INSIGHT

Transformative Technology in Document Security

Arianna Valentini

IDC OPINION

The majority of organizations have taken steps in making sure that their IT environments are secure. *Worldwide Security and Vulnerability Management 2014-2018 Forecast and 2013 Vendor Shares* (IDC #250223, August 2014) predicts that revenue from security software will obtain a compound annual growth rate (CAGR) of 10% from 2013 to 2018 and that security software will be a $4.9 billion dollar industry in 2015. That said, many companies still overlook their printing assets and print-related technologies, which may leave the organization vulnerable. These points of access provide entry points for cyberattacks even in secure organizations and are part of the reason why technology suppliers have made greater efforts to ensure that they provide increased protection for these soft spots in organizations. Complicating matters is the increased use of 3rd Platform technologies such as mobile, cloud, and big data by organizations. Other factors include:

- As the number of cyberattacks on major institutions continues to grow, so does the rate at which enterprise workers work from and bring their own mobile devices, pushing CEOs and CIOs to expand investments in cybersecurity solutions. IDC forecasts that by 2018, 69% of mobile devices for business use will be employee liable (see *Worldwide Business Use Smartphone 2013-2017 Forecast Update*, IDC #244840, December 2013).
- Enterprises are looking for cloud-based solutions as a means to deploy and store documents. IDC currently forecasts the security products market to reach $42.8 billion in 2018, representing a compound annual growth rate of 6.9% from 2013 to 2018, with the majority of investments going to cloud security (see *Worldwide IT Security Products 2014-2018 Forecast and 2013 Vendor Shares: Comprehensive Security Product Review*, IDC #253371, December 2014).
- Hardcopy managed print and document services technology suppliers are concentrating their efforts on print device security that prevents hackers from entering enterprise networks via print devices.

IN THIS INSIGHT

This IDC Insight reviews how transformative technology such as mobile, cloud, and big data plays a role in technology suppliers expanding their print security service offerings. In addition, this document provides technology suppliers and other organizations offering print security services or solutions with insights on how the 3rd Platform will affect document security and the types of solutions business users will need to maintain safe work environments.

SITUATION OVERVIEW

It is no secret that cyberattacks are increasing. In parallel with the rising threats of cyberattacks, enterprises are dealing with increased use of employee-liable mobile devices, cloud deployment of traditionally on-premise solutions, and integration of other Internet-connected devices and services to

their infrastructures. The culmination of these shifts in the enterprise is causing CEOs and CIOs to expand their investments in cybersecurity solutions. *Worldwide Security and Vulnerability Management 2014–2018 Forecast and 2013 Vendor Shares* (IDC #250223, August 2014) predicts that revenue from security software will obtain a compound annual growth rate of 10% from 2013 to 2018.

While enterprise workers are aware that their security is at risk through device hardware and networks, adoption of security-based systems for printers and MFPs is relatively low. A 2014 survey of 370 workers who influence technology purchases in their organization showed that 27% of respondents were concerned with security breaches from employees breaching company policy or the law by transferring company proprietary information by printing, scanning, faxing, or copying documents. In an attempt to frame the discussion around the security of hardcopy devices within the enterprise, IDC's Hardcopy Industry Transformation and Page Volume Analysis service has developed four core security pillars that each organization and technology supplier should take into consideration for best practices of security. Table 1 shows these pillars along with the need for technology suppliers to provide consultative and auditing services for their customers in parallel with these best practices.

TABLE 1

Hardcopy Transformation Security Pillars

Security Pillar	Definition	Examples
Networks	Refers to the connectivity of the hardcopy device and other devices on to an organization's network	▪ IP address filtering ▪ Port and protocol access ▪ Logging and auditing of MFP users on network
Hardware	Refers to the security of the physical device during the entire life cycle	▪ Hard drive encryption/locking/overwriting ▪ Virtual shredding end of life cycle
Content	Refers to the security of corporate content, both print and electronic, structured and unstructured	▪ Encrypted print or scan ▪ Content overwriting ▪ Digital signature encryption
Accessibility	Refers to the control, monitoring, tracking, and reporting of who accesses the device and for what purpose	▪ Tracking and auditing of users for document repository access ▪ MFPs only available to authorized mobile devices

