



הגן על צי המדפסות שלך עם אבטחת מדפסות פשוטה, המבוססת על מדיניות

הרחב את העסק שלך בדרך המאובטחת - עם HP JetAdvantage Security Manager



העסק שלך מתמודד עם אתגרי אבטחה מדי יום

החברה שלך יוצרת כל הזמן נתונים סודיים ורבי ערך, ההכרחיים לניהול העסק. וסביר להניח שאתה משתמש במגוון שיטות של אבטחת מידע - כולל אימות זהות, הצפנה וניטור - כדי להגן על הנתונים הללו במחשבים האישיים שלך, ברשתות ובשרתים. אבל האם סביבת ההדפסה וההדמיה שלך מאובטחת כמו שאר התשתית שלך? פרצות באבטחה ועלויות הקשורות בכך עלולות להיות גבוהות, בין אם כתוצאה מהשארת מסמכים במדפסת, עיבוד נתונים וגישים מהמחשב למדפסת, או שמירת מידע סודי ב כוננים קשיחים. כדי לעזור להגן על העסק שלך, אתה צריך פתרון שמפשט ומחזק את אבטחת המידע בכל סביבת ההדפסה וההדמיה, שיחסוך לעסק שלך זמן וכסף שיכולים לבוא לידי שימוש טוב יותר במקום אחר.

מקום ראשון בתעשייה בניהול אבטחת מידע

לכן HP פיתחה את HP JetAdvantage Security Manager, שהיא גישה זורמת המבוססת על מדיניות לאבטחת התקני ההדפסה וההדמיה של HP. עם HP Security Manager, תוכל לשפר את אבטחת המידע של צי ההדפסה וההדמיה של HP שלך לפני שתגיש את המתח הכרוך בחוויית פריצה לנתונים - מה שיעזור להגן על ההתקנים שלך ועל המידע שבזכותו החברה שלך פועלת.

HP Security Manager מציע תהליך פשוט ואינטואיטיבי לאבטחת צי המדפסות שלך. פרוס את המדפסות ונטר אותן ביעילות באמצעות החלת מדיניות אבטחת מידע אחידה על פני כל הצי, ואבטח התקני HP חדשים בוגע שהם מתחברים לרשת שלך באמצעות HP Instant-on Security. כהל באופן פעיל את התחזוקה ודא את התאימות לכללי מדיניות אבטחת מידע שהגדרת בעזרת הבקרה והדיווח האוטומטיים המבוססים על נתונים של HP Security Manager. סמוך על הפריסה והעדכון האוטומטיים של אישורי זהות המחזקים את אבטחת המידע, בעוד הם מפחיתים עלויות תקורה מנהליות.

אבטח את צי המדפסות שלך עם הפתרון ש - Buyers Laboratory (BLI) מכנה "פורץ דרך".¹ HP JetAdvantage Security Manager הוא פתרון אבטחת המידע המקיף ביותר בשוק, המציע גישה יעילה המבוססת על מדיניות, לאבטחת התקני ההדפסה וההדמיה של HP.



