



Chraňte svou síť nejzabezpečenějším tiskem společnosti HP.¹

94 %

finančních firem tvrdí, že zabezpečení kopírky/tiskárny je důležité nebo velmi důležité.²



61 %

organizací ohlásilo v loňském roce minimálně jedno narušení ochrany dat v souvislosti s tiskem.³



43 %

společností ve svých postupech zabezpečení koncových zařízení nebere v úvahu tiskárny.⁴





Pouze 18 % společností monitoruje tiskárny z hlediska hrozeb.⁴ Co ta vaše?

Odhalte skrytá rizika

IT má za cíl neustále chránit důvěrné informace včetně osobních údajů zaměstnanců a zákazníků v nejrůznějších zařízeních a prostředích. Mnoho oddělení IT sice aplikuje bezpečnostní opatření na jednotlivých počítačích a ve firemní síti, tisková a zobrazovací zařízení jsou však často přehlížena, a stávají se tak snadným terčem. Přítomnost nezabezpečených zařízení může celou síť vystavit riziku kybernetického útoku.

Uvědomte si potenciální náklady

Každé narušení bezpečnosti je potenciálně nákladné. Pokud dojde k ohrožení soukromých údajů v důsledku nezabezpečeného tisku a zobrazování, může to mít následky v podobě krádeže identity nebo informací přinášejících konkurenční výhodu, poškozeného dobrého jména značky a soudních sporů. Za nedodržení zákonů a předpisů navíc hrozí vysoké pokuty.

HP vám nabízí pomoc

Chraňte svou síť nejzabezpečenějším tiskem společnosti HP.¹ Tiskárny HP jsou vždy ve střehu, neustále detekují a zastavují hrozby a dokážou se přizpůsobit novým. Široké portfolio řešení HP vám umožní automatizovat ochranu zařízení, dat a dokumentů. Naši odborníci na zabezpečení tisku vám pomohou sestavit a zavést ucelenou strategii zabezpečení zařízení pro tisk a zpracování obrazu.

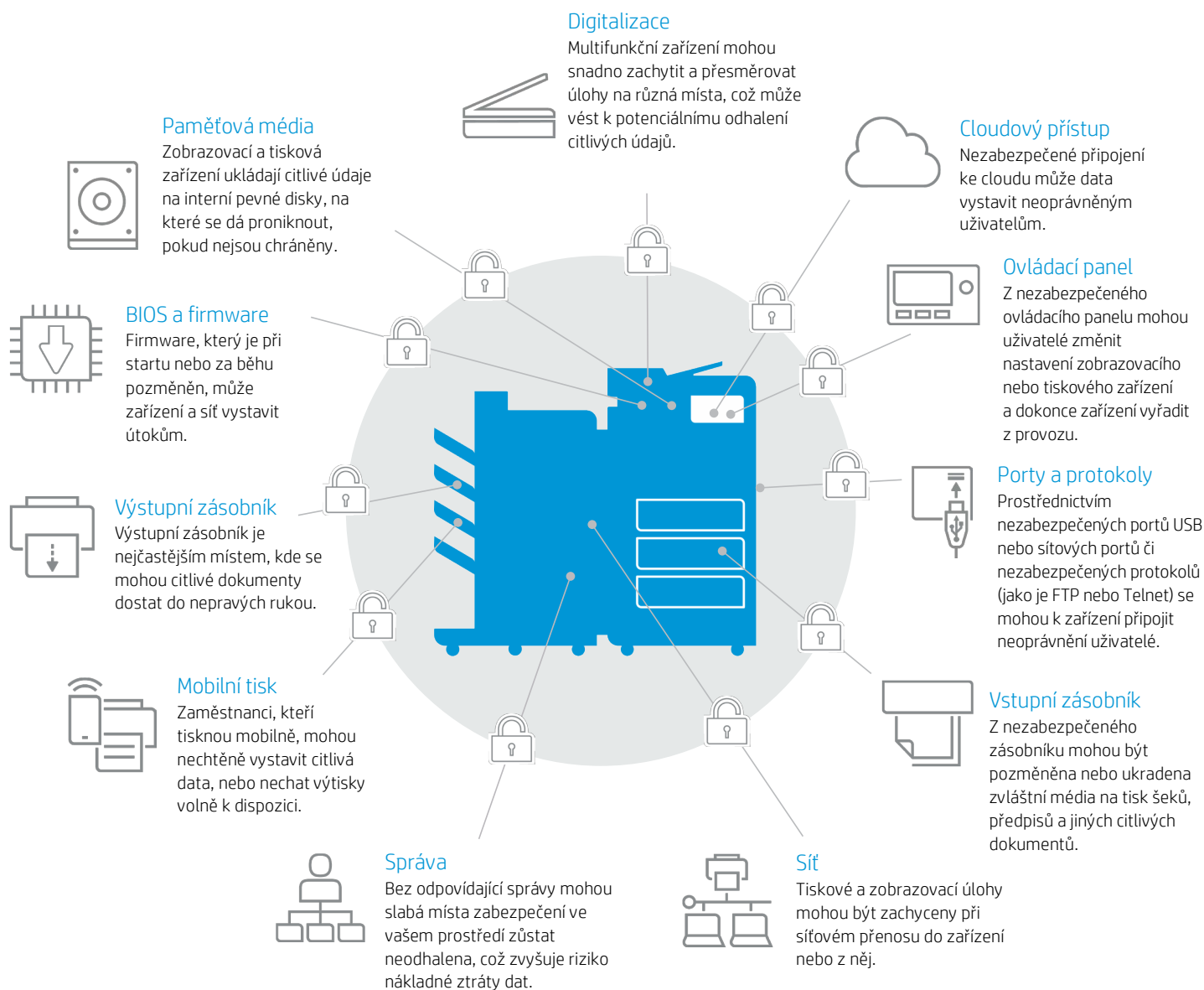
„Důkazem dlouhodobé investice do zabezpečení tisku je nejširší a nekomplexnější portfolio bezpečnostních řešení a služeb společnosti HP na trhu.“

