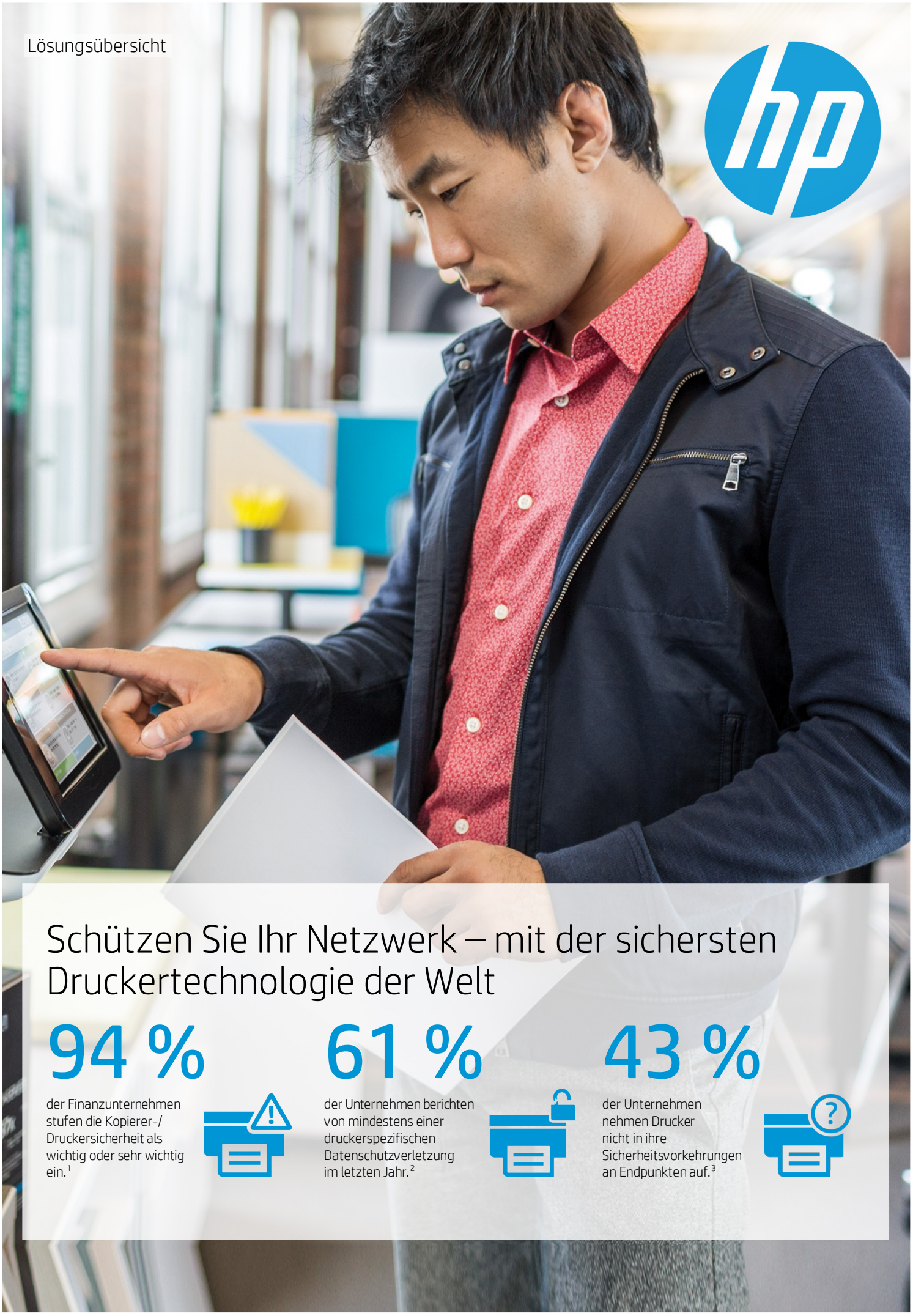
Lösungsübersicht



# Schützen Sie Ihr Netzwerk – mit der sichersten Druckertechnologie der Welt

**94 %**

der Finanzunternehmen stufen die Kopierer-/Druckersicherheit als wichtig oder sehr wichtig ein.[1]

**61 %**

der Unternehmen berichten von mindestens einer druckerspezifischen Datenschutzverletzung im letzten Jahr.[2]

