



## Sharpen your device, data, and document security

**64%**

of IT managers state their printers are likely infected with malware<sup>1</sup>



**73%**

of CISOs expect a major security breach within a year<sup>2</sup>



**\$7.7M**

is the average annual cost of cyber crime<sup>3</sup>





## Recognize hidden risks

IT is continually tasked with protecting confidential information, including employee identities and customer data, across multiple devices and environments. This need to support a broad range of people in different locations makes unanticipated IT security threats a constant challenge.

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. The security threats are real, and as printing and imaging devices become increasingly sophisticated, they offer greater opportunities for attackers to compromise the device or the entire network.

## 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 litigation, loss of licensing, identity theft, and a tarnished brand image or reputation.

A breach could also result in untold financial damage. Every year, millions of dollars are lost to private and corporate lawsuits, government fines, public relations disasters, industry violations, employee and customer identify theft, and stolen competitive information.

## HP can help

It's time to develop and deploy an end-to-end imaging and printing security strategy. The embedded security features in HP Pro devices offer strong protection, while HP Enterprise devices with HP FutureSmart Firmware have the industry's deepest level of printer security.<sup>4</sup> Combined with a broad portfolio of HP JetAdvantage solutions and services, HP can help give you the strategic foundation to assess, manage, and fortify security for:

- Imaging and printing fleets
- Data in transit and at rest
- Printed documents
- Cloud access
- Printing from mobile devices

# Protect your printer from bootup to shutdown

## Find out more

HP embedded security features  
[hp.com/go/PrintersThatProtect](http://hp.com/go/PrintersThatProtect)

## HP Enterprise self-healing print security features

The latest generation of HP PageWide and LaserJet Enterprise printing devices are unique in the marketplace, because they offer three key technologies designed to thwart attackers' efforts and self-heal.<sup>4</sup> These features automatically trigger a reboot in the event of an attack or anomaly.

After a reboot occurs, HP JetAdvantage Security Manager automatically assesses and, if necessary, remediates device security settings to comply with pre-established company policies.<sup>5</sup> There's no need for IT to intervene. Administrators can be notified via Security Information and Event Management (SIEM) tools such as ArcSight.

- **HP Sure Start** works behind the scenes when printing and imaging devices power on—helping to safeguard your device from attack. HP Sure Start validates the integrity of the BIOS code at every boot cycle. If a compromised version is discovered, the device restarts using a safe, “golden copy” of the BIOS.
- **Whitelisting** helps ensure only authentic, known-good HP FutureSmart Firmware—digitally signed by HP—that has not been tampered with is loaded into memory. If an anomaly is detected, the device reboots to a secure, offline state. It then sends a notice to IT to reload the firmware.
- **Run-time intrusion detection** helps protect devices while they are operational and connected to the network—right when most attacks occur. This feature checks for anomalies during complex firmware and memory operations. In the event of an intrusion, the device automatically reboots.

With the investment protection that FutureSmart Firmware provides, you can add some of these embedded features to selected existing Enterprise printer models.<sup>4</sup>

## HP Pro print security features

The latest HP Pro devices also include embedded features designed to protect from attack— included with the HP OfficeJet Pro 8730/8740, PageWide Pro 400/500 series, and LaserJet Pro M252, M277, and M400/M500 series.

- **Secure boot** validates the integrity of the boot code at every boot cycle. If the code has been compromised, the device is placed in recovery mode with limited functionality until HP genuine code can be reinstalled.
- **Firmware integrity validation** validates firmware updates prior to being loaded. During the device startup process, if the code signature is not validated as genuine HP, the device reboots to a secure recovery state and waits for a valid firmware update. Notification of invalid firmware code is displayed via a control panel message.
- **Run-time code integrity** prevents intruders from introducing malicious code while the printer is running. All run-time code memory is write-protected and all data memory is rendered non-executable.

IT can use HP JetAdvantage Security Manager to remediate device security settings to comply with company policies.<sup>5</sup>

## 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.

### Check printer settings

HP JetAdvantage Security Manager checks and fixes any affected device security settings.

### Protect memory

Protects operations while device is running.



### Load BIOS/boot code

Prevents the execution of malicious code during bootup by ensuring only HP-signed, genuine code is loaded.

