



Schützen Sie Ihr Netzwerk mit der weltweit höchsten Drucksicherheit¹

94 %

der Finanzunternehmen stufen die Sicherheit von Kopierern/Druckern als wichtig oder sehr wichtig ein.²



61 %

der Unternehmen berichten von mindestens einer druckerspezifischen Datenschutzverletzung im letzten Jahr.³



43 %

der Unternehmen nehmen Drucker nicht in ihre Sicherheitsvorkehrungen für Endpunkten auf.⁴





Nur 18 % der Unternehmen überwachen Drucker im Hinblick auf Sicherheitsbedrohungen.⁴ Gehört Ihr Unternehmen dazu?

Versteckte Risiken erkennen

Die IT ist ständig damit beschäftigt, vertrauliche Informationen wie Mitarbeiter- und Kundendaten über verschiedene Geräte und Umgebungen hinweg zu schützen. Viele IT-Abteilungen haben mittlerweile strenge Sicherheitsmaßnahmen durchgesetzt, um einzelne Computer und das Netzwerk zu schützen. Dennoch werden Druck- und Bildverarbeitungsgeräte, wie z. B. Multifunktionsdrucker, häufig außer Acht gelassen und stellen daher ein Sicherheitsrisiko dar. Ungeschützte Geräte können aber dazu führen, dass das gesamte Netzwerk einem Cyberangriff zum Opfer fällt.

Potenzielle Kosten

Schon ein einziger Sicherheitsverstoß kann sehr kostspielig werden. Wenn die Vertraulichkeit von Daten aufgrund unsicherer Druck- und Bildverarbeitungsverfahren gefährdet wird, kann dies den Diebstahl von persönlichen Daten und Informationen über die Wettbewerbssituation, eine Schädigung des Markenimages oder des Unternehmensrufs und Rechtsstreitigkeiten nach sich ziehen. Verstöße gegen Vorschriften und gesetzliche Bestimmungen können zudem hohe Bußgelder verursachen.

HP kann Sie unterstützen

Schützen Sie Ihr Netzwerk mit der weltweit höchsten Drucksicherheit.¹ HP Drucker sorgen für kontinuierlichen Schutz, erkennen und stoppen Sicherheitsbedrohungen und stellen sich auf neue Bedrohungen ein. HP kann Ihrem Unternehmen mit einem breiten Spektrum an Lösungen dabei helfen, den Schutz von Geräten, Daten und Dokumenten zu automatisieren. Unsere Experten für die Drucksicherheit helfen Ihnen, eine umfassende Sicherheitsstrategie für Bildverarbeitungs- und Druckumgebungen zu entwickeln und zu implementieren.

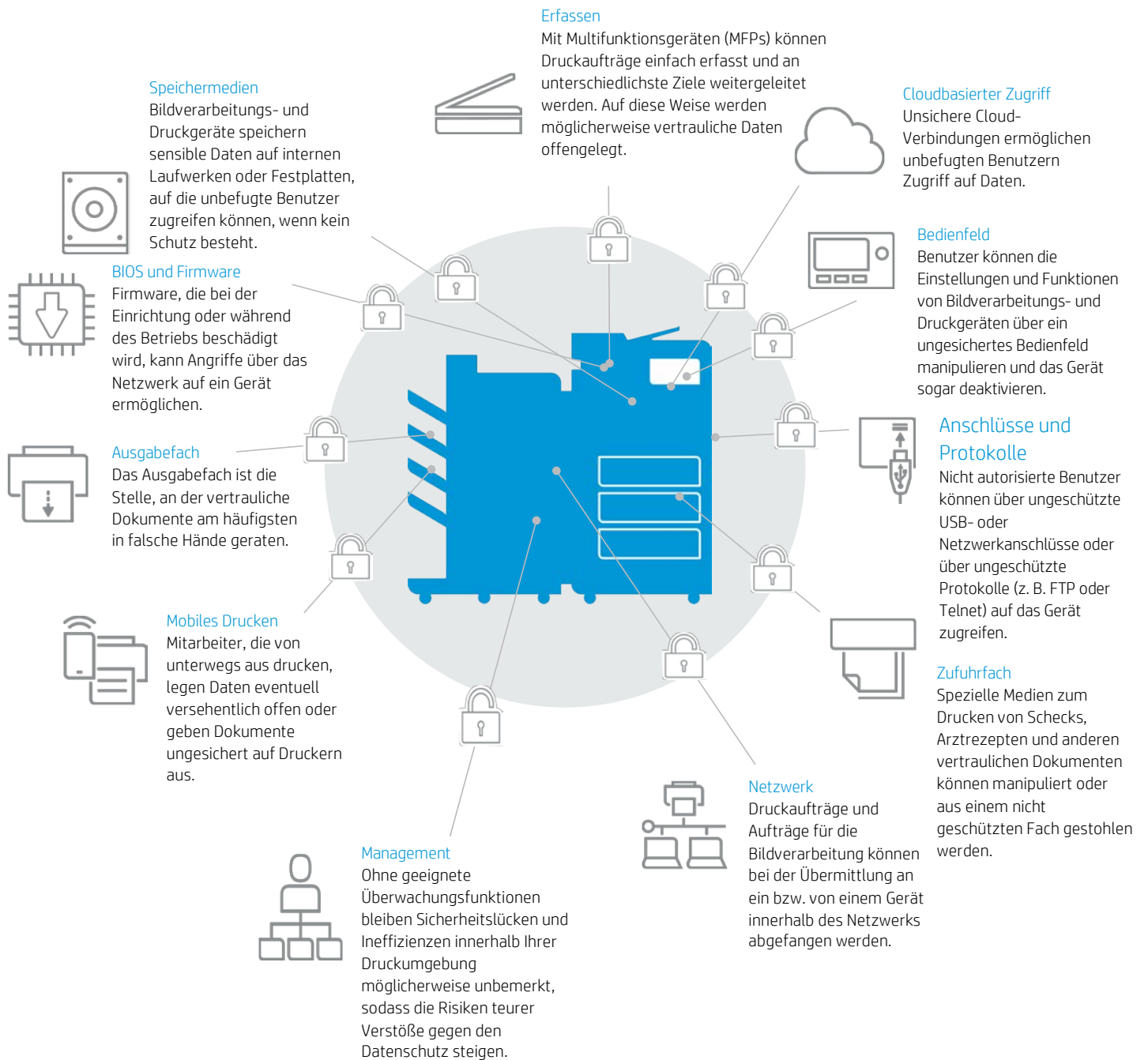
„HP investiert seit Langem in die Drucksicherheit und hat daher das umfangreichste und differenzierteste Portfolio an Sicherheitslösungen und -services auf dem Markt.“

