



احم شبكتك باستخدام الطباعة الأكثر أمانًا من HP¹

43%



من الشركات تجاهلت
الطباعات في ممارسات
أمان الأجهزة الطرفية⁴
لديها

61%



من المؤسسات أبلغت
بحدوث اختراق بيانات
واحد على الأقل ذي صلة
بالطباعات خلال العام
الماضي³

94%



من الشركات المالية
تقول أن أمان أجهزة
النسخ/الطباعات مهم
أو مهم للغاية²



18% من الشركات فقط تراقب الطابعات لمنع التهديدات.⁴ ماذا عن شركتك؟

التعرف على المخاطر الخفية

يتم تكليف أقسام تكنولوجيا المعلومات باستمرار بحماية المعلومات السرية، بما في ذلك هويات الموظفين وبيانات العملاء عبر العديد من الأجهزة والبيئات. وعلى الرغم من تطبيق الكثير من إدارات تكنولوجيا المعلومات تدابير أمان صارمة على كل جهاز كمبيوتر وكذلك الشبكة، فعادة ما يتم تجاهل أجهزة الطباعة والتصوير وتركها دون حماية. وعندما تكون هناك أجهزة غير مؤمنة، فمن الممكن أن تكون الشبكة بأكملها عرضة للهجمات الإلكترونية.

معرفة التكاليف المحتملة

حتى اختراق الأمان الواحد من المحتمل أن يكون مكلفًا. إذا تعرضت المعلومات الخاصة للخطر نتيجة للطباعة والتصوير غير الآمنين، فقد يؤدي ذلك إلى حدوث عواقب تتضمن سرقة الهوية وسرقة المعلومات التنافسية وتشويه العلامة التجارية والسمعة والتعرض للتقاضي. وبالإضافة إلى ذلك، قد يؤدي عدم الامتثال التنظيمي والقانوني إلى غرامات باهظة.

تقدم لك شركة HP سبل المساعدة

اعمل على حماية شبكتك باستخدام تقنية الطباعة الأكثر أمانًا من HP.¹ فطابعات HP تتمتع دائمًا بالحماية وتكتشف التهديدات وتوقفها بشكل مستمر إلى جانب التكيف مع المتغيرات الجديدة. ومن الممكن أن تساعدك HP في أتمتة عمليات الحماية بالجهاز والبيانات والمستندات باستخدام مجموعة كبيرة من الحلول. ويمكن لخبراء أمان الطباعة لدينا مساعدتك في تطوير استراتيجية أمان للتصوير والطباعة ونشرها بشكل متكامل.

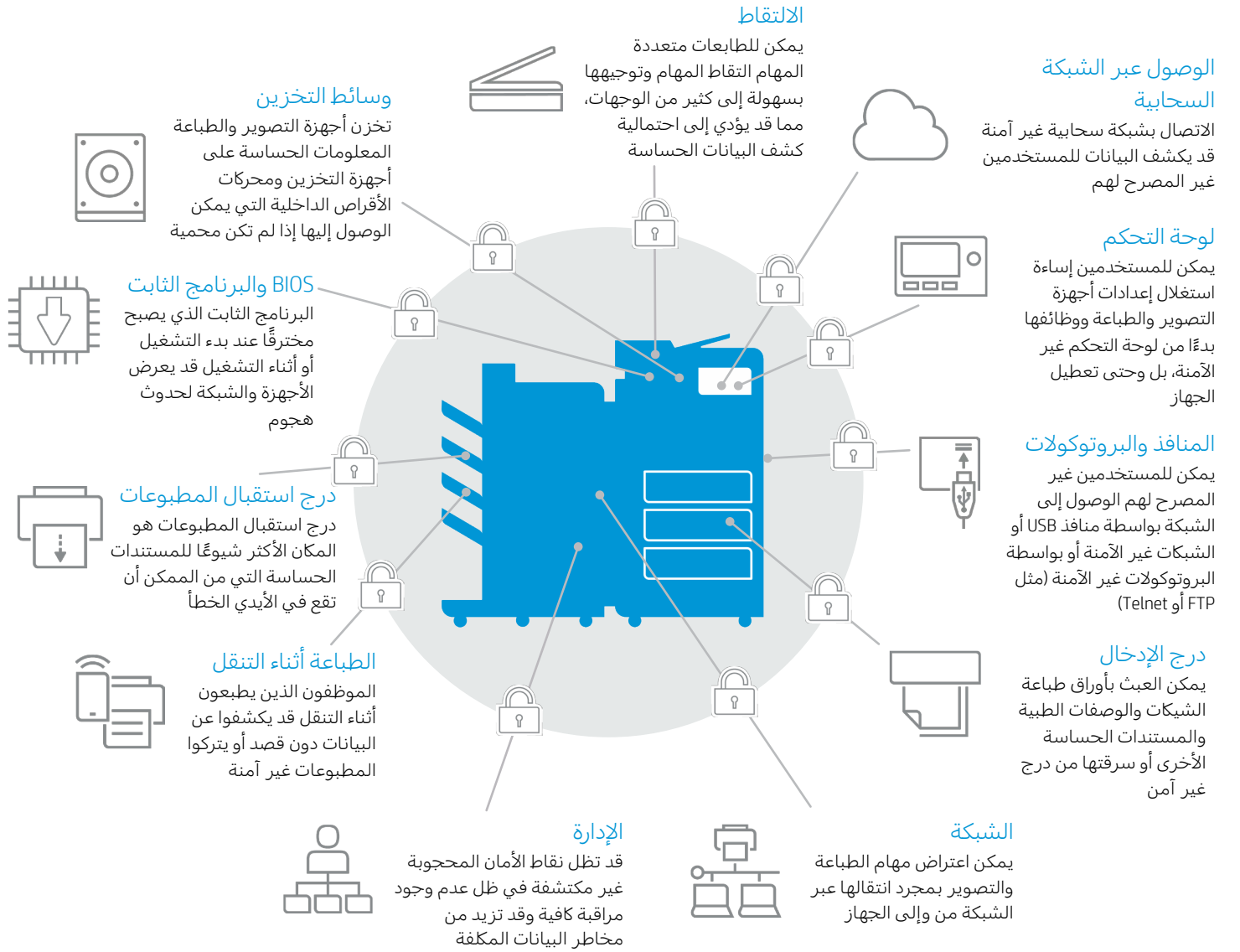
"تأكيدًا على استثمارها
الطويل في أمان الطباعة،
تمتلك شركة HP مجموعة
حلول وخدمات الأمان
الأكبر والأعمق في
السوق."

