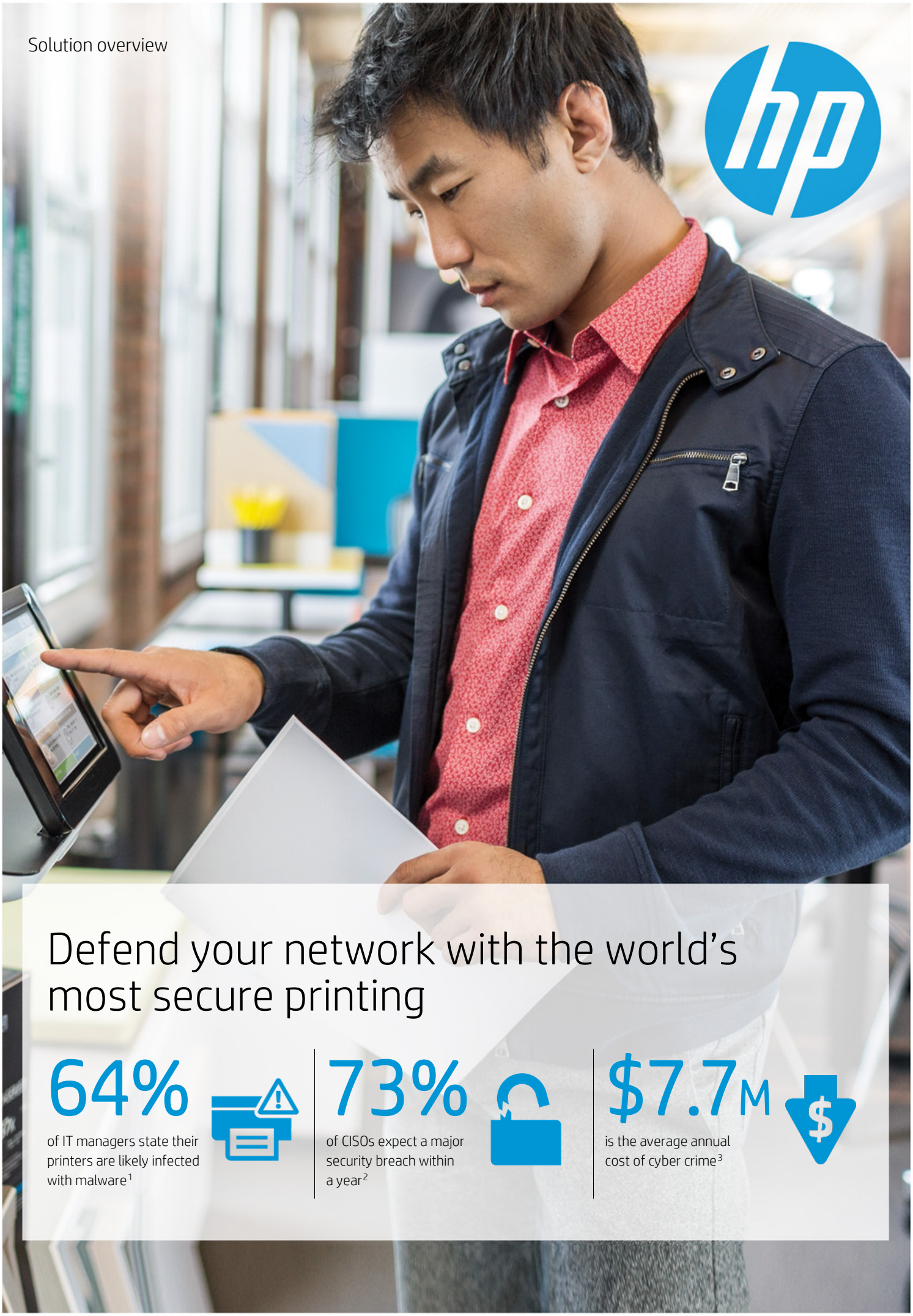
Solution overview



# 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]

**$7.7M**

is the average annual cost of cyber crime[3]

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

## Recognise 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 jeopardised 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.

