Defend Your Network With The World's Most Secure Printing[1]

19%

of ITDMs say they are completely confident in the security of their print infrastructure.[2]

61%

have had a print-related data loss in the past year.[2]

80%

of security leads felt that implementing a Zero Trust strategy across an extended network wasn't going to be easy.[4]

Print Infrastructure Is Now Viewed By Organizations As A Top Security Risk

Recognize risks

Today, work happens anywhere. More people across more places need secure access to critical business systems, documents, and IT infrastructure. Distributed endpoints mean an expanded attack surface area that intruders are constantly scanning for the weakest link. Although IT departments rigorously apply security measures to individual computers and the network, printing and imaging devices are often overlooked and left exposed. When devices are unsecured, the entire network can be exposed 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. Regulatory and legal noncompliance can result in heavy fines.

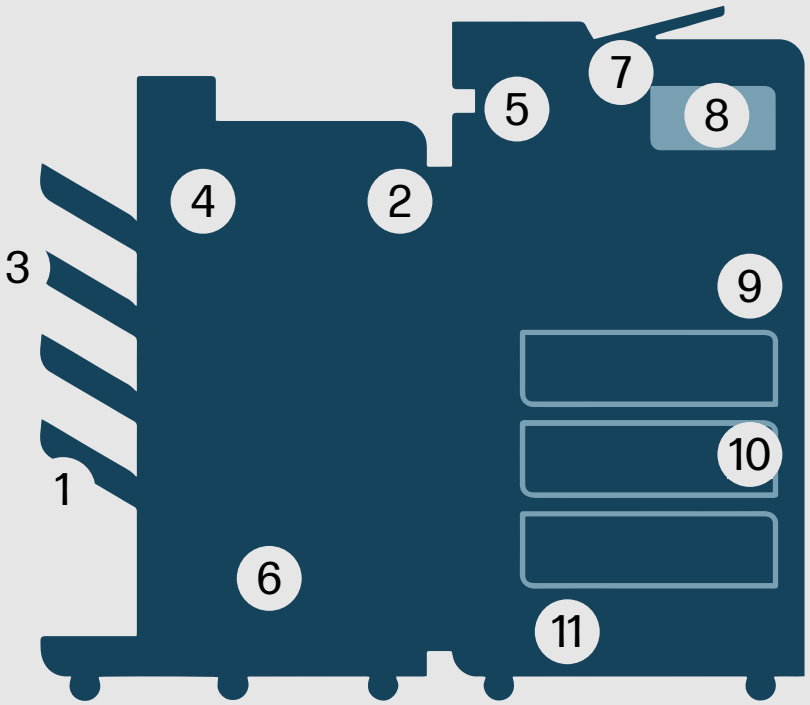
HP can help

Defend your network and build cyber resilience with the world's most secure printing.[1] HP Managed and Enterprise printers are always on guard,continually detecting and stopping threats while adapting to new ones. HP can help you automate device, data, and document protections with a broad portfolio of solutions and services. Our print security experts can help you develop and deploy an end-to-end printing and imaging security strategy—based on the most comprehensive printer security[1] that's rooted in Zero Trust pinciples. HP delivers layered security defenses that start at the hardware level and extend across software and services, providing extensive print security from startup protection to ongoing detection.

Defend Your Devices, Data, and Documents

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

Printing and imaging vulnerability points



1 Mobile printing

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

2 Storage media

Printing and imaging devices store sensitive information on internal drives or hard disks, which can be accessed if not protected

3 Output tray

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

4 BIOS and firmware

Firmware that becomes compromised during startup, or while running, could open a device and the network to attack

5 Capture

MFPs can easily capture and route jobs to many destinations, potentially exposing sensitive data

6 Management

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

7 Identity access management

Unsecured cloud connectivity may expose data to unauthorized users

8 Control panel

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

9 Ports and protocols

Unauthorized users can access the device via unsecured USB or network ports or via older protocols (such as FTP or Telnet)

10 Input tray

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

11 Network

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

Protect the Device

HP printers are designed to work together with security monitoring and management solutions to help reduce risk, improve compliance, and build cyber resilience with the most comprehensive Zero Trust Print Security. (Not all features and solutions are available on every HP device[5]).