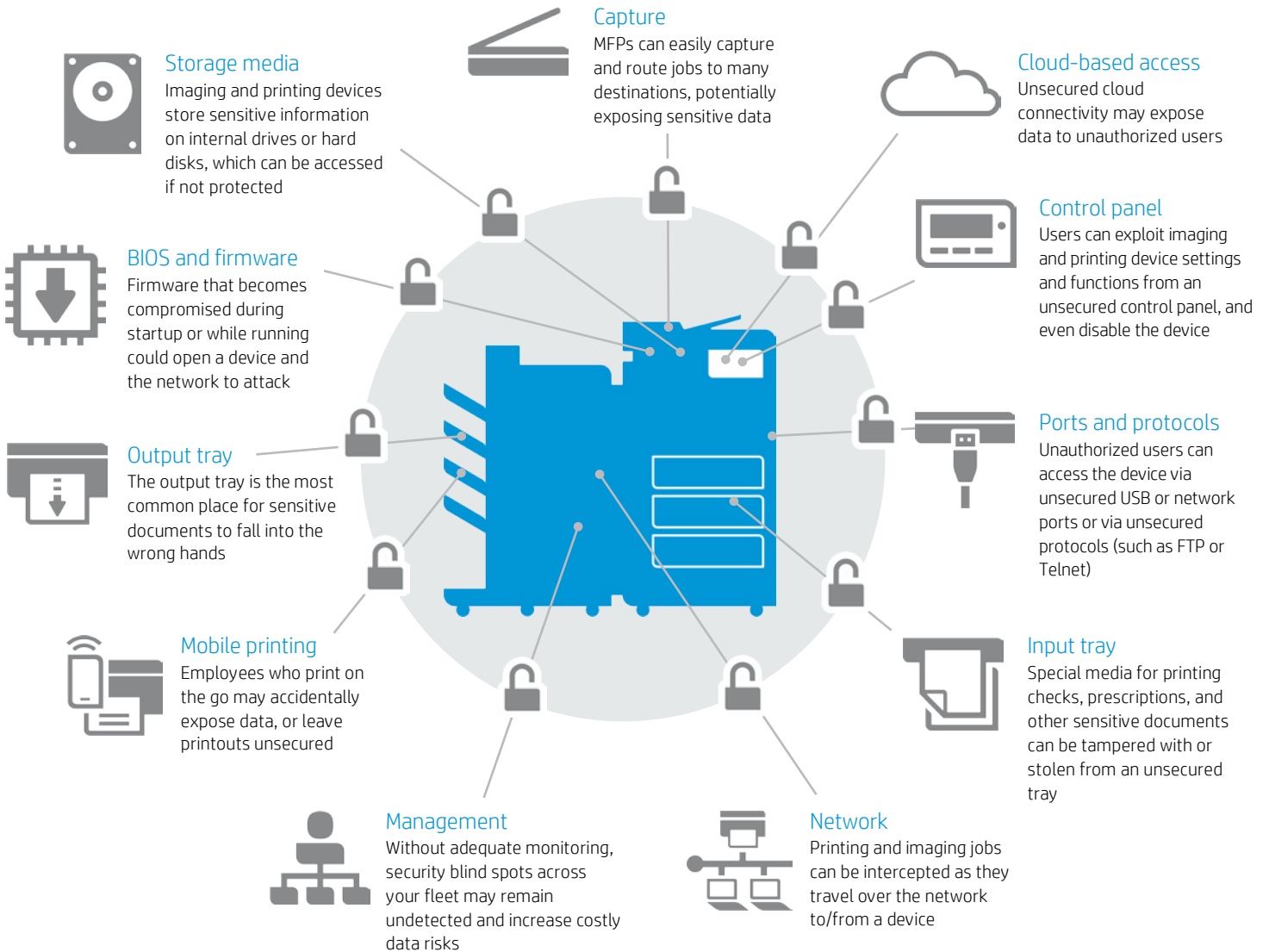
### Check firmware

Validates the firmware as genuine HP code at device startup.

# Mind the security gap

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



# Defend your imaging and printing environment

Even when you understand the vulnerabilities, creating a complete imaging and printing security strategy can be complicated. It requires coordinated protection of devices, data, and documents, plus comprehensive security monitoring and management solutions.

HP printers are designed to work together with 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).<sup>6</sup>



## Find out more

HP Access Control Secure Authentication  
[hp.com/go/hpac](http://hp.com/go/hpac)

## Protect the device

Embedded features and add-on solutions can help you defend your printers and reinforce simple but effective security habits.<sup>6</sup>

### Count on embedded security features to help protect from attack

Multi-level, built-in features help protect your printer against complex security threats from bootup to shutdown. HP Enterprise devices can self-heal in the event of an attack, with HP Sure Start to securely boot the device, whitelisting to validate the integrity of the firmware code, and run-time intrusion detection that continually guards against attacks.<sup>4</sup> In HP Pro devices, secure boot validates the boot code, firmware integrity validation ensures firmware updates are authentic, and run-time code integrity prevents intruders from introducing malicious code while the printer is running.

### Physically secure your devices

Protect each device from theft and tampering by using a lock that requires a physical key for removal. Disable physical ports to prevent unauthorized access or use.

