

Soluții de securitate de la Epson

# Soluții de securitate pentru imagistica de afaceri

Gamele WorkForce  
Enterprise 2 și AM-C



**EPSON®**

# Protejați securitatea rețelei oriunde se realizează imprimarea

Este ușor să treceți cu vederea unele măsuri de securitate importante pentru orice dispozitiv conectat în rețea în cadrul companiei dvs.

Și, deși poate că nu v-ați gândit la acest lucru, multifuncționalele (MFP), scannerile și orice alt dispozitiv conectat sau în rețea pot fi expuse la deficiențe de securitate.

Avansul înregistrat de munca la domiciliu și munca hibridă a amplificat acest risc. Un studiu realizat de Quocirca<sup>1</sup> a arătat că, deși 70% dintre factorii de decizie din domeniul IT consideră că imprimarea este esențială sau foarte importantă pentru afacerea lor, 31% dintre aceștia sunt îngrijorați de riscurile de securitate asociate cu imprimarea de la distanță/la domiciliu și doar 19% sunt complet încrezători că infrastructura lor de imprimare este sigură.

În condițiile în care costul mediu al unei încălcări a securității datelor legate de imprimare se ridică la 4.299.000 RON\*, nu este ceva ce vă puteți permite să tratați cu superficialitate.

Cu toate acestea, datorită abordării Epson în ceea ce privește securitatea imprimantelor, acesta este un risc pe care îl puteți reduce, indiferent de locul în care se realizează imprimarea business.



## 70%

dintre factorii de decizie din domeniul IT consideră că imprimarea este esențială sau foarte importantă pentru compania lor

## 31%

sunt îngrijorați de riscurile de securitate asociate cu imprimarea la distanță/la domiciliu

## 19%

se simt complet încrezători că infrastructura lor de imprimare este sigură

\* Pe baza valorii de 743.000 de lire sterline cotate de Quocirca și convertită în 4.299.000 RON utilizând rata de schimb valutar de pe xe.com la data de 09.01.2024.

# Abordarea Epson în materie de securitate

Consolidarea capacităților de rețea ale dispozitivelor dvs. este esențială pentru abordarea noastră în materie de securitate. Pentru a asigura securitatea dispozitivelor Epson pe tot parcursul ciclului de viață al acestora, fiecare imprimantă Epson WorkForce este construită pe trei principii de bază:

1. Securitatea produselor reprezintă baza pentru calitate
2. Informațiile și cunoștințele despre securitate sunt partajate în mod activ, astfel încât să fiți mereu la curent cu noutățile
3. Vulnerabilitățile sunt evaluate în mod constant pentru a maximiza protecția dispozitivelor

## Caracteristici de securitate concepute pentru a vi se potrivi

Datele protejate și rețelele securizate fac parte din dotarea standard a multifuncționalelor Epson, folosind funcții care vă pot ajuta în ceea ce privește Regulamentul general privind protecția datelor (GDPR) și responsabilitatea socială a întreprinderilor (CSR). Aceste măsuri de securitate, integrate direct în produsele noastre, vă oferă garanția că afacerea dvs. îndeplinește cerințele de securitate.

### Imprimare și scanare securizată

Puteți să asigurați confidențialitatea documentelor și să împiedicați persoanele neautorizate să vizualizeze documentele rezultate nesupravegheate, trimițând documentele dvs. ca „Lucrare confidențială” din driverul de imprimare/scanare.

Restricționarea accesului la funcțiile dispozitivului se poate face cu ajutorul blocării panoului frontal.

### Pe echipament

Cu funcția Epson Device Admin, securitatea pe dispozitiv devine mai ușor de gestionat. Compatibilă cu o gamă largă de imprimante conectate în rețea, aceasta permite utilizatorilor să controleze totul prin intermediul unei interfețe inteligente și intuitive. Cu ajutorul unui singur instrument uniform, administratorii își pot securiza imprimarea și imagistica, inclusiv blocarea de la distanță a ecranelor pentru a preveni modificările neautorizate ale profilurilor.

### Comunicare securizată

Filtrați adresele IP, serviciile, numerele de port de recepție și de transmisie care au acces la dispozitivele Epson. Puteți, de asemenea, cripta toate comunicările în rețea cu ajutorul funcției IPSec.

