

The Vanishing Window: Why Third-Party Risk Management Must Go Continuous

Written by:

Philip Harris

Research Director

Published:

September 2026

This IDC Spotlight highlights that third-party risk management is shifting from periodic vendor audits to continuous, evidence-based, threat-informed monitoring, driven by regulation and growing breach involvement.

Introduction

Annual, point-in-time vendor risk assessments no longer match a third-party threat landscape that can change within hours of the last questionnaire response. IDC believes third-party risk management (TPRM) is in the middle of a structural shift from periodic audits toward continuous, evidence-driven, threat-informed operations, and that the vendors who help enterprises make that shift will capture a disproportionate share of buyers' reallocated spend.

- Cyberassurance is shifting from periodic audits to continuous, evidence-driven operations as continuous compliance, vulnerability management, attack surface management, and exposure management converge around shared data and machine-readable evidence.
- Closing the long-standing gap between GRC and security operations, and pairing risk scoring with predefined, automated response, is now a prerequisite for defensible third-party oversight — not an optional maturity step.
- Confidence in third-party risk posture remains among the lowest-scoring dimensions of enterprise GRC program maturity, even as regulatory frameworks such as NIST CSF 2.0, DORA, and NIS2 push organizations toward continuous, machine-readable compliance evidence.
- Third-party compliance and automation have become near-equal priorities for security leaders: In an August 2026 IDC survey, 25.9% of organizations named ensuring third-party compliance among their top cybersecurity priorities, alongside 28.3% citing risk oversight and 26.0% citing automation, AI, and machine learning — evidence that these agendas are converging in practice, not just in theory (IDC's *Third-Party Risk Management Software Survey*, August 2026).
- Organizations that make this shift gain more than visibility. They gain a defensible, evidence-based posture that they can bring into board, regulator, and cyber-insurance conversations.
- That shift is already visible in the data: 37.6% of organizations now use continuous, API-based monitoring as their primary TPRM cadence, yet only 16.2% describe continuous monitoring as their overall assurance method.
- IDC believes the structural shift underway is larger than incremental automation of existing steps. Within the horizon of this decade, the core TPRM assessment and monitoring life cycle could become more than 90% automated, with human analysts moving from active assessors to periodic reviewers who audit automated findings rather than generating them.

Definitions

- **Third-party risk management:** The set of processes an organization uses to identify, assess, and monitor risk introduced by vendors, suppliers, and other external parties
- **Continuous compliance:** An operating model in which compliance evidence is collected and evaluated on an ongoing basis, rather than at scheduled audit intervals
- **Threat-informed monitoring:** Continuous monitoring that incorporates external threat intelligence to prioritize findings by active exploitation risk, not just severity
- **Inside-out scanning:** Telemetry generated by a third party's own systems (e.g., IAM, EDR, CMDB, or CSPM) and consumed continuously by the assessing organization, as distinct from outside-in scanning of a vendor's external attack surface
- **Confidence score:** A composite risk indicator, typically built from external intelligence sources, intended to give non-security stakeholders a usable signal for onboarding and ongoing risk decisions
- **Right-to-audit (RTA):** A contractual clause granting an organization the ability to audit a vendor's controls or environment, historically exercised through onsite inspection
- **Fourth-party risk:** Risk introduced by the vendors and subcontractors of an organization's own third parties, one step removed from the direct contractual relationship

Scenarios: The third- and fourth-party risk surface is expanding

The scale problem will get worse before it gets better. Large enterprises now manage relationships with thousands of third and fourth parties, and IDC research describes continuous monitoring and risk scoring at that scale as mathematically incompatible with human-paced review cycles — meaning automation is no longer a nice-to-have, but the only realistic path to coverage. At the same time, attackers are compressing the time defenders have to respond. IDC finds that threat actors, increasingly augmented by their own AI systems, are already compressing attack life cycles from days to hours and, in the near term, from hours to minutes. Third-party involvement in breaches has tracked this acceleration. The 2026 Verizon Data Breach Investigations Report (DBIR) puts third-party involvement in breaches at 48%, up 60% year over year — a sharper climb than the prior two years combined.