**43 %**

der Unternehmen nehmen Drucker nicht in ihre Sicherheitsvorkehrungen an Endpunkten auf.[3]

# Nur 18 % der Unternehmen überwachen Drucker auf Bedrohungen.[3] Wie sicher sind die Drucker in Ihrem Unternehmen?

## Erkennen Sie versteckte Risiken

Die IT ist ständig damit beschäftigt, vertrauliche Informationen wie Mitarbeiter- und Kundendaten über verschiedene Geräte und Umgebungen hinweg zu schützen. Auch wenn viele IT-Abteilungen mittlerweile strenge Sicherheitsmaßnahmen durchgesetzt haben, um einzelne Computer und das Netzwerk zu schützen, fallen die Druck- und Bildbearbeitungsgeräte oft durch das Raster und stellen so ein Sicherheitsrisiko dar. Ungesicherte Geräte ermöglichen es den Angreifern, Cyberattacken auf das gesamte Netzwerk zu starten.

## Erfassen Sie potenzielle Kosten

Schon ein einziger Sicherheitsverstoß kann sehr kostspielig werden. Wenn die Vertraulichkeit von Daten aufgrund ungesicherter Druck- und Bildverarbeitungstechnologien gefährdet wird, kann dies den Diebstahl von Identitäten, wettbewerbsrelevanten Informationen, eine Schädigung des Markenimages oder des Rufs und Rechtsstreitigkeiten nach sich ziehen. Zudem kann die Nichteinhaltung von gesetzlichen und Compliance-Vorgaben zu erheblichen Kosten führen.

## HP kann Sie unterstützen

Schützen Sie Ihr Netzwerk mit der sichersten Druckertechnologie der Welt[5] – einschließlich Geräten, die Angriffe erkennen und automatisch unterbinden können. HP kann Ihnen mit einem breit gefächerten Lösungsportfolio helfen, den Schutz für Geräte, Daten und Dokumente zu automatisieren. Unsere Experten für Drucksicherheit unterstützen Sie bei der Entwicklung und Implementierung einer umfassenden Sicherheitsstrategie für Bildverarbeitungs- und Druckumgebungen.

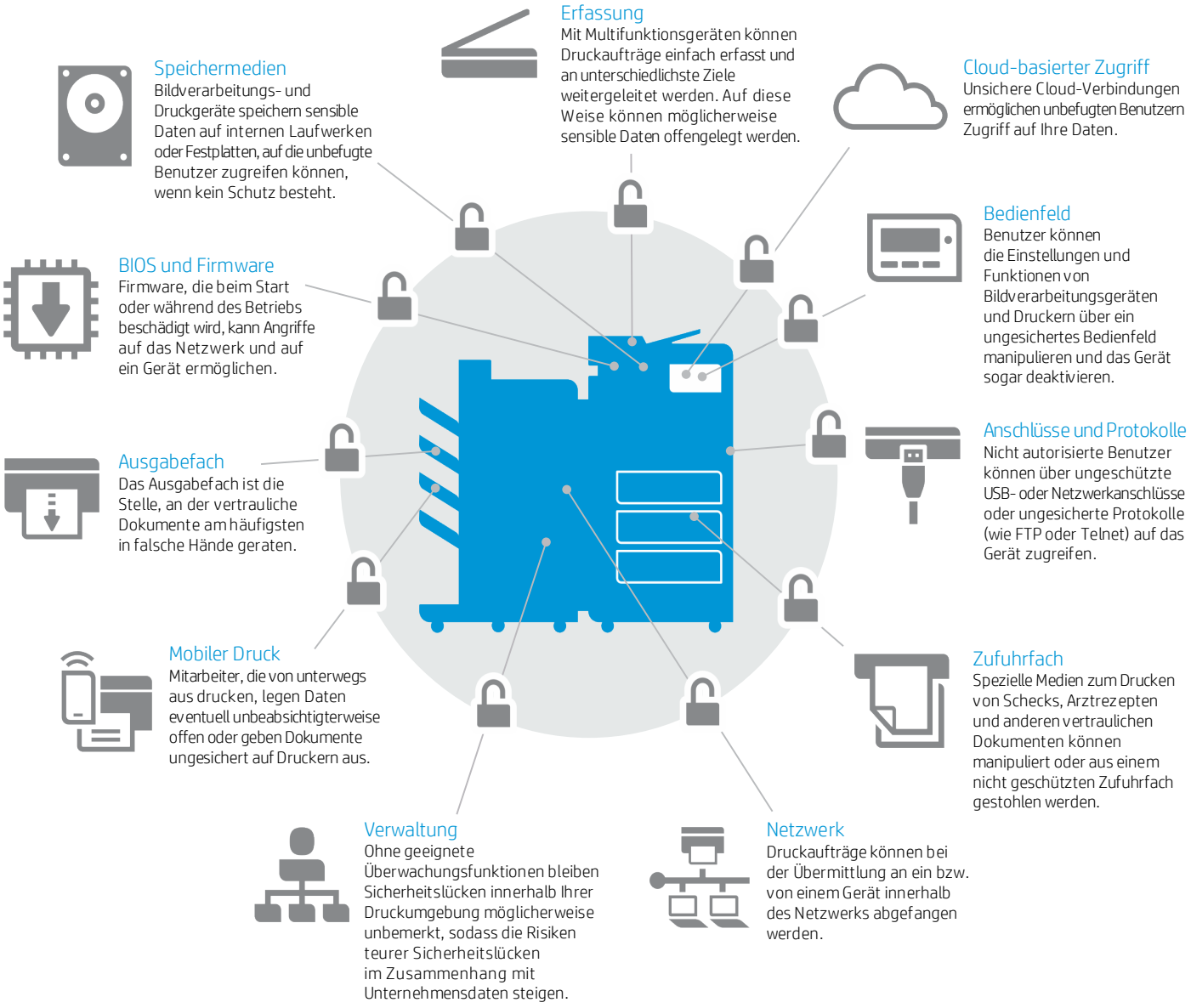
*„HP investiert seit Langem in die Drucksicherheit und hat daher das umfangreichste und differenzierteste Portfolio an Sicherheitslösungen und -services auf dem Markt.“*

