Solution overview

Defend your network with the world's most secure printing

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]

6 of 10 companies have unsecured printers.[1] How about yours?

Recognize hidden risks

IT is continually tasked with protecting confidential information, including employee identities and customer data, across multiple devices and environments. Although many IT departments rigorously apply security measures to individual computers and the network, printing and imaging devices are often overlooked and left exposed. Unsecured devices can open the entire network to a cybersecurity attack.

Understand potential costs

Even one security breach has the potential to be costly. If private information is jeopardized due to unsecured printing and imaging, the ramifications could include identity theft, stolen competitive information, a tarnished brand image and reputation, and litigation. Plus, regulatory and legal noncompliance can result in heavy costs.

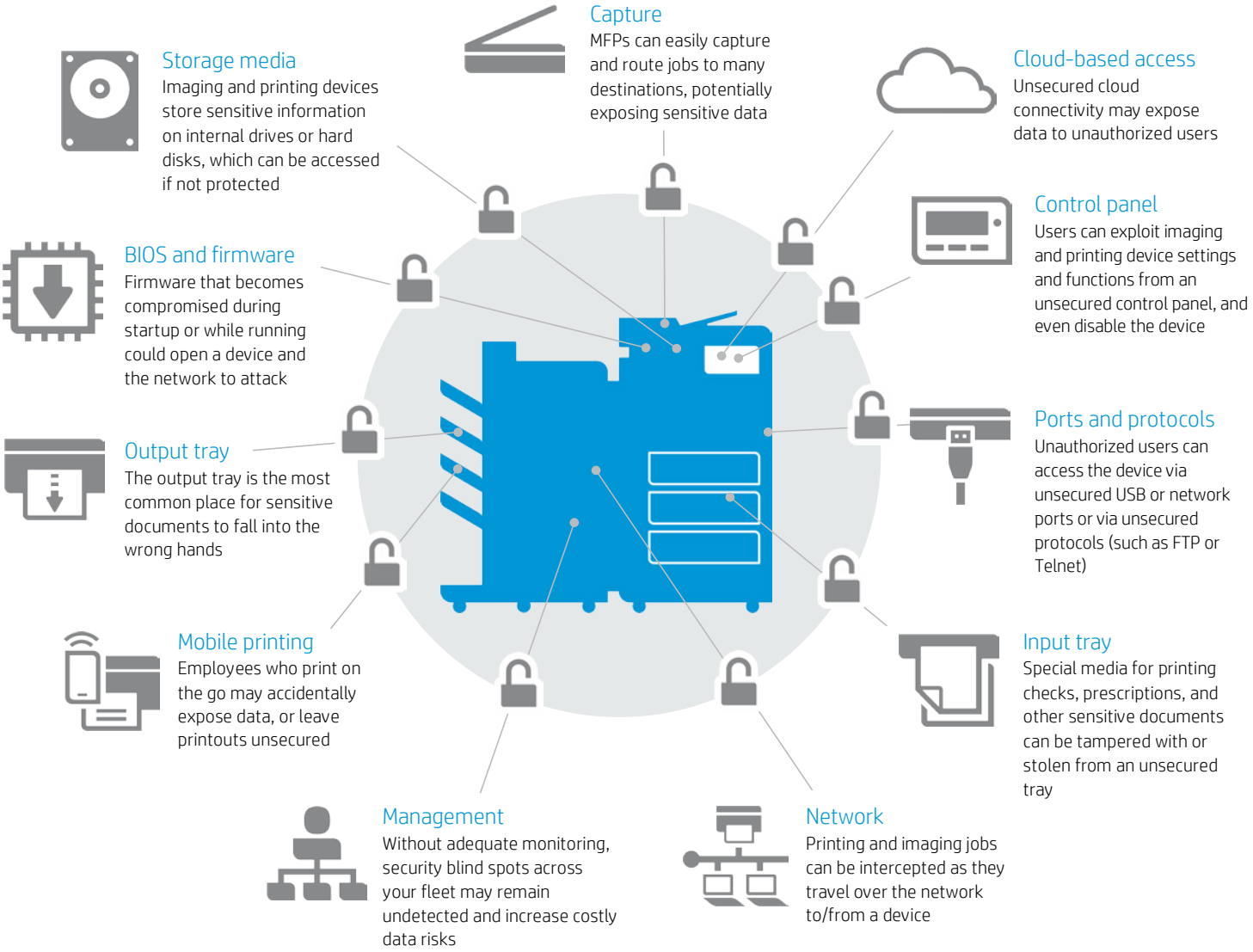
HP can help

Defend your network with the world's most secure printing[4]—including devices that can automatically detect and stop an attack. HP can help you automate device, data, and document protections with a broad portfolio of solutions. Our print security experts can help you develop and deploy an end-to-end imaging and printing security strategy.

