



Chránite svoju sieť najbezpečnejšou tlačou od HP¹

94 %

firiem z oblasti finančníctva tvrdí, že zabezpečenie kopírok alebo tlačiarne je dôležité alebo veľmi dôležité²



61 %

organizácií minulý rok nahlásilo aspoň jeden únik dát v súvislosti s tlačiarnami³



43 %

spoločností ignoruje tlačiarne pri zabezpečovaní svojich koncových zariadení⁴





Iba 18 % spoločností monitoruje hrozby tlačiarňí.⁴ Robí to aj vaša?

Pochopenie skrytých rizík

Úlohou pracovníkov IT je neustále chrániť dôverné informácie (vrátane identít zamestnancov a dát zákazníkov) v rôznych zariadeniach a prostrediach. Hoci mnohé IT oddelenia starostlivo chránia jednotlivé počítače a sieť samotnú, tlačové a zobrazovacie zariadenia sú zvyčajne prehliadané a nechránené. Nechránené zariadenia môžu celú sieť vystaviť bezpečnostnému riziku a kybernetickému útoku.

Pochopenie možných nákladov

Aj jeden bezpečnostný prienik môže vyjsť drahú. Ohrozenie osobných údajov z dôvodu nezabezpečenia tlače a zobrazovania môže mať za následok krádež identity, krádež informácií o konkurencii, poškodenie mena značky a súdne spory. Okrem toho môže nesúlad s regulačnými a právnymi normami vyústiť do vysokých pokút.

HP dokáže pomôcť

Chráňte svoju sieť najbezpečnejšou tlačou HP.¹ Tlačiarne HP sú vždy v strehu, neustále nachádzajú a zastavujú hrozby a dokážu sa prispôbiť novým. Spoločnosť HP vám vďaka širokému portfóliu produktov pomôže zautomatizovať ochranu zariadení, dát a dokumentov. Naši experti na bezpečnosť tlače vám pomôžu navrhnúť a nasadiť komplexnú bezpečnostnú stratégiu tlače a zobrazovania.

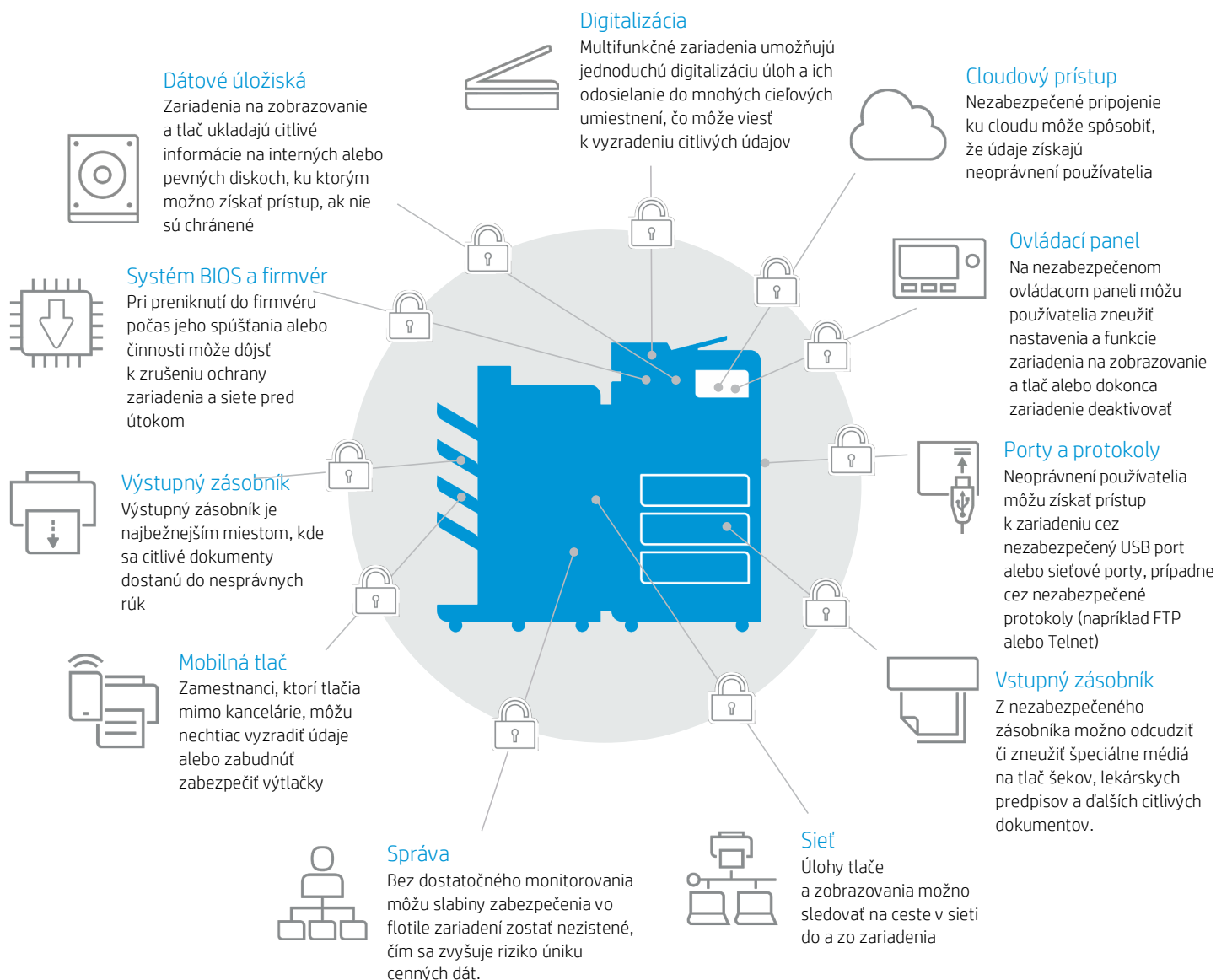
„Na základe dlhoročných investícií do zabezpečenia tlače má spoločnosť HP najširšie a najpodrobnejšie portfólio riešení a služieb zabezpečenia na trhu.“

