

Bescherm al uw printers eenvoudig met beveiliging op basis van beleid

Laat uw bedrijf veilig groeien – met HP JetAdvantage Security Manager



€8,7M

De gemiddelde schade na één dataschending¹



Uw bedrijf heeft dagelijks te maken met beveiligingsproblemen



Beveilig uw printerpark met de oplossing die door Buyers Laboratory (BLI) wordt omschreven als 'trailblazing' (baanbrekend).² HP JetAdvantage Security Manager is de meest complete oplossing voor beveiligd printen, die het mogelijk maakt om HP printers en scanners te beveiligen op basis van policy's (beleid).³

Op uw kantoor worden voortdurend waardevolle, vertrouwelijke gegevens gecreëerd die essentieel zijn voor uw bedrijf. En waarschijnlijk maakt u gebruik van meerdere beveiligingsmethoden zoals authenticatie, versleuteling en monitoring om deze gegevens veilig te houden op uw pc's en servers en in het netwerk. Maar zijn uw printers en scanners net zo veilig als de rest van uw infrastructuur?

Beveiligingsrisico's en de bijkomende kosten kunnen hoog zijn, of ze nu veroorzaakt worden door documenten die onbeheerd worden achtergelaten bij een printer, vertrouwelijke gegevens die van de computer naar de printer worden gestuurd of vertrouwelijke gegevens op een harde schijf. Om uw bedrijf te beschermen heeft u een oplossing nodig die de beveiliging van al uw printers en scanners vereenvoudigt en verbetert. Zo bespaart u tijd en geld, en beide komen altijd goed van pas.



De eerste in zijn soort op het gebied van beveiliging

HP heeft HP JetAdvantage Security Manager ontwikkeld, een gestroomlijnde oplossing die op basis van beleid uw HP printing- en imagingapparaten beschermt en helpt uw beveiligingsproblemen op te lossen. Met HP Security Manager kunt u de beveiliging van uw HP printers en scanners verbeteren voordat u tegen de problemen van een beveiligingslek aanloopt. Zo kunt u de apparaten en gegevens van uw bedrijf beter beschermen.

HP Security Manager biedt een eenvoudig, intuïtief proces om uw printerpark te beveiligen. U kunt apparaten efficiënt inzetten en monitoren door één beveiligingsbeleid toe te passen op alle apparaten. Nieuwe HP apparaten kunt u met HP Instant-on Security beveiligen zodra ze aan uw netwerk worden toegevoegd.⁴ U kunt de compliance met uw beveiligingsbeleid actief onderhouden en controleren met behulp van de geautomatiseerde monitoring- en risicorapportages van HP Security Manager. Vertrouw op het automatisch activeren en updaten van identiteitscertificaten die gegevens nog beter beveiligen en de administratieve overhead aanzienlijk reduceren.

Hoe HP Security Manager uw printerpark beveiligt

HP Security Manager biedt een eenvoudige methode om al uw HP apparaten te beveiligen die uw compliance versterkt en risico's verkleint.



Beveilig al uw apparaten door eenvoudig beleid te definiëren

Met de gebruiksvriendelijke HP Policy Editor kunt u eenvoudiger beleid creëren met behulp van een intuïtieve regel-engine die richtlijnen biedt en u helpt een uitgebreid beleid te definiëren voor uw omgeving. Pas uw beveiligingsbeleid aan zodat het beter aansluit op de behoeften van uw bedrijf en de regels en standaards binnen uw branche.

HP Security Manager Base Policy-sjabloon

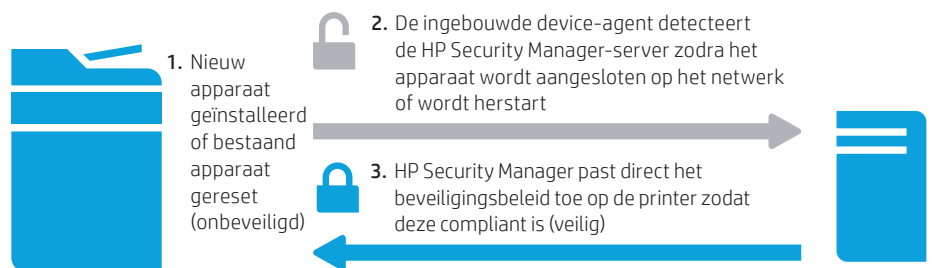
Creëer eenvoudig een beveiligingsbeleid voor uw printomgeving met behulp van het HP Security Manager Base Policy-sjabloon. Het sjabloon biedt een uitgangsbeleid voor het beveiligen van een gemiddelde enterprise-printomgeving, maar kan eenvoudig worden aangepast aan individuele beveiligingseisen. Het sjabloon combineert instellingen van het Amerikaanse National Institute of Standards and Technology en HP Security Best Practices Checklist met door de klant voorgestelde beveiligingsinstellingen en creëert zo een veilige, productieve printomgeving.⁵



Voeg apparaten op verschillende manieren aan uw beleid toe

U kunt eenvoudig HP apparaten toevoegen aan HP Security Manager.

