IDC MarketScape

IDC MarketScape: Worldwide Print Security Solutions and Services Hardcopy 2025-2026 Vendor Assessment

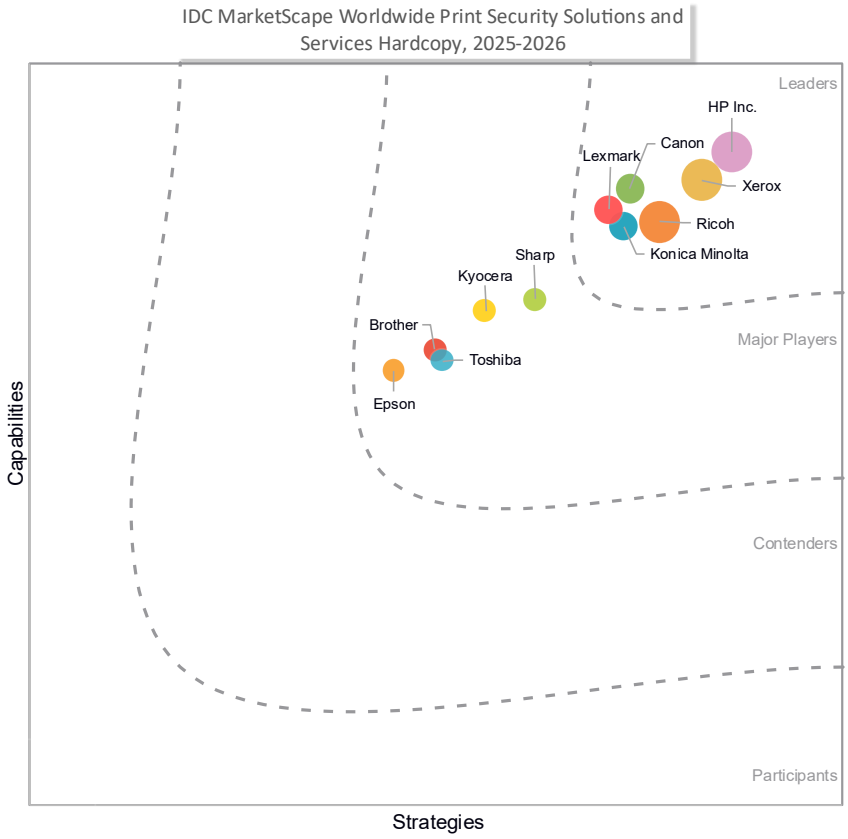
Robert Palmer

THIS EXCERPT FEATURES RICOH AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Print Security Solutions and Services Hardcopy Vendor Assessment



Source: IDC, 2025

December 2025, IDC #US52993425e

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

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Print Security Solutions and Services Hardcopy 2025-2026 Vendor Assessment (Doc # US52993425).

IDC OPINION

This IDC study assesses the market for print 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 document includes an analysis of 11 major hardcopy equipment manufacturers with broad services and solutions portfolios to specifically address the needs for print and document security on a global scale. The vendor must offer a large portfolio of workgroup-class printing hardware, security, and software/solutions while demonstrating participation in the managed print services (MPS) market (either direct or through indirect channels). Excluded from the study were IT outsourcing companies, business process outsourcing (BPO) providers, and software manufacturers that either offer print and document 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

Although organizations continue to prioritize investments in cybersecurity measures, the print environment remains an unrecognized security vulnerability. Cyberhackers always take the path of least resistance, and attacks targeting print devices are on the rise. A rash of printer-related vulnerabilities was identified in 2023, prompting security expert warnings and remediation actions from both printer vendors and software companies. According to IDC's research, the number of print-related security breaches is on the rise. Among companies that have suffered a print security breach, over half have experienced productivity loss, while more than a third have experienced damage to the company's reputation.

Meanwhile, the shift to flexible work practices has fueled increased security concerns related to the print environment, driven by the need to support remote users, cloud-based applications, and outside assets. IDC's 2024 *U.S. MPDS Benchmark Survey* shows that only 61% of businesses say they are "very confident" in their organization's overall print security program, and less than half say that print and document security is very integrated into the organization's overall IT security strategy and governance programs.

Meanwhile, 72% of businesses say keeping pace with print security issues has become more challenging due to the ongoing transition to hybrid work.

Surprisingly, most companies continue to operate on the false assumption that printers are protected because these devices sit behind the corporate firewall. However, the network security perimeter is crumbling, and every device is now a standalone endpoint security risk. Today's printers and multifunction printers (MFPs) have essentially become IoT devices, with embedded processors and data storage, built-in web servers, and direct connectivity to cloud-based applications, services, and document repositories.