Device practices—Fundamental security practices

Secure disposal

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

Secure printer repair access

Checking that printer maintenance vendors follow security best practices can help protect sensitive data and keep settings secure. Choose HP Secure Managed Print Services (MPS) or HP partners for expert assistance.

Hardened print devices for unused ports/protocols

Reduce the attack surface through proper policy-based device configuration employing a Zero Trust framework. Password-protect or disable physical ports and unsecure protocols (FTP, Telnet, SNMP v1/v2) to prevent unauthorized access.

Administrator access control for device configuration change

Use modern authentication and access control protocols so only authorized personnel can set up and configure device settings.

Find Out More

- HP CUSTOM RECYCLING SERVICES
- HP SECURE MANAGED PRINT SERVICES

Device features—Fundamental security practices

Encrypted storage on device

Any sensitive information stored on the internal drive or hard disk is potentially vulnerable to theft. Many enterprise HP devices come with built-in hard disk encryption to make data inaccessible and unreadable.

Physical security (locks)

Equip your printers and MFPs with locking input trays to help prevent theft and fraud if you use specialized media for sensitive documents like checks and prescriptions.

Advanced security practices

Print security features automatically detect and stop attacks

HP printers heal themselves before malware runs wild. Defend your network from evolving threats and automatically recover from attacks with the world's most secure printers.[1] HP business printers include security features deeply rooted in Zero Trust principles. HP Wolf Enterprise Security delivers layered security defenses that start at the hardware level and extend across software and services, providing extensive print security from startup protection to ongoing detection.

HP business printers, from Pro[6] through Enterprise,[1] are always on guard, continually detecting and stopping threats during all phases of operation.

Find Out More

EMBEDDED PRINT SECURITY FEATURES:

- HP Sure Start (BIOS integrity)
- Allowlisting of firmware code
- HP Memory Shield TM
  - Run-time Intrusion Detection
  - Control Flow Integrity
- HP Connection Inspector

1

DURING START UP

The core boot code (i.e., BIOS) loads critical hardware components and initiates the firmware. The integrity of the code is validated at every boot cycle—helping to safeguard your device from attack.

2

WHEN LOADING FIRMWARE

HP's Allowlisting automatically checks firmware during startup to determine if it's authentic, good code—digitally signed by HP.

3

DURING RUN-TIME

HP embedded features help protect device memory while devices are powered on and connected to the network—right when most attacks occur. In the event of an attack, HP Pro devices shut down and notify IT. HP Managed and Enterprise devices initiate a self-healing reboot.

HP Managed and Enterprise devices can self-heal and send threat notifications to SIEM tools

In addition to being able to detect and stop threats, HP Managed and Enterprise printers automatically self-heal from attacks, so IT doesn't need to intervene.[1] These features automatically trigger a reboot in the event of an attack or detected anomaly. Administrators can connect devices to leading Security Information and Event Management (SIEM) tools such as ArcSight, Splunk, McAfee, SIEMonster, and IBM QRadar for real-time threat notifications.

- HP Sure Start is the industry's only out-of-the-box, self-healing BIOS that doesn't require human intervention. If the BIOS is compromised, HP Sure Start restarts from a safe "golden copy" of its BIOS.
- HP Memory Shield TM has two major components that are self healing which allows the device to reboot to a safe state if affected.
  - Hardware-based Run-time Intrusion Detection's integrated chip provides hardware-level protection of a device's memory to detect attacks while in operation. This gives the benefit of making it more difficult for hackers to disable while allowing more frequent memory checks with minimal performance impact
  - Control Flow Integrity prevents malware attacks by ensuring the execution flow on the device cannot be altered. The devices also monitor for potential zero-day attacks.
- HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and thwart malware by automatically triggering a self-healing reboot

With the investment protection of upgradeable HP FutureSmart firmware, you can add whitelisting, run-time intrusion detection, and HP Connection Inspector to many existing HP Managed and Enterprise printers.[1]

