



ÍGY VÉDJE IRODÁJÁT

Canon



MENNYIRE VANNAK AZ INFORMÁCIÓK BIZTONSÁGBAN AZ ÖN IRODÁJÁBAN?

A mai vállalkozások nagyban támaszkodnak az információkra: az egymással összekapcsolt technológiák, folyamatok, emberek és szervezetek összetett hálózatait hozzák létre, amelyek az országhatárokon is átívelnek. Új, agilis munkavégzési formák bukkannak fel, átformálva az irodát és az emberek információalkotási, -megosztási és -fogyasztási módját. Az adatok biztonságáról minden eddigénél nehezebb gondoskodni ebben a bonyolult környezetben, a legtöbb vállalkozás pedig kifinomult technológiákba – például áthatolhatatlan tűzfalakba, naprakész vírusvédelmi rendszerbe, biztonsági szoftverekbe és egyebekbe – ruház be. Ugyanakkor gyakran elmulasztják felismerni, hogy ezt a védelmet az irodai nyomtatókra is ki kell terjeszteniük, ami sebezhetőbb helyzetbe hozza őket, mint azt gondolnák.



GONDOLJON A NYOMTATÓIRA!

A korszerű multifunkciós nyomtatók (MFP) olyan nagy teljesítményű eszközökké fejlődtek, amelyek a számítógépekhez és szerverekhez hasonlóan operációs rendszerrel és óriási merevlemezekkel rendelkeznek, hálózathoz és az internethez csatlakoztatják őket, a felhasználók pedig közösen veszik igénybe azokat, hogy nap mint nap nagyszámú, üzleti szempontból döntő jelentőségű dokumentumot dolgozzanak fel a segítségükkel.



MILYEN KOCKÁZATOKKAL KELL SZÁMOLNI?

- Illetéktelen felhasználók is megtekinthetik a védelem nélküli multifunkciós készülékeken tárolt érzékeny információkat.
- A helytelen üzemeltetés veszélyeztetheti a nyomtatási infrastruktúra rendelkezésre állását.
- Rosszindulatú kívülállók a nyomtatón keresztül hozzáférést szerezhetnek a hálózathoz, majd ezt kihasználva további támadásokat indíthatnak.
- A nyomtatás után a gyűjtőtálcában felejtett bizalmas dokumentumok tartalma illetéktelenek előtt válhat ismertté.
- Különböző felhasználókhoz tartozó nyomtatott anyagok keveredhetnek össze.
- Gépelési hibák miatt helytelen címzettek kaphatják meg a faxon vagy e-mailben küldött dokumentumokat.
- A nyomtatási vagy szkennelési adatok a küldés során hackerek kezébe kerülhetnek.
- Haszonbérleti időtartamuk végén a nyomtatók gondatlan selejtezése miatt adatvesztés léphet fel.

„Az információbiztonság alapvető intézkedéseit igencsak megéri bevezetni az irodában, ahol valószínűleg óriási adatmennyiségeket kezelnek. A nyomtató napjainkban többé már nem egy ostoba gépezet, hanem egy szerver, amely történetesen papírra nyomtat.”

(A Publicis Groupe információbiztonsági igazgatója)

BIZTONSÁGOS NYOMTATÁSI MEGOLDÁSOK VÁLLALKOZÁSA SZÁMÁRA

Beépített biztonság és adatvédelem

Amikor technológiákat, termékeket és szolgáltatásokat tervezünk vagy választunk ügyfeleink számára, akkor azt a lehetséges információbiztonsági hatást is figyelembe vesszük, amelyet azok az ügyfél környezetére gyakorolhatnak. Multifunkciós irodai nyomtatóink épp ezért a biztonsági funkciók széles választékával vannak felszerelve – alap- és opcionális kivitelben egyaránt –, amely mérettől függetlenül minden vállalkozásnak lehetővé teszi a kívánt szintű védelmet, legyen szó:



ESZKÖZÖKRŐL



HÁLÓZATOKRŐL



DOKUMENTUMOKRŐL



AZ ÖN VÁLLALKOZÁSÁRÓL



NEMZETKÖZILEG ELISMERT SZABVÁNYOK ÉS TANÚSÍTVÁNYOK

Multifunkciós nyomtatókból álló imageRUNNER ADVANCE termékcsaládunk rendszeresen átesik a Common Criteria-módszertan szerinti, valamint a nyomtatott példányokat előállító eszközök biztonságára vonatkozó IEEE2600-szabványok követelményeinek megfelelő értékelésen és tanúsításon.



