

Brožura

Chraňte své tiskárny jednoduchým zabezpečením tisku podle firemních zásad

Rozvíjejte své podnikání bezpečným způsobem – s řešením HP JetAdvantage Security Manager



9,5 mil. USD

Průměrné náklady při úniku dat¹



Vaše firma řeší otázky zabezpečení každý den



Zabezpečte všechny své tiskárny řešením, které laboratoř Buyers Laboratory (BLI) označila za průkopnické.²

HP JetAdvantage Security Manager je nejkomplexnější řešení pro zabezpečení tisku na trhu, nabízející účinný, na firemních zásadách založený, přístup k zabezpečení tiskových a zobrazovacích zařízeních HP.³

Vaše společnost neustále vytváří důvěrná, hodnotná data, jež jsou pro vaše podnikání klíčová. A vy pravděpodobně používáte různé metody zabezpečení – včetně ověřování, šifrování a monitorování – abyste tato data ve svých počítačích, sítích a na serverech ochránili. Je však vaše tiskové a zobrazovací prostředí stejně tak zabezpečené jako zbytek vaší infrastruktury?

Nedostatečné zabezpečení může vést k vysokým nákladům, ať už v důsledku zanechání dokumentů bez dozoru v tiskárně, přenosu citlivých informací při jejich zpracování z počítače do zařízení nebo uchovávání důvěrných informací na pevných discích zařízení. K zajištění ochrany vašeho podnikání potřebujete řešení, které zjednoduší a posílí zabezpečení celého vašeho tiskového a zobrazovacího prostředí, a ušetří vám pracovní čas a peníze, jež můžete lépe využít někde jinde.



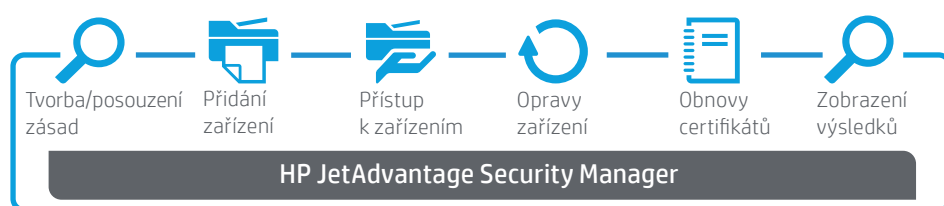
První ve správě zabezpečení z celého odvětví

Společnost HP vám chce pomáhat s překonáváním bezpečnostních hrozeb, a vyvinula proto HP JetAdvantage Security Manager – efektivní přístup k zabezpečení tiskových a zobrazovacích zařízení HP, založený na zásadách. S řešením HP Security Manager zlepšíte zabezpečení všech svých tiskových a zobrazovacích zařízení HP a předejdete stresu ze zneužití dat – pomůžete tak chránit svá zařízení a informace důležité pro chod vaší společnosti.

HP Security Manager nabízí jednoduchý, intuitivní proces zabezpečení všech tiskáren. Zabezpečení HP Instant-on Security vám umožní účinně nasadit jednotné zásady zabezpečení pro všechny tiskárny a monitorovat je, a okamžitě zabezpečit nově přidaná zařízení HP do vaší sítě.⁴ Pomocí funkcí automatického monitorování a generování sestav o rizicích, jež jsou součástí řešení HP Security Manager, můžete aktivně spravovat a ověřovat dodržování vámi stanovených zásad zabezpečení. Spolehněte se na automatické nasazení a aktualizace identifikačních certifikátů, které posilují bezpečnost informací a současně výrazně snižují administrativní náklady.

Jak řešení HP Security Manager chrání všechny vaše tiskárny

HP Security Manager nabízí zjednodušený přístup k zabezpečení všech zařízení HP, takže posiluje soulad se zásadami a snižuje riziko.



Sestavte zabezpečení všech tiskáren pomocí jednoduchého nástroje pro tvorbu zásad

Zásady vytvoříte snadno v jednoduchém editoru HP Policy Editor s intuitivním nástrojem pravidel, jenž vás povede jednotlivými kroky a pomůže vám vytvořit komplexní zásady pro vaše prostředí. Své zásady zabezpečení můžete snadno upravovat, aby co nejlépe vyhovovaly měnícím se potřebám vaší společnosti, nařízením nebo průmyslovým normám.

