WorkForce Enterprise řady 2 a AM

Business tiskárny
Bezpečná řešení

EPSON®

Chraňte zabezpečení sítě bez ohledu na to, kde se tiskne

Je snadné přehlédnout důležitá bezpečnostní opatření na síťových zařízeních ve vaší firmě. A ačkoli jste o tom možná ještě neuvažovali, mohou být multifunkční tiskárny (MFP), skenery a jiná připojená nebo síťová zařízení náchylná k ohrožení zabezpečení.

Rozšiřování práce z domova a hybridní práce toto riziko ještě více zvýšilo. Studie společnosti Quocirca[1] zjistila, že 56 % organizací utrpělo kvůli narušení bezpečnosti tisku alespoň jednu ztrátu dat, přičemž 83 % očekává, že v nadcházejícím roce zvýší své náklady na bezpečnost tisku. Hlavními obavami pro organizace jsou zabezpečení domácího tisku (28 %), ochrana důvěrných nebo citlivých dokumentů před tiskem (28 %) a pochopení typů hrozeb a zranitelnosti jejich tiskové infrastruktury (25 %).

Průměrné náklady za únik dat v souvislosti s tiskem představují 953 000 eur*, což nelze brát na lehkou váhu.

Díky přístupu společnosti Epson k zabezpečení tiskáren však lze toto riziko zmírnit, bez ohledu na to, kde tisk ve vaší firmě probíhá.

3 hlavní výzvy v oblasti zabezpečení tisku

28 %

Zabezpečení tisku ve vzdáleném/domácím prostředí

28 %

Ochrana citlivých nebo důvěrných dokumentů před tiskem

25 %

Pochopení typů hrozeb a zranitelnosti naší tiskové infrastruktury

* Založeno na hodnotě 820 000 liber (po převodu 953 000 eur) podle odhadu ceny společností Quocirca s použitím kurzu FX z xe.com k 7. 7. 2025.

Prohlášení společnosti Epson o bezpečnosti

Pro náš přístup k zabezpečení je důležité posílení síťových schopností vašich zařízení. Každá tiskárna Epson WorkForce je postavena na třech základních principech, které zajišťují bezpečnost zařízení Epson po celou dobu jejich životnosti:

1. Zabezpečení produktů je základem pro kvalitu.
2. Informace a znalosti o bezpečnosti jsou aktivně sdíleny, takže máte vždy aktuální informace.
3. Zranitelná místa jsou neustále kontrolována, aby se maximalizovala ochrana zařízení.

Zabezpečeno již od návrhu

Chráněná data a zabezpečené sítě jsou standardně dodávány s multifunkčními zařízeními Epson využívajícími funkce, které mohou pomoci s obecným nařízením o ochraně osobních údajů (GDPR) a společenskou odpovědností firem (CSR). Tato bezpečnostní opatření, která jsou integrována přímo do našich produktů, vám dávají jistotu, že vaše firma splňuje vaše bezpečnostní požadavky.

Naše zařízení jsou nezávisle testována a bezpečnost ověřena společností Keypoint Intelligence. Patentovaná standardní tiskárna a technologie firmwaru společnosti Epson chrání informace o zákaznících a produkty před bezpečnostními hrozbami.

(2)

Bezpečný tisk a skenování

Chcete-li zajistit ochranu osobních údajů dokumentů a zabránit neoprávněným osobám v prohlížení výstupu bez dozoru na zařízení, odešlete vaše dokumenty jako „důvěrnou práci“ z tiskového ovladače.

Přístup k funkcím zařízení lze omezit pomocí zámku předního panelu.

Zabezpečená komunikace

Můžete filtrovat IP adresy, služby, čísla příjmových a přenosových portů, které mají přístup k zařízením Epson. Pomocí funkce IPSec můžete také šifrovat veškerou síťovou komunikaci.