– Quocirca, leden 2017⁵

Chraňte svá zařízení, data a dokumenty

V prostředí zobrazovacích a tiskových zařízení se může vyskytnout několik kritických slabých míst. Když se s těmito slabými místy seznámíte, dokážete lépe riziko omezit.

Zranitelná místa tisku a zpracování obrazu





Ochrana zařízení



Další informace

Služby HP Custom Recycling Services
hp.com/go/businessrecycling

HP Secure Managed Print Services
hp.com/go/securemps

Tiskárny HP jsou navrženy tak, aby spolupracovaly s řešeními pro správu a monitorování zabezpečení. Pomůže to snížit rizika, zlepšit soulad a celkově ochránit síťové prostředí. (Všechny funkce a řešení nemusejí být k dispozici pro všechna zařízení HP.⁶⁾)

Základní bezpečnostní postupy

Šifrované úložiště a bezpečné mazání

Všechny citlivé údaje uložené na interním pevném disku jsou potenciálně zranitelné. Mnoho zařízení HP je vybaveno vestavěným šifrováním, které zajišťuje bezpečnost údajů. Když uložená data nejsou nadále zapotřebí, využijte integrovaných možností zařízení k bezpečnému přepsání dat a odstranění citlivých údajů.

Bezpečná likvidace

Služba *HP Custom Recycling Services* se postará o to, že před odpovědnou recyklací vyřazených produktů budou data z pevných disků vymazána.

Zabezpečený přístup k opravě tiskáren

Pokud znáte bezpečnostní postupy firem, které zajišťují údržbu tiskáren, můžete lépe chránit citlivá data. Odbornou pomoc získáte prostřednictvím *HP Secure Managed Print Services (MPS)* nebo u partnerů HP.

Zakázání nepoužívaných portů a protokolů

Správnou konfigurací zařízení omezíte počet míst citlivých k útoku. Zakázáním fyzických portů a nezabezpečených protokolů (jako FTP nebo Telnet) předejdete neoprávněnému přístupu nebo použití.

Řízení administrátorského přístupu k zařízením

Nastavte hesla správce, aby k nastavení a konfiguraci zařízení měli přístup pouze pracovníci IT nebo jiný oprávněný personál.

Seznamy povolených kódů firmwaru

Na následující straně se dozvíte, jak seznamy povolených programů pomohou ochránit vaše zařízení před malwarem.