Source: IDC, 2015

Most institutions have done a good job in securing and investing in securing their overall IT ecosystems. IDC research shows that printers and MFPs can be the last unsecure piece of the puzzle – even basic table stakes technology such as wiping the discs of the hard drive of MFPs at the end of the device's life cycle must be practiced by organizations. Printers and MFPs are part of the network of the enterprise and need to be treated as such, especially as these hardware devices become more accessible as employees use more 3rd Platform-based technology in the workplace. For example, because the mobile-based workforce is only expected to grow, IDC expects increased growth of the mobile printing market at a 12% CAGR from 2014 to 2018 (see *Worldwide and U.S. Document Solutions Software 2014–2018 Forecast*, IDC #252308, November 2014). It is for this reason that it is critical that enterprises secure their printers and MFPs to make sure they know how and when hardcopy devices are used as well as who is using them – especially when such use enables workers to also share and store documents.

Transformative Technology

Enterprises looking to invest in security for their documents and printing networks/devices often develop a print and document security policy, which consists of interrelated capabilities for device security such as device management, authentication (access and auditing), and content security. Typically, these capabilities are rolled into a software suite within the device and are the minimum requirements for document and hardware security for print within the enterprise. That said, hardcopy and software technology suppliers realize that to increase adoption of such table stakes-based technology, they must use transformative technology such as cloud, mobile, and big data in order to encourage adoption.

Cloud Deployment

Today, more organizations are using some form of a software-as-a-service model, preferring cloud-based deployment of solutions without ever owning or deploying software on-premise for their organization. IDC research shows that cloud software currently makes up 10.9% of the worldwide software market but estimates it to grow to over 20% by 2018, meaning $1 of every $4 spent on applications will be consumed via the cloud (see *Worldwide SaaS and Cloud Software 2014–2018 Forecast and 2013 Vendor Shares*, IDC #249834, July 2014). While cloud allows for better agility for daily functions including the deployment of new services, organizations can be at risk of a security breach due to hacking through routers or even printers. For many organizations, security passwords or compliance for such entry points are not even a thought. That said, cloud-based solutions allow for the ability to integrate hardware- and software-based services into one cohesive workflow, allowing for better tracking of documents in paper and digital form. While enterprise environments see value in the cloud, the true value proposition for cloud-based document services can be found in small to medium-sized business (SMB) environments. For SMBs, cloud document management means less investment in the overall IT infrastructure while maintaining the power of a robust document management system. IDC research of 744 United States-based SMBs showed that over half have adopted cloud deployment for many IT-related processes (see *Regional 2015 SMB Cloud Adoption Survey: Benchmarking Cloud Maturity Against Line-of-Business Growth*, IDC #254023, February 2015). SMBs also may have less security requirements for implementing cloud-based solutions than enterprise environments; that said, cloud-based document solutions should still allow for remote configurations of security protocols.

An important part of document security is that it allows end users to configure settings for more secure printing environments. Document management solutions allow for functionalities such as the ability to set passwords on devices, resetting a password on the device, or the ability to program hard drives. Technology suppliers that offer solutions for document management that are deployed in the cloud can offer enhanced services to their clients for security. For example, Canon's MDS Cloud has the ability for end users to take advantage of a remote monitoring service that offers meter read collection, supply-level management, and break/fix service alerts for both Canon and non-Canon devices. MDS Cloud also provides the ability to remotely change device configurations and user settings.

Mobile

IDC estimates that by 2018, 69% of mobile devices for business use will be employee liable or BYOD – meaning that most organizations may not always be able to ensure that all mobile devices in their networks are up to security standards (see *Market Analysis Perspective: Worldwide Mobile Enterprise Device Solutions, 2014 – Business Agility Through BYOD in 2015 and Beyond*, IDC #253082, December 2014). In addition, the proliferation of mobile devices means that mobile printing and scanning will likely also grow among businesses with heavy mobile users. IDC expects increased

growth of the mobile printing market at a 12% CAGR from 2014 to 2018 (see *Worldwide and U.S. Document Solutions Software 2014–2018 Forecast*, IDC #252308, November 2014). That said, organizations cannot ignore the BYOD shift in the work environment, and it must be accepted as the norm. The management of employee-liable devices is an organization's best hope in combating what is one of the largest vulnerabilities to security in the company as a whole. One way organizations can seek to better secure documents is through device access and auditing.

