Gamma WorkForce Enterprise 2 e AM

Stampanti per l'ufficio

Soluzioni sicure

EPSON®

Proteggere la sicurezza della rete ovunque si stampi

Quando si utilizzano dispositivi in rete in azienda, le misure di sicurezza sono spesso sottovalutate. Sebbene possa può succedere di trascurare questo aspetto, i multifunzione, gli scanner e altre apparecchiature connesse o in rete potrebbero presentare una serie di vulnerabilità.

L'aumento del lavoro domestico e ibrido ha amplificato questo rischio. Secondo quanto rivelato da uno studio condotto da Quocirca[1], il 56% delle organizzazioni ha subito almeno una perdita di dati a causa di una violazione della sicurezza legata alla stampa, mentre l'83% prevede di aumentare la spesa destinata alla sicurezza in tal ambito nel prossimo anno. Le principali preoccupazioni per le organizzazioni sono la sicurezza della stampa a casa (28%), la protezione dei documenti riservati o sensibili dalla stampa (28%) e la comprensione del tipo di minacce e vulnerabilità associate alla loro infrastruttura di stampa (25%).

Alla luce del costo medio di una violazione di dati riconducibile alla stampa, che si aggira intorno ai 953.000 €*, non è un fattore che si può prendere alla leggera.

Grazie all'approccio di Epson alla sicurezza delle stampanti, tuttavia, è un rischio che si può ridurre, indipendentemente da dove si effettua la stampa aziendale.

Le 3 principali sfide per la sicurezza della stampa

28%

Protezione della stampa in un ambiente remoto/domestico

28%

Protezione dei documenti sensibili o riservati dalla stampa

25%

Comprensione dei tipi di minacce e vulnerabilità associati alla nostra infrastruttura di stampa

*Equivalente al valore di 820.000 £ citato da Quocirca, convertite in 953.000 € utilizzando il tasso di cambio di xe.com al 07/07/2025.

Dichiarazione di sicurezza di Epson

Potenziare le funzionalità di rete dei dispositivi è uno degli aspetti centrali del nostro approccio alla sicurezza. Per garantire protezione durante il loro intero ciclo di vita, le stampanti e i multifunzione Epson WorkForce sono studiati secondo i tre principi seguenti:

1. Sicurezza come base per la qualità del prodotto
2. Condivisione attiva delle informazioni e delle conoscenze sulla sicurezza per poter essere sempre aggiornati
3. Esame continuo delle vulnerabilità per ottimizzare la protezione dei dispositivi

Sicurezza sin dalla progettazione

Grazie a funzionalità in linea con quanto previsto dal regolamento generale sulla protezione dei dati (GDPR) e dalle norme di responsabilità sociale d'impresa (CSR), dati protetti e reti sicure sono lo standard per i multifunzione Epson. Queste misure di sicurezza, integrate direttamente nei nostri prodotti, garantiscono che l'azienda soddisfi i requisiti di sicurezza specifici della tua azienda.

I nostri dispositivi sono testati in modo indipendente e la sicurezza è convalidata da Keypoint Intelligence. La tecnologia del SoC della stampante/scanner e della piattaforma firmware proprietaria di Epson protegge le informazioni e i prodotti dei clienti dalle minacce alla sicurezza.

[2]

Stampa e scansione in tutta sicurezza

Inviando i documenti come "Lavoro Confidenziale" dal driver di stampa, garantisci la privacy dei documenti e impedisci che persone non autorizzate accedano al materiale in uscita da un dispositivo non custodito.

La limitazione dell'accesso alle funzioni sul dispositivo può essere effettuata utilizzando il blocco del pannello di controllo frontale.

Comunicazione sicura

Filtra gli indirizzi IP, i servizi e i numeri delle porte di trasmissione e ricezione che hanno accesso ai dispositivi Epson. Non solo: puoi anche crittografare tutte le comunicazioni di rete mediante la funzione IPSec.

