Printer Security: The New IT Imperative

Research Shows That the "Humble Printer" Remains a Security Blind Spot

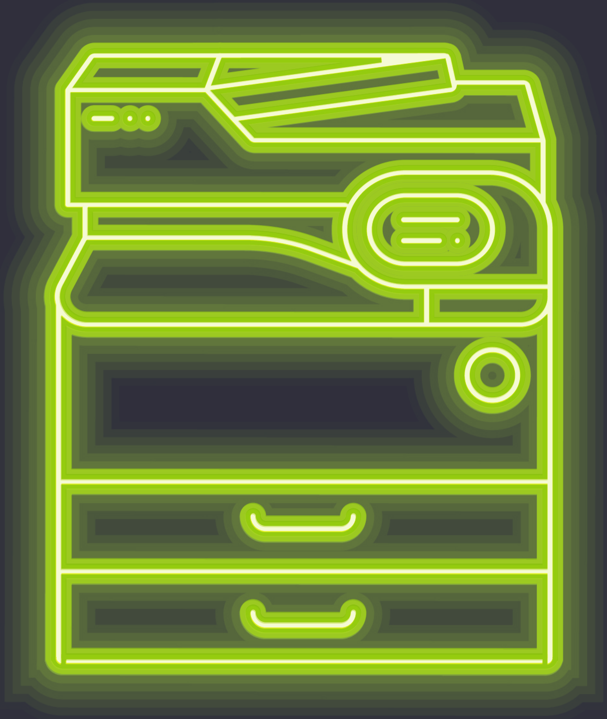


Table of Contents

Introduction

Even as IT security threats are increasing, hardware security efforts often aren't keeping up. Perhaps nowhere is that more evident than with printers. Though IT professionals are increasingly aware of the dangers unprotected printers pose to the network, printers continue to hide in the security blind spot, with the majority of them running under-protected.

"Vulnerabilities are being exposed in all kinds of network-attached devices, including the humble network printer," says Ben Vivoda, director of printing systems for HP South Pacific. **"Typically, we're seeing the printer gets left out and overlooked and left exposed. Businesses can no longer afford to overlook print when it comes to their overall IT cybersecurity strategy."[1]**

In fact, according to a recent survey conducted by Spiceworks, printers are the source of an increasing number of security threats. Today, a printer is 68% more likely to be the source of an external threat or breach than it was in 2016; it is 118% more likely to be the source of an internal threat or breach.

Yet only 30% of IT pros recognize that printers pose a security risk. While this figure has roughly doubled since 2016, it is still too low, and reflects a dangerous reality. Many IT pros seem to hold an outdated view of printer security, perhaps hanging on to the legacy perception that printers are safe inside the perimeter of the network.

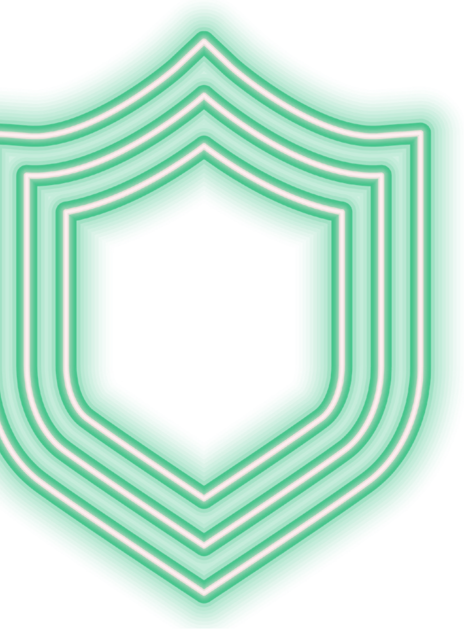
Even for those IT pros who recognize the risk, securing the glut of end-user devices often takes top priority, leaving printers wide open and networks vulnerable.[2] While it is understandable that printer security has taken a backseat to other endpoints in the past, it is critical that IT organizations start addressing the risks unsecured printers pose to their broader IT infrastructure and overall company risk governance.