Na zařízení

Se správcem zařízení Epson (EDA) se zabezpečení zařízení spravuje jednodušeji. Jelikož je kompatibilní se širokou řadou našich síťových tiskáren, uživatelé mohou vše ovládat prostřednictvím chytrého a intuitivního rozhraní.

Ochrana PDF

Přidejte do naskenovaných souborů PDF funkci ochrany heslem[3], abyste je ochránili před neoprávněným prohlížením a zabránili úpravám a tisku dokumentů.

Zpracování dokumentů a správa dat

Spravujte centrálně více úloh, od profilů úloh skenování po přístupová práva uživatelů. Správci mohou centrálně spravovat různé úkoly, od profilů úloh skenování po přístupová práva uživatelů. Správci IT mají mnoho způsobů, jak kontrolovat přístupová práva k pracovním pozicím, včetně ID karet, přihlašovacích jmen/hesel a PIN kódů.

Bezproblémová integrace do infrastruktury IT s místní databází uživatelů nebo adresářovými službami, jako jsou Microsoft EntraID a Google Cloud Directory.

Další informace o zabezpečení nebo řešeních společnosti Epson naleznete po naskenování kódů nebo na níže uvedených odkazech.

Epson Solutions Suite

Epson Solutions Suite

Bezpečnost produktů

Uznávané zabezpečení po celém světě

Ve společnosti Epson udáváme kritéria našeho zabezpečení v globálním měřítku. Splňujeme normu ISO/IEC 15408[3], která se také nazývá Společná kritéria (CC), což je mezinárodní standard pro bezpečnostní opatření v IT produktech a systémech, a certifikaci CCRA, která prokazuje, že produkt byl certifikován v souladu s japonským plánem hodnocení a certifikace bezpečnosti informačních technologií (JISEC).

Zabezpečení sítě

Hlavní prioritou zabezpečení sítě je, že správci mohou nastavit individuální oprávnění a omezení pro širokou škálu síťových úkolů. S našimi tiskárnami WorkForce Enterprise řady 2 mohou správci filtrovat také IP adresy, typy služeb, čísla přijímacích a přenosových portů pomocí funkce filtrování IP Sec / IP a rozhodovat, zda přijmout nebo zablokovat konkrétní IP adresy. Podporujeme také šifrování e-mailů SNMPv3 a TLS1.3.

Ochrana all-in-one tiskárny

Pro další ochranu vašich tiskáren můžete zablokovat přístup z počítače prostřednictvím USB a deaktivovat paměťovou kartu a paměťová rozhraní USB. Můžete také použít vodoznak proti kopírování[5], abyste zabránili neoprávněnému duplikování původních dokumentů, a šifrování PDF[5], abyste zajistili, že digitální dokumenty zůstanou v bezpečí.

Zabezpečený tisk/skenování

Možnost „důvěrná úloha“ znamená, že můžete chránit soukromí dokumentů a zabránit nechtěnému zobrazení výstupu bez dozoru.

WPA3

Nejnovější multifunkční zařízení Epson podporují technologii WPA3[5], což je nejnovější ověřovací a šifrovací technologie pro Wi-Fi (bezdrátová síť LAN), která firmám poskytuje robustnější a silnější ochranu jejich dat prostřednictvím bezdrátové sítě.

Ochrana dokumentů

Zvyšte produktivitu a monitorujte využití pomocí bezpečného tisku, skenování a kopírování prostřednictvím ověřování uživatelů.

Řízení přístupu

Ověřování uživatele a omezení funkcí.

Ochrana zařízení

Ověřování podpisů firmwaru, zabezpečené spouštění a detekce napadení malwarem.

Inkoust odolný proti nevhodné manipulaci

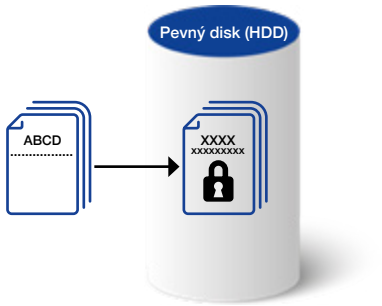
Náš inkoust DURABrite™ proniká pevně do vláken papíru, čímž chrání důležité dokumenty před neoprávněnou manipulací a splňuje normu ISO 11798:2023.

