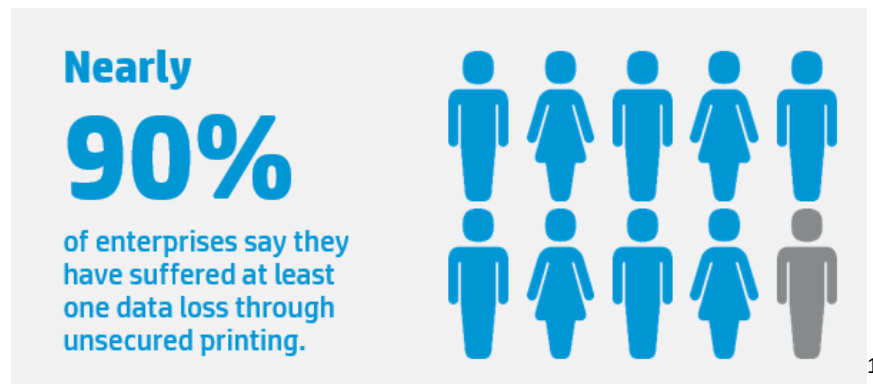


HP: PROTECTING PRINTERS WITH ENTERPRISE-GRADE SECURITY

EXECUTIVE SUMMARY



In today's Internet of Things (IoT) environment, security is not only critical, it's essential. Newly connected IoT devices such as thermostats, vending machines, HDTV's and wearables create some of the largest potential security gaps in the IT infrastructure. As users demand mobility, cloud-based applications and collaboration, both inside and outside their company or organizations firewalls, the threat of a malicious attack or industrial espionage is around every corner.

Moor Insights & Strategy (MI&S) believes that printing is an often overlooked segment of [IoT](#) that has great potential risks. Documents that are printed are generally time sensitive, high priority and important, making them essential to secure. We also believe that HP holds a leadership position in both global security services, and the hardcopy peripheral market, with the LaserJet line of printers and multi-function devices. As a leader in both these segments HP has the ability to provide integrated security not just for their printers, but across the entire organizational spectrum including servers, storage, networking, personal computers, and tablets. This breadth of software, hardware and services is what makes HP unique in the security market.

The recent addition of key new offerings including the HP Printing Security Advisory Services, as well as an upgrade to the HP Imaging and Printing Security Center

¹ Managed Print Services Landscape, 2014" Quocirca June 2014.

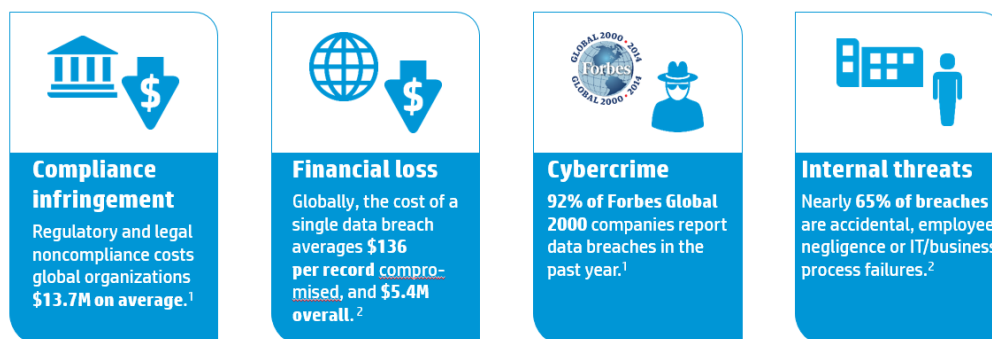
Software allow HP to expand their printing security leadership by providing organizations with the ability to audit, plan and deploy secure print policies that will allow them to both avoid accidental breaches and defend their environments against malicious attacks.

We also believe, based on HP's security investments across PC, server, networking, storage, and software business units, HP printers and printing services can offer a time-to-market advantage with the latest security innovations.

THE RISK OF LAX PRINTING SECURITY

Security breaches have become almost commonplace in today's business news. On December 19, 2013 Target Corporation released information of a massive data breach that entered the POS environment via the HVAC system compromising 40 million credit card and debit card accounts. That breach not only cost the CEO and CIO their respective jobs, but fourth-quarter profit fell 46 percent on a revenue decline of 5.3 percent, as the breach scared off customers, and the expected lawsuits could hit harder. More recently Home Depot has disclosed a data breach at it's US and Canada stores that may be the largest in history.

IoT security breaches are just beginning to appear as new devices are being connected to the internet at a rapid rate. The first recorded large IoT breach was found by Proofpoint and included a variety of compromised gadgets — everything from routers and smart televisions to at least one smart refrigerator. This hack sent more than 750,000 malicious emails to targets between December 26, 2013 and January 6, 2014.