– Quocirca, január 2017⁵

Ochrana zariadení, dát a dokumentov

Kritické riziká môžu existovať na viacerých miestach vo vašom prostredí zobrazovania a tlače. Keď týmto rizikám porozumíte, môžete ich jednoduchšie eliminovať.

Rizikové body pri zobrazovaní a tlači





Ochrana zariadenia



Ďalšie informácie

HP Custom Recycling Services
hp.com/go/businessrecycling

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

Tlačiarne HP sú navrhnuté na spoluprácu s riešeniami monitorovania a správy zabezpečenia, aby pomáhali znižovať riziká, zaistiť lepší súlad s platnými normami a chrániť celú sieť. (Dostupnosť funkcií závisí od konkrétneho zariadenia HP.⁶)

Základné bezpečnostné opatrenia

Šifrované úložisko s bezpečným vymazávaním

Všetky citlivé informácie uložené na internej jednotke alebo pevnom disku sú ohrozené potenciálnou krádežou. Mnoho zariadení HP má na ochranu dát zabudované šifrovanie. Keď už uložené dáta nie sú viac potrebné, pomocou funkcií integrovaných v zariadení ich môžete bezpečne prepísať a citlivé informácie bezpečne odstrániť.

Bezpečná likvidácia

Služba *HP Custom Recycling Services* dokáže pred zodpovednou recykláciou starých produktov zabezpečiť odstránenie dát z pevných diskov.

Zabezpečený prístup pri oprave tlačiarne

Ak poznáte bezpečnostné postupy poskytovateľov údržby tlačiarne, budete môcť lepšie chrániť citlivé údaje. Expertnú pomoc vám poskytne *HP Secure Managed Print Services (MPS)* alebo partneri spoločnosti HP.

Deaktivácia nepoužívaných portov a protokolov

Zmenšíte oblasť možného útoku správnou konfiguráciou zariadenia. Deaktiváciou fyzických portov a nezabezpečených protokolov (ako napríklad FTP či Telnet) zabránite neoprávnenému prístupu alebo používaniu.

Správcovský prístup k ovládaniu zariadenia

Nastavte heslá správcu tak, aby nastavenia zariadení mohli nastavovať a konfigurovať iba pracovníci IT oddelenia alebo iní autorizovaní pracovníci.

Overovanie vstupných údajov kódu firmvéru

Informácie o tom, ako overovanie vstupných údajov kódu pomáha chrániť vaše zariadenia pred malvérom, nájdete na ďalšej strane.

Pokročilé bezpečnostné opatrenia

Certifikácia Common Criteria Certification

Podnikové tlačiarne HP sú certifikované a v súlade s medzinárodne uznávanými bezpečnostnými štandardmi – certifikáciou Common Criteria Certification (CCC) a FIPS 140. Na zachovanie súladu sa uistite, že aktualizácie firmvéru zariadení sú podpísané kódom potvrdzujúcim pravosť a integritu kódu.