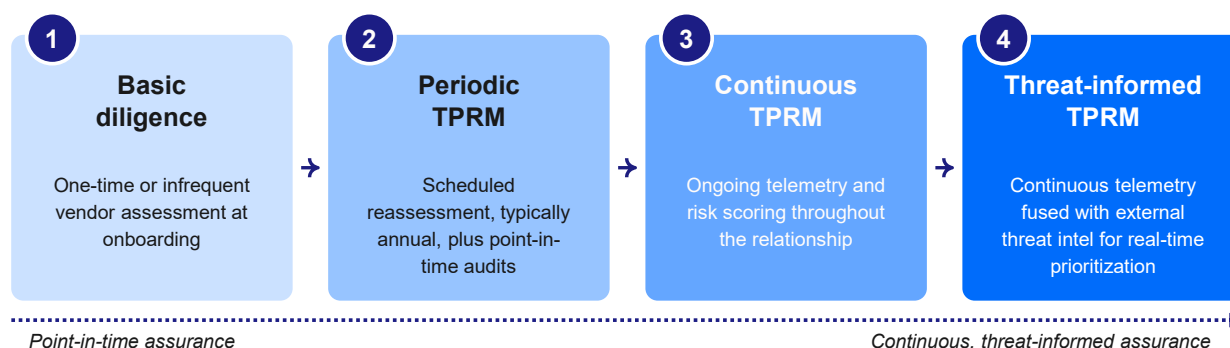
None of this can be managed inside the old organizational boundaries. GRC and security operations have historically run on separate data, cadences, and owners. IDC's research shows that exposure management is increasingly discussed in terms of discovery, validation, prioritization, and remediation — a framing that only works if GRC and security operations converge around shared, threat-informed data. Third-party risk programs will need to mirror that convergence to keep pace with the risk surface before them.

IDC's own August 2026 survey of 1,226 organizations using TPRM software confirms that this shift is already underway, if unevenly. On timing and cadence, just 16.5% of organizations still rely on pure point-in-time assessment; 45.5% have moved to event-driven reassessment, and 37.6% now use continuous control monitoring with near-real-time, API-based evidence pulls as their primary approach. However, when asked to characterize their overall assurance method, only 16.2% describe continuous monitoring — security ratings, attack surface monitoring, and breach and vulnerability intelligence feeds — as the model in use, versus 40.2% still centered on evidence-based assessment (SOC 2 reports, ISO 27001 certificates, and pen test summaries) and 16.8% on audit-based deep assessment. The gap between those two findings is telling: Continuous elements are being layered onto existing processes faster than they are replacing them (IDC's *Third-Party Risk Management Software Survey*, August 2026).

This shift is best understood as a maturity progression (see Figure 1).

Figure 1

The shift from periodic to continuous, threat-informed TPRM



Source: IDC, 2026; SecurityScorecard 2026 Supply Chain Cybersecurity Trends Report

Inside-out scanning and API-based telemetry

One of the more promising responses to the audit-effectiveness gap is what IDC describes as the inside-out audit opportunity: a model in which the third party's own systems generate verified, tamper-resistant telemetry that the auditing organization can consume continuously without a site visit. In practice, this means agent- or API-based telemetry pulled continuously from a vendor's own identity and access management (IAM), endpoint detection and response (EDR), configuration management database (CMDB), and cloud security posture management (CSPM) systems, rather than a scheduled site visit or a static questionnaire. A small set of vendors — including Safe Security, DigitalXForce, and TrustCloud — is already building toward this model.

How that telemetry is collected matters as much as what it contains. API-based telemetry consumption and correlation, rather than agentic tools scanning inside a vendor's environment, is emerging as the more workable path for vendors wary of autonomous tools touching their

own systems directly. Continuous evidence collection and continuous control monitoring are becoming the expected baseline, and telemetry gathered at onboarding is increasingly repurposed for early detection of exploitation rather than being treated as a one-time gate.

However, software adoption still lags behind the concept. In an August 2026 IDC survey, only 13.4% of TPRM software users said their platform offers inside-out, right-to-audit-style scanning as a feature, and only 15.2% reported threat-intelligence data feeds integrated into their tool — evidence that inside-out scanning and threat-informed correlation remain emerging capabilities rather than standard functionality across the market (IDC's *Third-Party Risk Management Software Survey*, August 2026).

Future outlook

Continuous prioritization is the next step beyond continuous telemetry. IDC's research points to AI-assisted questionnaire analysis, multiparty audit workflow coordination, and outside-in visibility into vendor-facing risk indicators between audit cycles. This emerging toolkit could give a confidence score built from external intelligence real operational teeth, turning it into a practical tool for procurement and business owners managing risk in real time, rather than waiting for the next renewal cycle.

Exposure management platforms are already being used to deduplicate assets, normalize findings, enrich telemetry with business and technical context, and prioritize remediation using factors beyond CVSS scoring alone. IDC expects vendor risk platforms to follow the same trajectory, aggregating scan data with threat intelligence to help enterprises get ahead of exploitation rather than simply reporting on it afterward. A continuously documented security posture is also starting to do double duty as the evidentiary foundation for linking vendor risk to cyber-insurance pricing and terms.