– Quocirca, Januar 2017[4]

# Schützen Sie Ihre Geräte, Daten und Dokumente

Kritische Sicherheitslücken können an verschiedenen Stellen innerhalb Ihrer Umgebung auftreten. Indem Sie eine bessere Kenntnis dieser Schwachstellen erlangen, können Sie das Risiko leichter minimieren.

## Schwachstellen in Bildverarbeitungs- und Druckumgebungen



# Schutz für Geräte

HP Drucker wurden zur Verwendung in Kombination mit Sicherheitsüberwachungs- und -verwaltungslösungen entwickelt, um Risiken zu minimieren, die Compliance zu verbessern und Ihr gesamtes Netzwerk zu schützen. (Nicht alle Funktionen und Lösungen sind auf jedem HP Gerät verfügbar.)[6]

## Verfahren für grundlegende Sicherheit

**Speicherverschlüsselung und sicheres Löschen**
Vertrauliche Informationen, die auf dem internen Laufwerk oder auf der Festplatte eines Geräts gespeichert sind, können offengelegt und durch unbefugte Benutzer verwendet werden. HP Geräte sind mit integrierten Verschlüsselungsfunktionen zum Schutz von Daten ausgestattet. Verwenden Sie die integrierten Funktionen Ihrer Geräte, um gespeicherte Daten, die Sie nicht länger benötigen, sicher zu überschreiben und vertrauliche Informationen sicher zu entfernen.

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

**Sichere Druckerreparaturen**
Wenn Ihnen die Sicherheitsverfahren der Unternehmen vertraut sind, die Ihre Drucker warten, können Sie den Schutz sensibler Daten besser gewährleisten. Entscheiden Sie sich für HP Secure Managed Print Services (MPS) oder HP Partner und verlassen Sie sich auf die Unterstützung von Experten.

**Deaktivierung nicht verwendeter Anschlüsse und Protokolle**
Verringern Sie die Angriffsfläche durch eine ordnungsgemäße Gerätekonfiguration. Deaktivieren Sie Anschlüsse und unsichere Protokolle (wie FTP oder Telnet), um den Zugriff oder die Nutzung durch nicht autorisierte Benutzer zu unterbinden.

**Zugriffssteuerungen für Administratoren**
Legen Sie Administrator-Kennwörter fest, sodass nur IT-Mitarbeiter oder andere autorisierte Benutzer die Geräteeinstellungen einrichten und konfigurieren können.

**Whitelisting von Firmwarecode**
Auf der nächsten Seite finden Sie weitere Informationen darüber, wie Sie Ihre Flotte mithilfe von Whitelisting vor Malware schützen können.