Ďalšie informácie

Integrované funkcie zabezpečenia tlače:

- HP Sure Start (Integrita systému BIOS)
- Overovanie vstupných údajov kódu firmvéru
- Detekcia narušenia počas prevádzky
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Automatické zisťovanie a zastavovanie útokov bezpečnostnými funkciami tlače

Podnikové tlačiarne HP obsahujú bezpečnostné funkcie, ktoré ich pomáhajú chrániť, aby sa nestali vstupným bodom útokov na vašu sieť. Zabezpečenie tlače od spoločnosti HP ponúka zisťovanie v reálnom čase, automatizované monitorovanie a integrované softvérové overovanie hrozieb od momentu, kedy vzniknú.⁷

Podnikové tlačiarne HP Pro⁸ až Enterprise⁷ sú stále v strehu a neustále zisťujú a zastavujú hrozby počas všetkých fáz prevádzky:

- **Počas spúšťania.** Spúšťací kód (v zariadeniach Pro) alebo BIOS (v zariadeniach Enterprise) je súbor pokynov na načítanie kritických hardvérových súčastí a spustenie firmvéru. Integrita kódu sa overuje pri každom spúšťacom cykle, čo pomáha chrániť vaše zariadenie pred útokom.
- **Počas načítavania firmvéru.** *Overovanie vstupných údajov* (whitelisting) automaticky skontroluje firmvér počas spúšťania a overuje, či ide o autentický kód, ktorý je digitálne podpísaný HP. Ak sa zistí anomália, zariadenie sa reštartuje do bezpečného offline stavu a upozorní IT oddelenie.
- **Počas prevádzky.** Integrované funkcie od HP pomáhajú chrániť pamäť zariadení v čase prevádzky a pripojenia k sieti. Vtedy totiž dochádza k väčšine útokov. V prípade útoku sa zariadenie vypne.

Zariadenia HP Enterprise sa dokážu automaticky opravovať

Okrem toho, že dokážu zisťovať a odhaľovať útoky, dokážu tlačiarne HP Enterprise automaticky spustiť samoliečbu z útokov, takže IT oddelenie nemusí zasiahnuť.⁷ V prípade útoku alebo anomálie dokážu funkcie tlačiarne spustiť automatický reštart. Správcovia môžu dostať upozornenie prostredníctvom nástrojov Security Information and Event Management (správy bezpečnostných informácií a udalostí – SIEM), ako sú ArcSight, Splunk a SIEMonster.

- *HP Sure Start* je špičkový BIOS s funkciou automatickej opravy chýb.⁷ V prípade preniknutia do systému BIOS reštartuje HP Sure Start zariadenie s bezpečnou oficiálnou kópiou systému BIOS.
- *Zisťovanie neoprávnených vniknutí počas prevádzky* monitoruje komplexné operácie firmvéru a v pamäti zariadenia, automaticky zastavuje narušenia a v prípade útoku reštartuje zariadenie.
- *HP Connection Inspector* vyhodnocuje odchádzajúce sieťové pripojenia, aby mohol určiť, čo je normálne, zastavovať podozrivé žiadosti a zastavovať malvér automatickým spustením reštartu.

S inovovateľným firmvérom HP FutureSmart môžete nasadiť funkcie overovania vstupných údajov, zisťovania neoprávnených vniknutí počas prevádzky a HP Connection Inspector do mnohých aktuálne používaných tlačiarň HP Enterprise a chrániť tak svoje investície.⁷

Cyklus kontroly dokončí HP JetAdvantage Security Manager

HP JetAdvantage Security Manager automaticky vyhodnotí situáciu po reštarte alebo vždy, keď sa do siete pridá nové zariadenie, a ak je to potrebné, automaticky upraví bezpečnostné nastavenia zariadenia tak, aby bolo v súlade s prednastavenými politikami spoločnosti.⁹ Zásah IT oddelenia nie je potrebný.

Ako to funguje?

Integrované funkcie zabezpečenia riešia štyri primárne kroky v cykle zariadenia HP.

V prípade útoku sa zariadenia HP Enterprise dokážu reštartovať a automaticky opraviť chyby.

Cyklus kontroly dokončí softvér HP JetAdvantage Security Manager.

Štyri. Nepretržité monitorovanie

Chráni procesy a zastavuje útoky, keď je zariadenie spustené.

Pomocou kontroly odchádzajúcich sieťových pripojení zastavuje podozrivé žiadosti (iba zariadenia Enterprise).

Tri. Kontrola nastavení

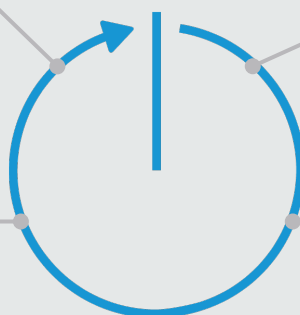
Po reštartovaní HP JetAdvantage Security Manager skontroluje a opraví všetky zmeny v nastaveniach zabezpečenia zariadenia.