Accordingly, organizations should consider the following:

- **Maximize print security in an increasingly distributed environment.** Few organizations have provided proper security guidance to remote employees regarding the procurement and use of printers. Policies range from allowing the use of personal printing devices for business use to providing company-approved devices, or allowing employees to purchase new devices from a preapproved list or based on personal preference. This lack of uniformity across the organization poses significant security risks and has become a focal point for IT managers. Implementing security policies for employee-owned remote printers is the key print security priority over the next two years, according to IDC's research.
- **Support zero trust principles:** Identity is the new perimeter, which is why organizations are moving quickly toward zero trust security principles. Zero trust is a security framework whereby all users, whether in or outside the organization's network, must be authenticated, authorized, and continuously validated for security configuration and posture before being granted access to applications and data. In a zero trust environment, all devices are treated as potential endpoint security threats within a framework designed to "trust nobody and verify everyone." Your print security strategy should be built around a zero trust framework.
- **Consider security as part of a broader print modernization strategy.** Print modernization refers to the overhaul of traditional printing processes to leverage modern technologies and practices. It's about optimizing print processes and document workflow to better enable the future of work. Print modernization is inclusive of policies, processes, and technologies that govern the print and document ecosystem — including creation and capture, workflow and management, security and data protection, and the production and delivery of both print and electronic documents.

- **Shift print to the cloud.** Print modernization begins with shifting print infrastructure to the cloud. Moving away from on-premises servers to cloud-based print management systems allows for remote device access, centralized control, and easier integration with other digital tools. It is also crucial to facilitating the modern security practices essential for today's work environment. According to IDC's research, 67% of organizations say that a cloud-based model would provide for a more secure print environment compared with on-premises print infrastructure.
- **Provide continuous protection through a unified approach.** With a cloud-based print management platform, firmware updates and security patches could be automated and deployed systemwide as needed. This has become a common pain point for businesses with aging print infrastructure, often made up of multiple hardware brands and disparate servers that have been acquired over time. Organizations could expect consistency in security protection with a cohesive set of solutions, services, and best practices deployed across a standardized fleet of devices. A cloud-based model also provides customers with a mobile-ready print ecosystem that allows users to authenticate to and access any print device on the network, supporting secure printing between physical locations within a single office environment and across multiple remote locations.
- **Be future ready.** Printer manufacturers have worked diligently over the past few years to ensure device hardening through continued advancements in embedded endpoint protection. However, the print and document security threat landscape continues to evolve as cyberattacks grow more sophisticated. Emerging technologies, like AI, are being used both as tools of defense and as weapons by attackers while quantum computing threatens to break traditional encryption. Businesses must consider these factors and work closely with their hardware and print service providers to better understand the long-term measures in place for managing these evolving threats, with a focus on enabling a future-ready environment.

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 each vendor's strengths and challenges.

Ricoh

Ricoh is positioned in the Leaders category in this 2025-2026 IDC MarketScape for worldwide print security solutions and services hardcopy.

Founded in 1936, Ricoh's headquarters are in Tokyo, Japan.

Quick facts about Ricoh include:

- **Number of employees:** 78,665 (as of March 31, 2025)
- **Global market coverage:** Operates in approximately 200 countries in the Americas, EMEA, and Asia/Pacific
- **Go-to-market and delivery channels:** Ricoh sells direct and through various commercial channel partners and office equipment dealers.
- **Services and solutions evaluated:** Global study to evaluate solutions and services that address security concerns in the print and document infrastructure, including device-level features and capabilities, software solutions, or professional and managed services
- **Delivery models evaluated:** Scope and focus include capabilities and strategies deployed by hardcopy vendors in support of direct engagements and channel-delivered printing products, solutions, and services.
- **Key differentiator:** Ricoh has leveraged its long-standing printing heritage to expand deeper into digital workplace solutions and information management. The company now offers a full range of advanced digital solutions tailored to support the demands of today's increasingly distributed workforce. Along with its printers and MFPs, Ricoh's portfolio spans business process automation, IT and cloud services, digital workflow design, audio/visual (AV) technologies, and managed services. Ricoh notes that security is integrated into every aspect of these offerings, supported by multilayered protections, industry certifications, and consultative services. Through this integrated approach, Ricoh seeks to help organizations modernize operations, safeguard sensitive data, support compliance initiatives, and maintain trust.