Dispositivo

Con Epson Device Admin (EDA), la sicurezza sul dispositivo diventa più facile da gestire. Compatibile con un'ampia gamma di stampanti in rete, consente di controllare tutti i dispositivi tramite un'interfaccia intuitiva e intelligente.

PDF protetti

Prevedendo l'inserimento di una password[3] per l'apertura dei file PDF acquisiti, solo gli utenti autorizzati potranno visualizzare, modificare o stampare un determinato documento.

Elaborazione dei documenti e gestione dei dati

Gestisci più attività a livello centralizzato, inclusi i profili di scansione e i diritti di accesso degli utenti. Gli amministratori possono gestire una serie di opzioni a livello centralizzato, dai profili di scansione ai diritti di accesso degli utenti. Gli amministratori IT possono controllare i diritti di accesso ai processi in vari modi, ad esempio mediante documenti d'identità, login/password e codici PIN.

Integrazione perfetta nell'infrastruttura IT con il database utenti locale o servizi di directory come Microsoft EntraID e Google Cloud Directory.

Per ulteriori informazioni sulla sicurezza o sulle soluzioni Epson, scansiona i codici o visita i link qui sotto.

Epson Solutions Suite

Epson Solutions Suite

Sicurezza del prodotto

Sicurezza riconosciuta in tutto il mondo

In Epson misuriamo la nostra sicurezza su scala globale. Soddisfiamo lo standard ISO/IEC 15408[3], chiamato anche Common Criteria (CC), uno standard internazionale per le misure di sicurezza nei prodotti e sistemi IT, e la certificazione CCRA, che dimostra l'avvenuta certificazione del prodotto in conformità con il Japan Information Technology Security Evaluation and Certification Scheme (JISEC).

Sicurezza di rete
Poiché la sicurezza di rete è una priorità importante, gli amministratori possono impostare autorizzazioni e restrizioni individuali su un'ampia gamma di attività di rete. Con le stampanti WorkForce Enterprise gli amministratori possono anche filtrare indirizzi IP, tipi di servizio e numeri di porta di ricezione e trasmissione utilizzando la funzione IP Sec/Filtro IP e decidere se accettare o bloccare indirizzi IP specifici. Supportiamo anche la crittografia e-mail SNMPv3 e TLS1.3.

Protezione della stampante multifunzione
Per una protezione aggiuntiva delle stampanti, è possibile scegliere di bloccare l'accesso da un computer tramite USB e disabilitare la scheda di memoria e le interfacce di memoria USB. È inoltre possibile utilizzare la filigrana anticopia[5] per impedire la duplicazione non autorizzata dei documenti originali e la crittografia PDF[5] per garantire che i documenti digitali rimangano al sicuro.

Stampa/scansione sicura
L'opzione "Lavoro Confidenziale" consente di proteggere la privacy dei documenti e impedire qualsiasi visualizzazione indesiderata da dispositivo incustodito.

WPA3
Le stampanti multifunzione più recenti di Epson supportano WPA3[5], la più recente tecnologia di autenticazione e crittografia per il WiFi (LAN wireless), offrendo alle aziende una protezione più solida e più forte dei propri dati sulla rete wireless.

Protezione dei documenti
Aumenta la produttività e monitora l'utilizzo con la stampa, la scansione e la copia sicure tramite l'autenticazione dell'utente.

Controllo dell'accesso
Autenticazione dell'utente e restrizioni di funzione.

Protezione del dispositivo
Verifica firma firmware, avvio sicuro e rilevamento in runtime delle intrusioni di malware.

Inchiostro antimanomissione
Il nostro inchiostro DURABrite™ Pro penetra saldamente nelle fibre della carta, proteggendo documenti importanti da manomissioni e rispettando la norma ISO 11798:2023.

