WorkForce Enterprise 2 és AM termékcsalád

Üzleti nyomtatók
Biztonságos megoldások

EPSON®

Védje a hálózati biztonságot, bárhol is nyomtat

Könnyű figyelmen kívül hagyni a fontos biztonsági intézkedéseket a vállalkozásában használt hálózati eszközökkel kapcsolatban. Talán még nem gondolt rá, de a többfunkciós nyomtatók (MFP-k), szkennerek és bármely más csatlakoztatott vagy hálózatba kapcsolt eszköz használata biztonsági kockázatot jelenthet.

Az otthoni és a hibrid munkavégzés térnyerése tovább növelte ezt a kockázatot. A Quocirca egyik tanulmányában[1] megállapították, hogy a szervezetek 56%-a tapasztalt már adatvesztést a nyomtatáshoz kapcsolódó biztonsági rés miatt, és 83%-uk tervezi növelni a nyomtatási biztonságra fordított kiadásait a következő évben. A szervezetek legfőbb aggodalmai a következők: az otthoni nyomtatás biztonságának garantálása (28%), a bizalmas vagy érzékeny dokumentumok nyomtatás elleni védelme (28%), valamint a nyomtatási infrastruktúrájukat fenyegető veszélyek és sebezhetőségek megértése (25%).

Mivel a nyomtatással kapcsolatos adatvédelmi incidensek átlagos költsége 953 000 EUR*, nem lehet ezeket félvállról venni.

Az Epson nyomtatóbiztonsággal kapcsolatos megközelítésének köszönhetően azonban ez a kockázat csökkenthető, függetlenül attól, hogy hol történik az üzleti célú nyomtatás.

A 3 legfontosabb nyomtatásbiztonsági kihívás

28%

A nyomtatás biztonsága távoli/otthoni környezetben

28%

Az érzékeny vagy bizalmas dokumentumok nyomtatás elleni védelme

25%

A nyomtatási infrastruktúra fenyegetéseinek és sebezhetőségének megértése

*A Quocirca által meghatározott 820 000 fontnyi összeg 953 000 euróra váltva, az xe.com 2025. július 7-i árfolyamán.

Az Epson biztonsági nyilatkozata

Biztonsági megközelítésünk kulcsa az eszközök hálózati képességeinek megerősítése. Annak érdekében, hogy az Epson eszközök biztonsága az egész életciklusuk alatt biztosított legyen, minden Epson WorkForce nyomtató három alapelvre épül:

1. A termékbiztonság a minőség alapja
2. A biztonsággal kapcsolatos információkat és ismereteket aktívan megosztjuk, így Ön mindig naprakész lehet
3. A sebezhetőségeket folyamatosan felülvizsgáljuk az eszközök védelmének maximalizálása érdekében

Felépítésből adódó biztonság

A védett adatok és a biztonságos hálózatok az Epson többfunkciós eszközeinek alapszintű velejárói, olyan funkciókkal, amelyek segíthetnek az általános adatvédelmi rendelet (GDPR) és a vállalati társadalmi felelősségvállalás (CSR) betartásában. A közvetlenül a termékeinkbe integrált biztonsági intézkedések biztosítékot nyújtanak arra, hogy vállalkozása megfelel a biztonsági követelményeknek.

[2]

Eszközeinket független módon teszteljük, és a Keypoint Intelligence hitelesíti a biztonságukat. Az Epson saját fejlesztésű nyomtató/szkenner SoC és firmware platform technológiája védi az ügyfelek adatait és termékeit a biztonsági fenyegetésektől.

Biztonságos nyomtatás és szkennelés

Biztosíthatja a dokumentumok titkosságát, és megakadályozhatja, hogy illetéktelen személyek megtekinthessék a készülék felügyelet nélküli kimenetét, ha a nyomtatási illesztőprogramból „Bizalmas feladat” címkével küldi el a dokumentumokat.

A készülék funkcióihoz való hozzáférés korlátozása az előlapi zár segítségével történik.

Biztonságos kommunikáció

Az IP-szűrés funkcióval szűrhet azokra az IP-címekre, szolgáltatástípusokra, átviteli és a továbbítási portszámokra stb., amelyek hozzáférnek az Epson eszközökhöz. Az IPSec funkcióval titkosíthatja a hálózati kommunikációt.

Az eszközön

Az Epson Device Admin (EDA) segítségével könnyebben kezelhetővé válik az eszközön belüli biztonság. Számos hálózatra csatlakoztatott nyomtatóval kompatibilis, és egyetlen intelligens és intuitív interfészen keresztül minden eszköz vezérelhető.