– شركة Quocirca، يناير 2017⁵

حماية الأجهزة والبيانات والمستندات

قد تحدث ثغرات خطيرة في نقاط متعددة داخل بيئة التصوير والطباعة لديك. وبمجرد التعرف على نقاط الضعف هذه، يمكنك تقليل المخاطر التي تتعرض لها بطريقة أكثر سهولة.

نقاط ضعف التصوير والطباعة





حماية الجهاز

صُممت طابعات HP لتعمل مع حلول مراقبة وإدارة الأمان للمساعدة في تقليل المخاطر وتحسين الامتثال وحماية شبكتك بأكملها. (لا تتوفر جميع الميزات والحلول على جميع أجهزة HP.⁶)

ممارسات الأمان الأساسية



اكتشاف المزيد

خدمات إعادة تدوير مخصصة من HP
hp.com/go/businessrecycling

خدمات الطباعة المدارة الآمنة من HP
hp.com/go/securemps

التخزين المشفر مع المسح الآمن

أي معلومات حساسة مخزنة على محرك الأقراص الداخلي أو القرص الثابت من المحتمل أن تكون عرضة للسرق. لذا، يأتي كثير من أجهزة HP بتشغيل مضمّن لحماية بياناتك. وعندما لا تكون هناك حاجة إلى البيانات المخزنة، استخدم إمكانيات الجهاز المضمّنة لاستبدال البيانات وإزالة المعلومات الحساسة بشكل آمن.

التخلص الآمن

تضمن خدمات إعادة التدوير المخصصة من HP إزالة البيانات من محركات الأقراص الثابتة قبل إعادة تدوير المنتجات القديمة بطريقة مسؤولة.

الوصول الآمن لإصلاح الطابعة

ستساعد معرفة الممارسات الأمنية لموردي صيانة الطابعة في حماية البيانات الحساسة. اختر خدمات الطباعة المدارة الآمنة من HP (MPS) أو شركاء HP للحصول على مساعدة الخبراء.

تعطيل المنافذ غير المستخدمة والبروتوكولات

قلل معدل الهجمات من خلال التكوين المناسب للجهاز. عطّل المنافذ الفعلية والبروتوكولات غير الآمنة (مثل FTP أو Telnet) لمنع الوصول أو الاستخدام غير المصرح به.

التحكم في وصول المسؤول إلى الجهاز

تمكن من تعيين كلمات المرور للمسؤول بحيث لا يمكن إلا لموظفي تكنولوجيا المعلومات أو الموظفين الآخرين المصرح لهم ضبط إعدادات الجهاز وتكوينها فقط.

الإدراج في القائمة البيضاء لكود البرنامج الثابت

راجع الصفحة التالية للاطلاع على معلومات حول كيفية مساعدة ميزة الإدراج في القائمة البيضاء في حماية أسطولك من البرامج الضارة.

ممارسات أمان متقدمة

شهادة المعايير الشائعة

تم اعتماد طابعات الأعمال من HP باعتبارها متوافقة مع معايير الأمان المعترف بها دوليًا، مثل شهادة المعايير الشائعة (CCC) و FIPS 140. وهذا يضمن أن تكون تحديثات البرنامج الثابت للجهاز موفّعة بكود لتأكيد أصالة وسلامة الكود والمحافظة على الامتثال.

