IDC MarketScape

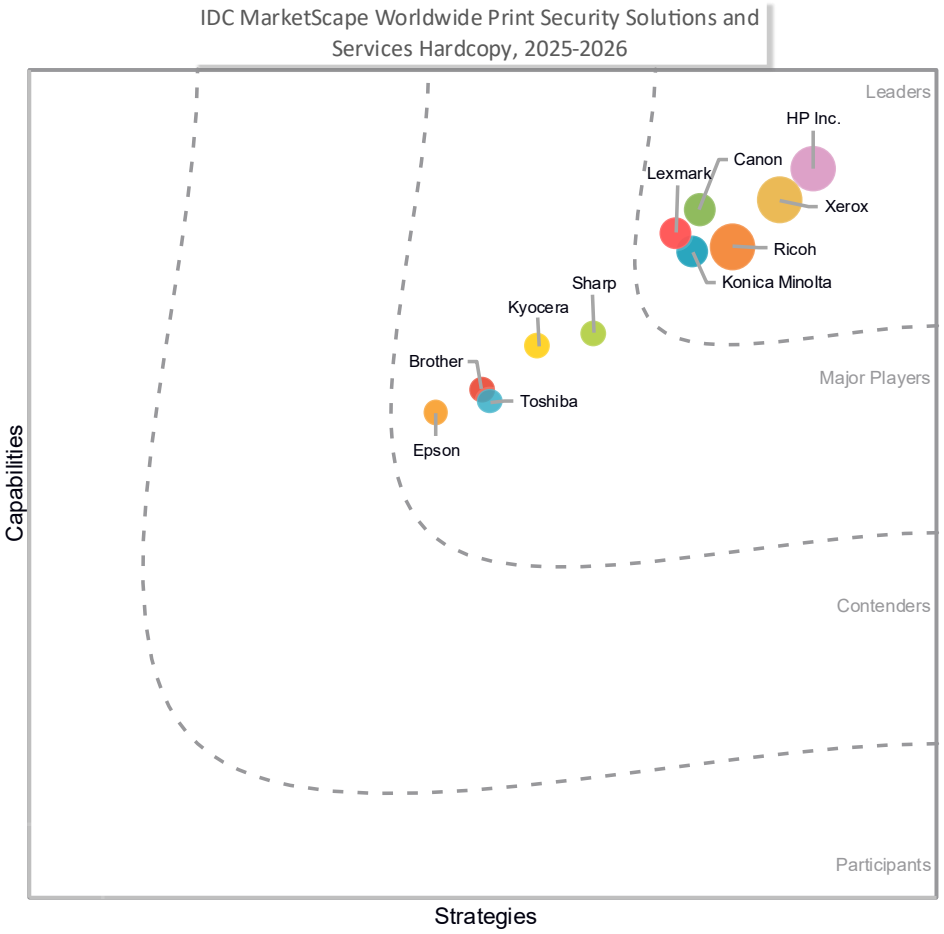
IDC MarketScape: Worldwide Print Security Solutions and Services Hardcopy 2025-2026 Vendor Assessment

Robert Palmer

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Print Security Solutions and Services Hardcopy Vendor Assessment



Source: IDC, 2025

December 2025, IDC #US52993425

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

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 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.

Brother

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

Brother Industries Ltd. is headquartered in Nagoya, Japan and was formed in 1908.

Quick facts about Brother include:

- **Number of employees:** 42,801 (as of March 31, 2025)

- **Global market coverage:** Operates in more than 100 countries in the Americas, Europe, Japan, Asia/Oceania, and the Middle East and Africa
- **Go-to-market and delivery channels:** Brother partners with various commercial channels (e.g., IT VARs, resellers, and office equipment dealers) and retail partners for sales of its printing products.
- **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:** Brother's go-to-market approach helps set the company apart. Rather than relying on a direct sales force, Brother works solely through a network of distribution partners and authorized resellers. Brother's channel partners are empowered with the flexibility to draw from a wide range of resources, enabling them to deliver highly customized security solutions that precisely match each customer's unique requirements.

Strengths

- **Three core pillars:** Brother's approach to print and document security is built on three core pillars. Through device and workflow security, Brother addresses security and data protection across the entire print environment while providing monitoring and reporting capabilities. Brother also collaborates with software providers to deliver enhanced security features and workflow solutions. Professional services available through Brother support teams are designed to support channel partners and customers with assessments, field engineering, and guidance on security policy development and configuration deployment. Last, Brother's development policy involves ongoing market monitoring and collaboration with industry experts to identify emerging threats and evolving standards, enabling Brother to continuously introduce new security features to address evolving vulnerabilities.
- **Holistic security philosophy:** Brother emphasizes what it calls a "triple layer security" approach, which is designed to safeguard devices, documents, and the network. Brother focuses not only on protecting against external threats like ransomware and phishing attacks, but it also takes a proactive approach to limiting unintended breaches by controlling and monitoring access to device functions and preventing accidental leaks. Combining these capabilities with centralized monitoring and management tools, Brother can help customers maintain a strong security posture through timely security updates and firmware

patch management, visibility and security auditing, and ensuring fast and efficient response to threats across the print environment.

- **Brother Solutions Interface (BSI):** The Brother Solutions Interface provides a secure platform for integrating applications with printers and MFPs by ensuring that no applications run directly on the device itself. This unique approach provides Brother customers with a security advantage, as the hardware is incapable of hosting or executing onboard applications, eliminating potential vulnerabilities associated with local software. Instead, BSI enables secure communication between the device and external applications, which are managed on a centralized server. This server-based approach allows for management, control, and protection of applications, with all data exchanges secured through digital certificates and HTTPS protocols.
- **Extended support teams:** Brother's overall device/solutions security approach is strengthened by a dedicated assessment team that works in close partnership with Brother's field engineers and subject matter experts (SMEs). Together, these teams provide professional services to both channel partners and corporate clients, helping identify security risks, strengthen client infrastructure, and implement strategic action plans. This includes expert guidance on deployment and update processes, ensuring a seamless and secure rollout tailored to the organization.

