Sales battle card

HP print security

Security threats are evolving every day. Every device on a company's network is a vulnerability point, including network printers. HP's innovative device, data, and document security can help protect the fleet, address compliance requirements, and proactively identify gaps in defenses.

64%

of IT managers state their printers are likely infected with malware[1]

73%

of CISOs expect a major security breach within a year[2]

26%

of all significant data breaches reported by IT managers involved their printers[3]

Target clients

Organizations of all sizes, all geographies, and all industries with needs for securing their shared imaging and printing environments.

Contact target

- CISO (Chief Information Security Officer) or IT Security Leader
- CIO
- Security/compliance managers
- IT management and decision makers

Ideal client characteristics

- Increasing security requirements due to threats and regulatory compliance
- Can't accept the risks of an opening to their network to breaches
- Are facing costly compliance fines due to regulations involving the handling of customer data
- Use highly confidential data as part of their day-to-day business operations (e.g., FSI, HC, and PS)

Market situation

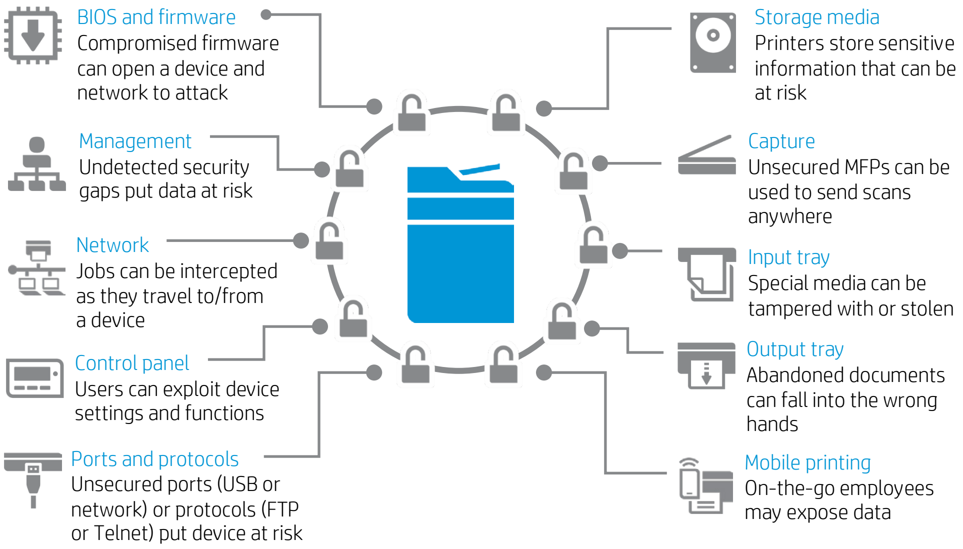
While many organizations have contracted with an MPS provider to optimize their print infrastructure to drive efficiencies and reduce output costs, print security has been largely overlooked in the contract requirements. But due to the growing sophistication and perseverance of cybercriminals, network firewalls are proving to be insufficient security measures. Organizations need to fortify their end points behind the firewall, including network printers.

Whether it's a malicious cyberattack, an accidental internal breach, or regulatory and legal non-compliance, the cost of resolving a security breach can be huge. Average annual cost is about $7.7 million[4] and can include fines, loss of business, damaged reputation, and class-action lawsuits.

Regulatory and compliance requirements are getting more complicated. Organizations need devices and solutions that help them stay compliant.

Client security challenges

Although many IT departments rigorously apply security measures to individual computers and the business network, printing and imaging devices are often overlooked and left exposed.



BIOS and firmware
Compromised firmware can open a device and network to attack

Management
Undetected security gaps put data at risk

Network
Jobs can be intercepted as they travel to/from a device

Control panel
Users can exploit device settings and functions

Ports and protocols
Unsecured ports (USB or network) or protocols (FTP or Telnet) put device at risk

Storage media
Printers store sensitive information that can be at risk

Capture
Unsecured MFPs can be used to send scans anywhere

Input tray
Special media can be tampered with or stolen

Output tray
Abandoned documents can fall into the wrong hands

Mobile printing
On-the-go employees may expose data

Assessment tools

Encourage your customers to use HP tools to assess the security of their print environment.

- HP Secure Print Analysis survey: Online self-assessment to determine if they are following best practices in print security: hp.com/go/SPA
- HP Quick Assess: Free technical evaluation of top 13 settings on up to 20 HP printers (phone consultation available in U.S.): hp.com/go/quickassess

Client security needs

Your customers need easy ways to protect their devices, data, and documents. They also want streamlined print security management and compliance reporting to save IT time.