Jeden. Kontrola systému BIOS/spúšťacieho kódu

Bráni spusteniu škodlivého kódu počas spúšťania zariadenia tým, že umožňuje načítanie iba originálneho kódu s podpisom HP.

Dva. Kontrola firmvéru

Načíta sa iba overený firmvér – s digitálnym podpisom HP.





Ochrana dát



Ďalšie informácie

HP Web Jetadmin
hp.com/go/wja

Univerzálny tlačový ovládač HP Universal Print Driver s funkciou Secure Encrypted Print
hp.com/go/upd

Riešenia pracovných postupov HP JetAdvantage
hp.com/go/documentmanagement

Riadenie prístupu HP
hp.com/go/hpac

Dáta vyžadujú neustálu ochranu, či už sú uložené, alebo sa prenášajú. Uvádzame niekoľko základných krokov, ako zabezpečiť ich bezpečný prenos do cieľa a používanie.⁶

Základné bezpečnostné opatrenia

Sieťové štandardy 802.1x alebo IPsec

Na ochranu sieťovo prenášaných dát medzi zariadeniami a nástrojmi správy, ako sú *HP Web Jetadmin* alebo *Zabudovaný webový server HP*, použite šifrované sieťové štandardy.

Šifrovanie prenášaných dát

Chráňte tlačové úlohy putujúce do zariadenia pomocou šifrovania, ako je protokol IPPS (internetový tlačový protokol cez TLS). Ďalšou možnosťou je *Univerzálny tlačový ovládač HP Universal Print Driver Secure Encrypted Print* poskytujúci skutočne symetrické šifrovanie a dešifrovanie tlačových úloh na strane klienta štandardom AES256 založenom na hesle vytvorenom používateľom. Heslo využíva overené kryptografické knižnice spoločnosti Microsoft® spĺňajúce štandard FIPS 140.

Počas skenovania pomáhajú *Riešenia pracovných postupov HP JetAdvantage* chrániť citlivé informácie a zároveň zvyšovať efektivitu. HP Capture and Route sa napríklad bezchybne spája s Riadením prístupu HP a posilňuje bezpečnosť. Výhodou je iba jedno overenie totožnosti a možnosť monitorovania obsahu na správu informácií.¹⁰

Šifrovanie nepoužívaných dát

Chráňte citlivé obchodné informácie uložené na pevnom disku pomocou zabudovaného šifrovania. Ďalšiu úroveň zabezpečenia môžete do zariadenia pridať pomocou voliteľného doplnku HP Trusted Platform Module (TPM), ktorý posilňuje ochranu šifrovaných prihlasovacích údajov a dát automatickým zapečatením kryptovacích kľúčov zariadenia pomocou TPM. Generovaním a ochranou privátnych kľúčov k certifikátu poskytuje bezpečnú identitu zariadenia.

Ochrana bránou firewall

Zabráňte malvéru a vírusom preniknúť do siete tým, že obmedzíte prístup tlačiarne k výpočtovým zariadeniam v sieti.

Natívne overenie používateľa

Znížte náklady a riziká zabezpečenia vyžadovaním prihlásenia používateľa pomocou kódov PIN/PIC, protokolu LDAP alebo autentifikáciou v protokole Kerberos. Tieto riešenia môžete tiež integrovať do služby Active Directory.

Riadenie prístupu podľa rolí

HP Access Control Rights Management pomáha znižovať náklady a riziká zabezpečenia pomocou obmedzenia funkcií tlačiarne. Riadenie prístupu na základe rolí vám umožňuje priradiť rôzne funkcie rôznym používateľom alebo dokonca celým oddeleniam podľa ich potrieb. Môžete napríklad obmedziť, kto môže faxovať, skenovať do e-mailu alebo skenovať do faxu.

Pokročilé bezpečnostné opatrenia

Pokročilé overenie a sledovanie

Ďalší stupeň zabezpečenia a kontroly pridáte nasadením pokročilých riešení overovania a sledovania, ako sú heslá, bezkontaktné karty, karty Smart card a biometrické údaje.



Ďalšie informácie

Riadenie prístupu HP
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

- *HP Access Control Secure Authentication* obnovuje kontrolu, posilňuje bezpečnosť a znižuje náklady. Získajte širokú škálu pokročilých ovládacích prvkov a možností vrátane mobilných zariadení s overovaním dotykom pomocou NFC.
- *HP Access Control Job Accounting* vám pomáha presne sledovať a zhromažďovať dáta, analyzovať výsledky a vytvárať či posilať výkazy. Získané dáta môžete použiť na alokovanie nákladov na tlač, motivovanie zamestnancov, aby tlačili efektívnejšie a poskytnutie potrebných informácií IT oddeleniu na zlepšenie predpovedí týkajúcich sa všetkých tlačových zariadení.