Challenges

- Brother has historically been strong in small and medium-sized business (SMB) and the small office/home office (SOHO) markets, but its penetration into larger enterprise and B2B environments remains limited with the exception of multisite businesses — such as retail, quick service restaurants, and convenience stores — where many devices must be deployed, managed, and maintained across multiple locations. Brother stands out as a differentiated and capable partner in multisite environments. Brother is also able to leverage alliances with other vendors such as Ricoh and Toshiba to extend support into the larger organizations and global opportunities. As it works to expand its workgroup-class product portfolio, Brother must continue to develop a strong set of distributors and channel partners with capabilities to support the broader security and IT needs of larger organizations.
- Brother's range of direct delivered professional and managed services varies by region. In some regions, Brother relies on channel partners to deliver these services alongside its product portfolio.

Consider Brother When

Organizations seeking a comprehensive approach to print and document security should consider Brother for its holistic security strategy. Brother demonstrates notable strength in device, workflow, and network security, which is supported by professional security services and dedicated teams that assist with security policy development, deployment, and ongoing management. Brother's expertise is particularly evident in the SMB sector, where the company's tailored solutions and support are well suited to the unique needs of smaller businesses. For organizations prioritizing robust security, policy guidance, and a secure, closed platform, Brother offers a compelling choice that aligns with both operational and compliance requirements.

Canon

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

Founded in 1937, Canon's headquarters are in Tokyo, Japan.

Quick facts about Canon include:

- **Number of employees:** 170,340 (as of December 31, 2024)
- **Global market coverage:** Operates in approximately 220 countries in the North America, Europe, Latin America, Europe, Middle East, Africa, and APAC
- **Go-to-market and delivery channels:** Canon sells direct to large enterprise accounts. For SMB customers, Canon's products are sold through various channel partners (e.g., IT VARs, resellers, and office equipment dealers) and retail distribution.
- **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:** Canon stresses a multlayered approach to security, which allows it to meet customer requirements across all customer segments and operating environments. This approach is rooted in five key pillars: device security, document security, print security, information security, and cybersecurity. Throughout this holistic approach, Canon emphasizes direct alignment with the NIST Cybersecurity Framework (CSF) and zero trust security principals.

Strengths

- **Built-in security at every level:** Canon's approach to security is rooted in a "secure by design" philosophy, meaning security is embedded from the ground up rather than added as an afterthought. This commitment spans six critical dimensions. Canon devices are engineered with integrated security features such as secure boot, data encryption, and user authentication. Canon software solutions and application platforms are developed using secure life-cycle practices, including regular updates and proactive vulnerability management. Canon's internal infrastructure and systems are safeguarded by robust security protocols to ensure resilience and data integrity. Managed and professional services encompass secure print, document handling, and compliance support, while secure deployment and configuration practices minimize risks during delivery and implementation. Last, Canon support provides ongoing monitoring, incident response, and proactive updates, reflecting a comprehensive commitment to maintaining security throughout the product life cycle.
- **Continuous innovation:** Canon has a broad portfolio of security offerings, beginning with device-level functionality/hardening and extending outward to provide solutions and services that ensure continuous protection for documents and data. Canon has been at the forefront for driving adoption and implementation of secure printing features and technologies, driving innovation in areas such as information security, access, and management while helping ensure compliance with data protection regulations and reducing data leaks.
- **Global consistency and future-ready approach:** Canon has expanded its security portfolio to align with customer priorities and regional needs. By establishing dedicated organizations and acting as a trusted advisor, Canon ensures that its security, software, and device offerings remain both local in relevance and global in quality. The company's forward-looking approach also allows it to anticipate the next phase of cybersecurity challenges. Through this comprehensive approach, Canon looks to evolve in tandem with market demands and technological shifts, striving to deliver resilient, future-ready solutions that adapt to a rapidly changing digital environment.
- **Subscription security services:** Canon offers a comprehensive range of subscription security services designed to protect devices throughout the entire life cycle. These services fall into four primary categories: **Discovery** (assessments to establish a security profile), **Before Use** (preconfiguring devices based on the determined security profile), **In Use** (data backup, firmware updates, continuous monitoring, and management of the secure profile), and **After Use** (data destruction services to prevent data leakage at end of life). The subscription security services are available in Enhanced and Premium levels and

can be purchased on a per-device, per annum basis depending on customer needs.

Challenges

- Canon's overall security approach combined with the company's broad security solutions and services portfolio have been instrumental in driving the company's direct MPS business. Enabling channel partners to take advantage of these same capabilities is crucial for Canon as the market for MPS and other contractual print services continues to move downmarket to SMB.
- Canon should continue to tailor its print and document security solutions to meet the distinct requirements of specific vertical sectors. Industries such as healthcare, finance, and legal have unique compliance, data protection, and workflow needs. Canon has already done much in this area, but it will need to stay current with evolving requriements to ensure ongoing protection and regulatory compliance.

Consider Canon When

Organizations should consider Canon when looking for a vendor with specific expertise in both secure information management and device-level protection. Canon excels in safeguarding data and managing devices, offering advanced solutions and services that address security requirements across the entire product life cycle — from deployment to end of life. Canon's global consistency in both solutions and service delivery provides reliable protection and support for multinational enterprises, ensuring standardized security practices, regardless of location. With a proven history of innovation in print and document security, Canon stands out as a trusted partner capable of delivering advanced, reliable, and forward-looking security solutions.

Epson

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

Formed in 1942, Epson is a public company based in Nagano, Japan.

Quick facts about Epson include:

- **Number of employees:** 75,350 (as of March 31, 2025)
- **Global market coverage:** Operates in more than 150 countries in North America, Latin America, Europe, and APAC
- **Go-to-market and delivery channels:** Epson sells primarily through a distributor-based sales model, leveraging commercial channels (e.g., IT VARs,

resellers, and office equipment dealers) and retail partners for sales of its printing products.