Ochrana údajů uživatelů

Na svých tiskárnách Epson můžete také nastavit jedinečná hesla pro sdílená pole[5], dokumenty a adresáře. Pro úplné zabezpečení jsou data vymazána z tiskárny, jakmile jsou úlohy dokončeny nebo je vypnuto napájení. Pokud má zařízení pevný disk, všechna data jsou šifrována a po každé tiskové úloze jsou vymazána. Pro zvýšenou ochranu může správce také přepsat pevný disk.
Přečtěte si více v naší příručce o zabezpečení.

Ochrana údajů

Šifrování pevného disku, bezpečné vymazání dat na pevném disku, čip Trusted Platform Module (TPM) a šifrování hesel.



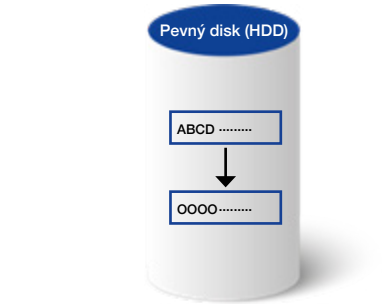
Šifrování dat uložených na pevném disku

Při ukládání dat na interní pevný disk v all-in-one tiskárně vždy chráníme data zákazníků šifrováním. Šifrování dat brání neoprávněnému přístupu nebo útoku na osobní údaje v případě odcizení pevného disku. Pevný disk se dodává se samošifrovací jednotkou a dokumentová data jsou šifrována pomocí AES-256.

Sekvenční odstranění dat úlohy

Pokud je tato funkce povolena, odstraněná data na pevném disku[5] se přepíší následujícími způsoby, aby se zabránilo obnovení. Existuje několik možností:

1. Rychlé odstranění: Šifrovací klíč se změní, aby se zabránilo obnovení odstraněných dat.
2. Bezpečné sekvenční odstranění: Šifrovací klíč se změní a odstraněná data na pevném disku budou přepsána nulami, aby se dále zajistilo, že odstraněná data nebude možné obnovit.



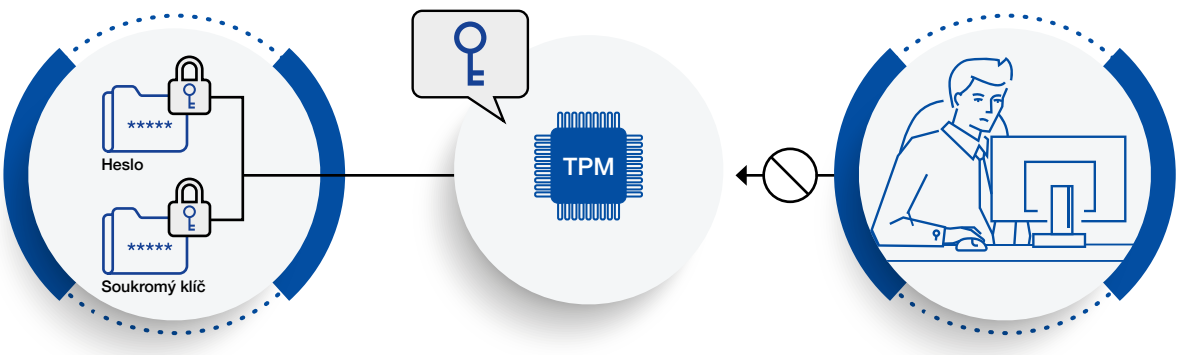
Podrobné pokyny pro vymazání dat úlohy naleznete v uživatelské příručce k produktu.

