Solution overview

Defend your network with the world's most secure printing[1]

11%

of security incidents reported by organizations over the past year were print-related[2]

59%

of organizations reported a print-related data loss incident in the past year (70% for retail)[2]

55%

of printers are behind in security patches (of over 1.2M printers evaluated by the HP firmware tool)[3]

Print infrastructure is now viewed as one of the top security risks by organizations.[2]

"HP Inc. continues to lead and shape the market for print security, testament to its extensive security heritage and technology innovation which continues to drive new industry standards."

– Quocirca, Jan 2019[2]

Recognize 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. When there are unsecured devices, 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. Plus, regulatory and legal noncompliance can result in heavy fines.

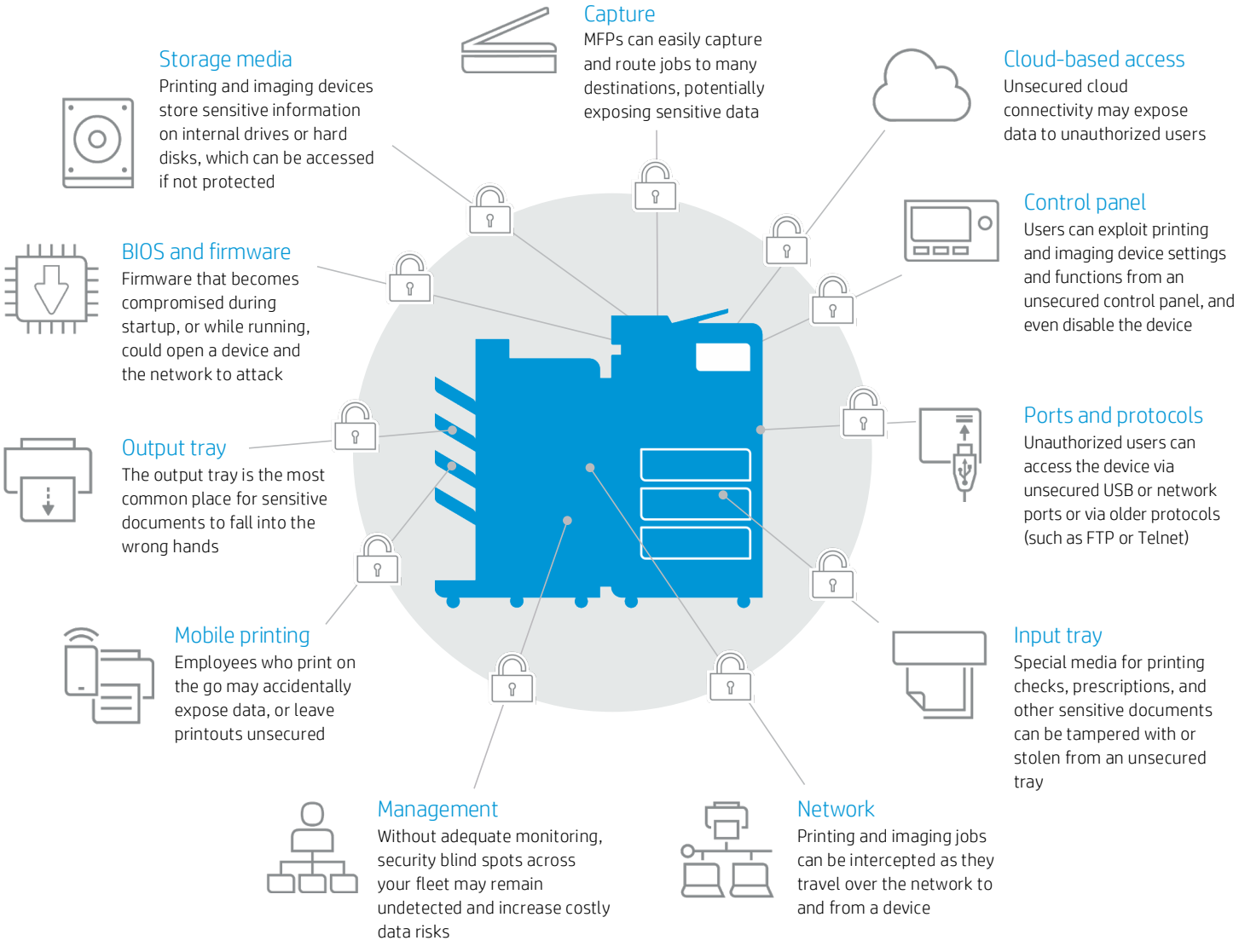
HP can help

Defend your network with the world's most secure printing.[1] HP 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.

