IDC MarketScape

IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2022—2023 Vendor Assessment

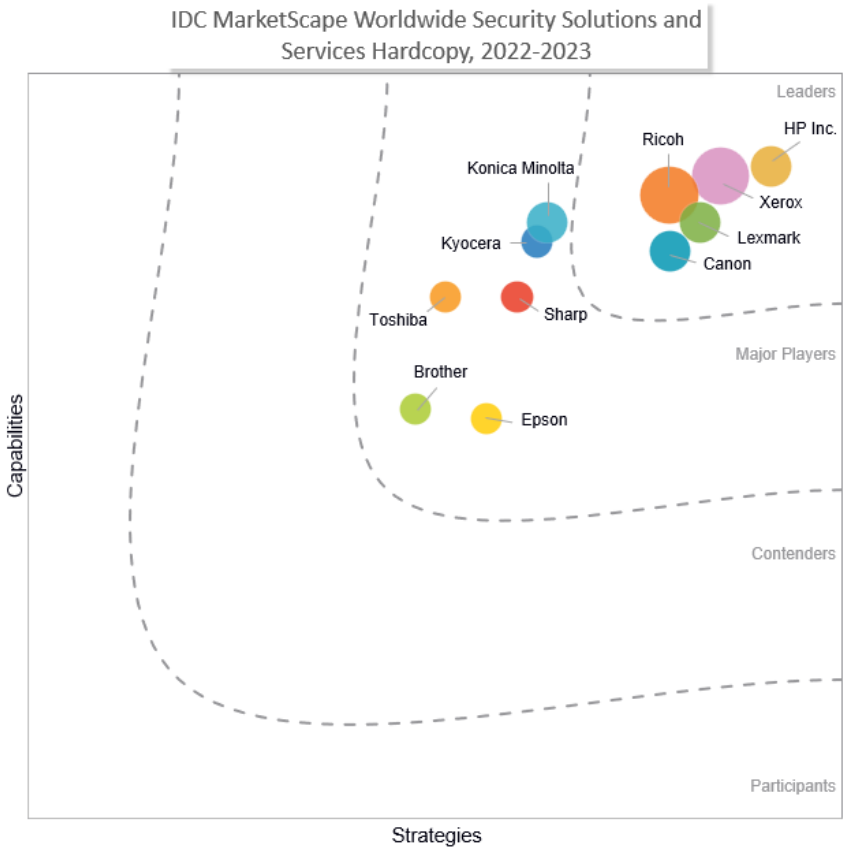
Robert Palmer

THIS IDC MARKETSCAPE EXCERPT FEATURES LEXMARK

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Security Solutions and Services Hardcopy Vendor Assessment



Source: IDC, 2023

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

January 2023, IDC #US48851622e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2022–2023 Vendor Assessment (Doc # US48851622). 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 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 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
- Capabilities and strategies to help customers determine how to best approach securing the print environment within the constructs of a zero trust security framework
- A holistic approach to delivering horizontal and vertical security solutions and services through both direct and indirect channels
- A focus on operational and service delivery excellence, which includes consistent service delivery on a local, regional, and global basis
- Capabilities and strategies to address specific security challenges associated with security in the hybrid working model, including transition to cloud-based print and print infrastructure
- 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 research includes analysis of 11 prominent hardcopy equipment manufacturers with broad hardware portfolios to specifically address office workgroup/departmental printing environments on a global scale. The vendor must offer a large portfolio of standalone security solutions and services while dedicating a significant percentage of total R&D spend to the category. 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 those services to hardcopy vendors. Indirect channel partners of the hardcopy equipment manufacturers have also been excluded from this study.

ADVICE FOR TECHNOLOGY BUYERS

Security remains a top priority among businesses of all sizes. Historically, however, print security initiatives have lagged similar programs aimed at securing the overall IT environment. Many CISO's 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.