Protezione dei dati utente

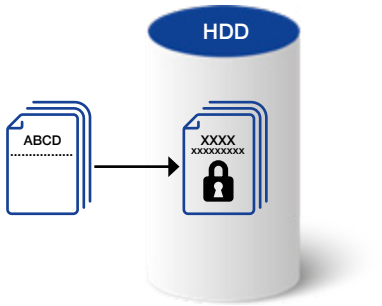
È anche possibile impostare sulle stampanti Epson password univoche per caselle condivise[5], documenti e rubriche. Per una sicurezza completa, i dati vengono cancellati dalla stampante una volta completati i lavori o quando l'alimentazione viene disattivata. Se il dispositivo ha un disco rigido, tutti i dati vengono crittografati e cancellati dopo ogni lavoro di stampa. Per una maggiore protezione, l'amministratore può anche sovrascrivere il disco rigido. Scopri di più nel nostro manuale sulla sicurezza.

Protezione dei dati

Crittografia HDD, cancellazione sicura dei dati HDD, Trusted Platform Module (TPM) e crittografia password.

Crittografia dei dati salvati su HDD

Proteggiamo sempre i dati degli utenti con la crittografia quando salviamo i dati sull'unità HDD interna di una stampante multifunzione. La crittografia dei dati impedisce l'accesso non autorizzato o l'attacco malevolo a dati personali qualora l'unità HDD venga rubata. L'unità HDD viene fornita con un'unità di crittografia automatica e i dati dei documenti vengono crittografati con la codifica AES-256.

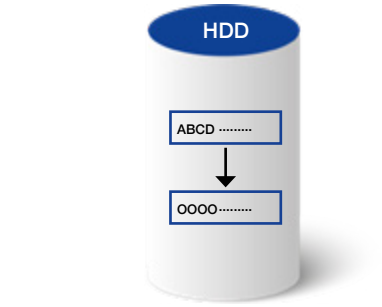


Eliminazione sequenziale dei dati del lavoro

Quando la funzione è attivata, i dati eliminati sul disco rigido[5] vengono sovrascritti nei seguenti modi, per evitare che vengano ripristinati.
Sono disponibili diverse opzioni:

1. Eliminazione rapida: la chiave di crittografia viene cambiata per impedire che i dati eliminati vengano ripristinati.
2. Eliminazione sequenziale sicura: la chiave di crittografia viene cambiata e i dati eliminati sul disco rigido vengono sovrascritti con zeri a ulteriore garanzia che non possano essere ripristinati.

Consultare il manuale utente del prodotto per una spiegazione dettagliata dell'eliminazione dei dati di lavoro.

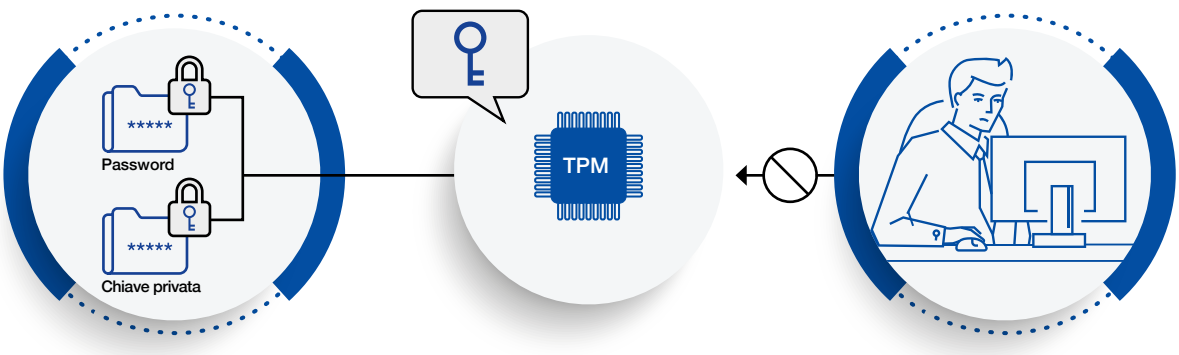


TPM

Nei modelli con TPM (Trusted Platform Module), il livello di sicurezza viene ulteriormente migliorato come indicato di seguito:

- Le chiavi di crittografia per il ripristino delle password crittografate e delle informazioni delle chiavi private vengono archiviate nel chip TPM.
- Il chip TPM può essere protetto da un'analisi non autorizzata a livello di hardware, dato che non è possibile accedervi dal di fuori della stampante.
- I numeri casuali del TPM vengono usati come chiavi di sessione per la comunicazione con il browser (configurazione web).
- I numeri casuali del TPM vengono usati nella generazione di chiavi di autenticazione per le unità HDD crittografate.