A BIZTONSÁG TESZTELÉSE

Az irodai berendezések ágazatában a Canon alkalmazza az egyik legszigorúbb biztonságtesztelési rendszert. A termékportfóliónkba beépített technológiák ugyanazon a rendkívül magas követelményeket támasztó tesztelési eljáráson mennek át, mint amelynek teljesítése saját vállalkozásunkkal szemben is elvárás.

A Canon az irodai és vállalati célközönségnek készülő innovatív nyomtatási és információkezelési megoldások fejlesztése terén iparági vezető céggént az ügyfelekkel együttműködve segíti az információbiztonság befogadó megközelítését meghonosítani a vállalkozásoknál, amely a szélesebb információs „ökoszisztéma” részeként veszi figyelembe irodai technológiánk biztonsági következményeit.



VÉDJE ESZKÖZÉT

Átfogó védelem fizikai eszközei számára



FELHASZNÁLÓAZONOSÍTÁSI MEGOLDÁSOK

Védje eszközét az illetéktelen használatlalt szemben a felhasználói hozzáférés szabályozásával, felhasználóazonosítás segítségével. A megoldás további előnye, hogy gyorsabb hozzáférést nyújt a felhasználóknak az általuk előnyben részesített beállításokhoz és nyomtatási feladatokhoz, miközben az elszámoltathatóságot és az ellenőrzést is fokozza. Az irodai nyomtatóink fel vannak szerelve az Universal Login Manager alkalmazással, amely egy rugalmas felhasználóazonosítási megoldás, amely a berendezésen létrehozott felhasználói adatbázis alapján teszi lehetővé a felhasználói, Active Directory- vagy uniFLOW-kiszolgálón keresztül pedig a tartományi hitelesítést. Mindez lehetőséget ad a vállalkozásoknak arra, hogy ne csupán felügyeljék az eszközök elérését, hanem a megfelelő egyensúlyt is megteremtsék a felhasználók kényelme és a biztonság között.



ELLENŐRZÖTT ESZKÖZFELÜGYELET

Az eszközkonfiguráció – így például a hálózati beállítások és az egyéb felügyeleti lehetőségek – csak a rendszergazdai jogosultságokkal rendelkező felhasználóknak érhető el, ami megakadályozza a szándékos vagy véletlen módosításokat.



HOZZÁFÉRÉS-KEZELŐ RENDSZER

Ez a szolgáltatás az eszközfunkciók aprólékos hozzáférés-felügyeletére ad módot. A rendszergazdák a sztenderd szerepkörök mellett személyre szabott beállításokat is használhatnak, megadva a hozzáférési jogok kívánt szintjét. Például bizonyos felhasználók számára letiltható a dokumentumok másolása vagy a küldési funkció használata.



A BIZTONSÁGI HÁZIREND BEÁLLÍTÁSA

A legújabb imageRUNNER ADVANCE készülékek biztonsági házirend kezelésére szolgáló funkcióval is el vannak látva, amelynek révén a rendszergazda a biztonsággal kapcsolatos beállítások mindegyikét egyetlen menüben érheti el, valamint a berendezésen való életbeléptetésük előtt elvégezheti azok szerkesztését is. Az életbelépést követően a berendezés használata és a beállítások módosítása kötelezően a házirend szerint történik. A biztonsági házirend külön jelszóval védhető, így a hozzáférés egy erre kijelölt IT-biztonsági szakemberre korlátozható, ami még magasabbra emeli a felügyelet és a biztonsági ellenőrzés szintjét.