### Secure code

Choose devices certified as compliant with internationally recognized security standards. Ensure device updates are code signed to confirm authenticity and integrity of the code.

### Control access

Require authentication for access to device settings and functions to reduce potential security breaches. Enable administrative access controls, as well as user access controls such as PIN or LDAP authentication, smart cards, or biometric solutions.

Restore control, reinforce security, and reduce costs using HP Access Control Secure Authentication. This solution offers advanced authentication options, including touch-to-authenticate with NFC-enabled mobile devices.





## Find out more

HP Universal Print Driver featuring Secure Encrypted Print  
[hp.com/go/upd](http://hp.com/go/upd)

HP Web Jetadmin  
[hp.com/go/wja](http://hp.com/go/wja)

HP JetAdvantage Workflow Solutions  
[hp.com/go/documentmanagement](http://hp.com/go/documentmanagement)

## Protect the data

Stored or in transit, your data requires constant protection. Here are some essential steps to help ensure safe arrivals and usage.<sup>6</sup>

### Authenticate users

Ensure that only authorized employees can access data on your printing and imaging device by using PINs, LDAP authentication, proximity cards, smart cards, or biometric access control solutions.

### Secure keys, credentials, and certificates

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.

### Encrypt print jobs to protect data in transit

Make print jobs virtually impossible to read if intercepted. Protect your network and documents with a variety of encryption options.

For added security, choose end-to-end Secure Encrypted Print. HP Universal Print Driver 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®.

### Encrypt data in storage

Any sensitive data stored on the internal drive or hard disk is potentially vulnerable. HP devices come with built-in encryption to help protect sensitive business information.

### Remove sensitive data

Storing data about completed jobs on your devices creates unnecessary risk of exposure. Use built-in device capabilities to securely overwrite stored data, and safely remove sensitive information. This is especially important when disposing of devices or returning leased equipment. HP Custom Recycling Services can ensure data is eliminated from hard drives before responsibly recycling old products.

### Protect management data

Device management data that travels over the network between the device and HP Web Jetadmin and other management tools can also be protected. All connections to the device Embedded Web Server administration interface can be securely encrypted.

### Secure capture and route

Ensure scans are protected with document encryption features or encrypted email. Control where users are able to route scans and monitor content for information governance. HP also offers a rich portfolio of HP JetAdvantage Workflow Solutions that provide advanced capture and route capabilities with enterprise level security.

### Safeguard cloud content and access

Secure access and retrieval of documents for printing via the cloud requires specialized tools that extend document protection beyond your physical network. Look for a security solution that enforces user authentication and data access control regardless of where data travels and how it printed.



### Find out more

HP JetAdvantage Private Print  
[hpjetadvantage.com/ondemand](http://hpjetadvantage.com/ondemand)

HP Access Control Secure Pull Printing  
[hp.com/go/hpac](http://hp.com/go/hpac)

HP JetAdvantage Connect  
[hp.com/go/JetAdvantageConnect](http://hp.com/go/JetAdvantageConnect)

HP Access Control  
[hp.com/go/hpac](http://hp.com/go/hpac)

HP ePrint Enterprise  
[hp.com/go/ePrintEnterprise](http://hp.com/go/ePrintEnterprise)

HP and TROY Secure Document Printing  
[hp.com/go/HPandTROY](http://hp.com/go/HPandTROY)



Hewlett-Packard Company  
**NFC/WiFi Direct**

Outstanding Achievement in Innovation

Buyers Laboratory, LLC gave HP an Outstanding Achievement in Innovation award for its use of NFC/Wi-Fi Direct to bring security and simplicity to mobile printing.

## Protect documents

Integrate smart hardware and software solutions with your larger IT security plan to protect the thousands of documents printed organization-wide every day.<sup>6</sup>

### Activate secure pull printing

Pull printing stores print jobs on a protected server, in the cloud, or on your PC. Users identify themselves with a PIN or other verification method at their chosen print location to pull and print their jobs. These security measures also eliminate unclaimed prints, which can reduce cost and waste.

- *HP JetAdvantage Private Print*—With HP's 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.<sup>7</sup>
- *HP Access Control Secure Pull Printing*—This optional robust server-based solution offers multiple forms of authentication including badge release, as well as enterprise level security, management, and scalability.

### Enable secure mobile printing

Help employees stay productive with effortless HP mobile printing from their smartphones, tablets, and notebooks—while maintaining security policies and managing printer access. With HP's wireless direct printing or NFC touch-to-print, employees can print from their mobile devices without connecting to your network, using a secure peer-to-peer connection.

If you're looking to deploy mobile printing across a printer fleet, HP offers server-based solutions that provide secure pull-printing, as well as advanced management and reporting capabilities.