Weitere Informationen

HP Custom Recycling Services
hp.com/go/businessrecycling

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

Weitere Informationen

Integrierte Funktionen für die Drucksicherheit:
- HP Sure Start (BIOS-Integrität)
- Whitelisting von Firmwarecode
- Angriffserkennung für die Laufzeitumgebung

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager
hp.com/go/securitymanager

## Verfahren für erweiterte Sicherheit

**Common-Criteria-Zertifizierung**
HP Business-Drucker sind mit international anerkannten Sicherheitsstandards wie Common Criteria Certification (CCC) und FIPS 140 konform. Stellen Sie sicher, dass bei Firmware-Updates die Codesignierung überprüft wird, um die Authentizität und Integrität des Codes zu garantieren und die Compliance zu gewährleisten.

**Funktionen für die Drucksicherheit für das automatische Erkennen und Unterbinden von Angriffen**
HP Business-Drucker sind mit Sicherheitsfunktionen ausgestattet, die verhindern, dass die Geräte zu Einfallstoren für Angriffe auf Ihr Netzwerk werden. Nur HP Lösungen für sicheres Drucken bieten Optionen zur Erkennung von Bedrohungen in Echtzeit, eine automatisierte Überwachung und eine integrierte Funktion zur Überprüfung von Software, um Bedrohungen abzuwehren, sobald sie auftreten.[7]

HP Business-Drucker – Pro[8] und Enterprise Geräte[7] – können Angriffe in allen Betriebsphasen automatisch erkennen und unterbinden:

- **Beim Systemstart.** Der Startcode (Pro-Geräte) bzw. das BIOS (Enterprise-Geräte) besteht aus Boot-Anweisungen, über die grundlegende Hardwarekomponenten geladen werden und Firmware gestartet wird. Beim Einschalten wird jedes Mal die Integrität des Startcodes überprüft, um so zum Schutz Ihres Geräts vor Angriffen beizutragen.
- **Beim Laden von Firmware.** Whitelisting stellt sicher, dass nur authentischer, bekannter und sicherer HP Code, der von HP digital signiert wurde, in den Speicher geladen wird. Bei Abweichungen wird das Gerät in einem abgesicherten Offline-Modus neu gestartet, um auf ein gültiges Firmware-Update zu warten.
- **Während das Gerät in Betrieb ist.** Integrierte HP Funktionen dienen zum Schutz von Geräten, die in Betrieb und mit dem Netzwerk verbunden sind. Sie schützen also genau dann, wenn die meisten Angriffe erfolgen. Im Fall eines Angriffs wird das Gerät heruntergefahren.

**Sicherheitsfunktionen mit automatischer Fehlerbehebung auf HP Enterprise Geräten**
Abgesehen von den Funktionen zum Erkennen und Unterbinden von Angriffen sind HP Enterprise Drucker mit Sicherheitsfunktion zum automatischen Wiederherstellen des Systemstatus ausgestattet, um die Betriebszeit zu optimieren und den Wartungsaufwand zu verringern.[7] Im Falle eines Angriffs oder einer Abweichung lösen diese Features automatisch einen Neustart aus.

- *HP Sure Start* ist der branchenweit erste BIOS-Schutz mit automatischer Fehlerbehebung.[7] Ist das BIOS gefährdet, erzwingt HP Sure Start einen Neustart des Geräts und lädt eine sichere „goldene Kopie" des BIOS.
- *Die Angriffserkennung für die Laufzeitumgebung* überwacht den Speicher und veranlasst im Angriffsfall einen Neustart. Administratoren können per SIEM-Tools (Sicherheitsinformationen und Ereignis-management) wie ArcSight oder Splunk benachrichtigt werden.

Dank des Investitionsschutzes der aufrüstbaren FutureSmart Firmware können Sie auch bestimmte bereits erworbene Enterprise-Drucker mit einigen dieser integrierten Funktionen versehen.[7]

**HP JetAdvantage Security Manager vervollständigt den Prüfzyklus**
Nach einem Neustart oder dem Hinzufügen eines neuen Geräts zum Netzwerk analysiert HP JetAdvantage Security Manager automatisch die Sicherheitseinstellungen des Geräts und korrigiert sie bei Bedarf so, dass sie den vorgegebenen Unternehmensrichtlinien entsprechen.[9] Ein Eingreifen seitens der IT ist nicht erforderlich.

