



EBOOK

AI-Powered TPRM: An Answer to Endless Questionnaires

The current state of third-party risk management (TPRM) is a dangerous paradox. According to industry data, 90% of security leaders express confidence in their ability to maintain seamless operations during a vendor cybersecurity incident.¹ However, 78% of organizations admit their internal cybersecurity programs cover less than half of their total ecosystem.² This precarious dynamic of high confidence and low visibility creates serious blind spots across the risk landscape.

Unfortunately, the legacy approach to TPRM relies on reactive tools and static, checkbox-driven assessment cycles that are biannual or even longer. Organizations often dispatch massive spreadsheets containing up to 200 questions to their suppliers, forcing risk teams to endure assessment delays of six weeks or longer. This framework leads to questionnaire fatigue, with repetitive requests burying vendor bandwidth while manual evidence evaluation overwhelms internal risk teams.

The changing threat landscape makes this approach even more precarious. According to Verizon Business, third parties are now involved in 48% of all data breaches.³ That's an increase of 60% from the previous year.⁴

When a breach actually occurs, disconnected tools and outdated frameworks often fail to provide immediate context, and teams scramble to answer basic questions. How many vendors are affected? Do they need to be contacted? Is their contact information even correct? What steps must they take immediately to protect the organization?

At the pace of supply chain threats today, this type of delay is an active risk to the business itself. Modernizing workflows and reducing manual compliance workflows is necessary for organizations to secure their vendor ecosystems and eliminate the visibility gap. Going forward, AI-driven automation provides the continuous strategic advantage needed to power that transition.

Perception vs. Coverage

90%

Confident in vendor incident resilience

Actual ecosystem coverage

22%

More than half covered

78%

Less than half covered

Resolving the false sense of security

Traditional, static risk management models rely entirely on manual vendor inquiry. A shift to embrace automation fundamentally changes the vendor assessment paradigm from broad inquiry to precise verification.

Organizations can leverage AI to evaluate existing public data before any questions are sent to the vendor. For example, natural language processing instantly parses complex compliance evidence and audit reports. AI may also automatically evaluate ISO certifications without manual human intervention. These systems can even map vendor claims accurately against real-time technical realities.

As a result, human analysts only need to manage and verify the relatively small percentage of unverified data. Without the burden of extensive manual inputs and tasks, they're free to focus on proactive, strategic risk management instead.

A shift to embrace automation fundamentally changes the vendor assessment paradigm from broad inquiry to precise verification.

By the numbers: Solving the “questionnaire gap” with AI

42

hours, down from 42 days, is the new timeline for vendor onboarding.⁵

UP TO
18x

faster processing speeds are now possible for GRC and Security teams.⁶

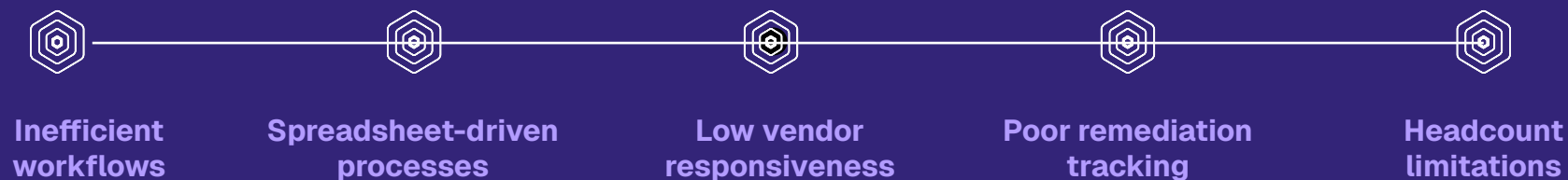
45

minutes is all it takes to process standard questionnaires.⁷

Accelerating TPRM with new capabilities and efficiencies

TPRM leaders and GRC teams, in particular, are consistently constrained by challenges related to manual workload requirements. The consequences impact their organizations both operationally and culturally.