Pokročilé bezpečnostní postupy

Certifikace podle společných kritérií

Firemní tiskárny HP jsou certifikovány v souladu s mezinárodně uznávanými bezpečnostními standardy, jako je Certifikace podle společných kritérií (CCC) či standard FIPS 140. Kontrolujte, že kód aktualizací firmwaru je podepsán, aby byla zajištěna jeho pravost a integrita a dodrženy předpisy.



Další informace

Funkce integrovaného zabezpečení tisku:

- HP Sure Start (integrita systému BIOS)
- Seznamy povolených kódů firmwaru
- Detekce neoprávněného vniknutí za běhu
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Funkce zabezpečení tisku automaticky odhalí a zastaví útoky

Firemní tiskárny HP obsahují funkce zabezpečení, díky nimž se nestanou vstupní branou pro útoky na vaši síť. Zabezpečení tisku společnosti HP odhaluje hrozby v reálném čase díky automatickému monitorování a integrovanému softwaru pro zastavení hrozeb ve chvíli, kdy se objeví.⁷

Firemní tiskárny HP, od řady Pro⁸ po Enterprise,⁷ jsou vždy ve střehu a neustále detekují a zastavují hrozby ve všech fázích provozu.

- **Při spuštění.** Spouštěcí kód (u zařízení Pro) nebo BIOS (u zařízení Enterprise) je sada pokynů pro načtení kritických hardwarových komponent a spuštění firmwaru. Integrita kódu je ověřována při každém spuštění a pomáhá tak ochránit vaše zařízení před útokem.
- **Při načítání firmwaru.** *Povolování programů* při spuštění kontroluje firmware a zjišťuje, zda je kód důvěryhodný a správný (digitálně podepsaný společností HP). V případě odhalení neobvyklého chování se zařízení restartuje do bezpečného stavu offline a upozorní oddělení IT.
- **Při provozu.** Vestavěné funkce HP pomáhají chránit paměť zařízení, když jsou zařízení zapnuta a připojena k síti. Právě tehdy probíhá nejvíce útoků. V případě útoku se zařízení automaticky vypne.

Zařízení HP Enterprise se dokážou automaticky zotavit

Tiskárny HP Enterprise dokážou nejen odhalit a zastavit hrozby, ale také se automaticky zotavit z útoků, takže není nutný zásah pracovníků IT.⁷ Tyto funkce v případě detekce útoku nebo neobvyklého chování automaticky zařízení restartují. Správci mohou dostat upozornění prostřednictvím nástrojů pro správu bezpečnostních informací a událostí (SIEM), jako je ArcSight, Splunk a SIEMONSTER.

- Program *HP Sure Start* je systém typu bios, který dokáže automaticky opravovat problémy.⁷ V případě, že dojde k jeho poškození, HP Sure Start restartuje s bezpečnou originální verzí.
- *Detekce neoprávněného vniknutí za běhu* kontroluje složité operace ve firmwaru a paměti, dokáže automaticky zastavit neoprávněné vniknutí a v případě útoku vynutit restartování.
- *Nástroj HP Connection Inspector* vyhodnocuje odchozí připojení k síti, aby mohl určit normální chování, zastavit podezřelé požadavky a automaticky vynutit restart a zabránit tak spuštění malware.

Díky ochraně investic, kterou firmware HP FutureSmart s možností upgradu poskytuje, můžete seznamy povolených programů, detekci neoprávněného vniknutí za běhu a nástroj HP Connection Inspector přidat k mnoha stávajícím modelům tiskáren HP Enterprise.⁷

Nástroj HP JetAdvantage Security Manager dokončí cyklus kontroly

Po restartu nebo při každém přidání nového zařízení do sítě nástroj *HP JetAdvantage Security Manager* automaticky vyhodnotí bezpečnostní nastavení zařízení a v případě potřeby je upraví tak, aby byla v souladu s definovanými podnikovými zásadami.⁹ Pracovníci oddělení IT nemusejí nijak zasahovat.

Jak to funguje?

Funkce integrovaného zabezpečení se zaměřují na čtyři hlavní kroky provozního cyklu zařízení HP.