- **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:** Epson's overall approach for print and document security centers on building trust through rigorous protection standards and transparent, life-cycle-based security management. The company integrates advanced safeguards into every stage of product planning, development, and operation, emphasizing that true security extends beyond device-level protection.

Strengths

- **Broad portfolio:** Epson offers a comprehensive portfolio of print and document security solutions that integrate hardware safeguards, software controls, and cloud-based services into a unified security framework. Epson's hardware products, ranging from printers and multifunction devices to scanners, are equipped with multilayered defenses addressing threats such as unauthorized access, data leakage, and network intrusions. Epson also offers a range of security services encompassing secure device deployment, ongoing operational safeguards, and maintenance assistance, helping customers maintain a secure print and document environment.
- **Epson life-cycle security concept:** Epson's life-cycle security concept is structured around the six key principles of the NIST Cybersecurity Framework. This framework guides Epson in developing comprehensive security measures that address both proactive and reactive needs. Epson is dedicated to meeting customer security requirements by continuously enhancing the functionality of its products and solutions.
- **Flexible delivery model:** Epson deploys a delivery model built on flexibility, interoperability, and life-cycle resilience. The company supports both on-premises and cloud-based environments through a portfolio of technologies designed to protect devices, data, and user interactions across complex infrastructures. This adaptable approach supports hybrid and remote environments, allowing businesses to maintain operational continuity while safeguarding sensitive information. For Epson, cloud systems security and reliable personal information protection are high priorities.

- **Hybrid work and zero trust:** Guided by an adherence to zero trust security measures, Epson works to ensure that its products can be deployed and utilized securely in any environment. As the need to support hybrid work models continues to expand, Epson sees a growing need among businesses of all sizes to maintain consistent security practices and policy management across remote and distributed environments.

Challenges

- Despite continued advancements in print and document security solutions and services, Epson's overall marketing and messaging is not as visible to the market as some of the company's competitors. IDC believes that Epson could benefit from driving increased awareness of its print and document security capabilities and expertise.
- Epson does not provide managed or professional services, such as direct managed print services, security assessment services, or ongoing security monitoring and management security services, through its own organization. Instead, Epson relies on channel partners to deliver these services alongside its product portfolio.

Consider Epson When

Organizations seeking comprehensive print and document security should consider Epson for its life-cycle-based security management philosophy, which ensures protection at every stage, from product development through deployment and end of life. Epson offers a broad portfolio of security solutions and services, providing foundational support for key guiding frameworks such as the NIST Cybersecurity Framework and zero trust principles. This alignment helps organizations meet regulatory requirements and industry best practices. Epson's flexible delivery models allow businesses to choose solutions that best fit their operational needs, whether on premises, cloud based, or hybrid. In addition, Epson excels in delivering secure solutions for remote and distributed environments.

HP Inc.

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

Formed in 1939, HP Inc.'s worldwide headquarters are in Palo Alto, California.

Quick facts about HP Inc. include:

- **Number of employees:** Approximately 58,000 (as of FY24)

- **Global market coverage:** Operates in 180+ countries in North America, Latin America, Europe, Middle East and Africa, and Asia/Pacific
- **Go-to-market and delivery channels:** HP Inc. sells products direct and through a network of channel partners (e.g., IT VARs, resellers, and office equipment dealers) and through retail distribution. In addition, HP Inc. offers managed print and document services direct and through its various channel partners.
- **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:** HP Inc.'s secure-by-design approach ensures that security is integrated throughout the ecosystem, from endpoint devices to workflow, solutions, services, and product development life cycle. HP Inc. recognizes that many organizations lack a future-ready infrastructure and often struggle with visibility and management of their device fleets. To address this, HP Inc. emphasizes the need for dynamic, endpoint-based security that is both easy to manage and aligned with zero trust principles. The company is committed to balancing security with usability while reducing risk and cost for customers by simplifying the management of security across their environments.

Strengths

- **Endpoint protection and detecting zero-day attacks:** Endpoint security is clearly a strong point for HP Inc., and the company has consistently looked to innovate around embedded device-level protection over the past several years. HP Inc.'s embedded device and solutions security strategy is built on the principle of "assume attack." As a result, the company strives to deliver HP Inc. printing devices that can detect, isolate, and neutralize threats dynamically while utilizing self-healing technology at all device-level stages. One key area of focus for HP Inc. is the detection of zero-day attacks, which has become crucial as threat actors increasingly use generative AI to modify malware to evade traditional defenses.
- **Future-proof security:** HP Inc.'s approach to delivering print and document security is fundamentally rooted in the belief that the future of work cannot exist without robust protection. HP Inc. distinguishes itself by pairing robust endpoint protection with security solutions specifically designed to ensure uptime. Through tools such as the HP Workforce Experience Platform and HP Security Manager, HP Inc. provides the resources needed to achieve visibility, control, and

resilience even as the organization expands. This overall approach is designed to help customers maintain an adaptive, future ready, and resilient security posture, not only across endpoint devices but also throughout workflows and service interactions.

- **Related security services:** Globally, HP Inc. delivers a total of 326 services offerings across all routes to market. The company's breadth of professional and consulting services offerings that complement its core print security capabilities spans a broad spectrum covering the IT environment.
- **Innovation:** HP Inc. has remained at the forefront of the industry when it comes to security for the office print environment. Over the past decade, HP Inc. has consistently pushed innovation through continued advancements in areas such as device hardening and threat detection, supply chain certification, zero trust initiatives, secure VPN, hardware-based intrusion detection, control flow integrity monitoring, bug bounty programs, AI-enabled security features, and quantum resistance. In April 2025, HP Inc. introduced the world's first quantum-resistant printers.