### Protecție PDF

Adăugați o funcție de protecție prin parolă<sup>3</sup> la fișierele PDF scanate pentru a le proteja împotriva vizualizărilor neautorizate și pentru a împiedica editarea și imprimarea documentelor.

### Prelucrare documente și gestionare date

Gestionați mai multe sarcini în mod centralizat, de la profilurile sarcinilor de scanare la drepturile de acces ale utilizatorilor. Administratorii pot gestiona central o varietate de sarcini, de la profiluri de lucrări de scanare până la drepturi de acces pentru utilizatori. Administratorii IT au capacitatea de a controla drepturile de acces la lucrări în numeroase modalități, inclusiv prin ID utilizator și parolă, LDAP Active Directory, conectare prin carte de identitate și cod PIN.

# Securitate recunoscută în întreaga lume

În cadrul Epson, ne evaluăm securitatea la scară globală. Respectăm standardul ISO/IEC 15408<sup>3</sup>, denumit și Criterii comune (Common Criteria, CC), care este un standard internațional pentru măsurile de securitate care vizează produsele și sistemele IT, și certificarea CCRA, care demonstrează că produsul a fost certificat în conformitate cu Sistemul japonez de evaluare și certificare a securității tehnologiei informației (Japan Information Technology Security Evaluation and Certification Scheme, JISEC).



## Securitatea rețelei

Având în vedere că securitatea rețelei reprezintă o prioritate majoră, administratorii pot stabili permisiuni și restricții individuale pentru o gamă largă de sarcini de rețea. Cu imprimantele noastre WorkForce Enterprise 2, administratorii pot, de asemenea, să filtreze adresele IP, tipurile de servicii, numerele porturilor de recepție și de transmisie utilizând funcția IP Sec/Filtrare IP. Și asta în timp ce decid dacă să accepte sau să blocheze anumite adrese IP. De asemenea, dispozitivele noastre acceptă criptarea e-mailurilor SNMPv3 și TLS1.3.



## Protejarea multifuncționalului dvs.

Pentru o protecție suplimentară a imprimantelor dvs., puteți alege să blocați accesul de la un computer prin USB și să dezactivați interfețele pentru carduri de memorie și memorii USB. De asemenea, puteți utiliza marcatul anti-copiere<sup>2</sup> pentru a preveni duplicarea neautorizată a documentelor originale și criptarea PDF<sup>2</sup> pentru a vă asigura că documentele digitale rămân în siguranță.



## Imprimare/scanare securizată

Opțiunea „Lucrare confidențială” vă permite să protejați confidențialitatea documentelor și să împiedicați orice vizualizare nedorită a rezultatelor nesupravegheate.



## WPA3

Cele mai recente multifuncționale Epson sunt compatibile cu WPA3<sup>2</sup>, care reprezintă cea mai recentă tehnologie de autentificare și criptare pentru WiFi (LAN wireless), oferind companiilor o protecție mai solidă și mai puternică pentru datele lor prin intermediul rețelei wireless.



## Protecție documente

Imprimare cu autentificare, scanare cu autentificare și înregistrarea lucrărilor.



## Control acces

Autentificare utilizator și restricții funcționale.



## Protecție dispozitiv

Verificarea semnăturii de firmware, pornire securizată și detecție malware.



### Protecție date utilizator

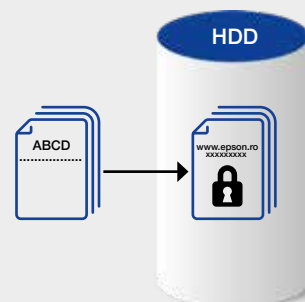
De asemenea, puteți seta parole unice pentru cutiile<sup>2</sup>, documentele și agendele partajate de pe imprimantele Epson. Pentru o securitate completă, datele sunt șterse din imprimantă imediat după ce lucrările sunt finalizate sau când alimentarea este oprită. În cazul în care dispozitivul are un hard disk, toate datele sunt criptate; de asemenea, datele sunt șterse după fiecare sarcină de imprimare. Pentru o protecție suplimentară, administratorul poate și să suprascrise hard disk-ul. Citiți mai multe în ghidul nostru de securitate disponibil pe adresa [epson.eu/bi-security-solutions](http://epson.eu/bi-security-solutions)

### Protecția datelor

Criptarea HDD, ștergerea sigură a datelor de pe HDD, modulul Trusted Platform Module (TPM) și criptarea parolilor.