Meanwhile, workforce dynamics have changed due to the COVID-19 pandemic, raising a whole new set of security concerns. The shift toward hybrid working is accelerating the push toward a zero trust security model, driven by the need to support remote users, cloud-based applications, and outside assets. It is basically no longer safe or even feasible to assume that everything that sits behind the corporate firewall is protected. Instead, each request must be treated as though it originates from an open network. As a result, a holistic approach must be taken when developing a print security strategy for today's business environment.

Accordingly, organizations should consider the following:

- **Print security in the hybrid world.** Few organizations have provided guidance to remote employees when it comes to the procurement and use of printers. Some have advised employees to use their personal printing devices, while others allow employees to purchase new devices and reimburse printing expenses later. This lack of uniformity across the organization poses significant security risks and must become a focal point for IT and security managers.
- **Balancing convenience, productivity, and security.** Organizations are now in the difficult position where they must provide a printing experience that is consistent and convenient for employees while ensuring that remote printers and MFPs are in line with the necessary corporate compliance and security policies. A recent IDC study shows that 43% of respondents cite security vulnerabilities and the ability to ensure that at-home print devices are compliant with corporate governance and security policies as a top challenge.

- **Integrating 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 business systems to provide further protection and to address governance and regulatory compliance issues.
- **Extending on-campus print security tools to include remote locations**. From a print management perspective, companies are challenged with monitoring and managing devices remotely. Traditional features of print management software including rules-based printing, secure printing, job tracking, and accounting are still essential for businesses to gain better visibility into print usage, particularly with a hybrid workforce where devices are often not visible and usage patterns are not so easily monitored.
- **Looking 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.
- **Identifying 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.
- **Zero trust**. Organizations should consider what might be required for including print within a zero trust security framework. Specific tools and technologies might be needed to ensure secure print workflows, such as secure application development, cloud-based pull printing, device certificates, layered device capabilities, encryption, and multifactor authentication. Cloud-based printing and print management tools are likely to be viewed as a key enabler for those organizations looking to simplify the need to provide a consistent print experience for work-from-home (WFH) employees.

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 in the Leaders category in this 2022-2023 IDC MarketScape for worldwide security solutions and services hardcopy. Lexmark headquarters are in Lexington, Kentucky.

Quick facts about Lexmark include:

- **Employees:** 7,780
- **Global market coverage:** Has offices in North America, Asia/Pacific, EMEA, and Latin America
- **Top industry focus:** Healthcare, finance, education, government, and legal, retail, and manufacturing
- **Ideal customer size:** SMB, upper midmarket, and enterprise
- **Services/solutions evaluated:** Print security solutions and services

- **Delivery models evaluated:** Delivered as embedded, device-level features; as standalone solutions; within the context of an MPDS engagement; and as non-MPDS professional and managed services
- **Key differentiator:** Has a long and storied history in the office printing market built from Lexmark's verticalized approach, which serves as a catalyst in the company's move to support a more services-oriented, customer-centric model (The approach has allowed Lexmark to target specific industries with a broad range of vertically oriented solutions and services. At the same time, Lexmark has leveraged the experience and expertise garnered from its vertical approach to address the full range of horizontal office applications.)
- **Interesting fact:** Among those enterprise businesses that Lexmark counts as customers to include an impressive list: 7 of the top 10 global banks, 9 of the top 10 global retailers, 10 of the top 10 U.S. retail pharmacy chains, 8 of the top 10 global manufacturers, and 7 of the top 10 U.S. federal agencies