The Risk to the Business

Are printers really a problem? In a word, yes. In an era where new security threats emerge every hour, a printer can make for an easy target. “Modern printers are essentially advanced, specialized network hosts, and as such, they should be given the same level of security attention as traditional computers,” says Kevin Pickhardt in *Entrepreneur*.[2] “Office printers are not only potential sources of data loss and confidentiality issues, but attack vectors that hackers can exploit.” Case in point: Last year a hacker reportedly used an automated script to access 150,000 publicly accessible printers, including a large number of receipt printers, and instructed them to run a rogue print job.[3]

Industry analysts agree. According to IDC, “Most printers have broad access to an internal network. **An attacker who compromises a printer can have unfettered access to an organization’s network, applications, and data assets.”[4]**

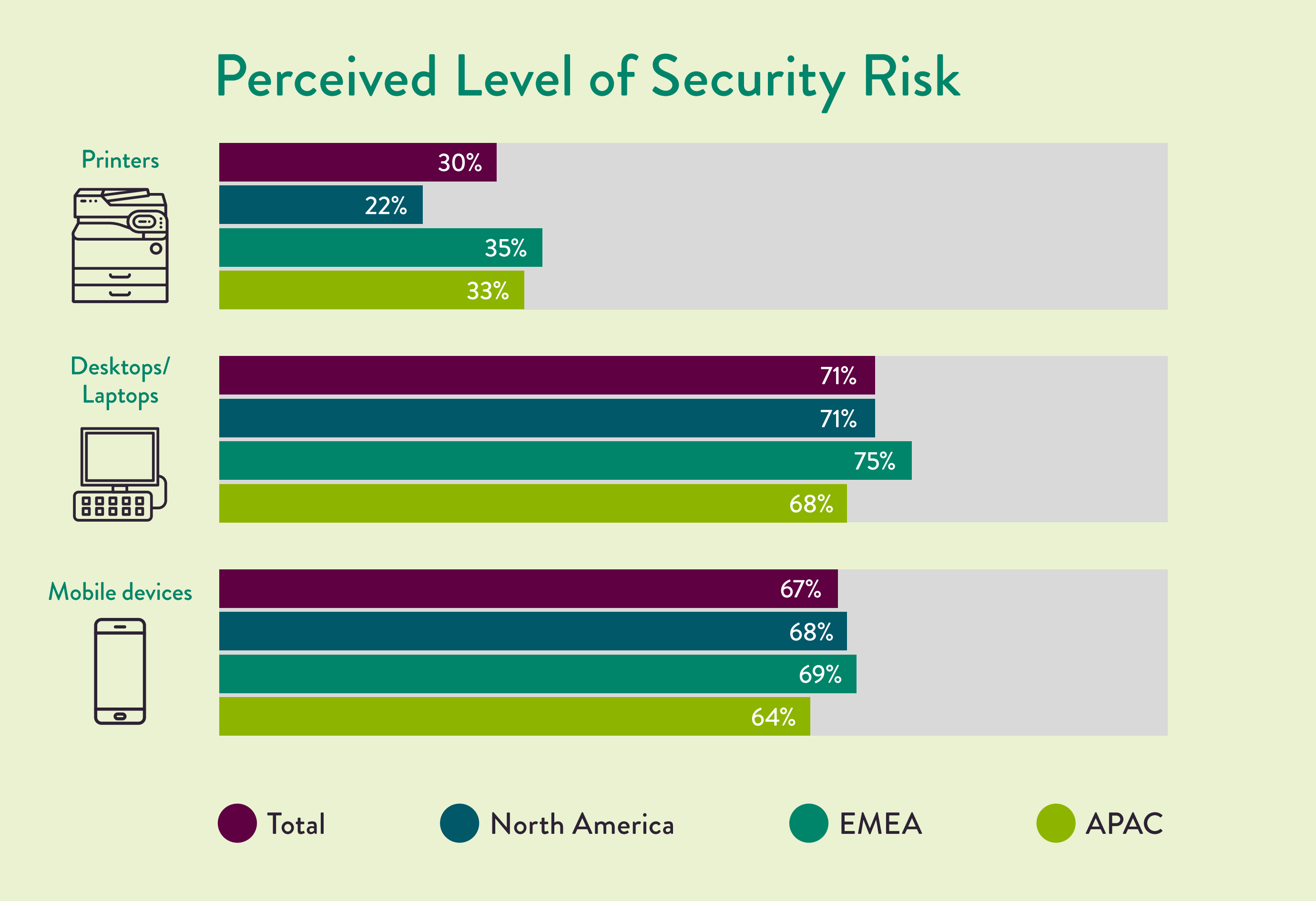
What does an under-protected network printer look like? It is not hardened and therefore left wide open to a wide range of network protocols. It requires no access controls (even setting an admin password is often overlooked). It allows sensitive documents to be printed without authentication, where they can languish in the output tray all day. It sends unencrypted data over the network. It runs outdated firmware, or is not monitored for security threats.