PDF-védelem

Adjon jelszóvédelmet[3] a beolvasott PDF-fájlokhoz, hogy megvédje azokat az illetéktelen kíváncsiskodókkal szemben, és megakadályozza a dokumentumok szerkesztését és nyomtatását.

Dokumentumfeldolgozás és adatkezelés

Kezeljen egyszerre több feladatot is központosítva, a beolvasási feladatprofiloktól a felhasználói hozzáférési jogokig. A rendszergazdák egyetlen helyről kezelhetik a különböző feladatokat a szkennelési munkaprofiloktól a felhasználói hozzáférési jogosultságokig. Az IT-rendszergazdák többféle módon szabályozhatják a munkakörökhöz való hozzáférési jogokat, például személyi igazolványokkal, bejelentkezésekkel/jelszavakkal és PIN-kódokkal.

Zökkenőmentes integráció az IT-infrastruktúrába a helyi felhasználói adatbázissal vagy olyan címtárszolgáltatásokkal, mint a Microsoft EntraID és a Google Cloud Directory.

Az Epson biztonsági- és egyéb megoldásaival kapcsolatos további információkért olvassa be a kódokat, vagy keresse fel az alábbi hivatkozásokat.

Epson Solutions Suite

Epson Solutions Suite

Termékbiztonság

Világszerte elismert biztonság

Az Epsonnál globális szinten mérjük biztonságunkat. Megfelelünk az ISO/IEC 15408[3], más néven Common Criteria (CC) szabványnak, amely az informatikai termékek és rendszerek biztonsági intézkedéseire vonatkozó nemzetközi szabvány, valamint a CCRA tanúsításnak, amely igazolja, hogy a terméket a Japán Informatikai Biztonsági Értékelési és Tanúsítási Rendszer (JISEC) szerint tanúsították.

Hálózati biztonság
Mivel a hálózati biztonság kiemelt fontosságú, a rendszergazdák egyéni engedélyeket és korlátozásokat állíthatnak be a hálózati feladatok széles körére vonatkozóan. A WorkForce Enterprise 2 nyomtatóink esetében a rendszergazdák az IP Sec/IP Filtering funkcióval IP-címekre, szolgáltatástípusokra, vételi és átviteli portszámokra is szűrhetnek. Közben Ön eldöntheti, hogy elfogadja vagy letiltja-e az egyes IP-címeket. Támogatjuk az SNMPv3 e-mail titkosítást és a TLS1.3 protokollt.

A többfunkciós nyomtató védelme
A nyomtatók további védelme érdekében dönthet úgy, hogy blokkolja a számítógépről történő USB-n keresztüli hozzáférést, és letiltja a memóriakártyát, valamint az USB-memória interfészeket. Használhat másolásgátló vízjelet[5] is az eredeti dokumentumok jogosulatlan másolásának megakadályozására, valamint PDF-titkosítást[5] a digitális dokumentumok biztonságának megőrzése érdekében.

Biztonságos nyomtatás/beolvasás
A „Bizalmas feladat” opcióval megvédheti a dokumentumok adatait, és megakadályozhatja a felügyelet nélkül hagyott nyomatokba való illetéktelen betekintést.

WPA3
Az Epson legújabb többfunkciós gépei támogatják a WPA3[5] használatát, amely a WiFi (vezeték nélküli LAN) legújabb hitelesítési és titkosítási technológiája, így a vállalkozásoknak megbízhatóbb és erősebb védelmet biztosítanak a vezeték nélküli hálózaton keresztül történő adatforgalom számára.

Dokumentumvédelem
Növelje a termelékenységet és ellenőrizze a használatot biztonságos nyomtatással, szkenneléssel és másolással, a felhasználó-hitelesítés révén.

Hozzáférés-vezérlés
Felhasználói hitelesítés és funkciókorlátozások.

Eszközvédelem
Firmware aláírásának hitelesítése, biztonságos rendszerindítás és a rosszindulatú programok behatolásérzékelése működés közben.

Hamisításbiztos tinta
DURABrite™ Pro tintánk szilárdan behatol a papír szálaiba, ami megvédi a fontos dokumentumokat a hamisítástól, és megfelel az ISO 11798:2023 szabványnak.