#### Criptarea datelor salvate pe HDD

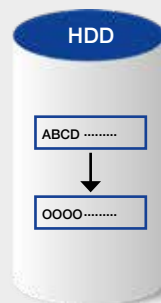
Protejăm întotdeauna datele clienților prin criptare atunci când salvăm date pe o unitate HDD internă a unui multifuncțional. Criptarea datelor previne accesul neautorizat sau atacurile rău intenționate la datele personale în cazul în care unitatea HDD este furată. Unitatea HDD este prevăzută cu o unitate de auto-criptare, iar datele documentelor sunt criptate cu AES-256.



#### Ștergere secvențială a datelor privind lucrarea

Atunci când această funcție este activată, datele șterse de pe hard disk<sup>2</sup> sunt suprascrise în următoarele moduri pentru a preveni restaurarea. Există mai multe opțiuni:

1. Ștergere rapidă: Cheia de criptare este modificată pentru a împiedica restaurarea datelor șterse.
2. Ștergere secvențială securizată: Cheia de criptare este modificată, iar datele șterse de pe hard disk sunt suprascrise cu „0” pentru a se asigura în continuare că ele nu pot fi recuperate.



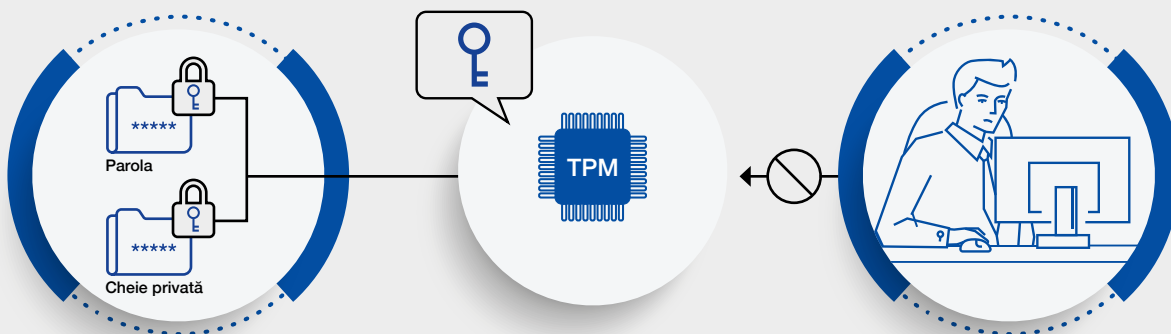
Vă rugăm să consultați manualul de utilizare al produsului dvs. pentru o explicație detaliată privind ștergerea datelor de lucru.

### TPM

În cazul modelelor cu TPM (Trusted Platform Module), nivelul de securitate se îmbunătățește după cum urmează:

- Cheile de criptare pentru restabilirea parolilor criptate și a informațiilor privind cheia privată sunt stocate pe cipul TPM.
- Cipul TPM poate fi protejat împotriva analizelor neautorizate la nivel hardware, deoarece acesta nu poate fi accesat din afara imprimantei.
- Numere aleatorii reale ale TPM-urilor sunt utilizate ca și chei de sesiune pentru comunicarea cu browser-ul (Web Config).
- Numere aleatorii reale ale TPM-urilor sunt utilizate pentru a genera cheia de autentificare pentru unitatea HDD criptată.

Multifuncționalul are un cip TPM 2.0.