However, none of this works if risk stays abstract. Exposure management is meant to unify vulnerabilities, misconfigurations, identities, and external risks with business context; risk-based prioritization shaped by business context and external exposure is now the standard buyers expect. A finding on an obscure vendor subsystem and a finding on a system tied to revenue-critical data are not the same risk — a mature TPRM program has to be able to say so, and act accordingly.

IDC believes this trajectory points toward a more fundamental restructuring of the TPRM function than most organizations are currently planning for. The building blocks already described — inside-out telemetry, API-based evidence collection, threat-informed correlation, and business-context-weighted prioritization — do not just make continuous monitoring more efficient; taken together, they remove most manual steps from the assessment and monitoring life cycle itself. IDC believes this could push automation past 90% of that life cycle within the decade, with the analyst's role shifting from actively running assessments to periodically reviewing automated findings — auditing the system's outputs rather than producing them. That is a structural change in what a TPRM analyst does day-to-day, not simply a faster version of

what they currently do; organizations planning their TPRM operating model, staffing, and vendor relationships should treat it as a planning assumption rather than a distant possibility.

About SecurityScorecard

SecurityScorecard positions its platform squarely against the continuous, threat-informed model described above: Rather than treating vendor risk as a periodic scoring exercise, the company frames its ratings as a continuously updated signal meant to sit alongside, and eventually inside, an enterprise's broader exposure management program.

The company's ratings methodology draws on its own threat intelligence and breach data assets. SecurityScorecard's Global Third-Party Breach report found that over 35% of breaches now trace back to a third party — a figure consistent with the broader market acceleration described above, even if the precise percentage differs from the figure of 48% in the Verizon DBIR, which measures third-party involvement using a different methodology. That positioning is backed by independent adoption data: In IDC's August 2026 survey, 10.7% of organizations using a TPRM module reported using SecurityScorecard as part of their toolset (n = 159), corroborating the company's own usage claims with third-party-verified survey evidence rather than sponsor-reported figures alone (IDC's *Third-Party Risk Management Software Survey*, August 2026).

SecurityScorecard's May 2026 acquisition of Driftnet extends that data asset into internet-exposed infrastructure specifically. The company states that, since the acquisition, it indexes 40% more internet-exposed hosts than any other intelligence provider, using nonstandard port enumeration, fingerprinting, and IPv6-focused discovery to surface hidden or misconfigured infrastructure that creates third-party exposure — the kind of shadow attack surface that traditional, questionnaire-based TPRM programs are structurally unable to see.

SecurityScorecard frames its own product road map around four stages of TPRM maturity: Basic Diligence, Periodic TPRM, Continuous TPRM, and Threat-Informed TPRM. That framing tracks closely with the shift IDC describes above and gives the company a natural narrative for moving existing customers from a point-in-time scoring relationship toward a continuous, threat-informed one.

The company also maps its relevance across six TPRM stakeholder personas: the enterprise CISO, the chief risk officer (risk-focused), the chief revenue officer (growth-focused), the TPRM/GRC program leader, security operations and vulnerability management teams, and dedicated threat intelligence teams. That breadth reflects the reality that third-party risk decisions increasingly touch functions well beyond the GRC team itself.

Table 1 maps SecurityScorecard's core capabilities to the continuous, threat-informed model described in this paper.

Table 1**SecurityScorecard capability mapping to the continuous/threat-informed model**

TPRM capability area	Continuous/threat-informed requirement	SecurityScorecard capability
Vendor risk scoring	Risk signal that updates continuously rather than at scheduled reassessment	Ratings platform continuously recalculates vendor scores from observed security posture data.
External attack surface visibility	Outside-in discovery of internet-exposed and hidden vendor infrastructure	Driftnet-powered scanning indexes 40% more internet-exposed hosts than other intelligence providers, using non-standard port enumeration, fingerprinting, and IPv6-focused discovery.
Threat intelligence correlation	Active threat and campaign data connected to specific vendor exposure, not just static findings	The STRIKE threat intelligence team feeds active-campaign data into the TITAN AI platform, correlating it against vendor-specific exposure.
Breach and incident evidence	Quantified, current data on third-party involvement in breaches	The Global Third-Party Breach report tracks third-party involvement in breaches over time.
Stakeholder-specific views	Risk information usable by both security and non-security stakeholders	Persona-specific reporting for the CISO, CRO (risk), CRO (revenue), TPRM/GRC leader, SecOps, and threat intelligence teams

