt a rosszindulatú keresések, az átverések, valamint a készülék és a többi eszköz (pl. számítógép) között megosztott adatok módosításának a megakadályozása érdekében.

## CSATLAKOZÓ-ELLENŐRZÉS

Konfigurálja csatlakozóit a biztonsági szabályzatnak megfelelően.

## AUTOMATIKUS REGISZTRÁCIÓ HITELESÍTÉSE

Ezzel a funkcióval a biztonsági hitelesítések fenntartásának a költsége drámai mértékben csökkenthető. Az ipari technológiát használva a rendszergazda automatikusan frissítheti és kiadhatja a hitelesítéseket, gondoskodva ezzel a biztonsági szabályzat folyamatos betartásáról.

## NAPLÓZÁSOK ELLENŐRZÉSE

Többféle naplózási móddal ellenőrizheti eszköze aktivitását, a blokkolt kommunikációs kéréseket is ideértve.

## WI-FI DIRECT

Anélkül engedélyezheti a peer-to-peer kapcsolatot a mobilnyomtatáshoz, hogy a mobil eszköznek csatlakoznia kellene a hálózatához.

## ADATOK TITKOSÍTÁSA AZ ESZKÖZRE TÖRTÉNŐ KÜLDÉS, ILLETVE A FOGADÁS SORÁN

Ez a beállítás titkosítja a számítógépről a többfunkciós nyomtató felé küldött adatokat. Az univerzális biztonsági funkciók engedélyezésével a PDF-formátumú szkennelt adatok is titkosíthatók.

## MOBIL VENDÉGNYOMTATÁS

A biztonságos hálózati nyomtatást és szkennelést biztosító szoftverünk külső feladatküldési útvonalat biztosít az e-mailen, interneten és mobilalkalmazáson keresztül érkező feladatok számára, így védelmet nyújt a mobil és vendégnyomtatások gyakori biztonsági kockázata ellen. Ezzel minimálisra csökken a támadás esélye, mert az MFD biztonságos forráshoz kapcsolódik.

## KETTŐS HÁLÓZAT

A legújabb technológia mostantól kettős hálózati lehetőséget biztosít: míg az elsődleges hálózat mindig vezetékes lesz, a másodlagos vonal a továbbiakban vezeték nélküli vagy vezetékes is lehet a hálózatok biztonságosabb elkülönítése érdekében.





# VÉDJE MEG DOKUMENTUMAIT

Minden vállalatnál vannak bizalmas dokumentumok, például szerződések, személyzeti bérszámfejtési adatok, ügyfeladatok, kutatási és fejlesztési tervek stb. Ha ezek a dokumentumok rossz kezekbe kerülnek, a következmények a hírnév csorbulásától a súlyos bírságokon át akár jogi lépésekig is terjedhetnek.

**A Canon számos olyan biztonsági megoldást kínál ügyfeleinek, amelyek megfelelő védelmet nyújtanak a bizalmas dokumentumok számára azok teljes életciklusa alatt.**



## A NYOMTATOTT DOKUMENTUMOK TITKOSSÁGA

### **Biztonságos nyomtatás**

A felhasználók nyomtatási PIN-kódot is beállíthatnak, így a dokumentum nyomtatása csak a helyes PIN-kód készüléken történő megadását követően indul meg. Ezzel lehetőség nyílik a felhasználó által bizalmasnak tartott dokumentumok védelmére.

### **Minden nyomtatási feladat leállítása**

Az imageRUNNER ADVANCE DX eszközökön a rendszergazda az összes elküldött nyomtatási feladatot leállíthatja, így a felhasználóknak először be kell jelentkezniük a nyomtatáshoz, ezzel is védve a nyomtatott anyagok titkosságát.



## DOKUMENTUMMÁSOLÁS VISSZASZORÍTÁSA ÉS MEGELŐZÉSE

### **Nyomtatás látható vízjelekkel**

Az illesztőprogramok látható jeleket tudnak nyomtatni az oldalakra, amelyek a dokumentum tartalma fölött vagy alatt jelennek meg. Ez felhívja a felhasználók figyelmét a dokumentum bizalmas voltára, így csökkentve a másolás esélyét.

### **Nyomtatás/másolás láthatatlan vízjelekkel**

A funkció használatakor az eszköz a dokumentumokat a háttérben elhelyezett rejtett szöveggel nyomtatja ki, amely másolásakor megjelenve a dokumentumon komoly elrettentő erővel bír.

### **Adatvesztés megelőzése vállalati szinten**

Az iW SAM Express és a uniFLOW egyesítésével tovább csökkentheti az adatvesztés kockázatát. Ennek a szerveralapú megoldásnak köszönhetően lehetővé válik a nyomtatóra érkező vagy onnan

### **Postaládák**

A nyomtatási feladatok vagy a szkennelt dokumentumok a későbbi felhasználás érdekében postaládákban is tárolhatók. A postaládák PIN-kóddal védhetők, ezzel biztosítva, hogy kizárólag a hozzárendelt tulajdonos tekinthesse meg a tárolt anyagot. Ennek köszönhetően a készülék védelmet igénylő, de gyakran használt dokumentumok tárolására is alkalmas (pl. űrlapok).