Challenges

- Many organizations still rely on legacy print infrastructure, which can be difficult to modernize and integrate with advanced security frameworks, cloud platforms, and digital workflows. Legacy devices with outdated firmware and unsupported security patches pose ongoing risks, and transitioning customers to modern, secure print environments remains a significant hurdle.
- Despite growing cybersecurity concerns, print security often remains a low priority for organizations compared with other IT initiatives. This challenge is compounded by the difficulty of engaging the right stakeholders in security discussions and the costs associated with modernizing print infrastructure. HP Inc. will need to continue to raise awareness around print security vulnerabilities while further strengthening its security messaging and thought leadership.

Consider HP Inc. When

Organizations seeking advanced print and document security should consider HP Inc. for its innovation and prioritized focus on endpoint protection and device hardening. HP Inc.'s robust IT backbone enables the delivery of a broad range of products, solutions, and services, seamlessly integrating print security within the wider IT environment. Supporting HP Inc.'s deep industry knowledge and experience is a strong bench of security subject matter experts, helping ensure expert guidance and support. Meanwhile, HP Inc. offers a comprehensive portfolio of security-related professional and managed services, providing tailored solutions for organizations of all sizes.

Konica Minolta

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

Founded in 1873, Konica Minolta's headquarters are in Tokyo, Japan.

Quick facts about Konica Minolta include:

- **Number of employees:** 35,631 (as of March 31, 2025)
- **Global market coverage:** Operates in more than 100 countries in North America, Europe, APAC, and the Middle East/Africa
- **Go-to-market and delivery channels:** Konica Minolta sells direct and partners with various commercial channels and office equipment dealers for sales of its printing products.
- **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:** Konica Minolta distinguishes itself from competitors through its vertically integrated security-by-design architecture. Key to this approach is the fact that Konica Minolta develops and manages firmware, applications, cloud services, and security operations entirely in-house. This approach eliminates supply chain vulnerabilities and prevents unauthorized code execution. Supporting this architecutre is a broad set of advance security measures, including firmware-level antivirus, embedded antimalware, automated remediation, and secure fleetwide patching, ensuring comprehensive and controlled protection across all devices.

Strengths

- **Layered security model:** Konica Minolta's layered security model for print and document security is designed to address the unique needs of each customer, recognizing that a one-size-fits-all approach is not effective. The model allows security measures to be scaled according to factors such as the customer's environment, fleet size, document types, risk appetite, and compliance requirements. At the foundational level, basic security features include document storage encryption, automatic deletion of documents, antivirus protection, and hardening of multifunction printers as secure endpoints. At the

highest level, centralized security management is provided, enabling real-time monitoring, policy enforcement, and automatic remediation of compromised security settings. This layered approach ensures that security policies remain effective and adaptable, supported by dashboards for visibility and control.

- **Governance and compliance:** Konica Minolta stresses that its MFPs, software, and managed services are designed and built under strict security governance guidelines. Konica Minolta's dedication to compliance with global industry standards and governance, along with partnerships with security vendors, ensures the safeguarding of sensitive information for all customers.
- **Embedded Bitdefender:** Konica Minolta incorporates Bitdefender antimalware technology directly within the firmware of its bizhub i-Series multifunction printers. The embedded solution provides real-time scanning and monitoring of files processed by the device, including documents transmitted through scanning, printing, or network transfers. The Bitdefender component operates as a low-cost, embedded license that requires minimal configuration. Once activated, it runs natively within the MFP's system software, enabling continuous threat detection without the need for separate installation or complex setup. Administrators can define automated response actions — such as logging, alerting, or quarantining — according to organizational security policies. Bitdefender's signature and heuristic updates are delivered frequently, helping ensure that the bizhub MFP remains protected against emerging malware variants. This integration enhances device-level security while maintaining low administrative overhead, aligning with enterprise efforts to extend endpoint protection to network-connected imaging devices.
- **Extended services portfolio:** Konica Minolta offers a comprehensive range of professional and managed consulting services to augment its core print security offerings. This includes an extensive set of managed IT and cybersecurity services, infrastructure and network services, managed print and document services, collaboration and cloud services, and workflow services. By combining the strengths of its print security solutions and consultative services, Konica Minolta can support the most complex customer environments and use cases to provide end-to-end security across the entire IT environment and document life cycle.

Challenges

- Konica Minolta has experienced financial pressures across its print-related business units. The company will need to ensure that it can continue to invest in solutions and services to address evolving needs related to next-generation print security.

- Given its holistic approach, Konica Minolta should continue to focus on helping customers address print security within the broader context of an overall IT security program. Integrating print security with existing IT security frameworks and compliance requirements can be complex, requiring specialized expertise and resources.

Consider Konica Minolta When

Organizations should consider Konica Minolta when seeking a vendor that maintains tight control over the entire design, development, and security operations of its products. The company's commitment to achieving compliance with global industry standards and certifications should also be considered, as this provides assurance for those organizations with stringent regulatory requirements. In addition, Konica Minolta's broad portfolio of print-related and nonprint-related services enables organizations to address a wide range of business needs with a single, trusted partner.

Kyocera

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

Kyocera Document Solutions (Kyocera) headquarters are in Osaka, Japan.

Quick facts about Kyocera include:

- **Number of employees:** 21,776 (as of March 2025)
- **Global market coverage:** Operates in 170+ countries in Africa, the Americas, Asia, Europe, and Oceania
- **Go-to-market and delivery channels:** Kyocera provides office equipment and print services through various channels, including direct, indirect, and distributors.
- **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:** With its approach to print and document security, Kyocera identifies the protection of customer information assets as a priority. The company implements a wide range of security measures to defend against increasingly sophisticated and diverse threats. Kyocera seeks to continuously

enhance the usability of its MFPs and printers while maintaining and improving high security standards.

