# Printers That Protect:

# Comprehensive HP Security Solutions

Security is important for all companies, but retail organizations have additional concerns. Have you taken steps to secure your network-connected printers?

Security is important for all companies, but retail organizations have additional concerns.

Retailers are vulnerable to threats posed by high employee turnover, large numbers of seasonal workers, and, in particular, "hire attacks" (in which attackers seek employment with the express purpose of obtaining inside information or to conduct corporate espionage.) Retailers also pose a tempting target because of the massive amounts of consumer information they collect. Yet, few retailers have taken steps to secure their network-connected printers.

Printers from HP offer security features to keep your data safe and protect your networks from harm in three main areas: device security, data security, and document security.

## Device security

HP can help defend your network with the world's most secure printing[1] — including devices that can automatically detect and stop an attack.

**HP Sure Start** and **run-time intrusion detection** are included on HP Enterprise printers to protect at start-up and during operation. If malware is detected, the printer automatically shuts down and reboots the device. Every time a printer is turned on or restarts with an error, HP Sure Start automatically validates the integrity of the BIOS code and self-heals if necessary.

HP Enterprise printers also include **whitelisting** to help ensure that only authentic, "known good" HP firmware — digitally signed by HP — is loaded into memory.

What's more, HP can help you stop malware from "calling home" to malicious servers, stealing data, and compromising your network. **HP Connection Inspector** evaluates outgoing network connections to determine what's normal, stop suspicious requests, and automatically trigger a self-healing reboot.

When a reboot occurs — or any time a new device is added to the network — **HP JetAdvantage Security Manager** automatically assesses and, if necessary, remediates device security settings to comply with your pre-established company policies.[2]

## Data security

As a retailer, you know how valuable data is to your organization. The more data you acquire and share, however, the more security risks and requirements you face. You are tasked continuously with protecting confidential information, including employee identities and customer data, across multiple devices and environments. And, today, even a false report of a data breach can cause customers to choose other retail options.

In short, a lot is riding on applying proper security measures across the entire IT infrastructure.

To protect data, you must make sure that only authorized users can access devices and the networks to which they are connected. Fleet-wide authentication solutions can require users to enter a password or PIN, or to scan their badges or fingerprints. HP solutions include **HP Universal Print Driver** and **HP Access Control** for PC network printing and **HP JetAdvantage Connect** and **HP Access Control** for mobile users.

Data in transit also should be encrypted. Data traveling between PCs and the network is often encrypted, but data flowing to and especially from printers is often overlooked. Administrators should use Wi-Fi® and network encryption protocols along with solutions such as HP Universal Print Driver, HP Access Control, and HP JetAdvantage Connect. They also should apply signed certificates to network printers and MFPs. Using HP JetAdvantage Security Manager saves time by automatically installing and renewing certificates.

## Document security

Unclaimed print jobs are one of the most common ways in which sensitive data is exposed. Any printed document is at risk of being stolen by an unauthorized person if the intended recipient isn't there when it comes out of the printer. Additionally, documents often are sent to the printer and forgotten — left unattended for anyone to claim.

Retail organizations should deploy a "pull print" and user authentication solution so that documents are not printed until the user authenticates at the device using identification security protocols. (This is a key concern for the HR department, which prints a high volume of sensitive employee documents due to frequent associate turnover.) HP offers several authentication and pull print solutions for a variety of situations and IT environments:

- **HP Access Control Secure Pull Print** is a server-based software solution that can be set to require all users to authenticate before retrieving their jobs.
- **HP JetAdvantage Secure Print** provides an option for print jobs to be sent and stored in a secure cloud queue until the user authenticates and prints the job.
- **HP Universal Print Driver** is a free solution that includes a secure encrypted printing feature for sensitive documents. It allows users to send print jobs to be held until they release the jobs via a PIN at the device.
- **The HP Proximity Card Reader** lets users authenticate quickly and print securely at a printer or MFP using their existing ID badges.

Now is the time to take proactive steps to reduce risk and help secure data:

- **HP Print Security Services** and specialists can help with print security assessments, planning, deployment, and ongoing management.
- **HP Print Security Advisory Services** can help retail organizations assess vulnerabilities and compliance, develop a custom print security policy, and make process and technology recommendations for improved security.
- **HP Print Security Governance** and Compliance can help retailers maintain security settings compliance across the printer fleet.

For more than 50 years, HP has been partnering with leading retailers, supplying the technical expertise and business savvy to help position them at the forefronts of their industries. This experience gives HP unique insight into your needs to reduce costs, increase productivity, ensure data security, and drive profitability. HP has the print solutions — and the industry's most recognized print management software — to help you reduce risk while improving efficiencies.

In today's volatile retail market, prioritizing security (and printer security in particular) can be daunting, especially when multiple decision-makers and influencers are involved. HP can help you reach consensus with confidence.

[1] "Most secure printing" claim based on HP review of 2016 published security features of competitive in-class printers. Only HP offers a combination of security features that can monitor to detect and automatically stop an attack, then self-validate software integrity in a reboot. For a list of printers, visit hp.com/go/PrintersThatProtect. For more information, see hp.com/go/printersecurityclaims.

[2] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager. Competitive claim is based on HP internal research on competitor offerings (Device Security Comparison, January 2015) and Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory, LLC (February 2015).