مميزات تأمين الطباعة تكتشف الهجمات وتوقفها تلقائيًا

تتضمن طابعات الأعمال من HP مميزات أمان تساعد في حمايتها من أن تكون نقطة دخول للهجمات على شبكتك. فمميزات أمان الطباعة من HP تكتشف التهديدات على الفور وتقدم مراقبة تلقائية علاوة على التحقق من صحة البرامج المضخنة لإيقاف التهديدات لحظة بدئها.⁷



اكتشاف المزيد

مميزات أمان مضمنة للطباعة:

- HP Sure Start (سلامة BIOS)
- الإدراج في القائمة البيضاء لكود البرنامج الثابت
- رصد الاختراقات وقت التشغيل
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager

hp.com/go/securitymanager

تمتاز طابعات الأعمال من HP بدءًا من طراز Pro⁸ حتى Enterprise⁷ بحماية دائمة، مما يمكنها من اكتشاف التهديدات وإيقافها بشكل مستمر أثناء جميع مراحل التشغيل:

- **أثناء بدء التشغيل.** كود بدء التشغيل (لأجهزة Pro) أو BIOS (لأجهزة Enterprise) هو عبارة عن مجموعة من الإرشادات المستخدمة لتحميل مكونات الأجهزة الهامة وبدء تشغيل البرنامج الثابت. إذ يتم التحقق من سلامة الكود في كل دورة بدء تشغيل، مما يساعد في حماية جهازك من الهجمات.
- **عند تحميل البرنامج الثابت.** تفحص ميزة الإدراج في القائمة البيضاء البرنامج الثابت أثناء بدء التشغيل للتأكد من الكود الأصلي الموفّع رقميًا من قبل HP. وفي حال اكتشاف أي حالة غير طبيعية، تتم إعادة تشغيل الجهاز وإعادته إلى الحالة الآمنة دون اتصال بالشبكة ويتم إبلاغ قسم تكنولوجيا المعلومات.
- **خلال وقت التشغيل.** تساعد المميزات المضمنة من HP في حماية ذاكرة الجهاز بينما يتم تشغيل الأجهزة وتوصيلها بالشبكة مباشرة عند حدوث معظم الهجمات. وفي حالة حدوث هجوم، يتم إيقاف تشغيل الجهاز.

يمكن لأجهزة HP Enterprise إصلاح نفسها

علاوة على قدرتها على اكتشاف التهديدات وإيقافها، تصلح طابعات HP Enterprise نفسها من الهجمات بحيث لا تحتاج إلى تدخل من قسم تكنولوجيا المعلومات.⁷ وتبدأ هذه الميزات إعادة التشغيل تلقائيًا في حالة حدوث هجوم أو شيء غير طبيعي. ويمكن إبلاغ المسؤولين بواسطة إدارة معلومات وأحداث الأمان (SIEM)، مثل ArcSight و Splunk و SIEMonster.

- HP Sure Start هو عبارة عن نظام BIOS ممتاز للإصلاح الذاتي.⁷ وإذا كان نظام BIOS مخترقًا، يعيد HP Sure Start بدء تشغيل الجهاز باستخدام "نسخة ذهبية" آمنة من نظام BIOS الخاص به.
- اكتشاف الاختراقات وقت التشغيل يراقب عمليات البرنامج الثابت والذاكرة المعقدة ويوقف التدخل تلقائيًا ويعيد التشغيل في حالة حدوث هجوم.
- HP Connection Inspector يقيم اتصالات الشبكة الصادرة لتحديد الطلبات الطبيعية وإيقاف الطلبات المريبة، ثم يوقف عمل البرامج الضارة عن طريق بدء إعادة التشغيل تلقائيًا.

وبفضل حماية الاستثمارات المدفوعة في الأجهزة التي يقدمها البرنامج الثابت HP FutureSmart القابل للترقية، يمكنك إضافة ميزة الإدراج في القائمة البيضاء واكتشاف الاختراق وقت التشغيل و HP Connection Inspector إلى الكثير من طابعات HP Enterprise الموجودة.⁷

يكمل برنامج HP JetAdvantage Security Manager دورة الفحص

بعد إعادة التشغيل أو إضافة جهاز جديد إلى الشبكة، يقيم HP JetAdvantage Security Manager إعدادات أمان الجهاز ويصلحها تلقائيًا إذا لزم الأمر، وذلك من أجل الامتثال لسياسات الشركة الموضوعية مسبقًا.⁹ ولن تكون هناك حاجة إلى تدخل قسم تكنولوجيا المعلومات.

كيف يعمل ذلك؟

تعالج مميزات الأمان المضمنة الخطوات الأساسية الأربعة في دورة عمل جهاز HP.

وفي حالة وقوع هجوم، يمكن إعادة تشغيل أجهزة HP Enterprise وإصلاحها ذاتيًا.