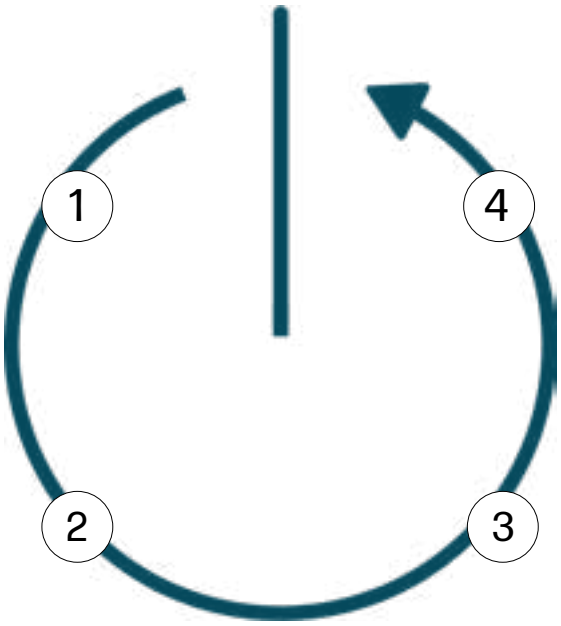
HP Security Manager brings clarity to compliance

Make compliance less complicated. Strengthen your security posture and make it consistent across your entire fleet of devices with HP Security Manager, which lets you monitor, manage, and automatically restore critical settings that make maintaining compliance simple.[7]

How Does It Work?

The embedded security features conform to a Zero Trust framework and address four primary steps in the cycle of an HP device. If attacked, HP Managed and Enterprise devices can reboot and self-heal. HP Security Manager completes the check cycle, providing dynamic, fleet-wide security compliance.[7]

1. **Check BIOS/boot code**
   Prevents the execution of malicious code during bootup by allowing only HP-signed, genuine code to be loaded.
2. **Check firmware**
   Allows only authentic, good firmware–digitally signed by HP–to be loaded.
3. **Check settings**
   After a reboot, HP Security Manager checks and fixes any affected device security settings.[7]
4. **Continuous monitoring**
   Protects operations and stops attacks while device is running. Inspects outgoing network connections to stop suspicious requests (Enterprise only).



Protect the Data

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

Network data– Fundamental security practices

802.1x or IPsec network standards

Apply these network standards to support device identification and data encryption within the network so unauthorized devices can't be added to the network and data is unreadable if intercepted.

Encrypt data in transit

Protect print jobs traveling to the device with encryption such as Internet Print Protocol over TLS (IPPS). Or use HP Universal Print Driver Secure Encrypted Print which 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®.

Often overlooked, scan files should be encrypted. HP workflow solutions, such as HP Capture and Route, HP Access Control Scan,[8] and HP Workpath apps, include safeguards to help protect sensitive information and address additional security and compliance issues.

Find Out More

- HP UNIVERSAL PRINT DRIVER FEATURING SECURED ENCRYPTED PRINT
- HP INTELLIGENT WORKFLOW SOLUTIONS AND SCAN AI ENHANCED
- HP CAPTURE AND ROUTE
- HP ACCESS CONTROL SCAN
- HP WORKPATH

Encrypt data at rest

Protect sensitive business information stored on the hard drive by using built-in encryption to make it unreadable. 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

Connect printers to a network only behind a firewall, since direct-connected printers or printers openly connected to the Internet could be discovered and accessed by hackers. While this is an important step, even printers behind a firewall may be vulnerable to threats such as phishing and "man-in-the-middle" attacks unless they have the layered embedded security features found on HP Managed and Enterprise printers and MFPs.

Network data– Advanced security practices

Apply digital certificates to printers

Just like a passport, digital certificates provide identifying information and are forgery resistant, allowing a device to securely exchange data over the internet with another device and helping to avoid a "man-in-the-middle" attack. HP Security Manager makes digital certificate management easy.[7]

Same day print/copy job removal

Keep sensitive documents from being stored on the printer longer than needed by using HP Secure Erase to erase the hard drive at regular intervals.

Controlling access–Fundamental security practices

Deploy native user authentication such as PIN, LDAP, or Kerberos

Help 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 Print provides management capabilities that can help reduce costs and security risks through printer feature restrictions.[8] 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 copy, fax, or scan.