– Quocirca, Januar 2017⁵

Schutz Ihrer Geräte, Daten und Dokumente

Kritische Sicherheitslücken können an verschiedenen Stellen Ihrer Bildverarbeitungs- und Druckumgebung auftreten. Wenn Sie ein besseres Verständnis für diese Schwachstellen entwickeln, können Sie das Risiko besser minimieren.

Schwachstellen bei Bildverarbeitung und Druck





Geräte schützen



Weitere Informationen

HP Custom Recycling Services
hp.com/go/businessrecycling

HP Secure Managed Print Services
hp.com/go/securemps

HP Drucker wurden zur Verwendung in Kombination mit Lösungen für Sicherheitsüberwachung und -verwaltung entwickelt, um das Risiko zu minimieren, die Einhaltung von Vorschriften und Richtlinien zu verbessern und das gesamte Netzwerk zu schützen. (Nicht alle Funktionen und Lösungen sind auf jedem HP Gerät verfügbar.⁶⁾)

Grundlegende Sicherheitsmaßnahmen

Verschlüsselter Speicher mit sicherem Löschen

Vertrauliche Daten, die auf dem internen Laufwerk oder auf der Festplatte eines Geräts gespeichert sind, können offengelegt und gestohlen werden. Viele HP Geräte sind bei Lieferung bereits mit integrierten Verschlüsselungsfunktionen zum Schutz der Daten ausgestattet. Verwenden Sie die integrierten Funktionen Ihrer Geräte, wenn die gespeicherten Daten nicht mehr benötigt werden, um die Daten sicher zu überschreiben und vertrauliche Informationen sicher zu entfernen.

Sichere Entsorgung

HP Custom Recycling Services können sicherstellen, dass die Daten vollständig von den Festplatten gelöscht werden, bevor nicht mehr benötigte Produkte dem ordnungsgemäßen Recycling zugeführt werden.

Sicherer Druckerzugriff für Reparaturen

Die Kenntnis der Sicherheitsverfahren der Anbieter von Druckerwartungsleistungen trägt zum Schutz vertraulicher Daten bei. Entscheiden Sie sich für *HP Secure Managed Print Services (MPS)* oder HP Partner, um Unterstützung durch Experten zu erhalten.

Deaktivieren von nicht verwendeten Anschlüssen und Protokollen

Verringern Sie die Angriffsfläche durch eine ordnungsgemäße Gerätekonfiguration. Deaktivieren Sie physische Anschlüsse und unsichere Protokolle (z. B. FTP oder Telnet), um einem unberechtigten Zugriff oder einer unbefugten Nutzung vorzubeugen.

Administratorzugriff für Gerätesteuerung

Legen Sie Administrator Kennwörter fest, damit ausschließlich IT-Mitarbeiter oder andere autorisierte Mitarbeiter Geräteeinstellungen einrichten und konfigurieren.

Whitelisting des Firmware-Codes

Auf der nächsten Seite wird erläutert, wie Sie Ihre Geräteflotte mit Whitelisting vor Malware schützen können.

Erweiterte Sicherheitsmaßnahmen

Common Criteria-Zertifizierung

HP Business-Drucker sind als Geräte zertifiziert, die mit international anerkannten Sicherheitsstandards wie Common Criteria Certification (CCC) und FIPS 140 konform sind. Durch die Überprüfung der Codesignierung bei Firmware-Updates Ihrer Geräte werden die Authentizität und Integrität des Codes bestätigt und die Einhaltung von Richtlinien sichergestellt.