- **Automatische detectie:** Security Manager vindt uw HP apparaten vanzelf. U geeft gewoon aan hoe ver of waar in het netwerk moet worden gezocht (op basis van aantal hops of IP-adres). Daarna kiest u in de lijst de apparaten die u wilt beheren.
- **Txt- of xml-bestand:** U kunt een bestaande lijst met apparaten toevoegen door een .txt- of .xml-bestand met de IP-adressen of hostnamen van apparaten te importeren, inclusief .xml-exports van HP Web Jetadmin.⁶
- **Instant-On Security:** Gebruik de functie HP Instant-on Security om elk HP apparaat geheel automatisch toe te voegen aan Security Manager zodra het wordt aangesloten op uw netwerk (of na een reset). HP Instant-on Security is een unieke functie van HP Security Manager, die bovendien apparaten direct zodanig configureert dat ze compliant zijn met het specifieke beveiligingsbeleid van uw bedrijf. Zo bespaart u tijd en vermindert u risico's.⁴



HP Instant-on Security

Maximaliseer uw investeringen met proactieve compliance

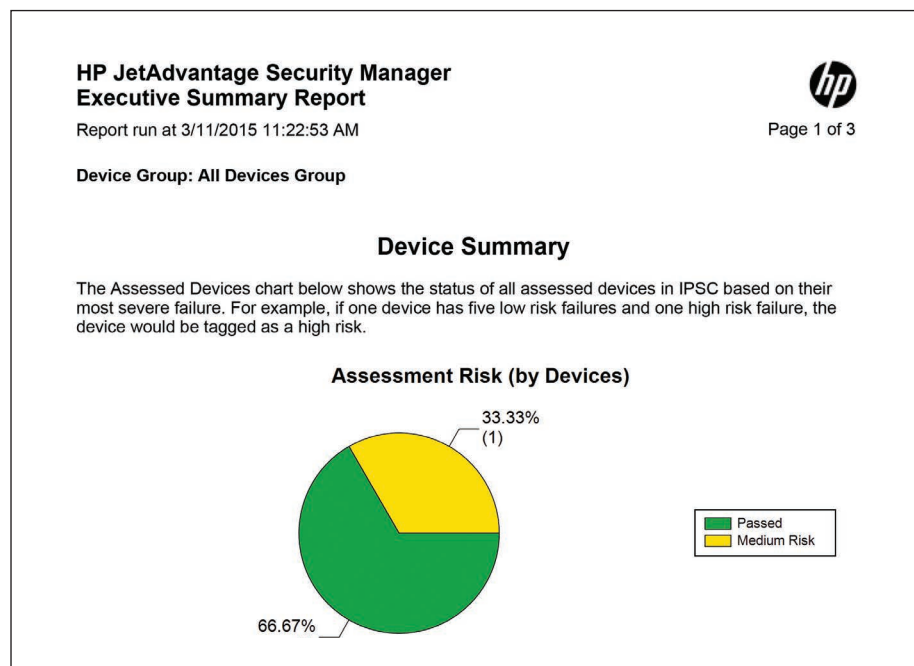
HP Security Manager houdt compliance in stand met behulp van voortdurende analyses en geautomatiseerd herstel. U bepaalt hoe vaak u uw apparaten wilt evalueren of evalueren en herstellen. Dagelijks, wekelijks of maandelijks – de keuze is aan u.

- **Analyse:** Tijdens de geplande analyse draait HP Security Manager op de achtergrond en controleert de beveiligingsinstellingen van al uw apparaten en vergelijkt ze met een bepaald beleid. Het analyseproces identificeert en rapporteert functies die niet compliant zijn.
- **Herstel:** HP Security Manager past automatisch de juiste beleidsinstellingen toe op functies die volgens de analyse niet compliant zijn. De compliant instelling wordt opnieuw geanalyseerd om te controleren of deze juist is toegepast.

Verlaag risico's met uitgebreide rapportages over al uw apparaten

Bescherm uw informatie met ingebouwde rapportage. Gebruikers kunnen overzichtsrapporten genereren over het globale risiconiveau van het printerpark en meer gedetailleerd ingaan op specifieke risico's per apparaat of per beveiligingsinstelling. Het is ook mogelijk om na elke automatisch geplande evaluatie en correctie een globaal rapport te laten versturen per e-mail.