Pull print authentication

HP Access Control Print improves security by integrating convenient authentication tools with existing network credentials such as LDAP and Active Directory.8 Device access protection includes options for ID badges, PICs, or PINs.

Mobile connectivity peer-to-peer or via a secure mobile print solution

Enabling a peer-to-peer printer feature like Wi-Fi Direct® allows employees to print from their mobile devices without connecting to the network. HP also offers fleet-wide mobile printing solutions that enable a range of security features from pull printing to management and reporting capabilities.

- HP Mobile Connector capabilities to mobile devices.[8] Mobile users can submit documents via a native print app, or simply 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 Secure Print and Insights also supports printing from and releasing jobs with mobile devices, and because it is a cloud-native solution, jobs can be sent securely from virtually anywhere.[10]

Find Out More

- HP ACCESS CONTROL PRINT
- HP SECURE PRINT AND INSIGHTS

Controlling access–Advanced security practices

Tracking of printed jobs from all devices, including mobile

HP Insights allows you to accurately track and monitor print device use, analyze the results, and create reports to continually optimize your print environment and improve efficiency.[11] HP Access Control Print includes job accounting capabilities to help you accurately track and analyze device and supplies usage.[8] Allocate print costs to a department, group, or cost center, and use job accounting data to help encourage cost-conscious printing habits and curb excessive printing. The reports can also help ensure sensitive information and customer data are managed in compliance with corporate security standards.

Connect your exisiting identity managment system to your printers

In today's evolving work landscape, a new security posture rooted in Zero Trust principles is crucial. IT leaders are seeking consistent authentication policies across all endpoints. With HP Authentication Suite, you can extend modern authentication to print devices, helping to provide a seamless and secure experience for end users. By unifying authentication, you enhance productivity, streamline workflows, and protect sensitive documents and data. Embrace modern authentication with a true, single sign-on experience that supports compliance and privacy objectives while meeting employee expectations.

Find Out More

- HP AUTHENTICATION SUITE.

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

Use optional PIN or pull printing to protect sensitive documents

Users can opt-in to PIN or pull printing, reducing 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.

Advanced security practices

Deploy features (MICR, watermarks, etc.) to deter counterfeit, fraud, or document tampering

Deploy features (MICR, watermarks, etc.) to deter counterfeit, fraud, or document tampering 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.

Deploy features to prevent scanning or faxing of sensitive documents

With HP Capture and Route Data Loss Prevention, you can prevent sensitive information from being scanned or faxed.

Require pull printing for any print job

Pull printing solutions can help protect confidential information, increase efficiency, and enhance device security with multiple forms of authentication including badge and mobile release. HP Secure Print is a cost-effective, cloud-native solution that is easy to set up and use, allows users to send jobs from desktops or mobile devices, and supports multivend or print devices.[10] HP Access Control Print is a server-based solution offering enterprise-level security and management features.[8] HP Access Control Print can support multivendor fleets.

Securely transform your workflows

Unleash your business's potential by taking your digital processes into the cloud with confidence. Simplify workflows while maintaining the security that hybrid workers need to collaborate freely. Authentication, job accounting, and pull-print solutions make it easy to maintain security while letting people work their way.

Find Out More

- CAPTURE AND ROUTE
- HP ACCESS CONTROL PRINT
- HP SECURE PRINT

Monitor And Manage Your Printing Environment

Security monitoring and management solutions can give you extensive print security from startup protection to ongoing detection and toolsets that enable active monitoring with the ability to act upon anomalous activity in real-time. Build cyber resilience and prevent gaps to help avoid costly fines.

Fundamental security practices

Update devices with the latest firmware/OS

Thwart evolving threats by regularly updating your printer firmware, which addresses known vulnerabilities to your devices' core functionality. Use HP Web Jetadmin to push firmware updates across the fleet, ensuring devices are up to date with the latest device protection and security features.[12]

Review printer security event logs

HP devices send printer events/notifications to a syslog server so IT can correct problems remotely or in person, if necessary.