TPM

U modelůs Trusted Platform Module (TPM) se úroveň zabezpečení zvyšuje následovně:

- Šifrovací klíče pro obnovení šifrovaných hesel a soukromých klíčových informací jsou uloženy na čipu TPM.
- Čip TPM lze chránit před neautorizovanou analýzou na úrovni hardwaru, protože k čipu TPM nelze přistupovat zvenčí tiskárny.
- Skutečná náhodná čísla TPM se používají jako klíče relace pro komunikaci s prohlížečem (konfigurace webu).
- Skutečná náhodná čísla TPM se používají při generování ověřovacích klíčů pro šifrovaný pevný disk.

Multifunkční tiskárny mají čip TPM 2.0.



	WorkForce Enterprise	WorkForce Enterprise AM	
Název produktu	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 a AM-M5500	AM-C400/C550/ C550z
Typ	A3	A3	A4
Zabezpečení sítě			
Komunikace TLS	✔	✔	✔
TLS1.1, TLS1.2, TLS1.3	✔	✔	✔
Kontrola oprávnění a vyloučení protokolu	✔	✔	✔
Filtrování 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	✔	✔	✔
Ověření IEEE802.1X	✔	✔	✔
EAP-TLS, PEAP-TLS	✔	✔	✔
PEAP/MSCHAPv2	✔	✔	✔
EAP-TTLS	✔	✔	✔
AES128/AES256/3DES/RC4	✔	✔	✔
SNMPv3	✔	✔	✔
WPA3	✔	✔	✔
Separace mezi rozhraními	✔	✔	✔
Ochrana all-in-one tiskárny			
Blokování připojení USB z počítače	✔	✔	✔
Vypnutí externího rozhraní	✔	✔	✔
Manipulace s viry zaváděnými pamětí USB	✔	✔	✔
Zabezpečení tisku/skenování			
Důvěrné pracovní pozice	✔*6	✔	✔
Ochranný vzorek proti kopírování[6]	✔	✔	✔
Vodoznak[6]	✔	✔	✔
Šifrování PDF	✔	✔	✔
S/MIME	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔
Omezení domény	✔*7	✔	✔
Autorizační heslo pro skenování do síťové složky / FTP, skenování do e-mailu a e-mailové oznámení	–	✔*7	✔
Podpora dlouhých ověřovacích hesel	–	–	✔ *8
Výchozí deaktivace přístupu k souborům z PDL	✔*7	✔	✔
Zabezpečený tisk	✔	✔	✔
Zabezpečení faxu[9]			
Omezení přímého vytáčení	✔	✔	✔
Potvrzení seznamu adres	✔	✔	✔
Detekce tónů vytáčení	✔	✔	✔
Opatření proti opuštěným faxům	✔	✔	✔
Zpráva o potvrzení přenosu	✔	✔	✔
Odstranění záložních dat pro přijaté faxy	✔	✔	✔
Omezení odesílání více příjemcům	✔	✔	✔
Bezpečnost tiskárny			
Automatické aktualizace firmwaru	✔	✔	✔
Ochrana proti nezákonným aktualizacím firmwaru	–	✔	✔
Zabezpečené spouštění	–	✔	✔
Detekce infiltrace malwaru	✔*7	✔	✔
Bezpečnostní opatření při likvidaci tiskárny			
Obnovit výchozí tovární nastavení	✔	✔	✔
Bezpečnostní certifikace a normy			
ISO15408/IEEE2600.2™	✔	✔	✔