V případě útoku se zařízení HP Enterprise dokážou restartovat a zotavit.

Nástroj HP JetAdvantage Security Manager dokončí cyklus kontroly.

Čtyři. Nepřetržité monitorování

Chrání zařízení a brání útokům za běhu. Kontroluje odchozí síťová připojení, aby zastavoval podezřelé požadavky (pouze zařízení Enterprise).

Tři. Kontrola nastavení

Po restartování HP JetAdvantage Security Manager zkontroluje a opraví případná vadná bezpečnostní nastavení zařízení.

Jedna. Kontrola systému BIOS / spouštěcího kódu

Umožní načtení pouze originálního kódu podepsaného společností HP a zabrání tak spuštění škodlivého kódu při startu.

Dvě. Kontrola firmwaru

Umožní načíst pouze autentický, ověřený firmware – s digitálním podpisem společnosti HP.





Ochrana dat



Další informace

HP Web Jetadmin
hp.com/go/wja

Univerzální tiskový ovladač HP s funkcí Secure Encrypted Print
hp.com/go/upd

Řešení pro pracovní postupy HP JetAdvantage Workflow
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Data vyžadují neustálou ochranu, jak při přenosu, tak při uložení. Představujeme několik základních kroků, které pomohou zajistit bezpečný přenos a použití.⁶

Základní bezpečnostní postupy

Síťové standardy 802.1x nebo IPsec

Použijte šifrované síťové standardy pro ochranu dat přenášených v síti mezi zařízením a nástroji pro správu, jako je *HP Web Jetadmin* nebo *HP Embedded Web Server*.

Šifrování přenášených dat

Tiskové úlohy odesílané do tiskárny můžete ochránit řadou možností šifrování, jako je protokol IPP přes TLS (IPPS). *HP Universal Print Driver Secure Encrypted Print* poskytuje při přenosu od klienta na tiskárnu symetrické šifrování a dešifrování tiskových úloh algoritmem AES256 na základě uživatelem definovaného hesla s využitím šifrovacích knihoven od společnosti Microsoft® ověřených standardem FIPS 140.

Řešení *HP JetAdvantage Workflow* dokážou při skenování snadno ochránit citlivé údaje a zároveň zvýšit efektivitu. Nástroj HP Capture and Route například bezproblémově spolupracuje s řešením HP Access Control a zvyšuje zabezpečení, přičemž můžete pohodlně využívat jediné ověření a možnost monitorovat obsah v rámci řízení informací.¹⁰

Šifrování neaktivních dat

Ochrňte citlivé podnikové údaje uložené pevném disku s vestavěným šifrováním. Pro další úroveň zabezpečení je vhodné přidat k zařízení volitelný doplněk HP Trusted Platform Module (TPM), který posílí ochranu šifrovaných přihlašovacích údajů a dat automatickým zapečetěním šifrovacích klíčů zařízení k TPM. Generuje a chrání soukromé klíče certifikátů a zajišťuje tak zabezpečenou identitu zařízení.

Ochrana branou firewall

Nedovolte malwaru a virům vniknout do vaší sítě omezením přístupu tiskárny k výpočetním zařízením v síti.

Nativní ověřování uživatelů

Povinné přihlášení uživatelů prostřednictvím kódu PIN/PIC, LDAP nebo ověřování Kerberos sníží náklady a bezpečnostní rizika. Tyto způsoby můžete také integrovat se službou Active Directory.

Řízení přístupu na základě rolí

HP Access Control Rights Management pomáhá snižovat náklady a bezpečnostní rizika omezením funkcí tiskárny. Řízením přístupu na základě rolí můžete různým uživatelům nebo – v závislosti na vašich potřebách – dokonce i celým oddělením přidělovat odlišné možnosti. Můžete například omezit přístup k faxu, skenování do e-mailu nebo skenování do faxu.

Pokročilé bezpečnostní postupy

Pokročilé ověřování a sledování

Pokročilá řešení pro ověřování (hesla, bezkontaktní karty, čipové karty nebo biometrické údaje) a sledování přinášejí větší zabezpečení a kontrolu.



