IDC MarketScape


Robert Palmer        Allison Correia

THIS IDC MARKETSCAPE EXCERPT FEATURES HP INC.

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Security Solutions and Services Hardcopy Vendor Assessment

Source: IDC, 2019
Please see the Appendix for detailed methodology, market definition, and scoring criteria.
IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment (Doc # US44811119). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

This IDC study assesses the market for print and document security solutions and services among select hardcopy vendors through the IDC MarketScape model. This assessment discusses both quantitative and qualitative characteristics that position vendors for success in this important market. This IDC MarketScape covers a variety of hardcopy vendors and is based on a comprehensive framework to evaluate security delivered as standalone features and solutions, within the context of a managed print and document services (MPDS) engagement, and as non-MPDS professional and managed services. Many hardcopy manufacturers offer print and document security solutions and services as a way of sustaining value for existing managed print and document services customers, though they are also developing practice areas that are independent of (or adjacent to) their managed services offering. Organizations using the IDC MarketScape for print and document security solutions and services can identify vendors with strong offerings and well-integrated business strategies aimed to keep the vendors viable and competitive over the long run. Capabilities and strategy success factors identified from this study include:

- Current solutions portfolio, device-level features, managed services, professional services, and other capabilities to address security concerns in the print and document infrastructure
- Ability to address core competencies in threat-level assessment, detection, and risk remediation
- Road map to address specific end-user challenges related to securing the print and document infrastructure
- Capabilities and strategies to help customers achieve and sustain security compliance and meet key industry standards
- A holistic approach to delivering horizontal and vertical security solutions and services through both direct and indirect channels
- Focus on operational and service delivery excellence, which includes consistent service delivery on a local, regional, and global basis
- Continued expansion into new geographic territories, vertical industries, and line-of-business applications
- Flexible service delivery, pricing, and billing models and the ability to support on-premises, private, and public cloud offerings

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This document includes an analysis of eight prominent hardcopy equipment manufacturers with broad hardware portfolios to specifically address office workgroup/departmental printing environments on a global scale. Vendors must offer a large portfolio of standalone security solutions and services while
dedicating a significant percentage of total R&D spend to the category. Given this approach, certain print and imaging vendors have been excluded even though they are among the top printing hardware firms based on worldwide revenue. Also excluded from the study were IT outsourcing companies, business process outsourcing (BPO) providers, and software manufacturers that either offer print, document, and security services as part of their IT services or subcontract these services to hardcopy vendors. Indirect channel partners of hardcopy equipment manufacturers have also been excluded from this study.

ADVICE FOR TECHNOLOGY BUYERS

Security remains an IT concern among businesses of all sizes. However, IDC’s research shows that a majority of organizations place a notable difference on the level of importance associated with IT security compared with print and document security. Many CISOs and IT managers have assumed that systems put in place to protect the network would extend to other connected peripherals. But security around the network perimeter is crumbling, and every device connected to the network is now an endpoint security risk, printers and MFPs included.

The result of a security breach to the print and document infrastructure is the same as that of any other security lapse: extensive costs related to downtime to identify and fix a security breach, fines associated with corporate governance and regulatory compliance, lost customers, or other harmful damage done to the company’s reputation.

In today’s business world, the IT infrastructure is only as secure as its weakest link and, for many businesses, the print and document infrastructure is one of the most vulnerable to security risks. Even so, there is an interesting dichotomy associated with the office MFP. On the one hand, the connected MFP is a potential threat as an unmanaged connected device. On the other hand, the MFP could be leveraged as a frontline asset for securing network access, managing content security, and protecting access to information. Steps that should be taken to develop a secure print strategy have proven difficult for many businesses.

Accordingly, organizations should consider the following:

- **Determine the level of complexity expected for print and document security over the next three years.** Features designed to provide endpoint security protection for printing devices continue to become more commonplace. However, organizations looking to develop a comprehensive print infrastructure security strategy should seek out solutions and services to extend protection well beyond the device.

- **Understand your current environment.** Evaluate the existing print and document infrastructure to identify security threats and vulnerability gaps. To do so, organizations should consider adoption of security auditing and assessment services as part of an overall IT security strategy.

- **Integrate print security within the context of your overall IT security strategy.** Develop a long-term plan that includes measures for ongoing monitoring and management of print and document security programs. 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.