A MEREVLEMEZEN LÉVŐ ADATOK VÉDELME

A többfunkciós nyomtató minden pillanatban nagy mennyiségű adatot tárol, amelynek gondoskodni kell a védelméről – a nyomtatásra váró feladatoktól kezdve, a fogadott faxokon és beolvasott adatokon át egészen a címjegyzékekig, tevékenységnaplókig és feladatelőzményekig. A Canon-eszközök számos módszert kínálnak az adatok védelmére az eszköz élettartamának bármely szakaszában, egyaránt gondoskodva az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséről.



MENNYIRE BIZTONSÁGOSAK AZ ESZKÖZEI?

1.

Eszközeit közösen használják, azok nyilvános területeken találhatók?

2.

A felhasználók biztonsági intézkedésekkel nem védett módon is hozzáférhetnek az eszközökhöz?

3.

Tettek lépéseket, hogy megvédjék az eszköz merevlemezén található információkat?

4.

Illetéktelen felhasználók is módosíthatják az eszköz beállításait?

5.

Mérlegelték már az eszköz élettartamát, valamint a biztonságos selejtezés lehetőségeit?

A MEREVLEMEZ TITKOSÍTÁSA

A biztonság fokozása érdekében imageRUNNER ADVANCE készülékeink a merevlemezre kerülő valamennyi adatot titkosítják. Az adattitkosításért felelős biztonsági chip megfelel az Egyesült Államok kormánya által bevezetett 2. szintű FIPS 140-2 biztonsági szabvány követelményeinek, tanúsítása pedig az Egyesült Államok és Kanada által kiépített kriptográfiai modul-érvényesítési program (CMVP), valamint a japán kriptográfiai modul-érvényesítési program (JCMVP) szerint történt.

A MEREVLEMEZ TÖRLÉSE

Egyes adatok – köztük a másolt vagy beolvasott képek, valamint a számítógépről kinyomtatott dokumentumok adatai – csupán ideiglenesen tárolódnak a merevlemezén, majd a művelet befejezését követően a nyomtató törli azokat. A hátramaradó adatok megőrzésének kiküszöbölésére készülékeink olyan merevlemezrel vannak felszerelve, amely a feladatfeldolgozás részeként felkínálja a hátramaradó adatok rendszeres törlésének lehetőségét.

MINDEN ADAT ÉS BEÁLLÍTÁS INICIALIZÁLÁSA

A merevlemez cseréje vagy leselejtezése során fellépő adatszivárgás megakadályozására a merevlemezén minden dokumentum és adat felülírható, a készülékbeállítások pedig visszaállíthatók a gyári alapértékekre.

A MEREVLEMEZ TÜKRÖZÉSE*

A vállalkozásoknak egy külön rendelhető merevlemez segítségével lehetőségük van a készülékük merevlemezén lévő adatokról biztonsági másolatot készíteni. A tükrözés végrehajtása során az adatok mindkét merevlemezén teljes körű titkosításon esnek át.

ELTÁVOLÍTHATÓ MEREVLEMEZKÉSZLET*

Ez az opció lehetővé teszi a merevlemez eltávolítását a berendezésből, hogy azt biztonságos tárolóhelyre vigyék, amíg a gép nincs használatban.

*Választható. A teljes irodai nyomtatási portfólióra jellemző funkciók és külön rendelhető opciók rendelkezésre állásáról Canon-képviselőjétől kaphat részletes tájékoztatást.



TARTSA BIZTONSÁGBAN HÁLÓZATÁT



NYOMTATÓJA VAJON KOCKÁZATOT JELENTHET HÁLÓZATÁRA NÉZVE?

- Nyitva hagyják a hálózati portokat, amelyek így védtelenek a támadással szemben?
- A vendégek anélkül végezhetnek nyomtatást és szkennelést, hogy ezzel veszélybe sodornák a hálózatot?
- A munkahelyi saját eszközhasználatra vonatkozó szabályzatok biztonságosak és támogathatók?
- A nyomtatási adatfolyamok titkosítottak a számítógép és a kimeneti eszköz között?
- Gondoskodnak a nyomtatás és szkennelés adatainak küldés közbeni védelméről?

A Canon biztonsági megoldások széles skáláját kínálja, amellyel a belső és külső támadásokkal szemben egyaránt biztonságban tudhatja hálózatát és adatait.