### **uniFLOW biztonságos nyomtatás\***

A uniFLOW MyPrintAnywhere biztonságos nyomtatással a felhasználók az univerzális illesztőprogramot használva küldhetik el a nyomtatási feladatokat, és a hálózathoz csatlakoztatott bármelyik nyomtatón kinyomtathatják azokat.

távozó dokumentumok rögzítése és archiválása, valamint a dokumentumban szereplő szövegek és jellemzők elemzése és értelmezése a biztonsági kockázatok kiszűrése érdekében.

### **A dokumentum eredetének visszakövetése\***

A beágyazott kód segítségével a dokumentum egészen a forrásáig visszakövethető.



## MENNYIRE VANNAK BIZTONSÁGBAN DOKUMENTUMAI?

1

Hozzáférhetnek jogosulatlan felhasználók a nyomtatókon levő bizalmas dokumentumokhoz?

2

A megosztott eszközön keresztülmenő összes felhasználói dokumentum titkosságát biztosítani tudja?

3

Vissza tudja követni a dokumentum forrását?

4

El tudna sétálni valaki a nyomtatótól bizalmas dokumentumokkal a kezében?

5

El tudja kerülni az eszközről való dokumentumküldéskor előforduló gyakori hibákat?



### ELLENŐRIZZE A DOKUMENTUMOK KÜLDÉSÉT ÉS FAXOLÁSÁT

#### A címzettek korlátozása

Az információszivárgás kockázatának csökkentése érdekében a rendszergazdák korlátozhatják a címzetteket azon címekre, amelyek szerepelnek a címjegyzékben, az LDAP-szerveren, továbbá a bejelentkezett felhasználók körére és bizonyos tartományokra.

#### Címek automatikus kitöltésének letiltása

Az e-mail-címek automatikus kitöltésének letiltásával megakadályozhatja a dokumentumok rossz címre küldését.

#### Címjegyzék védelme

Az eszköz címjegyzékéhez PIN-kódot állíthat be, így megakadályozhatja, hogy jogosulatlan felhasználók módosítsák annak tartalmát.

#### Faxszám megerősítése

Előírhatja a felhasználók számára, hogy küldés előtt kétszer írják be a faxszámot – ily módon megakadályozható, hogy a dokumentumok rossz címzethez kerüljenek.

#### A beérkező faxok titkossága

Állítsa be a készüléken, hogy a dokumentumokat nyomtatás nélkül kívánja tárolni a memóriában. A beérkező faxok titkosságát PIN-kódok használatával, illetve olyan feltételek beállításával is megőrizheti, amelyek hatására a rendszer egy bizalmas postaládába helyezi a faxot.



### DOKUMENTUMOK EREDETÉNEK ÉS HITELESSÉGÉNEK ELLENŐRZÉSE DIGITÁLIS ALÁÍRÁSOKKAL

#### Eszközalírás

Egy kulcs és egy igazolási mechanizmus használatával a PDF- vagy XPS-formátumú szkennelt dokumentumon eszközalírás helyezhető el. A címzett ennek alapján könnyedén ellenőrizheti a dokumentum eredetét és hitelességét.

#### Felhasználói aláírás\*

Ez a beállítás lehetővé teszi a felhasználók számára, hogy egy hitelesítésszolgáltató által megadott egyedi digitális felhasználói aláírással ellátva küldjenek PDF- vagy XPS-fájlokat. Így a címzett azonosítani tudja, melyik felhasználó írta alá a dokumentumot.



### SZABÁLYZATOK ALKALMAZÁSA AZ ADOBE LIFECYCLE MANAGEMENT ES INTEGRÁLÁSÁVAL

A felhasználók védelemmel láthatják el a PDF-fájlokat, továbbá a dinamikus szabályzatok segítségével szabályozhatják a hozzáférési és felhasználási jogokat, ezzel védve az érzékeny és nagy értékű adatokat a véletlenszerű vagy rosszdindulatú megosztással szemben. A

biztonsági szabályzatok szerverszintűek, tehát a jogok azt követően is módosíthatók, hogy a fájl kiosztották. Az imageRUNNER ADVANCE DX sorozat az Adobe® ES integrációjához is konfigurálható.

\*Opcionális. Az irodai nyomtatási portfólió funkcióira és beállításaira vonatkozó további információkért vegye fel a kapcsolatot a Canon képviselőjével.