- *HP Access Control Secure Authentication* obnoví kontrolu, posílí zabezpečení a sníží náklady. Získáte celou řadu pokročilých opatření a možností, jako je například dotykové ověření pomocí mobilních telefonů s NFC.
- *HP Access Control Job Accounting* pomáhá přesně sledovat a shromažďovat údaje, analyzovat výsledky a vytvářet a zasílat přehledy. S využitím získaných dat můžete rozpočítat náklady na tisk, motivovat zaměstnance k efektivnějšímu tisku a dodat oddělení IT potřebné informace k vylepšení předpovědí pro podniková zařízení.

Další informace

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

Řešení HP Capture and Route
hp.com/go/hpcr

Mobilní zařízení jsou zahrnutá v přístupu k síti

Použijte mobilní zařízení k řízení přístupu k tiskárnám jako součást svých globálních zásad tiskové bezpečnosti. Společnost HP nabízí serverová řešení poskytující bezpečný tisk ze serveru a také pokročilé funkce pro správu a vykazování.

- *HP JetAdvantage Connect** nabízí intuitivní a spolehlivý mobilní tisk určený pro podniky. Pomáhá ušetřit čas a peníze, protože dokáže ke správě mobilního tisku hladce využít stávající síťové nástroje a zásady IT.¹¹ Uživatelé mohou bezpečně tisknout z celé řady smartphonů a tabletů, kdykoli a kdekoli to potřebují, stejně snadno jako z počítače.
- *HP Access Control* zahrnuje možnosti správy mobilního tisku. Využívá stávající e-mailovou infrastrukturu a umožňuje mobilním uživatelům zaslat tiskovou úlohu do fronty e-mailem a poté ji vytisknout na kterékoli tiskárně nebo multifunkčním zařízení podporujícím toto řešení. Ochraňte tisková zařízení v síti funkcemi zabezpečeného ověřování, jako je Mobile Release.

Zastavte úniky dat hned v počátku

Řešení společnosti HP poskytují možnosti, které chrání před ztrátou dat. S preventivním programem *HP Capture and Route Data Loss* ochráníte citlivé informace před skenováním nebo faxováním. Preventivní program *HP Access Control Print Data Loss* zabrání vytištění citlivých dokumentů. Sledujte svá nejdůležitější data, abyste předešli jejich úniku, aniž by se zpomalila práce. Podle toho, jaké podmínky si vyberete, budete dostávat bezpečnostní výstrahy.

Nastavení digitálních certifikátů u tiskáren

Použijte v síťových tiskárnách a multifunkčních zařízeních digitální certifikáty a zlepšete tak zabezpečení tiskového prostředí. Ušetřete čas použitím nástroje HP JetAdvantage Security Manager, který se postará o automatickou instalaci a obnovu certifikátů.⁹



Ochrana dokumentů



Další informace

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Ochrana dokumentů společností HP a TROY
hp.com/go/HPandTROY

Integrujte inteligentní hardwarová a softwarová řešení do širšího plánu zabezpečení IT. Ochraňte tak citlivé údaje v tištěných dokumentech.⁶

Základní bezpečnostní postupy

Kontrola přístupu k předtištěným formulářům

Vybavte své tiskárny a multifunkční zařízení zásobníky papíru, které lze uzamknout, a zabráníte tak krádeži speciálního papíru pro tisk šeků, předpisů nebo jiných citlivých dokumentů.

Pro ochranu citlivých údajů použijte volitelný kód PIN nebo tisk s ověřením.

Uživatelé si mohou zvolit tisk s kódem PIN nebo s ověřením a omezit tak svou závislost na osobních tiskárnách i riziko, že se vytisknuté úlohy dostanou do nepovolených rukou. Tato bezpečnostní opatření také omezí počet nevytisknutých výtisků, což sníží náklady a plýtvání.

Při tisku s kódem PIN uživatelé po odeslání důvěrné tiskové úlohy zvolí PIN, který je zapotřebí zadat na tiskárně pro uvolnění úlohy.

