Solution Brief

Sharpen your device, data and document security

HP JetAdvantage Security solutions for imaging and printing

Recognize hidden risks

You know how valuable data is to your organization. But the more data you acquire and share, the more security risks and requirements you face. Your imaging and printing environment is not immune. Security gaps can leave sensitive data dangerously exposed.

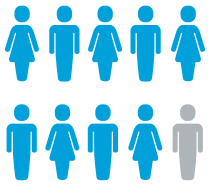
To counter the risks, organizations must integrate imaging and printing security needs into their larger IT security strategy. Otherwise, the consequences and costs can be steep.

Unattended printed documents are especially vulnerable. A financial institution reported that an unauthorized employee viewed—and then publicly shared—sensitive information about an initial public offering from a document left on the printer near his desk. This security lapse resulted in an estimated loss of $7 million.

We can help you develop and deploy an end-to-end imaging and printing security strategy. With the embedded security features in HP devices and a broad portfolio of HP JetAdvantage solutions, we can give you the strategic foundation to assess, manage, and fortify security for:

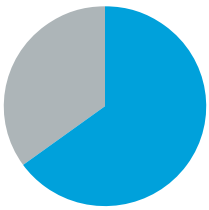
- Imaging and printing fleets
- Data in transit and at rest
- Printed documents
- Cloud access
- Printing from mobile devices
- Content management

Nearly 90%



of enterprises say they have suffered at least one data loss through unsecured printing.[1]

65%



of breaches are accidental employee negligence or IT/ business process failures.[2]

$5.4M Overall

the cost of a single data breach averages $136 per record compromised, and $5.4M overall.[2]

[1] "Managed Print Services Landscape, 2014," Quocirca June 2014.
[2] Ponemon 2013 Cost of a Data Breach: Global Analysis, May 2013

Mind the security gap

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

Figure 1. Imaging and printing vulnerability points

Output tray
The output tray is the most common place for sensitive documents to fall into the wrong hands.

Storage media
Imaging and printing devices store files on internal drives or hard disks, from which anyone can access sensitive information.

Capture
MFPs can easily capture & route jobs to many destinations, potentially exposing sensitive data.

Control panel
Users can exploit imaging and printing device settings and functions from an unsecured control panel, and even disable the device.

Input tray
Special media for printing checks, prescriptions, and other sensitive documents can be tampered with or stolen from an unsecured tray.

Cloud-based access
Unsecured cloud connectivity may expose data to unauthorized users.

Management
Without adequate monitoring, security blind spots and inefficiencies across your fleet may remain undetected and increase costly data risks.

Mobile printing
Employees who print on the go may accidentally expose data, or leave printouts unsecured.

Document tampering
Critical documents can be forged or altered.

Network
Printing and imaging jobs can be intercepted as they travel over the network to/from a device.

Defend your data

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 provides an imaging and printing security framework that safeguards data and documents at each stage.

HP Access Control Secure Authentication

Transform imaging and printing practices to restore control, reinforce security, and reduce costs with this convenient authentication solution for local, mobile, and remote users. Seamlessly secure devices with a variety of authentication options, including PIN/PIC codes, proximity cards, smart cards, or touch-to-authenticate with NFC-enabled mobile devices.

1. Protect the imaging and printing hardware.

Embedded features and add-on solutions can help you defend your data at the printing source and reinforce simple but effective security habits.

- **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 & 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 using Personal Identification Number (PIN) authentication, Lightweight Directory Access Protocol (LDAP) authentication, smart cards, proximity badges, and biometric solutions.

Embedded security features in HP devices

Many security features are built into HP printers and MFPs. Starting with code signed firmware, network protection, and the ability to physical secure the device. Embedded security options such as PIN or LDAP authentication can be activated to control access. Enterprise printers or MFPs also offer secure storage options to provide advanced protection of stored data, and the ability to securely overwrite and safely remove sensitive data. Securely scan and send with encrypted PDFs & emails.

HP Trusted Platform Module (TPM) Accessory

Add an extra level of security safeguard to sensitive information. The optional TPM securely stores security keys, passwords, and certificates. Plus, it's simple to install and use.

HP Universal Print Driver (UPD) featuring Secure Encrypted Print

Now you can simplify printing management fleet-wide and protect sensitive data as it travels to the printer in one versatile tool. With Secure Encrypted Print, the HP UPD is the first fleet driver to provide true symmetric AES256 print job encryption and decryption from the client to the page. These safeguards are based on a user-defined password using FIPS 140 validated cryptographic libraries from Microsoft®.

Learn more
hp.com/go/upd

2. Protect the data.

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

- **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**
  Strengthen protection of encrypted credentials and provide secure device identity with a Trusted Platform Module.
- **Encrypt print jobs to protect data in transit**
  Make print jobs nearly impossible to read if intercepted. Protect your network, documents, and management safeguards by using embedded, device security settings. Or deploy solutions that can enforce security protocols to encrypt data traveling to and from your devices.
- **Encrypt the data in storage**
  Any sensitive data stored on the internal drive or hard disk is potentially vulnerable to abuse. Choose devices equipped 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.
- **Secure capture and route**
  Ensure scans are protected with document encryption features or encrypted email. Control where users are able to route scans & monitor content for information governance.
- **Safeguard cloud content and access**
  Ensuring 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.

HP Pull Printing

Have documents held and released only to the person who printed them.

HP JetAdvantage Pull Print
With HP's cloud-based pull print you get the advantages of pull print, without the complexity. It is bundled with select HP devices & is simple to set up.

Learn more
hpjetadvantage.com

HP Access Control Secure Pull Print
This optional robust server-based solution offers multiple forms of authentication including badge release, as well as enterprise level security, management, and scalability.