	WorkForce Enterprise	WorkForce Enterprise AM	
Název produktu	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 a AM-M5500	AM-C400/C550/ C550z
Typ	A3	A3	A4
Bezpečnostní funkce díky kompatibilitě se softwarem třetích stran			
Model kompatibilní s otevřenou platformou	✔	✔	✔
Epson Print Admin (EPA) / EPA Serverless			
Ověřování uživatelů pomocí identifikačních karet / přihlašovacích údajů / PIN kódu	✔	✔	✔
Úplná kontrola nad činnostmi zařízení na jednotlivce	✔	✔	✔
Přizpůsobení nabídky multifunkčních zařízení	✔	✔	✔
Tisk s ověřením a přímý tisk	✔	✔	✔
Skenování a odeslání mně (e-mail, složka)	✔	✔	✔
Skenování do cloudových služeb (OneDrive for Business, SharePoint Online, Teams a Google Drive)[10]	✔	✔	✔
Skenování souborů PDF chráněných heslem	✔	✔	✔
Pokročilá nastavení pracovního postupu skenování[11]	✔	✔	✔
Tisk bez ovladače z cloudových služeb (OneDrive pro firmy, SharePoint Online a Teams)[10]	✔	✔	✔
Synchronizace s adresářovou službou (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google secure LDAP a cloudový adresář Google)[10]	✔	✔	✔
Reporty – Nastavení ochrany uživatele – Skrýt název souboru	✔	✔	✔
Zásady pro hesla, uzamčení účtu[11]	✔	✔	✔
Pravidla a zásady tisku[11]	✔	✔	✔
Sledování a reportování	✔	✔	✔
Kvóta[10]	✔	✔	✔
Zabezpečený mobilní tisk (AirPrint a Mopria)[12]	–	✔	✔
Ochrana údajů uživatelů			
Zabezpečení boxu	✔	✔	✔
Ochrana vašeho adresáře	✔	✔	✔
Zpracování dat pomocí all-in-one tiskárny	✔	✔	✔
Šifrování uložených dat na pevném disku	✔	✔	✔
Sekvenční odstranění dat úlohy	✔	✔	✔
Šifrování heslem	✔	✔	✔
TPM	✔*13	✔	✔
Zrcadlení pevného disku	–	✔	–
Provozní omezení			
Zámek panelu	✔	✔	✔
Řízení přístupu	✔	✔	✔
Ověřený tisk / skenování[8]	✔	✔	✔
Zásady pro hesla	✔	✔	✔
Protokol auditu	✔	✔	✔

Další informace vám poskytne obchodní zástupce společnosti Epson.

Jméno:

Tel.:

E-mail:

1. Print Security Landscape, 2025 – Identity, AI, and Quantum: Navigating the New Threat Landscape', Quocirca, červenec 2025.
2. Keypoint Intelligence Security Validation Testing Seal 2024-2026 se vztahuje na AM-C400 a AM-C550.
3. Norma ISO/IEC 15408 se nedodává se standardní konfigurací. Je vyžadován speciální firmware a speciální proces nastavení.
4. Logo certifikace CCRA potvrzuje, že produkt byl hodnocen a certifikován v souladu s japonským plánem hodnocení a certifikace bezpečnosti informačních technologií (JISEC). Neznamená to, že produkt je zcela bez zranitelností. Neznamená to také, že produkt je vybaven všemi nezbytnými bezpečnostními funkcemi v každém provozním prostředí.
5. Úplný seznam specifikací modelů naleznete na adrese support.epson.net/security/en.
6. Podporován je pouze ovladač tiskárny pro Windows.
7. Chcete-li tuto funkci použít, aktualizujte firmware tiskárny na nejnovější verzi.
8. Vyžaduje ověřenou metodu tisku.
9. K dispozici pouze při instalaci volitelné faxové desky.
10. Platí pro Epson Print Admin a pouze na konkrétní produkty na serveru Epson Print Admin Serverless.
11. Platí pouze pro Epson Print Admin.
12. Platí pouze pro Epson Print Admin Serverless.
13. V závislosti na regionu nemusí být podporováno. Ohledně dostupnosti ve vaší zemi kontaktujte místní prodejní kancelář.

Recyklujte odpovědně

EPSON EUROPE B.V.
Organizační složka
Greenline Kačerov, Jihlavská 1558/21
140 00 Praha - Michle
Česká republika

Infolinka: +420 246 037 281
www.epson.cz

@epsonczsk
epson-cesko-a-slovensko

A21406-cs-CZ 10/25

EPSON®