Drucksicherheitsfunktionen für die automatische Erkennung und Abwehr von Angriffen

HP Business-Drucker beinhalten Sicherheitsfunktionen, über die die Geräte davor geschützt sind, zum Einfallstor für Angriffe auf das Netzwerk zu werden. Nur die Druckersicherheit von HP bietet Erkennung in Echtzeit, automatisierte Überwachung und integrierte Softwarevalidierung, um Bedrohungen gleich zu Beginn abzuwehren.⁷

HP Business-Drucker, von den Pro-⁸ bis zu den Enterprise-Modellen,⁷ sorgen für kontinuierlichen Schutz und erkennen und stoppen Sicherheitsbedrohungen in allen Phasen des Betriebs:

- **In der Startphase.** Der Boot-Code (bei Pro-Geräten) oder das BIOS (bei Enterprise-Geräten) ist ein Satz von Bootanweisungen zum Laden kritischer Hardwarekomponenten und zum Starten der Firmware. Die Integrität des Codes wird bei jedem Startvorgang geprüft, was zum Schutz des Geräts vor Angriffen beiträgt.
- **Beim Laden der Firmware.** *Whitelisting* überprüft die Firmware automatisch beim Systemstart, um festzustellen, ob es sich um authentischen Code handelt, der von HP digital unterzeichnet wurde. Wenn eine Unregelmäßigkeit festgestellt wird, startet das Gerät neu in einem sicheren Offline-Modus und sendet eine Benachrichtigung an die IT.
- **Während des Betriebs.** Integrierte Funktionen von HP unterstützen beim Schutz des Gerätespeichers, wenn sie eingeschaltet und mit einem Netzwerk verbunden sind – dann, wenn die meisten Angriffe auftreten. Bei einem Angriff fährt das Gerät herunter.

HP Enterprise-Geräte mit automatischer Fehlerbehebung

HP Enterprise-Drucker sind nicht nur in der Lage, Sicherheitsbedrohungen zu erkennen und zu stoppen, sondern auch Fehler nach Angriffen automatisch zu beheben. Die IT muss daher nicht eingreifen.⁷ Diese Funktionen leiten bei einem Angriff oder einer Unregelmäßigkeit automatisch einen Neustart ein. Die Administratoren werden über SIEM-Tools (Security Information and Event Management) wie ArcSight, Splunk und SIEMonster informiert.

- *HP Sure Start* ist das branchenweit einzige BIOS mit automatischer Fehlerbehebung.⁷ Wenn das BIOS beschädigt ist, wird das Gerät über HP Sure Start mit einer sicheren „Golden Copy“ des BIOS neu gestartet.
- Die *Angriffserkennung im laufenden Betrieb (HP run-time intrusion detection)* überwacht komplexe Firmware- und Speicherprozesse, stoppt den Angriff automatisch und startet das Gerät im Falle eines Angriffs neu.
- *HP Connection Inspector* analysiert abgehende Netzwerkverbindungen, um festzustellen, welche Vorgänge normal sind, verdächtige Anfragen zu stoppen und Malware durch einen automatischen Neustart mit automatischer Fehlerbehebung zu bekämpfen.

Dank des Investitionsschutzes der erweiterbaren HP FutureSmart-Firmware lassen sich viele vorhandene HP Enterprise-Drucker um *Whitelisting*, *Angriffserkennung im laufenden Betrieb (HP run-time intrusion detection)* und *HP Connection Inspector* ergänzen.⁷

HP JetAdvantage Security Manager schließt den Prüfungszyklus ab.

Nach einem Neustart – und nach jedem Hinzufügen eines neuen Geräts zum Netzwerk – korrigiert *HP JetAdvantage Security Manager* automatisch die Sicherheitseinstellungen des Geräts, um die Einhaltung vorgegebener Unternehmensrichtlinien sicherzustellen.⁹ Ein Eingreifen seitens der IT ist nicht erforderlich.



Weitere Informationen

Integrierte Funktionen zur Drucksicherheit:

- HP Sure Start (BIOS-Integrität)
 - Whitelisting des Firmware-Codes
 - Angriffserkennung im laufenden Betrieb (HP run-time intrusion detection)
 - HP Connection Inspector
- hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:
hp.com/go/securitymanager

Die Funktionsweise dieses Systems:

Die integrierten Sicherheitsfunktionen umfassen die vier wichtigsten Schritte des HP Gerätezyklus.

Im Fall eines Angriffs können HP Enterprise-Geräte neu starten, und es kann eine automatische Fehlerbehebung erfolgen.

HP JetAdvantage Security Manager schließt den Prüfungszyklus ab.

4. Durchgehende Überwachung

Schutz von Prozessen und Abwehr von Angriffen während des Gerätebetriebs
Überprüft abgehende Netzwerkverbindungen, um verdächtige Anfragen zu stoppen (nur Enterprise-Geräte).

3. Überprüfen der Einstellungen

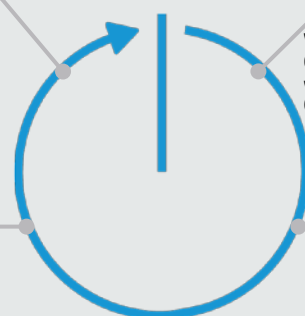
HP JetAdvantage Security Manager prüft und korrigiert nach einem Neustart die betroffenen Sicherheitseinstellungen.

