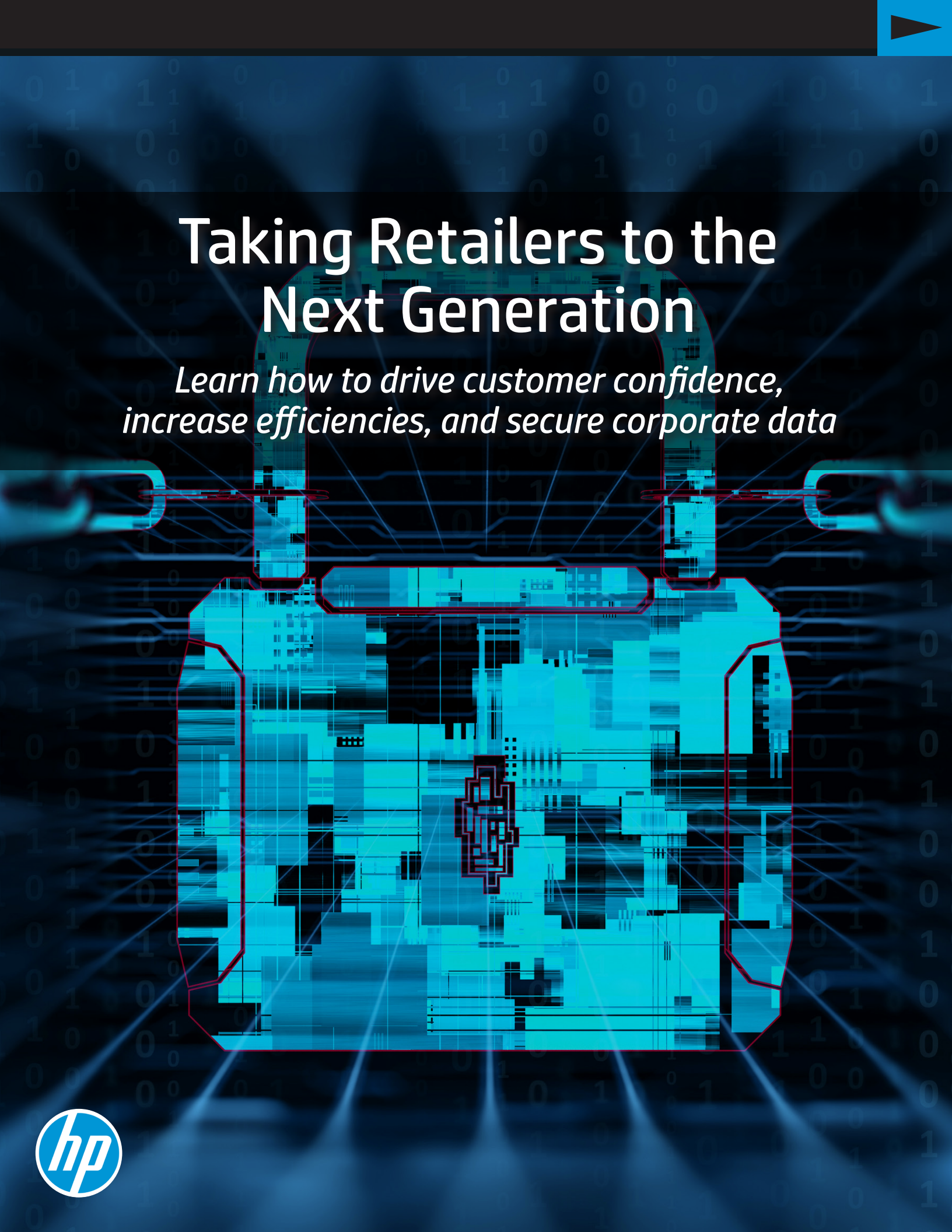
Taking Retailers to the Next Generation

Learn how to drive customer confidence, increase efficiencies, and secure corporate data



Security is important for all companies, but retail organizations have some unique challenges.

They're a tempting target because of the massive amounts of consumer information they collect. And they're vulnerable to threats posed by seasonal workers with high turnover rates, and attackers who seek employment to obtain inside information.

Use this eBook to learn how **HP Print Security** can help you stay ahead.

Aging Retail Systems: Penny-Wise, Pound-Foolish?

Here's why relying on aging, less secure technology can be a costly bet

Retail businesses typically are low-margin operations, which is why they are often loath to invest in new technology for ongoing operations, or add to information security budgets. Two years after U.S. payment card networks shifted fraud liability from issuers to merchants, for example, **half of retailers still shoulder the risk** by using older, non-EMV payment terminals.