## Wie funktionieren diese Technologien?

Die integrierten Sicherheitsfunktionen zielen auf drei wesentliche Schritte beim Betrieb von HP Geräten ab.

Bei einem Angriff starten Enterprise-Geräte neu und beheben automatisch Fehler.

HP JetAdvantage Security Manager vervollständigt den Prüfzyklus.

**1.** BIOS/Startcode laden

Verhindert die Ausführung von Malware während des Systemstarts, indem sichergestellt wird, dass authentischer und von HP signierter Code geladen wird.

**2.** Firmware überprüfen

Stellt sicher, dass nur authentischer, bekannter und sicherer HP Firmware-Code, der von HP digital signiert wurde, in den Speicher geladen wird.

**3.** Laufzeit-Codespeicher schützen

Arbeitsvorgänge werden geschützt und Angriffe unterbunden, während das Gerät in Betrieb ist.

**4.** Überprüfungen abschließen

HP JetAdvantage Security Manager prüft die Sicherheitseinstellungen von betroffenen Geräten.


# Schutz für Daten

Weitere Informationen

HP Web Jetadmin
hp.com/go/wja

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

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

HP Access Control
hp.com/go/hpac

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

## Verfahren für grundlegende Sicherheit

**802.1x- oder IPsec-Netzwerkstandards**
Verwenden Sie Standards für die Verschlüsselung, um vom Gerät über das Netzwerk an Verwaltungstools wie HP Web Jetadmin oder Embedded Web Server übertragene Daten zu schützen.

**Verschlüsseln Sie Daten während der Übermittlung**
Schützen Sie Druckaufträge während der Übertragung an das Gerät durch Verschlüsselung, beispielsweise per Internet Print Protocol over TLS (IPPS). Oder per HP Universal Print Driver, der eine echte symmetrische AES256-Druckauftragsverschlüsselung und -entschlüsselung vom Client zur Seite basierend auf einem benutzerdefinierten Kennwort mittels FIPS-140-geprüftem Verschlüsselungsmodul von Microsoft bietet.

Beim Scannen können HP JetAdvantage Workflow-Lösungen zum Schutz sensibler Informationen und zur Effizienzsteigerung beitragen. Beispielsweise lässt sich HP Capture and Route nahtlos in HP Access Control integrieren. Gemeinsam bilden sie eine sichere, bequeme Lösung für die Authentifizierung und die Überwachung von Inhalten zum Zweck der Information Governance.[10]

**Verschlüsseln Sie gespeicherte Daten**
Schützen Sie sensible Business-Informationen auf der Festplatte durch integrierte Verschlüsselungsfunktionen. Für zusätzliche Sicherheit können Sie das betreffende Gerät mit dem optionalen Zubehör HP Trusted Platform Module (TPM) aufrüsten, um den Schutz verschlüsselter Anmeldeinformationen und Daten zu verstärken, indem Geräteverschlüsselungscodes an das TPM automatisch hinzugefügt werden. Das Modul sorgt für eine sichere Geräteidentität, indem private Schlüssel für Zertifikate generiert und geschützt werden.

**Firewall-Schutzfunktion**
Verhindern Sie das Eindringen von Malware und Viren in Ihr Netzwerk, indem Sie den Zugriff von Druckern auf Rechengeräte im Netzwerk beschränken.

**Systemeigene Benutzerauthentifizierung**
Vermeiden Sie Kosten und Sicherheitsrisiken, indem Sie von den Benutzern das Anmelden per PIN/PIC, LDAP oder Kerberos-Authentifizierung verlangen. Diese können auch in Active Directory integriert werden.

**Rollenbasierte Zugriffskontrolle**
*HP Access Control Rights Management.* Tragen Sie durch Beschränkung der Druckerfunktionen zu Kosten- und Risikominimierung bei. Mithilfe einer rollenbasierten Zugriffssteuerung können Sie verschiedenen Benutzertypen oder sogar ganzen Abteilungen je nach ihren Anforderungen unterschiedliche Berechtigungen erteilen. Beispielsweise können Sie so eingrenzen, welche Benutzer faxen oder an E-Mail bzw. an Fax scannen dürfen.