Learn more
hp.com/go/hpac

HP Secure Mobile Print

Give your employees enterprise-level print security wherever they need to work.

HP ePrint Enterprise
Allows your employees to print from their mobile devices to any company-networked printer, while keeping your data safely within your company network.

HP's wireless direct and touch-to-print
Let employees print from their mobile devices without connecting to your network, thanks to the secure peer-to-peer connection.

Learn more
hp.com/go/businessmobileprinting

HP and TROY Secure Document Printing Solution

Help prevent document fraud with the HP and TROY Secure Document Printing Solution. This server-based offering embeds fraud prevention technologies into your most critical documents helping you meet government, regulatory, and internal compliance mandates.

Learn more
hp.com/go/gsc

3. 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.

- **Activate secure pull or push printing**
  Pull printing stores print jobs on a protected server or your PC. Users identify themselves with a PIN or other verification method at their chosen print location to pull and print their jobs. With other solutions that enable push printing, the device receives an encrypted file and holds it in memory until the user enters a password to decrypt and print the document. These security measures also eliminate unclaimed prints, which reduces cost and waste.
- **Enable secure mobile printing**
  Ensure your mobile employees can print on the go with the same level of security as if they were inside your network. Equip your team with mobile printing software that enables secure printing measures, such as pull printing and encryption.
- **Secure input trays containing sensitive media**
  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 Imaging and Printing Security Center (IPSC)

Take advantage of the industry's first policy-based compliance solution that helps you increase security, strengthen compliance, and reduce risk across your imaging and printing fleet.[3] Reduce cost and resources to maintain fleet security by using automated monitoring and HP Instant-on Security.

HP IPSC also improves the security of your infrastructure and device communications with efficient fleet management of unique certificates.

Learn more
hp.com/go/ipsc

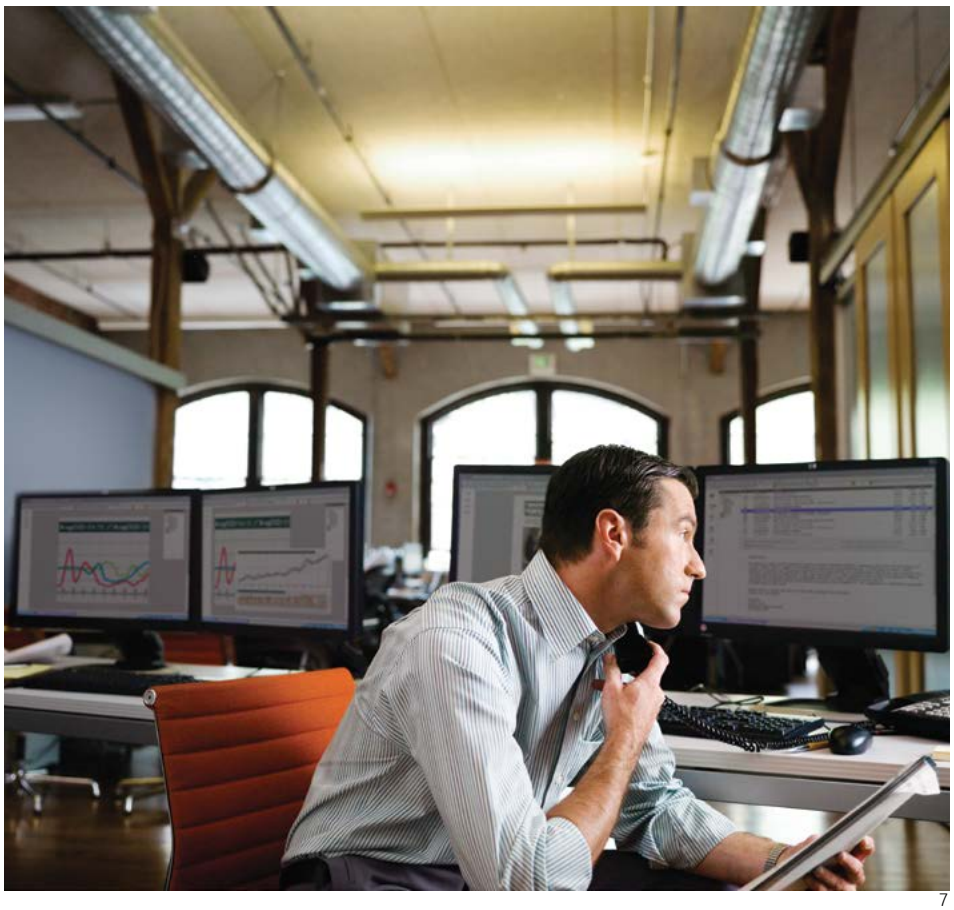
HP ArcSight Printer Integration

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

4. Monitor and manage printing environments.

Security monitoring and management solutions can help you establish a unified, policy-based approach to protecting data, strengthening compliance, and reducing risk.

- **Assess security risks and adjust accordingly**
  An effective monitoring solution can help you identify vulnerabilities, implement policies to resolve them, generate assessment reports, and adjust your print security policy as needed.
- **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.
- **Monitor for risks & 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. Monitor for potential security breaches with broader IT security tools, like Security Information & Event Management software. Reports can also help you build a business case to update security measures that reduce risk and control costs.



[3] Based on an HP assessment of printer manufacturer security offerings in market as of November 1, 2011.

Get help from the experts

Let us help you develop a plan that meets your security needs.

- **HP Printing Security Advisory Services**
  We'll work with you to engage stakeholders, gather information about your current security posture, develop a cohesive security strategy, and implement 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)**
  Don't put your security at risk because your budget is short. 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 & services that can set you on the path of greater protection and peace of mind.

Learn more about HP imaging and printing security solutions
hp.com/go/secureprinting

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA3-1295ENW, August 2014