Device security

- Protect BIOS and firmware from attack and malware
- Upgradeable firmware
- Secure device settings and passwords

Data security

- Encryption in transit and at rest
- Device level CA-signed digital certificates
- Secure hard disk erase and disposal
- Advanced authentication and access control
- Secure mobile printing solutions

Document security

- Secure pull printing solutions
- Fraud and anti-counterfeit solutions

Fleet security monitoring and compliance

- Automatic deployment and remediation of device security settings across the print fleet (an Enterprise MFP has over 250 security settings)
- Proactive security vulnerabilities detection and reporting
- Advanced reporting to help prove compliance

Client value proposition

- Minimize the risk of costly cyberattacks
- Protect sensitive data and documents
- Save time by automating fleet security management
- Keep your business in compliance with industry regulations—and get easy access to data for compliance reporting

Partner value proposition

- A growth opportunity, since clients are actively investing in print security (“Enhance security” is now driver #1 for organizations to move to MPS[5])
- Drives a value conversation so you can sell higher into the organization; HP innovations in security can shift the conversation from price to value-add
- Signals to your clients that HP is actively investing in print security innovation and sustaining its security leadership

Qualifying questions

Ask your customer these questions:

- Do you have a security strategy for your imaging and printing devices?
- Are you handling sensitive information, such as employee identities or customer data?
- Do you encrypt print jobs?
- Are your printers protected from malware and viruses?
- How often do you apply printer firmware updates?
- Have you applied administrative passwords to your printers or can anyone walk up and change device settings?
- How much time does IT spend configuring your printers?

HP security offerings

The security features built into HP devices, along with HP's industry-leading software solutions and services, can help companies protect their devices, data, and documents. Plus, they help your customers more easily manage fleet security and compliance.

Secure printers

The world's most secure printers[7] to protect, detect, and recover: HP LaserJet and PageWide Enterprise printers and MFPs. Unique security features include:

- HP FutureSmart—Upgradable firmware for investment protection; easily add new features across the existing fleet
- HP Sure Start—Validates the integrity of the BIOS code; if the BIOS is compromised, the device reboots and loads a safe, "golden copy" of the BIOS
- Whitelisting—Ensures only authentic, known-good HP code is loaded into memory
- Run-time intrusion detection—Detects anomalies during complex firmware and memory operations; in the event of an intrusion, the device automatically reboots
- Hard disk drive encryption—HP uses 256-bit Advanced Encryption Standard (AES) hard disk data encryption and decryption
- SIEM integration—HP Enterprise printers can be configured to supply printer data to ArcSight, Splunk, or SIEMonster for security threat monitoring

Secure software

Beyond the device, HP offers solutions to detect, protect, monitor and manage the fleet and secure data and documents over time.

- HP JetAdvantage Security Manager—The industry's only policy-based print security compliance tool[6] automates fleet security management.
  - Supports print security policy creation and deployment to the fleet
  - The Instant-on Security feature automatically configures new devices or devices that have been rebooted
  - Risk-based reporting helps IT quickly view fleet status and prove compliance
  - Automated application and updating of unique CA-signed device certificates
- HP Access Control—This powerful management software suite helps secure print jobs and devices, improve workflows, and monitor printing practices—all while helping to reduce costs and supporting organization-wide security, compliance, and environmental initiatives. Advanced authentication limits access to devices, while secure pull printing protects documents.
- HP JetAdvantage Secure Print—An affordable cloud-based pull-print solution designed for SMB. Jobs can be stored in the cloud or on the user's desktop. It's easy to set up and use, allows users to release jobs from a mobile device, and supports multi-vendor devices.[8]
- HP JetAdvantage Connect—Intuitive, reliable mobile printing designed for business. Leverage existing IT network tools and policies to manage mobile printing.[9] Users can securely print from smartphones and tablets—where and when they need to.
- HP and TROY Secure Document Printing Solution—Embed fraud prevention technologies into critical documents, helping to meet government, regulatory, and internal compliance mandates. Enables HP LaserJet black-and-white PCL 5 printers to print secure documents on plain paper.

Secure services

- HP custom recycling services—Make sure data is eliminated from hard drives before responsibly recycling old products. More details at hp.com/go/businessrecycling.