מקור: "Managed Print Services Landscape, 2014" Quocirca, June 2014



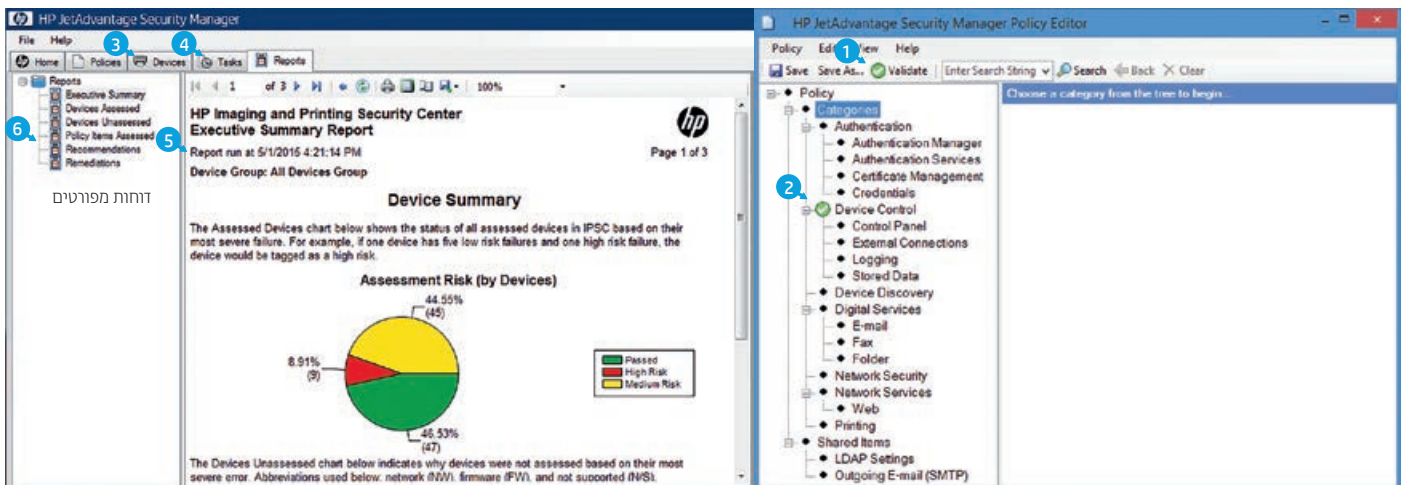
כיצד HP Security Manager מאבטח את צי המדפסות שלך

HP Security Manager מציע גישה הוליסטית לאבטחת צי המדפסות של HP, המחזקת את התאימות לתקנות ומפחיתה סיכונים.

מספק אבטחה לצי המדפסות באמצעות יצירת מדיניות ללא מאמץ

HP Policy Editor הוא כלי קל לשימוש המפשט את יצירת המדיניות בעזרת מנוע כללים אינטואיטיבי שמספק הדרכה ועוזר ליצור מדיניות מקיפה עבור סביבת העבודה שלך. שנה בקלות את מדיניות אבטחת המידע שלך כך שתתאים בדיוק לצרכים המשתנים בחברה שלך, להגולציה או לתקני התעשייה.

HP Security Manager Base Policy – צור בקלות מדיניות אבטחת מידע לסביבת ההדפסה שלך באמצעות תבנית של HP Security Manager Base Policy. התבנית מספקת גישה בסיסית לאבטחת מידע של סביבת ההדפסה הנפוצה בארגונים, אך ניתן להתאים אותה בקלות לזרישות מיוחדות בתחום המדיניות של אבטחת מידע. התבנית משלבת הגדרות מתוך רשימת נהלי האבטחה הטובים ביותר של HP, שאושרה על-ידי המכון הלאומי לתקנים וטכנולוגיה (NIST), ביחד עם תובנות הלקוח לגבי הגדרות האבטחה הנחוצות לו ליצירת בסיס אבטחה מאובטחת גם יעילה.³



- 1 אימות המדיניות מזהה פריטים שהוחצו והתנגשויות פוטנציאליות
- 2 בדיק היכן המדיניות שלך מאומתת והיכן יש אזהרות או התנגשויות
- 3 הוסף, אמת וקבץ התקנים
- 4 הערך ותקן את ההתקנים שלך והגדר משימות חוזרות
- 5 דיווח מבוסס סיכונים ברמה ביצועית
- 6 דוחות מפורטים על הערכות ותיקונים

חבר התקנים למדיניות שלך במגוון דרכים

קל להוסיף התקני HP אל HP Security Manager.

- **גילוי אוטומטי** – תן ל- Security Manager גלות את התקני HP שלך בעזרת הגילוי האוטומטי. הגדור אותו לחפש מספר מסוים של דילוגים ברשת או בטווח מסוים של כתובות IP. לאחר מכן, בחר אילו התקנים תרצה לנהל מתוך הרשימה.
- **קובץ txt או xml**. – הוסף התקנים רבים על-ידי ייבוא של קובצי txt או xml. עם כתובות IP או שמות מארח (host) של ההתקנים, כולל קובצי xml. המיוצאים מ-HP Web JetAdmin.
- **Instant-On Security** – השתמש במאפיין HP Instant-on Security כדי להוסיף באופן אוטומטי כל התקן HP אל Security Manager ברגע שהוא מתחבר לרשת שלך או מאופס מחדש, ללא כל התערבות. רק ב-HP Security Manager, המאפיין HP Instant-on Security גם מגדיר באופן מיידי את תצורת ההתקנים כך שיתאימו למדיניות אבטחת המידע הספציפית בארגון שלך – ובכך חוסך לך זמן ומצמצם סיכונים למינימום.