Při tisku s ověřením jsou tiskové úlohy uloženy v cloudu nebo na počítači uživatele. Uživatelé pak provedou ověření na zvoleném místě tisku a mohou úlohu vytisknout. Společnost HP nabízí dvě cloudová řešení tisku s ověřením:*

- *HP JetAdvantage Secure Print* je cenově dostupná možnost určená pro malé a střední podniky. Tiskové úlohy jsou uloženy v cloudu nebo na počítači uživatele. Nastavení i použití je snadné, uživatelé mohou úlohy uvolnit z mobilního zařízení a řešení podporuje zařízení od různých dodavatelů.¹²
- *HP JetAdvantage Private Print* je bezplatné cloudové řešení společnosti HP, které přináší výhody tisku s ověřením bez zbytečné složitosti. Nastavení je snadné a nevyžaduje server, instalaci ani údržbu.¹³

Pokročilé bezpečnostní postupy

Tisk s ověřením pro všechny tiskové úlohy

HP Access Control Secure Pull Printing pomáhá chránit důvěrné údaje, zlepšit zabezpečení zařízení a zvýšit efektivitu. Toto volitelné robustní serverové řešení nabízí mnoho způsobů ověřování, včetně identifikační karty, a zabezpečení na firemní úrovni a funkce pro správu.

Použijte MICR, vodoznaky a další funkce, které brání kopírování a úpravám.

Řešení proti padělení HP a TROY* zahrnují bezpečnostní toner, který znehodnotí papír, pokud dojde k chemické manipulaci, přidávají různé vodoznaky na vytištěné strany a začleňují strojově čitelné kódy pro sledování jednotlivých dokumentů. Při tisku citlivých dokumentů, jako jsou předpisy, rodné listy nebo přepisy, lze na multifunkčním zařízení použít funkce proti podvodům – vlastní podpisy, loga společnosti a bezpečnostní fonty.



Monitorování a správa tiskového prostředí



Další informace

Program na správu zabezpečení HP
JetAdvantage Security Manager
hp.com/go/securitymanager

Řešení pro monitorování a správu zabezpečení pomohou odhalit slabá místa a zavést jednotný přístup k ochraně dat založený na zásadách. Posílí tak dodržování zásad a omezí rizika.⁶ Odstraňte nedostatky v zabezpečení a předejdete tak nákladným pokutám.

Základní bezpečnostní postupy

Aktualizace zařízení na nejnovější firmware/OS

Pomocí aplikace HP Web Jetadmin¹⁴ můžete aktualizovat firmware na všech podnikových zařízeních, takže budou mít vždy nejnovější funkce ochrany a zabezpečení.

Kontrola protokolu událostí zabezpečení tiskárny

Zařízení HP zasílají události a oznámení tiskárny na server syslog, takže pracovníci IT mohou v případě potřeby odstranit problémy.

Vyhodnocení a úprava nastavení zařízení

Sada *HP Print Manageability Integration Kit* (MIK), plug-in pro software Microsoft® System Center Configuration Manager (SCCM), umožňuje spravovat základní nastavení všech tiskáren. Microsoft SCCM je populární řešení pro správu, které zajišťuje vzdálené plánování, nasazení, konfiguraci a sledování koncových zařízení. Sada HP Print MIK dokáže zjistit, vyhodnotit a upravit 15 nejdůležitějších bezpečnostních nastavení a vykázat výsledky.

Pokud stojíte o kompletní řešení pro správu zabezpečení všech zařízení, zvolte *HP JetAdvantage Security Manager*.⁹ Toto řešení pomůže snížit náklady a využití zdrojů, nastavit jednotné bezpečnostní zásady pro všechna zařízení, automatizovat úpravu nastavení a instalovat a obnovit jedinečné certifikáty. Zároveň poskytuje protokoly potřebné k doložení souladu.



Další informace

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Pokročilé bezpečnostní postupy

Použijte software SIEM pro detekci a zaznamenávání hrozeb

Data událostí ze zařízení HP FutureSmart lze zasílat do nástrojů pro detekci incidentů, jako je ArcSight, Splunk a SIEMonster, a zajistit tak monitorování v reálném čase. Zabezpečení IT může snadno zobrazit tiskárny jako součást širšího ekosystému IT a odhalit a vyřešit tak bezpečnostní výstrahy.

Automatická konfigurace nových tiskových zařízení po připojení k síti

Funkce Instant-on Security, která je součástí aplikace HP JetAdvantage Security Manager, automaticky nakonfiguruje nová zařízení při přidání do sítě nebo po restartování.