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



Protect the device

Find out more

HP Custom Recycling Services
hp.com/go/recycle

HP Secure Managed Print Services
hp.com/go/securemps

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.[4])

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 device configuration. 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
Set unique administrator passwords so only IT staff or other authorized personnel can set up and configure device settings.

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 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

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.

HP is the first and only print vendor to earn all three Keypoint Intelligence-Buyers Lab (BLI) Security Validation Testing seals—for Device Penetration, Policy Compliance, and Firmware Resilience.

Find out more

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

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:
hp.com/go/securitymanager

Independent security validation

Help ensure printers and MFPs are safeguarded against vulnerabilities by choosing devices that have been validated to meet industry-standard security benchmarks. HP is the first and only print vendor to complete all three levels of the Keypoint Intelligence-Buyers Lab (BLI) Security Validation Testing program for MFPs and printers. HP has earned program seals for Device Penetration, Policy Compliance (using security management software), and Firmware Resilience for its FutureSmart v4+ Enterprise firmware platform for HP Enterprise and Managed printers and MFPs.

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.[1]

HP business printers, from Pro[5] through Enterprise,[1] are always on guard, continually detecting and stopping threats during all phases of operation:

- **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.
- **When loading firmware.** HP's *Whitelisting* is Common Criteria Certified and automatically checks firmware during startup to determine if it's authentic, good code—digitally signed by HP.
- **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 Enterprise devices initiate a self-healing reboot.

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

In addition to being able to detect and stop threats, HP 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 self-healing BIOS.[1] If the BIOS is compromised, HP Sure Start restarts from a safe "golden copy" of its BIOS.
- *Run-time intrusion detection* monitors complex firmware and memory operations, automatically stops the intrusion, and reboots in the event of an attack. Run-time intrusion detection is Common Criteria Certified.
- *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 Enterprise printers.[1]

HP JetAdvantage Security Manager completes the check cycle, providing dynamic fleet compliance

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 four primary steps in the cycle of an HP device.

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

HP JetAdvantage Security Manager completes the check cycle, providing dynamic, fleet-wide security compliance.

One. Check BIOS/boot code

Prevents the execution of malicious code during bootup by allowing only HP-signed, genuine code to be loaded.

Two. Check firmware

Allows only authentic, good firmware—digitally signed by HP—to be loaded.

Three. Check settings

After a reboot, HP JetAdvantage Security Manager checks and fixes any affected device security settings.

Four. 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.[4]

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*,[7] and *HP Workpath* apps, include safeguards to help protect sensitive information and address additional security and compliance issues.

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 Enterprise and Managed printers and MFPs.

Find out more

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

HP JetAdvantage Workflow Solutions
hp.com/go/documentmanagement

HP Capture and Route
hp.com/go/hpcr

HP Access Control Scan
hp.com/go/hpadvance

HP Workpath
hp.com/go/workpath

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 JetAdvantage Security Manager* makes digital certificate management easy.

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.[7] 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.

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 Roam for Business* enables users to print effortlessly from any device, virtually anywhere, to any HP Roam-enabled device, securely through the cloud.
- *HP PrinterOn Enterprise* offers dependable, secure in-network mobile printing for enterprise, along with basic management and reporting capabilities. Connect virtually any desktop or mobile device to printers from multiple vendors both on and off the trusted network.
- *HP Mobile Connector* extends *HP Access Control Print* capabilities to mobile devices.[7] 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 JetAdvantage Secure Print* 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.[9]

Controlling access—Advanced security practices

Advanced authentication (passwords, proximity cards, etc.)
HP Access Control Print improves security by integrating convenient authentication tools with existing network credentials such as LDAP and Active Directory.[7] Device access protection includes options for ID badges, PICs, or PINs.

Tracking of printed jobs from all devices, including mobile
HP JetAdvantage 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.[10] *HP Access Control Print* includes job accounting capabilities to help you accurately track and analyze device and supplies usage.[7] 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.

Find out more

HP Access Control Print
hp.com/go/hpadvance

HP Roam for Business and HP PrinterOn Enterprise
hp.com/go/businessmobileprinting

HP JetAdvantage Secure Print
hp.com/go/jetadvantagesecureprint

HP JetAdvantage Insights
hp.com/go/jetadvantageinsights

SD-PAC

HP Access Control Print, HP JetAdvantage Secure Print, HP JetAdvantage Insights, HP JetAdvantage Security Manager, and HP FutureSmart 4+ firmware have earned Secure Development Practices Assessment Certification.[8] This certification provides third-party validation that robust secure software development practices were incorporated into a product's design, development, and testing.