ويكمل برنامج HP JetAdvantage Security Manager دورة الفحص.

أربعة. المراقبة المستمرة

تحمي العمليات وتوقف الهجمات أثناء تشغيل الجهاز.
يفحص اتصالات الشبكة الصادرة لإيقاف الطلبات المريبة (طرز Enterprise فقط).

واحد. فحص كود بدء التشغيل/BIOS

يمنع تنفيذ تنفيذ الأكواد الضارة أثناء بدء التشغيل عن طريق عدم السماح بالتحميل إلا للكود الأصلي الموقع من HP فقط.

ثلاثة. فحص الإعدادات

بعد إعادة التشغيل، يبحث HP JetAdvantage Security Manager عن إعدادات حماية الجهاز المتأثرة ويصلحها.

اثنان. فحص البرنامج الثابت

لا يسمح إلا بتحميل الكود الأصلي — الموقع رقميًا من قبل HP.



حماية البيانات

تتطلب بياناتك حماية متواصلة أثناء تخزينها أو نقلها. فيما يلي بعض الخطوات الأساسية للمساعدة في ضمان الوصول والاستخدام الآمن.⁶

ممارسات الأمان الأساسية

معايير 802.1x أو IPsec للشبكة

استخدم معايير الشبكة المشفرة لحماية البيانات التي يتم نقلها عبر الشبكة بين الجهاز والأدوات الإدارية، مثل HP Web Jetadmin أو HP Embedded Web Server.

تشفير البيانات أثناء نقلها

احم مهام الطباعة أثناء نقلها إلى الجهاز باستخدام تشفير مثل بروتوكول عبر TLS (IPPS). أو سيوفر HP Universal Print Driver Secure Encrypted Print تشفير AES256 قويًا ومتسقًا لمهام الطباعة بالإضافة إلى فك التشفير من العميل إلى الصفحة استنادًا إلى كلمة مرور معرفة من قبل المستخدم باستخدام مكتبات FIPS 140 للتشفير من Microsoft® تم التحقق من صحتها.

وعند المسح الضوئي، ستساعدك حلول HP JetAdvantage Workflow في حماية المعلومات الحساسة مع زيادة الكفاءة. على سبيل المثال، يتكامل HP Capture and Route بسلاسة مع HP Access Control للحصول على أمان محشن بالإضافة إلى المصادقة الفريدة التي تتميز بالسهولة وإمكانية مراقبة المحتويات لإدارة المعلومات بسهولة.¹⁰

تشفير البيانات أثناء التخزين

احم معلومات العمل الحساسة المخزنة على القرص الثابت باستخدام تشفير مضمّن. للحصول على مستوى أمان إضافي، يمكن إضافة وحدة نمطية للنظام الأساسي الموثوق به من HP (TPM) إلى الجهاز لتقوية حماية بيانات الاعتماد المشفرة والبيانات عن طريق ربط مفاتيح تشفير الجهاز تلقائيًا بالوحدة النمطية للنظام الأساسي الموثوق به. فهي توفر هوية آمنة للجهاز عن طريق توليد مفاتيح خاصة بالشهادات وحمايتها.

الحماية عن طريق جدار الحماية

تمكن من منع البرامج الضارة والفيروسات من دخول شبكتك عن طريق تحديد وصول الطابعة إلى أجهزة الكمبيوتر في الشركة.

المصادقة الأصلية للمستخدم

تمكن من تقليل التكاليف ومخاطر الأمان عن طريق طلب تسجيل الدخول من المستخدمين باستخدام مصادقة PIN/PIC أو LDAP أو Kerberos. ويمكنك أيضًا دمج المصادقة بالدليل النشط Active Directory.

عناصر التحكم في الوصول المستندة إلى أدوار

يساعد HP Access Control Rights Management في خفض التكاليف ومخاطر الأمان من خلال قيود ميزات الطباعة، تتيح لك عناصر التحكم في الوصول المستندة إلى أدوار منح القدرات التي تختلف باختلاف المستخدم أو القسم الذي ينتمي إليه وفقًا لاحتياجاته. على سبيل المثال، يمكنك تحديد الأشخاص الذين يستخدمون وظائف الفاكس أو الإرسال إلى البريد الإلكتروني أو المسح الضوئي إلى الفاكس.



اكتشاف المزيد

HP Web Jetadmin
hp.com/go/wia

يوفر برنامج تشغيل الطباعة العام
من HP طباعة آمنة مشفرة
hp.com/go/upd

حلول HP JetAdvantage Workflow
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

ممارسات أمان متقدمة

المصادقة والتعقب المتقدمين

تمكن من نشر مصادقة متقدمة (مثل كلمات المرور أو بطاقات التقارب أو البطاقات الذكية أو القياسات الحيوية) وحلول التعقب للحصول على تحكم وأمان إضافيين.