Understandably, retailers want to focus investments in areas that will increase customer engagement, as brick and mortar retailers confront the growing threat of online retailers. According to an annual **RIS/Gartner Retail Technology Study**, the top-rated challenge among retailers over the next three years is retiring legacy systems.

Retailers are focused on unified commerce, personalized marketing, and customer engagement, according to that same report. That means budgets are going to remain tight for investments in areas that don't lead to results in these key areas.

Costly bets with aging equipment

But relying on aging, less secure technology could be a costly bet. In fact, many retailers are likely overlooking the security of network-attached printers that could provide unintended gateways into payment networks. And, as the **Target point-of-sale (POS) data breach** illustrated, any network access is good as gold to a cybercriminal.

According to a **report in Krebs on Security**, a Target-commissioned report following the breach indicates that "consultants were able to directly communicate with point-of-sale registers and servers from the core network. In one instance, they were able to communicate directly with cash registers in checkout lanes after compromising a deli meat scale located in a different store."

Many retailers are incorporating innovative technologies such as mobile and social media into environments that are riddled with aging legacy equipment (such as outdated POS systems). In doing so, they may be opening greater outside access to internal systems that are difficult, if not impossible, to secure.

It's probably a safe bet that most retailers have even less insight into their printer networks than their POS networks. A **2016 survey from research firm Quocirca** found retailers lagging behind financial and professional services companies when it comes to security for their print infrastructure.

Ripe for exploitation

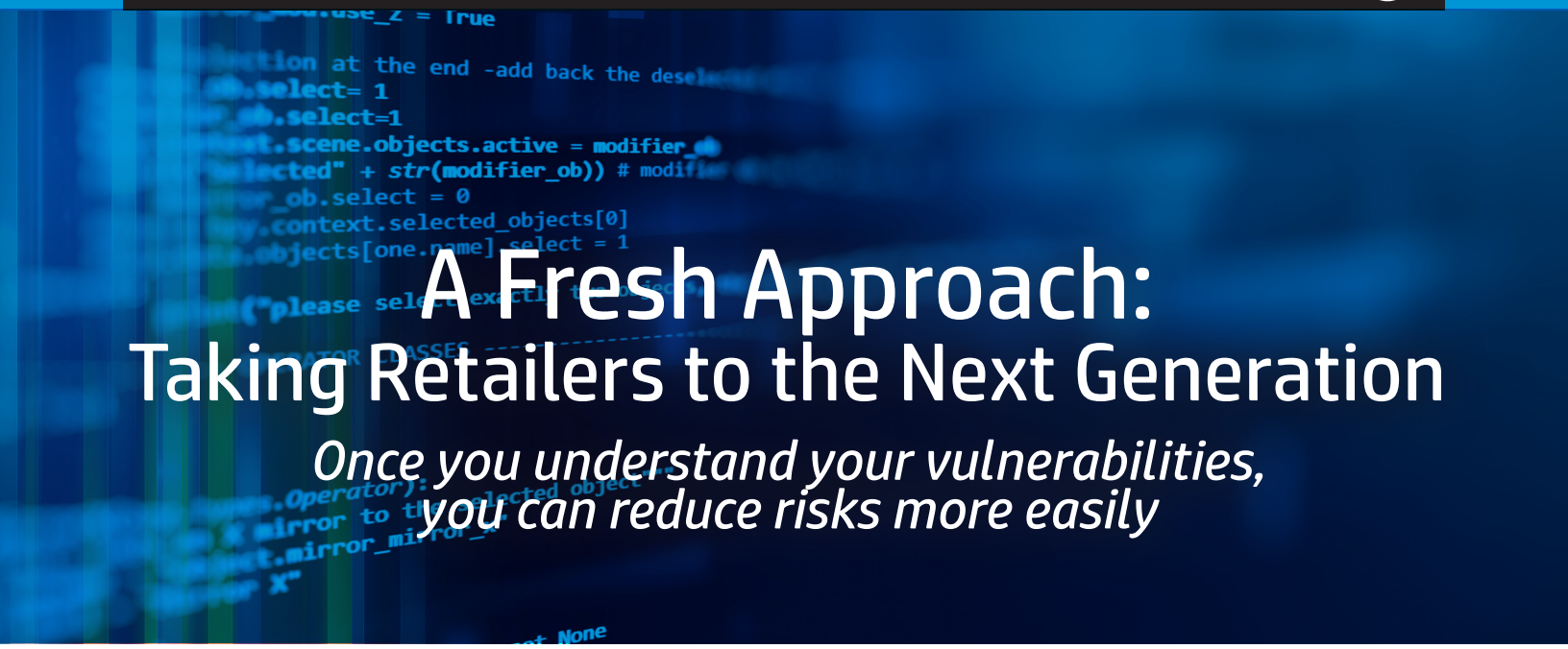
But those printers, sitting often unattended in open offices, may include operating systems, storage media, and software that are ripe for exploitation. Because they require little if any technical skills to operate, printers and other imaging devices are often overlooked in the security infrastructure. However, many of these devices incorporate software-implemented communications "ports" that provide potential points of vulnerability for criminals to exploit with internet protocols. Others have USB slots that could allow an attacker to upload malware to the network, collect sensitive data, and transmit it over the internet.