HP JetAdvantage Security Manager
Secure your HP printing fleet with the solution Buyers Laboratory (BLI) calls trailblazing[6]

HP security vs. the competition

While a few competitors offer a small subset of HP's standard baseline security features, they fall short when compared to HP's full suite of solutions, including policy-based security management with HP JetAdvantage Security Manager.[10]

		HP	Xerox	Lexmark	Ricoh	Konica Minolta	Kyocera	Canon
Device	Sure Start (self-healing BIOS protection)	✓	⊘	⊘	⊘	⊘	⊘	⊘
	Whitelisting	✓	✓	✓	⊘	⊘	⊘	⊘
	Run-time intrusion detection	✓	⊘	⊘	⊘	⊘	⊘	⊘
	Security policy deployment and remediation	✓	⊘	⊘	⊘	⊘	⊘	⊘
Data	Access control	✓	✓	✓	✓	✓	✓	✓
	Encrypted communications	✓	✓	✓	✓	✓	✓	✓
	TPM availability	✓	⊘	⊘	✓	✓	⊘	✓
	Integrated encrypted hard drives with secured storage erase	✓	✓	✓	Optional	✓	✓	✓
Document	Pull-PIN print solutions	✓	✓	✓	✓	✓	✓	✓
	Counterfeit and fraud deterrent	✓	✓	✓	✓	✓	✓	✓

Competitive comparisons

None of the competitors listed below offers a policy-based fleet security management tool. They also have serious shortcomings when compared to HP device security.[10]

Xerox: Secure boot, run-time intrusion detection, and SIEM integration are not available. Xerox relies on their partnership with McAfee (Intel Security) to provide whitelisting and protection/notification for attempted system file tampering (at an extra cost per device). Xerox does not offer a Trusted Platform Module (TPM) for added security.

Lexmark: Lexmark's secure boot feature does not self-heal—service is required to remediate the device. Run-time intrusion detection and TPM are not available. For security management, Lexmark pushes model-specific configurations, which lack key settings.

Ricoh: Ricoh's secure boot feature does not self-heal—service is required to remediate the device. Whitelisting, run-time intrusion detection, and SIEM integration are not available.

Konica Minolta: Their secure boot feature does not self-heal—service is required to remediate the device. Whitelisting, run-time intrusion detection, and SIEM integration are not available.

Kyocera: Secure boot, whitelisting, run-time intrusion detection, SIEM integration, and TPM are not available.

Canon: Secure boot, whitelisting, and run-time intrusion detection are not available.

Overcoming objections

Printer security is not our priority right now. We are busy with other projects.

Given the increase in cybercrime and printer breaches, security should be a top priority. A breach can result in loss of business, costly industry fines, and a damaged reputation.

We have a firewall (e.g., Cisco, Juniper, etc.). All devices behind the firewall, including our network printers, are protected.

Deploying printers behind a firewall is a good security practice but does not eliminate all the risks of a breach. Nearly 65% of all breaches are accidental, employee negligence, or business process failure.[11] Hardening your printers inside the firewall helps to reduce Internal threats, whether unintentional or malicious.

Are HP devices secure out of the box?

New HP Enterprise devices come with built-in security features like HP Sure Start, whitelisting, and run-time intrusion detection. (Legacy HP LaserJet Enterprise devices can be upgraded with the most recent firmware to enable whitelisting and run-time intrusion detection.)

HP devices also have security settings that can be configured to address your specific requirements. Print providers typically ship their devices “open” so that customers can use them immediately in their environment. HP is the only print manufacturer to offer policy-based print security compliance software to help streamline the process of configuring security settings on HP printers and MFPs.[6]

HP is continually investing in security features, solutions, and services to help our customers improve their security stance. Starting in Spring 2015, HP disabled FTP and Telnet by default, and in Fall 2016, implemented stronger password requirements in Enterprise printers. HP continues to explore additional ways to reduce the attack surface of our devices.

We use a SIEM product (e.g., McAfee Nitro, Splunk, LogRhythm, or ArcSight), so we’re protected.

SIEM tools use log data to provide real-time analysis and notify IT admins of possible intrusions, but they don’t fix problems. Most SIEM applications are focused on computing devices and network security, and printers are often not included in end-point monitoring. HP has led the industry in developing connectors for ArcSight, Splunk, and SIEMonster.

And when you deploy HP JetAdvantage Security Manager, you can automate the process of keeping network printers in compliance.[6] The solution manages the security settings to ensure the device is hardened to the company standard.