Weitere Informationen

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

## Verfahren für erweiterte Sicherheit

**Erweiterte Authentifizierung und Nachverfolgung**
Implementieren Sie erweiterte Authentifizierungslösungen (beispielsweise Kennwörter, Näherungskarten, Smart Cards oder biometrische Lösungen) und Lösungen zur Nachverfolgung für zusätzliche Sicherheit und Kontrolle.

- *HP Access Control Secure Authentication*. Verwenden Sie diese zuverlässige Authentifizierungslösung, um die Kontrolle zu behalten, das Sicherheitsniveau zu erhöhen und Kosten zu senken. Profitieren Sie von erweiterten Steuerfunktionen und Optionen einschließlich Touch-Authentifizierung bei NFC-fähigen mobilen Geräten.
- *HP Access Control Job Accounting*. Erleichtert 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 zur Steuerung des Netzwerkzugriffs**
Setzen Sie Ihre mobilen Geräte als Teil Ihrer übergeordneten Richtlinie für die Drucksicherheit zur Steuerung des Zugriffs auf Drucker ein. HP bietet serverbasierte Lösungen, die sicheres Pull-Printing ermöglichen und erweiterte Verwaltungs- und Berichterstellungsfunktionen umfassen.

- *HP JetAdvantage Connect*. Technologie für intuitives, verlässliches mobiles Drucken, entwickelt für Unternehmen. Tragen Sie zu Kosten- und Zeiteinsparungen bei, indem Sie einfach Ihre vorhandenen IT-Netzwerktools und Richtlinien nutzen, um das mobile Drucken zu verwalten.[11] Benutzer können jederzeit und überall sicher und so bequem wie von einem PC von einer Vielzahl an Smartphones und Tablets aus drucken.
- *HP Access Control*. Diese Lösung umfasst Funktionen zum Verwalten des mobilen Drucks und 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.

**Digitale Zertifikate für Drucker**
Erhöhen Sie die Sicherheit Ihrer Druckumgebung, indem Sie digitale Zertifikate für Netzwerkdrucker und -MFPs verwenden. Sparen Sie Zeit, indem Sie HP JetAdvantage Security Manager zum automatischen Installieren und Erneuern von Zertifikaten nutzen.[9]

# Schutz für Dokumente

Binden Sie intelligente Hardware- und Softwarelösungen in Ihren umfassenderen IT-Sicherheitsplan ein, um die sensiblen Informationen in Ihren ausgedruckten Dokumenten zu schützen.[6]

## Verfahren für grundlegende Sicherheit

**Steuern Sie den Zugriff auf vorgedruckte Formulare**
Rüsten Sie Ihre Drucker und Multifunktionsgeräte mit abschließbaren Zufuhrfächern aus, um den Diebstahl spezieller Medien zu verhindern, die zum Drucken von Schecks, ärztlichen Rezepten oder anderen vertraulichen Dokumenten verwendet werden.

**Verwenden Sie optionale Technologien wie PIN oder Pull-Printing zum Schutz sensibler Dokumente**
Benutzer können sich per PIN oder Pull-Printing anmelden, wodurch die Abhängigkeit von Einzelplatzdruckern beseitigt und gleichzeitig das Risiko vermieden wird, dass ausgedruckte Dokumente in die falschen Hände gelangen. Mit diesen Sicherheitsmaßnahmen wird zudem verhindert, dass Dokumente gedruckt und nicht am Drucker abgeholt werden. So lassen sich sowohl die Kosten als auch das Abfallvolumen reduzieren.

Beim PIN-Druck weisen Benutzer beim Senden vertraulicher Druckaufträge eine PIN zu, die zur Freigabe des Auftrags am Drucker eingegeben werden muss.

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

- *HP JetAdvantage Secure Print*. Mit dieser kostengünstigen Lösung für KMUs können Aufträge in der Cloud oder auf den Desktops der Benutzer gespeichert werden. Sie lässt sich einfach einrichten und verwenden, ermöglicht die Freigabe von Druckaufträgen über mobile Geräte und unterstützt Geräte unterschiedlicher Hersteller.[12]
- *HP JetAdvantage Private Print*. Mit dieser Lösung profitieren Sie von den Vorteilen der Pull-Printing-Technologie, ohne die sonst damit verbundene Komplexität in Kauf nehmen zu müssen. Sie lässt sich leicht einrichten und es sind keine Server, Installationen oder Wartungen erforderlich.[13]

## Verfahren für erweiterte Sicherheit

**Verlangen Sie Pull-Printing bei jedem Druckauftrag**
*HP Access Control Secure Pull Print*. Schützen Sie Ihre vertraulichen Informationen, verstärken Sie die Gerätesicherheit und steigern Sie die Effizienz. Diese zuverlässige serverbasierte Lösung bietet unterschiedliche Möglichkeiten zur Authentifizierung wie Badge Release sowie Sicherheits- und Verwaltungsfunktionen der Unternehmensklasse.

