IDC MarketScape

IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment

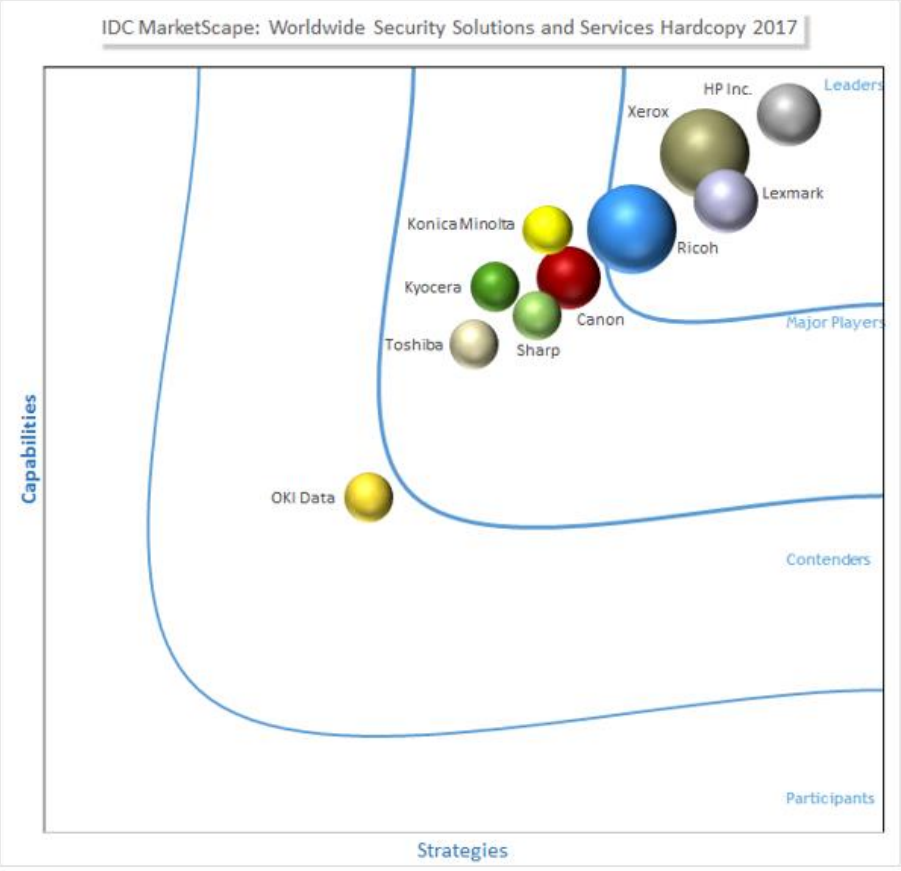
Robert Palmer Allison Correia

THIS IDC MARKETSCAPE EXCERPT FEATURES: RICOH

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Security Solutions and Services Hardcopy Vendor Assessment



Source: IDC, 2017

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

October 2017, IDC #US41988517e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment (Doc # US41988517). 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, although 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 (LOB) 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 10 major hardcopy equipment manufacturers with broad hardware portfolios to specifically address office workgroup/departmental printing environments on a global scale. Given this approach, vendors such as Brother and Epson have been excluded even though they are among the top printing hardware firms based on worldwide revenue because the

majority of their product line is designed for desktop or small work team environments. 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 has become a top-level IT concern among business of all sizes. Nevertheless, IDC's research suggests that print security solutions and services initiatives lag well behind overall IT security for most organizations. Indeed, securing the print environment is often an overlooked element of a comprehensive IT security strategy.

Meanwhile, there is a growing concern over the need to more effectively manage access to information. The ongoing shift to 3rd Platform technologies, including mobile and cloud-based workflows, is changing the way businesses work with documents and business-critical content. Employees, clients, and other knowledge workers now require 24 x 7 access to information from both inside and outside the corporate firewall. CIOs and IT departments face mounting pressure to gain better control over information management.

