IDC MarketScape

IDC MarketScape: Worldwide Third-Party Risk Management Software 2026 Vendor Assessment

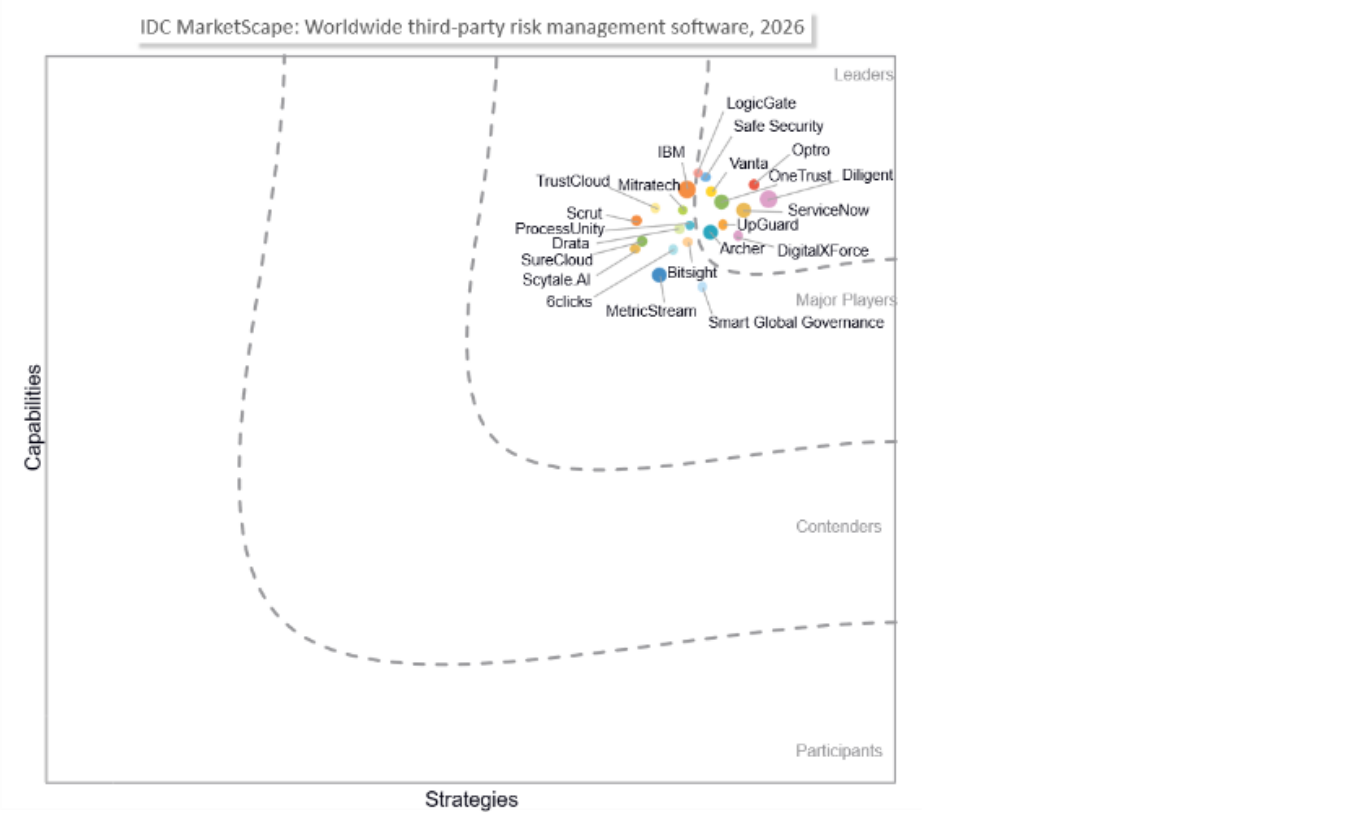
Philip D. Harris, CISSP, CCSK

THIS EXCERPT FEATURES VANTA AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide third-party risk management software vendor assessment



Source: IDC, 2026

September 2026, IDC #US53007725e

Please 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 Third-Party Risk Management Software 2026 Vendor Assessment (Doc #US53007725).

IDC OPINION

The worldwide third-party risk management (TPRM) market is undergoing its most significant architectural shift in two decades, driven by the convergence of agentic AI, continuous monitoring maturation, and an accelerating global regulatory mandate environment. IDC believes that the traditional model of periodic, questionnaire-based vendor assessment is structurally inadequate for the risk velocity organizations face in 2026, where third-party breaches now account for more than one-third of all enterprise cyberincidents. Compounding this inadequacy is a fundamental limitation inherent in conventional outside-in monitoring, which can observe exposed attack surfaces but cannot assess the quality of internal security controls, configuration states, or actual IT hygiene operating within a vendor's environment. Emerging inside-out scanning capabilities directly address this critical visibility gap by deploying lightweight agents or API-based connectors within consenting third-party IT estates, enabling risk teams to observe actual configuration data, patch currency, endpoint states, and access control effectiveness in near real time, dramatically increasing the accuracy and depth of vendor risk intelligence at enterprise scale.