Mobilné zariadenia zahrnuté do sieťového prístupu

Využívajte svoje mobilné zariadenia v rámci celkových bezpečnostných pravidiel vzťahujúcich sa na tlač a riadenie prístupu k tlačiarňam. Spoločnosť HP ponúka serverové riešenia, ktoré poskytujú zabezpečené zadržiavanie tlačových úloh, ako aj rozšírené funkcie správy a vytvárania zostáv.

- *HP JetAdvantage Connect** prináša intuitívne a spoľahlivé riešenie mobilnej tlače určené pre podniky. Pomáha šetriť čas aj peniaze, pretože dokáže pri správe mobilnej tlače bezproblémovo využívať existujúce sieťové IT nástroje a politiky.¹¹ Používatelia môžu bezpečne tlačiť zo širokej škály smartfónov a tabletov – kedykoľvek a kdekoľvek, rovnako jednoducho, ako pri tlači z počítačov.
- Súčasťou *Riadenia prístupu HP* sú možnosti na správu mobilnej tlače. Využíva už existujúcu e-mailovú infraštruktúru, vďaka čomu môžu mobilní používatelia poslať tlačovú úlohu do tlačového frontu e-mailom a následne ju zadržať a vytlačiť v ktorejkoľvek tlačiarňi alebo multifunkčnom zariadení podporujúcom toto riešenie. Pomocou zabezpečených funkcií overenia, ako napríklad *Mobile Release*, môžete chrániť tlačové zariadenia v sieti.

Okamžité zabránenie možného úniku dát

Riešenia HP ponúkajú funkcie, ktoré vás pomôžu chrániť pred stratou dát. S nástrojom *HP Capture and Route Data Loss Prevention* môžete zabrániť skenovaniu a faxovaniu citlivých informácií. *HP Access Control Print Data Loss Prevention* umožňuje zabrániť tlači citlivých dokumentov. Sledujte svoje najdôležitejšie dáta, aby ste odrádzali od prienikov a predchádzali im bez spomalenia pracovných postupov. Získajte inteligentné výstrahy zabezpečenia podľa podmienok, ktoré si sami určíte.

Používanie digitálnych certifikátov v tlačiarňach

Zlepšite bezpečnosť svojho tlačového prostredia použitím digitálnych certifikátov na sieťové tlačiarne a multifunkčné zariadenia. Ušetríte čas použitím softvéru *HP JetAdvantage Security Manager*, ktorý sa stará o automatickú inštaláciu a obnovu certifikátov.⁹



Ochrana dokumentov

Integrujte inteligentné hardvérové a softvérové riešenia do širšieho plánu zabezpečenia IT na ochranu citlivých informácií v tlačených dokumentoch.⁶

Základné bezpečnostné opatrenia

Kontrola prístupu k predtlačeným formulárom

Vybavte tlačiarne a multifunkčné zariadenia uzamykatelnými vstupnými zásobníkmi, aby ste zabránili krádežiam špeciálneho papiera používaného na tlač šekov, predpisov alebo iných citlivých dokumentov.

Ochrana dokumentov PIN kódom alebo zadržiavaním tlačových úloh

Používatelia si môžu vybrať medzi použitím PIN kódu alebo zadržaním tlačovej úlohy. Vďaka tomu nebudú musieť v takej miere používať osobné tlačiarne a zároveň sa eliminuje nebezpečenstvo, že tlačové úlohy skončia v nesprávnych rukách. Takéto bezpečnostné opatrenia zároveň znižujú aj počet neprebraných výtlačkov, čím pomáhajú znížiť náklady a množstvo odpadu.

Pri tlači s PIN kódom používateľa pridávajú k dôvernému dokumentu PIN kód, s ktorým spustia jeho tlač až po príchode k tlačiarni.

Pri zadržiavaní tlačových úloh sa tlačové úlohy ukladajú v cloude alebo v počítači používateľa. Vybraná tlačiareň, pri ktorej si používateľ overí svoju totožnosť, si dané tlačové úlohy načíta a vytlačí. Spoločnosť HP ponúka dve cloudové tlačové riešenia na zadržiavanie tlačových úloh:*

- *Zabezpečená tlač HP JetAdvantage Secure Print* je dostupné riešenie navrhnuté pre protokol SMB, ktoré ukladá tlačové úlohy v cloude alebo v používateľovom počítači. Nastavenie a používanie je jednoduché, umožňuje tlač úloh z mobilných zariadení a podporuje zariadenia od viacerých dodávateľov.¹²
- *Súkromná tlač HP JetAdvantage Private Print* je bezplatné cloudové riešenie od spoločnosti HP ponúkajúce výhody zadržiavania tlačových úloh bez zložitostí. Nastavenie je jednoduché a nevyžaduje server, inštaláciu či údržbu.¹³