**Verwenden Sie MICR, Wasserzeichen oder andere Funktionen, damit Dokumente nicht kopiert oder geändert werden können**
HP und TROY Lösungen zur Bekämpfung von Fälschungen 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. MFPs können 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

Dokumentenschutz von HP und Troy
hp.com/go/HPandTROY

# Überwachen und verwalten Sie Ihre Druckumgebung

Mit Lösungen zum Überwachen und Verwalten der Sicherheit können Sie Schwachstellen erkennen und einen einheitlichen, richtlinienbasierten Ansatz umsetzen, um Daten zu schützen, Risiken zu minimieren und die Compliance sicherzustellen.[6] Sorgen Sie für lückenlosen Schutz und vermeiden Sie Geldbußen.

## Verfahren für grundlegende Sicherheit

**Aktualisieren Sie Geräte mit der neuesten Firmware/Betriebssystemversion**
Verwenden Sie Web Jetadmin,[14] um flottenweit Firmware-Updates zu installieren und sicherzustellen, dass die Geräte über die neuesten Schutz- und Sicherheits-funktionen verfügen.

**Überprüfen Sie Ereignisprotokolle zur Druckersicherheit**
HP Geräte senden Druckereignisse/Benachrichtigungen an einen Syslog-Server, damit die IT ggf. Probleme beheben kann.

**Analysieren und korrigieren Sie die Geräteeinstellungen**
*HP JetAdvantage Security Manager*. Verringern Sie die Kosten und den Ressourcenbedarf für die Aufrechterhaltung der Flottensicherheit mit dem branchenweit einzigen Tool für die Einhaltung richtlinienbasierter Drucksicherheit.[9] Implementieren Sie eine flottenübergreifende Sicherheitsrichtlinie, automatisieren Sie die Korrektur der Sicherheitseinstellungen von Geräten und installieren und erneuern Sie eindeutige Zertifikate, während Sie gleichzeitig die Berichte abrufen, um die Compliance nachzuweisen.

## Verfahren für erweiterte Sicherheit

**Implementieren Sie SIEM-Software zum Erkennen und Dokumentieren von Bedrohungen**
Ereignisdaten von HP FutureSmart Geräten können an Tools für die Erkennung von Störungen wie HP ArcSight oder Splunk zur Echtzeit-Überwachung übermittelt werden. Die IT-Sicherheit kann die Druckerendgeräte als Teil des weiteren IT-Systems ohne großen Aufwand darstellen und bei Sicherheits-warnungen Gegenmaßnahmen ergreifen.

**Nutzen Sie die automatische Konfiguration neuer Druckgeräte im Netzwerk**
Mit der in HP JetAdvantage Security inbegriffenen Instant-on Security Funktion lassen sich neue Geräte problemlos schützen, sobald diese dem Netzwerk hinzugefügt oder neu gestartet werden.

**Compliance-Berichte zu Audit-Zwecken für die Sicherheit der Druckerflotte**
Verwenden Sie HP JetAdvantage Security Manager, um Berichte zum Nachweis der Compliance zu erstellen und die Anwendung von Sicherheitsrichtlinien für Drucker und den Schutz von Kundendaten zu belegen.


HP JetAdvantage Security Manager
Schützen Sie Ihre HP Druckerflotte mit der Lösung, die Buyers Laboratory (BLI) als „wegweisend“ bezeichnet.[9]
hp.com/go/securitymanager

# Mit HP erhalten Sie die Hilfe, die Sie benötigen

Wir lassen Sie nicht allein, wenn es darum geht, Ihre Druckumgebung und Ihr Netzwerk zu schützen. Ein Support-Team mit Beratern kann Ihnen zeigen, wie sich die Sicherheit Ihrer Daten, Geräte und Dokumente verbessern lässt.