Šablona základních zásad HP Security Manager

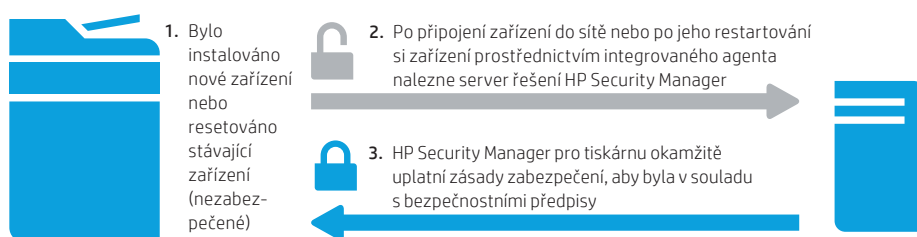
Vytvořte snadno zásady zabezpečení pro své tiskové prostředí pomocí šablony HP Security Manager Base Policy. Šablona poskytuje základní přístup k zabezpečení tiskového prostředí běžného podniku, kterou však lze snadno přizpůsobit tak, aby odpovídala individuálním požadavkům firemních zásad zabezpečení. Tato šablona spojuje nastavení Národního institutu standardů a technologie USA a kontrolní seznam osvědčených postupů zabezpečení společnosti HP s vlastními preferencemi bezpečnostního nastavení zákazníka, tak aby vzniklo bezpečné a zároveň produktivní tiskové prostředí.⁵



Uplatňujte vlastní zásady zabezpečení pro svá zařízení různými způsoby

Přidání zařízení HP do HP Security Manager je jednoduché.

- **Automatické zjištění:** Nechte řešení Security Manager, aby našlo vaše zařízení HP pomocí automatického zjištění. Nastavte jej, aby hledalo v rámci určitého počtu úseků sítě nebo rozsahu IP adres. Potom si ze seznamu vyberte zařízení, která chcete spravovat.
- **.txt nebo .xml soubor:** Stávající seznam zařízení můžete přidat importováním ze souboru .txt nebo .xml s IP adresami nebo názvy zařízení, včetně exportovaných souborů .xml z nástroje HP Web Jetadmin.⁶
- **Instant-On Security:** Pomocí funkce HP Instant-on Security můžete automaticky přidat každé zařízení HP do nástroje Security Manager, jakmile je připojíte k síti (nebo po resetování) bez zásahu oddělení IT. Funkce HP Instant-on Security jakožto součást HP Security Manager rovněž jedinečným způsobem okamžitě konfiguruje zařízení, aby byla v souladu s vašimi specifickými firemními zásadami zabezpečení – a šetří tak váš čas a minimalizuje riziko.⁴



HP Instant-on Security

Maximalizujte svou investici proaktivním dodržováním předpisů

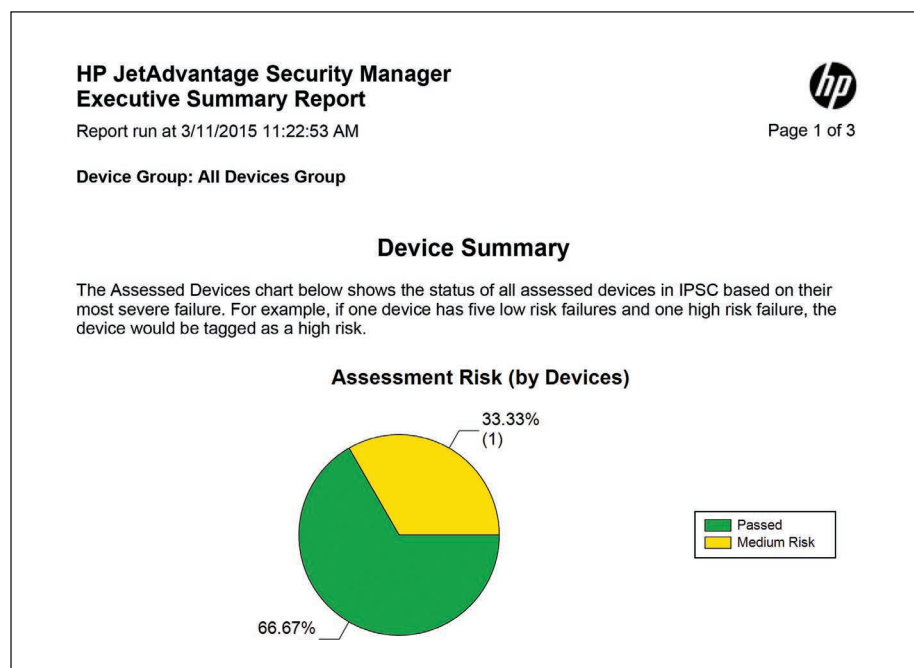
HP Security Manager hlídá dodržování předpisů na základě průběžných kontrol a automatické obnovy. Můžete se sami rozhodnout, jak často chcete vyhodnotit, nebo vyhodnotit a upravit, bezpečnostní nastavení zařízení. Denně, týdně nebo měsíčně – je to na vás.