Pokročilé bezpečnostné opatrenia

Vyžadovanie zadržiavania tlačových úloh pri tlači každej úlohy

HP Access Control Secure Pull Printing pomáha chrániť dôverné informácie, zlepšiť zabezpečenie zariadenia a zvýšiť efektivitu. Toto robustné serverové riešenie ponúka viacero spôsobov overenia vrátane identifikačnej karty spolu so zabezpečením a funkciami správy úrovne enterprise.

Ochrana proti kopírovaniu alebo úprave pomocou rozpoznávania znakov magnetického atramentu (MICR), vodotlače alebo ďalších prvkov

Súčasťou riešení spoločností HP a TROY na odradenie od falšovania* je použitie bezpečnostného toneru, ktorý zanecháva flaky na papieri v prípade, že je s ním chemicky manipulované, pridanie rôznych vodoznakov s variabilnými údajmi na vytlačenej stránke a implementovanie rôznych strojovo rozpoznateľných kódov, ktoré sledujú a kontrolujú jednotlivé dokumenty. Multifunkčné zariadenia môžu obsahovať funkcie proti falšovaniu, medzi ktoré patria vlastné podpisy, logá spoločnosti a bezpečnostné fonty, ktoré využijete pri tlači citlivej dokumentácie, ako sú recepty, rodné listy alebo prepisy.



Ďalšie informácie

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

Riadenie prístupu HP
hp.com/go/hpac

Ochrana dokumentov od spoločností HP a TROY
hp.com/go/HPandTROY



Monitorovanie a správa pracovného prostredia



Ďalšie informácie

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Riešenia monitorovania zabezpečenia a správy vám pomôžu identifikovať slabé miesta zabezpečenia a vytvoriť jednotný prístup založený na pravidlách, aby ste chránili dáta, znížili riziká a naďalej zachovávali súlad.⁶ Zabráňte nedostatkom v zabezpečení a vyhnite sa drahým pokutám.

Základné bezpečnostné opatrenia

Aktualizácia zariadení najnovším firmvérom alebo operačným systémom

Na inštalovanie aktualizácií firmvéru na všetky tlačové zariadenia použite HP Web Jetadmin¹⁴. Zaisťujete tak, že zariadenia sú neustále aktualizované a používajú najnovšie funkcie ochrany zariadení a zabezpečenia.

Kontrola denníka udalostí zabezpečenia tlačiarne

Zariadenia HP posielajú udalosti alebo upozornenia na syslog server, takže pracovníci IT oddelenia môžu v prípade potreby opraviť problémy.

Posúdenie a oprava nastavení zariadenia

HP Print Manageability Integration Kit (MIK), doplnok riešenia Microsoft® System Center Configuration Manager (SCCM), umožňuje spravovať základné nastavenia tlačiarne v celej skupine tlačových zariadení. Microsoft SCCM je široko rozšírené riešenie správy na vzdialené plánovanie, nasadzovanie, nastavovanie a monitorovanie koncových zariadení. HP Print MIK dokáže odhaliť, posúdiť a opraviť 15 najčastejších nastavení zabezpečenia a podať správu o výsledkoch..

Ak potrebujete komplexné zabezpečenie vo všetkých svojich tlačových zariadeniach, vyberte si HP JetAdvantage Security Manager.⁹ Toto riešenie vám pomôže znížiť náklady a zdroje pri určovaní bezpečnostných pravidiel všetkých tlačových zariadení, automatizovaní opráv nastavení zariadení a inštalácii a obnove jedinečných certifikátov. Poskytuje aj zostavy potrebné na preukázanie zhody.



Ďalšie informácie

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Pokročilé bezpečnostné opatrenia

Zisťovanie a dokumentovanie hrozieb pomocou softvéru SIEM

Dáta o udalostiach zo zariadení HP FutureSmart je možné odosielať priamo do nástrojov na zisťovanie incidentov (napr. ArcSight, Splunk, a SIEMonster), a zabezpečiť tak monitorovanie v reálnom čase. Oddelenie zabezpečenia IT si môže jednoducho prezerat tlačové koncové zariadenia ako súčasť širšieho IT ekosystému, aby mohlo zisťovať a riešiť výstrahy zabezpečenia tlačiarne.

Automatická konfigurácia nových tlačových zariadení pri ich pridaní do siete

Funkcia Instant-on Security, ktorá je súčasťou riešenia HP JetAdvantage Security Manager, automaticky nastavuje nové zariadenia po ich pridaní do siete alebo po reštarte.

