



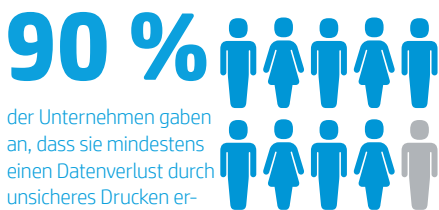
Schützen Sie Ihre Flotte durch einfache, richtlinienbasierte Drucksicherheit

Sicheres Unternehmenswachstum – mit HP JetAdvantage Security Manager



Schützen Sie Ihre Geräteflotte mit der Lösung, die Buyers Laboratory (BLI) als „wegweisend“ bezeichnet.¹ HP JetAdvantage Security Manager ist eine der umfassendsten Sicherheitslösungen für Druckumgebungen auf dem Markt, die auf einem effektiven, richtlinienbasierten Konzept für den Schutz von HP Geräten für Bildverarbeitung und Druck aufbaut.

Fast



Quelle: „Managed Print Services Landscape, 2014“, Quocirca, Juni 2014.

Tägliche Sicherheitsherausforderungen für Ihr Unternehmen

In Ihrem Unternehmen werden ständig vertrauliche, wertvolle Daten erstellt, die für Ihre Geschäftstätigkeit entscheidend sind. Und Sie setzen wahrscheinlich mehrere Sicherheitsverfahren (darunter Authentifizierung, Verschlüsselung und Überwachung) ein, um diese Daten auf Ihren PCs, Netzwerken und Servern zu schützen. Aber ist Ihre Umgebung für Bildverarbeitung und Druck genauso sicher wie der Rest Ihrer Infrastruktur? Die Sicherheitsrisiken und zugehörigen Kosten können sehr hoch sein, unabhängig davon, ob das Risiko durch ungeschützte Dokumente an einem Drucker, durch die Übertragung vertraulicher Daten vom Computer an das Gerät oder durch vertrauliche Informationen auf den Festplatten der Geräte entsteht. Für den kontinuierlichen Schutz Ihres Unternehmens benötigen Sie eine Lösung, die die Sicherheit in Ihrer gesamten Umgebung für Bildverarbeitung und Druck vereinfacht und verbessert. So spart Ihr Unternehmen Zeit und Geld – Ressourcen, die Sie für andere Zwecke einsetzen können.

Branchenweit führend beim Sicherheitsmanagement

Aus diesem Grund wurde HP JetAdvantage Security Manager von HP entwickelt, ein optimierter, richtlinienbasierter Ansatz für den Schutz von HP Geräten für Bildverarbeitung und Druck. Mit HP Security Manager können Sie Ihre HP Flotte für Bildverarbeitung und Druck umfassend schützen und so bereits im Vorfeld unnötige Stresssituationen durch Datenschutzverletzungen vermeiden. Sie schützen dadurch nicht nur Ihre Geräte, sondern auch die darauf befindlichen Informationen, die für den Betrieb Ihres Unternehmen besonders wichtig sind.

HP Security Manager bietet einen einfachen, intuitiven Prozess für den Schutz Ihrer Flotte. Durch Anwendung einer einzigen Sicherheitsrichtlinie für die gesamte Flotte können Sie Geräte effizient implementieren und überwachen. Mit HP Instant-on Security sind neue HP Geräte sofort geschützt, wenn sie dem Netzwerk hinzugefügt werden.² Dank der automatisierten Überwachung und den risikobasierten Berichten von HP Security Manager können Sie die Compliance aktiv verbessern und überprüfen. Durch die automatische Implementierung und Aktualisierung von Identitätszertifikaten erhöht sich die Datensicherheit, während der Verwaltungsaufwand deutlich sinkt.