- **Kontrola:** Během plánované kontroly běží HP Security Manager na pozadí a ověřuje nastavení zabezpečení všech vašich tiskáren vůči specifickým zásadám zabezpečení. Kontrolní proces rozpoznává a oznamuje jakékoli funkce, které nejsou v souladu se zásadami.
- **Oprava:** HP Security Manager automaticky uplatní správné zásady zabezpečení pro jakékoli funkce porušující pravidla, jež byly během kontroly zjištěny. Opravené nastavení se znovu ověřuje, aby se potvrdilo, že zásady byly úspěšně zavedeny.

Omezte riziko s využitím komplexních sestav o zabezpečení všech tiskáren

Chraňte své informace integrovanou funkcí generování sestav. Uživatelé mají k dispozici jak souhrnné sestavy o celkové míře rizika všech tiskáren, tak sestavy o konkrétních rizicích podle zařízení nebo nastavení zabezpečení. Lze rovněž povolit vysokou četnost sestav zasílaných e-mailem, které se pak odesílají po každé automaticky naplánované kontrole a opravě.

HP Security Manager dokáže také posoudit riziko, a pomoci tak identifikovat zařízení s nižší úrovní zabezpečení. Méně zabezpečená zařízení nemusí mít nainstalovaný nejnovější firmware zařízení, firmware Jetdirect, nebo nemusí mít povolené funkce Sure Start, detekce narušení runtime nebo seznam povolených firmwarů.



Jednoduché, intuitivní posouzení rizik



Společná správa certifikátů pro všechna zařízení vám usnadní pracovní postupy

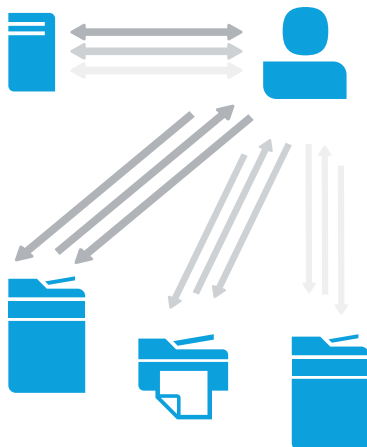
Certifikáty jsou zásadní pro ochranu toku informací z a do vašich zařízení. Používají se k prokázání identity a šifrování dat a zajišťují bezpečnou komunikaci mezi důvěryhodnými subjekty. Manuální instalace jedinečných certifikátů může být náchylná k chybám, pracná a časově náročná – až 15 minut na jedno zařízení. Kvůli tomu se mnoho zákazníků rozhodne certifikáty raději vůbec nepoužívat nebo je nedostatečně spravuje.

Nejnovější inovace řešení HP Security Manager tento proces zjednodušuje nasazením certifikátů s jedinečnou identitou napříč všemi tiskárnami a jejich průběžným monitorováním, kterým ověřuje jejich platnost s tím, že zrušené nebo prošlé certifikáty automaticky nahrazuje.²

HP Security Manager efektivním způsobem zavádí a aktualizuje certifikáty ID a CA – a zvyšuje tak zabezpečení vaší infrastruktury, aplikací a komunikací mezi zařízeními.

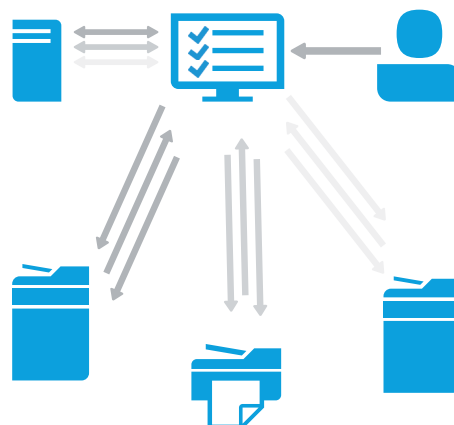
Dříve

Ruční, časově náročný proces náchylný k chybám, který se musel provádět samostatně pro každé zařízení



Nyní

Jednoduché, účinné a jednorázové nastavení pro všechny tiskárny pomocí řešení HP Security Manager





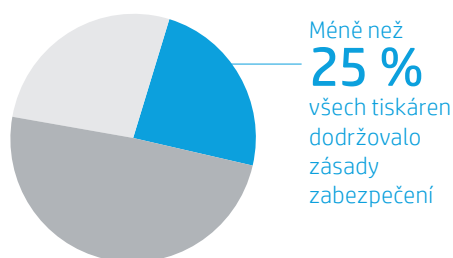
Jaké vám může toto snadno použitelné řešení přinášet výhody?

HP Security Manager je všestranné řešení zabezpečení, které lze použít pro různé účely a obchodní situace.

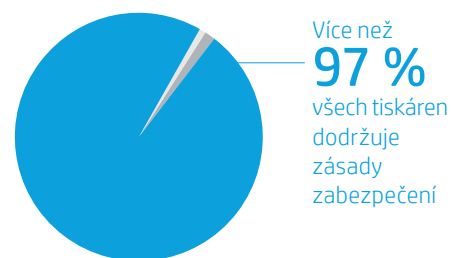
Například firmy poskytující finanční služby vědí, že ochrana informací o klientech je zásadní pro jejich úspěšné podnikání a je vyžadována nařízeními v odvětví. Pokud však tisková zařízení v celé firmě dosahují tisíců kusů, je správa jejich zabezpečení spojena se značnými správními náklady.