Hlášení zabezpečení tiskových zařízení pro účely kontroly souladu

Pomocí aplikace HP JetAdvantage Security Manager můžete vytvořit hlášení o souladu s pravidly a doložit použití bezpečnostních zásad u tiskáren a zabezpečení zákaznických údajů.

Porušení předpisů může poškodit váš podnik

Koncová zařízení s žádnou nebo nedostatečnou ochranou jsou snadným terčem pro kybernetickou kriminalitu. Ve snaze rostoucí hrozbu omezit zavádějí vládní organizace po celém světě přísné bezpečnostní předpisy, které vyžadují, aby podniky údaje svých zákazníků lépe chránily.

Organizace, které je nedodrží, riskují vysoké náklady v podobě pokut, ušlého

zisku, poškození dobré pověsti a hromadných žalob.

Je zcela zásadní nasadit zařízení a řešení, jako jsou tiskárny HP Enterprise a software HP JetAdvantage Security Manager, která vám pomohou splnit zákonné požadavky a ochránit podnikové údaje před bezpečnostními hrozbami.



Získejte potřebnou pomoc

Ochranu a zabezpečení nemusíte zajišťovat na vlastní pěst. Poradci z týmu podpory vám mohou ukázat, jak zlepšit zabezpečení dat, zařízení a dokumentů.

Společně s odborníky na zabezpečení tisku zhodnotíte slabá místa stávající ochrany. Pomůžeme vám vytvořit ucelené zásady zabezpečení tisku, vycházející z potřeb vašeho podniku a osvědčených postupů, a plán na zlepšení zabezpečení ve vašem konkrétním prostředí.

Ve svém oboru nemá konkurenci

První zpráva IDC MarketScape věnovaná hodnocení dodavatelů bezpečnostních řešení a tiskových služeb z celého světa a jejich výsledků v roce 2017 o společnosti HP hovoří jako o špičce v oboru. (Studii si můžete přečíst [zde](#).) Zpráva uvádí, že „přístup společnosti HP k zabezpečení zohledňuje veškerou infrastrukturu tisku a dokumentů, od zamknutí zařízení po všechny aspekty používání zařízení a ochrany obsahu.“ Zde zobrazený graf je z hodnocení dodavatelů IDC pro rok 2017.¹⁵

Model analýzy dodavatelů IDC MarketScape poskytuje přehled o konkurenceschopnosti dodavatelů informačních a komunikačních technologií na daném trhu. Metodologie výzkumu používá přísnou metodiku hodnocení založenou na kvalitativních i kvantitativních kritériích, díky nimž je pozice každého dodavatele na daném trhu jednotlivě znázorněna na grafice. Výsledky hodnocení schopností poměří produkt dodavatele, připravenost na trh a výkonnost podniku v krátkodobém časovém horizontu. Výsledky hodnocení strategie měří, zda strategie dodavatelů odpovídá v 3- až 5letém časovém horizontu požadavkům zákazníků. Podíl trhu dodavatele představuje velikost ikony.¹⁵

Začínáme

Kontaktujte svého prodejního zástupce a požádejte o další informace o bezpečnostních funkcích, řešeních a službách HP, které vám mohou přinést lepší ochranu a jistotu, že je vše pod kontrolou.

Více informací

hp.com/go/printsecurity

¹ Tvzení o „nejlépe zabezpečeném tisku“ vychází z průzkumu publikovaných bezpečnostních funkcí tiskáren HP stejné třídy, který provedla společnost HP v roce 2017. Společnost HP nabízí kombinaci bezpečnostních funkcí, které monitorují, odhalují a automaticky zastavují útoky a následně automaticky ověřují integritu softwaru po restartování. Seznam produktů naleznete na stránce hp.com/go/LJCompatibility.

² InfoTrends, „Designing Hardware & Solutions“ (Návrh hardwaru a řešení), Brendan Morse, říjen 2016.

³ Quocirca, „Managed Print Services Landscape, 2016“ (Prostředí služeb spravovaného tisku), quocirca.com/content/managed-print-services-landscape-2016, červenec 2016.