Strengths

- **Zero trust and hybrid work:** Ricoh emphasizes the importance of supporting zero trust security in the face of accelerating trends around remote work, cloud adoption, and the increased sophistication of cyberthreats. In response, Ricoh has embedded zero trust principles into its service design, customer engagements, and internal security architecture to ensure that customers can operate securely, regardless of where data resides. Ricoh applies zero trust

principles across its print and document ecosystem, IT services, and cloud platforms.

- **Print modernization:** The ability to help organizations modernize print operations by shifting all or parts of their print infrastructure to the cloud is a key part of Ricoh's overall approach to print and document security. Through a broad set of both Ricoh developed and partner solutions, customers can leverage the flexibility of cloud and on-premises delivery models while maintaining security and compliance across the print and document environment. As part of this approach, Ricoh offers a range of secure print routing options, including offline direct print, cloud secure print, client PC secure print, and edge printing with gateway integration to enhance security and ensure flexibility in print management.
- **Ricoh IoT Command Center:** Ricoh's IoT Command Center is a central component of the company's print and document security strategy, offering a device-agnostic platform for real-time monitoring and management while providing actionable insights across connected devices. Through a single, centralized dashboard, administrators gain visibility into the status and performance of their entire device fleet, enabling rapid detection and resolution of issues. The platform also drives efficiencies by automated tasks such as firmware upgrades and batch configurations, which helps keep devices current with the latest security patches and features. Advanced analytics powered by AI and machine learning enable predictive management and anomaly detection, while traffic data analysis helps identify potential security threats. The IoT Command Center also provides end-to-end security monitoring, automated compliance auditing, and integration with tools like ServiceNow and Streamline NX.
- **Extended security services offerings:** Ricoh's extended security services play a vital role in the company's overall print and document security strategy. The company provides a comprehensive suite of consultancy and implementation services backed by a deep bench of subject matter experts who help customers assess risks, design secure architectures, and implement solutions that are tailored to specific operational and compliance requirements. These services include integration with legacy business systems, such as ERP and EMR platforms, to ensure seamless interoperability and continuity across the organization's workflows. In addition, Ricoh offers ongoing advisory support to help customers stay aligned with evolving regulatory requirements, including new mandates like NIS2 and the Cybersecurity Resilience Act.

Challenges

- Ricoh may face challenges in helping customers grasp the complexities of modernizing print infrastructure. Many organizations underestimate the technical aspects and integration hurdles involved, often viewing upgrades as straightforward. Bridging this knowledge gap requires clear communication, education, and support to ensure customers fully understand the risks and requirements of modernization.
- Ricoh should continue to work on helping its channel partners to effectively educate SMB customers on the importance of print and document security. Many SMBs lack awareness of security risks associated with print environments, and channel partners may have limited expertise or resources to deliver compelling security messaging and solutions tailored to smaller organizations.

Consider Ricoh When

Organizations seeking to align print and document security with broader initiatives around information management, document workflow, and digital transformation should consider Ricoh. Ricoh's expertise in process optimization, digital workplace solutions, and print modernization can help organizations looking to streamline operations while maintaining high security standards. Those companies looking to deploy secure and effective print programs for hybrid workforces in support of remote and distributed teams should also consider Ricoh. Ricoh's print security model is rooted in zero trust principles, ensuring robust protection across all environments.

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 this 2025-2026 IDC MarketScape for worldwide print security solutions and services hardcopy, 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:

- Endpoint protection and device hardening
- 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 and antimalware/spyware
- Security event management
- Round-the-clock monitoring and management of intrusion detection systems and firewalls
- Overseeing patch management and upgrades
- Performing vulnerability assessments and security audits
- Content security, privacy, and data integrity (hardware and software)

- Installation, configuration, and usage of equipment
- Use of AI across a range of print security applications
- 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 2026 Predictions* (IDC #US53858425, October 2025)
- *Market Analysis Perspective: Worldwide Outsourced Document Services, 2025* (IDC #US52811325, September 2025)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast, 2025–2029* (IDC #US52811525, July 2025)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares, 2024: Modernization Fuels New Opportunities* (IDC #US52811625, July 2025)
- *Windows Protected Print: A Comprehensive Look at the Impact of Microsoft's Efforts to Modernize Office Printing* (IDC #US53439325, May 2025)

Synopsis

This IDC study assesses the market for print 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.

"In today's hybrid work environment, print modernization and zero trust principles are essential for robust document security," says Robert Palmer, research VP for IDC's Imaging, Printing, and Document Solutions Group. "Organizations should work with their print services providers to prioritize secure print environments, leveraging advanced authentication and cloud-based controls to protect sensitive data, mitigate risks, and enable seamless, secure workflows across distributed teams."

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

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