- HP Access Control Secure Authentication يستعيد التحكم ويعزز الأمان ويقلل التكاليف. احصل على مجموعة متنوعة من عناصر التحكم والخيارات المتقدمة، بما في ذلك اللمس للمصادقة باستخدام أجهزة محمولة مزودة بتقنية الاتصالات قريبة المدى.
- HP Access Control Job Accounting يساعدك في تعقب البيانات وجمعها بدقة وتحليل النتائج ثم إنشاء التقارير وإرسالها. استخدم ميزة التنقيب في البيانات لتخصيص تكاليف الطباعة وتحفيز الموظفين للطباعة بطريقة أكثر ذكاءً وتقديم المعلومات الضرورية لقسم تكنولوجيا المعلومات لتحسين التوقعات على نطاق الأسطول.



اكتشاف المزيد

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

الأجهزة المحمولة مضمّنة في الوصول إلى الشبكة

استخدم أجهزتك المحمولة كجزء من سياسة أمان الطباعة بشكل عام للتحكم في الوصول إلى الطباعة. إذ تقدم شركة HP حلاً تستند إلى خادم توفر طباعة آمنة بالسحب، بالإضافة إلى إمكانيات الإدارة وإعداد التقارير المتقدمة.

- HP JetAdvantage Connect* يوفر طباعة سهلة ويُعتمد عليها مصممة للشركات عن طريق الأجهزة المحمولة. ساعد في توفير الوقت والمال من خلال الاستفادة بسلاسة من أدوات وسياسات الشبكات الحالية لتكنولوجيا المعلومات اللازمة لإدارة الطباعة عن طريق الأجهزة المحمولة.¹¹ إذ يمكن للمستخدمين الطباعة بأمان عن طريق العديد من الهواتف الذكية وأجهزة الكمبيوتر اللوحية أينما ووقتما احتاجوا إليها، وبنفس سهولة الطباعة من الكمبيوتر.
- HP Access Control يتضمن إمكانيات لإدارة الطباعة عن طريق الأجهزة المحمولة. فهو يعزز بنية البريد الإلكتروني الحالية، مما يسمح لمستخدمي الأجهزة المحمولة بإرسال مهمة طباعة بالبريد الإلكتروني إلى قائمة انتظار الطباعة الخاصة بهم، ثم سحبها من أي طابعة عادية أو متعددة المهام تم تمكين أي حل بها. احم خدمات الطباعة عبر الشبكة باستخدام ميزات المصادقة الآمنة، بما في ذلك "إصدار الجهاز المحمول".

قم بسد تسرب البيانات قبل أن يبدأ

توفر حلول HP القدرات التي تساعدك على الوقاية من فقدان البيانات. مع الخدمة الواقية *HP Capture and Route Data Loss Prevention* يمكنك منع البيانات الحساسة من أن يتم تصويرها أو إرسالها بالفاكس. الخدمة الواقية *HP Access Control Print Data Loss Prevention* تتيح لك منع طباعة المستندات الحساسة. تمكن من تعقب بياناتك المهمة للغاية لإيقاف الاختراقات ومنعها دون إبطاء سير العمل. احصل على تنبيهات الأمان الذكية استناداً إلى شروط تحددها أنت.

تطبيق الشهادات الرقمية على الطابعات

تمتع بتحسين أمان بيئة الطباعة لديك عن طريق تطبيق الشهادات الرقمية على الطابعات العادية ومتعددة المهام للشبكات. وفر الوقت باستخدام *HP JetAdvantage Security Manager* لتثبيت الشهادات وتجديدها تلقائياً.⁹



حماية المستندات

يمكن من دمج حلول الأجهزة والبرامج باستخدام خطة أشمل لأمان تكنولوجيا المعلومات لحماية المعلومات الحساسة في مستنداتك المطبوعة.⁶

ممارسات الأمان الأساسية

التحكم في الوصول إلى النماذج المطبوعة مسبقًا

زود طابعاتك العادية ومتعددة المهام بأدراج إدخال مزودة بأقفال للمساعدة في منع سرقة الأوراق الخاصة المستخدمة لطباعة الشيكات أو الوصفات الطبية أو المستندات الحساسة الأخرى.

استخدام رقم تعريف شخصي أو الطباعة بالسحب لحماية المستندات الحساسة

يمكن للمستخدمين اختيار استخدام رقم تعريف شخصي أو الطباعة بالسحب، مما يقلل من الاعتماد على الطابعات الشخصية، فضلاً عن خطر وقوع مهام الطباعة في الأيدي الخطأ. كما تقلل إجراءات الأمان هذه عمليات الطباعة غير المطلوبة التي يمكن أن تقلل التكاليف والنفقات.

وبخصوص الطباعة باستخدام رقم تعريف شخصي، عندما يرسل المستخدمون مهام طباعة سرية، يعيّنون رقم تعريف شخصيًا يلزم إدخاله في الجهاز لتحرير المهمة.