Le stampanti multifunzione hanno un chip TPM 2.0.



	WorkForce Enterprise	WorkForce Enterprise AM	
Nome prodotto	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 e AM-M5500	AM-C400/C550/C550z
Tipo	A3	A3	A4
Sicurezza di rete			
Comunicazione TLS	✔	✔	✔
TLS1.1, TLS1.2, TLS1.3	✔	✔	✔
Controllo dei permessi e delle esclusioni del protocollo	✔	✔	✔
Applicazione di filtri IPsec/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	✔	✔	✔
Autenticazione IEEE802.1X	✔	✔	✔
EAP-TLS, PEAP-TLS	✔	✔	✔
PEAP/MSCHAPv2	✔	✔	✔
EAP-TTLS	✔	✔	✔
AES128/AES256/3DES/RC4	✔	✔	✔
SNMPv3	✔	✔	✔
WPA3	✔	✔	✔
Separazione fra interfacce	✔	✔	✔
Protezione della stampante multifunzione			
Blocco della connessione USB dal computer	✔	✔	✔
Disattivazione dell'interfaccia esterna	✔	✔	✔
Gestione dei virus introdotti tramite memoria USB	✔	✔	✔
Sicurezza di stampa e scansione			
Lavori riservati	✔*6	✔	✔
Motivo anticopia[6]	✔	✔	✔
Filigrana[6]	✔	✔	✔
Crittografia PDF	✔	✔	✔
S/MIME	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔
Restrizioni del dominio	✔*7	✔	✔
Password di autorizzazione per la scansione alla cartella di rete/FTP, la scansione di indirizzi e-mail e la notifica e-mail	–	✔ *7	✔
Supporto per password di autenticazione lunghe	–	–	✔ *8
Disattivazione predefinita dell'accesso ai file da PDL	✔*7	✔	✔
Stampa sicura	✔	✔	✔
Sicurezza fax[9]			
Limitazioni al direct dialing	✔	✔	✔
Conferma dell'elenco indirizzi	✔	✔	✔
Rilevamento del segnale di chiamata	✔	✔	✔
Misure contro i fax abbandonati	✔	✔	✔
Rapporto di conferma della trasmissione	✔	✔	✔
Eliminazione dei dati di backup per i fax ricevuti	✔	✔	✔
Limite di invio a più destinatari	✔	✔	✔
Sicurezza della stampante			
Aggiornamenti automatici del firmware	✔	✔	✔
Protezione contro aggiornamenti firmware illegali	–	✔	✔
Avvio protetto	–	✔	✔
Rilevamento di infiltrazioni malware	✔*7	✔	✔
Misure di sicurezza quando si smaltisce una stampante			
Ripristino delle impostazioni di fabbrica	✔	✔	✔
Certificazioni e standard di sicurezza			
ISO15408/IEEE2600.2™	✔	✔	✔