- *HP JetAdvantage Connect* offers 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.<sup>8</sup> 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* 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 authentication features, including Mobile Release.
- *HP ePrint Enterprise* allows users to print from their mobile device to company-networked printers. It offers guest printing, MDM integration, multi-vendor device support, email send functionality, and PIN printing.<sup>9</sup> The solution scales to meet the demands of any enterprise.

### Protect sensitive media with secure input trays

Equip your printers and MFPs with input trays that can be secured to prevent theft of special paper used for printing checks, prescriptions, or other sensitive documents.

### Prevent tampering and alteration

Anti-counterfeiting 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. Embed anti-fraud features—including custom signatures, company logos, and security fonts—in sensitive printed documents such as prescriptions, birth certificates, or transcripts.



HP JetAdvantage Security Manager  
Secure your HP printing fleet with the solution  
Buyers Laboratory (BLI) calls trailblazing.<sup>5</sup>  
[hp.com/go/securitymanager](http://hp.com/go/securitymanager)

HP ArcSight Printer Integration  
[hp.com/go/printsecurity](http://hp.com/go/printsecurity)

## Monitor and manage printing environments

Security monitoring and management solutions can help you identify vulnerabilities and establish a unified, policy-based approach to protecting data, strengthening compliance, and reducing risk.<sup>6</sup>

### Set fleet-wide security settings, and establish access and usage policies

Centralized management allows you to apply a single security policy fleet-wide to prevent protection gaps. Choose from built-in options or added software applications to establish access and usage policies for groups and individuals.

HP JetAdvantage Security Manager is the most comprehensive printing security solution in the market, offering an effective, policy-based approach to securing printing and imaging devices.<sup>5</sup> Reduce cost and resources to maintain fleet security by using automated monitoring and HP Instant-on Security, which automatically adds and configures new devices. HP Security Manager also provides efficient fleet management of unique identify certificates.

### Monitor for risks and maintain compliance

Get all the details at a glance with software or services that let you track compliance to your security policies and audit usage. Accurate data allows you to zero in on vulnerabilities and unnecessary usage. Reports can also help you build a business case to update security measures that reduce risk and control costs.

Get real-time monitoring of the security posture of HP FutureSmart imaging and printing devices with the industry-leading Security Information and Event Management (SIEM) tool, HP ArcSight Printer Integration. IT security can easily view printer endpoints as part of the broader IT ecosystem and can take corrective actions.

## Get help from the experts

*HP Printing Security Advisory Services.* We'll work with you to engage stakeholders, assess the current state of your security, develop a cohesive security strategy, and recommend solutions to protect your business.

*HP Managed Print Services.* We can do it all—deliver a full-service, no-hassle solution, or develop a customized strategy to help resolve the imaging and printing security areas you specify.

*HP Financial Services (HPFS).* When you implement an HP security solution to protect your business, we can offer flexible leasing and financing options to help you invest in the latest products and services. HPFS also protects data by wiping or destroying the disk drives on returned devices.

### Take the next step

Contact your HP 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

[hp.com/go/printsecurity](http://hp.com/go/printsecurity)

<sup>1</sup> Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study," March 2015.

<sup>2</sup> Help Net Security, "Why enterprise security priorities don't address the most serious threats," July 2015.

<sup>3</sup> Ponemon Institute, "2015 Global Cost of Cyber Crime Study," October 2015.

<sup>4</sup> Based on HP review of 2015 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. Some features will be made available as a HP FutureSmart service pack update on selected existing Enterprise printer models. For list of compatible products, see [hp.com/go/LJCompatibility](http://hp.com/go/LJCompatibility). For more information, visit [hp.com/go/printersecurityclaims](http://hp.com/go/printersecurityclaims).

<sup>5</sup> HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit [hp.com/go/securitymanager](http://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.

<sup>6</sup> Solutions may not be supported in all HP devices; solutions may require additional purchase.

<sup>7</sup> HP JetAdvantage Private Print is available at no charge and requires that the printer be connected to the Internet with web services enabled. Not available in all countries. For more information, see [hpjetadvantage.com/ondemand](http://hpjetadvantage.com/ondemand).

<sup>8</sup> 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](http://hp.com/go/JetAdvantageConnect).

<sup>9</sup> HP ePrint Enterprise requires HP ePrint Enterprise server software. App-based option requires Internet- and email-capable BlackBerry® smartphone OS 4.5 or newer, iPhone® 3G or newer, iPad® and iPod touch® (2nd gen) devices running iOS 4.2 or later, or Android devices running version 2.1 or newer, with separately purchased wireless Internet service and the HP ePrint Enterprise app. Email-based option requires any email-capable device and authorized email address. Solution works with PCL5/6, PCL3, and PCL3GUI printers (HP and non-HP).

### Sign up for updates

[hp.com/go/getupdated](http://hp.com/go/getupdated)



Share with colleagues



Rate this document