Strengths

- **Secure cloud services:** Lexmark has assembled one of the broadest portfolios of cloud services aimed at helping organizations modernize print infrastructure and migrate to a print-as-a-service model. Lexmark Cloud Services are grouped into three main categories: Cloud Print Management, Cloud Fleet Management, and Apps and Connectors. Modules within each of these categories provide customers with a broad array of options for cloud connectivity, configuration and management services, asset management, print management, and analytics. The information gathered by all Lexmark Cloud Services modules provides visibility into an organization's unique printing practices and workflows, providing control over information and processes for a higher level of security and overall protection.
- **Secure by Design:** Lexmark notes that it has been historically ahead of the curve when it comes to print security, with significant investments in data and endpoint protection reaching back over a decade. Lexmark's security strategy is built on what the company calls "Secure by Design," an umbrella term for the firm's systematic approach to ensuring that Lexmark devices and data are protected at every step along the way. Lexmark devices support a full range of embedded features for device hardening and endpoint protection. Coupled with the firm's broad solutions and services portfolio, Lexmark can provide comprehensive security coverage to address device/firmware protection, fleet management, documentation and data security, security training, corporate governance, and support for industry standards and security certifications.
- **Zero trust framework:** Lexmark's security strategies support zero trust infrastructures, which is crucial for those customers considering new security challenges associated with the hybrid working model and the evolution of the workplace. Technologies that Lexmark leverages to address these needs include device management and conformance tools, on-device runtime and firmware protections, and security analysis and analytics services. Through these tools and services, Lexmark can ensure that the print environment fits within an overall zero trust framework for security by supporting guiding principles such as segmenting and compartmentalizing data; ensuring endpoint security; never trust, always verify; and least privileged access.
- **MPS and Lexmark Cloud Bridge:** Lexmark offers a full spectrum of advanced print services, including a range of managed print services offerings tailored to meet specific customer needs based on company size and vertical industry. As part of its MPS programs, Lexmark offers a host of MPS security services in areas such as asset management, consumables management, break/fix, help desk integration, predictive service, security assessment, and configuration management. Key to the company's overall MPS strategy is Lexmark Cloud

Bridge technology, which brings Lexmark's most advanced managed print services functionality to all hybrid network environments. With Lexmark Cloud Bridge, customers of all sizes can take advantage of the value proposition of MPS by leveraging cloud and the Internet of Things to simplify and optimize print environments.

Challenges

- **Go to market:** The overall go-to-market strategy of Lexmark could benefit from increased marketing activities to drive brand awareness and thought leadership around its security offerings, particularly in areas where it offers differentiation such as cloud, IoT, and hybrid work.
- **Channel enablement:** Lexmark needs to continue to enable its channel partners by providing access to the broad range of security tools, solutions, and services it has developed through its direct enterprise engagements. This is particularly important as Lexmark looks to drive print as a service into the SMB sector.

Consider Lexmark When

Organizations should consider Lexmark when looking for a vendor with deep industry knowledge and expertise. Lexmark should also be on the short list of vendors when considering factors such as security to meet hybrid work challenges, moving print infrastructure to the cloud, developing a strong security posture that can expand and evolve over time, and a need for consistent global service delivery.

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 specific market segment being assessed.

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 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 2022–2023 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:

- Identity and access management
- Encryption policies and best practices
- Device malware protection
- BIOS, operating system, and firmware updates and password management
- Hard disk and removable storage media
- Antivirus, 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 2023 Predictions* (IDC #US49751022, October 2022)

- *Market Analysis Perspective: Worldwide Next-Gen Document Services, 2022* (IDC #US49326522, August 2022)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast, 2022-2026* (IDC #US47975222, July 2022)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares, 2021: Hybrid Work Drives Cloud Adoption* (IDC #US48532922, July 2022)
- *Enabling a New Print Services Model for the Hybrid Workforce, Part 3: Security and Zero Trust* (IDC #US49104022, May 2022)

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.

"Organizations need help understanding how hybrid work models will impact print and document security," says Robert Palmer, research vice president for IDC's Imaging, Printing, and Document Solutions group. There are many security vulnerabilities associated with the print ecosystem that will only be exacerbated when remote devices are brought into the mix, and proper consideration needs to be given to issues such as endpoint security, data protection, and zero trust 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

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com