IDC MarketScape

IDC MarketScape: Worldwide Data Protection and Governance Services 2025 Vendor Assessment

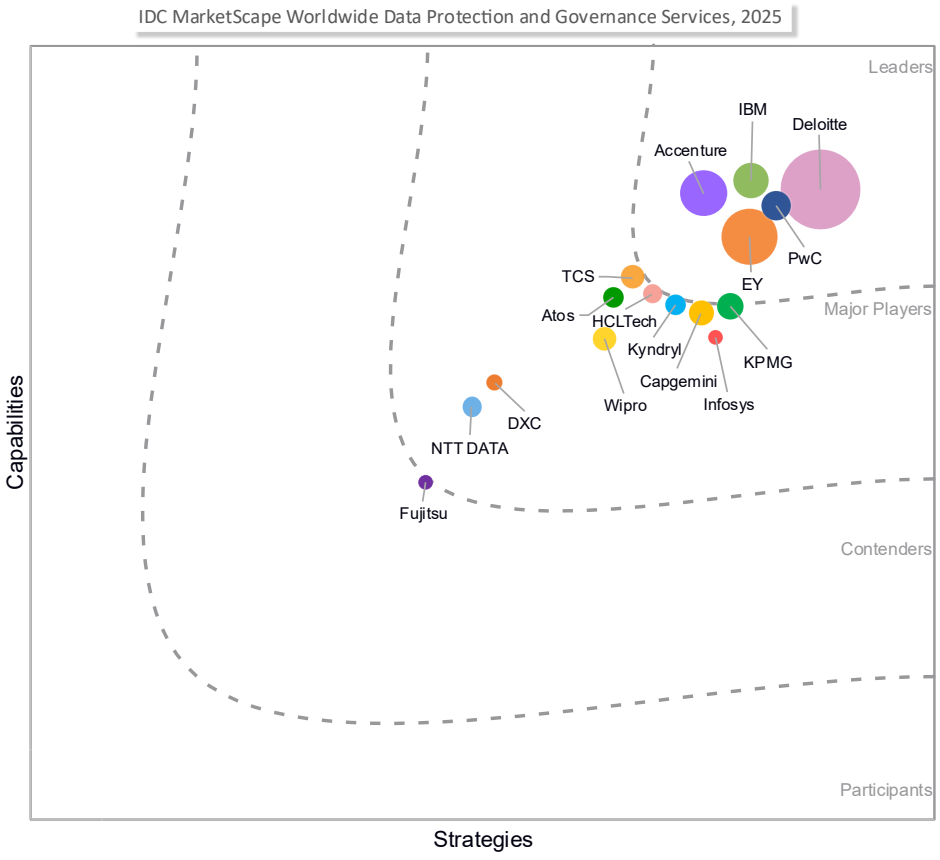
Cathy Huang

THIS EXCERPT FEATURES ACCENTURE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Data Protection and Governance Services Vendor Assessment



Source: IDC, 2025

October 2025, IDC #US52973625e

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 Data Protection and Governance Services 2025 Vendor Assessment (Doc # US52973625).

IDC OPINION

The convergence of artificial intelligence (AI) transformation, quantum computing–backed threats, and explosive regulatory complexity has created a perfect storm that exposes the inadequacy of traditional governance approaches when data has become the most critical strategic asset. Organizations today face unprecedented data governance, security, and privacy challenges that threaten to derail their AI transformation ambitions.

The trends point to a fundamental breakdown in how organizations structure, govern, and protect their most critical asset — data — precisely when they need it most for AI-driven innovation. This challenge manifests through multiple interconnected failures (e.g., generative AI [GenAI]–specific data risks, shadow AI, "harvest now, decrypt later" threats) that create exponential risk when organizations attempt to scale AI from experimental pilots to production-ready systems.

Data sovereignty issues present additional challenges as regulations across the globe continue to evolve and countries become increasingly possessive about their data, making compliance a complex, multijurisdictional challenge that traditional governance approaches cannot manage effectively.

This IDC MarketScape assessment of 16 global providers and 5 emerging vendors in the Vendors to Watch section reveals a market fundamentally shifting from a siloed, compliance-focused approach to integrated and AI-fused data protection and governance functions. The data protection and governance (DPG) services market has reached an inflection point, driven by three converging forces:

- **AI-first revolution:** Organizations are rapidly adopting AI-enhanced data discovery, automated classification, and AI-driven risk assessments. Many data protection and governance services providers have adopted AI-first approach and deployed hundreds of AI agents to automate traditional manual processes that previously required weeks or months of human effort.
- **Quantum-safe imperative:** The approaching quantum computing threat has accelerated post-quantum cryptography adoption beyond theoretical planning to concrete preparation. With the help of data protection and governance services

provider, an increasing number of organizations are conducting quantum risk assessments, cryptographic inventory discovery, developing migration road maps, and preparing themselves to be quantum ready.