1. Überprüfung des BIOS/Boot-Codes

Verhindert die Ausführung von schädlichem Code beim Booten, indem sichergestellt wird, dass nur von HP signierter Originalcode geladen wird.

2. Überprüfen der Firmware

Lässt nur das Laden von authentischer, einwandfreier Firmware zu, die von HP digital signiert wurde.





Daten schützen

Daten müssen ununterbrochen geschützt werden – nach dem Speichern ebenso wie während der Übertragung. Im Folgenden sind einige wichtige Schritte aufgeführt, um eine sichere Übermittlung und Nutzung zu gewährleisten.⁶

Grundlegende Sicherheitsmaßnahmen



Weitere Informationen

HP Web Jetadmin
hp.com/go/wja

HP Universal Print Driver (UPD) mit Secure Encrypted Print
hp.com/go/upd

HP JetAdvantage Workflow-Lösungen
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

802.1x- oder IPsec-Netzwerkstandards

Verwenden Sie verschlüsselte Netzwerkstandards, um im Netzwerk übertragene Daten zwischen dem Gerät und Verwaltungstools wie *HP Web Jetadmin* oder *HP Embedded Web Server* zu schützen.

Verschlüsselung von Daten bei der Übertragung

Schützen Sie Druckaufträge, die an das Gerät übertragen werden, mit Verschlüsselungen (z. B. Internet Print Protocol over TLS (IPPS)). *HP Universal Print Driver Secure Encrypted Print* bietet echte, symmetrische AES256-Verschlüsselung und -Entschlüsselung für Druckaufträge vom Client bis zur Dokumentseite. Die Verschlüsselung basiert auf einem benutzerdefinierten Kennwort und verwendet die validierten FIPS 140-Kryptographiebibliotheken von Microsoft®.

HP JetAdvantage Workflow-Lösungen schützen vertrauliche Informationen und verbessern die Effizienz beim Scannen. Beispielsweise verbessert die nahtlose Integration von *HP Capture and Route* und *HP Access Control* die Sicherheit und bietet den Komfort einer einmaligen Authentifizierung sowie die Möglichkeit, Inhalte zum Zwecke der Information Governance zu überwachen.¹⁰

Verschlüsselung von Daten im Ruhezustand

Schützen Sie vertrauliche Geschäftsinformationen, die auf dem Festplattenlaufwerk gespeichert sind, mit integrierten Verschlüsselungsfunktionen. Verbessern Sie den Schutz verschlüsselter Zugangsdaten und der Daten auf einem Gerät mit einem optionalen HP Trusted Platform Module (TPM). Dazu werden die Schlüssel zur Geräteverschlüsselung automatisch auf dem TPM versiegelt. Das TPM stellt eine sichere Geräteidentität bereit, indem private Zertifikatsschlüssel generiert und geschützt werden.

Firewall-Schutz

Schützen Sie Ihr Netzwerk vor Malware und Viren, indem Sie den Zugriff auf Drucker, auf PCs und Server aus Ihrem Netzwerk beschränken.

Native Benutzerauthentifizierung

Verringern Sie Kosten und Sicherheitsrisiken, indem Sie festlegen, dass sich Benutzer mit PIN/PIC-, LDAP- oder Kerberos-Authentifizierung anmelden müssen. Diese Verfahren lassen sich auch in Active Directory integrieren.

Rollenbasierte Zugriffssteuerung

HP Access Control Rights Management trägt durch die Einschränkung der Druckerfunktionen zur Senkung von Kosten und Sicherheitsrisiken bei. Mithilfe einer rollenbasierten Zugriffssteuerung können Sie verschiedenen Benutzern oder ganzen Abteilungen je nach ihren Anforderungen unterschiedliche Berechtigungen erteilen. Beispielsweise können Sie den Kreis der Benutzer eingrenzen, die zum Faxen, zum Scannen an E-Mail oder zum Scannen an Fax berechtigt sind.



Weitere Informationen

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Erweiterte Sicherheitsmaßnahmen

Erweiterte Authentifizierung und Überwachung

Führen Sie erweiterte Authentifizierungs- und Überwachungslösungen ein (z. B. Kennwörter, Transponderkarten, Smart Cards oder biometrische Funktionen), um ein höheres Maß an Sicherheit und Kontrolle zu erreichen.

- *HP Access Control Secure Authentication* stellt die Kontrolle wieder her, erhöht die Sicherheit und verringert Kosten. Sie profitieren von einer Vielzahl erweiterter Kontrollen und Optionen, z. B. Touch-Authentifizierung bei NFC-fähigen mobilen Geräten.
- *HP Access Control Job Accounting* ermöglicht die genaue Verfolgung und Erfassung von Daten, die Analyse der Ergebnisse und das anschließende Erstellen und Senden von Berichten. Nutzen Sie analysierte Daten, um Druckkosten zuzuordnen, die Mitarbeiter für intelligenteres Drucken zu motivieren und der IT die notwendigen Informationen für bessere flottenweite Prognosen bereitzustellen.