⁴ Průzkum společnosti Spiceworks, kterého se zúčastnilo 309 činitelů odpovědných za IT ze Severní Ameriky, oblasti EMEA a oblasti APAC, jménem společnosti HP, listopad 2016.

⁵ Quocirca, „Print security: An imperative in the IoT era“ (Zabezpečení tisku: Základ v éře internetu věcí), quocirca.com/content/print-security-imperative-iot-era, leden 2017.

⁶ Řešení nemusí být podporována ve všech zařízeních HP. Některá řešení vyžadují zakoupení dodatečného příslušenství.

⁷ Zařízení HP Enterprise s firmwarem FutureSmart 4.5 nebo novějším využívají nejpokročilejší integrované bezpečnostní funkce společnosti HP. Údaje vycházejí z průzkumu publikovaných integrovaných bezpečnostních funkcí tiskáren HP stejné třídy, který provedla společnost HP v roce 2017. Společnost HP nabízí kombinaci bezpečnostních funkcí pro kontrolu integrity až po systém BIOS a možnosti automatického zotavení.

⁸ Vybraná zařízení HP LaserJet Pro a PageWide Pro obsahují vestavěné funkce, které dokážou odhalit a zastavit útok. Další informace naleznete na stránce hp.com/go/LJCompatibility.

⁹ Produkt HP JetAdvantage Security Manager je třeba zakoupit samostatně. Další informace naleznete na stránce hp.com/go/securitymanager.

¹⁰ Při zasílání informací do koncového úložiště chráněného heslem je zapotřebí zadat další heslo.

¹¹ HP JetAdvantage Connect podporuje přední mobilní zařízení. Na zařízení s operačním systémem Android™, Google Chrome™ a Microsoft® je třeba nainstalovat jednorázový modul plug-in. Podrobnosti a seznam všech podporovaných operačních systémů naleznete na stránce hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Tisk s ověřováním lze použít na kterékoli tiskárně nebo multifunkční tiskárně s připojením k síti. Ověřování v zařízení je k dispozici pro celou řadu zařízení HP LaserJet, PageWide a OfficeJet Pro a vybraná zařízení jiných výrobců. Některá zařízení mohou vyžadovat aktualizaci firmwaru. Uložení a přístup k tiskovým úlohám z cloudu vyžaduje připojení k internetu. Provedení tiskové úlohy z mobilních zařízení vyžaduje síťové připojení a kód QR. Další informace a seznam podporovaných tiskáren a multifunkčních zařízení naleznete na stránce hp.com/go/JetAdvantageSecurePrint.

¹³ Technologie HP JetAdvantage Private Print je k dispozici zdarma. Vyžaduje připojení tiskárny k internetu a povolení webových služeb. Není k dispozici ve všech zemích. Více informací naleznete na stránce hp.com/go/JetAdvantagePrivatePrint.

¹⁴ Aplikace HP Web Jetadmin je zdarma ke stažení na stránce hp.com/go/webjetadmin.

¹⁵ Podle analýzy dodavatelů tiskových řešení provedené společností IDC a vyjádření k přední pozici společnosti HP: „Společnost HP se opírá o kvalitní služby a funkce IT, ... a nabízí ucelenou, integrovanou bezpečnostní strategii pro celou infrastrukturu IT.“ ZDROJ: [Zpráva IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](#), Allison Correia a Robert Palmer, říjen 2017, č. dokumentu společnosti IDC: US41988517.

* Dostupnost řešení tisku se mohou podle země lišit.

Přihlásit se k odběru novinek

hp.com/go/getupdated



Sdílet dokument s kolegy

© Copyright 2014–2018 HP Development Company, L.P. Uvedené informace mohou být změněny bez předchozího upozornění. Jediná záruka k produktům a službám společnosti HP je určena záručními podmínkami přiloženými k těmto produktům a službám. Ze žádných zde uvedených informací nelze vyvodit existenci dalších záruk. Společnost HP není odpovědná za technické či redakční chyby ani za opomenutí vyskytující se v tomto dokumentu.

Android a Google Chrome jsou registrované ochranné známky společnosti Google Inc. Microsoft je registrovaná ochranná známka skupiny společností Microsoft v USA.

4AA3-1295CSE, leden 2018, vyd. 11