IDC observes that the TPRM vendor landscape in 2026 is meaningfully stratified across at least four distinct buyer archetypes: regulated financial institutions and critical infrastructure operators demanding deep regulatory content and multitier supply chain governance; technology companies and SaaS organizations seeking compliance-integrated vendor risk management with AI-powered questionnaire automation; security-first organizations prioritizing continuous external monitoring, inside-out estate visibility, and cyber-risk quantification; and midmarket organizations requiring cost-competitive, rapid-deployment platforms with hybrid managed services support. No single platform currently satisfies all four archetypes equally, and IDC advises buyers to align platform selection to their primary use case, regulatory jurisdiction, and TPRM program maturity rather than seeking a single universal solution.

The emergence of autonomous agentic AI represents the most transformative shift in TPRM software architecture since the introduction of continuous monitoring a decade ago, and IDC's assessment of this IDC MarketScape reflects a market at an inflection point where AI capability differentiation is rapidly becoming the primary basis of competitive advantage,

supplanting traditional differentiators such as questionnaire library breadth and regulatory content depth. Unlike earlier AI implementations that offered recommendation engines or automated questionnaire scoring, agentic AI platforms now deploy purpose-built agents capable of executing end-to-end TPRM workflows with minimal human intervention, from vendor onboarding and evidence collection through risk scoring, escalation, and remediation tracking.

Leading vendors are deploying agents that compress assessment cycles from weeks to hours, scale portfolio coverage well beyond what available head count could sustain, and synthesize multisource risk intelligence into prioritized, board-ready decisions without analyst mediation. Vendors that have made substantive, production-ready investments in agentic AI, including autonomous vendor profiling, AI-driven document analysis, predictive risk scoring, and machine-speed continuous monitoring, are establishing durable competitive separation from those that have added AI features incrementally to legacy workflow architectures. IDC anticipates significant market consolidation over the next 24 months as enterprise buyers rationalize fragmented TPRM tool stacks in favor of unified platforms delivering measurable, AI-driven program efficiency at scale.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC evaluated vendors worldwide that provide third-party risk management software. The vendors included in the study had to meet certain criteria to qualify for this vendor assessment:

- **Geographic presence:** Each vendor is required to operate TPRM in more than one region throughout the world.
- **Customer base:** Vendors have customers in one or more regions around the world.
- **TPRM capability:** Each vendor possesses a TPRM software that has trained professional cybersecurity TPRM staff with expertise in third-party risk management.

ADVICE FOR TECHNOLOGY BUYERS

As the TPRM market undergoes rapid transformation driven by agentic AI, expanding regulatory mandates, the emergence of inside-out third-party scanning capabilities, and the growing complexity of global supply chain ecosystems, technology buyers face an increasingly consequential platform selection decision. The cost of choosing the wrong TPRM platform, measured in unmanaged vendor risk exposure, regulatory examination findings, and the operational burden of replacing entrenched tooling, has never been higher. IDC recommends that buyers ground their evaluation in the following guidance to ensure platform selection reflects their organization's specific risk profile, regulatory obligations, program maturity, and long-term operational capacity:

- Align TPRM platform selection to your organization's primary risk driver, regulatory compliance, cyber-risk monitoring, supply chain visibility, or compliance automation, rather than selecting the most feature-complete platform available regardless of organizational fit.
- Evaluate AI capabilities based on production-ready agentic functionality, autonomous vendor discovery, document analysis, evidence collection, and continuous monitoring, rather than marketing claims, and require live demonstrations of AI performance against real vendor portfolios before contract execution.
- Distinguish between outside-in and inside-out scanning capabilities when evaluating continuous monitoring depth; outside-in approaches observe exposed attack surfaces, while inside-out scanning, deployed with vendor consent via lightweight agents or API connectors, provides direct visibility into internal configuration states, patch currency, and access control effectiveness that external signals cannot reveal.
- Prioritize platforms that express vendor risk in financial terms using quantitative methodologies such as FAIR, enabling board-level and executive risk communication that connects third-party cyberexposure to measurable business impact and capital allocation decisions.
- Assess continuous monitoring data provenance carefully, distinguishing between platforms that own proprietary threat intelligence and those that aggregate purchased third-party signals, as data ownership directly affects monitoring latency, accuracy, and attribution quality.
- Require vendors to demonstrate fourth-party and nth-party supply chain mapping capabilities, as single-tier vendor visibility is insufficient for organizations whose most significant breach exposure increasingly originates from vendors' vendors rather than from direct contractual relationships.
- Evaluate total cost of ownership across a three-year horizon, including implementation, configuration, ongoing managed services, and per-vendor monitoring fees, as initial licensing costs frequently under-represent the full investment required to operationalize enterprise-scale TPRM programs effectively.
- Consider the regulatory content depth of candidate platforms against your specific jurisdictional obligations, such as DORA, OCC Third-Party Risk Guidance, NIST SP 800-161, FFIEC, or NIS2, rather than accepting broad framework alignment claims as evidence of regulatory-specific program support.
- Do not underestimate internal staffing requirements when selecting a pure software platform; organizations with limited TPRM analyst capacity should evaluate hybrid platform-plus-managed services models that supplement internal teams with expert-delivered assessment, remediation, and advisory capabilities.
- Validate that AI-assisted TPRM capabilities, including those underpinning autonomous agent workflows and inside-out scanning decision logic, are governed