Denumire produs	WorkForce Enterprise			AM-C		
	WF-C21000	WF-C20600	WF-C20750	AM-C6000	AM-C5000	AM-C4000
<b>Tip</b>	A3	A3	A3	A3	A3	A3
<b>Securitatea rețelei</b>						
Comunicare TLS	✓	✓	✓	✓	✓	✓
TLS1.1	✓	✓	✓	✓	✓	✓
TLS1.2	✓	✓	✓	✓	✓	✓
TLS1.3	✓*1	✓*1	✓*1	✓	✓	✓
Controlul permisiunilor și excluderilor de protocol	✓	✓	✓	✓	✓	✓
IPsec/Filtrare IP	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓
Autentificare IEEE802.1X	✓	✓	✓	✓	✓	✓
EAP-TLS	✓	✓	✓	✓	✓	✓
PEAP-TLS	✓	✓	✓	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓	✓	✓	✓
EAP-TTLS	✓	✓	✓	✓	✓	✓
AES128/AES256/3DES/RC4	✓	✓	✓	✓	✓	✓
SNMPv3	✓	✓	✓	✓	✓	✓
WPA3	✓	✓	✓	✓	✓	✓
Separare între interfețe	✓	✓	✓	✓	✓	✓
<b>Protejarea multifuncționalului dvs.</b>						
Blocare conexiune USB de la computer	✓	✓	✓	✓	✓	✓
Dezactivare interfață externă	✓	✓	✓	✓	✓	✓
Tratarea virușilor introduși de memoria USB	✓	✓	✓	✓	✓	✓
<b>Securitate imprimare/scanare</b>						
Lucrări confidențiale	✓*2	✓*2	✓*2	✓	✓	✓
Tipar anti-copiere	✓*2	✓*2	✓*2	✓*2	✓*2	✓*2
Marcaj	✓*2	✓*2	✓*2	✓*2	✓*2	✓*2
Criptare PDF	✓	✓	✓	✓	✓	✓
S/MIME	✓	✓	✓	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓	✓	✓	✓
Securitate fax	✓	✓	✓	✓	✓	✓
<b>Securitate fax</b>						
Restricții domeniu	✓*1	✓*1	✓*1	✓	✓	✓
Parolă de autorizare pentru opțiunile Scanare în fișierul de rețea/FTP, Scanare către e-mail și Notificare prin e-mail	-	-	-	✓*1	✓*1	✓*1
Imprimare securizată	✓	✓	✓	✓	✓	✓
Dezactivare implicită a accesului la fișiere din PDL	✓*1	✓*1	✓*1	✓	✓	✓
Restricții apelare directă	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Confirmare listă de adrese	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Detectare ton de apel	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Măsuri împotriva faxurilor abandonate	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Raport de confirmare a transmiterii	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Ștergere date de rezervă pentru faxurile primite	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Limitare trimitere către mai mulți destinatari	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3

\*1. Pentru a utiliza această funcție, actualizați programul firmware al imprimantei la cea mai recentă versiune.

\*2. Acceptă doar driver-ul de imprimare pentru Windows.

\*3. Funcție disponibilă doar atunci când este instalată placa de fax opțională.