2

² ¹ Ponemon Institute, "Mega Trends in Cyber Security Expert Opinion Study," May 2013; ² Ponemon 2013 Cost of a Data Breach: Global Analysis, May 2013

MI&S believes that of the many IoT connections in the business environment, printer security is a large potential hole in today's security systems. Print documents are often timely and proprietary, which make them a giant target. The risks associated with sharing or losing this data could be massive. Organizations that ignore security risk non-compliance and regulatory issues, financial liabilities and losses, data breaches, and malicious internal threats. The following provide two actual examples of printer based security breaches:

INSIDER TRADING BASED ON INFO PRINTED BY SOMEONE ELSE

- An employee of an investment bank read what his colleagues were printing on a shared printer by his desk. The printouts contained data about upcoming mergers and investment decisions. The employee used the information for his own trading, without ever removing the print jobs from the printer, and he made roughly \$7M. The bank was fined for insider trading, and the employee was sent to prison for several years.

MISUSE OF PATIENT RECORDS

- At the Palisades Medical Center in North Bergen, N.J a nurse printed George Clooney's confidential medical records to the wrong printer on a different floor. The nurse then reprinted it on the correct printer without collecting the original print. Another nurse collected the output that had gone to the wrong printer, and proceeded to make copies and distribute to others. The actions resulted in 27 nurses being suspended for one month.

Both of these examples could have been avoided by a secure print environment.

NOT YOUR FATHER'S OLD PRINTER – NOT THE SAME OLD USE MODEL - NOT THE SAME OLD SECURITY



Flow M525



Color
Flow M575



OJ Ent Color
Flow M585



Flow M630



Color
Flow M680



Flow M855



Color Flow M880

As the definition of printer has changed from “just a printer” to a highly-functional networked printer/scanner with both cloud and local storage, the potential damage of unauthorized use of the Multi-Function Printer (MFP) has become a major threat to organizational security. The addition of features and functions has made the printer more like a PC or server than legacy printers. Today’s printers may include:

- PC-class processor running a Windows or Linux operating system
- Internal storage
- Display
- Scanner
- Network (wired and wireless)
- Mobile access
- Cloud based access
- Integrated HTML-based browser and email client

Not only have MFPs gone through a hardware change, but MFPs are now enablers to corporate and business processes with capture and workflow, allowing business to seamlessly move from paper to digital and back. MI&S believes that these changes require organizations to promote these devices to “equal citizens” on the network, and secure them like any other device. And the process to do so must be easy and cost effective to deploy...just like securing PCs, laptops, smartphones, etc.

PRINTER SECURITY: THE HP BIG PICTURE

HP JetAdvantage Security Portfolio

End to end print security



24 © 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



The HP JetAdvantage security solutions portfolio provides a holistic approach to securing devices, data and documents throughout the enterprise. HP provides solutions to address these key areas:

- Network Security
- Data Protection
 - HP Secure Content Management and Monitoring
- Access Control
- Device Security
- Monitoring and Management
 - HP Printing Security Advisory Services
 - HP ArcSight SIEM Printer Integration
 - HP Imaging and Printing Security Center (IPSC)
- Document Security
 - HP JetAdvantage Pull Print

This report is focused on evaluating HP printer security, as such we will focus on what's new in the Data Protection, Monitoring and Management and Document Security sections.

HP PRINTING SECURITY ADVISORY SERVICES



HP has introduced what they call the HP Printing Security Advisory Services (PSAS). HP security consultants will help organizations audit their existing printer security status, provide education on their current security status and risk, provide information on best practices, and assist them in developing a comprehensive security policy and plan.

MI&S believes that having the ability to provide seasoned security consultants to assist corporations to protect their vital assets is a strong differentiator for HP. First, it allows HP to leverage their large security customer knowledge base across all their clients (and potential clients). This allows them to continue to develop not only a growing database of best practices, but to continue to develop future solutions that better meet customers needs. . Second, auditing organization's existing infrastructure gives them a broad view of existing hardware and software, providing plenty of opportunity to not only recommend HP software and hardware (where appropriate) but also to identify other existing equipment that doesn't offer the same level of security. Clearly PSAS provides HP not only the ability to continually increase their security knowledge, but also to provide more secure environments for clients and have a competitive advantage.