S řešením HP Security Manager ušetří firmy poskytující finanční služby čas a peníze díky plánovaným každodenním kontrolám a opravám jejich tiskových a zobrazovacích zařízení HP. Jejich prostřednictvím zajistíte, že všechny tiskárny budou v souladu s firemními zásadami zabezpečení a svému IT týmu poskytnete prostor pro jiné činnosti. Integrované sestavy o všech tiskárnách, jednotlivých zařízeních nebo podle funkcí si správci mohou rovněž vytisknout nebo uložit, a podle nich snadno ověřovat, zda jsou informace o klientech dostatečně zabezpečené.

Před nasazením řešení HP Security Manager



Po nasazení řešení HP Security Manager





Technické specifikace

Podporované síťové operační systémy	HP Security Manager je podporován na 32bitových i 64bitových operačních systémech: Microsoft® Windows® 7 SP1, 8, 8.1, 10; Microsoft Server® 2008 R2 (pouze 64bitová verze), 2012, 2012 R2, 2016
Podporované databáze	Microsoft SQL Server Express 2012, Microsoft SQL Server 2012 (Enterprise), Microsoft SQL Server Express 2014 (v balíčku), Microsoft SQL Server 2014 (Enterprise)
Testované prohlížeče	Internet Explorer 11 a Google Chrome™ v55.0 a vyšší
Verze rozhraní .NET	Vyžaduje rozhraní .NET 3.5 a 4.6.2
Podporovaná zařízení	Kompatibilitu zařízení zjistíte na hp.com/go/securitymanager
Systémové požadavky	Požadavky na server: Minimálně 2,33GHz dvoujádrový procesor, minimálně 4 GB RAM (pro 32bitové systémy), minimálně 8 GB RAM (pro 64bitové systémy) Požadavky na klienta: PC s minimálně 1,8GHz procesorem, minimálně 3 GB RAM (pro 32bitové systémy), minimálně 4 GB RAM (pro 64bitové systémy) Požadavky na úložiště: Minimálně 4 GB dostupného prostoru na disku. Požadovaná velikost úložiště databáze se u řešení HP Security Manager liší v závislosti na: počtu kontrolovaných zařízení, rozsahu zásad uplatňovaných při kontrolách, počtu zásad používaných ke kontrolám, četnosti kontrol a na doporučeních vyplývajících z kontrol. Důrazně se doporučuje, aby se pro správu více než 1 000 zařízení použila plná instance SQL.
Výkon	Společnost HP testovala až 10 000 zařízení na serveru (možný je i vyšší počet) s tím, že za použití základní šablony zásad HP Security Manager Base Policy dosáhla 1 500 zkontrolovaných zařízení za hodinu.
Podporované jazyky	Angličtina

Více informací

Více informací o tom, jak učinit z řešení HP JetAdvantage Security Manager nedílnou součást celkové firemní strategie zabezpečení IT, nebo jak získat bezplatnou zkušební verzi, zjistíte na hp.com/go/securitymanager, nebo získáte od zástupce HP či odborníka HP na řešení pro dokumenty.

Více se dozvíte na
hp.com/go/securitymanager

¹ Studie společnosti Ponemon „2016 Cost of Cyber Crime Study & the Risk of Business Innovation“ z roku 2016, podpořená společností HPE.

² Zdroj: Zpráva Solutions Report o řešení HP JetAdvantage Security Manager 2.1 od společnosti Buyers Laboratory LLC z února 2015.

³ Na základě zprávy o zabezpečení interních dat, zveřejněné společností HP (Srovnání zabezpečení zařízení, leden 2015), a zprávy o řešeních HP JetAdvantage Security Manager 2.1 zveřejněné laboratoří Buyers Laboratory LLC, únor 2015.

⁴ Dostupné u vybraných modelů a firmwarových verzí.

⁵ Tento nástroj slouží pouze pro obecné srovnání. Tyto informace vycházejí z údajů zveřejněných výrobcí a interních specifikací a údajů a algoritmů, které jsou předmětem vlastnictví. Přesnost informací není společností Hewlett-Packard Company zaručena. Zásady zabezpečení použité pro analýzu si mohou uživatelé přizpůsobit, což může ovlivnit výsledky. Skutečné výsledky se mohou lišit.

⁶ Aplikace HP Web Jetadmin je zdarma ke stažení na stránce hp.com/go/webjetadmin.

Objednejte si aktualizace na
hp.com/go/getupdated



Sdílet dokument s kolegy