Správy pre audit súladu zabezpečenia tlačového portfólia

Pomocou riešenia HP JetAdvantage Security Manager môžete vytvárať správy o zhode, ktoré demonštrujú uplatňovanie bezpečnostných pravidiel pre tlačiarne a zabezpečenie dát zákazníkov.

Prípadný nesúlad môže poškodiť vaše podnikanie

Nechránené alebo nedostatočne chránené koncové zariadenia vytvárajú viac príležitostí na kybernetický útok. V rámci boja proti zväčšujúcej sa hrozbe začali úrady po celom svete presadzovať prísne bezpečnostné pravidlá, ktoré od organizácií vyžadujú lepšiu ochranu informácií o zákazníkoch.

Organizácie, ktoré ich nespĺňajú, môžu čeliť vysokým pokutám, zákazu

činnosti, poškodeniu mena a hromadným žalobám.

Je veľmi dôležité nasadiť zariadenia a riešenia, ako sú tlačiarne HP Enterprise a riešenie HP JetAdvantage Security Manager, ktoré pomáhajú naplňať požiadavky zabezpečenia a ochrany obchodných informácií pred bezpečnostnými hrozbami.



Získajte potrebnú pomoc

O ochranu a zabezpečenie sa nemusíte starať len vy sami. Tím konzultantov vám ukáže, ako môžete zlepšiť zabezpečenie dát, zariadení a dokumentov.

Spolupracujte s expertmi na zabezpečenie tlače, ktorí vám pomôžu odhaliť aktuálne riziká zabezpečenia tlače. Pomôžeme vám pri vytváraní komplexných bezpečnostných pravidiel založených na potrebách vašej firmy a overených postupoch a vytvoríme plán na zlepšenie zabezpečenia vášho jedinečného prostredia.

Líder v odvetví

Spoločnosť IDC vo svojej prvej správe IDC MarketScape hodnotiacej dodávateľov celosvetových riešení a služieb zabezpečenia tlačových riešení za rok 2017 označila HP za lídra v tejto oblasti. (Správu nájdete [tu](#).) Podľa správy „prístup spoločnosti HP Inc. k zabezpečeniu berie do úvahy celú infraštruktúru tlače a dokumentov, pričom tento prístup začína zamykaním zariadení a zahŕňa všetky aspekty používania zariadenia a ochrany obsahu.“ Zobrazený graf pochádza zo správy IDC hodnotiacej dodávateľov za rok 2017.¹⁵

Model analýzy dodávateľov IDC MarketScape je navrhnutý tak, aby poskytoval prehľad úrovne konkurencieschopnosti dodávateľov ICT na danom trhu. Metodológia výskumu využíva striktnú metodológiu hodnotenia založenú na kvalitatívnych aj kvantitatívnych kritériách, výsledkom ktorých je jedno grafické znázornenie pozície každého dodávateľa na danom trhu. Skóre funkcií meria produkt dodávateľa, uvedenie na trh a krátkodobý výkon podniku. Strategické skóre meria súlad stratégií dodávateľa s požiadavkami zákazníkov v časovom rámci 3 až 5 rokov. Trhový podiel dodávateľa je znázornený veľkosťou ikon.¹⁵

Začnite

Kontaktujte obchodného zástupcu, ktorý vám poskytne ďalšie informácie o bezpečnostných funkciách, riešeníach a službách spoločnosti HP, ktoré vám pomôžu získať väčšiu ochranu a zabezpečenie.

Ďalšie informácie

hp.com/go/printsecurity

¹ Tvrdenie o najbezpečnejšej tlači je založené na prieskume funkcií zabezpečenia v tlačiarniach HP danej triedy vykonanom spoločnosťou HP v roku 2017.

Spoločnosť HP ponúka spojenie bezpečnostných funkcií, ktoré pomocou monitorovania dokážu zistiť a automaticky zastaviť útok a overiť integritu softvéru počas automatického reštartovania. Zoznam produktov nájdete na stránke hp.com/go/LJCompatibility.

² InfoTrends, Designing Hardware & Solutions (Navrhovanie hardvéru a riešení), Brendan Morse, október 2016.

³ Quocirca, Managed Print Services Landscape (Prostredie spravovaných tlačových služieb), 2016, quocirca.com/content/managed-print-services-landscape-2016, júl 2016.

⁴ Prieskum spoločnosti Spiceworks, ktorý sa uskutočnil v novembri 2016 v mene spoločnosti HP medzi 309 vedúcimi pracovníkmi IT v Severnej Amerike, regiónoch EMEA a APAC.

