HP Managed Print Services
Topic of Influence: Security

February 2020

Introduction

Organisations are looking for more than just somebody to take care of their office printing needs. They want a partner who can look at their environment and processes more holistically and support the onsite and offsite printing needs of all their departments, from legal and accounting to marketing and engineering. Essentially, companies are shifting from a product-based to an outcome-based approach.

The Topics of Influence series covers the significant factors driving the agenda. In this brochure, discover how HP invests in the future to create long-term value for our clients.
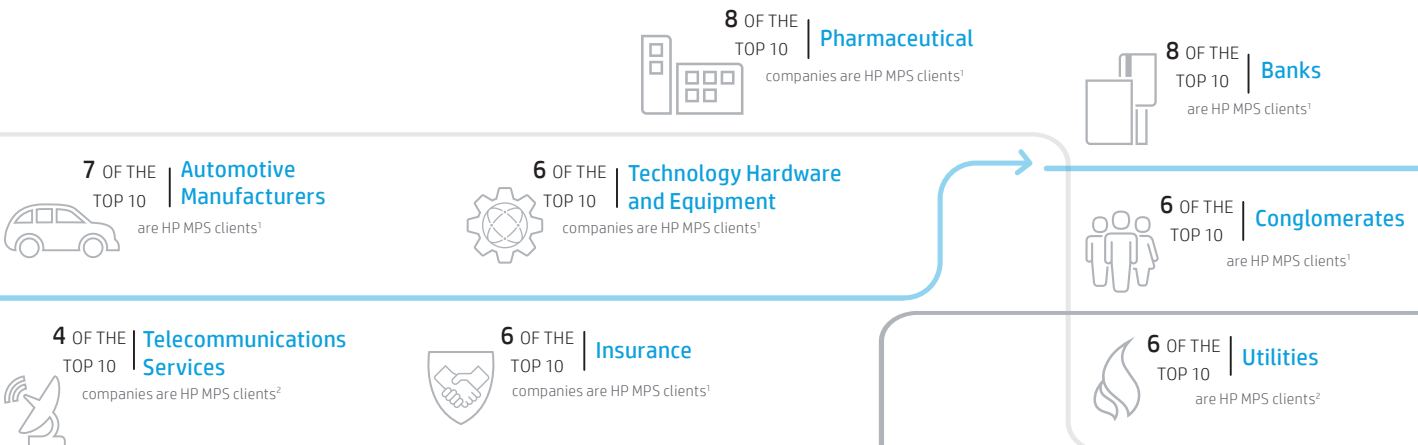
Other topics of influence include the following (for details, click the name to open the brochure for that topic):

- **Diversity.** Helping your organisation realise the benefits of diversity and inclusion as a business value.

- **Doing good in communities.** Discover how HP employees contribute to communities around the world to create a brighter future for all.

- **Financial strength.** Investing our healthy profits in high-quality, innovative products and solutions to improve your business.

- **Global.** Harnessing technology internationally and optimising its use to reduce operational costs.

- **Mobility.** Implementing a strategy that works for your organisation as it adjusts to changing processes around paper, devices, and the workplace.

- **Service and Delivery.** Ensuring quality, predictability, and reliability with a seamless transition.

- **Sustainability.** Providing the services, products, and solutions to help you optimise resource use and recycling.

- **Vision.** Continually reinventing our company and our technologies so that industries, communities, and individuals can keep creating what matters most to them.

- **Workflow.** Working collaboratively to drive process efficiencies in document capture and digitisation.

- **Workplace.** Transforming your organisation to deliver an efficient work environment for the future.

HP has the most flexible, comprehensive, and scalable offering in the industry. HP Managed Print Services (MPS) is a comprehensive suite of hardware, software, and services delivered in a consultative engagement. With global expertise, we leverage our experience to help you meet business outcomes.

Read how HP, as your global, innovative, and strategic partner, is ready to work with you to create solutions that meet your unique needs and help position you at the forefront of your industry.