Source: SecurityScorecard, 2026

Challenges

- Vendors and buyers alike have raised concerns about agentic and autonomous scanning tools operating directly inside third-party environments. Trust and permissioning remain unresolved and are likely to slow adoption of agent-based approaches relative to API-based telemetry.
- Persistent silos between GRC and security operations continue to slow adoption of a unified, threat-informed operating model, even where the underlying data already exists to support one. An August 2026 IDC survey found that no single ownership model dominates TPRM programs today: 35.3% run a centralized TPRM office, 20.7% are cybersecurity-led, 18.8% are federated, 10.0% sit with enterprise risk/compliance, 9.5% are decentralized by business unit, and 5.5% are procurement-led — a fragmented picture that makes shared, threat-informed data harder to operationalize (IDC's *Third-Party Risk Management Software Survey*, August 2026).
- Fifty-five percent of organizations still rely on manual outreach after a breach (SecurityScorecard, 2026), leaving significant white space for automated, continuous alternatives. IDC's own survey data reinforces the size of that gap: Only 16.2% of organizations describe continuous monitoring as their primary TPRM assurance method today, versus 40.2% still centered on evidence-based assessment and 16.8% on audit-based deep assessment — underscoring both the opportunity and the distance still to travel (IDC's *Third-Party Risk Management Software Survey*, August 2026).

- Legacy vulnerabilities in third-party code persist despite periodic penetration testing, underscoring the structural limits of point-in-time assurance, regardless of how frequently it is repeated.

Opportunities

- Growing buyer preference for continuous, API-based telemetry over more invasive agent-based scanning of vendor environments plays to SecurityScorecard's existing outside-in data model.
- An emerging link between documented, continuous security posture and cyber-insurance underwriting creates a new value driver for TPRM investment beyond compliance alone.
- Confidence scoring and accelerated onboarding create room to bring procurement and business owners directly into real-time risk decisions, rather than routing every decision through a GRC bottleneck.
- Aggregating scan data with real-time threat feeds — an area where the Driftnet acquisition adds meaningful depth — positions the platform to help customers prioritize vulnerabilities proactively rather than simply reporting on them after the fact.
- The TPRM software market is in flux: 30.9% of organizations say they are likely to switch TPRM software providers within the next 18 months (IDC's *Third-Party Risk Management Software Survey*, August 2026) — a level of churn that rewards vendors able to differentiate clearly on continuous, threat-informed capability.

Conclusion

The third-party risk model built around annual questionnaires and dormant right-to-audit clauses no longer matches the threat environment for which it was designed. IDC believes continuous, threat-informed TPRM — built on inside-out telemetry, API-based data collection, and risk scoring tied to business context — will keep displacing point-in-time assessment as the baseline operating model over the next several years, and that the endpoint of this shift is a TPRM life cycle that is more than 90% automated, with analysts reviewing machine-generated findings rather than producing them by hand. To the extent that SecurityScorecard can help customers travel the path from periodic to continuous to threat-informed TPRM, and can translate its expanded visibility into internet-exposed infrastructure into faster, more actionable prioritization, the company has a meaningful opportunity to grow alongside a market moving in its direction.

About the IDC analyst



Philip D. Harris, CISSP, CCSK

Research Director, Governance, Risk, and Compliance (GRC) Solutions

Phil Harris is Research Director for GRC Solutions at IDC, where he develops and promotes IDC's point of view on risk, advisory, privacy, and compliance services and software. He conducts research on business strategies and the impact of relevant offerings on enterprises, collaborating with worldwide and regional analysts to deliver thought leadership and actionable insights for IT buyers and suppliers.

More about [Philip D. Harris](#)

Message from the sponsor

From point-in-time snapshots to continuous, threat-informed risk visibility

Third-party risk management is moving from periodic assessment to continuous, threat-informed operations. SecurityScorecard supports this shift by combining continuously updated security ratings with threat intelligence, giving organizations ongoing visibility into vendor risk rather than a point-in-time snapshot.

The company's ratings are built on its own breach and threat-intelligence data, extended by its 2026 acquisition of Driftnet, which added visibility into internet-exposed infrastructure, including nonstandard ports and IPv6-based assets that traditional scanning can miss. SecurityScorecard organizes its platform around four stages of TPRM maturity — Basic Diligence, Periodic TPRM, Continuous TPRM, and Threat-Informed TPRM — to help organizations progress from questionnaire-based assessment toward continuous, evidence-based oversight of third-party risk.

To learn more about SecurityScorecard's approach to continuous, threat-informed third-party risk management, visit [SecurityScorecard | Supply Chain & Third-Party Risk Platform](#).

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for [external use](#), and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



IDC Research, Inc.

One Beacon Street, Suite 33100, Boston, MA 02108, USA

T +1 508 872 8200

blogs.idc.com | LinkedIn [@IDC](#) | www.idc.com

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 and industry opportunities and trends in over 110 countries.