- **Regulatory acceleration:** The proliferation of data protection regulations — spanning GDPR, CCPA, DORA, NIS2, and emerging AI acts — has created unprecedented demand for deep expertise and unified compliance frameworks capable of addressing multiple jurisdictions and technology environments simultaneously.

IDC believes that organizations that build comprehensive data governance programs addressing three critical areas — AI integration, quantum security, and regulatory compliance — will gain significant advantages and help them unlock the full potential of AI initiatives.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied vendors that provide data protection and governance services throughout the world. The vendors included in the study must meet certain criteria to qualify for this vendor assessment:

- The vendor's data protection and governance services portfolio meets more than 80% of IDC's defined core capabilities, including:
  - Data classification — frameworks and taxonomy/definitions
  - Data discovery across structured and unstructured data
  - Data protection and controls across web, network, cloud, and so forth
  - Data life-cycle management
  - Data security posture management
  - Data encryption and tokenization
  - Post-quantum cryptography (PQC)/quantum ready as encryption methods designed to withstand attacks from future quantum computers
  - Consent management
  - Data privacy mapping
  - Data residency and sovereignty
  - Key and secrets management
  - Data risk assessment
  - Data resiliency and data recoverability
  - GenAI-specific data risks (e.g., data poisoning)
- The provider operates with a multinational footprint.

- The provider supports a wide range of industry sectors, including financial services, manufacturing, healthcare and life sciences, government, telecommunications, energy, and utilities.
- The provider has a total revenue of data protection and governance services that exceeded $50 million in 2024.

ADVICE FOR TECHNOLOGY BUYERS

The evolution of data protection and governance services represents one of the most significant shifts in enterprise technology in the past decade. The question is no longer whether to invest in data governance, but how to do so in a way that creates a dynamic and effective data protection and governance program that delivers quantifiable risk reductions while meeting necessary compliance requirements. Organizations that invest strategically in modern governance capabilities today — selecting the right partners, implementing robust frameworks, and building organizational competencies — will be best positioned to thrive in an increasingly AI-driven and regulated world. IDC offers the following recommendations:

- **Future proof your data protection and governance strategy.** Given the rapid pace of change, build adaptability into your data protection and governance strategy, for example:
  - Quantum-safe cryptography road maps beginning with hybrid implementations
  - AI governance frameworks that can evolve with technological advancement
  - Regulatory monitoring systems that proactively identify emerging requirements
  - Technology assessment processes that evaluate new governance solutions systematically
- **Prioritize business value on top of compliance.** While compliance remains essential, focus on building governance as a business enabler:
  - Data monetization opportunities enabled by trusted, high-quality data
  - Operational efficiency gains through automated workflows and reduced manual processes
  - Innovation acceleration via democratized access to governed data
  - Customer trust enhancement through transparent privacy practices
- **Adopt a platform-first approach.** Traditional point solutions are giving way to integrated platforms that aggregate metadata, data lineage, classification, and access controls across cloud and on-premises environments. When evaluating providers, prioritize:

    - Unified data visibility that can monitor data flows, detect anomalies, and enforce policies ubiquitously
    - Scalable automation capabilities that grow with organizational needs
    - Real-time monitoring and alerting for proactive risk management
- **Plan for multivendor ecosystems.** No single provider excels across all data protection and governance domains. Successful enterprises architect multivendor strategies:
    - Best-of-breed specialization for critical use cases (e.g., AI-enhanced classification, cryptography, or privacy-preserving analytics)
    - API-first architecture where diverse solutions communicate through APIs, supported by unified policy management and oversight
    - Risk management strategies that avoid over-dependence on single vendors
    - Selecting the right data protection and governance services provider based on chosen use cases or selected technology
- **Invest in organizational capabilities.** Technology alone cannot deliver governance success. Organizations must invest in:
    - Data stewardship programs that embed governance into business processes
    - Change management initiatives that drive adoption across the enterprise
    - Continuous education programs that keep pace with evolving requirements
    - Cross-functional collaboration between legal, compliance, IT, and business teams

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.

Accenture

Accenture is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide data protection and governance services.

Accenture's Data Protection and Governance practice is a sizable business line within its global security division, giving it the financial headroom, talent bench, and R&D budget to keep pace with surging AI, quantum readiness, and regulatory demands. The practice has more than 3,200 certified privacy and security professionals operating from over 100 countries.