8 OF THE TOP 10 | **Pharmaceutical**
companies are HP MPS clients[1]

8 OF THE TOP 10 | **Banks**
are HP MPS clients[1]

7 OF THE TOP 10 | **Automotive Manufacturers**
are HP MPS clients[1]

6 OF THE TOP 10 | **Technology Hardware and Equipment**
companies are HP MPS clients[1]

6 OF THE TOP 10 | **Conglomerates**
are HP MPS clients[1]

4 OF THE TOP 10 | **Telecommunications Services**
companies are HP MPS clients[2]

6 OF THE TOP 10 | **Insurance**
companies are HP MPS clients[1]

6 OF THE TOP 10 | **Utilities**
are HP MPS clients[2]

1 Claims based on Forbes 2018 – Global 2000 World's Leading Companies, published June 6, 2018; HP Internal Data.
2 Claims based on Fortune 2018 – Global 500, published July 19, 2018; HP Internal Data.

Security

Enter PIN,

Current situation

HP has an industry-leading position in print security, a compelling range of services and solutions, and helping to consistently evolve the best security practices and standards across the industry.[3]

Cybersecurity has become one of the most urgent and complicated issues facing businesses of all sizes today. As the volume and complexity of these attacks continues to grow, businesses are trying to keep pace with the latest policies and technologies that will help protect against the crippling and costly effects of a data security breach or cybersecurity attack.[4]

Your organisation is continuously creating confidential, valuable data that's crucial to operations. And you're probably using multiple security methods— including authentication, encryption, and monitoring—to protect this data on your networks, PCs, and servers. But is your printing and imaging environment as secure as the rest of your infrastructure? The security exposure and associated costs can be high, whether it's from unattended documents on a printer, sensitive data processing from the computer to the device, or confidential information on device hard drives. To help keep your organisation protected, you need a solution that simplifies and strengthens security throughout your printing and imaging environment, saving you time and money that can be better spent elsewhere.

In today's business environment, IT security spending has never been higher. Yet major breaches seem to occur almost weekly, and the time and cost to respond can leave you lagging behind. Especially when faced with the increasing number of security regulations in every industry. With the average cost to resolve a cybercrime incident at $9.5 million, it's crucial not only to protect every vulnerability but also to use improved security to drive business performance.[3]

Key security insights for shared printing environments

- Unsecured printers can open the network to attack

- Users can change device settings, access data, or send scanned documents anywhere