Wie HP Security Manager Ihre Flotte schützt

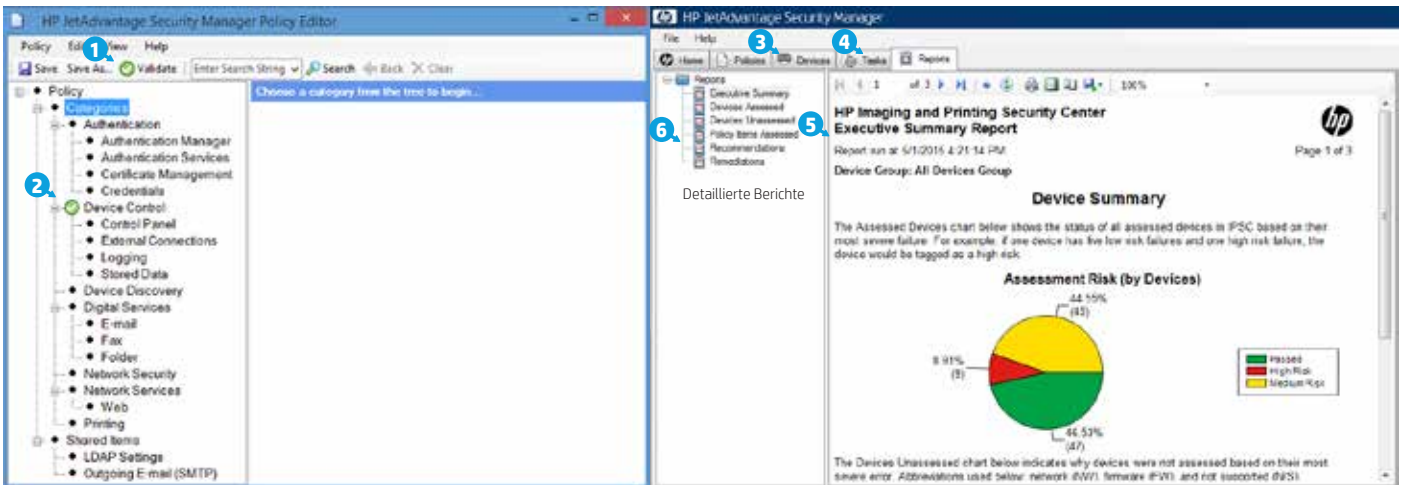
HP Security Manager bietet einen holistischen Ansatz für die HP Flottensicherheit, der die Compliance verbessert und Risiken reduziert.



Flottensicherheit durch mühelose Richtlinienerstellung

Der benutzerfreundliche HP Policy Editor vereinfacht die Erstellung von Richtlinien durch eine intuitive Regel-Engine, die Anleitungen bereitstellt und Sie beim Erstellen einer umfassenden Richtlinie für Ihre Umgebung unterstützt. Zudem können Sie Ihre Sicherheitsrichtlinien problemlos an neue Unternehmensanforderungen, Vorschriften oder Branchenstandards anpassen.

- **HP Security Manager Base Policy** – Erstellen Sie mithilfe der HP Security Manager Base Policy auf einfache Weise eine Sicherheitsrichtlinie für Ihre Druckumgebung. Diese Vorlage stellt einen grundlegenden Ansatz für den Schutz einer typischen Druckumgebung in Unternehmen zur Verfügung; sie lässt sich jedoch auch leicht anpassen, wenn Sie individuelle Anforderungen an Sicherheitsrichtlinien haben. Die Vorlage kombiniert Einstellungen aus der HP Security Best Practices-Checkliste, die vom National Institute of Standards and Technology in den USA überprüft wurden, mit dem Feedback von Kunden zu den Sicherheitseinstellungen, die erforderlich sind, um eine sichere und gleichzeitig produktive Druckumgebung zu erstellen.³



