The world's most secure printing[1]

11%
of security incidents reported by organisations over the past year were print-related[2]

59%
of organisations reported a print-related data loss incident in the past year (70% for retail)[2]

62%
of organisations look to their MPS provider for print management and security skills[2]

Innovative device, data, and document security to help protect your fleet

Strengthen compliance

HP devices and solutions can help your organisation comply with industry compliance and regulations such as EU General Data Protection Regulation, EU Network and Security Infrastructure Directive, PCI DSS, PCI-DSS, ISO 27001, HIPPA, US CERT recommendations, and the NIST Framework.

✓ Security controls and procedures documented and maintained for all systems

✓ Print fleet infrastructure regularly scanned for vulnerabilities and remediated

✓ Controls in place to protect systems from viruses and malicious code

✓ All sensitive information encrypted at rest and in transit

✓ Printer fleet systems reporting compliance data

Cybercrime, internal breaches, compliance infringement and more can hurt your business. In addition to expensive fines and lawsuits, a security breach can result in loss of revenue and a damaged reputation.

Although many IT departments rigorously apply security measures to computers and the network, printing and imaging devices are often overlooked. As threats continue to evolve, unsecured printers offer opportunities for attackers to compromise the device, your data, or the entire network.

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

Only HP print security offers real-time detection, automated monitoring, and built-in software validation to help stop threats the moment they start.[1] HP business printers, from Pro to Enterprise, include security features that can automatically detect and stop an attack. HP Enterprise printers then self-validate software integrity in a reboot.[1]

Stay informed by integrating printer threat event data into the major security monitoring and incident detection (SIEM) tools, such as ArcSight, Splunk, McAfee, or SIEMonster.

Automate device, data and document protections

HP JetAdvantage security solutions provide unmatched, automated print security to help protect your network, achieve compliance, and reduce the time and effort to maintain protections.

Device security. Manage security across the fleet with HP JetAdvantage Security Manager.[3] Establish a fleet-wide security policy, automate device remediation, and install and renew unique certificates while getting the reports you need to prove compliance.

Data security. Help protect data to and from the device with data encryption and authentication solutions. Extend these protections to mobile devices with HP Roam for Business or the business-class management features of HP PrinterOn Enterprise.

Document security. Reduce unclaimed print jobs, protect confidential documents and improve efficiency with an HP pull print solution. And, for certain sensitive document printing, consider HP counterfeit deterrent solutions.

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.