- Too many confidential print jobs get left uncollected

- Security breaches can be costly, especially if customer data is compromised

- Mobile workers need to print wherever they are— without sacrificing security

- IT needs tools to manage security across the fleet more efficiently

3 Managed Print Services Landscape, Louella Fernandes, December 2019
4 HP Wins BLI/Keypoint Intelligence Pacesetter Award for Security, Shivaun Albright, Chief Technologist of Printing Security & Solutions, December 2019
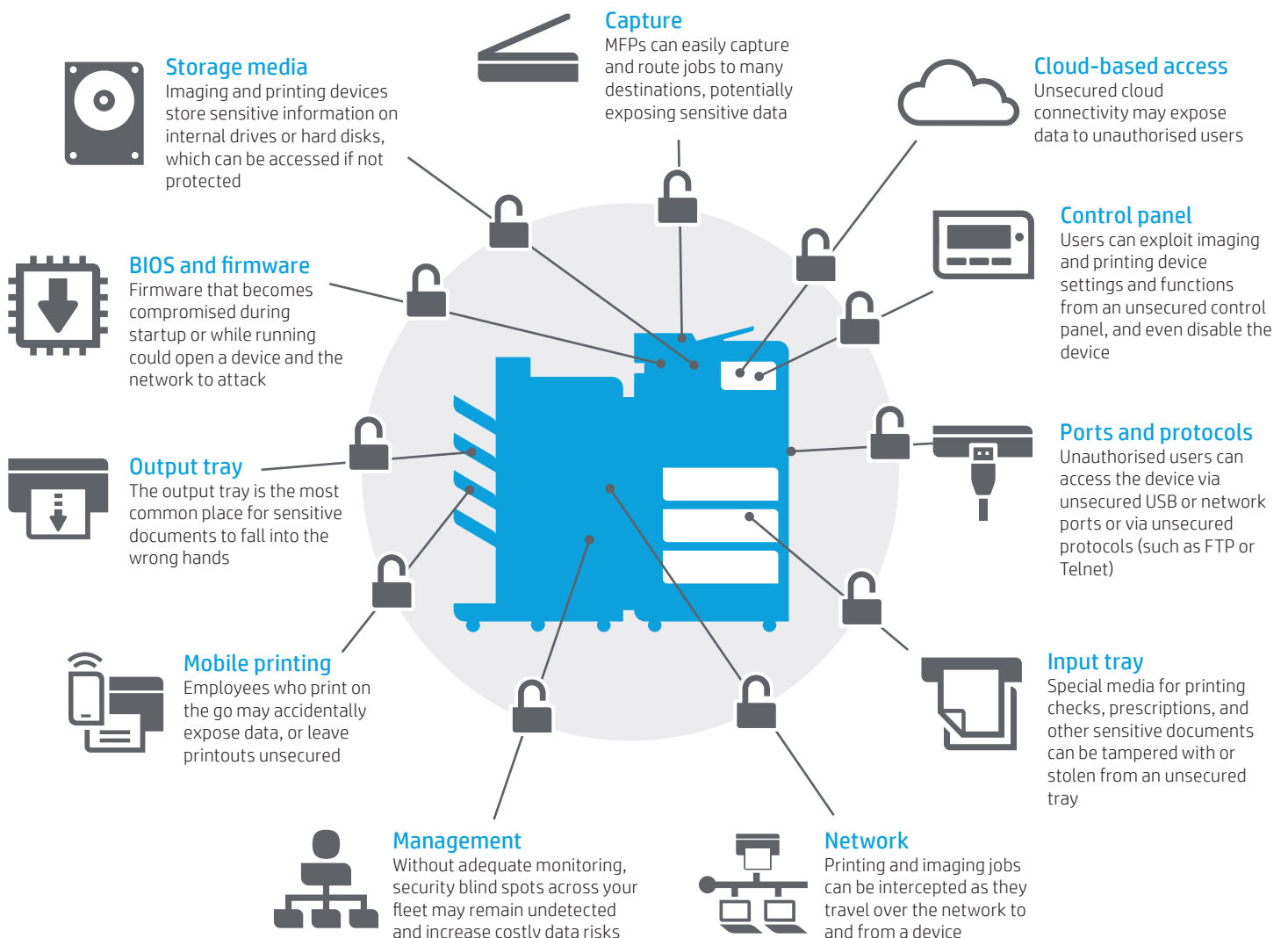5 Ninth Annual Cost of Cybercrime Study, Accenture, March 2019.

Challenges facing clients

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

Today, organisations have strong security policies in place to secure computing network endpoints, but many have overlooked their print infrastructure. Integrating printing and imaging security needs into a larger IT security strategy has never been more important. 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.

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 unsecured 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

Current situation

63% of IT decision makers say that security is the most important area of investment for their organization between now and 2025.[6]

54% of IT decision makers say that the ability to provide security expertise, services and solutions will be an important supplier selection criterion by 2025.[6]

Lawmakers across the European Union have been aware of the threat to personal information for many years with the first directive on Data Protection dating back to 1995 (Directive 95/46/EC). In recent years, the massive growth of online content, and the growing online threat to physical things including the national critical infrastructure of the member states, has resulted in the ratification of two information security directives in late 2015.

The EU General Data Protection Regulation (GDPR), which became effective on 17 December 2015, updates the 1995 Directive and gives more power and independence to the Data Protection Commissioners of each of the member states. The Netherlands was one of the first countries to implement this into national law with the Breach Notification Act of 1st January 2016. Organisations in the Netherlands who incur a data breach involving personal information must report the breach and demonstrate that they have carried out risk analysis and implemented an appropriate level of security based upon the level of risk.