Felhasználói adatvédelem

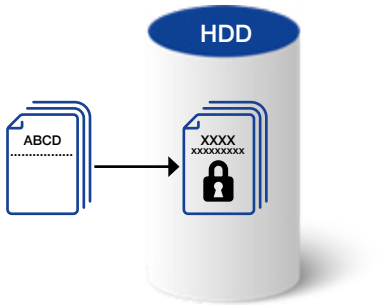
Egyedi jelszavakat is beállíthat az Epson nyomtatók megosztott tárhelyeihez[5], dokumentumaihoz és címjegyzékéhez. A teljes biztonság érdekében az adatok törlődnek a nyomtatóból, amint a munkák befejeződnek vagy a készülék kikapcsol. Ha a készülék rendelkezik merevlemezzel, minden adat titkosításra kerül, és az adatok minden nyomtatási feladat után törlődnek. A további védelem érdekében a rendszergazda felülírhatja a merevlemezt. További információk a biztonsági útmutatónkban találhatók.

Adatvédelem

HDD titkosítás, HDD biztonságos adattörlés, megbízható platformmodul (TPM) és jelszótitkosítás.

A merevlemezen tárolt adatok titkosítása

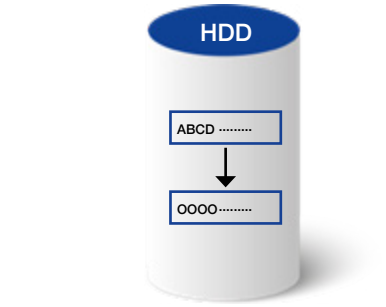
Az ügyfelek adatait mindig titkosítással védjük, amikor azokat egy többfunkciós nyomtató belső merevlemezére mentjük. Az adatok titkosítása megakadályozza a személyes adatokhoz való illetéktelen hozzáférést vagy a rosszindulatú támadást, ha a merevlemezt ellopják. A merevlemez egy öntitkosító meghajtóval van ellátva, és a dokumentumadatok AES-256-os titkosítással lesznek titkosítva.



Feladatadatok szekvenciális törlése

Ha a funkció engedélyezve van, a merevlemezen[5] lévő törölt adatokat a következő módon írja felül a rendszer a visszaállítás megakadályozása érdekében. Több lehetőség áll rendelkezésre:

1. Gyorstörlés: A titkosítási kulcs módosításra kerül, hogy megakadályozzák a törölt adatok visszaállítását.
2. Biztonságos szekvenciális törlés: A titkosítási kulcs módosításra kerül, és a merevlemezen lévő törölt adatokat „0”-val írja felül, hogy azok ne legyenek visszaállíthatók.



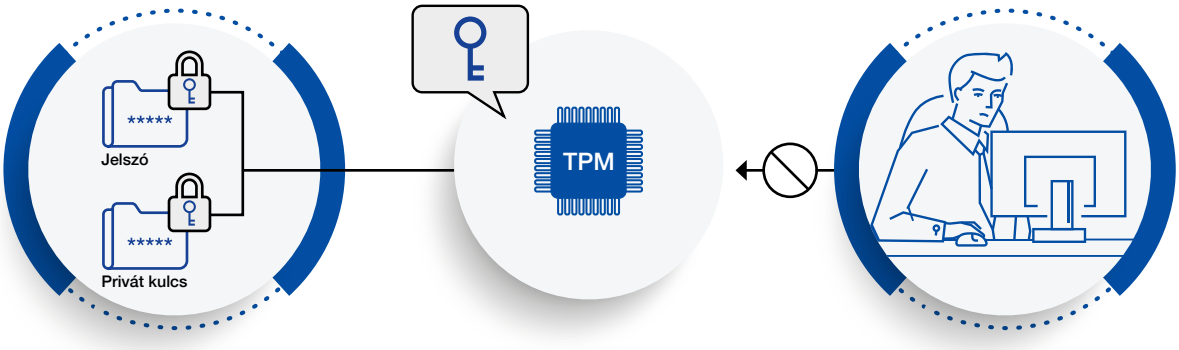
A munkaadatok törlésével kapcsolatos részletes magyarázatot a termékek felhasználói kézikönyvében talál.

TPM

A TPM-mel (Trusted Platform Module) ellátott modellekben a biztonsági szint a következőképpen lép magasabb szintre:

- A titkosított jelszavak és a titkos kulcsinformációk helyreállításához szükséges titkosítási kulcsokat a TPM-chip tárolja.
- A TPM-chip hardveres szinten védhető az illetéktelen elemzéstől, mivel a TPM-chiphez a nyomtatón kívülről nem lehet hozzáférni.
- A TPM esetében valódi véletlen számokat használnak munkamenetkulcsként a böngészővel való kommunikációhoz (Web Config).
- A TPM esetében valódi véletlen számokat használnak a titkosított merevlemez hitelesítési kulcsainak generálásához.