HP Instant-on Security

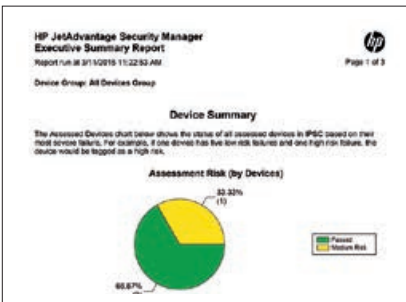


מקסם את ההשקעות שלך עם תאימות פרואקטיבי לתקנות

HP Security Manager עוזר לשמור על תאימות בעזרת הערכות קבועות ותיקונים אוטומטיים. אתה מחליט באיזו תכיפות תרצה לוודא שההתקנים שלך תואמים למדיניות אבטחת המידע שלך. מדי יום, שבוע או חודש – ההחלטה היא שלך.

- **הערכה** – במהלך ההערכה המתוזמנת מראש, HP Security Manager פועל ברקע ומאמת את הגדרות האבטחה של צי המדפסות שלך בהשוואה למדיניות מסוימת. לאחר מכן, תהליך ההערכה מזהה ומדווח על כל מאפיין שאינו תואם.
- **תיקון** – HP Security Manager מחיל אוטומטית את הגדרות המדיניות הנכונות על כל מאפיין שזוהה כאינו תואם במהלך ההערכה. הגדרות התאימות עוברת הערכה נוספת כדי לוודא שהחולה בהצלחה.

הפחת את הסיכונים בעזרת דיווח מקיף על אבטחת צי המדפסות



הערכת סיכונים פשוטה ואינטואיטיבית

הגן על המידע שלך עם דיווח מובנה. משתמשים יכולים להריץ דוחות מסכמים על רמת הסיכון הכוללת של צי המדפסות, ולאחר מכן לתחקר לתוך סיכונים ספציפיים לפי התקן או הגדרות אבטחה. ניתן להגדיר גם קבלת דוחות ברמה גבוהה בדוא"ל לאחר כל הערכה מתוזמנת אוטומטית ותיקון.

HP Security Manager יכול גם לבצע הערכה על מנת לעזור לך לזהות התקנים מאובטחים פחות. התקנים מאובטחים פחות הם אלה שאין להם את קושחת ההתקן העדכנית ביותר, קושחת Jetdirect, או שאין להם יכולות של Sure Start, גילוי פריצה בזמן ריצה או שימוש ברשימות לבנות.

הגן על זרימת העבודה שלך עם ניהול האישורים של צי המדפסות

אישורים הם מצעים חיוניים להגנה על זרימת המידע מההתקנים שלך ואליהם. הם משמשים כדי להוכיח זהות ולהצפין נתונים, ומאפשרים תקשורת מאובטחת בין ישויות אמינות. עם זאת, לקוחות המעוניינים לאבטח את התקני ההדפסה שלהם בתקלים בכמה אתגרים כשמדובר באישורים. התקנה ידנית של אישורים ייחודיים עלולה להיות משימה רגישה לטעויות, מייגעת וממושכת – עד 15 דקות למדפסת. זה גורם ללקוחות לוותר לחלוטין על השימוש באישורים או על תחזוקה ראויה שלהם.