- **Look to your existing hardcopy vendors.** When evaluating print and document security needs, ensure your existing hardcopy vendors are included in the mix. These vendors likely have a
compelling set of security solutions and services with a clear road map for incorporating technologies to meet evolving business needs.

- **Identify industry-specific capabilities.** Security needs and regulatory compliance issues vary greatly by vertical market. Seek out vendors with core competencies in print and document workflow, content management, and secure print services that meet the needs of your specific business.

- **Consider your organizational needs regarding service delivery.** This may include the need to support cloud-enabled services, platform as a service, and global consistency in solutions and services delivery.

## VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of the vendor's strengths and challenges.

### HP Inc.

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

HP Inc. is a public company headquartered in Palo Alto, California. HP Inc. considers the entire cybersecurity landscape with its approach to print and document security. The firm deploys a customer-centric model to identify specific business needs and priorities based on the "security mindset" of the customer. According to HP Inc., customers tend to fall into one of three segments based on their maturity levels: security unfamiliar, security aware, and security insistent. Working within this customer framework, HP Inc. takes a holistic view of print, document, and fleetwide network security, focusing especially on endpoint device security, management, and monitoring.

HP Inc. understands that printers and MFPs are not protected by antivirus programs that run on the PC. As a result, customers must rely on the print manufacturer to provide this capability. For HP Inc., this means designing hardware with security in mind, including capabilities from the hardware on up. With this approach, in-depth protections such as automated self-healing and recovery are layered natively in the device itself. For example, HP Inc.'s FutureSmart printers and MFPs come equipped at no extra charge with HP Sure Start, which detects and prevents the execution of malicious code and self-heals the system BIOS without requiring IT intervention. HP Inc.'s Runtime Intrusion Detection, which is Common Criteria certified, provides real-time monitoring and detection of malware attacks during runtime memory operations and, if detected, notifies security managers or IT administrators via control panel alerts and syslog event messages. HP Connection Inspector's network behavior anomaly detection monitors printer network connections and detects any unexpected behavior atypical to normal print runtime network activities. When detected, the device initiates a self-healing reboot and notifies administrators with control panel, syslog event, and smartphone notifications of an intrusion as the device returns itself to a secure running state. HP Inc. provides customers with "Secure by Default" firmware and Common Criteria certified whitelisting to ensure that only authentic firmware is validated at both load time and runtime. HP Inc. also focuses on privacy and data protection surrounding applications running on HP Inc. devices including HP Inc.-branded and ISV partner solutions. These applications are third-party validated and certified for secure development life-cycle best practices by Security Innovation's Software Development Practices Assessment Certification (SD-PAC) process.
HP Inc. continues to expand its suite of print and document security solutions, which is based on a mix of owned technology and partner-delivered capabilities. These solutions support a broad range of security features and functionality, delivered in the form of integrated software or apps that can be downloaded and run directly from the MFP. With its flagship fleet compliance and management software, HP JetAdvantage Security Manager, HP Inc. provides customers with a robust, security-focused, fleetwide security policy compliance and management tool with a fully enabled platform for managing device and content security. HP JetAdvantage Security Manager enables customers to develop a comprehensive print security policy, assess and remediate devices against that policy, and provide audit and reporting measures based on predefined guidelines.

HP Inc. is also working to help businesses deal with specific challenges associated with printing and cloud connectivity. According to HP Inc., cloud-connected MFPs and printers need additional protection because customer IT administrators may worry about loss of device control and require trusted communication over untrusted networks. For customers concerned about adding applications that communicate with cloud services and enable users to print over the internet, HP Inc.’s approach is a combination of secure devices, secure connections to cloud services, and optimized security best practices through the company’s secure cloud infrastructure.

Leveraging its broad solutions portfolio, HP Inc. also offers an array of security-based services, beginning with an extensive set of security assessment tools and services. Some of these programs are offered free of charge, while others require additional fees. For channel partners, HP Inc.’s firmware vulnerability assessment is a free tool that can assess fleet firmware status in seconds and the HP Quick Assess tool can be installed at the customer site by an HP Inc. channel partner. The tool can assess up to 50 HP Inc.-branded devices at once with 15 essential settings from HP’s JetAdvantage Security Manager compliance solution. With HP Print Security Governance and Compliance, HP Inc. provides trained experts to monitor and manage security compliance. These services enable remote management of security settings, remediate, and generate reports that demonstrate proof of compliance. Other services that leverage the expertise of HP Inc. consultants on technology, security, and industry are also available (such as HP Print Security Advisory Services).