IP- ÉS MAC-CÍMEK SZŰRÉSE

Védje hálózatát a külső felek általi illetéktelen hozzáféréssel szemben úgy, hogy a bejövő és kimenő kommunikáció esetében is csupán a megadott IP- vagy MAC-címmel rendelkező eszközökkel engedélyezi a kommunikációt.

PROXYKISZOLGÁLÓ KONFIGURÁLÁSA

Állítson be egy proxyt, hogy a berendezése helyett az kezelje a kommunikációt, majd használja azt, amikor a hálózatán kívüli eszközökhöz csatlakozik.

IEEE 802.1X PROTOKOLL SZERINTI HITELESÍTÉS

Az illetéktelen hálózati hozzáférést egy olyan LAN-kapcsoló tiltja le, amely kizárólag a hitelesítési kiszolgáló által engedélyezett eszközöknek biztosít elérési jogosultságokat.

IPSEC-KOMMUNIKÁCIÓ

Az IPSec-kommunikáció megakadályozza, hogy külső felek elfogják vagy módosítsák az IP-hálózaton keresztül továbbított IP-csomagokat.

TLS-titkosítású kommunikáció igénybevételel meggátolhatja a berendezés és az egyéb eszközök, például számítógépek között küldött adatok elemzését, meghamisítását és módosítását.

PORTFELÜGYELET

Végezze el a portok konfigurálást a biztonsági házirend beállítása keretében.

LOGOK NAPLÓZÁSA

A különféle logok lehetővé teszik a készülékkel folytatott tevékenységek, így többek között a letiltott kommunikációs kérélmek megfigyelését.

WI-FI DIRECT

A mobilnyomtatás érdekében engedélyezheti az egyenrangú (peer-to-peer) kapcsolatot, így a mobil eszköznek nem szükséges hozzáférnie az Ön hálózatához.

ADATTITKOSÍTÁS A KÉSZÜLÉK ÉS MÁS ESZKÖZÖK KÖZÖTTI ADATKÜLDÉS SORÁN

Ez az opció titkosítja a felhasználó számítógépéről a multifunkciós nyomtatóra továbbított nyomtatási feladatokat. Az univerzális biztonsági funkciókészlet engedélyezésével a PDF formátumban beolvasott adatok is titkosíthatók.

VENDÉGEK ÁLTALI MOBILNYOMTATÁS

Biztonságos hálózati nyomtatás- és szkenneléskezelő szoftverünk úgy oldja meg a mobil- és vendégek általi nyomtatásban rejlő gyakori kockázatok kezelését, hogy külső feladatküldési útvonalakat biztosít e-mailen, weben és a Mobil alkalmazáson keresztül. Ez minimálisra csökkenti a támadási lehetőségeket azáltal, hogy biztonságos forrásokra korlátozza a multifunkciós készülék kezelését.



ÓVJA DOKUMENTUMAIT

Minden vállalkozás kezel érzékeny dokumentumokat, például szerződéseket, megállapodásokat, személyzeti bérjegyzék-információkat, ügyféladatokat, kutatás-fejlesztési terveket és egyébeket. Ha ezek a dokumentumok rossz kezekbe kerülnek, a következmények a hírnévromlástól kezdve, a súlyos pénzbírságokon át egészen a peres eljárásokig terjedhetnek.

A Canon biztonsági megoldások tárházát kínálja, amely teljes élettartamuk alatt képes gondoskodni érzékeny dokumentumaik védelméről.



A NYOMTATOTT DOKUMENTUMOK BIZALMAS KEZELÉSE

Védett nyomtatás

A felhasználó beállíthat egy PIN-kódot a nyomtatáshoz, hogy csak a helyes PIN-kód berendezésen való megadása után legyen végrehajtható a dokumentum nyomtatása. Ez lehetőséget ad a felhasználóknak a bizalmasnak vélt dokumentumok védelmére.

Az összes nyomtatási feladat várakoztatása

Az imageRUNNER ADVANCE termékcsaládban a rendszergazda kikényszerítheti az összes elküldött nyomtatási feladat felfüggesztését, hogy így védje valamennyi nyomtatott anyag bizalmas jellegét, így a felhasználóknak először be kell jelentkezniük ahhoz, hogy sor kerüljön a feladatok nyomtatására.