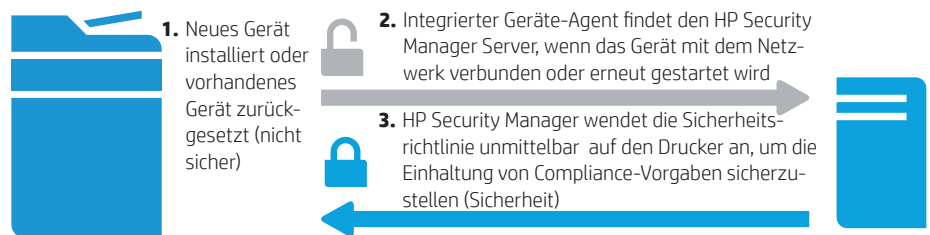
- 1 Bei der Richtlinienvvalidierung werden fehlende Elemente und potenzielle Konflikte erkannt
- 2 Anzeigen, wo die Richtlinie validiert wurde, sowie ob Warnungen oder Konflikte vorliegen
- 3 Geräte hinzufügen, überprüfen und gruppieren
- 4 Geräte analysieren und korrigieren und wiederholt auszuführende Tasks einrichten
- 5 Risikobasierte Berichte für die Managementebene
- 6 Detaillierte Berichte zu Analysen und Korrekturen

Verschiedene Möglichkeiten für die Verbindung von Geräten mit Ihrer Richtlinie

Das Hinzufügen von HP Geräten zu HP Security Manager ist sehr leicht.

- **Auto-Discovery** – Überlassen Sie die Erkennung Ihrer HP Geräte durch die automatische Erkennungsfunktion lieber Security Manager. Sie können diese Funktion so einstellen, dass eine bestimmte Anzahl von Netzwerk hops oder ein bestimmter IP-Adressbereich durchsucht wird. Dann geben Sie an, welche Geräte Sie über die erstellte Liste verwalten wollen.
- **.txt- oder .xml-Datei** – Wenn Sie mehrere Geräte hinzufügen wollen, importieren Sie eine .txt- oder .xml-Datei mit den IP-Adressen oder Hostnamen der Geräte. Sie können auch aus HP Web Jetadmin exportierte .xml-Dateien verwenden.
- **Instant-On Security** – Nutzen Sie die HP Instant-on Security Funktion, um jedes HP Gerät ohne Benutzereingriff automatisch in Security Manager hinzuzufügen, sobald es mit dem Netzwerk verbunden oder zurückgesetzt wird. HP Security Manager bietet zudem das Alleinstellungsmerkmal, dass HP Instant-on Security die Geräte sofort für die Einhaltung Ihrer jeweiligen unternehmensweiten Sicherheitsrichtlinie konfiguriert. So sparen Sie Zeit und minimieren die Risiken.

HP Instant-on Security



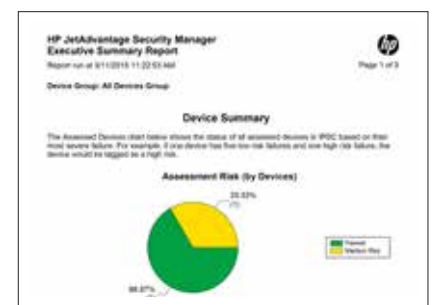
Maximaler Ertrag Ihrer Investitionen durch proaktive Compliance

HP Security Manager hilft Ihnen mit regelmäßigen Analysen und automatisierter Korrektur bei der Erfüllung von Compliance-Anforderungen. Sie legen fest, wie oft Sie sicherstellen möchten, dass die Geräte Ihre Sicherheitsrichtlinien einhalten. Täglich, wöchentlich oder monatlich – die Entscheidung liegt bei Ihnen.

- **Analyse** – Bei der geplanten Analyse vergleicht HP Security Manager im Hintergrund die Sicherheitseinstellungen Ihrer Flotte mit einer bestimmten Richtlinie. Im weiteren Verlauf des Analyseprozesses werden nicht übereinstimmende Einstellungen ermittelt und in einem Bericht dokumentiert.
- **Korrektur** – HP Security Manager wendet automatisch die korrekten Richtlinieneinstellungen auf die nicht übereinstimmenden Funktionen an, die während der Analyse ermittelt wurden. Die korrigierte Einstellung wird erneut analysiert, um zu überprüfen, ob sie erfolgreich angewendet wurde.