# VÁLLALATI INFORMÁCIÓ- BIZTONSÁG

A Canon átfogó módon tud hozzájárulni szervezete adatvédelmi intézkedéseéhez.

## **A RÖGZÍTÉSI ÉS KÜLDÉSI MŰVELETEK TELJES ELLENŐRZÉSE**

Moduláris kimenetkezelési szoftverünkkel a vállalkozások biztonságosan megoszthatják hálózati eszközeiket, így biztonságosan nyomtathatnak a kimenetkezelési kiszolgálóhoz kapcsolódó összes nyomtatón. A mobilfelhasználókat egy központilag vezérelt szolgáltatás támogatja, amely segítségével mind a belső, mind a vendégfelhasználók biztonságosan hozzáférhetnek a nyomtatóhoz mobileszközeikről.

A vállalati rögzítési igények terén pedig a szkennelőmodul képes rögzíteni, tömöríteni és átalakítani a dokumentumokat, majd eljuttatni azokat a többfunkciós eszközről a különböző célállomásokra, köztük akár felhőalapú rendszerekbe. Ezenfelül a felhasználó biztonságosan a legmegfelelőbb nyomtatóra továbbítja a nyomtatási munkákat, így optimalizálva az egyes dokumentumok nyomtatási költségét. Az általunk kínált megoldás a vállalat egészében képes javítani a dokumentumok biztonságát, emellett a dokumentumkövetési megoldással teljesen átláthatóvá teszi a felhasználók, az eszközök és az osztályok tevékenységeit.

## **KÖZPONTI FLOTTAKEZELÉS**

IW MC eszközkezelő szoftverünk lehetővé teszi az eszközbeállítások, a biztonsági szabályzatok, a jelszavak és a tanúsítványok használatát, valamint funkcióinak köszönhetően a firmware-t a hálózathoz kapcsolódó összes Canon-eszközön egyszerre lehet frissíteni. Ezzel értékes időt spórol meg IT-csapatának, és segít naprakészen tartani nyomtatási infrastruktúrájának biztonsági rendszerét.

## **ÁTFOGÓ DOKUMENTUMVIZSGÁLAT**

Irodai dokumentumszolgáltatási rendszerünket rendelhető opciókkal még tovább fejlesztheti, így az imageRUNNER ADVANCE DX eszközökön átfutó valamennyi dokumentum teljes rekordját (tehát a szkennelt anyagot és a feladat metaadatait egyaránt) rögzítheti.

## **FELÜGYELT NYOMTATÁSI SZOLGÁLTATÁSOK**

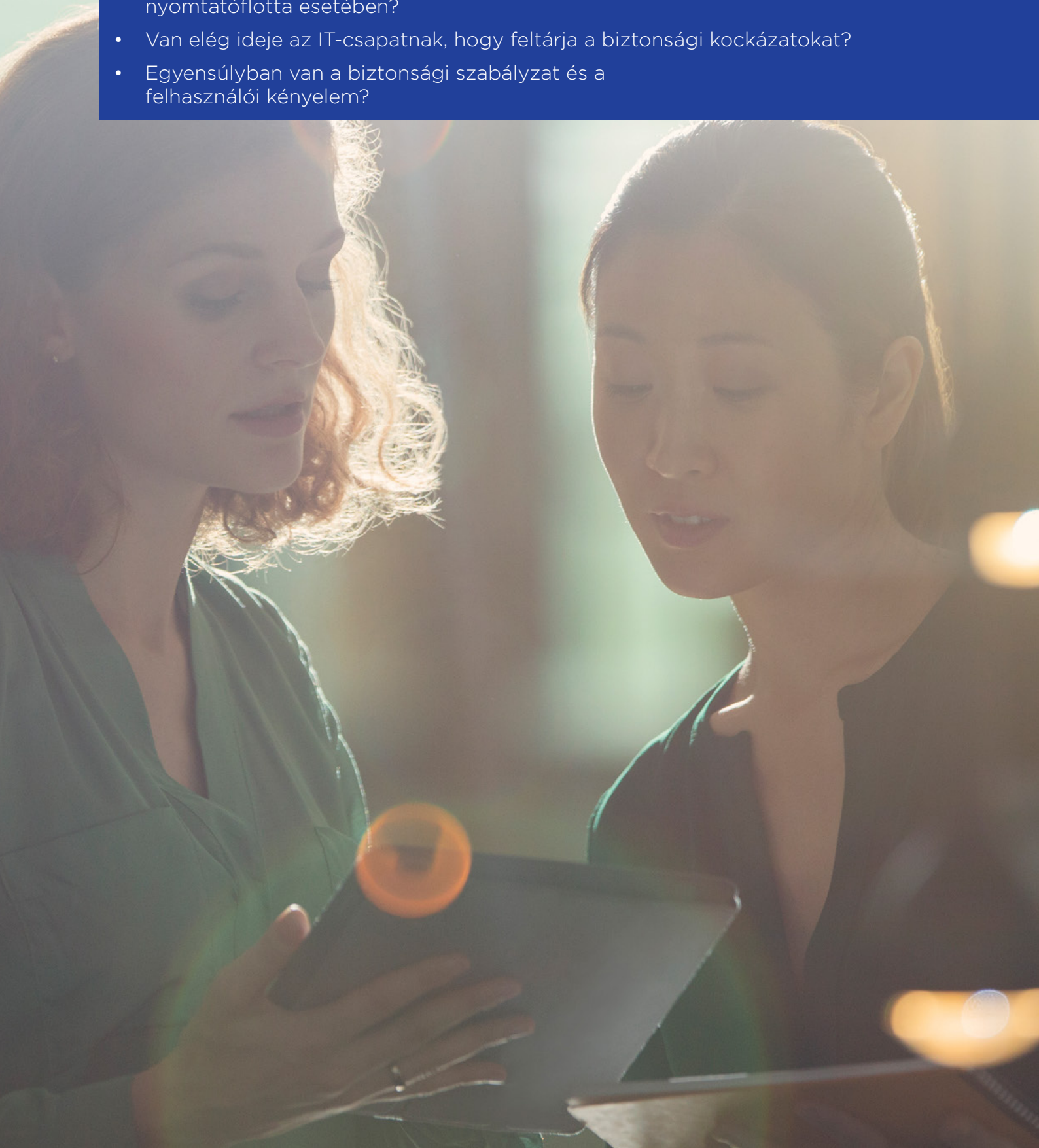
A Canon MPS az innovatív technológiai megoldásokat és szoftvereket kiváló szolgáltatásokkal kombinálja, így az IT-csapat további terhelése nélkül képes garantálni az Ön igényeinek megfelelő nyomtatási és dokumentumkezelési élményt. Nyomtatási infrastruktúrájának és dokumentum-munkafolyamatainak proaktív kezelésével és folyamatos optimalizálásával segítünk Önnek elérni biztonsági célkitűzéseit, mindezt a vállalati költségek csökkentése és a termelékenység növelése mellett.