أما الطباعة بالسحب، فتخزن مهام الطباعة في السحابة أو على كمبيوتر المستخدم. إذ تتم مصادقة المستخدمين في مواقع الطباعة التي يختارونها لسحب مهامهم وطابعاتها. لذا، تقدم HP حلي الطباعة بالسحب التاليين اللذين يستندان إلى سحابة*:

- HP JetAdvantage Secure Print هو حل ميسور التكلفة مصمم للشركات الصغيرة والمتوسطة التي تخزن مهام الطباعة في السحابة أو على مكتب المستخدم. فهو سهل الإعداد والاستخدام، مما يتيح للمستخدمين تحرير المهام من الأجهزة المحمولة ودعم الأجهزة من موردين متعددين.¹²
- HP JetAdvantage Private Print هو حل مجاني من HP يستند إلى سحابة يوفر ميزات الطباعة بالسحب دون تعقيد. فهو سهل الإعداد ولا يتطلب خادمًا أو التثبيت أو الصيانة.¹³

ممارسات أمان متقدمة

فرض الطباعة بالسحب لأي مهمة طباعة

HP Access Control Secure Pull Printing يساعد في حماية المعلومات السرية وتحسين أمان الجهاز وزيادة الكفاءة. فهذا الحل القوي المستند إلى خادم يقدم أشكالاً متعددة للمصادقة، بما في ذلك إصدار الشارات بالإضافة إلى ميزات أمان وإدارة بمستوى المؤسسات.

استخدم ميزات MICR أو العلامات المائية أو الميزات الأخرى لمنع النسخ أو التعديل

تتضمن حلول ردع التزييف HP and TROY استخدام مسحوق حبر آمن يلطخ الورق إذا تم تعريضه للعبث الكيميائي وإضافة علامات مائية للبيانات المتغيرة إلى الصفحات المطبوعة ودمج رموز قابلة للقراءة آليًا تتعقب المستندات الفردية وتراجعها. ويمكن أن تتضمن الطابعات متعددة المهام ميزات مكافحة للاحتيال تشمل توقعات مخصصة وشعارات الشركة وخطوط للأمان في المستندات الحساسة المطبوعة، مثل الوصفات الطبية أو شهادات الميلاد أو كشوف الدرجات.



اكتشاف المزيد

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

HP and TROY document protection
hp.com/go/HPandTROY



مراقبة بيئة الطباعة لديك وإدارتها

تساعدك حلول المراقبة والإدارة في التعرف على نقاط الضعف وتضع نهجًا موحدًا يستند إلى سياسة لحماية البيانات وخفض التكاليف والمحافظة على الامتثال.⁶ وبالتالي، يمكنك سد الثغرات والمساعدة في تجنب الغرامات المكلفة.

ممارسات الأمان الأساسية



اكتشاف المزيد

تحديث الأجهزة بأحدث برنامج ثابت/نظام تشغيل

استخدام HP Web Jetadmin¹⁴ لإجراء تحديثات البرامج الثابتة عبر الأسطول، مما يضمن تحديث الأجهزة بأحدث ميزات الحماية والأمان للأجهزة.

مراجعة سجلات أحداث الأمان للطابعات

ترسل أجهزة HP أحداث/إشعارات الطباعة إلى خادم سجل النظام بحيث يمكن لقسم تكنولوجيا المعلومات إصلاح المشاكل إذا لزم الأمر.

HP JetAdvantage Security Manager
hp.com/go/securitymanager

تقييم إعدادات الجهاز ومعالجتها

يمكن من إدارة إعدادات الأمان الأساسية للطباعة عبر الأسطول باستخدام HP Print Manageability Integration Kit (MIK) فهي عبارة عن مكون إضافي لنظام Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM هو حل إداري يستخدم على نطاق واسع لتخطيط الأجهزة الطرفية ونشرها وتكوينها ومراقبتها عن بُعد. ويمكن لمجموعة HP Print MIK اكتشاف أهم 15 إعدادًا للأمان وتقييمها ومعالجتها وإعداد تقارير بالنتائج.

للحصول على إدارة شاملة للأمان عبر الأسطول، اختر HP JetAdvantage Security Manager.⁹ فهذا الحل يساعدك في خفض التكاليف والموارد لوضع سياسة أمان شاملة على نطاق الأسطول وأتمتة معالجة إعدادات الجهاز وتثبيت الشهادات الفريدة وتجديدها مع الحصول على التقارير التي تحتاج إليها لإثبات الامتثال.

ممارسات أمان متقدمة

نشر برنامج SIEM لاكتشاف التهديدات وتوثيقها

يمكن إرسال بيانات الأحداث من أجهزة HP FutureSmart devices إلى أدوات الكشف عن الحوادث، مثل ArcSight و Splunk و SIEMonster للمراقبة في الوقت الحقيقي. ويمكن لنظام أمان تكنولوجيا المعلومات عرض الأجهزة الطرفية للطابعة بسهولة كجزء من النظام البيئي لتكنولوجيا المعلومات لاكتشاف تنبيهات الأمان للطابعة ومعالجتها.