A többfunkciós nyomtatók TPM 2.0 chippel rendelkeznek.



	WorkForce Enterprise	WorkForce Enterprise AM	
Terméknév	WF-C21000/C20600/C20750	AM-C4000/C5000/C6000 és AM-M5500	AM-C400/C550/C550z
Típus	A3-as	A3-as	A4-es
Hálózati biztonság			
TLS-kommunikáció	✔	✔	✔
TLS1.1, TLS1.2, TLS1.3	✔	✔	✔
Protokollengedélyek és kizárások ellenőrzése	✔	✔	✔
IPsec/IP-szűrés	✔	✔	✔
IKEv1, IKEv2	✔	✔	✔
ESP:AES-CBC-128/AES-CBC-192/AES-CBC-256/3DES	✔	✔	✔
ESP:AES-GCM-128/AES-GCM-192/AES-GCM-256	✔	✔	✔
ESP/AH:SHA-1/MD5	✔	✔	✔
ESP/AH:SHA-256/SHA-384/SHA-512	✔	✔	✔
IEEE802.1X hitelesítés	✔	✔	✔
EAP-TLS, PEAP-TLS	✔	✔	✔
PEAP/MSCHAPv2	✔	✔	✔
EAP-TTLS	✔	✔	✔
AES128/AES256/3DES/RC4	✔	✔	✔
SNMPv3	✔	✔	✔
WPA3	✔	✔	✔
Elkülönített interfészek	✔	✔	✔
A többfunkciós nyomtató védelme			
USB-kapcsolat blokkolása a számítógépről	✔	✔	✔
A külső interfész letiltása	✔	✔	✔
Az USB-adathordozóval behurcolt vírusok kezelése	✔	✔	✔
Nyomtatási/szkennelési biztonság			
Bizalmas feladatok	✔*6	✔	✔
Másolás elleni minta[6]	✔	✔	✔
Vízjel[6]	✔	✔	✔
PDF titkosítás	✔	✔	✔
S/MIME	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔
Tartománykorlátozások	✔*7	✔	✔
Engedélyezési jelszó a hálózati mappába/FTP-re történő beolvasáshoz, beolvasás e-mailbe és e-mail értesítéshez	–	✔ *7	✔
Hosszú hitelesítési jelszavak támogatása	–	–	✔ *8
A fájlhozzáférés alapértelmezett letiltása a PDL-ből	✔*7	✔	✔
Biztonságos nyomtatás	✔	✔	✔
Faxolási biztonság[9]			
Közvetlen tárcsázásra vonatkozó korlátozások	✔	✔	✔
Címlista megerősítése	✔	✔	✔
Tárcsahang érzékelése	✔	✔	✔
Az elhagyott faxok elleni intézkedések	✔	✔	✔
Adatátviteli visszaigazolási jelentés	✔	✔	✔
A kapott faxok biztonsági mentési adatainak törlése	✔	✔	✔
Több címzettnek történő küldés korlátozása	✔	✔	✔
Nyomtató biztonsága			
Automatikus firmware-frissítések	✔	✔	✔
Jogellenes firmware-frissítések elleni védelem	–	✔	✔
Biztonságos boot-folyamat	–	✔	✔
Rosszindulatú programok beszűrődésének észlelése	✔*7	✔	✔
Biztonsági intézkedések a nyomtató leselejtezésekor			
Gyári alapbeállítások visszaállítása	✔	✔	✔
Biztonsági tanúsítvány és szabványok			
ISO15408/IEEE2600.2™	✔	✔	✔