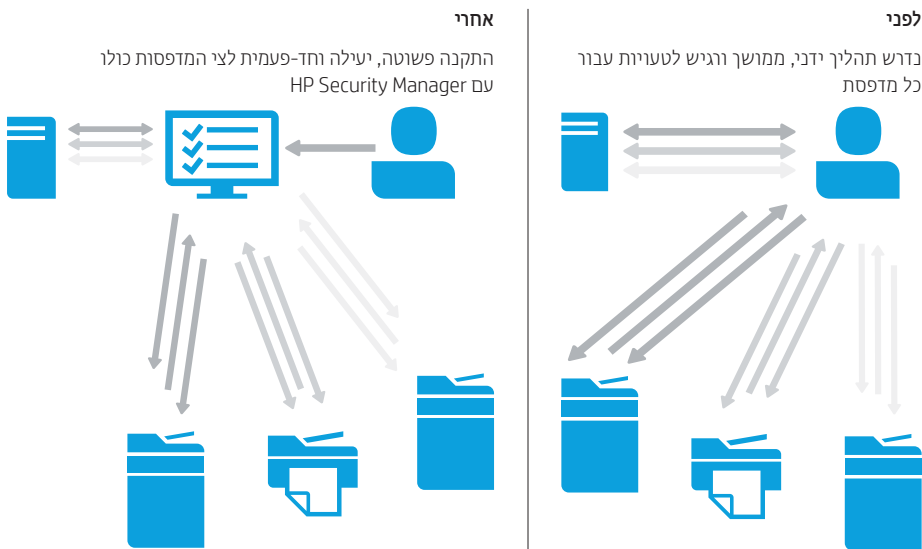
היחידשים האחרונים של HP Security Manager מפשטים תהליך זה באמצעות פריסה של אישורי זהות ייחודיים בכל צי המדפסות שלך, ניטור רצוף שלהם כדי לוודא שהם עדיין בתוקף, והחלפה אוטומטית של אישורים שבוטלו או שפג תוקפם?

HP Security Manager מחיל ומעדכן ביטולות אישורי זהות ו-CA – ובכך מגביר את אבטחת התשתית, האפליקציות והתקשורת בין ההתקנים.

- **התקנה מהירה** – התקן אישורי זהות ייחודיים בכל צי התקני HP שלך עם תקורה מנהלית נמוכה יותר מזו של התקנת אישורים ידנית בהתקן יחיד.
- **שילוב קל** – שלב אישורים במדיניות HP Security Manager הקיימת שלך ובהערכות והתיקונים הסטנדרטיים.
- **חידוש ועדכונים אוטומטיים** – השתמש בהערכה ובתיקונים אוטומטיים כדי לזהות ולחדש אישורים לפני שתוקפם פג, והחלף אישורים שפג תוקפם ללא התערבות אנושית.
- **משוב אינפורמטיבי** – היכנס לדוחות על תוקף האישורים, ובצע תהליך פתרון בעיות כדי לפתור בעיות בתשתית באמצעות ההמלצות המפורטות של HP Security Manager.

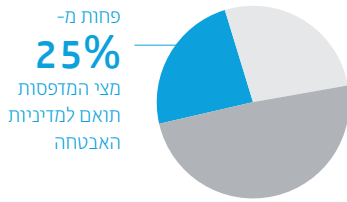
ניהול אישורים אוטומטי

הקל על מנהלי ה-IT לנהל את תהליך האישורים - ועזור לעסק שלך לחסוך זמן וכסף.



כיצד תרוויח מהפתרון הקל לשימוש הזה?

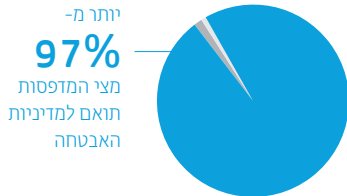
לפני HP Security Manager



HP Security Manager הוא פתרון מגוון לאבטחת מידע שיכול להתאים למבחר של הקשרים ומצבים עסקיים.

לדוגמה, חברות שירותים פיננסיים יודעות שהשמירה על מידע של לקוחות היא חיונית להצלחת העסק שלהם, ונדרשת על-פי תקנות התעשייה. יחד עם זאת, כשמדובר בצי מדפסות הכולל לעתים קרובות אלפי מדפסות, תחזוקה של אבטחת מידע מחייבת השקעה רבה באדמיניסטרציה.