These various security failures will have consequences. Gartner predicts that, by 2020, more than half of Internet of Things (IoT) projects will expose sensitive information due to failures to leverage hardware security features, up from less than 5% today.[4]

A Problem of Perception

Despite the research, however, IT pros are still behind in acknowledging the risks that printers pose. In North America, not even one-quarter of IT pros (22%) recognize printers as a security risk, whereas across Europe, the Middle East, and Africa (EMEA), that number is still barely more than one-third, at 35%.



By contrast, IT pros ranked the threat posed by desktops and laptops at 71%, and ranked the threat posed by mobile devices at 67%.

The Spiceworks research further reveals that the IT pros who do take preventive measures have taken a very splintered approach. And it is no wonder, considering the breadth of security requirements. No single solution is sufficient; a firewall alone is not enough, for example. As with any network device, printer security must be addressed from multiple angles. And as with any security strategy, the most effective solutions will be integrated, automated, and easy to use and manage.

Exacerbating the challenge is the fact that each brand of printer has its own proprietary software and operating systems. Many IT pros may not have sufficient knowledge to configure printer software to meet their security policies.

Current Practices

IT pros are taking a variety of approaches toward printer security, creating a custom mix of security practices and features based on the tools they have at hand and their understanding of those tools. In broad strokes, however, current printer security approaches fall into six buckets.

The percentage of respondents who currently have the following security practices in place for printers

42% Document security

31% Device security

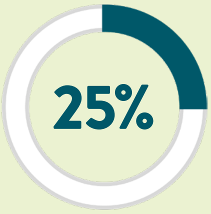
40% Network security

30% Security monitoring

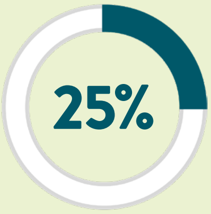
39% Access control

28% Data protection

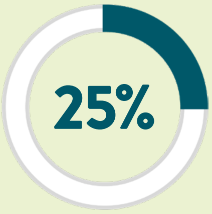
The research revealed that IT pros are taking a number of fundamental security steps within these categories, but unfortunately at very low rates.