Assess and remediate device settings

Manage essential printer security settings across the fleet with the HP Printer Security Plug-in for Microsoft System Center Configuration Manager (SCCM). Microsoft SCCM is a widely used management solution to remotely plan, deploy, configure, and monitor endpoints. The HP Printer Security Plug-in can discover, assess, and remediate the most essential 15 security settings and report on the results.

For comprehensive security management across your HP fleet, choose HP Security Manager.[7] This solution helps you reduce cost and resources to establish fleet-wide security policies and automate remediation of over 200 device settings.

Find Out More

- HP WEB JETADMIN
- HP SECURITY MANAGER

Advanced security practices

Quickly assess the vulnerability of device firmware across the fleet

HP Security Manager provides an integrated fleet firmware vulnerability assessment feature that identifies the various degrees of firmware vulnerability across all your devices.[7] Get immediate visibility into firmware that is outdated or has been flagged with a security bulletin.

Automated certificate management

Digital certificates require regular renewal for each device. Save time by using HP Security Manager to automatically install and renew certificates to easily maintain trusted communications. HP Security Manager includes complete SCEP (Simple Certificate Enrollment Protocol) support, expanding certificate support across a broad spectrum of leading certificate authorities.

Find Out More

HP SECURITY MANAGER

Auto-configure new print devices when added to the network

The Instant-on Security feature included with HP 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 Security Manager to create proof-of-compliance reports that demonstrate adherence to security and data protection policies.

Connecting to SIEM tool

Threat notifications from HP FutureSmart devices can be sent to incident detection tools such as ArcSight, Splunk, McAfee, SIEMonster, and IBM QRadar for real-time monitoring. IT security can easily view printer endpoints as part of the broader IT ecosystem to detect and resolve network threats.

Compliance infringement can hurt your business

Unprotected or under-protected endpoints create more opportunity for cybercrime. To help counter the growing threat, government bodies across the globe are implementing strict security regulations that require organizations to better protect customer information.

Organizations that aren't in compliance can face heavy costs including fines, lost business, damaged reputations, and classaction lawsuits. It's crucial to deploy devices and solutions—like HP Managed and Enterprise printers and HP Security Manager—that can help you meet compliance requirements and protect your business information from security threats.

Get The Help You Need

HP Print Security Services provide end-to-end assistance through an initial risk assessment, recommendations, and a roadmap to build a comprehensive print security policy based on Zero Trust principles. HP creates a plan to achieve improved cyber resilience by applying the recommendations with the Implementation Service and manages your fleet compliance over time with the Governance and Compliance Service. The Retainer Service provides flexible, ongoing assistance from a credentialed HP Cybersecurity professional.

Learn more at hp.com/go/printsecurity

HP WOLF SECURITY

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

1. HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of published features as of February 2023 of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/printersecurityclaims.
2. Quocirca Print Securoty Landscape, 2023
3. Enterprise Strategy Group, Zero Trust Impact Report, 2022,
4. Fortinet, The State of Zero Trust Report, 2022.
5. Solutions may not be supported in all HP devices; solutions may require additional purchase.
6. Select HP DesignJet printers, 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 and hp.com/go/DesignJetSecurity.
7. HP Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.
8. HP Access Control Print includes Secure Pull Printing, Secure Authentication, Job Accounting, Print Policies, and Print Management. HP Access Control Scan and HP Mobile Connector are separate solutions that can be bundled. To learn more, please visit hp.com/go/hpadvance
9. Secure Development Practices Assessment Certification: The development process for the application is validated by a third party to meet stringent security standards for the development of software. This certification does not guarantee that the application is secure from internal or external attack.
10. HP Secure Print works with most network-connected printers and MFPs. On-device authentication requires HP FutureSmart firmware 4.8 or newer. Supported card readers include X3D03A (HP USB Universal Card Reader) and Y7C05A (HP HIP2 Keystroke Reader). Internet connection required. For more information, see hp.com/go/secureprint
11. HP Insights is a web-based application that requires Internet access. It is bundled with HP Secure Print and can also be purchased separately. For more information, see hp.com/go/secureprint.
12. HP Web Jetadmin is available for download at no additional charge at hp.com/go/wja.

4AA3-1295ENW, March 2024