The second piece of legislation released was the EU Network and Information Security (NIS) Directive, which became effective on 13 December 2015. Germany actually implemented this law ahead of ratification in the form of the Federal IT Security Act in July 2015. Operators of national critical infrastructure are expected to meet four requirements, with risk analysis again central to the process. HP can help our clients meet the regulatory requirements for both the Dutch Breach Notification Act and the German IT Security Act with our Security Advisory Services. The law in Germany is particularly stringent in that it expects operators of National Critical Infrastructure to report Critical Risks before any breach has occurred.

As well as legal regulation, there are many industry-specific security standards and general information security standards, most notably ISO27001. This standard started life as British Standard BS7799, and was fully adopted by the International Standards Organization in 2005. As Security Risk Analysis, Security Risk Management, and the establishment of Security Controls are central to the standard, working to the standard can be used by organisations to demonstrate compliance with the law. HP has a service for this, namely our Security Advisory Service, which is built upon the controls in Annex A of ISO27001:2013.

6   Quocirca's Print 2025 Report, Second Edition, 2019.

Vision

HP Inc. is positioned as a **Leader** in the 2019-2020 IDC MarketScape for print and document security solutions and services worldwide.[7]

HP Inc.'s legacy of **print security innovation** combined with the company's ability to leverage and share security technologies across its print and PC business is also a considerable strength.[7]

Security remains a **priority** for HP Inc., serving as the foundation for its approach to the market and the backbone for its Secure MPS strategy.[7]

HP Inc. should be on the short list when customers are seeking a **trusted partner** and **expert** in security, with the ability to monitor and manage print security compliance as part of a broader IT security program or corporate governance initiative.[7]

Printing and imaging security isn't only about protecting devices, data, and documents. It's also about understanding how an organisation can implement an effective print security policy and proactively monitor and manage it. More importantly, it's about building security from the ground up—considering industry policies, rules, and guidelines and developing the right solution for every organisation.

HP Secure MPS security consultants work with you to:

- Assess your print security vulnerabilities

- Build a comprehensive print security policy based on business needs and best practices

- Identify and implement solution recommendations to achieve and maintain improved security within your unique environment

HP Secure MPS can also help your organisation comply with industry legal and regulatory requirements, such as:

- 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

7   IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment.

HP MPS capabilities

HP Managed Print Services combines an optimised set of hardware, software, and services to help organisations harness the power of improved security in printing and imaging environments. Leveraging more than 50 years of experience in security and industry standards, HP is a leader in understanding the needs of unique print environments. Taking this knowledge, HP MPS can help build the best comprehensive security policy for specific clients.

Since security is mission-critical, HP Secure MPS provides the advanced protections you need with the most comprehensive device, data, and document security. Plus, we provide the expertise to help you develop and deploy your print security strategy and then maintain your print environment over time.

HP can help provide leading end-to-end print security through our comprehensive HP JetAdvantage Security portfolio of printer features, solutions, and services.

Device security

Embedded features and add-on solutions can help you defend your printers and reinforce simple but effective security habits.

- Multi-level, built-in features help protect your printer against complex security threats from boot up to shut down. HP Sure Start securely boots the device, whitelisting validates the integrity of the firmware code, and run-time intrusion detection continually guards against attacks.

- 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.

- Choose devices certified as compliant with internationally recognised security standards. Ensure device updates are code signed to confirm authenticity and integrity of the code.

- 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.

Access control

- Require authentication for access to device settings and functions to reduce potential security breaches.

- Require users to sign in using a variety of methods, including PIN, LDAP, or Kerberos authentication.

- Enable administrative access controls, so critical device settings can't be tampered with. Role-based access controls allow you to give different capabilities to different types of users depending on their needs.

- HP Access Control Secure Authentication offers advanced authentication options, including touch-to-authenticate with NFC-enabled mobile devices.

- HP offers additional authentication solutions such as HP SmartCard Solutions for US Government or biometric solutions.

Network security

Don't allow your printers to compromise your network security.