Its core capabilities along with examples of innovative features illustrated in customer cases include:

- **Data discovery, classification, and minimization:** Accenture's proprietary mySecurity AI scans up to 4PB of structured, semistructured, and unstructured data per day, applying tunable differential privacy classifiers and Microsoft Purview labels in real time. In addition, a patent-backed Sensitive Data Discovery Engine increases on-target classification accuracy to 96% in multicloud estates. In addition, data minimization and tool rationalization help clients achieve millions of savings in data-related opex and capex spending.
- **Protection controls:** It includes full-spectrum enterprise data loss protection (DLP), tokenization, dynamic masking, and field-level encryption.
- **Post-quantum cryptography and cryptoagility:** It focuses on implementation with help across eight steps — inventory, risk score, prioritize, remediate, monitor, attest, automate, and refine.
- **Deepfake protection:** It is the result of investment and partnership with Reality Defender as well as innovation development through Accenture's GenAI centers that detects AI-generated audio/video spoofing and enables deepfake resilience.
- **Privacy, consent, and Data Subject Access Request (DSAR) automation:** GenAI "policy copilots" assemble Records of Processing Activities (RoPA) and DSAR responses from data lakes and policy stores, cutting RoPA drafting time from 21 days to 9 hours in one customer case and reducing regulatory risk-hours by 45% through consent anomaly detection.

Strengths

- **Scale and reach:** Accenture has a global network of 45 security centers, including 16 cyber fusion centers, 21 cyber incubation centers, 3 quantum security centers, and 1 GenAI security innovation hub that houses AI or quantum hardware (e.g., an H200 GPU cluster) for rapid prototyping and proof-of-concept builds, allowing clients to "touch and feel" solutions before committing to full deployment.
- **Certified data protection framework with multidisciplinary execution excellence:** Accenture's DPG services portfolio is organized around an ISO 27001/27701-certified client data protection (CDP) framework that enforces a repeatable runbook on every engagement. This framework is executed by multidisciplinary teams drawn from four internal practices — strategy, protection, resilience, and cyber–physical. According to client feedback, "Accenture has excellent attitude, being accountable and responsive to our requests."
- **AI-first automation:** Besides the mentioned mySecurity AI that automates discovery and classification, Accenture offers AI Refinery and Agentic AI Orchestration — an agent platform that integrates third-party AI services (e.g.,

Microsoft Copilot, CyberArk identity agents) into a governance mesh. In IDC's August 2025 *Data Protection and Governance Services Survey* (n = 1,018), Accenture received strong customer ratings for these areas — data classification and mapping, AI data risk assessment and governance, data lineage and provenance, and data recovery support.

- **Quantum-safe leadership:** In the same survey, Accenture received very strong rating for helping customers get quantum ready. Accenture's 24 PQC-related patents; strategic investments and partnerships with vendors like QuSecure, Aliro, and SandboxAQ; and real customer cases keep Accenture ahead of many providers on cryptoagility and quantum key distribution (QKD) proof of concepts (POC).

Challenges

Customer references applaud Accenture's overall skilled expertise, yet they note occasional gaps between presales experts and onsite delivery teams in very large, multiphase rollouts. Tighter mentoring and quality controls would reduce variance. In addition, Accenture justifies total cost of ownership through faster time to value and automation savings, yet price-sensitive enterprises may prefer phased deployments or a co-sourced model.

Consider Accenture When

Consider Accenture when organizations demand the following:

- AI-driven discovery/classification, self-healing controls, or deepfake defense capabilities
- Quantum-safe transformation, especially those exploring QKD or moving on to implementations
- Mission-critical resilience that is paramount and global security operations center (SOC) coverage that is nonnegotiable
- Conversion of sprawling data estates and complex regulations into measurable risk and cost reductions

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

IDC defines data protection and governance services as a range of professional security services that help organizations with comprehensive capabilities to discover, classify, secure, monitor, manage, and govern their business data. These services help organizations protect sensitive and confidential information from unauthorized access and breaches while ensuring regulatory compliance and effective data management

and maintaining data confidentiality, integrity, and availability across all environments and all use cases.