HP Security Manager kan bovendien een risico-assessment uitvoeren om onveilige apparaten te identificeren. Zulke minder veilige apparaten hebben bijvoorbeeld niet de meest recente firmware of Jetdirect-firmware, of ze bieden geen ondersteuning voor Sure Start, runtime inbraakdetectie of whitelisting.



Eenvoudige, intuïtieve risicoanalyse



Bescherm uw workflow met certificatenbeheer voor uw hele apparatuurpark

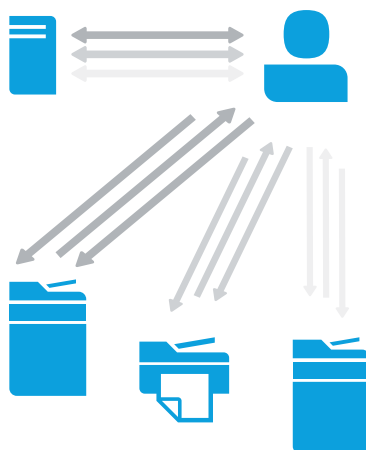
Certificaten zijn essentieel om de informatiestroom van en naar uw apparaten te beschermen. Ze worden gebruikt om de identiteit te controleren en gegevens te versleutelen, waardoor beveiligde communicatie tussen betrouwbare apparaten mogelijk is. Het handmatig installeren van unieke certificaten kan foutgevoelig, bewerkelijk en tijdrovend zijn – tot 15 minuten per apparaat. Met als gevolg dat veel klanten helemaal geen certificaten gebruiken of ze niet juist onderhouden.

De nieuwste innovatieve functie van HP Security Manager stroomlijnt dit proces door unieke identiteitscertificaten toe te kennen aan al uw apparaten en deze voortdurend te monitoren om er zeker van te zijn dat ze nog steeds geldig zijn. Ingetrokken of verlopen certificaten worden automatisch vervangen.²

HP Security Manager implementeert en vernieuwt zowel ID- als CA-certificaten op efficiënte wijze en maakt zo uw infrastructuur, applicaties en de communicatie tussen uw apparaten veiliger.

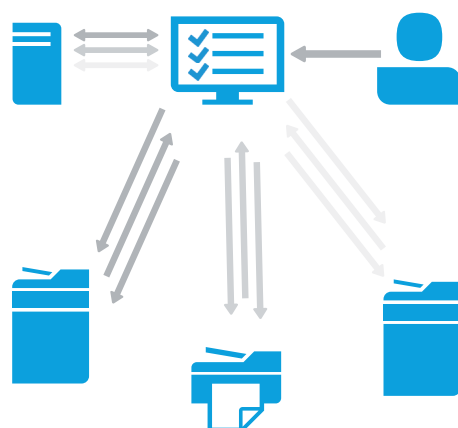
Vóór

Handmatig, tijdrovend en foutgevoelig proces moet op elk apparaat worden uitgevoerd



Na

Eenvoudige, efficiënte, eenmalige installatie voor alle apparaten met HP Security Manager





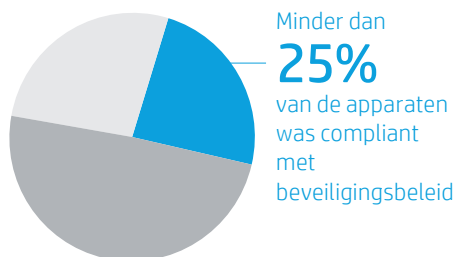
Welke voordelen heeft deze gebruiksvriendelijke oplossing voor u?

HP Security Manager is een veelzijdige beveiligingsoplossing die in veel verschillende bedrijfsomgevingen kan worden gebruikt.

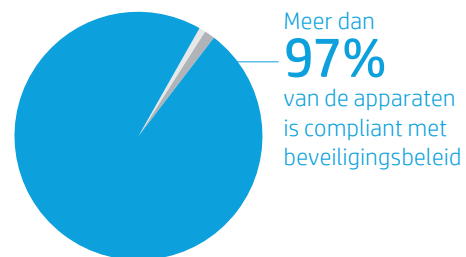
Financiële bedrijven weten bijvoorbeeld dat het beschermen van hun klantgegevens cruciaal is voor het succes van hun bedrijf en dat dit verplicht is volgens de regels in de financiële sector. Maar het onderhouden van de beveiliging van soms duizenden printers kost veel administratieve overhead.

Met HP Security Manager kunnen financiële bedrijven tijd en geld besparen door dagelijkse analyse- en herstelprocessen te plannen voor hun HP printers en scanners. Op deze manier blijven alle apparaten compliant met het beveiligingsbeleid van het bedrijf, terwijl het IT-team tijd overhoudt om zich op andere activiteiten te concentreren. Beheerders kunnen bovendien ingebouwde rapportages over alle apparaten, over individuele apparaten of over functies printen of opslaan als bewijs van compliance. Zo kan eenvoudig worden gecontroleerd of klantgegevens veilig zijn.