by transparent, auditable, and human-in-the-loop processes, as regulators in financial services, healthcare, and critical infrastructure are increasingly scrutinizing the AI governance controls applied to vendor risk decisioning workflows.

- Require vendors to demonstrate platform integration depth with your existing procurement; ERP; governance, risk, and compliance (GRC); and security operations tooling, as TPRM value is substantially diminished when vendor risk data cannot flow automatically into enterprise risk registers, audit workpapers, and board reporting environments.
- Assess whether the platform's continuous monitoring scope extends beyond cybersecurity signals to encompass financial health, geopolitical risk, business continuity indicators, and adverse media, as organizations monitoring only cyber-risk signals remain exposed to significant noncyber third-party disruption events that can be equally consequential to enterprise operations.
- Evaluate the vendor's own AI governance maturity, including whether the vendor holds independent certifications such as ISO/IEC 42001, as organizations deploying AI-assisted TPRM platforms, particularly those using autonomous agentic workflows and inside-out scanning, inherit regulatory and reputational exposure if the vendor's AI systems lack transparent governance, bias controls, and explainability mechanisms.

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.

Vanta

Vanta is positioned in the Leaders category in this 2026 IDC MarketScape for third-party risk management software.

Vanta is a San Francisco–based agentic trust management and compliance automation platform founded in 2018, having developed automated evidence collection and continuous control monitoring for frameworks including SOC 2, ISO 27001, HIPAA, GDPR, and PCI DSS, and now supports 35+ frameworks. Serving a growing number of customers using Vanta's TPRM capabilities across technology start-ups, SaaS companies, and midmarket technology organizations, it has expanded to include vendor risk management and AI-powered questionnaire response automation.

Vanta's Trust Management Platform enables vendor security posture assessment, compliance documentation collection, and vendor due diligence management linked to

internal control requirements. Automated vendor risk scoring and prebuilt templates support SOC 2 and ISO 27001 vendor management requirements. A Trust Center enables public sharing of certifications and security documentation with customers, prospects, and partners.

Vanta has built a strong network of trust in the market. Every Trust Center published, questionnaire completed, and commitment shared strengthens a connected ecosystem that benefits both vendors and buyers. By combining TPRM with Continuous Trust Management capabilities like Trust Center, Questionnaire Automation, and Commitments, Vanta creates a differentiated network effect.

Vanta's most distinctive TPRM AI capability is the company's dedicated Agent for TPRM, which automatically discovers vendors; runs end-to-end assessment life cycles without manual follow-up; autocollects and analyzes evidence from SOC 2 reports, DPAs, and questionnaires; and continuously monitors the vendor landscape for breaches, emerging threats, and material changes, automatically drafting tailored remediation plans when risks are identified. IDC research attributes a 526% three-year ROI to Vanta's platform, with TPRM teams reporting 54% productivity gains and organizations managing 50 vendors, saving approximately $81,000 annually through automated discovery, AI-powered reviews, and continuous monitoring.

Strong brand recognition, an active customer community, and high innovation velocity position Vanta as a formidable compliance automation platform in the technology market.

Strengths

- AI-powered Questionnaire Automation addresses both outbound TPRM assessments and inbound customer due diligence obligations within a single platform.
- Vanta offers an established compliance automation platform with one of the most trusted and widely adopted track records in the technology company market.
- The TPRM Agent autonomously discovers vendors, runs full assessment life cycles, monitors for breaches and material changes, and autodrafts remediation plans without manual intervention.