Protect the document

Integrate smart hardware and software solutions with your larger IT security plan to protect the sensitive information in your printed documents.[4]

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
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 JetAdvantage 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 multivendor print devices.[9] *HP Access Control Print* is a server-based solution offering enterprise-level security and management features.[7] HP Access Control Print can support multivendor fleets.

Find out more

HP Capture and Route
hp.com/go/hpcr

HP Access Control Print
hp.com/go/hpadvance

HP JetAdvantage Secure Print
hp.com/go/jetadvantagesecureprint

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.[4] Prevent protection gaps and 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*[11] 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 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 JetAdvantage Security Manager*.[6] 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.com/go/wja

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Find out more

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Advanced security practices

Quickly assess the vulnerability of device firmware across the fleet
HP JetAdvantage Security Manager provides an integrated fleet firmware vulnerability assessment feature that identifies the various degrees of firmware vulnerability across all your devices.[6] 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 JetAdvantage 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.

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 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 class-action lawsuits.

It's crucial to deploy devices and solutions—like HP Enterprise printers and HP JetAdvantage Security Manager—that can help you meet compliance requirements and protect your business information from security threats.

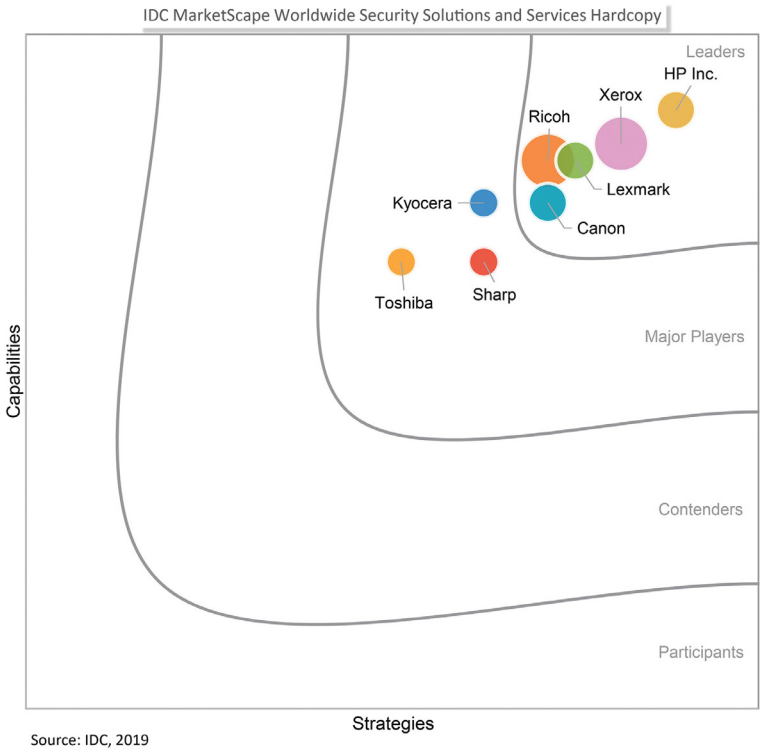
Get the help you need

With print security assessment services, you don't have to protect and secure on your own. Security experts can help you assess your print security vulnerabilities, 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.

Recognized as a leader in the industry

HP has been named a leader in the IDC MarketScape report on Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment. (See the IDC graph below; find the report here.) According to the report, "HP Inc. should be on the short list when customers are seeking a trusted partner and expert in security."[12]

IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of ICT suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market and business execution in the short-term. The Strategy score measures alignment of vendor strategies with customer requirements in a 3- to 5-year timeframe. Vendor market share is represented by the size of the icons.[12]



Source: IDC, 2019

Get started

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

Learn more
hp.com/go/printsecurity

[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 2019 published features 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 Global Print Security Study, Louella Fernandes, January 2019. For more information, see hp.com/go/analystscorner.

[3] Based on internal HP data from over 1.2 million printers evaluated using the HP firmware tool during HP Print Security customer engagements, as of April 2019.

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

[5] 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.

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

[7] 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.

[8] 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.

[9] HP JetAdvantage 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/jetadvantagesecureprint.

[10] HP JetAdvantage Insights is a web-based application that requires Internet access. It is bundled with HP JetAdvantage Secure Print and can also be purchased separately. For more information, see hp.com/go/jetadvantageinsights.

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

[12] Based on IDC review of hardcopy vendors and opinion regarding HP security leadership. SOURCE: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment, by Robert Palmer and Allison Correia , December 2019, IDC Doc #US44811119. To learn more, see idcdocserv.com/US44811119e_HP.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA3-1295ENW, May 2020, Rev. 14