Strengths

- **Confidentiality, integrity, and availability:** Kyocera's approach to print and document security centers on the three key attributes of confidentiality, integrity, and availability. Confidentiality is maintained through robust access controls, including identification and authentication functions that prevent unauthorized access to information and inadvertent disclosure of business-critical data. Integrity is enabled through secure technologies such as data encryption to safeguard against unauthorized attacks. Availability is ensured by features such as interface block functions to restrict network access and defend against denial-of-service attacks.
- **Product development and life-cycle security:** Kyocera's approach to product development and life-cycle security involves implementing robust countermeasures at every phase, from planning to post sales. In the planning phase, Kyocera monitors security trends and analyzes customer requirements to address issues early. During development, security functions are built-in and vulnerabilities are checked against both internal and third-party security evaluations. In production, strict operational processes ensure a secure environment. After sales, Kyocera remains responsive to market security concerns, providing timely support and updates as security needs evolve.
- **MPDS offerings:** Kyocera offers a full range of capabilities within its managed print and document services programs, ranging from fleet optimization to cloud-based print/scan, print and information security, governance and change management, break/fix support, tracking and reporting, and multivendor management. With its focus on document management and content-centric applications, Kyocera leverages its MPDS approach to help customers improve information security while driving workflow automation and efficiencies.

Challenges

- While Kyocera has made significant progress in expanding its security services, a key challenge remains in achieving greater global consistency across its capabilities and delivery model.
- Kyocera faces limited market awareness of its overall efforts in print and document security. Kyocera should look to enhance communication strategies to increase the visibility of its security capabilities and more clearly articulate the value of its solutions to customers, partners, and industry stakeholders.

Consider Kyocera When

Organizations should consider Kyocera when seeking a vendor with specific expertise in areas realted to ECM, document management, and content-centric applications. Kyocera offers a highly integrated approach to information security, device hardening, and network protection, providing a solid foundation for protecting business-critical assets.

Lexmark

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

With headquarters in Lexington, KY, Lexmark was founded in 1991 as a spinout of IBM.

Note: In July 2025, Xerox Corp. completed its acquisition of Lexmark International, Inc. from Ninestar Corp., PAG Asia Capital, and Shanghai Shouda Investment Centre. However, the two companies will continue to go to market with separate products and sales strategies for the near term, at least until 2026. For that reason, we have evaluated Xerox and Lexmark separately for this IDC MarketScape.

Quick facts about Lexmark include:

- **Number of employees:** Approximately 8,700 (as of July 2025)
- **Global market coverage:** Operates in 170+ countries in North America; Asia/Pacific; Europe, the Middle East, and Africa (EMEA); and Latin America
- **Go-to-market and delivery channels:** Lexmark 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:** Lexmark's approach to print and document security is defined by the company's "Secure by Design" framework, which is structured around four pillars: products, solutions, services, and standards. Beginning with products, Lexmark embeds robust security features into its devices, including endpoint protection, system hardening, secure data storage, and support for network safeguards, while remote management capabilities restrict configuration access to authorized personnel. Through its secure fleet

management solutions, Lexmark enables administrators to maintain compliance and enforce security policies across all devices. Lexmark offers a comprehensive set of security services to protect the entire print and document ecosystem through standardization, ongoing monitoring, and governance. Last, adherence to industry and government security standards is ensured through third-party certifications and oversight by a dedicated security governance team.

Strengths

- **Zero trust principles:** Lexmark emphasizes the importance of zero trust principles in supporting today's distributed print environments. The company's approach to enabling zero trust for print focuses on advanced device management, conformance tools, and robust on-device protections. Lexmark's solutions can enable and enforce strict access controls and continuous verification across hardware, software, and network layers. Its products feature runtime and firmware protections, security analytics, and tailored solutions to address diverse organizational risk profiles. Through device and data hardening, as well as comprehensive security services, Lexmark ensures that only authorized users and processes can access print resources, supporting a resilient and adaptive zero trust architecture for modern enterprises.
- **Supply chain security initiatives:** Lexmark stresses supply chain security as critical to its overall market approach. In fact, Lexmark points out that it was the first print vendor with an ISO 20243 supply chain security certification for the entire printing device, including cartridges, supplies, and integrated solutions. Throughout each stage of the supply chain, Lexmark emphasizes compliance, security, and social responsibility among employees, manufacturers, and suppliers. This approach is intended to ensure that its products and parts are produced according to specifications, ensuring authenticity and reducing customer risk.
- **Security services:** Lexmark offers a comprehensive range of security services grouped into three primary categories: security consulting, security assessment, and configuration management. Security consulting assists customers in identifying and addressing general print security concerns, while security assessment focuses on uncovering risks, vulnerabilities, and potential improvements specific to their print fleet. Configuration management protects printing and scanning environments through managed standardization and ongoing monitoring. Together, these services can help customers uncover vulnerabilities, map out a remediation strategy, and maintain security compliance through ongoing monitoring and management.
- **Implementation flexibility:** Lexmark supports a variety of implementation and delivery methods for its print solutions and services, including cloud, on

premises, and hybrid options. Lexmark works to ensure that its secure print and document solutions are aligned with each customer's technological journey, providing adaptability and future-ready capabilities. By delivering tailored security and deployment options, Lexmark ensures that customers can confidently manage their print environments as situations evolve.

Challenges

- As the threat landscape evolves, the frequency of print-related security breaches is increasing, with sophisticated attacks leveraging AI-driven methods becoming more commonplace. Lexmark must continually invest in advanced security capabilities to keep pace with emerging threats.
- Navigating diverse and evolving regulatory environments, such as data sovereignty and industry-specific compliance standards, can be challenging. While Lexmark has already done much in this area, it must continue to ensure that its solutions and services are adaptable to meet these evolving requirements, which may vary significantly across regions and vertical markets.

Consider Lexmark When

For businesses prioritizing security, compliance, and customer-driven innovation, Lexmark stands out as a reliable partner in the print and document security landscape. Lexmark's "Secure by Design" approach and holistic security coverage are rooted in advanced capabilities around fleet management, certificate management, security dashboards, cloud infrastructure, compliance, and much more. At the same time, Lexmark demonstrates broad support for industry standards and certifications, providing confidence in regulatory alignment.

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.