Mobile Geräte werden beim Netzwerkzugriff berücksichtigt

Setzen Sie Ihre mobilen Geräte als Teil Ihrer allgemeinen Richtlinie zur Druckersicherheit ein, um den Zugriff auf die Drucker zu steuern. HP bietet serverbasierte Lösungen, die sicheres Pull-Printing ermöglichen sowie erweiterte Verwaltungs- und Berichterstellungsfunktionen umfassen.

- *HP JetAdvantage Connect* bietet intuitive und zuverlässige mobile Drucklösungen für Unternehmen. Nutzen Sie vorhandene IT-Netzwerktools, um Zeit und Geld zu sparen.¹¹ Nutzer können über eine Reihe von Smartphones und Tablets sicher drucken – wo und wann sie es benötigen – fast wie über einen PC.
- *HP Access Control* umfasst Funktionen für mobiles Drucken. Es nutzt die vorhandene E-Mail-Infrastruktur. Mobile Benutzer können Druckaufträge per E-Mail an die Druckwarteschlange senden und dann die Dokumente von jedem Drucker oder MFP abrufen, auf dem diese Lösung aktiviert ist. Schützen Sie Druckgeräte im Netzwerk mit sicheren Authentifizierungsfunktionen einschließlich Mobile Release.

Beseitigen Sie Datenlecks vor deren Auftreten

HP Lösungen beinhalten Funktionen zum Schutz vor Datenverlusten. Mit *HP Capture and Route Data Loss Prevention* können Sie verhindern, dass vertrauliche Informationen gescannt oder gefaxt werden. Mit *HP Access Control Print Data Loss Prevention* können Sie verhindern, dass vertrauliche Dokumente gedruckt werden. Verfolgen Sie Ihre wichtigsten Daten bis ins Detail, um Sicherheitsverletzungen zu verhindern oder diesen vorzubeugen, ohne die Abläufe im Unternehmen zu verlangsamen. Definieren Sie die Ausgabe von Sicherheitshinweisen auf der Basis der von Ihnen gewählten Bedingungen.

Anwendung von digitalen Zertifikaten bei Druckern

Erhöhen Sie die Sicherheit in der Druckumgebung mithilfe von digitalen Zertifikaten für Netzwerkdrucker und MFPs. Sparen Sie Zeit, indem Sie HP JetAdvantage Security Manager zur automatischen Installation und Verlängerung von Zertifikaten verwenden.⁹



Dokumente schützen

Nehmen Sie intelligente Hardware- und Softwarelösungen in Ihren IT-Sicherheitsrahmenplan auf, um vertrauliche Informationen in gedruckten Dokumenten zu schützen.⁶

Grundlegende Sicherheitsmaßnahmen

Zugriff auf vorgedruckte Formulare kontrollieren

Rüsten Sie Ihre Drucker und MFPs mit verschließbaren Zufuhrfächern aus, um den Diebstahl von speziellen Medien zu verhindern, die zum Drucken von Schecks, Arztrezepten oder anderen vertraulichen Dokumenten verwendet werden.

Optionales Drucken mit PIN oder Pull-Printing für vertrauliche Inhalte

Benutzer können sich für PIN-Druck oder Pull-Printing entscheiden und sind somit nicht mehr auf Einzelplatzrechner angewiesen. Des Weiteren wird die Gefahr verringert, dass Druckaufträge in falsche Hände gelangen. Mit diesen Sicherheitsmaßnahmen wird zudem vermieden, dass Dokumente gedruckt und nicht am Drucker abgeholt werden. So lassen sich sowohl die Kosten als auch das Abfallvolumen reduzieren.

Beim PIN-Druck ordnen die Benutzer bei der Übertragung vertraulicher Druckaufträge eine PIN zu, die sie am Gerät eingeben müssen, um den Druckauftrag freizugeben.

Beim Pull-Printing werden Druckaufträge in der Cloud oder auf dem PC des Benutzers gespeichert. Benutzer authentifizieren sich am Drucker ihrer Wahl, um ihre Druckaufträge abzurufen und zu drucken. HP bietet zwei cloudbasierte Pull-Printing-Lösungen:

- *HP JetAdvantage Secure Print* ist eine kostengünstige Lösung für kleine und mittelständische Unternehmen, mit der Druckaufträge in der Cloud oder auf dem Desktop des Benutzers gespeichert werden. Die einfach einzurichtende und zu verwendende Lösung ermöglicht Benutzern, Druckaufträge von mobilen Geräten aus freizugeben, und unterstützt Geräte verschiedener Anbieter.¹²
- *HP JetAdvantage Private Print* ist die kostenlose cloudbasierte Lösung von HP. Sie ist alles andere als komplex und bietet alle Vorteile des Pull-Printing. Die Lösung lässt sich einfach einrichten und erfordert weder Server noch Installation oder Wartung.¹³

Erweiterte Sicherheitsmaßnahmen

Obligatorisches Pull-Printing für alle Druckaufträge

HP Access Control Secure Pull Printing schützt vertrauliche Informationen, verbessert die Gerätesicherheit und erhöht die Effizienz. Diese zuverlässige serverbasierte Lösung bietet verschiedene Authentifizierungsformen wie die Freigabe per Ausweis sowie Funktionen für unternehmensweite Sicherheit und Verwaltung.