Defend your devices, data, and documents

Critical gaps can occur at multiple points within your imaging and printing environment. Once you understand these vulnerabilities, you can more easily reduce the risks.

Figure 1. Imaging and printing vulnerability points



Protect the device

HP printers are designed to work together with security monitoring and management solutions to help reduce risk, improve compliance, and protect your network from end to end. (Not all features and solutions are available on every HP device.)[5]

Fundamental security practices

Encrypted storage with secure erase
Any sensitive information stored on the internal drive or hard disk is potentially vulnerable to theft. HP devices come with built-in encryption to protect data. When stored data is no longer needed, use built-in device capabilities to securely overwrite data and safely remove sensitive information.

Secure disposal
HP Custom Recycling Services can ensure data is eliminated from hard drives before responsibly recycling old products.

Secure printer repair access
Knowing the security practices of printer maintenance vendors will help protect sensitive data. Choose HP Secure Managed Print Services (MPS) or HP partners for expert assistance.

Disable unused ports and protocols
Reduce the attack surface through proper device configuration. Disable physical ports and unsecure protocols (such as FTP or Telnet) to prevent unauthorized access or use.

Administrator access control for device
Set administrator passwords so only IT staff or other authorized personnel can set up and configure device settings.

Whitelisting of firmware code
See the next page for information on how whitelisting can protect your fleet from malware.

Find out more

HP Custom Recycling Services
hp.com/go/businessrecycling

Find out more

Embedded print security features:
- HP Sure Start (BIOS integrity)
- Whitelisting of firmware code
- Run-time intrusion detection

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Advanced security practices

Common Criteria Certification

HP business printers are certified as compliant with internationally recognized security standards, such as Common Criteria Certification (CCC) and FIPS 140. Ensure device firmware updates are code signed to confirm authenticity and integrity of the code and to maintain compliance.

Print security features automatically detect and stop attacks

HP business printers include security features that help protect them from becoming an entry point for attacks on your network. Only HP print security offers real-time detection, automated monitoring, and built-in software validation to stop threats the moment they start.[6]

HP business printers, from Pro[7] through Enterprise,[6] can automatically detect and stop an attack during all phases of operation:

- **During start up.** The boot code (for Pro devices) or BIOS (for Enterprise devices) is a set of instructions used to load fundamental hardware components and initiate firmware. The integrity of the code is validated at every boot cycle—helping to safeguard your device from attack.
- **When loading firmware.** Whitelisting ensures that only authentic, known-good HP firmware—digitally signed by HP—is loaded into memory. If an anomaly is detected, the device reboots to a secure, offline state and waits for valid firmware to be loaded.
- **During run-time.** HP embedded features help protect device memory while devices are operational and connected to the network—right when most attacks occur. In the event of an attack, the device shuts down.

HP Enterprise devices can self-heal

In addition to being able to detect and stop threats, HP Enterprise printers include security features that can automatically recover the device to maximize uptime while minimizing IT interventions.[6] These features automatically trigger a reboot in the event of an attack or anomaly.

- *HP Sure Start* is the industry's only self-healing BIOS.[6] If the BIOS is compromised, HP Sure Start forces a reboot and reloads with an embedded "golden copy."
- *Run-time intrusion detection* monitors memory and reboots in the event of an attack. Administrators can be notified via Security Information and Event Management (SIEM) tools such as ArcSight or Splunk.

With the investment protection that upgradeable FutureSmart Firmware provides, you can add some of these embedded features to select existing Enterprise printers.[6]