Sharp

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

Sharp's headquarters are in Osaka, Japan. The company has been majority owned by Taiwanese Foxconn Group since 2016.

Quick facts about Sharp include:

- **Number of employees:** 39,955 (as of June 30, 2025)
- **Global market coverage:** Operates in 160+ countries in the Americas, EMEA, Asia/Pacific, China, and Japan
- **Go-to-market and delivery channels:** Sharp 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:** Sharp's unified security approach helps set the company apart from competitors in its ability to address print and document security. By integrating governance, design standards, and threat response capabilities across its portfolio — including multifunction printers, displays, and IT services — Sharp creates a consistent and enterprise-grade security ecosystem spanning multiple geographies. Sharp's Cross-Product Cybersecurity Centre of Excellence serves as the foundation for this strategy, ensuring that security practices are standardized across all solutions.

Strengths

- **Multilayered device protection:** Sharp utilizes a multilayered approach for device security to ensure that protection is embedded at every level. By integrating hardware-anchored controls with flexible, centrally managed policies, Sharp's MFPs and printers offer robust protection against threats such as firmware tampering, malware, network intrusion, and unauthorized access. The inclusion of optional third-party antivirus and comprehensive telemetry

capabilities enables real-time monitoring and rapid incident response, supporting IT administrators and security teams in maintaining a secure print environment. The Sharp Security Suite, which encompasses both native and optional security features, empowers organizations to plan and implement effective risk prevention and control strategies tailored to their specific needs.

- **Sharp Complete Print Security:** Sharp's Complete Print Security Offering is designed to provide customers with a turnkey IT security subscription service that protects MFPs from delivery through decommissioning. Tailored for small to medium-sized businesses, this service minimizes operational impact by handling all aspects of print security on behalf of the customer. The service integrates device security setup, based on customer feedback and automated security profiling, to ensure devices are delivered securely configured and aligned with organizational policies. Print management features, such as secure pull printing and auditing, are available through both on-premises and cloud solutions. Device management is maintained via remote monitoring, enforcing security policies throughout the MFP's life cycle. Meanwhile, security information and event management (SIEM) monitoring enables real-time threat detection and remediation.
- **Synappx solutions platform:** Sharp's Synappx solutions suite includes Synappx Go (collaboration and print and scan), Synappx Cloud Print, and Synappx Manage (remote monitoring and management). Running a secure, cloud-based framework, Synappx leverages zero trust principles, enterprise identity integration, and modern cloud standards to ensure robust security and compliance. The suite enables organizations to efficiently manage device fleets while maintaining high levels of data protection and regulatory compliance.
- **Related services portfolio:** Sharp offers a broad range of related managed and professional services designed to complement its approach to print and document security. Through its IT support offerings, Sharp can act as an outsourced IT department, provide 24 × 7 helpdesk support, or deliver comanaged IT services tailored to each client's needs, from basic troubleshooting to advanced cloud architecture. Backup and disaster recovery services include the design, implementation, and support of both on-premises and cloud-based solutions. Sharp's cybersecurity services encompass risk assessments, audits, security awareness training, endpoint management, email and firewall security, and compliance management. These services enhance Sharp's core print security capabilities.

Challenges

- Keeping pace with evolving customer needs for print and document security is challenging due to rapid technological change, complex compliance standards,

and rising cybersecurity threats. Sharp will need to continue to drive R&D investement to push security innovation across its entire portfolio of solutions and services.

- Establishing consistencies in global service delivery is difficult due to regional regulatory differences, varying customer expectations, and diverse infrastructure maturity. Like all vendors serving the SMB market, Sharp will need to continue to align technology, service standards, and support models worldwide while managing localization, language barriers, and partner capabilities.

Consider Sharp When

Consider Sharp when seeking a vendor with a unified security framework that can span across multiple IT assets, including multifunction printers, interactive displays, laptops, and IT services. Sharp benefits from the financial strength and global reach of the Foxconn Group, ensuring stability and scalability. In addition, Sharp's solid presence in the SMB segment, supported by a diverse network of trusted channel partners, enhances accessibility and responsiveness for smaller organizations looking to benefit from Sharp's portfolio and expertise.

Toshiba

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

Toshiba Tec Corp.'s headquarters are in Tokyo, Japan.

Quick facts about Toshiba include:

- **Number of employees:** 15,509 (Toshiba TEC, as of March 31, 2025)
- **Global market coverage:** Toshiba Tec operates in 140+ countries around the world.
- **Go-to-market and delivery channels:** Toshiba 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:** Toshiba's approach to print and document security centers on the company's SecureMFP framework, which delivers comprehensive

protection through a holistic focus on products, processes, and people. By combining advanced technology with proactive security assessments and expert services, Toshiba ensures that every aspect of the print environment is protected. This integrated strategy supports end-to-end security, addressing risks throughout the document life cycle, from creation and output to storage and disposal.

Strengths

- **Security across multiple vectors:** Toshiba's print and document security is structured around five key areas: device, access, document, fleet, and cloud. Toshiba ensures device integrity with BIOS protection, hard drive encryption, and defenses against unauthorized firmware. Access is secured through identity and access controls using multifactor authentication and roles-based policies. Toshiba's devices also offer built-in security for all input sources, providing safeguards for documents covering capture through distribution. In the U.S. market, fleetwide security management is achieved through Toshiba's Elevate Sky Suite, which enables consistent policy enforcement across organizations. Last, Toshiba's devices provide extra cloud security through built-in antimalware protection, which prevents ransomware and phishing attacks by prohibiting unauthorized software from running on the device.
- **Fleetwide security:** Through its cloud-based Elevate Sky suite of services, administrators can centrally monitor, apply, and manage security policies across all Toshiba multifunction printers. This unified platform simplifies oversight, enabling remote management and policy enforcement to align with organizational standards. By providing real-time visibility and accountability, Toshiba Elevate Sky helps organizations maintain strong security governance, minimize risks, and ensure compliance.