	WorkForce Enterprise			AM-C		
Denumire produs	WF-C21000	WF-C20600	WF-C20750	AM-C6000	AM-C5000	AM-C4000
Tip	A3	A3	A3	A3	A3	A3
<b>Funcții de securitate prin compatibilitatea cu un program software terț</b>						
Model compatibil cu Open Platform	✓	✓	✓	✓	✓	✓
<b>Epson Print Admin</b>						
Cote, reguli și politici de imprimare	✓	✓	✓	✓	✓	✓
Autentificare utilizatori prin intermediul documentelor de identitate/ credențialelor de autentificare/codului PIN	✓	✓	✓	✓	✓	✓
Acces la funcțiile atribuite rolului sau departamentului	✓	✓	✓	✓	✓	✓
Personalizare meniu MFP pe grup sau individual	✓	✓	✓	✓	✓	✓
Imprimare la cerere	✓	✓	✓	✓	✓	✓
Imprimare directă	✓	✓	✓	✓	✓	✓
Scanare și trimitere către mine (e-mail, folder)	✓	✓	✓	✓	✓	✓
Servicii Scan to Cloud (OneDrive for Business, SharePoint online, Google Drive)	✓	✓	✓	✓	✓	✓
Setări avansate ale fluxului de lucru pentru scanare	✓	✓	✓	✓	✓	✓
Sincronizare cu Directory Service (LDAP, Open LDAP, Azure AD, Azure AD DS, Google Secure LDAP și Google Cloud Directory)	✓	✓	✓	✓	✓	✓
Scanare în fișiere PDF protejate prin parolă	✓	✓	✓	✓	✓	✓
<b>Epson Print Admin Serverless</b>						
Autentificare utilizatori prin intermediul documentelor de identitate/ credențialelor de autentificare/codului PIN	✓	✓	✓	✓	✓	✓
Control complet al acțiunilor dispozitivelor pentru fiecare persoană	✓	✓	✓	✓	✓	✓
Imprimare la cerere	✓	✓	✓	✓	✓	✓
Imprimare directă	✓	✓	✓	✓	✓	✓
Scanare și trimitere către mine (e-mail, folder)	✓	✓	✓	✓	✓	✓
Monitorizare și raportare	✓	✓	✓	✓	✓	✓
Sincronizare cu Directory Service (LDAP și Open LDAP)	✓	✓	✓	✓	✓	✓
Suport pentru cote de imprimare	✓	✓	✓	✓	✓	✓
<b>Protecție date utilizator</b>						
Securitate casetă	✓	✓	✓	✓	✓	✓
Protejarea agendei dvs.	✓	✓	✓	✓	✓	✓
Manipulare a datelor procesate de un multifuncțional	✓	✓	✓	✓	✓	✓
Criptare a datelor salvate pe hard disk	✓	✓	✓	✓	✓	✓
Ștergere secvențială a datelor privind lucrarea	✓	✓	✓	✓	✓	✓
Criptare parolă	✓	✓	✓	✓	✓	✓
TPM	✓*4	✓*4	✓*4	✓	✓	✓
<b>Limitare operațională</b>						
Blocare panou	✓	✓	✓	✓	✓	✓
Control acces	✓	✓	✓	✓	✓	✓
Imprimare prin autentificare	✓*5	✓*5	✓*5	✓*5	✓*5	✓*5
Politica privind parolele	✓	✓	✓	✓	✓	✓
Jurnal de audit	✓	✓	✓	✓	✓	✓
<b>Securitate imprimantă</b>						
Actualizări automate de firmware	✓	✓	✓	✓	✓	✓
<b>Măsuri de securitate atunci când eliminați o imprimantă</b>						
Revenire la setările implicite din fabrică	✓	✓	✓	✓	✓	✓
<b>Certificare și standarde de securitate</b>						
ISO15408/IEEEE2600.2™	✓	✓	✓	✓*6	✓*6	✓*6

\*4. În funcție de regiune, este posibil ca funcția să nu fie acceptată. Vă rugăm să contactați biroul local de vânzări pentru disponibilitatea sa la nivelul țării dvs.

\*5. Necesită o metodă de imprimare cu autentificare.

\*6. Disponibilitate în T4 2023.

**Pentru informații suplimentare, contactați reprezentantul dvs. de vânzări Epson.**

Nume:

Telefon:

E-mail:

EPSON și WorkForce sunt mărci comerciale înregistrate, iar EPSON Exceed Your Vision este o marcă grafică înregistrată a Seiko Epson Corporation. Toate celelalte produse și denumiri de mărci sunt mărci comerciale și/sau mărci comerciale înregistrate ale companiilor respective. Epson nu își asumă niciunul dintre drepturile asupra acestor mărci.

1. „Peisajul securității imprimării, 2023 - Securizarea infrastructurii de imprimare pe fondul unui peisaj de amenințări în creștere”, Quocirca, mai 2023.
2. Pentru o listă completă a specificațiilor modelelor, vizitați [www.epson.eu/bi-security-solutions](http://www.epson.eu/bi-security-solutions).
3. ISO/IEC 15408 nu vine cu o configurație standard. Este necesar un firmware special și un proces de configurare special.
4. Aplicabilitate pentru WorkForce Enterprise 2
5. Aplicabilitate pentru gama AM-C



Vă rugăm să reciclați responsabil

EPSON Europe BV, Sucursala România  
AFI TECH PARK 1  
Bulevardul Tudor Vladimirescu, nr. 29A, etaj 4  
Sector 5, 050881, București  
Telefon: +40 21 402 5024  
Fax: +40 21 402 5020  
[www.epson.ro](http://www.epson.ro)

Call Center Epson  
Telefon: +40 21 794 0809  
Luni – Vineri, 09:00 – 18:00



EpsonRomania  
@epson\_romania  
epson-romania

Mărcile comerciale și mărcile înregistrate sunt proprietatea companiei Seiko Epson Corporation sau a deținătorilor respectivi. Informațiile privind produsul se pot modifica fără anunț prealabil.