Risikoreduzierung durch umfassende Berichte zur Flottensicherheit

Schützen Sie Ihre Informationen mithilfe integrierter Berichtsfunktionalität. Benutzer können zusammenfassende Berichte zur Risikostufe der Flotte ausführen und dann bestimmte Risiken nach Gerät oder Sicherheitseinstellung herausfiltern. Detaillierte Berichte können zudem nach jeder automatisch terminierten Bewertung und Korrektur per E-Mail versendet werden.



Einfache, intuitive Risikobewertung

Mit HP Security Manager lassen sich auch Geräte mit niedrigeren Sicherheitsstufen ermitteln. Auf weniger sicheren Geräten ist möglicherweise nicht die aktuelle Gerätefirmware, die Jetdirect-Firmware, installiert oder keine Sure Start-, Run Time Intrusion Detection- oder Whitelisting-Funktionalität aktiviert.

Schutz Ihres Workflows durch flottenweite Zertifikatsverwaltung

Zertifikate sind für den Schutz des Informationsflusses von den Geräten und an die Geräte von zentraler Bedeutung. Zertifikate sorgen für den Beweis der Identität und die Datenverschlüsselung und ermöglichen so die sichere Kommunikation zwischen vertrauenswürdigen Entitäten. Kunden, die ihre Druckgeräte schützen möchten, stehen vor mehreren Herausforderungen, wenn es um Zertifikate geht. Die manuelle Installation eindeutiger Zertifikate kann fehleranfällig und aufwändig sein und viel Zeit beanspruchen – bis zu 15 Minuten pro Gerät. Daher verzichten viele Kunden auf die Verwendung von Zertifikaten oder auf ihre ordnungsgemäße Pflege.

Die neueste Innovation von HP Security Manager vereinfacht diesen Prozess erheblich: Eindeutige Identitätszertifikate werden über die gesamte Flotte hinweg implementiert und kontinuierlich überwacht, um ihre Gültigkeit sicherzustellen. Widerrufene oder abgelaufene Zertifikate werden automatisch ersetzt.²

HP Security Manager implementiert und aktualisiert sowohl ID- als auch CA-Zertifikate sehr effizient. So erhöht sich die Sicherheit Ihrer Infrastruktur, Anwendungen und Gerätekommunikation.

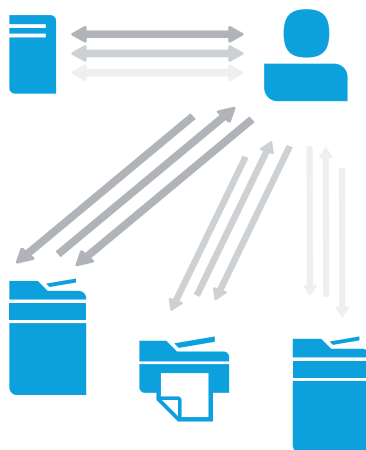
- **Schnelle Installation** – Geringerer Verwaltungsaufwand für die Installation eindeutiger Identitätszertifikate für die gesamte Flotte Ihrer HP Geräte im Vergleich zur manuellen Installation von Zertifikaten auf einem einzigen Gerät.
- **Einfache Integration** – Integration von Zertifikaten in Ihre vorhandene HP Security Manager Richtlinie sowie in die standardmäßigen Analyse- und Korrekturprozesse.
- **Automatische Verlängerung und Updates** – Automatische Analyse und Korrektur, um ohne Benutzereingriffe Zertifikate zu identifizieren und zu verlängern, bevor sie ablaufen, und widerrufene Zertifikate zu ersetzen.
- **Informatives Feedback** – Zugriff auf Berichte zur Gültigkeit der Zertifikate und Fehlerbehebung für Infrastrukturprobleme mithilfe detaillierter HP Security Manager Empfehlungen.

Automatische Zertifikatsverwaltung

Vereinfachen Sie die Verwaltung des Zertifikatsprozesses für die IT-Administratoren – und sparen Sie dadurch Zeit und Geld für Ihr Unternehmen.