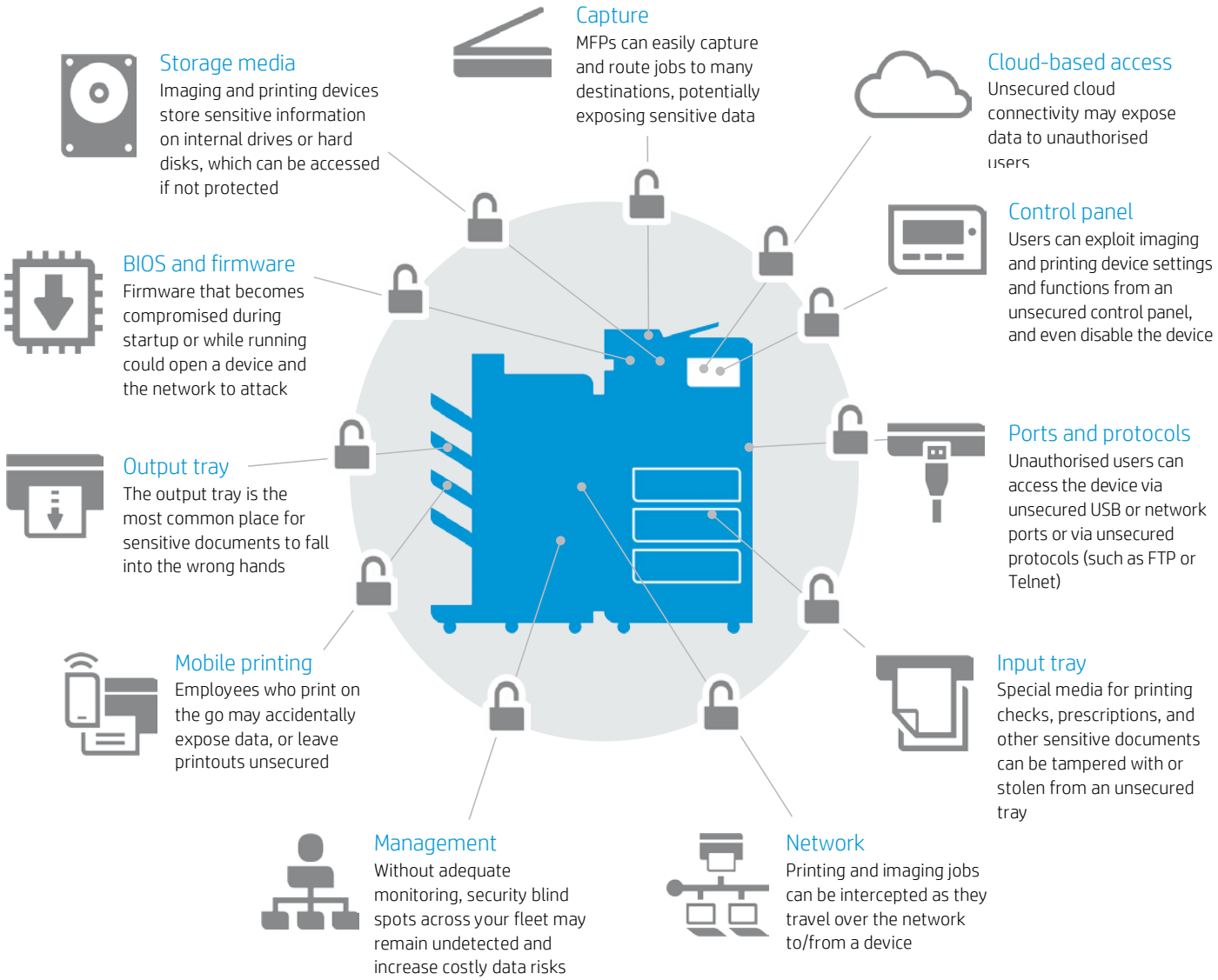
## HP can help

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

## Find out more

HP JetAdvantage Security Manager
hp.com/go/securitymanager

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]

### 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 unauthorised access or use.

### Ensure compliance with security standards

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

### Configured for security—automatically

Part of good device security is making sure that your device is configured properly. The default settings on HP business printers are designed to make them more secure from the start. And HP JetAdvantage Security Manager plays a key role in keeping them secure.[6] This policy-based print security compliance tool automates device remediation to save IT time.

Ensuring proper device configuration not only helps protect your network and data, it helps you meet compliance regulations and avoid costly fines.

