Secure Print Analysis
Assess your printer security strategy
Are your printers vulnerable to attack?

It’s time to find out

“An unsecured multifunction printer is a prime target for hacking into the enterprise.”

Angele Boyd, IDC Analyst Connection

Today’s multifunction printer does more than simply print. It scans, sends and stores potentially sensitive information. Innovations surrounding networked printers help streamline business processes and increase productivity. At the same time, implementing those additional features may leave your fleet vulnerable to attack. If your printer fleet connects like your computer fleet connects, it should be protected in the same way.

The HP Secure Print Analysis Tool will reveal the range of printer security options now available, and offer guidance on how you can calibrate your strategy accordingly against six printer security categories. Take the assessment to quickly evaluate your printer security practices and capabilities. Find out where you’re doing well, and where you may be falling short. It’s quick and easy.

When you’re done, you’ll receive a summary of your current printer security practices, and recommendations on what you should do next.

90% of enterprises say they have suffered at least one data loss through unsecured printing.1

1 “HP: Protecting printers with enterprise-grade security,” Moor Insights & Strategy, 2014

The six printer security hot spots

- **Network security features & standards**
  Multifunction printers have hard drives and network access. They can be hacked like computers and be an entry point for malware and viruses.

- **Mobile print security**
  In the absence of a user-friendly mobile device strategy, employees may implement workarounds that could violate established security policies.

- **User authentication & access control**
  Without requiring user credentials, it’s possible for sensitive documents to be retrieved by any user. Anyone who can access printer settings can exploit permissions.

- **Document security**
  Output trays are an easy way for sensitive data to fall into the wrong hands. Unprotected input trays could lead to special paper—like check stock—being stolen.

- **Fleet management**
  Lack of central control of printers can lead to inefficient, incomplete, and time intensive efforts by IT to establish and maintain security settings on printers.

- **Printer hard drive security**
  Printing and imaging devices store user credentials and other sensitive data that can be accessed if it’s not encrypted or periodically erased.

Start now

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.
Network security features & standards

Which of the following network printing features, standards and security measures has your organization applied?

- [ ] 802.1x or IPsec network standard to encrypt data between computing devices and networked printers
  
  Apply the 802.1x or IPsec network standards to encrypt data in transit. Encryption makes files nearly impossible to read if intercepted.

- [ ] Set administrative passwords to change multifunction printer settings

  It is highly recommended that your organization apply administrative passwords to lock down the multifunction printer control panel, as well as use SNMP passwords to manage networked devices.

- [ ] Apply digital certificates or encryption keys to printers and other network endpoints

  Save time by using a printer fleet management tool to automatically apply digital certificates to network printers and multifunction printers.

- [ ] Only purchase printers with encrypted hard disks

  Choose print devices with encrypted hard disks or deploy disk erase solutions to remove sensitive data.

- [x] None of the above / Unknown

Next question
It’s time to think differently about your printers

Explore the following resources to fortify your printer security strategy.

Audit your printer security strategy and identify the solutions that make sense. Learn about **HP Printing Security Advisory Services**

Partner with HP’s global network of printing and imaging experts to optimize your printing and digital workflow. Explore **HP Managed Print Services**

Learn how to reduce IT costs and enhance employee productivity through centralized printer fleet management. Discover **HP JetAdvantage solutions for fleet management**

Deploy a single security policy across your entire printer fleet, and monitor each device for non-compliance. Check out **HP JetAdvantage Security Manager**

Discover more about HP printing solutions at [hp.com/go/printsolutions](http://hp.com/go/printsolutions) or contact your HP representative.

“Less than 20% of respondents perceive their printers to be at moderate or high risk for security breaches.”
Spiceworks Voice of IT Survey²

² Spiceworks survey of 107 IT pros at companies with 250 or more employees in North America, Europe, Middle East and Africa (EMEA), and Asia Pacific and China (APAC), conducted on behalf of HP, January 2015.