Figure 1. 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 utilises 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.[4]
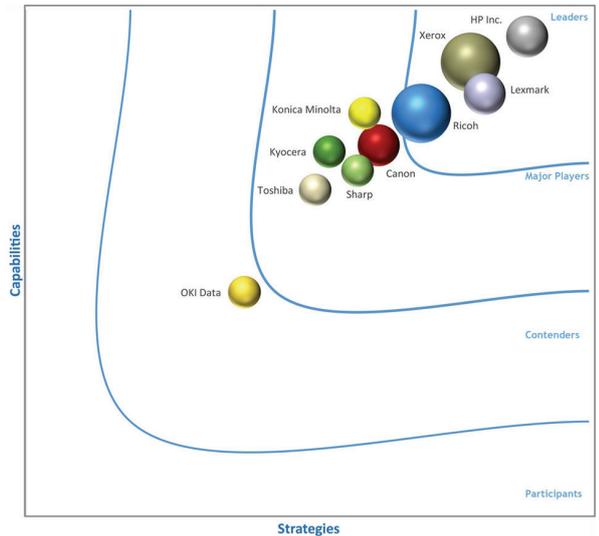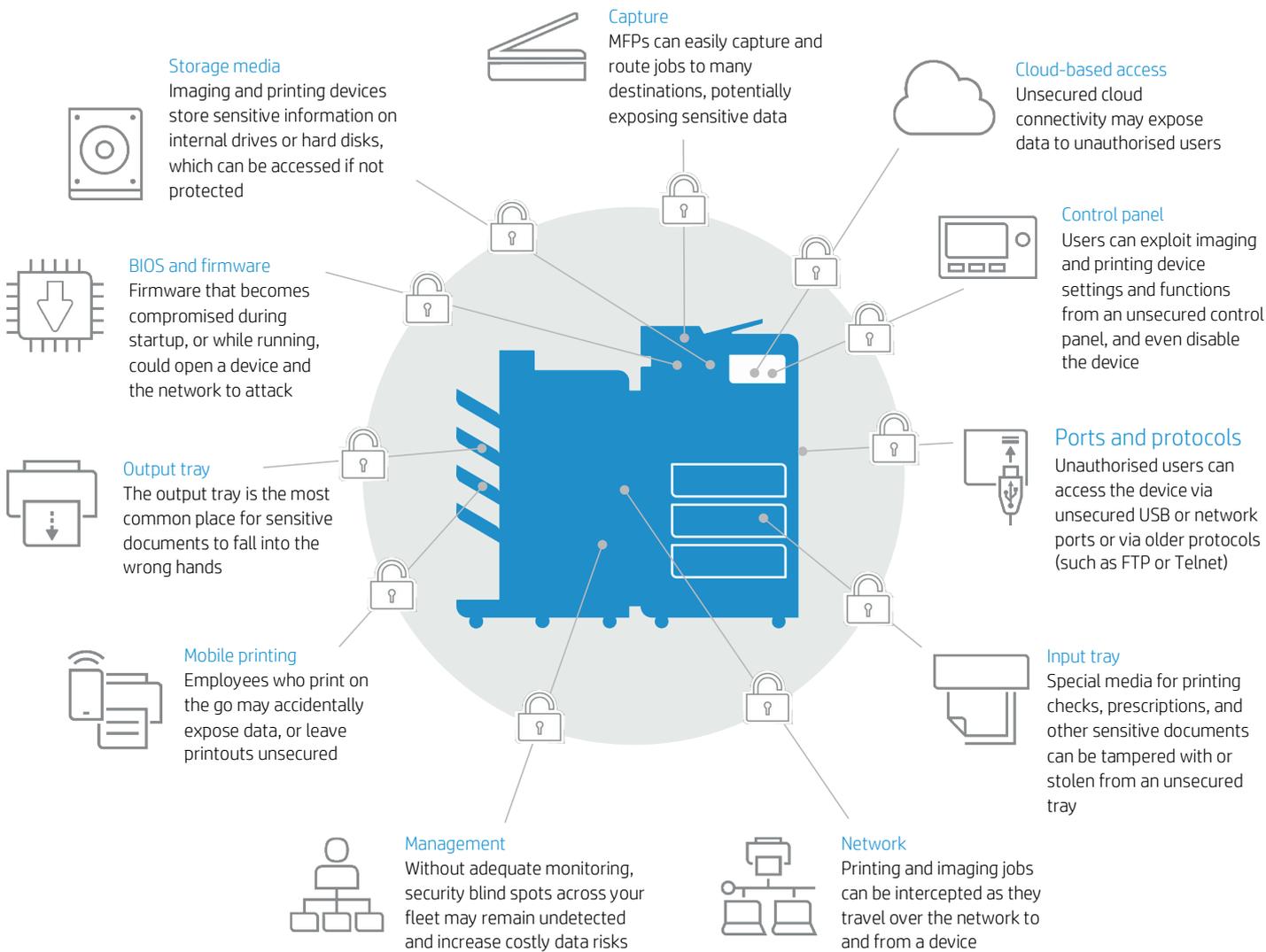
Recognised as a leader in the industry

HP has been named a leader in the first IDC MarketScape report on Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment.[4] (Find the report here.) According to the report, "HP Inc.'s approach to security takes the entire print and document infrastructure into account, beginning with locking down the device and extending into all aspects of device usage and content protection."

HP devices and solutions can help close the security gap

Critical gaps can occur at multiple points within your environment. Creating a complete imaging and printing security strategy requires coordinated protection of devices, data, and documents, plus comprehensive security monitoring and reporting solutions.

Figure 2. Imaging and printing vulnerability points

Storage media
Imaging and printing devices store sensitive information on internal drives or hard disks, which can be accessed if not protected

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

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

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

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

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

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

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

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

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

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

Help protect your business

HP offers the world's most secure printing, with devices that can self-heal after an attack.[1] (For details, see hp.com/go/PrintersThatProtect.) But printing and imaging security isn't only about device security. It's about comprehensive strategy that includes solutions to help secure data and documents, plus visibility and reporting to optimise your environment and help meet compliance regulations.

Protect the device

- Self-healing security features
- Upgradeable firmware
- Automated monitoring and remediation of device settings (HP JetAdvantage Security Manager)
- Print data integration with incident detection tools

Protect the data

- Encryption in transit and at rest
- Advanced authentication and access control (HP Access Control)
- Secure mobile printing solutions (HP Roam for Business, HP PrinterOn Enterprise)
- Customised compliant data recycling

Protect the document

- Secure pull printing solutions (HP JetAdvantage Secure Print, HP Access Control)
- Fraud and counterfeit deterrent solutions (HP and TROY Secure Document Printing)

Planning and reporting

- Advanced reporting
- Compliance support (HP JetAdvantage Security Manager)
- Help assessing risk and creating a print security plan

When you choose HP devices and solutions, you help protect your devices, data and documents with the world's most secure printing.[1]

Learn more
hp.com/go/SecurePrinting

Sign up for updates
hp.com/go/getupdated

Share with colleagues