- Protect your network and documents by using a variety of encryption options to secure communication to and from the device:

  - 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®.

  - 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's Embedded Web Server administration interface can be securely encrypted.

- Firewall settings and unique device identity certificates help protect your network.

Data protection

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

- HP devices come with built-in encryption to help protect sensitive business information stored on hard drives.

- Use built-in device capabilities to securely overwrite stored data, and safely remove sensitive information.

- 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 a variety of features and solutions for secure mobile printing.

- 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.

- At end of device life, HP Custom Recycling Services can ensure data is eliminated from hard drives before responsibly recycling old products.

Document security

Integrate smart hardware and software solutions with your larger IT security plan to protect the thousands of documents printed organisation-wide every day.

- Pull printing stores print jobs on a protected server, in the cloud, or on your PC. Users identify themselves with a PIN or other verification method at their chosen print location to pull and print their jobs. These security measures also eliminate unclaimed prints, which can reduce cost and waste.

  – HP Access Control Secure Pull Printing is a robust server-based solution that offers multiple forms of authentication including badge release, as well as enterprise-level security, management, and scalability.

  – HP JetAdvantage Private Print is a cloud-based solution that delivers the advantages of pull print, without the complexity. It is simple to set up and does not require a server, installation, or maintenance.

- Equip your printers and MFPs with secure input trays to prevent theft of special paper used for printing checks, prescriptions, or other sensitive documents.

- Anti-counterfeiting solutions, such as HP and TROY Secure Document Printing, 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.

Monitoring and management

With so many security settings to track, IT can easily feel overwhelmed. Security monitoring and management solutions can help you identify vulnerabilities and establish a unified, policy-based approach to protecting data, strengthening compliance, and reducing risk—all while saving significant time and resources.

- HP's automation monitoring and remediation of device settings is the most comprehensive printing security solution in the market, offering an effective, policy-based approach to securing printing and imaging devices. Reduce cost and resources to maintain fleet security by using automated monitoring and security, which automatically adds and configures new devices. It also provides efficient fleet management of unique identity certificates.

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

Keypoint Intelligence awarded HP the BLI PaceSetter award for Security in the Imaging Technology Leadership category. This award recognizes the document imaging OEM with the most comprehensive offerings and programs when it comes to print-environment ecosystems.

HP JetAdvantage Security Manager 3 was also awarded a Pick and Outstanding Achievement Award for Outstanding Security Compliance. These coveted honors recognize the most impressive solutions evaluated by Buyers Lab during the previous 12-month test cycle.

According to Keypoint Intelligence, "HP JetAdvantage Security Manager is a unique solution that centralizes and automates the process of bringing and keeping output devices in compliance with an organization's preferred security policies."[8]

- Ensure uncompromised device firmware to make it easy for IT to apply the latest security improvements across the fleet.

- HP's job accounting and auditing helps you gain control of your printing environment and costs. Monitor, allocate, and manage resources by tracking usage by device (HP or non-HP), user, project, department, and cost centre. Collect data and analyse the results to identify saving opportunities. Streamline imaging and printing practices by ensuring the right device is in the right place and used for the right job.

Print security services

Lean on the leader in IT security and print management, saving you time, costs, and resources while improving your overall security posture.

- Need help getting started? HP Printing Security Advisory Services will work with you to engage stakeholders, assess the current state of your security, develop a cohesive security strategy, and recommend solutions to protect your organisation.

- HP Managed Print Services is a suite of scalable and flexible solutions that can help you get the most out of your imaging and printing environment, and we work with you to tailor the right approach to meet your needs. This could be anything from providing you with the tools to manage the environment yourself, to a completely outsourced solution.

8   HP Wins BLI/Keypoint Intelligence Pacesetter Award for Security, Shivaun Albright, Chief Technologist of Printing Security & Solutions, December 2019.

Case study: HP's global MPS expertise in action

In 2016, an international bank, with over 7,500 offices based in 70 countries worldwide, and 35,000 printers, engaged HP to carry out Security Advisory Services.