MICR, Wasserzeichen oder sonstige Mittel zur Verhinderung von Kopien oder Änderungen

Lösungen zur Bekämpfung von Fälschungen von HP und TROY umfassen einen speziellen Sicherheitstoner, der bei Veränderung der chemischen Eigenschaften zu Flecken auf dem Papier führt, Wasserzeichen mit variablen Daten auf Ausdrucken einbettet und maschinenlesbare Codes hinzufügt, anhand derer sich einzelne Dokumente nachverfolgen und prüfen lassen. Auf MFPs können Sie bei vertraulichen Ausdrucken (z. B. Arztrezepte, Geburtsurkunden oder Verhandlungsprotokolle) Funktionen zum Verhindern von Betrugsfällen einbinden. Dazu zählen u. a. kundenspezifische Signaturen, Unternehmenslogos und Sicherheits-Fonts.



Weitere Informationen

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Dokumentschutz von HP und TROY
hp.com/go/HPandTROY



Überwachung und Verwaltung Ihrer Druckumgebung



[Weitere Informationen](#)

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Mit Lösungen zum Überwachen und Verwalten der Sicherheit können Sie Schwachstellen erkennen und einen einheitlichen, richtlinienbasierten Ansatz etablieren, um Daten zu schützen, Risiken zu mindern und die Compliance sicherzustellen.⁶ Sie können damit Lücken beim Datenschutz beseitigen und hohe Bußgelder vermeiden.

Grundlegende Sicherheitsmaßnahmen

Aktualisierung der Geräte mit den neuesten Versionen von Firmware/Betriebssystem

Mit HP Web Jetadmin¹⁴ können Sie Firmware-Updates über die gesamte Geräteflotte verteilen und sicherstellen, dass die Geräte mit den neuesten Schutz- und Sicherheitsfunktionen ausgestattet sind.

Überprüfung der Sicherheitsereignisprotokolle der Drucker

HP Geräte senden Druckerereignisse/-mitteilungen an einen Syslog-Server, damit die IT bei Bedarf Fehler beheben kann.

Beurteilung von Geräteeinstellungen und Fehlerbehebung

Mit dem *HP Print Manageability Integration Kit (MIK)*, einem Plug-in für Microsoft® System Center Configuration Manager (SCCM), lassen sich die grundlegenden Sicherheitseinstellungen für die Druckerflotte verwalten. Microsoft SCCM ist eine häufig verwendete Managementlösung, um Endpunkte per Fernzugriff zu planen, zu implementieren, zu konfigurieren und zu überwachen. Mit dem HP Print MIK können Sie die 15 wichtigsten Sicherheitseinstellungen erkennen, beurteilen, korrigieren und die Ergebnisse dokumentieren.

Entscheiden Sie sich für *HP JetAdvantage Security Manager*, um ein umfassendes Sicherheitsmanagement für die gesamte Geräteflotte zu erreichen.⁹ Mit dieser Lösung können Sie die Kosten und die Zahl der erforderlichen Mitarbeiter verringern, um eine Sicherheitsrichtlinie für die gesamte Geräteflotte festzulegen, die Behebung von Gerätefehlern zu automatisieren, spezielle Zertifikate zu installieren und zu verlängern sowie die erforderlichen Berichte zu generieren, um die Einhaltung der Bestimmungen nachzuweisen.

Erweiterte Sicherheitsmaßnahmen



Weitere Informationen

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Implementierung von SIEM-Software zur Erkennung und Dokumentation von Bedrohungen

Ereignisdaten von HP FutureSmart-Geräten können an Tools zur Erkennung von Sicherheitsverstößen wie ArcSight, Splunk und SIEMONSTER zur Überwachung in Echtzeit gesendet werden. Die Abteilung für IT-Sicherheit kann die Druckerendpunkte als Teil des umfassenderen IT-Ökosystems auf einfache Weise darstellen und auf Warnungen zur Druckersicherheit reagieren.

Automatische Konfiguration von neuen Geräten beim Hinzufügen zum Netzwerk

Die Instant-on Security-Funktion, die im Lieferumfang von HP JetAdvantage Security Manager enthalten ist, konfiguriert neue Geräte automatisch, wenn diese im Netzwerk hinzugefügt werden, bzw. nach einem Neustart.

Compliance-Auditberichte zur Sicherheit in der Druckerflotte

Verwenden Sie HP JetAdvantage Security Manager für die Generierung von Berichten, die die Einhaltung von Bestimmungen nachweisen. Sie können damit die Anwendung von Sicherheitsrichtlinien auf Druckern und den Schutz von Kundendaten nachweisen.

Die Nichteinhaltung von Bestimmungen kann Ihrem Unternehmen schaden

Nicht oder schlecht geschützte Endpunkte bieten Cyberkriminellen weitere Ansatzpunkte. Um der wachsenden Bedrohung zu begegnen, implementieren Regierungsbehörden auf der ganzen Welt strenge Sicherheitsvorschriften, die Unternehmen dazu zwingen, Kundeninformationen besser zu schützen.