تكوين أجهزة الطباعة الحديثة تلقائيًا عن إضافتها إلى الشبكة

تعمل ميزة "الحماية الفورية" Instant-on Security المضمنة مع HP JetAdvantage Security Manager على تكوين الأجهزة الحديثة تلقائيًا عندما تتم إضافتها إلى الشبكة أو بعد إعادة التشغيل.

إعداد تقارير لمراجعة الامتثال حول أمان أسطول الطباعة

استخدم HP JetAdvantage Security Manager لإنشاء تقارير إثبات الامتثال التي تثبت تطبيق سياسات الأمان على الطابعات وتأمين بيانات العملاء.



اكتشاف المزيد

HP JetAdvantage Security Manager
hp.com/go/securitymanager

انتهاك الامتثال قد يضر بأعمالك

العمل وتضرر السمعة والدعاوى القضائية. من الضروري نشر الأجهزة والحلول، مثل طابعات HP Enterprise و HP JetAdvantage Security Manager التي يمكن أن تساعدك في تلبية متطلبات الامتثال وحماية معلومات نشاطك التجاري من التهديدات الأمنية.

تخلق الأجهزة الطرفية غير المحمية أو التي لا تتمتع بحماية كافية مزيدًا من الفرص لجرائم الإنترنت. للمساعدة في التصدي للخطر المتزايد، تقوم الحكومات في مختلف أرجاء العالم بتطبيق لوائح أمنية صارمة تطالب الشركات بتحسين حماية معلومات العملاء.

وقد تتكبد الشركات غير الملتزمة تكاليف باهظة، بما في ذلك الغرامات وفقد



الحصول على المساعدة التي تحتاجها

من الآن لن تكون مضطراً إلى القيام بحماية شبكتك وتأمينها بمفردك. يمكن لفريق دعم من المستشارين توضيح كيفية تحسين أمان البيانات والخدمات والوثائق الخاصة بك.

تعاون مع خبراء أمان الطباعة لتقييم نقاط الضعف الحالية في أمان الطباعة لديك. إذ يمكننا مساعدتك في وضع سياسة أمان شاملة للطباعة تستند إلى احتياجات العمل وأفضل الممارسات وإعداد خطة للحصول على أمان محسن داخل بيئتك الفريدة.

معتزف به على أنه من رواد الصناعة

كانت شركة HP قح لقبية برائدة في أول تقرير لـ IDC MarketScape بعنوان Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment (التقرير [هنا](#)). أفاد التقرير بأن "الاتجاه التي تتخذه شركة HP Inc. تجاه الشؤون الأمنية تأخذ بعين الاعتبار جميع نواحي البنية الأساسية للطباعة والمستندات، بدءاً بقلل الجهاز توسعاً إلى جميع نواحي استخدام الجهاز وحماية المحتويات." الرسم الوارد هنا مأخوذ من تقييم الموردين IDC 2017 Vendor Assessment.¹⁵

تم تصميم نموذج تحليل الموردين IDC MarketScape لتقديم نظرة عامة حول اللياقة التنافسية لمزودي خدمات تقنية المعلومات والاتصالات (ICT) في أسواق معينة. تستخدم منهجية البحث منهجية تقييم دقيقة تستند إلى معايير نوعية وكمية على حد سواء، مما يوفر رسم بياني واحد لمكانة كل مورد في سوق معين. ويقيس مؤشر القدرات منتج المورد، والوصول إلى السوق، وتنفيذ الأعمال على المدى القصير. بنينا يقيس مؤشر الاستراتيجية مدى اتساق استراتيجيات المورد مع متطلبات العملاء في إطار زمني يتراوح بين 3 و 5 سنوات. يمثل حجم الرموز الحصة السوقية للمورد.¹⁵

بدء الاستخدام

اتصل بممثل المبيعات المخصص لك للحصول على مزيد من المعلومات حول ميزات الأمان والحلول والخدمات من HP التي يمكن أن تضعك على الطريق للحصول على حماية أفضل وراحة بال تامة.

تعرف على المزيد

hp.com/go/printsecurity

¹ يستند ادعاء "الطباعة الأكثر أمانًا" إلى مراجعة HP لميزات أمان الطابعات المنافسة من نفس الفئة HP المنشورة في عام 2017. تقدم شركة HP مجموعة من ميزات الأمان التي يمكنها مراقبة الهجمات واكتشافها وإيقافها تلقائيًا ثم التحقق الذاتي من سلامة البرامج عند إعادة التشغيل. للاطلاع على قائمة المنتجات، راجع hp.com/go/LJCompatibility.

² شركة InfoTrends، "تصميم الأجهزة والحلول"، بريندان مورس، أكتوبر 2016.

³ شركة Quocirca، "مشهد خدمات الطباعة المُدارة لعام 2016"، quocirca.com/content/managed-print-services-landscape-2016، يونيو 2016.