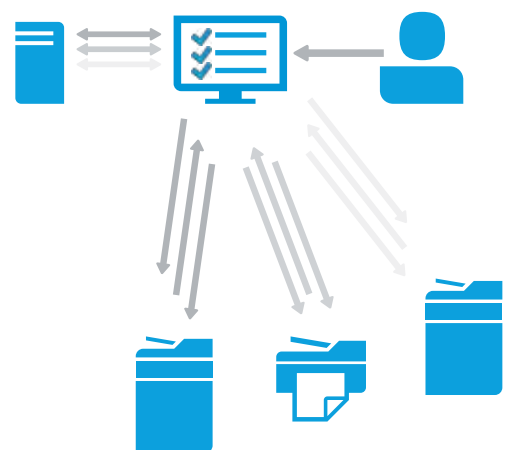
Vorher

Manuelle, zeitaufwändige und fehleranfällige Prozesse auf jedem Gerät



Nachher

Einfache, effiziente, einmalige Einrichtung für die gesamte Flotte mit HP Security Manager



Welche Vorteile bietet Ihnen diese benutzerfreundliche

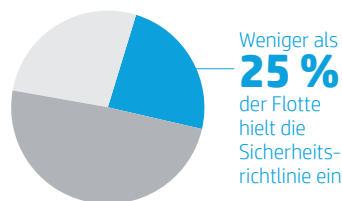
Lösung?

HP Security Manager ist eine vielseitig einsetzbare Sicherheitslösung, die in den unterschiedlichsten Kontexten und Geschäftssituationen zum Tragen kommen kann.

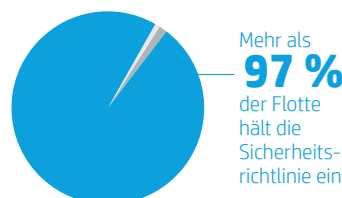
Beispielsweise wissen Finanzdienstleister, dass der Schutz ihrer Kundendaten nicht nur entscheidend für ihren Geschäftserfolg, sondern auch für ihre Branche gesetzlich vorgeschrieben ist. Bei Druckflotten, die oft Tausende von Geräten umfassen, ist das Management der Sicherheit jedoch mit einem hohen Verwaltungsaufwand verbunden.

Mit HP Security Manager können Finanzdienstleister einen Zeitplan für eine tägliche Analyse und Korrektur ihrer HP Flotte für Bildverarbeitung und Druck erstellen und so Zeit und Geld sparen. So ist sichergestellt, dass die Flotte die Sicherheitsrichtlinie des Unternehmens einhält. Gleichzeitig werden Ressourcen des IT-Teams freigesetzt, sodass dieses sich auf andere Aktivitäten konzentrieren kann. Administratoren können auch integrierte Berichte mit Informationen auf Flotten-, Geräte- oder Funktionsebene drucken oder speichern, mit deren Hilfe sehr leicht nachgewiesen werden kann, dass die Richtlinie eingehalten wird und die Kundendaten geschützt und sicher sind.