Unternehmen, die diese Vorschriften nicht einhalten, müssen hohe Kosten in Kauf nehmen, z. B. Bußgelder,

entgangene Umsätze, Imageverlust und Rechtsstreitigkeiten.

Es ist wichtig, Geräte und Lösungen wie HP Enterprise-Drucker und HP JetAdvantage Security Manager zu implementieren. Sie tragen dazu bei, Compliance-Anforderungen zu erfüllen und Geschäftsinformationen vor Sicherheitsbedrohungen zu schützen.



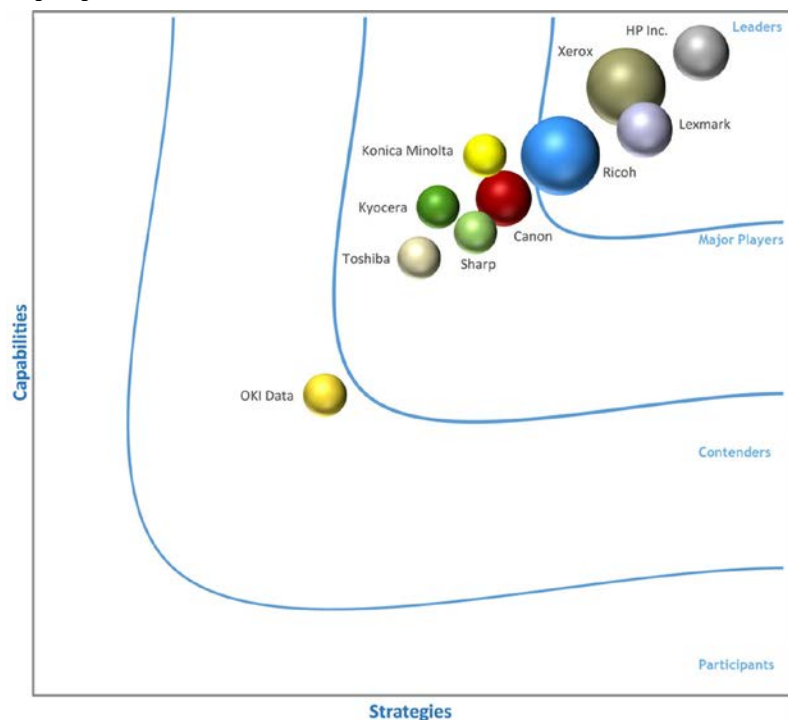
Hilfe, die Sie benötigen

Sie müssen Schutz und Sicherheit nicht selbst in die Hand nehmen. Ein Support-Team an Beratern unterstützt Sie dabei, die Sicherheit Ihrer Daten, Geräte und Dokumente zu erhöhen.

Arbeiten Sie mit Experten für Drucksicherheit zusammen, um aktuelle Sicherheitsschwachstellen in Ihrer Druckumgebung zu analysieren. Wir helfen Ihnen dabei, eine auf Best Practices basierende, umfassende Sicherheitsrichtlinie zu entwickeln, die die Anforderungen des Unternehmens berücksichtigt, und einen Plan zu erarbeiten, mit dem sich die Sicherheit in Ihrer individuellen Umgebung verbessern lässt.

Als in der Branche führend anerkannt

HP wurde im ersten IDC MarketScape Bericht „Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment“ als „Leader“ eingestuft. (Sie finden den Bericht [unter diesem Link](#).) Laut diesem Bericht „umfasst der Sicherheitsansatz von HP Inc. die gesamte Druck- und Dokumentinfrastruktur. Er beginnt beim Schutz der Geräte und erstreckt sich auf alle Aspekte bei der Gerätenutzung und dem Schutz von Inhalten“. Die hier gezeigte Grafik stammt aus „IDC 2017 Vendor Assessment“.¹⁵



Das IDC MarketScape-Anbieteranalysemodell soll einen Überblick über die Konkurrenzfähigkeit von ICT-Anbietern in einem bestimmten Markt geben. Dabei kommt eine konsequente Bewertungsmethodik zur Anwendung, die sowohl auf qualitativen als auch quantitativen Kriterien basiert. Dies führt letztendlich zu einer zentralen grafischen Darstellung der Position jedes Anbieters in einem bestimmten Markt. Beim Capabilities-Wert wird die kurzfristige Umsetzung von Faktoren wie Lieferantenprodukt, Go-to-Market und Business Execution gemessen. Beim Strategies-Wert wird die Ausrichtung von Lieferantenstrategien an den Kundenbedürfnissen in einem Zeitraum von 3 bis 5 Jahren gemessen. Der Marktanteil der Lieferanten wird durch die Größe der Symbole dargestellt.¹⁵

Einstieg

Wenden Sie sich an Ihren Vertriebsbeauftragten, um weitere Informationen zu HP Sicherheitsfunktionen, -lösungen und -services zu erhalten, die Ihnen den Weg ebnen, um für mehr Schutz und eine höhere Zuverlässigkeit zu sorgen.