	WorkForce Enterprise	WorkForce Enterprise AM	
Nome prodotto	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 e AM-M5500	AM-C400/C550/C550z
Tipo	A3	A3	A4
Funzionalità di sicurezza grazie alla compatibilità con software di terze parti			
Modello conforme a Open Platform	✔	✔	✔
Epson Print Admin (EPA) / EPA Serverless			
Autenticazione utente tramite carte d'identità/credenziali di accesso/codice PIN	✔	✔	✔
Controllo completo delle azioni dei dispositivi per individuo	✔	✔	✔
Personalizzazione del menu multifunzione	✔	✔	✔
Stampa in modalità pull e stampa diretta	✔	✔	✔
Scansione e invio (e-mail, cartella)	✔	✔	✔
Servizi di scansione sul cloud (OneDrive for Business, SharePoint Online, Teams e Google Drive)[10]	✔	✔	✔
Scansione in file PDF protetti da password	✔	✔	✔
Impostazioni avanzate del flusso di lavoro di scansione[11]	✔	✔	✔
Stampa senza driver da servizi cloud (OneDrive for Business, SharePoint Online e Teams)[10]	✔	✔	✔
Sincronizzazione con il servizio di directory (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google Secure LDAP e Google Cloud Directory)[10]	✔	✔	✔
Report - Impostazione protezione utente - Nascondi nome file	✔	✔	✔
Criteri per la password, Blocco account[11]	✔	✔	✔
Regole e criteri di stampa[11]	✔	✔	✔
Tracciatura e report	✔	✔	✔
Quota[10]	✔	✔	✔
Stampa da mobile sicura (AirPrint e Mopria)[12]	–	✔	✔
Protezione dei dati utente			
Sicurezza delle caselle	✔	✔	✔
Protezione della rubrica	✔	✔	✔
Gestione dei dati elaborati da una stampante multifunzione	✔	✔	✔
Crittografia dei dati salvati sul disco rigido	✔	✔	✔
Eliminazione sequenziale dei dati del lavoro	✔	✔	✔
Crittografia delle password	✔	✔	✔
TPM	✔*[13]	✔	✔
Mirroring del disco rigido	–	✔	–
Limiti operativi			
Blocco del pannello	✔	✔	✔
Controllo dell'accesso	✔	✔	✔
Stampa/scansione autenticata[8]	✔	✔	✔
Criteri per la password	✔	✔	✔
Registri di controllo	✔	✔	✔

Per maggiori informazioni, contattare il rappresentante Epson.

Nome:

Telefono:

E-mail:

1. Print Security Landscape, 2025 - Identity, AI, and Quantum: Navigating the New Threat Landscape', Quocirca, luglio 2025.
2. Keypoint Intelligence Security Validation Testing Seal 2024-2026 si applica ad AM-C400 e AM-C550.
3. ISO/IEC 15408 non viene fornito con la configurazione standard. Sono necessari un firmware speciale e un processo di configurazione speciale.
4. Il logo della certificazione CCRA indica che il prodotto è stato valutato e certificato in conformità al Japan Information Technology Security Evaluation and Certification Scheme (JISEC). Non garantisce che il prodotto sia completamente esente da vulnerabilità. Non implica nemmeno che il prodotto sia dotato di tutte le funzioni di sicurezza necessarie in ogni ambiente operativo.
5. Per un elenco completo delle specifiche del modello, visitare support.epson.net/security/it
6. Supportato solo il driver della stampante Windows.
7. Per utilizzare questa funzione, aggiornare il firmware della stampante alla versione più recente.
8. Richiede un metodo di stampa autenticato.
9. Disponibile solo quando è installata la scheda PS opzionale.
10. Si applica a Epson Print Admin e solo a prodotti specifici su Epson Print Admin Serverless.
11. Si applica solo a Epson Print Admin.
12. Si applica solo a Epson Print Admin Serverless.
13. Può non essere supportato per alcuni Paesi. Per conoscere la disponibilità dei prodotti nei singoli mercati, contattare il rappresentante Epson locale.

Riciclare responsabilmente

Epson Italia s.p.a.
Via M. Viganò De Vizzi, 93/95
20092 Cinisello Balsamo (MI)
Tel.: 02-660321
Hot Line prodotti Consumer: 02-30578340
Hot Line prodotti Business: 02-30578341

www.epson.it/contactus

Epson.Italia
@EpsonItalia
@EpsonItalia
epson-italia

A21406-it-IT 10/25

EPSON®