Vóór HP Security Manager



Na HP Security Manager





Technische specificaties

Ondersteunde netwerkbesturingssystemen	HP Security Manager wordt ondersteund op 32-bits en 64-bits besturingssystemen: Microsoft® Windows® 7 SP1, 8, 8.1, 10; Microsoft Server® 2008 R2 (alleen 64-bits), 2012, 2012 R2, 2016
Ondersteunde databases	Microsoft SQL Server Express 2012, Microsoft SQL Server 2012 (Enterprise), Microsoft SQL Server Express 2014 (gebundeld), Microsoft SQL Server 2014 (Enterprise)
Geteste browsers	Internet Explorer 11 en hoger, Google Chrome™ v55.0 en hoger
.NET-versies	.NET 3.5 en 4.6.2 zijn vereist
Ondersteunde apparaten	Ga voor compatibele apparaten naar hp.com/go/securitymanager
Systeemvereisten	Server: 2,33 GHz Dual-Core-processor of sneller, 4 GB RAM of meer (32-bits systemen), 8 GB RAM of meer (64-bits systemen) Client: pc met 1,8 GHz-processor of sneller, 3 GB RAM of meer (32-bits systemen), 4 GB RAM of meer (64-bits systemen) Opslag: 4 GB vrije schijfruimte of meer. De hoeveelheid vereiste databasruimte varieert voor HP Security Manager en is gebaseerd op: het aantal geanalyseerde apparaten, de omvang van het beleid op basis waarvan de analyse plaatsvindt, het aantal beleidsprocedures dat moet worden gebruikt, de frequentie van de analyses en de aanbevelingen die voortvloeien uit de analyses. Bij meer dan 1000 apparaten wordt sterk aanbevolen om een volledige versie van SQL te gebruiken.
Prestaties	HP heeft tot 10.000 apparaten getest op een server (hogere aantallen zijn waarschijnlijk mogelijk) en heeft 1500 apparaatanalyses per uur uitgevoerd op basis van de HP Security Manager Base Policy.
Ondersteunde talen	Engels

Meer informatie

Wilt u meer weten over hoe u HP JetAdvantage Security Manager kunt integreren in de IT-beveiligingsstrategie van uw bedrijf? Of wilt u een gratis proefprogramma? Ga naar hp.com/go/securitymanager of neem contact op met uw HP vertegenwoordiger of een HP Document Solutions Specialist.

Ga voor meer informatie naar
hp.com/go/securitymanager

¹ Onderzoek van Ponemon, gesponsord door HPE, naar de kosten van cybercriminaliteit en de risico's van bedrijfsinnovatie uit 2016, oktober 2016.

² Bron: Rapport over HP JetAdvantage Security Manager 2.1 door Buyers Laboratory LLC, februari 2015.

³ Gebaseerd op interne gegevens van HP (Device Security Comparison, januari 2015) en een Solutions Report over HP JetAdvantage Security Manager 2.1 van Buyers Laboratory LLC, februari 2015.

⁴ Beschikbaar op specifieke productmodellen en firmwareversies.

⁵ Deze tool dient alleen voor een algemene vergelijking. Deze informatie is gebaseerd op de gepubliceerde en interne specificaties van de fabrikant en propriëtaire gegevens en algoritmes. De correctheid van deze informatie kan niet worden gegarandeerd door Hewlett-Packard Company. Gebruikers kunnen het beveiligingsbeleid dat wordt gebruikt voor de analyse wijzigen en dit is van invloed op de resultaten. De daadwerkelijke resultaten kunnen variëren.

⁶ HP Web Jetadmin kan gratis worden gedownload van hp.com/go/webjetadmin.

Meld u aan voor updates op
hp.com/go/getupdated



Delen met collega's

© Copyright 2012-2017 HP Development Company, L.P. De informatie in dit document kan zonder voorafgaande kennisgeving worden gewijzigd. De van toepassing zijnde garanties voor HP producten en diensten zijn vastgelegd in de uitdrukkelijke garantiebepalingen die bij dergelijke producten en diensten op fysieke en/of elektronische wijze worden meegeleverd of gepubliceerd op website(s) van HP. Niets in dit document mag als een aanvullende garantie worden opgevat. HP is niet aansprakelijk voor technische en/of redactionele fouten c.q. weglatingen in dit document.

Google Chrome is een handelsmerk van Google Inc. Microsoft, Windows, Windows Server en SQL Server zijn in de V.S. geregistreerde handelsmerken van de Microsoft-groep.

4AA3-9275NLE, Juni 2017, Rev. 9