For deeper engagements with customers that have broader security requirements, the Print Security Baseline Assessment can be deployed to assess the entire imaging and printing environment for risks and regulatory compliance. With the HP Print Security Implementation Service, HP Inc. can help organizations roll out a security plan with technical experts to help deploy security settings, add security enhancements such as device certificates, and integrate printers into security information and event management (SIEM) systems (McAfee, SIEMONSTER, ArcSight, Splunk, or IBM QRadar).

**Strengths**

Over the past couple of years, HP Inc. has led the charge when it comes to raising awareness for securing the print infrastructure. The now famous Wolf campaign was very successful in helping HP Inc. drive thought leadership while providing a mechanism for engaging with customers in deeper conversations on the need for print security.

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. 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 businesses is also a considerable strength. Overall, HP Inc. has built a platform of solutions and services wrapped around a go-to-market strategy that is tailored to meet customer needs depending upon where they are in the security journey.
Meanwhile, HP Inc. continues to adapt and change its approach as the market evolves. The firm understands that more is not always better when it comes to security, primarily because customer needs vary depending upon maturity levels and overall mindset. This approach serves HP Inc. well as it seeks to help customers deal with issues related to digital transformation, IoT, mobility, and the future of work.

**Challenges**

IDC believes that HP Inc. could improve its overall approach to the market by further leveraging the integration between its print and PC businesses, particularly in the delivery of print and document security services. While it continues to make strides with its indirect channel, HP Inc.'s overall go-to-market strategy could also be improved by further enabling channel partners to sell and support the company's security offerings on a broader scale to the SMB market.

**Consider HP Inc. When**

Organizations should consider HP Inc. when looking for a vendor that can provide an end-to-end view of customer vulnerabilities and deep understanding of integrated detection, protection, remediation, recovery, and security management. 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.

**APPENDIX**

**Reading an IDC MarketScape Graph**

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor’s current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the managed print and document services (MPDS) market.
IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of a review board of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

For the purposes of the 2019 IDC MarketScape for worldwide print security services, IDC defines print and document security as "solutions and services to address security concerns in the print and document infrastructure, including device-level features and capabilities, software solutions, or professional and managed services with core competencies in threat-level assessment, detection, and remediation capabilities."

This IDC MarketScape evaluates measures for both device-level endpoint security and protection of data/content. Capabilities include, but are not necessarily limited to:

- User authentication and authorization
- Device management
- Device malware protection
- BIOS, operating system, and firmware updates and password management
- Hard disk and removable storage media protection
- Antivirus and antimalware/spyware
- Security event management
- Round-the-clock monitoring and management of intrusion detection systems and firewalls
- Overseeing patch management and upgrades
- Performing security assessments and security audits
- Content security, privacy, and data integrity (hardware and software)
- Installation, configuration, and usage of equipment
- Remote, BYOD, and mobile printing

Security solutions offered by hardcopy vendors could include any combination of software, hardware, and managed or professional services.

Security services could include consultancy and implementation services (professional and managed), including print and document security assessments and audits; security event and policy management; ongoing monitoring and management of intrusion detection systems and firewalls; overseeing patch management and upgrades; content security, privacy, and data integrity (data at rest and data in transit); installation, configuration, and usage of equipment; and secure systems for remote, BYOD, and mobile printing. Integration with legacy business systems and support for current and future regulatory compliance policies are also considered.
LEARN MORE

Related Research


Synopsis

This IDC study assesses the market for print and document security solutions and services among the most prominent global hardcopy vendors and identifies their strengths and challenges. This assessment discusses both quantitative and qualitative characteristics that position vendors for success in this important market. This IDC study is based on a comprehensive framework to evaluate security delivered as standalone features and solutions, within the context of an MPDS engagement, and as non-MPDS professional and managed services.

"Security within the print and document infrastructure continues to be problematic for most organizations," says Robert Palmer, research vice president for IDC's Imaging, Printing, and Document Solutions group. "Hardcopy vendors have demonstrated great strides in helping businesses address these vulnerability gaps, from providing embedded device-level protection to extended services for controlling access to content, managing user behavior, protecting business-critical information, and managing ongoing adherence to corporate security policies."

©2019 IDC

#US44811119e 8
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-community.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2019 IDC. Reproduction is forbidden unless authorized. All rights reserved.