Postafiókok

A nyomtatási feladatok vagy a beszkenelt dokumentumok postafiókban tárolhatók, hogy később innen elérhetők legyenek. A postafiókok PIN-kóddal védhetők, amely biztosítja, hogy kizárólag a hozzájuk rendelt tulajdonos tekintheti meg a tartalmukat. A berendezés ezen biztonságos területe alkalmas a gyakran nyomtatni kívánt, ugyanakkor körültekintő kezelést igénylő dokumentumok (például űrlapok) tárolására.

Biztonságos nyomtatás a uniFLOW segítségével*

A uniFLOW MyPrintAnywhere biztonságos nyomtatással a felhasználók az általános illesztőprogramon keresztül küldik el a nyomtatási feladatokat, majd a nyomtatottakat a hálózat bármely nyomtatójánál begyűjthetik.



A DOKUMENTUMOK SOKSZOROSÍTÁSÁNAK MEGAKADÁLYOZÁSA VAGY MEGELŐZÉSE

Nyomtatás látható vízjelekkel

Az illesztőprogramok képesek látható jelzéseket (vízjelet) nyomtatni a lapokra, amelyek a dokumentum tartalma felett vagy mögött is megjeleníthetők. Ez megakadályozza a másolásukat azáltal, hogy felhívja a felhasználók figyelmét a dokumentum bizalmas jellegére.

Nyomtatás/másolás láthatatlan vízjelekkel

A beállítás engedélyezésekor a dokumentumok beágyazott, láthatatlan szöveggel nyomtathatók vagy másolhatók, amely a sokszorosítás esetén megjelenik a dokumentumon.

Dokumentumszkennelési zár*

Ez a beállítás rejtett kódot ágyaz a nyomtatott vagy másolt dokumentumokba, amely megakadályozza az engedélyezett funkcióval rendelkező berendezésen történő további sokszorosítást. A rendszergazda választhat, hogy ezt a védelmet minden feladatra kiterjeszti, vagy a felhasználók belátására bízza. A beágyazáshoz TL- vagy QR-kód használható.

A dokumentumok eredetének nyomkövetése*

A beágyazott kód révén a dokumentum eredete egészen annak forrásáig visszakövethető.

MENNYIRE BIZTONSÁGOSAK A DOKUMENTUMAI?

1.

Meg tudják akadályozni, hogy illetéktelen felhasználók a nyomtatónál hozzáférhessenek a bizalmas dokumentumokhoz?

2.

A közösen használt készülékek esetén minden felhasználói dokumentum esetében biztosítani tudják a bizalmasságot?

3.

Nyomon tudják követni a nyomtatott dokumentumok eredetét?

4.

Előfordulhat, hogy valaki elvigyen a nyomtatóból érzékeny dokumentumokat?

5.

Képesek megelőzni a gyakori hibákat a készülékről küldött dokumentumok esetében?



A DOKUMENTUMKÜLDÉS ÉS FAXOLÁS FELÜGYELETE

Címzettek korlátozása küldéskor

Az információszivárgás kockázatának csökkentése érdekében a rendszergazdák a címjegyzékben vagy az LDAP-kiszolgálón lévőkre, a bejelentkezett felhasználó címére vagy bizonyos tartományokra korlátozhatják a küldés céljából elérhető címzettek körét.

A címek automatikus kiegészítésének letiltása

Akadályozza meg a dokumentumok helytelen címzetteknek történő elküldését azáltal, hogy letiltja az e-mail-címek automatikus kiegészítését.

Címjegyzékvédelem

Állítson be egy PIN-kódot a készülék címjegyzékének illetéktelen felhasználói módosítások elleni védelmére.

Faxszámok megerősítése

Előzze meg a dokumentumok nem a kívánt címzetteknek történő elküldését úgy, hogy megköveteli a felhasználóktól a faxszám kétszer történő megadását a küldés előtt megerősítés céljából.