Challenges

- Greater integration between Toshiba's print and document security solutions and the company's broader IT products and services would enhance its value proposition by delivering unified security management and improved visibility across environments.

Consider Toshiba When

Organizations should consider Toshiba when looking for a vendor with a strong portfolio of print and document security solutions and services. Toshiba's holistic approach to security ensures comprehensive protection across the entire print and document environment. Meanwhile, Toshiba's Elevate Sky suite provides a strong foundation for companies looking for secure cloud-based print management capabilities.

Xerox

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

Xerox's headquarters are in Norwalk, Connecticut.

Note: In July 2025, Xerox Corp. completed its acquisition of Lexmark International, Inc. from Ninestar Corp., PAG Asia Capital, and Shanghai Shouda Investment Centre. However, the two companies will continue to go to market with separate products and sales strategies for the near term, at least until 2026. For that reason, we have evaluated Xerox and Lexmark separately for this IDC MarketScape.

Quick facts about Xerox include:

- **Number of employees:** More than 16,500 in nearly 60 countries
- **Global market coverage:** Xerox operates in 145 countries around the world.
- **Go-to-market and delivery channels:** Xerox 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:** Xerox's approach to print and document security is differentiated by a comprehensive security framework based on a zero trust model that encompasses hardware, software, processes, content, and services. Its zero trust architecture is designed to combat threats across multiple vectors, including users, devices, network, applications, and data, all of which is supported by continuous measurement through internal and external assurance programs. Building on this foundation, Xerox now implements a cybersecurity mesh architecture, which unites diverse tools and controls to protect modern, distributed environments. This approach strengthens Xerox's ability to deliver secure workplace and production solutions aligned with its cloud-first, mobile-first strategy.

Strengths

- **Device-level security:** Xerox continues to push innovation in areas of device hardening and endpoint protection. Xerox's Secure Workplace Print strategy emphasizes automation to minimize human intervention in security delivery,

reinforcing the company's comprehensive security framework across all device operations. Its approach to device-level security begins with capabilities that provide built-in protection "out of the box," with safeguards embedded into all of its ConnectKey-enabled products. For Xerox, device security spans prevention, detection, and protection layers.

- **Cloud-first strategy:** Xerox's cloud-first strategy is central to the company's approach to print and document security, emphasizing flexibility, efficiency, and resilience across client environments. By architecting solutions as multitenant, native cloud applications rather than simply migrating on-premises systems, Xerox delivers scalable, secure services that align with modern enterprise needs. Through this approach, Xerox can help lower IT management costs, support a true SaaS model, enable zero trust security principles, and reduce print infrastructure footprint. Clients can deploy solutions on premises, in private clouds, or through Xerox's native cloud platform.
- **Broad solutions portfolio and services:** Xerox offers a broad portfolio of print-related solutions and services, including solutions for cloud print management, fleet security management (cloud and server based), secure device management, document management, workflow automation and optimization, and a host of others. Meanwhile Xerox's print and document security approach is supported by a range of professional and managed services that run the full gamut from security audits and assessments to security event and policy management, patch management, workplace services, cloud services, and an extensive range of MPS offerings.
- **IT services:** Xerox's continued efforts to broaden the company's capabilities in IT services bring added value to its overall security approach. With the acquisition of ITsavvy, has expanded its IT capabilities, enhancing its ability to strengthen the customers' cybersecurity posture and address evolving threats across the entire IT environment.

Challenges

- Xerox faces some integration challenges associated with the Lexmark acquisition as it works to develop a unified and cohesive approach to the office printing market. This is particularly true as it looks to unify its print services offerings.
- Xerox has established strong capabilities and expertise in the enterprise sector, which it can draw from as it looks to move further down market. However, Xerox will need to continue to tailor its solutions to meet the specific needs of SMB while further educating customers on the security risks associated with the print and document environment.

Consider Xerox When

For businesses prioritizing zero trust, cloud modernization, and holistic security, Xerox should be high on the list among vendors to consider. Xerox's comprehensive security framework is built around zero trust principles, which is key to addressing the evolving needs of distributed environments and hybrid workforces. With its cloud-first strategy, Xerox can help customers modernize their print infrastructure while strengthening security posture, offering scalable and flexible solutions that adapt to changing business requirements. At the same time, Xerox's broad portfolio of security solutions and services provides robust protection across the entire IT environment.

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.

Strategies and Capabilities Criteria

Tables 1 and 2 provide key strategy and capability measures for the success of hardcopy vendors in delivering print security solutions and services.

TABLE 1

Key Strategy Measures for Success: Worldwide Print Security Solutions and Services Hardcopy

Strategies Criteria	Definition	Weight (%)
Functionality or offering strategy	This demonstrates how the vendor plans to extend and develop its solutions and services to address security within the print and document infrastructure. A wide variety of approaches will be employed to ensure increased functional and industry capability, including market sensing capabilities, offering reinforcements, and strategic hiring and training. A strategic road map that addresses both device-level and content security issues should be emphasized. The road map should provide specific information regarding the use of advanced technologies (e.g., cloud, mobile, AI, and big data/analytics) within the offering, as well as address increasing requirements for regulatory compliance and specialization in vertical markets. It looks specifically at how vendors are executing on the road map. What is the planned rate of introduction of new features, functions, and capabilities targeting print and document security? This will evaluate features embedded at the device level, through standalone software solutions and professional and managed services. Vendors should also emphasize systems integration and interoperability, including current and planned support of third-party software solutions. To ensure maximum impact, organizations will need to increase their ability to construct offerings that address print and document security concerns across multiple vectors, including detection, remediation, and regulatory compliance. Current development of offerings will be relevant and attractive to customers over the next three to five years. In addition, effective firms must have a solid strategy for uncovering future customer requirements and articulating a road map strategy that aligns with evolving customer needs.	45.00

TABLE 1

Key Strategy Measures for Success: Worldwide Print Security Solutions and Services Hardcopy