Customer Rating of Data Protection and Governance Services Vendors

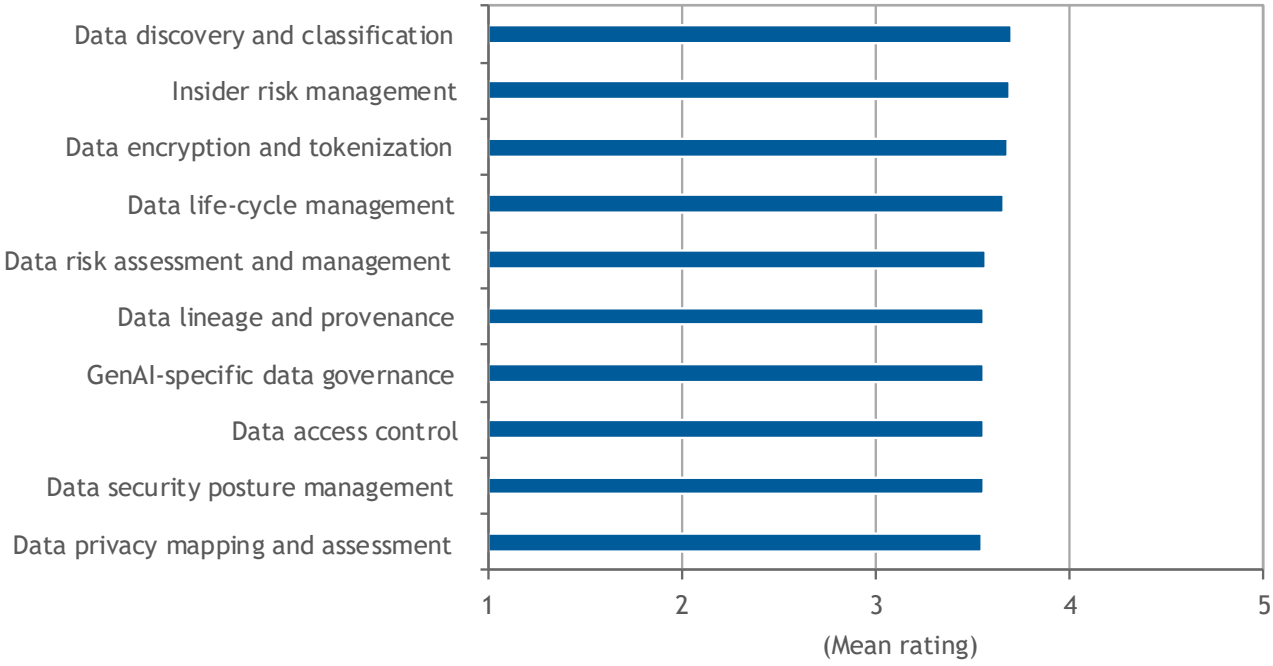
A significant component of this evaluation is the inclusion of the perceptions and ratings of data protection and governance services buyers. The buyers participating in IDC's 2025 *Data Protection and Governance Services Survey* have partnered with at least one of the participating vendors directly on a related services engagement within their company. The survey findings highlight primary drivers for selecting the vendor to provide data protection and governance services and satisfaction ratings for various aspects of data protection and governance capabilities.

Figure 2 illustrates the average satisfaction mean score for these data protection and governance capabilities surveyed in August 2025.

FIGURE 2

Data Protection and Governance Service Capabilities Satisfaction Level

Q. How satisfied are you with your select data protection and governance services provider for each of the data protection and governance capabilities that you indicated that you have used?



n = 1,018

Note: The mean rating is based on a scale of 1 to 5, where 1 indicates "not at all satisfied" and 5 indicates "extremely satisfied."

Source: IDC's *Data Protection and Governance Services Survey,* August 2025

LEARN MORE

Related Research

- *Which Verticals Are the Top Spenders for Data Protection and Governance Services and Software* (IDC #US53793525, September 2025)
- *How Effective Is Your Organization in Identifying, Managing, and Disposal of ROT Data?* (IDC #US53791525, September 2025)
- *Approximately What Percentage of GenAI Models Using Data Sets That Have Been Verified or Curated?* (IDC #US53793725, September 2025)
- *Has Your Organization Implemented Access Controls and Audit Logging for Data Used in AI Pipelines?* (IDC #US53793625, September 2025)
- *Data Classification Taxonomy: It Is All About the Data* (IDC #US53526025, June 2025)
- *How to Prepare for AI Compliance Regulations Starting Now* (IDC #US53300725, April 2025)
- *Fujitsu's Uvance: Driving Digital Transformation and Strategic Growth* (IDC #IcUS53312525, April 2025)

Synopsis

This IDC study represents a vendor assessment of the worldwide data protection and governance services market through the IDC MarketScape model. This study highlights the transformative challenges organizations face in data governance amid AI-driven innovation, quantum computing threats, and regulatory complexity. It evaluates 16 global providers and 5 emerging vendors, emphasizing the shift from siloed, compliance-focused approach to integrated, AI-driven approach.

"AI, quantum computing, and regulatory complexity are reshaping data protection and governance — organizations must adapt or risk derailing their AI transformation ambitions amid exponential challenges," notes Cathy Huang, senior research director, Worldwide Security Services.

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