⁵ Quocirca, Print security: An imperative in the IoT era (Zabezpečenie tlače: Imperatív v ére internetu vecí), quocirca.com/content/print-security-imperative-iot-era, január 2017.

⁶ Riešenia nemusia byť kompatibilné so všetkými zariadeniami HP. Riešenia si môžu vyžadovať dodatočný nákup.

⁷ Vyhlásenie o najpokročilejších integrovaných bezpečnostných funkciách od spoločnosti HP, ktoré sú dostupné v zariadeniach triedy HP Enterprise s firmvérom FutureSmart 4.5 alebo novším, je založené na prieskume spoločnosti HP týkajúcom sa integrovaných funkcií zabezpečenia tlačiarní HP danej triedy vykonaného v rokoch 2017. Spoločnosť HP ponúka kombináciu funkcií zabezpečenia na kontrolu integrity až po systém BIOS s možnosťami automatického odstraňovania chýb.

⁸ Vybrané zariadenia HP LaserJet Pro a PageWide Pro obsahujú integrované funkcie, ktoré dokážu odhaliť a zastaviť útok. Ďalšie informácie nájdete na stránke hp.com/go/LJCompatibility.

⁹ Softvér HP JetAdvantage Security Manager sa predáva samostatne. Ďalšie informácie nájdete na stránke hp.com/go/securitymanager.

¹⁰ Ďalší prístupový kľúč sa vyžaduje pri posielaní informácií do koncového zdroja chráneného prístupovým kľúčom.

¹¹ HP JetAdvantage Connect funguje v popredných mobilných zariadeniach. V zariadeniach s operačným systémom Android™, Google Chrome™ a Microsoft® je nutné nainštalovať jednorazový doplnok. Podrobnosti a zoznam podporovaných operačných systémov nájdete na stránke hp.com/go/JetAdvantageConnect.

¹² Zabezpečená tlač HP JetAdvantage Secure Print: Zadržiavanie tlačových úloh v tlačiarni funguje na všetkých tlačiarniach alebo multifunkčných zariadeniach pripojených do siete. Overovanie v zariadení je k dispozícii na mnohých modeloch HP LaserJet, PageWide a OfficeJet Pro a vybraných zariadeniach iných výrobcov. Niektoré zariadenia si môžu vyžadovať inováciu firmvéru. Na ukladanie tlačových úloh do cloudu a ich načítanie je potrebné internetové pripojenie. Na spustenie tlačovej úlohy z mobilného zariadenia sa vyžaduje sieťové pripojenie a QR kód. Ďalšie informácie spolu so zoznamom podporovaných tlačiarní a multifunkčných zariadení nájdete na stránke hp.com/go/JetAdvantageSecurePrint.

¹³ Funkcia HP JetAdvantage Private Print je k dispozícii zdarma a jej použitie si vyžaduje pripojenie tlačiarne s aktivovanými webovými službami na internet. Nie je k dispozícii vo všetkých krajinách. Ďalšie informácie nájdete na stránke hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin sa dá bezplatne stiahnuť na stránke hp.com/go/webjetadmin.

¹⁵ Založené na hodnotení dodávateľov tlačových riešení spoločnosťou IDC a jej názoru na vedúce postavenie spoločnosti HP: „Spoločnosť HP má výhodu vďaka svojim výkonným IT službám a funkciám... poskytuje komplexnú a integrovanú stratégiu v oblasti zabezpečenia v celej IT infraštruktúre.“ ZDROJ: [IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](http://www.idc.com/analysis/worldwide-security-solutions-and-services-hardcopy-2017-vendor-assessment), autori: Allison Correia a Robert Palmer, október 2017, číslo dokumentu IDC: US41988517.

*Dostupnosť tlačových riešení sa môže meniť podľa krajiny.

Registrácia na zasielanie noviniek

hp.com/go/getupdated



Zdieľať s kolegami

© Copyright 2014 – 2018 HP Development Company, L.P. Informácie uvedené v tomto dokumente sa môžu zmeniť bez predchádzajúceho upozornenia. Jedinými zárukami, ktoré sa vzťahujú na produkty a služby spoločnosti HP, sú záruky výslovne uvedené v záručných podmienkach priložených k jednotlivým produktom a službám. Žiadne informácie uvedené v tomto dokumente nemožno považovať za dodatočnú záruku. Spoločnosť HP nenesie žiadnu zodpovednosť za technické alebo redakčné chyby či vynechané informácie v tomto dokumente.

Android a Google Chrome sú registrované ochranné známky spoločnosti Google Inc. Microsoft je registrovaná ochranná známka skupiny spoločností Microsoft registrovaná v USA.

4AA3-1295SKE, január 2018, rev. 11

