IDC MarketScape

IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019–2020 Vendor Assessment

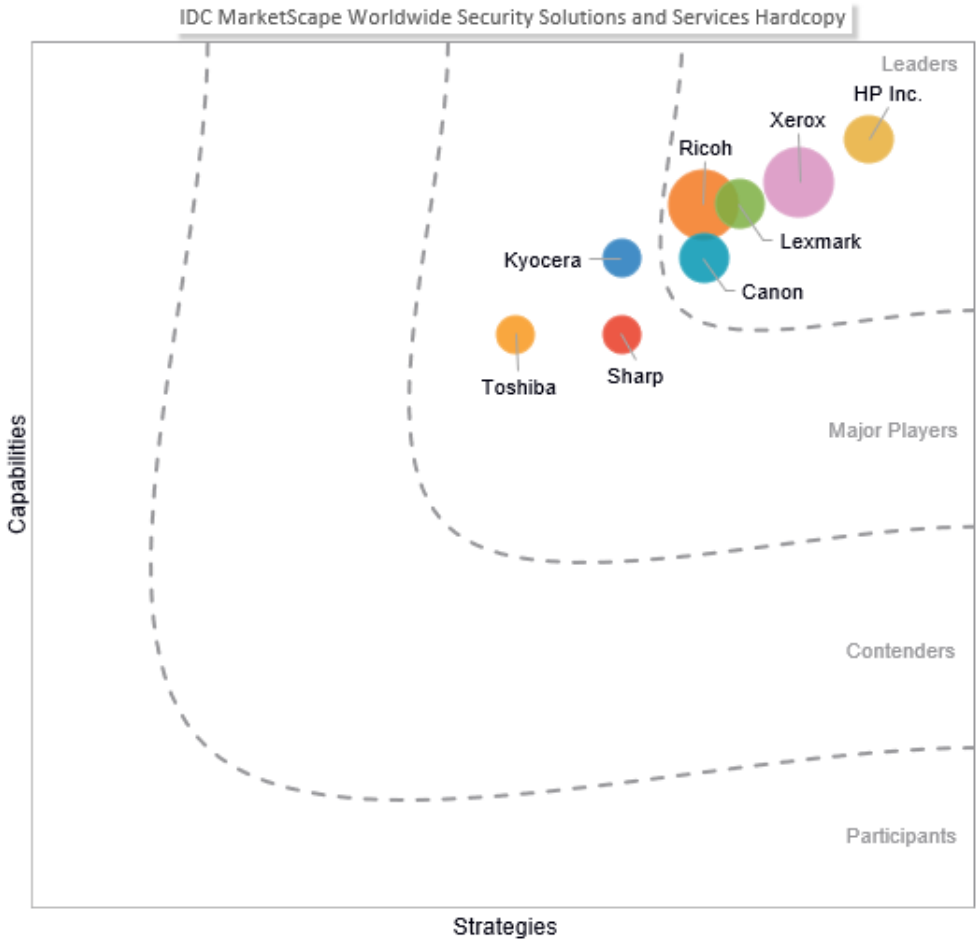
Robert Palmer Allison Correia

THIS IDC MARKETSCAPE EXCERPT FEATURES: LEXMARK

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Security Solutions and Services Hardcopy Vendor Assessment



Source: IDC, 2019

December 2019, IDC #US44811119e

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 PROFILES

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 each vendor's strengths and challenges.

Lexmark

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

Lexmark is a privately held American company that is headquartered in Lexington, Kentucky. Based on what it calls "Full Spectrum Security," Lexmark takes a holistic and systematic approach to protecting the print and document infrastructure that encompasses hardware security, secure development life cycles, supply chain risk management, and corporate governance. Full Spectrum Security begins with technologies and solutions for protecting the device, data, network, users, tools, services, and applications with what Lexmark calls its "secure by design" development process. Lexmark proclaims that security is built-in to its products and solutions as a fundamental premise beginning with the initial design concept and extending through development, manufacturing, and distribution. Lexmark's approach is to recommend, validate, and implement the appropriate level of protection to meet both near- and long-term security goals for the company's customers.