## 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.[4]

HP business printers, from Pro[7] through Enterprise,[4] 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. Only authentic, known-good HP 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 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.

### Find out more

HP embedded security features
hp.com/go/PrintersThatProtect

## 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 maximise uptime while minimising IT interventions.[4] 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.[4] 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 FutureSmart Firmware provides, you can add some of these embedded features to select existing Enterprise printers.[4]

## 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.[6] 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.

**One.** Load BIOS/boot code

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

**Two.** Check firmware

Helps ensure only authentic, known-good HP firmware–digitally signed by HP–is loaded into memory.

**Three.** Protect run-time memory

Protects operations and stops attacks while device is running.

**Four.** Complete the check cycle

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

# Protect the data

## Find out more

HP Access Control
hp.com/go/hpac

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

HP Web Jetadmin
hp.com/go/wja

HP JetAdvantage Workflow Solutions
hp.com/go/documentmanagement

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

### Authenticate users, control access, and track printing

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/PIC, proximity cards, smart cards, or biometric access control solutions and integrating these with Active Directory.

*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, analyse 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.

### Encrypt print jobs to protect data in transit

Protect your network and documents with a variety of encryption options. 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®.

### Encrypt data in storage and remove it when it's no longer needed

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.

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.

### 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.

### 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 offers a rich portfolio of HP JetAdvantage Workflow Solutions that provide advanced capture and route capabilities with enterprise level security. For example, HP Capture and Route integrates seamlessly with HP Access Control for enhanced security, with the convenience of single authentication.[8]

### Safeguard cloud content and access

Secure access and retrieval of documents for printing via the cloud requires specialised tools that extend document protection beyond your physical network. HP JetAdvantage solutions can help enforce user authentication and data access control regardless of where data travels and how it is printed.

# Protect the document

## 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 Secure Document Printing
hp.com/go/HPandTROY

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP ePrint Enterprise
hp.com/go/ePrintEnterprise

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

### Improve efficiency with secure pull printing

Pull printing stores print jobs on a protected server, in the cloud, or on your PC. Users authenticate at their chosen print location to pull and print their jobs. These security measures also reduce unclaimed prints, which can cut costs and waste.

- *HP JetAdvantage Secure Print*—An affordable cloud-based 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.[9]
- *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.[10]
- *HP Access Control Secure Pull Printing*—This robust server-based solution offers multiple forms of authentication including badge release, as well as enterprise level security and business class management features.

### Protect sensitive media with locking input trays

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.

### Prevent tampering and alteration

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

## 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. 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.[11] 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.
- *HP ePrint Enterprise*—Users can 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.[12] The solution scales to meet the demands of any enterprise.

# Monitor and manage printing environments


HP JetAdvantage Security Manager
Secure your HP printing fleet with the solution Buyers Laboratory (BLI) calls trailblazing[6]
hp.com/go/securitymanager

Learn more at
hp.com/go/secureprinting

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.

*HP JetAdvantage Security Manager*—Reduce cost and resources to maintain fleet security with the industry's only policy-based print security compliance tool.[6] Establish a fleet-wide security policy, automate device remediation, and install and renew unique certificates while getting the reports you need to prove compliance. HP Instant-on Security automatically configures new devices.

Integrate print data with incident detection (SIEM) tools such as ArcSight or Splunk for real-time monitoring of HP FutureSmart devices. IT security can easily view printer endpoints as part of the broader IT ecosystem and can take corrective actions.

## Get help from the experts

Collaborate with HP print security experts to assess the current state of your security, develop a comprehensive print security policy, and maintain your print security and compliance plan over time.

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.

[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] Ponemon Institute, "2015 Global Cost of Cyber Crime Study," October 2015.
[4] "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 http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA6-1177EEW. For more information, visit hp.com/go/printersecurityclaims.
[5] Solutions may not be supported in all HP devices; solutions may require additional purchase.
[6] 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.
[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] An additional password is required when you send information to a password-protected end repository.
[9] 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.
[10] 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 hp.com/go/JetAdvantagePrivatePrint.
[11] 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.
[12] 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 authorised email address. Solution works with PCL5/6, PCL3, and PCL3GUI printers (HP and non-HP).

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document



4AA3-1295EEW, September 2016, Rev. 5