HP ARCSIGHT SECURITY INFORMATION & EVENT MANAGEMENT PRINTER INTEGRATION & HP SECURE CONTENT MANAGEMENT & MONITORING

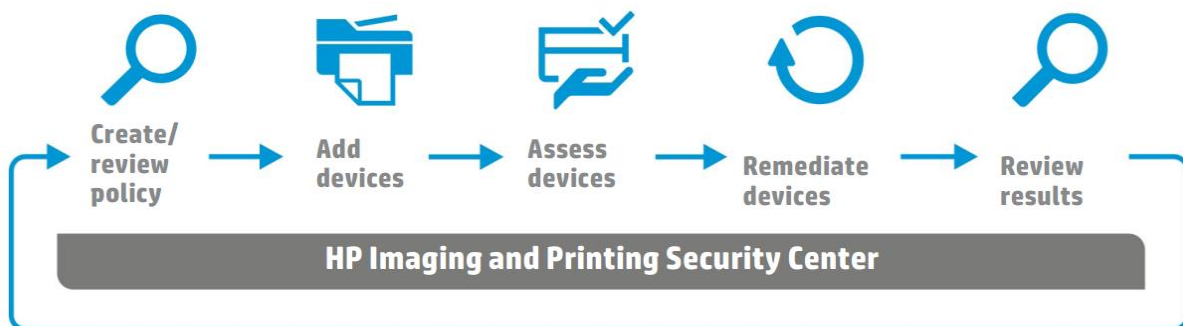
Leveraging their strength across the entire hardware and software lines, HP has aggressively integrated MFPs into the overall IT security ecosystem. MI&S believes that this overall integration provides HP with a significant advantage over competing offerings.

First, HP has integrated printer monitoring in with their ArcSight Security Information and Event Management (SIEM) tool. This allows organizations to monitor in real-time the entire IT infrastructure including printer security.

Second, HP has integrated print device content into their Enterprise Content Management (ECM solution), HP Autonomy. This integration allows HP to improve compliance and records management by extending the offering to the print environment.

HP is applying a holistic approach to security, integrating software and hardware offerings to strengthen the overall system and increase their value to organizations. A single source of monitoring allows corporations to leverage existing resources, reduces costs and reduce chances of non-compliance.

HP IMAGING AND PRINTING SECURITY CENTER 2.1



The HP Imaging and Printing Security Center (IPSC) software is the heart of HP's printer security strategy. IPSC has the ability to provide a cost effective method of managing security for any organization's HP fleet. MI&S believes the key to the

IPSC system is the consistency it provides and minimum manpower needed to manage and maintain security on a fleet of HP printers. Key features include:

- Automated deployment of print security policies
- On-going monitoring of fleet to assure compliance
- HP Instant-on Security for out of the box security
- Automated generation and deployment of unique, identity certificates

The strength of the IPSC offering is significant. HP has added the ability to automate the management of identity certificates to their solution. Used in conjunction with the automated deployment of policies, IPSC allows organizations to greatly leverage their manpower and costs. MI&S believes this will provide not only more secure systems, but reduce overall time to deploy new systems and reduce overall IT/security labor costs.

- Automated certificates and policy deployment provides strong and consistent security
- Time to add nodes is reduced since deployment can be immediate upon adding a new node to the network.
- Resources can be reduced since IT staff is not required to manually configure (or visit) each new printer
- Updated policies can be immediately deployed across the entire fleet

HP JETADVANTAGE PULL PRINT

HP has bundled JetAdvantage Pull Print with their new printers and MFPs. Pull Print is a process to allow organizations to securely store and retrieve cloud-based jobs and print them at the MFP (US/Canada only for now, with plans to expand to other regions in 2015). MI&S continues to believe that mobile access will expand. Adding the ability to send prints to the cloud and retrieve them later, securely, will keep HP in line with the way today's organizations are adapting to the mobile workforce.

SUMMARY: CALL TO ACTION

Printers, a critical piece of the IoT corporate infrastructure, are often afterthoughts when it comes to security. New features and functions have made MFPs look much more like PCs or servers, and organizations must work to bring the corporate print fleet up to the same security standards they deploy in the rest of their environments.

MI&S recommends organizations conduct security audits to determine holes in their printer security processes and make sure to include printers in their overall security strategy moving forward. Costs should be allocated for security for new and expanded implementations, as well as for software, firmware and equipment upgrades to bring existing equipment up to modern (and secure) standards and close existing security holes.

MI&S recommends HP printers and security solutions are strongly considered for large organizations and enterprises that prioritize security. HP JetAdvantage Security Portfolio is a well-designed suite of software and services that today provide clients with piece of mind, not only in their print environment, but also across the entire connected infrastructure.

HP's current feature set for print security is strong, and the recent introductions of Printing Security Advisory Services and expansion of the Imaging and Printing Security Center are exciting additions to an already robust portfolio.

In addition, by leveraging the rest of their product line HP can integrate their security software and services across servers, storage, networking, personal computers, tablets, and security appliances – providing an integrated, easy-to-use and cost effective security solution across the entire networked infrastructure. Competitors may have pieces of the puzzle, but no other organization has the ability to provide security software across such a broad range of enterprise products.

IMPORTANT INFORMATION ABOUT THIS PAPER

AUTHOR

[Patrick Moorhead](#), President & Principal Analyst at [Moor Insights & Strategy](#)
[Mike Krell](#), Analyst at [Moor Insights & Strategy](#)

REVIEW

[Patrick Moorhead](#), President & Principal Analyst at [Moor Insights & Strategy](#)

INQUIRIES

Please contact us here if you would like to discuss this report and Moor Insights & Strategy will promptly respond.

CITATIONS

This note or paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

DISCLOSURES

Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper, including HP. HP commissioned this white paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

Company and product names are used for informational purposes only and may be trademarks of their respective owners.