Device access and auditing (i.e., authentication) allow for IT staff to enable the appropriate access to devices based on an end user's credentials or policies set in place by the organization. Authentication becomes critical in BYOD environments, especially when mobile devices are left unattended or not secured with a password that also have access to mobile printing or capture capabilities enabled. Since mobile printing or scanning often involves gaining access to internal networks or connecting to content or document management solutions, it is critical that printing and scanning policies are implemented.

Vendors that are within the mobile printing and capture space have taken steps to enable such security capabilities for mobile devices. Many mobile printing and scanning solutions now are available with a version of a pull printing capability, where a pin number or password on either the hardcopy or the mobile device must be used to access functionality. However, such capabilities are just the beginning. In order to truly offer improved mobile-based security for documents, mobile printing and scanning technology suppliers need to look into building solutions that fit in with mobile enterprise management software.

Mobile enterprise management software includes products offering standalone mobile device management (MDM), standalone mobile application management (MAM), or combined MDM-MAM functionality. These solutions can also include mobile enterprise security capabilities and the ability to wipe applications and/or data remotely. MAM permits corporate policy control of applications and content including enabling data storage, offline access, document sharing, and copy/paste.

In addition, mobile printing and scanning technology suppliers can provide even better security by working with mobile email solution providers that specialize in security such as Good Technology, VMware, and MobileIron. For example, HP's ePrint mobile printing solution works with Good Technology and allows print functionality for email and calendar with mobile devices. It is important to remember in cases of mobility that the security of the device falls under not only the organization but the hardware manufacturers as well. It is for this reason that IDC has seen increased activity by hardware manufacturers such as AT&T and IBM, which have actively acquired and aggressively developed security solutions for mobility.

Big Data and Analytics

For many organizations, the feeling that they have workers following compliance standards for security means that they are in effect protected from both internal and external security threats. However, compliance does not equal security, and organizations need to understand that a big part of protection relies on detection. Using big data analytics is one of the ways in which companies can practice both compliance and detection for document security, especially as many organizations are dealing with unknowns. IDC research indicates that nearly 30% of business users have trouble locating documents even when in known repositories. When documents are hard to find, it also means that IT staff within the organization may have a harder time tracking when documents are accessed outside of typical security protocols. For technology suppliers, these challenges that organizations face can be an opportunity to grow in big data analytics offerings.

Technology suppliers can use big data to expand the extraction capabilities of content from scanned or printed documents to make sure information is properly stored in a secured area or does not fall into the wrong hands. It can also be used as a way to mine documents by keywords or phrases to ensure better document tracking and auditing. By partnering with enterprise content management technology suppliers or big data analytics providers, technology suppliers have the ability to become a part of the overall enterprise application workflow, resulting in better security for documents that are input through not only traditional print and scan hardware but also mobile devices.

In addition to content extraction, there is the opportunity to offer equipment monitoring and tracking of data. Hardcopy manufacturers can implement the use of big data and analytics to allow customers to better manage data flows and devices. By tracking user behavior on scanning and printing devices, IT staff can determine abnormal worker behaviors or access from hardware. Such offerings could include the ability to deploy tools to collect, analyze, and correlate print device log events that allow risks to be automatically highlighted and sent to IT staff.

FUTURE OUTLOOK

Organizations can no longer rely on compliance to safeguard them from IT security threats. Instead, they must take the time to invest in hardcopy and document solutions that provide overarching security features — this means not only investing in hardware but investing in services and assessments for security as well. As cloud, mobility, and big data become greater parts of the technology landscape, it is likely that the buying and assessment process for the end user will become more complicated than ever before. As a result of these challenges, end users will require technology suppliers that have a clear understanding of an organization's needs and can provide the following:

- Authentication of hardcopy devices and document solutions through tools that incorporate mobility
- Access control and the ability to set rules for both cloud-deployed and on-premise document solutions
- Connection encryption for mobile devices to document repositories
- Activity monitoring and detection through the use of big data or predictive analytics
- Data encryption that allows for the protection of information of content obtained from hardcopy devices, scans, or document repositories

Security software is expected to have double-digital growth over the next five years, and organizations will be looking to invest in technology suppliers that can provide the best solutions possible that can address transformative technology in their environments. Technology vendors in the hardcopy and document solutions space have the opportunity to take advantage of this growth by providing unique solutions for the needs of document infrastructure, thus becoming thought leaders in this heavily competitive marketplace.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com