Weitere Informationen

hp.com/go/printsecurity

¹ Die Aussage „höchste Drucksicherheit“ basiert auf einer von HP durchgeführten Prüfung der 2017 veröffentlichten Angaben zu Sicherheitsfunktionen von vergleichbaren Druckern von Wettbewerbern. Nur HP bietet eine Kombination aus Sicherheitsfunktionen, die durch Überwachung einen Angriff erkennen und automatisch stoppen und danach bei einem Neustart die Integrität der Software eigenständig prüfen können. Eine Liste der Drucker finden Sie hier: hp.com/go/PrintersThatProtect. Weitere Informationen: hp.com/go/printersecurityclaims.

² InfoTrends, „Designing Hardware & Solutions“, Brendan Morse, Oktober 2016.

³ Quocirca, „Managed Print Services Landscape, 2016“, quocirca.com/content/managed-print-services-landscape-2016, Juli 2016.

⁴ Spiceworks Befragung von 309 IT-Entscheidungssträgern in Nordamerika, EMEA und APAC im Auftrag von HP, November 2016.

⁵ Quocirca, „Print security: An imperative in the IoT era“, quocirca.com/content/print-security-imperative-iot-era, Januar 2017.

⁶ Die Lösungen werden möglicherweise nicht von allen HP Geräten unterstützt. Einige Lösungen erfordern den Erwerb zusätzlicher Optionen.

⁷ Die innovativsten integrierten Sicherheitsfunktionen von HP sind bei Geräten der HP Enterprise-Klasse mit FutureSmart Firmware 4.5 oder höher verfügbar. Zu diesem Ergebnis kommt eine von HP durchgeführte Prüfung der 2017 veröffentlichten Angaben zu integrierten Sicherheitsfunktionen von vergleichbaren Druckern anderer Wettbewerber. Nur HP bietet eine Kombination aus Sicherheitsfunktionen für Integritätsprüfungen, die selbst das BIOS einschließen und Technologien zur automatischen Fehlerbehebung umfassen. Eine Liste der kompatiblen Produkte finden Sie unter hp.com/go/PrintersThatProtect. Weitere Informationen finden Sie unter hp.com/go/printersecurityclaims.

⁸ Ausgewählte HP LaserJet Pro- und PageWide Pro-Geräte verfügen über integrierte Funktionen, die Hackerangriffe erkennen und stoppen. Weitere Informationen finden Sie unter hp.com/go/PrintersThatProtect.

⁹ HP JetAdvantage Security Manager muss separat erworben werden. Weitere Informationen finden Sie unter hp.com/go/securitymanager.

¹⁰ Wenn Sie Informationen an ein kennwortgeschütztes Endrepository senden, wird ein zusätzliches Kennwort benötigt.

¹¹ HP JetAdvantage Connect kann mit den führenden mobilen Geräten verwendet werden. Für Geräte unter den Betriebssystemen Android™, Google Chrome™ und Microsoft® ist die einmalige Installation eines Plug-ins erforderlich. Weitere Einzelheiten und eine Liste der unterstützten Betriebssysteme finden Sie unter hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Pull-Printing funktioniert mit Druckern oder MFPs, die mit einem Netzwerk verbunden sind. Die Authentifizierung am Gerät ist bei vielen HP LaserJet-, PageWide- und OfficeJet Pro-Geräten sowie bei bestimmten Geräten anderer Anbieter möglich. Bei einigen Geräten ist ggf. ein Firmware-Upgrade erforderlich. Zum Abrufen von Druckaufträgen und zum Speichern von Aufträgen in der Cloud wird eine Internetverbindung benötigt. Für die Freigabe von Druckaufträgen über ein mobiles Gerät werden eine Netzwerkverbindung und ein QR-Code benötigt. Weitere Informationen und eine Liste der unterstützten Drucker und MFPs finden Sie unter hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print ist ohne Zusatzkosten verfügbar, der Drucker muss mit dem Internet verbunden und die Web-Services müssen aktiviert sein. Nicht in allen Ländern verfügbar. Weitere Informationen finden Sie unter hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin kann ohne zusätzliche Kosten unter hp.com/go/webjetadmin heruntergeladen werden.

¹⁵ Basierend auf der IDC-Bewertung von Druckdienstleistern und der Meinung über die führende Position von HP: „HP hat durch sein umfassendes Spektrum an IT-Services und -Leistungen einen Vorteil ... und ermöglicht dadurch eine umfassende und integrierte Sicherheitsstrategie über die gesamte IT-Infrastruktur hinweg“. QUELLE: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, von Allison Correia und Robert Palmer, Oktober 2017, IDC-Dokument Nummer US41988517.

Melden Sie sich noch heute an.

hp.com/go/getupdated



An Kollegen weiterleiten

© Copyright 2014-2018 HP Development Company, L.P. Die enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Die Garantien für HP Produkte und Services werden ausschließlich in der entsprechenden, zum Produkt oder Service gehörigen Garantieerklärung beschrieben. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. HP haftet nicht für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen.

Android und Google Chrome sind eingetragene Marken von Google Inc. Microsoft ist eine in den USA eingetragene Marke der Microsoft-Unternehmensgruppe.

4AA3-1295DEE, Januar 2018, Rev. 11