## **EGYEDI FEJLESZTÉS**

Házon belüli fejlesztőcsapatunk az Ön egyedi helyzetének és igényeinek megfelelő egyedi megoldást is ki tud alakítani.

## MENNYIRE ÁTFOGÓ A VÁLLALAT BIZTONSÁGI MEGKÖZELÍTÉSE?

- A biztonsági szabályzat a többfunkciós eszközök flottájára is kiterjed?
- Hogyan éri el, hogy a nyomtatási infrastruktúra naprakész legyen, valamint hogy a bővítések és hibajavítások időben és hatékonyan meg legyenek valósítva?
- Tudnak a vendégek anélkül nyomtatni és szkennelni, hogy veszélybe sodornák a hálózatot?
- Biztonságos és fenntartható a saját eszköz használatára vonatkozó irányelv a nyomtatóflotta esetében?
- Van elég ideje az IT-csapatnak, hogy feltárja a biztonsági kockázatokat?
- Egyensúlyban van a biztonsági szabályzat és a felhasználói kényelem?



# MIÉRT ÉRDEMES A CANON TERMÉKEIT VÁLASZTANI?



## SZAKÉRTELEM

A **merevlemez- és szoftverintegráció** csökkenti a rendszer jogosulatlan használatának esélyét.



## PARTNERI KAPCSOLAT

Segítünk ügyfeleinknek, hogy sikerebben végezhesék tevékenységüket, annak tudatában, hogy **előrelátóan szállunk szembe az adatbiztonsági fenyegetésekkel.**



## SZOLGÁLTATÁS

Ugyanaz **az információbiztonsági csapat** kezeli saját belső IT biztonsági rendszerünket, mint az ügyfeleinkét.

A vállalat tűzfalán belüli és azon túli minden potenciális veszélyforrást számba veszünk.



## INNOVÁCIÓ

Termékeink és szolgáltatásaink **intelligens módszereket alkalmaznak** a lehetséges információbiztonsági kockázatok minimalizálása érdekében



„Erősen javasolt” az információbiztonsági szakértelmet elismerő **2017 SCA Awards Europe** legjobb biztonsági csapat kategóriájában.

A Canon U.S.A. két **BLI PaceSetter díjat kapott 2017-ben** (Dokumentumleképezés-biztonság és Mobilnyomtatás).

**Canon Inc.**  
Canon.com

**Canon Europe**  
Canon-europe.com

Hungarian edition  
© Canon Europa N.V., 2019

**Canon Hungária Kft.**  
1031 Budapest,  
Graphisoft Park 1.  
(Záhony utca 7.)  
Telefon: (+361) 2375904  
Fax: (+361) 2375901  
canon.hu

**Canon**

**McAfee**  
PROTECTED