HP JetAdvantage Security Manager completes the check cycle

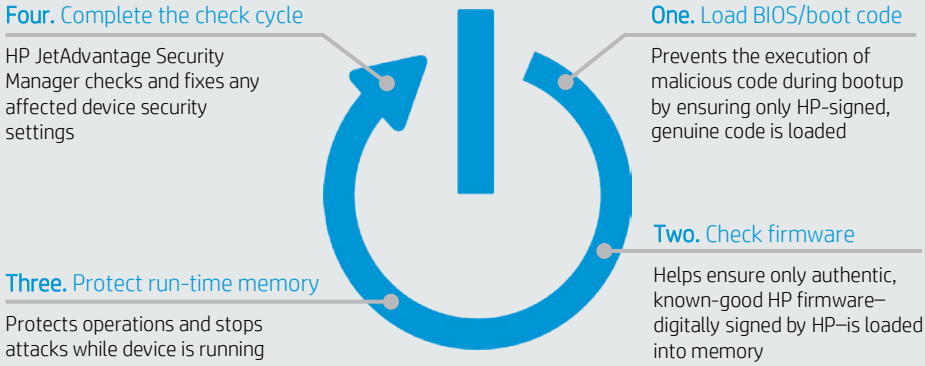
After a reboot occurs—or any time a new device is added to the network—HP JetAdvantage Security Manager automatically assesses and, if necessary, remediates device security settings to comply with pre-established company policies.[8] There's no need for IT to intervene.

How does it work?

The embedded security features address three primary steps in the cycle of an HP device.

If attacked, Enterprise devices can reboot and self-heal.

HP JetAdvantage Security Manager completes the check cycle.



Protect the data

Stored or in transit, your data requires constant protection. Here are some essential steps to help ensure safe arrivals and usage.[5]

Fundamental security practices

802.1x or IPsec network standards
Use encrypted network standards to protect data travelling over the network between the device and management tools such as HP Web Jetadmin or the Embedded Web Server.

Encrypt data in transit
Protect print jobs traveling to the device with encryption such as Internet Print Protocol over TLS (IPPS). Or, HP Universal Print Driver Secure Encrypted Print provides true symmetric AES256 print job encryption and decryption from the client to the page based on a user-defined password using FIPS 140 validated cryptographic libraries from Microsoft®.

When scanning, HP JetAdvantage Workflow Solutions can help protect sensitive information while increasing efficiency. For example, HP Capture and Route integrates seamlessly with HP Access Control for enhanced security, with the convenience of single authentication and the ability to monitor content for information governance.[9]

Encrypt data at rest
Protect sensitive business information stored on the hard drive with built-in encryption. For an extra level of security, the optional HP Trusted Platform Module (TPM) accessory can be added to the device to strengthen protection of encrypted credentials and data by automatically sealing device encryption keys to the TPM. It provides secure device identity by generating and protecting certificate private keys.

Firewall protection
Prevent malware and viruses from entering your network by limiting printer access to computing devices in network.

Native user authentication
Reduce costs and security risks by requiring users to sign in with PIN/PIC, LDAP, or Kerberos authentication. You can also integrate these with Active Directory.

Role-based access controls
HP Access Control Rights Management. Help reduce costs and security risks through printer feature restrictions. Role-based access controls allow you to give different capabilities to different users, or even entire departments, depending on their needs. For example, you can limit who can fax, scan to email, or scan to fax.

Find out more

HP Web Jetadmin
hp.com/go/wja

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

HP JetAdvantage Workflow Solutions
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Find out more

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

Advanced security practices

Advanced authentication and tracking

Deploy advanced authentication (such as passwords, proximity cards, smart cards, or biometrics) and tracking solutions for additional security and control.

- *HP Access Control Secure Authentication.* Restore control, reinforce security, and reduce costs with this robust authentication solution. Get a variety of advanced controls and options, including touch-to-authenticate with NFC-enabled mobile devices.
- *HP Access Control Job Accounting.* Accurately track and gather data, analyze the results, and then create and send reports. Apply mined data to allocate print costs, motivate employees to print smarter, and provide IT with the necessary information to improve fleet-wide forecasts.

Mobile devices included in network access

Utilize your mobile devices as part of your overall print security policy for printer access control. HP offers server-based solutions that provide secure pull-printing, as well as advanced management and reporting capabilities.

- *HP JetAdvantage Connect.* Intuitive, reliable mobile printing designed for business. Help save time and money by seamlessly leveraging existing IT network tools and policies to manage mobile printing.[10] Users can securely print from a variety of smartphones and tablets—where and when they need to—with similar ease of printing as from a PC.
- *HP Access Control.* This solution includes capabilities to manage mobile printing. It leverages existing email infrastructure, allowing mobile users to email a print job to their print queue, and then pull it from any solution-enabled printer or MFP. Protect network print devices with secure authentication features, including Mobile Release.

Apply digital certificates to printers

Improve the security of your print environment by applying digital certificates to network printers and MFPs. Save time by using HP JetAdvantage Security Manager to automatically install and renew certificates.[8]

Protect the document

Integrate smart hardware and software solutions with your larger IT security plan to protect the sensitive information in your printed documents.[5]

Fundamental security practices

Control access to preprinted forms
Equip your printers and MFPs with locking input trays to help prevent theft of special paper used for printing checks, prescriptions, or other sensitive documents.