Doesn’t HP Web Jetadmin provide the same capabilities as Security Manager?

HP Web Jetadmin is a robust fleet management tool that can help push settings to the fleet. It is not meant to address security compliance like HP Security Manager.

HP Security Manager is the only printing policy solution[6] that automates the process of keeping devices in compliance with a company’s policies, saving IT staff time. The solution also offers Instant-On which enables a newly deployed printer to receive the security policy within minutes of being added to the network. Plus, it can manage CA signed identity certificates across the fleet.

Can HP JetAdvantage Security Manager support devices from other manufacturers?

No. Security Manager requires access to the device’s firmware to manage the device, and currently only works on HP network printers and MFPs.

What security standards does HP JetAdvantage Security Manager use?

The base policy in Security Manager is based on the National Institute of Standards of Technology (NIST) standards.

Set your services apart

Infuse security practices into all aspects of your managed print services:

- Train your whole MPS staff on security
- Sell HP security offerings from printers with built-in malware protection to security management tools—these unique offerings go a long way to build defenses
- Incorporate industry-driven security best practices into your managed print service delivery capabilities

Contact your HP representative for the latest information on HP security training, security offerings, security sales tools, and support.

How much effort will it take to install and configure HP Security Manager to maintain ongoing security?

HP Security Manager is a quick installation and full capabilities are unlocked with a simple license file. To add devices, you can import a device list from tools like HP Web Jetadmin or run an automatic discovery on your network.[12]

After the devices are added you will need to build your security policy. To make it easier, HP Security Manager provides a base policy mapped to NIST security standards.

After the policy(s) have been created, HP Security Manager can be set to automatically assess and remediate daily, weekly or monthly to keep your devices compliant.

If you use Security Manager to manage device identity certificates, it can save you approximately 15 minutes per device (compared to doing it one-by-one with the Embedded Web Server). That equates to a significant time savings when looking at a fleet of devices.

Why we win

It's vital for businesses to take print security seriously. HP offers industry-leading products and solutions that can help protect devices, data, and documents.

- The world's most secure printers—only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities[7]
- HP JetAdvantage Security Manager is the industry's only policy-based print security compliance tool[6]
- HP takes security beyond the device—including printing from mobile devices, data in transit, and cloud access
- HP printer data can be integrated with SIEM tools such as ArcSight, Splunk, or SIEMonster
- HP has 40+ years of innovation in the security business

Learn more at
hp.com/go/printsecurity

[1] Ponemon Institute, "Insecurity of Network-Connected Printers," October 2015.

[2] Help Net Security, "Why enterprise security priorities don't address the most serious threats," July 2015.

[3] 26.2% of survey respondents experienced a significant IT security breach that required remediation, and more than 26.1% of these incidents involved print. IDC, "IT and Print Security Survey 2015" IDC #US40612015, September, 2015.

[4] Ponemon Institute, "2015 Global Cost of Cyber Crime Study," October 2015.

[5] Quocirca, Managed Print Services Landscapes for 2014 and 2015.

[6] Competitive claim 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. HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

[7] "Most secure printers" claim applies to HP Enterprise-class devices introduced beginning in 2015 and is based on HP review of 2016 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. A FutureSmart service pack update may be required to activate security features. For a list of compatible products, see hp.com/go/PrintersThatProtect. For more information, visit hp.com/go/printersecurityclaims.

[8] HP JetAdvantage Secure Print: Pull printing works with any network-connected printer or MFP. On-device authentication is available for many HP LaserJet, PageWide, and OfficeJet Pro devices and selected non-HP devices. Some devices may require a firmware upgrade. Internet connection required for cloud storage and retrieval of print jobs. Print-job release from a mobile device requires a network connection and QR code. For more information and a list of supported printers and MFPs, see hp.com/go/JetAdvantageSecurePrint. Not available to HP partners in all countries.

[9] HP JetAdvantage Connect works with leading mobile devices. A one-time plug-in must be installed for devices running Android™, Google Chrome™, and Microsoft® operating systems. For details and a list of supported operating systems, see hp.com/go/JetAdvantageConnect. Not available to HP partners in all countries.

[10] Based on the manufacturers' published product specifications and internal HP analysis, as of August 2016.

[11] Ponemon Institute, "2015 Global Cost of a Data Breach Study," October 2015.

[12] HP Web Jetadmin is available for download at no additional charge at hp.com/go/webjetadmin.

Share with colleagues

4AA6-8888ENW, December 2016