אחרי HP Security Manager



עם HP Security Manager, חברות שירותים פיננסיים יכולות לחסוך זמן וכסף על-ידי תזמון מראש של הערכה ותיקון יומיים של צי ההדפסה וההדמיה של HP שלהן. דבר זה עוזר להבטיח שצי המדפסות ממשיך להיות תואם למדיניות אבטחת המידע של החברה, בעוד שהוא משחרר את צוות ה-IT לפעילויות אחרות. מנהלנים יכולים גם להדפיס או לשמור דוחות מובנים על צי המדפסות, ההתקנים או המאפיינים כהוכחת תאימות למדיניות, מה שמקל לודא שהמידע של לקוחות נשמר באופן בטוח ומאוטומט.

מפרט טכני

Windows 7 (32 ו-64 bit), Windows 8 (32 ו-64 bit), Windows 8.1 (32 ו-64 bit), Windows Server 2012 (32 ו-64 bit), Windows Server® 2008 R2 (64 bit), Windows Server 2012 R2 (32 ו-64 bit)	מערכות הפעלה של רשתות הנתמכות על-ידי המערכת
<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) 	מסדי נתונים נתמכים
למידע על תאימות התקנים, אנא בקרו באתר hp.com/go/securitymanager	התקנים נתמכים
<p>דרישות שרת: 2.33 GHz dual-core processor minimum, 4 GB RAM minimum (32-bit systems), 8 GB RAM minimum (64-bit systems)</p> <p>דרישות לקוח: PC עם 1.8 GHz processor minimum, 4 GB RAM מינימום (מערכות 64-bit), 3GB RAM minimum (מערכות 32-bit)</p> <p>דרישות אחסון: מינימום מקום זמין בכונן: 4 GB. כמות אחסון מסד הנתונים הדרושה עבור HP Security Manager משתנה והיא מבוססת על המדדים: מספר המדפסות המוערכות, גודל המדיניות שיש להעריך כנגדה, מספר התקנונים המשמשים להערכה, תדירות ההערכות והמלצות מההערכות. מומלץ מאוד להשתמש ב-SQL מלא כאשר מנהלים יותר מ-1,000 התקנים.</p>	דרישות המערכת
HP בדקה עד 10,000 מדפסות לשרת (כמויות גדולות יותר עשויות להיות אפשריות), והשיגה 1,500 הערכות התקן בשעה באמצעות HP Security Manager Base Policy.	ביצועים
אנגלית	שפות נתמכות

מידע על הזמנות

מוצר

- HP JetAdvantage Security Manager - אישור תוכנה:
 - 10 אישורי התקן (A6A49BAE)
 - 50 אישורי התקן (A6A38BAE)
 - 250 אישורי התקן (A6A39BAE)
 - 1,000 אישורי התקן (A6A40BAE)
- האישורים הם לצמיתות וניתנים לסידור בכל שילוב כדי להגיע לכמות ההתקנים הרצויה.



למידע נוסף

כדי ללמוד יותר על הפיכת HP JetAdvantage Security Manager לחלק בלתי נפרד מאסטרטגיית אבטחת המידע הכוללת בחברה שלך או כדי לקבל התנסות בחינם, בקר באתר hp.com/go/securitymanager, צור קשר עם נציג HP שלך, או צור קשר עם מומחה HP Document Solutions.

פרטים נוספים באתר

hp.com/go/securitymanager

¹ מבוסס על נתוני HP Internal secured (השוואת אבטחת מידע של מדפסות, ינואר 2015), דוחות פתרון על HP JetAdvantage Security Manager 2.1 ב-Buyers Laboratory LLC, פברואר 2015.
² זמין בדגמי מוצר וגרסאות קושחה נבחרים. ראה בעמוד 5 את רשימת המוצרים הנתמכים, או בקר באתר hp.com/go/securitymanager לקבלת פרטים.
³ כלי זה מסופק למטרת השוואה כללית בלבד. מידע זה מבוסס על מפרטי יצון שפורסמו ומפרטים פנימיים, ועל נתונים ואלגוריתמים קבייביים. Hewlett-Packard Company אינה ערבה לדיוק המידע. משתמשים יכולים להתאים את מדיניות האבטחה המשמשת לניתוח, אך זה ישיפע על התוצאות. התוצאות בפועל עשויות להשתנות.

הירשם לקבלת עדכונים
hp.com/go/getupdated