Use optional PIN or pull printing to protect sensitive documents
Users can opt in to PIN or pull printing, reducing both the reliance on personal printers as well as the risk of print jobs falling into the wrong hands. These security measures also reduce unclaimed prints, which can cut costs and waste.

For PIN printing, when users send confidential print jobs, they assign a PIN which they must enter at the device to release the job.

Pull printing stores print jobs in the cloud or on the user's PC. Users authenticate at their chosen print location to pull and print their jobs. HP offers two cloud-based pull-print solutions:

- *HP JetAdvantage Secure Print*. With this affordable 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.[11]
- *HP JetAdvantage Private Print*. With HP's free cloud-based solution you get the advantages of pull print, without the complexity. It is simple to set up and does not require a server, installation, or maintenance.[12]

Advanced security practices

Require pull print for any print job
HP Access Control Secure Pull Printing. Protect confidential information, enhance device security, and increase efficiency. This robust server-based solution offers multiple forms of authentication including badge release, as well as enterprise level security and management features.

Use MICR, watermarks or other features to prevent copying or modification
HP and TROY counterfeit deterrent solutions include using security toner that stains the paper if subjected to chemical tampering, adding variable data watermarks to printed pages, and incorporating machine-readable codes that track and audit individual documents. MFPs can embed anti-fraud features—including custom signatures, company logos, and security fonts—in sensitive printed documents such as prescriptions, birth certificates, or transcripts.

Find out more

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

HP and TROY document protection
hp.com/go/HPandTROY

Monitor and manage your printing environment

Security monitoring and management solutions can help you identify vulnerabilities and establish a unified, policy-based approach to protecting data, reducing risk, and maintaining compliance.[5] Prevent protection gaps and help avoid costly fines.

Fundamental security practices

Update devices with the latest firmware/OS
Use HP JetAdvantage Security Manager[8] or Web Jetadmin[13] to push firmware updates across the fleet, ensuring devices are up to date with the latest device protection and security features.

Review printer security event logs
HP devices send printer events/notifications to a syslog server so IT can correct problems if necessary.

Assess and remediate device settings
HP JetAdvantage Security Manager. Reduce cost and resources to maintain fleet security with the industry's only policy-based print security compliance tool.[8] Establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates while getting the reports you need to prove compliance.

Advanced security practices

Deploy SIEM software to detect and document threats
Event data from HP FutureSmart devices can be sent to incident detection tools such as ArcSight or Splunk for real-time monitoring. IT security can easily view printer endpoints as part of the broader IT ecosystem to detect and resolve printer security alerts.

Auto-configure new print devices when added to the network
The Instant-on Security feature included with HP JetAdvantage Security Manager automatically configures new devices when they are added to the network or after a reboot.

Compliance audit reporting of print fleet security
Use HP JetAdvantage Security Manager to create proof-of-compliance reports that demonstrate application of security polices to printers and securing of customer data.

HP JetAdvantage Security Manager
Secure your HP printing fleet with the solution Buyers Laboratory (BLI) calls trailblazing[8]
hp.com/go/securitymanager

Get the help you need

You don't have to protect and secure on your own. A support team of consultants can show you how to improve the security of your data, devices, and documents.

Collaborate with print security experts to assess your current print security vulnerabilities. We can help you build a comprehensive print security policy based on business needs and best practices, and create a plan to achieve improved security within your unique environment.

Get started

Contact your sales representative for more information about HP security features, solutions and services that can set you on the path of greater protection and peace of mind.

Learn more at
hp.com/go/printsecurity

Notes

[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] "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: hp.com/go/printersecurityclaims.

[5] Solutions may not be supported in all HP devices; solutions may require additional purchase.

[6] 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.

[7] Select HP LaserJet Pro and PageWide Pro devices include embedded features that can detect and stop an attack. For more information, please visit hp.com/go/PrintersThatProtect.

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

[9] An additional password is required when you send information to a password-protected end repository.

[10] 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.

[11] 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.

[12] HP JetAdvantage Private Print is available only in North America and select European countries. Card reader is available for separate purchase for selected HP printers and MFPs with touchscreens. Learn more at hp.com/go/JetAdvantagePrivatePrint.

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

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA3-1295ENW, November 2016, Rev. 6