Lexmark protects devices from potential attack vectors through various methods, beginning with features enabled at the control panel to provide role-based authentication and systems integration. The firm also offers numerous capabilities for protecting data stored on its devices with data overwrite, data encryption, and out-of-service wiping, and other end-of-life management policies/services.

Lexmark also offers an extensive portfolio of security solutions comprised of both owned IP and integrated support for various third-party applications. Lexmark Print Management (LPM) is the firm's flagship on-premises solution for delivering secure access control to users across the enterprise. LPM provides a unified platform for delivering secure pull-print functionality to mobile devices as well as desktops and laptops. LPM is made up of three primary components: print release, document accounting, and mobile print; each of which plays a critical role in Lexmark's overall approach to print management security.

Cloud technologies represent another major component of Lexmark's approach to print and document security. One example is Lexmark Cloud Print Infrastructure as a Service (CPI) introduced earlier this year. Delivered as a subscription-based, as-a-service solution, Lexmark CPI allows businesses to fully outsource their print capacity needs as opposed to acquiring and managing individual components within the print infrastructure. Taking advantage of its IoT-enabled hardware, Lexmark is helping customers eliminate the need for on-premises print servers and migrate to a fully outsourced, consumption-based model for print. Along with these benefits, Lexmark CPI provides consistency across the fleet and eliminates the risks associated with servers posed by down-level firmware, operating systems, and security patches.

To support its products and solutions, Lexmark offers a vast range of security services, including assessments designed to help customers evaluate and understand security threats, benchmark against industry best practices, and make informed decisions to mitigate potential risks. Lexmark is looking to continue to drive integration of security services into its managed services programs while expanding its team of security experts to support customized implementations. At the same time, the firm continues to partner with prominent providers of security tools and services to further strengthen its offerings and provide a consistent set of security features across its full product line.

Strengths

Lexmark leverages a broad array of tools, services, data, devices, network technologies, applications, and solutions to address the entire customer environment. Lexmark's holistic approach allows it to provide systematic security for the device, the fleet, and across the network infrastructure. Lexmark's strategy is to first understand the security landscape of the customer environment in order to develop a security program that addresses organizational goals, human factors, network content, vulnerabilities, and network architecture. Lexmark stresses the importance of owning its own IP, but continued efforts to build expertise and partnerships also strengthens its position in the market.

Lexmark maintains a verticalized approach to the market and its ability to develop and leverage industry-specific security solutions and services help set it apart from competitors. A majority of Lexmark's security offerings can be delivered onsite or remotely through the cloud by license, subscription, or SaaS-based billing models. Lexmark continues to expand its cloud options for delivery of print and document security solutions and services, making it easier for enterprise and SMB customers to migrate to a cloud-first strategy. Lexmark Professional Services includes a deep bench of consultants, field systems engineers, and subject matter experts globally, with specific skills, training, and certification in security. Lexmark's technology and industry expertise combined with the company's consistency in global service delivery help position the firm effectively as the market for print and document security continues to evolve.

Challenges

IDC believes that Lexmark needs to continue its efforts to build partnerships and alliances to further strengthen and expand its offerings portfolio. In addition, Lexmark's go-to-market strategy could be improved through marketing programs to raise awareness around the company's security solutions and strategies, particularly as it relates to ongoing investments in cloud, IoT-enabled hardware, and print infrastructure as a service.

Consider Lexmark When

Organizations should consider Lexmark when looking for a vendor with deep industry knowledge, global consistency, and the ability to develop a security policy/program designed to address specific

organizational goals, human factors, network content, vulnerabilities, and network architecture. Lexmark should also be on the short list for those companies looking to deploy a security strategy as part of a broader IT initiative, with flexibility in pricing and service delivery models.

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

- *IDC FutureScape: Worldwide Imaging, Printing, and Document Solutions and 3D Printing 2020 Predictions* (IDC #US45586119, October 2019)
- *Market Analysis Perspective: Worldwide and U.S. Next-Gen Document Services, 2019* (IDC #US44634019, September 2019)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares, 2018: Why the Channel Matters* (IDC #US43832819, July 2019)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast, 2019-2023* (IDC #US45237919, July 2019)

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."

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