Strategies Criteria	Definition	Weight (%)
Delivery	Plans are in place for support of delivery and billing models to match shifting customer preferences for adoption/consumption in the next five years. The plan should identify and address current gaps/opportunities in various print and document security solutions and services delivery models, with strategies to address target product/customer segments, focusing on a diverse set of delivery models (e.g., packaged software versus SaaS). The delivery model strategy should articulate how the vendor intends to extend print and document security features, solutions, and professional services across borders, as well as where the vendor expects to make these capabilities available. To the extent possible, vendor should identify global consistencies and/or localized differentiation in its overall security approach. Strategies for leveraging and extending partner channel-delivered solutions and services to address specific industries and customer segments should also be emphasized.	20.00
Innovation	Vendor has provided consistent innovation in facing the challenges of meeting customer needs within the print and document environment. Emphasis should be placed on areas such as print and document security, cloud-based print and print management, fleet optimization, and supporting a zero trust framework for hybrid work.	10.00
Growth	The growth strategy covers the mission, direction, and goals by which a vendor will capture a growing share of the total addressable market for print and document security solutions and professional services. This category assesses the clear and convincing articulation of the vendor's positioning, market opportunity, and goals for increasing the vendor's share of the total addressable market.	15.00
R&D pace/ productivity	The company's innovation model maximizes its potential to generate market value around securing the print and document infrastructure. The vendor has demonstrated an understanding that to increase the capabilities of its offering it will need to tap not only its internal development resources but also partner with other companies to bring differentiated and innovative capabilities to the market. Vendor has a clear strategy for both R&D investments and partnering worldwide and in the United States, in the next three to five years.	10.00
Total		100.00

Source: IDC, 2025

TABLE 2

Key Capability Measures for Success: Worldwide Print Security Solutions and Services Hardcopy

Capabilities Criteria	Definition	Weight (%)
Functionality or offering	This evaluates the vendor's portfolio of capabilities, solutions, and services to address security concerns in the print and document infrastructure. This evaluation will consider the overall breadth and depth of vendor's security offerings, including device-level features and support, software solutions, or professional and managed services with core competencies in threat-level assessment, detection, and remediation capabilities. Evaluation will also consider solutions and support offerings from third-party partners. This evaluates the vendor's ability to address core market requirements in key areas of print and document security, including user authentication and authorization; device management; data encryption; device malware protection; BIOS and operating system protection; quantum resistance; firmware updates and password management; hard disk disposal, image overwrite, and removable storage media; and antivirus and antimalware/spyware. Compliance with industry standards and key security certification will also be evaluated. This evaluates vendor's consultancy and implementation services (professional and managed) to deliver maximum customer benefit. Excellence is seen as offering the full spectrum of security services, 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 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. This evaluates a vendor's ability to provide a broad range of security solutions and services through a variety of delivery models and platforms. This will include an analyst evaluation in areas related to service delivery, implementation, ongoing management, execution against targeted SLAs, and support. Specific areas of focus will include the overall delivery model (on-premises/cloud, local/remote, onshore/offshore, or hybrid models), solutions and technology deployment, interoperability with existing systems, global delivery, and ongoing program management and support.	50.00

TABLE 2

Key Capability Measures for Success: Worldwide Print Security Solutions and Services Hardcopy

Capabilities Criteria	Definition	Weight (%)
Portfolio benefits	This assesses the breadth of professional and consulting service offerings beyond print and device management. Offerings demonstrate the ability to support the most complex use cases and should be well supported and/or enhanced by a portfolio of complementary services, including (but not limited to) managed print and document services (MPDS), IT services, infrastructure services, cloud services, and workflow services. This evaluates the vendor's portfolio of solutions to augment its security offerings for the print and document infrastructure. This evaluation will consider the full range of complementary solutions, including (but not limited to) print and device management, intelligent scan/capture and workflow automation, ECM and/or document management, and other horizontal and vertical-specific applications. Evaluation will consider the OEMs own intellectual property (IP) and direct application or integration with third-party partner solutions.	20.00
Go-to-market capabilities	This demonstrates the vendor's sales force alignment and identifies resources dedicated to sales/support of print and document security solutions and services. This evaluates the expertise of a vendor's salespeople, as well as the mix of local and international capabilities, sales force alignment by vertical industry, and the ability for salespeople to make decisions locally and/or draw on international resources. We also evaluate the ability to sell services through partnerships and channel, targeting local, multicountry, and global deals. This evaluates the vendor's capability to generate awareness and leverage market demand for print and document security solutions and services within the next 12–18 months. Evaluation will include both direct marketing and resources developed specifically for channel partners. Vendor should demonstrate clear messaging to the market that it has the capabilities and expertise required to secure the print and document infrastructure, including vertical-specific programs and activities to address regulatory compliance.	10.00
Pricing model or structure of product/offering	This demonstrates the vendor's range of pricing, packaging, and billing models to address current and future customer needs around print and document security. This looks at the vendor's ability to support a broad range of pricing and billing models for both customers and channel-delivered solutions and services, including fee-based, seat-based, and subscription-based services; licensing models; SaaS; and other pricing/billing models.	5.00

TABLE 2

Key Capability Measures for Success: Worldwide Print Security Solutions and Services Hardcopy

Capabilities Criteria	Definition	Weight (%)
Customer satisfaction	It describes customer's perception of overall satisfaction with vendor's offering and ability to achieve stated objectives. Areas for consideration will include alignment with business goals and objectives, time to value (TTV), return on investment (ROI), ease of use and management, integration capabilities, ability to meet compliance and regulatory requirements, vendor's performance, reliability, and support.	10.00
Customer service delivery	It demonstrates the vendor's global capabilities for the delivery of print and document security solutions and services. This evaluates how well the vendor's customer service is vertically aligned and able to service and support global customers and partners, showcase local presence, penetrate the existing customer base, and impact customer retention.	5.00
Total		100.00

Source: IDC, 2025

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

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. 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/about/worldwideoffices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2025 IDC. Reproduction is forbidden unless authorized. All rights reserved.