An organization's own print environment is unique in that it is central to managing data, documents, and information in both the digital and paper formats. The lack of oversight within the print and document environment leaves businesses vulnerable to data- and device-level security breaches through compromised firmware, unsecured networks and document repositories, and information/data leakage. The end result could be extensive staff time and costs to address the breach, fines, and damage to the business reputation. Neglecting to secure the print environment as part of an overall IT strategy leaves an organization vulnerable to significant internal and external cyberthreats.

Accordingly, organizations should consider the following:

- **Determine the level of complexity expected for print and document security over the next three years.** Built-in features designed to provide endpoint security protection for printing devices will become more commonplace in the coming years. But 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.
- **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.

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.

Ricoh

Ricoh is a Leader in our IDC MarketScape for print and document security solutions and services worldwide. Ricoh is headquartered in Tokyo, Japan, with more than 109,000 employees globally.

Ricoh's security offerings fan out from the device at the core through the user interface, embedded applications, network, server, and services. Ricoh focuses on three key areas to mitigate risk in the print environment: print security, information security, and cybersecurity. Ricoh is also taking several steps to address mounting customer concerns regarding security compliance requirements, including expanding risk and compliance assessment offerings and offering assessment-based solutions catering to specific customer needs.

Ricoh offers built-in security features that come standard with its office-class MFP models. These features include encryption keys protected by Trusted Platform Module; firmware signature validation; unauthorized copy protection; user authentication and access restriction, including LDAP authentication and Windows authentication; authentication password encryption; user lockout function; PDF password protection for scanned documents; locked print; hard disk drive encryption unit; and DataOverwriteSecurity System (DOSS). Ricoh also offers IEEE 2600.2 certification via the ISO/IEC 15408 Common Criteria for select products.

Ricoh also offers a broad range of security solutions and services designed to help organizations identify vulnerability gaps, mitigate security risks, and remain compliant with government and industry regulations. Ricoh's managed security services address endpoint and network security, identity access management, and email security. Ricoh's cybersecurity program has been developed in accordance with the defense-in-depth paradigm, and the company's security services map directly to requirements from various regulations such as HIPAA, PCI, and the Gramm-Leach-Bliley Act. Ricoh offers services designed to help businesses manage the removal and disposal of printing hardware.

Strengths

Ricoh's security solutions portfolio, combined with core competencies in managed services, infrastructure services, workflow services, and software development, helps position the firm as one of the leading vendors for addressing security within the print and document environment. Ricoh's global service delivery model enables the firm to deliver consulting services in a standard and consistent manner, which helps set it apart from many of its competitors.

Challenges

IDC believes that Ricoh's overall delivery could be improved with more consistency between direct and indirect go-to-market strategies. Ricoh's marketing strategies could also be improved by articulating

how innovation is being leveraged to drive the technology road map and developing outbound campaigns to increase awareness and promote the company's leadership around print and document security.

Consider Ricoh When

Organizations should consider Ricoh when looking for a broad security solutions and services portfolio, emphasis on network security beyond device protection, and a balanced global service delivery model. Ricoh should also be on the short list when users are looking for a true partner in an ongoing engagement to address evolving technology and compliance changes in real time.

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 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 2017 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

- *Market Analysis Perspective: Worldwide and U.S. Managed Print and Document Services, 2017* (IDC #US41988617, August 2017)
- *IDC MaturityScape Benchmark: Print and Document Management in the United States, 2017* (IDC #US41265117, July 2017)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast, 2017-2021* (IDC #US41264717, May 2017)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares, 2016: Growth in the Midmarket* (IDC #US41264817, May 2017)
- *IDC MarketScape: Worldwide Document Workflow Services Hardcopy 2016 Vendor Assessment* (IDC #US40994416, September 2016)

Synopsis

This IDC study assesses the market for print and document security solutions and services among the top 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.

"For many organizations, print and document security is often overlooked when it comes to developing a comprehensive IT security strategy," says Robert Palmer, research director for IDC's Imaging, Printing, and Document Solutions group. "Despite measures taken to protect IT infrastructure, the lack of visibility and oversight within the print environment creates a weak link that leaves organizations vulnerable to hackers and other cybersecurity threats."

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