	WorkForce Enterprise	WorkForce Enterprise AM	
Terméknév	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 és AM-M5500	AM-C400/C550/ C550z
Típus	A3-as	A3-as	A4-es
Biztonsági funkciók a harmadik fél szoftverekkel való kompatibilitás révén			
Open Platform-kompatibilis modell	✔	✔	✔
Epson Print Admin (EPA) / EPA Serverless			
Felhasználói hitelesítés azonosítókártyákkal/bejelentkezési hitelesítő adatokkal/PIN-kóddal	✔	✔	✔
Eszközműveletek teljes körű ellenőrzése személyenként	✔	✔	✔
MFP menü személyre szabása	✔	✔	✔
Behúzós nyomtatás és közvetlen nyomtatás	✔	✔	✔
Szkennelés és „küldés nekem” (e-mail, mappa)	✔	✔	✔
Beolvasás felhőszolgáltatásokba (OneDrive for Business, SharePoint online, Teams, Google Drive)[10]	✔	✔	✔
Szkennelés jelszóval védett PDF-fájlokba	✔	✔	✔
Speciális szkennelési munkafolyamat-beállítások[11]	✔	✔	✔
Driver nélküli nyomtatás felhőszolgáltatásokból (OneDrive for Business, SharePoint Online és Teams)[10]	✔	✔	✔
Szinkronizálás könyvtárszolgáltatással (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google secure LDAP és Google felhőkönyvtár)[10]	✔	✔	✔
Jelentések – Felhasználóvédelmi beállítás – Fájlnév elrejtése	✔	✔	✔
Jelszóra vonatkozó irányelv, fiókok kizárása[11]	✔	✔	✔
Nyomtatási szabályok és irányelvek[11]	✔	✔	✔
Felügyelet és jelentéskészítés	✔	✔	✔
Kvóta[10]	✔	✔	✔
Biztonságos mobilnyomtatás (AirPrint és Mopria)[12]	–	✔	✔
Felhasználói adatvédelem			
Dobozbiztonság	✔	✔	✔
Címjegyzék védelme	✔	✔	✔
Többfunkciós nyomtató által feldolgozott adatok kezelése	✔	✔	✔
A merevlemezen tárolt adatok titkosítása	✔	✔	✔
Feladatadatok szekvenciális törlése	✔	✔	✔
Jelszó-titkosítás	✔	✔	✔
TPM	✔*13	✔	✔
A merevlemez tükrözése	–	✔	–
Üzemeltetési korlátozások			
Panelzár	✔	✔	✔
Hozzáférés-vezérlés	✔	✔	✔
Hitelesített nyomtatás / szkennelés[8]	✔	✔	✔
Jelszóra vonatkozó irányelvek	✔	✔	✔
Felügyeleti napló	✔	✔	✔

További információért forduljon a helyi Epson forgalmazóhoz.

Név:

Telefon:

E-mail:

1. Print Security Landscape, 2025 – Identity, AI, and Quantum: Navigating the New Threat Landscape', Quocirca, 2025. július.

5. A modellspecifikációk teljes listájáért látogasson el a 12-13 days www.epson.eu/bi-security-solutions oldalra.

3. Az ISO/IEC 15408 szabványhoz nem tartozik standard konfiguráció. Speciális firmware és speciális beállítási folyamat szükséges.

2. A Keypoint Intelligence 2024-2026-os biztonsági validálási pecsétje az AM-C400 és AM-C550 modellekre vonatkozik.

4. A CCRA tanúsítási logó azt jelzi, hogy a terméket a japán IT-biztonságra vonatkozó értékelési és tanúsítási rendszer (JISEC) szerint értékelték és tanúsították. Ez nem jelenti azt, hogy a termék teljes mértékben mentesül a sebezhetőségtől. Nem jelenti azt sem, hogy a termék az összes működési környezetben rendelkezik valamennyi szükséges biztonsági funkcióval.

6. Csak a Windows illesztőprogramja esetén támogatott.

7. A funkció használatához frissítse a nyomtató firmware-ét a legújabb verzióra.

8. Hitelesített nyomtatási módszert igényel.

9. Csak akkor érhető el, ha az opcionális faxkártya telepítve van.

10. Az Epson Print Admin szolgáltatásra, és csak bizonyos termékekre vonatkozik az Epson Print Admin Serverless szolgáltatás esetén.

11. Csak az Epson Print Adminra szolgáltatásra vonatkozik.

12. Csak az Epson Print Admin Serverless szolgáltatásra vonatkozik.

13. A régiótól függően előfordulhat, hogy nem támogatott. Kérjük, forduljon a helyi értékesítési irodához az Ön országában való elérhetőséggel kapcsolatban.

Kérjük, hasznosítsa újra felelősségteljesen

Epson Europe B.V.
Magyarországi Fióktelepe
Köztelek u. 6. 4. emelet City Gate 1
1092 Budapest
Tel: +36 1 382 7680

Ingyenesen hívható ügyfélszolgálat:
+36 (1) 577-9932
www.epson.hu/contactus

@Epson_Magyarorszag
epson-magyarorszag

A21406-hu-HU 10/25

EPSON®