And it's not just sophisticated cyber schemes that threaten the print environment. Documents left unattended in a printer output tray could allow a passerby to quickly scoop up confidential information, potentially causing compliance violations if customer data is involved.

Printers that require little more than the replacement of ink and paper may seem like low-priority risks, but in an era of constant threats, retailers need to look into upgrading devices that provide little in the way of security protection or, worse, provide relatively unfettered access to corporate networks as readily as a laptop or desktop computer.

In addition to tightening up security policies and implementing best practices, retailers can look to modern printers from HP that contain sophisticated technologies to make them active parts of the security defense. Today's printers can incorporate continuous monitoring and intrusion detection; when malware is detected, they automatically reboot to prevent the execution of malware and can even self-heal the internal BIOS.

To find out more, check out the YouTube video *The Fixer* from HP.



A Fresh Approach:
Taking Retailers to the Next Generation

Once you understand your vulnerabilities, you can reduce risks more easily

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. IT is tasked continuously with protecting confidential information, including employee identities and customer data, across multiple devices and environments.

In 2016, the retail industry represented 22% of all data-breach incidents — the largest single share — of the total reported by Trustwave.[1] In 2017, fast-food chains Arby's, Sonic Drive-In, and Wendy's reported major compromises to their POS systems, as did retail chains Forever 21, The Buckle Inc., and Brooks Brothers, along with the Whole Foods grocery chain.

"With credit and debit cards serving as a de facto currency for many transactions today, modern cyber criminals have found it is more efficient to hack into computer databases to steal consumers' names and card numbers than to rob a bank for cash," the National Retail Federation has observed.[2]

A data breach can have immediate costs. The Ponemon Institute has estimated an average of $3.62 million per incident.[3] Data breaches also can cause abnormal customer turnover, increased customer acquisition activities, reputation loss, and diminished goodwill.

Overlooked and exposed

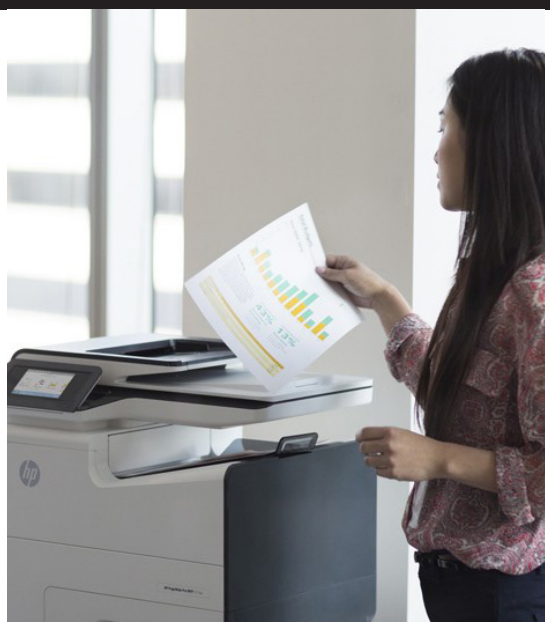
Although many IT departments rigorously apply security measures to individual computers and the network, they often overlook printing and imaging devices, leaving them exposed. Unsecured devices, in turn, can expose the entire network to a cybersecurity attack. A report by market research firm IDC concluded that three-quarters of businesses have no print or document security system in place.[4]

Consider, too, that printing and imaging devices can be easy to use, even if personnel have no technical skills. So, it's easy to forget that these are sophisticated devices that include firmware, software, and networking protocols, each of which represents a potential vulnerability to be exploited by cybercriminals.