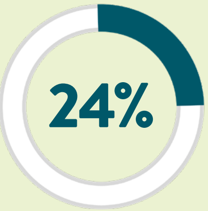
Closing unused open ports



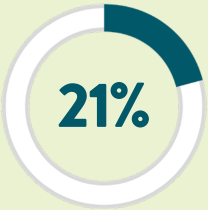
Enabling the "sent from" feature



Securing printer repair access



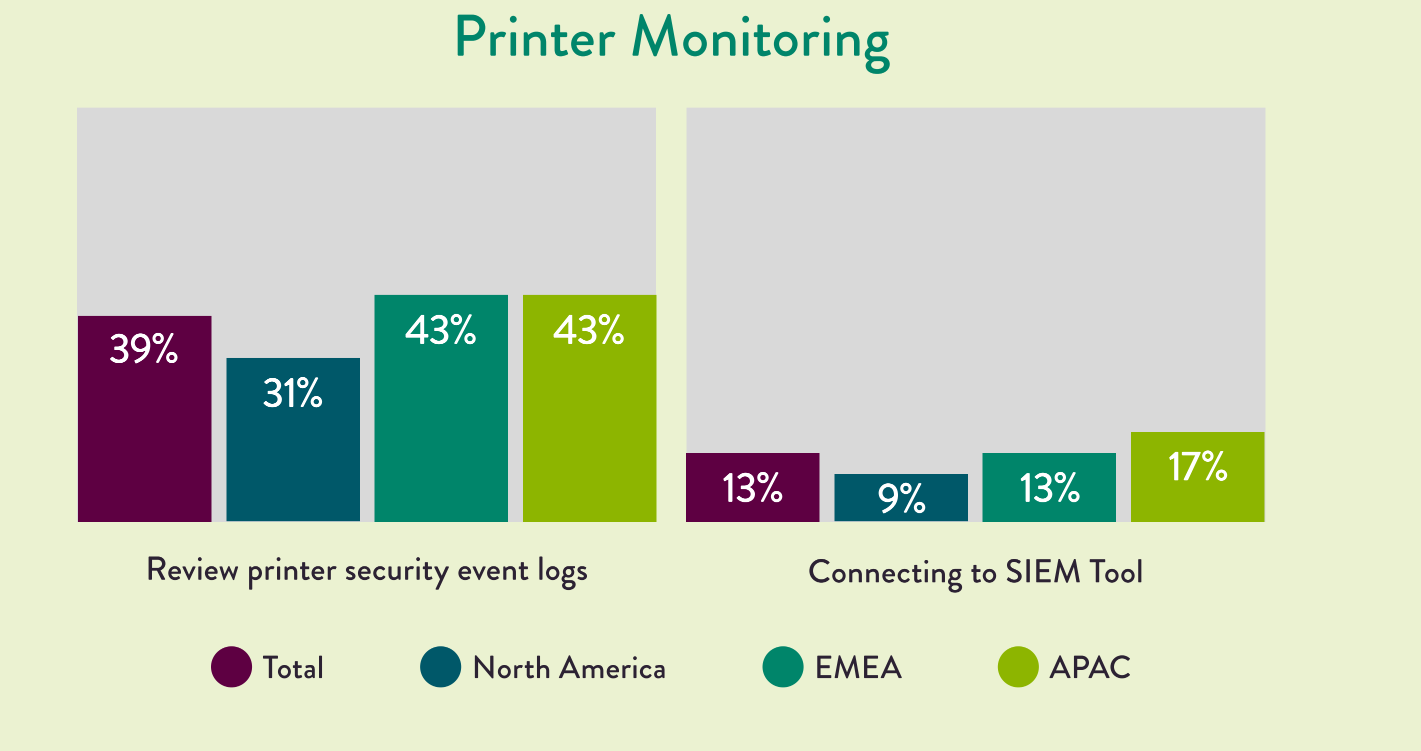
Implementing privacy ("pull") printing



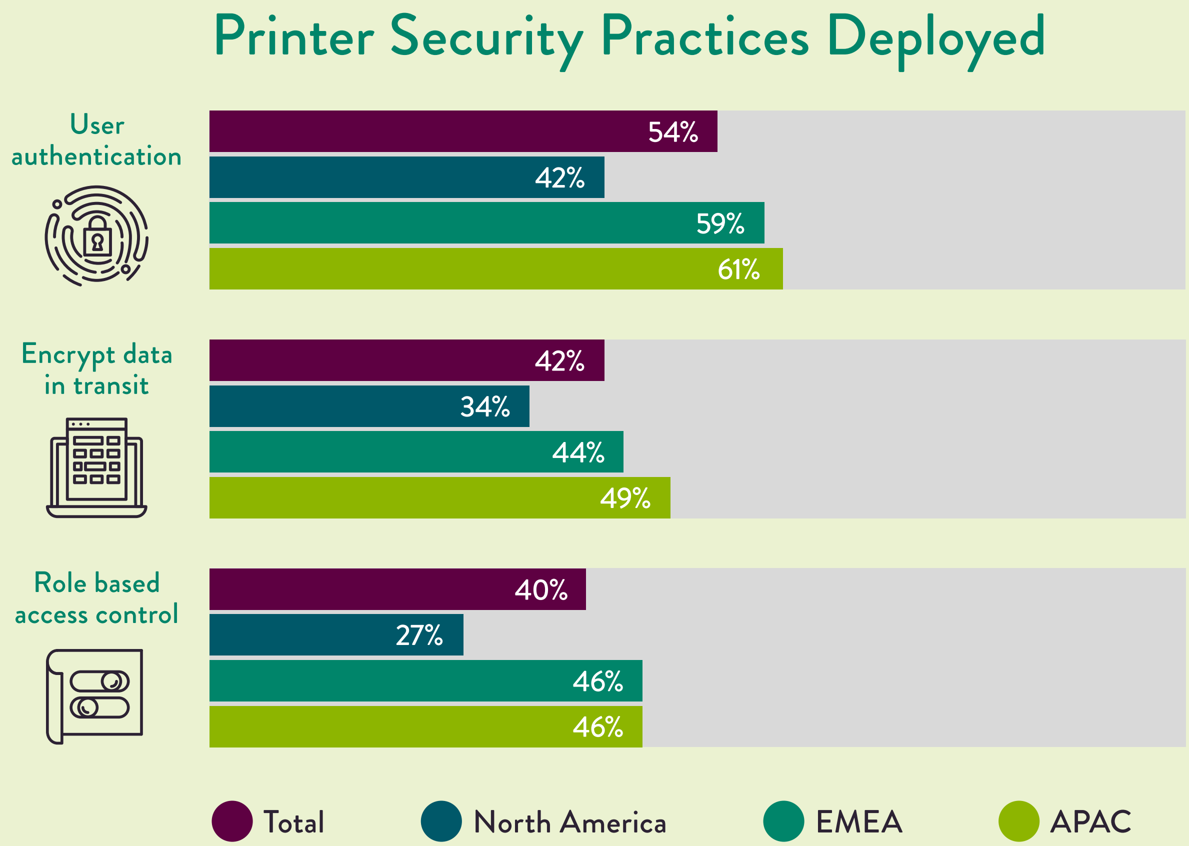
Routinely erasing printer hard drives

Even fewer numbers of IT pros expire or purge jobs on a scheduled basis, require admin access for configuration changes, or automate certificate management.

IT pros *are* performing printer security monitoring more frequently than other activities, but the rates are still low, with only 39% of IT pros saying that they routinely review printer logs—and only 31% in North America. As for connecting printers to SIEM tools, only 13% report having done that. Not monitoring printer logs and not integrating printers with SIEM keeps IT pros in the dark, unaware of cybercriminals who may be using unmonitored infrastructure to hide on a network and exfiltrate data.