Problem

- Client wanted to achieve a better view of the security risk posture of their printer fleet

"It's great. It's a good report, and it gives us a lot to think about."

"It's more than I expected… the risk grading has saved us a job."

Feedback from the client

HP solution

- Carry out a pre-onsite analysis for two weeks before visiting the client

- Install a trial version of HP Security Manager software on a client test server

- Perform onsite analysis over three days, covering extended printing infrastructure, including databases, servers, and workflows

- Produce final report and publish recommendations three weeks later

Results

- Client received a very clear view of the security configuration of its devices and how it varied from region to region

- Client saw how effective HP Security Manager software is in greatly reducing the risk of its infrastructure

- The analysis led the client to see more security functionality in its existing HP Capture and Route software, which could be utilised to mitigate an existing internal audit finding

- The client is now considering VPSX software, which is an HP partner software, for further reducing risk around its core banking system

- The HP account team was able to identify some simple changes to the process, which enhanced the security of the service being delivered to the client

Why HP?

HP MPS is an industry leader when it comes to security. We are uniquely positioned to provide you with end-to-end security solutions. While many of our peers focus on security products, they cannot provide the consulting or management services that you often need. By providing services at every step of the security journey—education, onsite workshops and risk assessments, and solution delivery—HP MPS can engage with your security and IT teams in entirely new ways to optimise, manage, and improve security in your printing and imaging environment.

When you engage HP Printing Security Advisory Services, you can expect comprehensive risk analysis, recommendations, and guidance to improve your security environment:

- An HP security advisor will work with your security and IT team to review your current environment to better understand your organisation's concerns, practices, and vulnerabilities.

- A security workshop will bring together key stakeholders, educate them on threats, and help them reach consensus on the goals of a new printing security strategy—one that strikes the right balance between security, cost, and ease of use.

- Security advisors gather detailed information and interview employees about daily printing and imaging practices.

- Your advisor can also deploy HP JetAdvantage tools such as HP Web Jetadmin and HP JetAdvantage Security Manager to evaluate your current printing security posture against regulatory requirements and industry best practices.

- Armed with the qualitative and quantitative data gained during the security assessment, your HP security advisor will help you identify risks, estimate their potential impact, and present you with recommendations to secure your printing environment.

Our commitment

HP offers superior protection for your print environment, providing the latest security technologies and processes for the advanced management of devices, data, and documents. With HP, you have our commitment to not only securing your print fleets and documents today, but also proactively maintaining your security status against the ever-changing threat landscape and evolving compliance requirements.

KeyPoint
Intelligence awards[9]

HP serves
6,600
enterprise clients

Leader
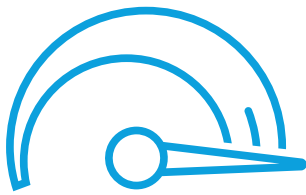for print and document security solutions and services[10]
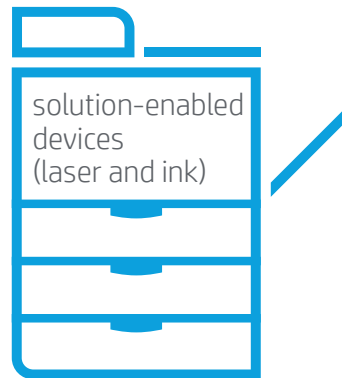
37 billion
annual pages under an HP MPS contract

HP remains an **MPS leader** – Quocirca[11]

#11
of best-managed companies[12]

HP manages **1 million**
solution-enabled devices (laser and ink)

HP is an **MPS market leader** – IDC[13]

9   HP has received awards in the healthcare, education, retail, financial services, security and mobility categories, as well as numerous product awards.
10   IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment (#US44811119), December 2019.
11   Quocirca, Managed Print Services Landscape, 2019; Louella Fernandes, December 2019.
12   The Wall Street Journal, 2019.
13   "IDC MarketScape: Contractual Print and Document Services Hardcopy Vendor Assessment" (#US44387318), December 2018.