A fogadott faxok bizalmas kezelése

Beállíthatja a berendezést, hogy a dokumentumokat nyomtatás nélkül a memóriában tárolja. A fogadott faxdokumentumok bizalmas jellegét emellett azzal is védheti, hogy feltételeket alkalmaz a bizalmas beérkezett üzenetek tárolóhelyének megállapításához, valamint PIN-kódokat is beállíthat.



A DOKUMENTUMOK EREDETÉNEK ÉS HITELESSÉGÉNEK ELLENŐRZÉSE DIGITÁLIS ALÁÍRÁSOKKAL

Készülék-aláírás

A készülék-aláírás egy kulcs és egy tanúsítási mechanizmus segítségével PDF vagy XPS formátumú szkennelt dokumentumokra alkalmazható. Az aláírás révén a címzett nem csupán a dokumentum eredetét, hanem annak hitelességét is ellenőrizheti.

Felhasználói aláírás*

Ezzel a lehetőséggel a felhasználók hitelesítésszolgáltatótól beszerzett egyedi felhasználói digitális aláírással küldhetnek PDF- vagy XPS-fájlokat. Ezáltal a címzett ellenőrizni tudja, hogy mely felhasználó írta alá az általa kapott fájlt.



HÁZIRENDEK ALKALMAZÁSA AZ ADOBE LIVECYCLE MANAGEMENT ES-INTEGRÁCIÓ RÉVÉN

A felhasználók gondoskodhatnak a PDF-fájlok védelméről, valamint állandó, dinamikus házirendeket alkalmazhatnak a hozzáférés és a használati jogok felügyelete érdekében, amellyel megóvhatják az érzékeny és nagy értéket képviselő információkat a véletlen vagy

rosszindulatú szivárogtatással szemben. Mivel a biztonsági házirendek karbantartása kiszolgálói (server) szinten történik, így a jogok még a fájlok terjesztését követően is módosíthatók. Az imageRUNNER ADVANCE sorozat konfigurálható az Adobe® ES-integráció számára.

*Választható. A teljes irodai nyomtatási portfólióra jellemző funkciók és külön rendelhető opciók rendelkezésre állásáról Canon-képviselőjétől kaphat részletes tájékoztatást.



NAGYVÁLLALATI SZINTŰ ADATBIZTONSÁG

A Canon képes hozzájárulni az Ön szervezetében az információk átfogó védelméhez.



TELJES KÖRŰ FELÜGYELET A VÉGPONTTÓL VÉGPONTIG TARTÓ RÖGZÍTÉSI ÉS KIMENETI IGÉNYEK FELETT

Moduláris kimenetkezelési szoftverünk segítségével a vállalkozások élvezhetik a hálózati eszközök biztonságos megosztásának előnyeit, hiszen a kimenetkezelő kiszolgálóra csatlakozó nyomtatók bármelyikén biztonságosan elvégezhetik a feladatok nyomtatását. A mobilfelhasználókat egy központilag felügyelt szolgáltatás támogatja, ahol a belső és vendégfelhasználók egyaránt biztonságosan férhetnek hozzá a mobilkészülökekről végzett nyomtatáshoz. A nagyvállalati környezet szkennelési igényeihez a beolvasási modul biztosítja a dokumentumok rögzítését, tömörítését, átalakítását és terjesztését a többfunkciós készüléktől a célállomások széles választékára, többek között felhőalapú rendszerekbe is. Ugyanígy biztonságosan átirányíthatja a nyomtatási feladatokat a legmegfelelőbb nyomtatóra, amellyel minden egyes dokumentum esetében optimalizálhatja a nyomtatás költségét. Megoldásunk fokozza a dokumentumok biztonságát a vállalat egészében – ehhez teljes körű dokumentumköltség-figyelés is párosul, ami a tevékenységek teljes láthatóságát nyújtja felhasználó, készülék és részleg szerinti bontásban.



KÖZPONTOSÍTOTT ESZKÖZPARKKEZELÉS

IW MC készülékkezelési szoftverünk lehetővé teszi a készülékbeállítások, biztonsági házirendek, jelszavak és tanúsítványok – sőt, akár a firmware – frissítését és Canon-eszközparkon belüli terjesztését a hálózaton, ami értékes időt takarít meg az informatikai csapatnak, valamint segít naprakészen tartani a nyomtatási infrastruktúra védelmét.