⁴ استطلاع للرأي أجرته شركة Spiceworks شارك فيه 309 من أصحاب القرار في مجال تكنولوجيا المعلومات في أمريكا الشمالية وأوروبا والشرق الأوسط وأفريقيا وآسيا والمحيط الهادئ نيابة عن HP في نوفمبر 2016.

⁵ شركة Quocirca، "أمان الطباعة: ضرورة في عصر إنترنت الأشياء"، quocirca.com/content/print-security-imperative-iot-era، يناير 2017.

⁶ قد تكون الحلول غير مدعومة في جميع أجهزة HP؛ قد تتطلب الحلول عملية شراء إضافية.

⁷ تتوفر ميزات الأمان المضمنة الأكثر تطورًا من HP في أجهزة HP من فئة Enterprise التي تتضمن البرنامج الثابت FutureSmart إصدار 4.5 أو الأحدث والتي تستند إلى ميزات الأمان المضمنة في طابعات HP من نفس الفئة المنشورة في مراجعة HP الصادرة بتاريخ 2017. إذ تقدم شركة HP مجموعة من ميزات الأمان لفحص السلامة بما في ذلك نظام BIOS المزود بقدرات الإصلاح الذاتي.

⁸ اختر أجهزة HP LaserJet Pro و HP PageWide Pro التي تحتوي على ميزات مضمّنة يمكنها اكتشاف الهجمات وإيقافها. للمزيد من المعلومات، يرجى زيارة hp.com/go/LJCompatibility.

⁹ يتعين شراء HP JetAdvantage Security Manager بشكل منفصل. لمعرفة المزيد، تفضل بزيارة hp.com/go/securitymanager.

¹⁰ تلزم كلمة مرور إضافية عند إرسال المعلومات إلى مستودع محمي بكلمة مرور.

¹¹ يعمل HP JetAdvantage Connect مع الأجهزة المحمولة الرائدة. ويتعين تثبيت مكون إضافي مرة واحدة للأجهزة التي تعمل بنظام تشغيل Android™ و Google Chrome™ و Microsoft®. للحصول على قائمة كاملة بأنظمة التشغيل المدعومة، راجع hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: تعمل الطباعة بطريقة السحب باستخدام أي طابعة عادية أو متعددة المهام متصلة بالشبكة. تتوفر المصادقة على الجهاز للعديد من أجهزة HP LaserJet و HP PageWide و OfficeJet Pro وأجهزة مختارة من شركات أخرى غير HP. قد تحتاج بعض الأجهزة إلى ترقية البرنامج الثابت. يلزم اتصال بالإنترنت للتخزين السحابي أو استرداد مهام الطباعة. يتطلب إصدار مهام الطباعة من جهاز محمول اتصال إنترنت ورمز QR للاستجابة السريعة. للحصول على مزيد من المعلومات وقائمة بالطابعات العادية ومتعددة المهام المدعومة، راجع hp.com/go/JetAdvantageSecurePrint.

¹³ يتوفر حل HP JetAdvantage Private Print مجانًا ويتطلب توصيل الطابعة بالإنترنت مع تمكين خدمات الويب. لا يتوفر في جميع الدول. تعرف على المزيد من الموقع hp.com/go/JetAdvantagePrivatePrint.

¹⁴ يمكن تنزيل برنامج HP Web Jetadmin مجانًا من موقع hp.com/go/webjetadmin.

¹⁵ استنادًا إلى مراجعة مؤسسة IDC لموردي خدمات الطباعة والآراء بخصوص ريادة شركة HP: "تتميز شركة HP Inc. عن غيرها نظرًا لخدماتها وقدراتها القوية في مجال تكنولوجيا المعلومات...وتوفير استراتيجية أمان شاملة ومتكاملة عبر بنية تكنولوجيا المعلومات بأكملها." المصدر: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, October 2017, IDC Doc #US41988517, by Allison Correia and Robert Palmer.

*قد يختلف توفر حلول الطباعة حسب الدولة.



المشاركة مع الزملاء

التسجيل للحصول على التحديثات

hp.com/go/getupdated



© Copyright 2014-2018 HP Development Company, L.P. المعلومات الواردة بهذه الوثيقة عرضة للتغيير دون إشعار. وتقتصر الضمانات الوحيدة لمنتجات HP وخدماتها على تلك المعلن عنها ضمن بنود بيان الضمان الصريح المرفق مع مثل هذه المنتجات والخدمات. ولا يوجد هنا ما يمكن تفسيره على أنه يشكل ضمانًا إضافيًا. ولا تتحمل شركة HP مسؤولية أي أخطاء فنية أو تحريرية أو أي حذف بهذه الوثيقة.

تُعد Google Chrome و Android علامتين تجاريتين مسجلتين لشركة Google Inc. وتُعد Microsoft علامة تجارية مسجلة لمجموعة شركات Microsoft.

4AA3-1295ARE، يناير 2018، مراجعة 11