It should also be noted that retailers, in particular, 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 conducting corporate espionage).

Over the past year, bomb threats have been transmitted across networked printers and faxes.[5] One hacker accessed 150,000 printers to print out warning notices in a demonstration of potential security vulnerabilities.[6]

Security teams, meanwhile, may overlook the threat because these devices are viewed as low-risk and behind the enterprise firewall. In today's world, though, there's no such thing as a low-risk connected device. According to one survey, 61% of large enterprises have experienced a print-related breach.[7] Despite this threat, a Spiceworks survey found that 43% of surveyed organizations ignore printers in their end-point security practices.[8]



Any connected intelligent device is a potential gateway for cybercriminals.

Defend your devices, data, and documents

Critical gaps can occur at multiple points within your imaging and printing environment. Too often, printers and imaging devices are left unattended, unmonitored, and even outside the scope of established security policies and processes. When a retailer grows through acquisition, it can be especially difficult to maintain a solid infrastructure. In some cases, retailers also have to contend with an overly complex infrastructure.

Once you understand these vulnerabilities, you can reduce the risks more easily. For example, most printers today incorporate USB ports that, when unprotected, provide a physically present hacker with an opportunity to upload malicious code that can access resources across the network. Additionally, many printers are equipped with software-implemented communications "ports" that provide potential points of vulnerability for criminals to exploit with internet protocols.

Some printers and imaging devices incorporate File Transfer Protocol (FTP) software-based servers that can be used to transmit sensitive data across the internet. Like other sophisticated computing devices, printers and imaging devices can be exploited to spread ransomware, which locks up infected computers and disrupts normal operations.[9]

How HP can help

Any connected intelligent device is a potential gateway for cybercriminals. You can take steps to protect your organization from such threats, however. Components of a print security solution can be relatively simple, such as employing locked input trays that prevent misappropriation of items such as paycheck forms.

Likewise, print security can be as sophisticated as HP's comprehensive access control system modules that provide print authentication, auditing, authorization, and accounting. Secure "pull" printing capabilities can store print jobs in the cloud or on a PC until the user is physically present to authenticate the action at a chosen print location. Run-time intrusion detection can check for anomalies during complex firmware and memory operations, and automatically reboot a device in the event of an intrusion.

HP can help you defend your network with the world's most secure printing[10] — including devices that can automatically detect and stop an attack. HP's print security experts can help you develop and deploy an end-to-end imaging and printing security strategy, with a broad portfolio of solutions featuring encryption and configuration administration, as well as BIOS and firmware protection options.

In recognition of HP's competitive strengths in print security, IDC recently positioned the company as a leader in the *IDC MarketScape: Wordlwide Security Solutions and Services 2017 Vendor Assessment*. According to IDC, "HP's approach to security takes the entire print and document infrastructure into account, beginning with locking down the device and extending into all aspects of device usage and content protection."[11]

In today's volatile and ever-changing retail market, only HP printers can stop an attack the moment it starts with unique security features. To find out how, go to **HP Print Security.**

---

[1] 2017 Trustwave 2017 Global Security Report

[2] National Retail Federation, Data Security,, 2017

[3] Ponemon, 2017 Global Report on the Cost of Cyber Crime, August 2017

[4] "Are your business processes stifling your market opportunity? Cost-efficient print and document management through smart MFPs," Jacqui Hendriks, IDC, February 2016

[5] USA Today, "After bomb threat 'hoax,' universities face concerns about network security," June 5, 2017

[6] CSO, "Hacker stackoverflowin pwning printers, forcing rogue botnet warning print jobs," February 5, 2017

[7] Quocirca, "Print Security: An Imperative in The IoT Era," January 2017

[8] Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016

[9] Enterprise Times, "Another wave of Locky Ransomware arrives," September 27, 2017

[10] "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.

[11] *IDC MarketScape: Wordlwide Security Solutions and Services 2017 Vendor Assessment*, IDC, October 2017

Printers That Protect: Comprehensive HP Security Solutions

Why device, data, and document security services are essential

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 startup 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.

Retail organizations should deploy a "pull print" and user authentication solution so that documents are not printed until the user authenticates 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.

Secure Managed Print Services

Critical gaps can occur at multiple points within your environment. Creating a complete imaging and printing security strategy requires coordinated protection of devices, data, and documents, plus comprehensive monitoring and reporting solutions. With HP Secure Managed Print Services, you're more secure on every level, so the trouble that's out there stays out.

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.

Learn more at HP Print Security.

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).