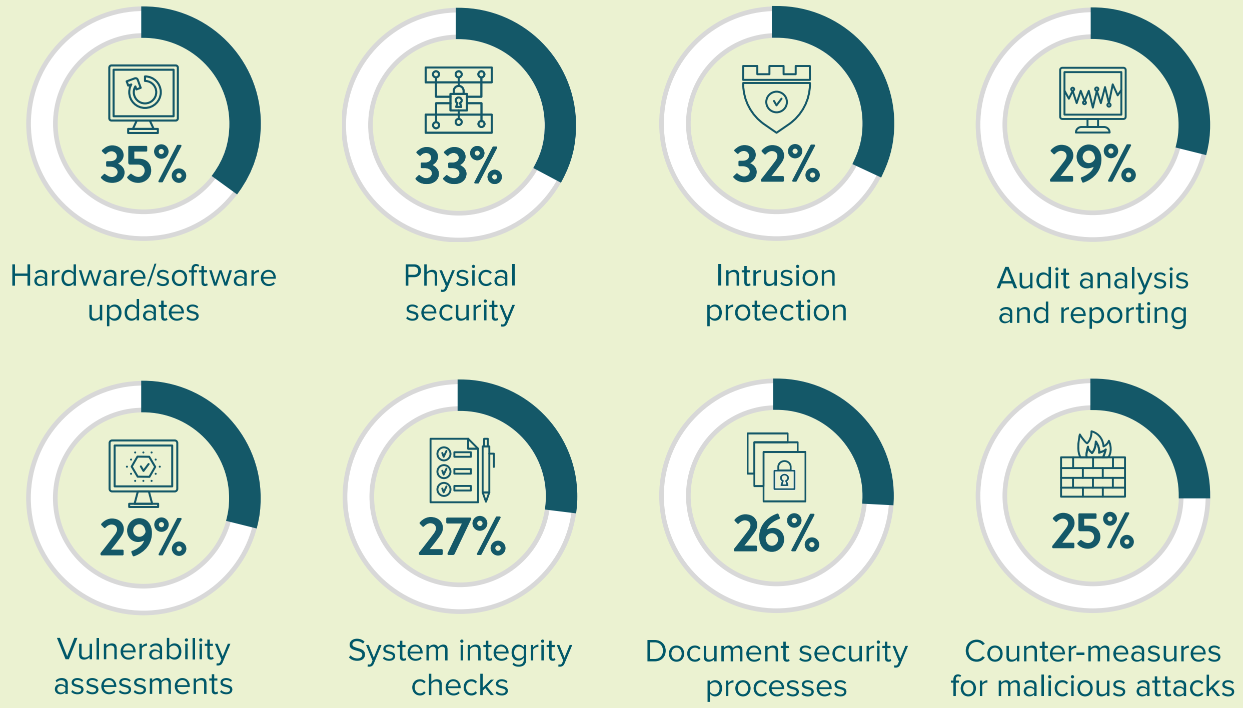


The research reveals other geographical differences in specific areas of printer security, where again North America lags. This is especially true for access controls and encryption. IT pros in APAC are far more likely than those in North America to encrypt data in transit, require authentication at the device, and deploy access controls based on the role of the user.



Finally, when it comes to meeting compliance with data privacy regulations, IT pros again rely on multiple approaches, with some printer controls subsumed within the overall IT compliance strategy. The Spiceworks survey asked IT pros which compliance controls they have implemented, based on the Center for Internet Security's "CIS Controls V7."[5]

Compliance Controls in Use



This data reveals that IT pros often overlook the most basic printer security precautions, such as updating firmware, with only about one-third making that a routine part of their compliance activities. Industry research concurs. According to IDC, printers are typically not upgraded with the latest firmware because organizations so often underestimate the risk.[4] In addition, they may not have the time it takes to review, test, and accept new firmware for printers across the fleet.

Toward Comprehensive Printer Security

Of the 84% of IT pros who report having a security policy, only 64% say that printing is included in that policy. For North America, only 52% do. This is one reason why it is so important to seek out integrated and automated printer security controls—and to actually implement them. Printers with built-in security features help minimize your risk while maximizing your IT spend.

IDC analysts have also found this to be true: "Printers are much more difficult to harden once they are shipped, underscoring the importance of selecting printers that are already rich in foundational and advanced security features."[4] Gartner says, "To exploit emerging print market dynamics, technology strategic planners must build a comprehensive print security solution portfolio by using solution tiers that exceed security industry best practices. Integrate those solutions with the broader security solution ecosystem."[6]

Managed Print Services providers are expanding their services to help cover IT departments that don't have the staff bandwidth of knowledge to address printer security. Says IDC, "Vendors offer an expanded array of device- and data-level protection services, many of which are designed to integrate with existing document management and enterprise content management (ECM) systems to provide further protection and to address governance and regulatory compliance issues."[7]

Fortunately for IT pros, today's advanced printers offer dozens of embedded security features for your print security portfolio, including threat detection, protection, notification, and self-healing, making it easier than ever to harden one of the most vulnerable endpoints on your network—the humble printer.

It's time to harden your print security.

Learn More

About the Survey

HP commissioned Spiceworks to conduct a survey in May 2018. This survey targeted IT decision-makers, including IT directors, IT managers, and other IT staff, to understand current printer security practices and identify areas of risk. Survey results included responses from approximately 500 participants in North America, EMEA, and APAC who work at organizations with 250 or more employees.

Sources

[1] McLean, Asha, “Unsecured printers a security weak point for many organisations: HP,” *ZDNet*, April 18, 2017.
https://www.zdnet.com/article/unsecured-printers-a-security-weak-point-for-many-organisations-hp/

[2] Pickhardt, Kevin, “Why Your Innocent Office Printer May Be a Target For Hackers,” *Entrepreneur*, January 31, 2018.
https://www.entrepreneur.com/article/308273

[3] Peyser, Eve, “Hacker Claims He Hacked 150,000 Printers to ‘Raise Awareness’ About Hacking,” *Gizmodo*, February 6, 2017.
https://gizmodo.com/hacker-claims-he-hacked-150-000-printers-to-raise-aware-1792067012

[4] Brown, Duncan, et al., “IDC Government Procurement Device Security Index 2018,” *IDC*, May 2018.

[5] “CIS Controls,” *Center for Internet Security*, March 2018.
https://www.cisecurity.org/controls/

[6] Von Manowski, Kristin Merry and Deborah Kish, “Market Insight: IoT Security Gaps Highlight Emerging Print Market Opportunities,” *Gartner*, October 31, 2017
https://www.gartner.com/doc/reprints?id=1-4OCKFKG&ct=180110&st=sb

[7] Palmer, Robert and Allison Correia, “IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, IDC, 2017.