Challenges

- Fourth-party and nth-party supply chain risk visibility is absent, limiting organizations requiring automated multitier vendor ecosystem mapping beyond direct third-party relationships.
- Prebuilt regulatory reporting packages and assessment content for TPRM-specific mandates, including DORA, OCC Guidance, and NIST SP 800-161, are less comprehensive than purpose-built TPRM platforms.

Consider Vanta when

- Your technology company needs to unify compliance automation, third-party risk management, and inbound questionnaire response automation in one platform.
- You need to stay ahead of vendor risk with always-on monitoring built directly into your TPRM workflow, not a separate tool, integration, or paid add-on.
- You want an autonomous TPRM Agent to discover vendors, run assessments, monitor continuously, and draft remediation plans, delivering 54% team productivity gains without adding head count.
- You want to holistically tie third-party risk to first-party risk, all in the same platform.

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 reflects each vendor's market share 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

TPRM programs are designed to help organizations identify, assess, mitigate, and monitor risks associated with third-party engagements and/or acquisitions. These programs span a spectrum from advisory and consulting to fully outsourced managed services, offering scalable solutions tailored to the complexity and maturity of an organization's cybersecurity risk posture and cybersecurity compliance needs.

TPRM software provides the tools and capabilities needed to navigate this complexity, ensuring resilience, compliance, and operational excellence. TPRM software can offer real-time business and cybersecurity intelligence, AI- and ML-driven automation, strategic governance, integrated platforms, and significant automation. Organizations that invest in robust TPRM programs and software will not only mitigate risks but also ensure business resilience and unlock value from their third-party ecosystems. Modern TPRM programs and software are designed to support the full life cycle of third-party engagement and management. The various components provide the following functions:

- TPRM programs:
  - Risk identification and profiling
  - Due diligence and risk assessment
  - Risk mitigation and remediation
  - Continuous monitoring
  - Reporting and governance
  - Managed TPRM services
- TPRM software:
  - Third-party inventory
  - Third-party ownership, classification, and categorization
  - Business owners
  - Classification
  - Categorization
  - Risk identification
  - Risk and compliance assessment
  - Risk analysis and scoring
  - Risk and compliance mitigation and remediation
  - Continuous monitoring
  - Reporting and dashboards
  - AI, automation, and integration
- Managed TPRM services:

- Vendor onboarding and offboarding
- Assessment execution
- Risk intelligence integration
- Remediation management
- Audit support

LEARN MORE

Related research

- *Worldwide Security Governance, Risk, and Compliance Services and Software Forecast, 2025–2029* (IDC #US53611425, June 2025)
- *Worldwide Security Governance, Risk, and Compliance Services Forecast, 2025–2029* (IDC #US53611525, June 2025)
- *Worldwide Security Services Taxonomy, 2025* (IDC #US53294625, April 2025)
- *Cybersecurity Metrics — A Data-Driven Framework for the Future* (IDC #US52699424, November 2024)
- *Continuous Compliance Management Increases Resilience to Cyberattack* (IDC #US52638324, October 2024)
- *Choosing the Right Security Framework* (IDC #US49291622, July 2022)

Synopsis

This IDC study assesses worldwide TPRM software vendors' capabilities and strategy, focusing on how AI-native platforms are displacing legacy, questionnaire-driven approaches to vendor risk management. The worldwide TPRM market has reached a structural inflection point in 2026, driven by the convergence of agentic AI, accelerating regulatory mandates, and the growing complexity of multitier digital supply chains. Vendors that have embedded AI as a foundational operating model, enabling autonomous vendor discovery, continuous evidence analysis, and real-time risk decisioning, are establishing durable competitive separation from those applying AI incrementally to legacy workflow architectures. This IDC MarketScape reflects a market in which AI capability differentiation is rapidly displacing traditional differentiators, such as questionnaire library breadth and regulatory content depth.

IDC's assessment reveals a meaningfully stratified vendor landscape serving at least four distinct buyer archetypes: regulated enterprises, technology company compliance buyers, security-first continuous monitoring adopters, and midmarket organizations requiring hybrid managed services support. No single platform satisfies all four archetypes equally, and platform selection decisions grounded in regulatory jurisdiction, program maturity, and the

primary risk driver will outperform those based solely on feature breadth. IDC anticipates significant market consolidation over the next 24 months as enterprise buyers rationalize fragmented TPRM tool stacks in favor of unified, AI-driven platforms delivering measurable program efficiency at scale.

“The TPRM market is no longer about who has the most questionnaire templates; it’s about which vendors have made AI a foundational operating model that transforms periodic vendor assessment into continuous, autonomous risk intelligence.” — Philip Harris, research director, Governance, Risk, and Compliance Solutions, IDC

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

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @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 idc.com/about/offices. 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 2026 IDC. Reproduction is forbidden unless authorized. All rights reserved.