ÁTFOGÓ DOKUMENTUMAUDITOK

Irodai dokumentumkezelési szolgáltatásokból álló architektúránk továbbfejleszthető olyan megrendelhető kiegészítőkkel, amelyek teljes nyilvántartást vezetnek (azaz a beolvasás mellett a feladat metaadatait is rögzítik) minden imageRUNNER ADVANCE készülékeken keresztül feldolgozott dokumentumról.



AZ ADATVESZTÉSSSEL SZEMBENI VÉDELEM INTEGRÁCIÓJA

A Canon lehetővé teszi adatvesztés-megelőzési stratégiájának kiterjesztését a nyomtatók hálózatára, amellyel, hogy az összes nyomtatási, másolási és szkennelési művelet adata számára is biztosítja a döntő fontosságú naplózást.



MENEDZSELT NYOMTATÁSI SZOLGÁLTATÁSOK

A Canon MPS az innovatív technológiát és szoftvereket a megfelelő szolgáltatásokkal egyesíti, hogy az informatikai csapatainak okozott járulékos bonyodalmak nélkül a kívánt nyomtatási és dokumentumkezelési élményt nyújthassa Önnek. Nyomtatási infrastruktúrájuk, valamint dokumentumkezelési munkafolyamataik proaktív kezelése és folyamatos optimalizálása révén segíthetünk elérni Önöknek biztonsági célkitűzéseiket, miközben a költségek optimalizálásáról és a termelékenység fokozásáról is gondoskodunk vállalkozásuknál.



EGYEDI FEJLESZTÉS

Házon belüli, fejlesztőkből álló csapatunk egyedi körülményeit figyelembe véve, vagy az egyéni követelményeinek megfelelő személyre szabott megoldást tud összeállítani és ajánlani Önnek.

MENNYIRE BEFOGADÓ AZ ÖNÖK VÁLLALATI BIZTONSÁGI MEGKÖZELÍTÉSE?

- Biztonsági házirendjük hatálya a multifunkciós készülékek eszközparkjára is kiterjed?
- Hogyan gondoskodnak a nyomtatási infrastruktúra naprakész állapotáról, valamint a fejlesztések és hibajavítások időben történő, hatékony alkalmazásáról?
- A vendégek anélkül végezhetnek nyomtatást és szkennelést, hogy ezzel veszélybe sodornák a hálózatot?
- A saját eszközhasználatra vonatkozó szabályzatok biztonságosak és támogathatók a teljes nyomtatóflottában?
- Informatikai csapatuknak elég ideje van a biztonsági problémák kivizsgálására?
- Megfelelő egyensúlyt teremtettek a biztonság szavatolása és a felhasználói kényelem között?



MIÉRT A CANON?



SZAKÉRTELEM

A **hardver- és szoftver-integráció** csökkenti a rendszerbiztonság megsértésének kockázatát.



PARTNERSÉG

Segítünk az ügyfeleknek üzletvitelük fejlesztésében – hiszen tudják azt, hogy **mi proaktív módon gondoskodunk az adatbiztonságot érintő fenyegetésekről.**



SZOLGÁLTATÁS

Az ügyfeleknek szolgáltatást nyújtó **információbiztonsági csapat** felügyeli saját belső informatikai biztonságunkat is.

A vállalati tűzfalon belüli és kívüli lehetséges fenyegetéseket egyaránt mérlegeljük.



INNOVÁCIÓ

Termékeink és szolgáltatásaink **intelligensebb módszerek bevonásával** minimalizálják a lehetséges információbiztonsági kockázatokat.



„Kimondottan ajánlaná” minősítés a legjobb biztonsági csapat kategóriában a **2017. évi európai SCA Awards díjátadón** – az elismerés a kiberbiztonsági szakértelemnek szól.

A Canon U.S.A. két **BLI PaceSetter Awards 2017** díjban is részesült (a dokumentumok képkalkotó technológiájának biztonsága és mobilnyomtatás kategóriában).

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

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Hungarian edition
© Canon Europa N.V., 2018