Ohne HP Security Manager



Mit HP Security Manager



Technische Daten

Unterstützte Netzwerke/ Betriebssysteme	Microsoft® Windows® 8.1 (32 und 64 Bit), Windows 8 (32 und 64 Bit), Windows 7 (32 und 64 Bit), Windows Server® 2008 R2 (64 Bit), Windows Server 2012 (32 und 64 Bit), Windows Server 2012 R2 (32 und 64 Bit)
Unterstützte Datenbanken	<ul style="list-style-type: none"> • Microsoft SQL Server Express 2012 • Microsoft SQL Server 2012 (Enterprise) • Microsoft SQL Server Express 2014 (Bundled) • Microsoft SQL Server 2014 (Enterprise)
Unterstützte Geräte	Informationen zur Gerätekompatibilität finden Sie unter hp.com/go/securitymanager
Systemvoraussetzungen	<p>Servervoraussetzungen: Mindestens Dual-Core-Prozessor mit 2,33 GHz, mindestens 4 GB RAM (32-Bit-Systeme), mindestens 8 GB RAM (64-Bit-Systeme)</p> <p>Clientvoraussetzungen: PC mit 1,8-GHz-Prozessor, 3 GB RAM (32-Bit-Systeme) bzw. 4 GB RAM (64-Bit-Systeme) als Mindestvoraussetzung</p> <p>Speichervoraussetzungen: Mindestens 4 GB verfügbarer Speicherplatz. Der erforderliche Datenbankspeicherplatz für HP Security Manager variiert und ist von Folgendem abhängig: Anzahl der analysierten Geräte, Größe der Richtlinie für den Vergleich, Anzahl der Richtlinien für die Analyse, Häufigkeit der Analyse und Empfehlungen aus den Analysen. Bei der Verwaltung von mehr als 1.000 Geräten wird dringend die Verwendung einer vollständigen SQL-Instanz empfohlen.</p>
Leistung	HP hat bis zu 10.000 Geräte auf einem Server getestet (auch eine höhere Anzahl kann möglich sein). Mit der HP Security Manager Base Policy wurden 1.500 Geräteanalysen pro Stunde erzielt.
Unterstützte Sprachen	Englisch



Bestellinformationen

Produkt

- HP JetAdvantage Security Manager Softwarelizenz:
 - Lizenz für 10 Geräte (A6A49BAE)
 - Lizenz für 50 Geräte (A6A38BAE)
 - Lizenz für 250 Geräte (A6A39BAE)
 - Lizenz für 1.000 Geräte (A6A40BAE)
- Die Lizenzen gelten unbefristet und können kombiniert werden, um die gewünschte Anzahl an Geräten zu erreichen.

Weitere Informationen

Weitere Informationen dazu, wie Sie HP JetAdvantage Security Manager zum integralen Bestandteil der IT-Sicherheitsstrategie Ihres Unternehmens machen oder wie Sie Ihre kostenlose Testversion erhalten, finden Sie unter hp.com/go/securitymanager. Sie können sich auch an Ihren HP Ansprechpartner oder einen HP Document Solutions Specialist wenden.

Weitere Informationen unter
hp.com/go/securitymanager

- ¹ Basierend auf internen geschützten HP Daten (Device Security Comparison, Januar 2015) und dem Solutions Report zu HP JetAdvantage Security Manager 2.1 von Buyers Laboratory LLC, Februar 2015.
- ² Für ausgewählte Produktmodelle und Firmware-Versionen verfügbar. Seite 5 enthält eine Liste der unterstützten Produkte. Unter hp.com/go/securitymanager finden Sie ebenfalls weitere Informationen hierzu.
- ³ Dieses Tool wird nur zu allgemeinen Vergleichszwecken zur Verfügung gestellt. Diese Informationen basieren auf den veröffentlichten und internen Spezifikationen des Herstellers sowie auf proprietären Daten und Algorithmen. Die Korrektheit dieser Informationen wird von der Hewlett-Packard Company nicht garantiert. Benutzer können die in der Analyse verwendeten Sicherheitsrichtlinien anpassen. Dies wirkt sich auf die Ergebnisse aus. Die tatsächlichen Ergebnisse können abweichen.

Melden Sie sich noch heute an.
hp.com/go/getupdated



An Kollegen weiterleiten

© Copyright 2012-2015 Hewlett-Packard Development Company, L.P. Änderungen vorbehalten. Die einzigen Garantieansprüche für HP Produkte und Services werden in den Garantieerklärungen aufgeführt, die diesen Produkten und Services beiliegen. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. HP übernimmt keine Verantwortung für die Richtigkeit und Vollständigkeit der Angaben.

Microsoft®, Windows®, Windows Server® und SQL Server® sind in den USA eingetragene Marken der Microsoft Corporation.

4AA3-9275DEE, Februar 2016, Rev. 8