Arbeiten Sie mit Experten für die Drucksicherheit zusammen, um die Sicherheitslücken Ihrer Druckumgebung zu bewerten. Wir können Ihnen helfen, unter Berücksichtigung geschäftlicher Anforderungen und Best Practices umfassende Richtlinien für die Drucksicherheit zu entwickeln und einen Plan zu erarbeiten, um die Sicherheit in Ihrer speziellen Umgebung zu erhöhen.

## Die ersten Schritte

Wenden Sie sich an Ihren Vertriebskontakt, 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 unter
hp.com/go/printsecurity

[1] InfoTrends, „Designing Hardware & Solutions“, Brendan Morse, Oktober 2016.

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

[3] Spiceworks Befragung von 309 IT-Entscheidungsträgern in Nordamerika, EMEA und APAC im Auftrag von HP, November 2016.

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

[5] Basierend auf Untersuchungen von HP zu im Jahr 2016 veröffentlichten integrierten Sicherheitsfunktionen vergleichbarer Drucker anderer Hersteller. Nur HP bietet eine Kombination aus Sicherheitsfunktionen zur Überwachung, die Angriffe erkennen und automatisch unterbinden und anschließend die Softwareintegrität nach einem Neustart eigenständig überprüfen können. Eine Liste mit Druckern finden Sie unter hp.com/go/PrintersThatProtect. Weitere Informationen finden Sie unter hp.com/go/printersecurityclaims.

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

[7] Gilt für Anfang 2015 eingeführte HP Geräte der Enterprise-Klasse und basiert auf Untersuchungen von HP zu im Jahr 2016 veröffentlichten integrierten Sicherheitsfunktionen vergleichbarer Drucker anderer Hersteller. Nur HP bietet eine Kombination aus Sicherheitsfunktionen für Integritätsprüfungen, die selbst das BIOS einschließen und Technologien zur automatischen Fehlerbehebung umfassen. Möglicherweise ist ein FutureSmart Service-Pack-Update erforderlich, um die Sicherheitsfunktionen zu aktivieren. Eine Liste kompatibler 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 sind mit integrierten Funktionen zum Erkennen und Unterbinden von Angriffen ausgestattet. Weitere Informationen finden Sie unter hp.com/go/PrintersThatProtect.

[9] HP JetAdvantage Security Manager ist separat erhältlich. Weitere Informationen finden Sie unter hp.com/go/securitymanager. Angaben basieren auf internen HP Daten zu Angeboten anderer Anbieter (Vergleich zur Gerätesicherheit, Januar 2015) und einem Lösungsbericht zu HP JetAdvantage Security Manager 2.1 von Buyers Laboratory LLC, Februar 2015.

[10] Für das Senden von Dokumenten an eine kennwortgeschützte Datenbank ist ein zusätzliches Kennwort erforderlich.

[11] HP JetAdvantage Connect ist für die führenden mobilen Geräte verfügbar. Für Geräte mit den Betriebssystemen Android™, Google Chrome™ und Microsoft muss einmalig ein Plug-in installiert werden. Weitere Informationen und eine Liste der unterstützten Betriebssysteme finden Sie unter hp.com/go/JetAdvantageConnect.

[12] HP JetAdvantage Secure Print: Pull-Printing eignet sich für alle mit dem Netzwerk verbundenen Drucker oder MFPs. Die Funktionen zur Authentifizierung am Gerät sind für viele HP LaserJet, PageWide und OfficeJet Pro Geräte sowie für ausgewählte Geräte anderer Hersteller verfügbar. Für einige Geräte ist möglicherweise ein Firmware-Upgrade erforderlich. Für die Nutzung des Cloud-Speichers und den Abruf von Druckaufträgen ist ein Internetzugang erforderlich. Für die Freigabe von Druckaufträgen über mobile Geräte sind eine Netzwerkverbindung und QR-Code erforderlich. Weitere Informationen und eine Liste der unterstützten Drucker und MFPs finden Sie unter hp.com/go/JetAdvantageSecurePrint.

[13] HP JetAdvantage Private Print ist nur in Nordamerika und bestimmten europäischen Ländern verfügbar. Kartenlesegerät ist separat für ausgewählte HP Drucker und MFPs mit Touchscreen erhältlich. Weitere Informationen unter hp.com/go/JetAdvantagePrivatePrint.

[14] HP Web Jetadmin HP Web Jetadmin kann kostenlos unter hp.com/go/webjetadmin heruntergeladen werden.

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

An Kollegen weiterleiten



4AA3-1295DEE, April 2017, Rev. 8