Where the work breaks down



By using AI to replace manual follow-up work with structured and repeatable outreach processes, TPRM and GRC teams can gain more of the capabilities they need while significantly reducing the inefficiencies that compromise their work.

The integration of AI into the assessment lifecycle allows teams to achieve as much as a 92% reduction in manual effort.⁸ Automation eliminates the manual evaluation of not only lengthy questionnaires but also complex SOC 2 reports. The implementation enables teams to drive measurable, positive outcomes for program effectiveness and elevate TPRM beyond simple compliance tracking. These efficiencies also directly benefit program scalability without requiring additional headcount investments.

Solidifying SecOps with amplified threat intelligence

More than ever, security operations and vulnerability teams are overwhelmed by high vulnerability volumes. Teams experiencing alert fatigue often struggle to prioritize threats. Even when internal assets are secure, suppliers can inadvertently expose critical attack paths that create dangerous third-party blind spots.

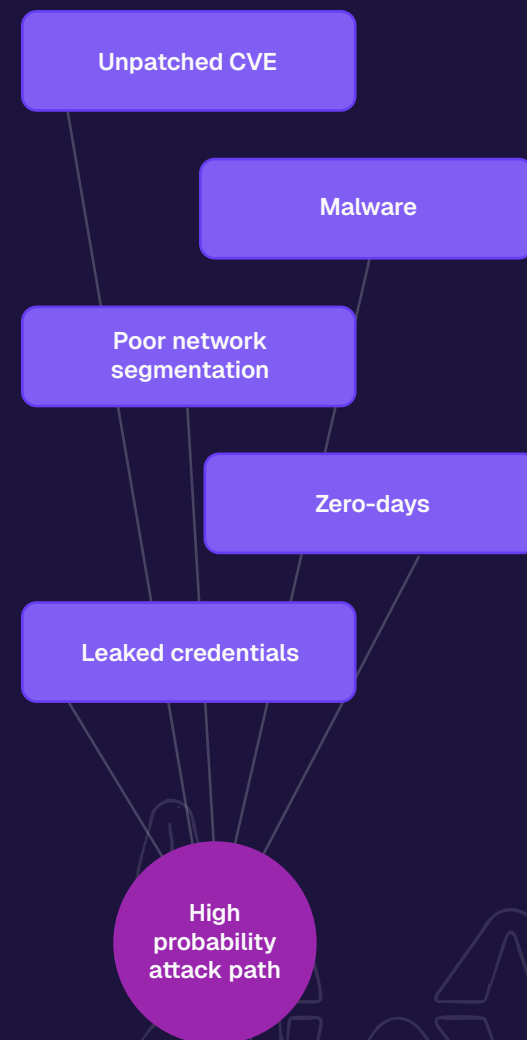
AI provides the context required to identify real, exploitable risks across the third-party ecosystem. For example, a vendor may have an unpatched CVE, malware and poor networking segmentation that combined present high risk, something AI can flag and even send relevant communications about.

Security teams can use AI to correlate combinations to reveal high-probability attack paths that isolated alerts may otherwise miss.

Another key complication occurs when TPRM teams scramble to react to breach headlines and provide clarity to worried executives. With AI-powered workflows, they can gather a list of vendors impacted by Common Vulnerabilities and Exposures (CVE) as soon as news breaks about them — and before their CISO even asks for it. Automation can take this a step further by requesting action from exposed vendors or offering policy-aligned remediation advice.

Additionally, continuous external monitoring provides real-time detection of zero-days, leaked credentials, and malware-related issues. Armed with this intelligence, analysts no longer have to view vulnerabilities in a vacuum. Instead, they can focus their limited time on active risks that lead to exploitation. This shared visibility enables TPRM and SecOps teams to work more closely together and align their priorities with regard to potential risks.

AI adds context where isolated alerts cannot.



Proactive remediation with a unified defense

40%

of organizations cite manual communication as the primary barrier to timely risk resolution.⁹

+50%

of organizations still rely on outdated phone numbers and emails to coordinate with vendors during active breaches.¹⁰

8+ days

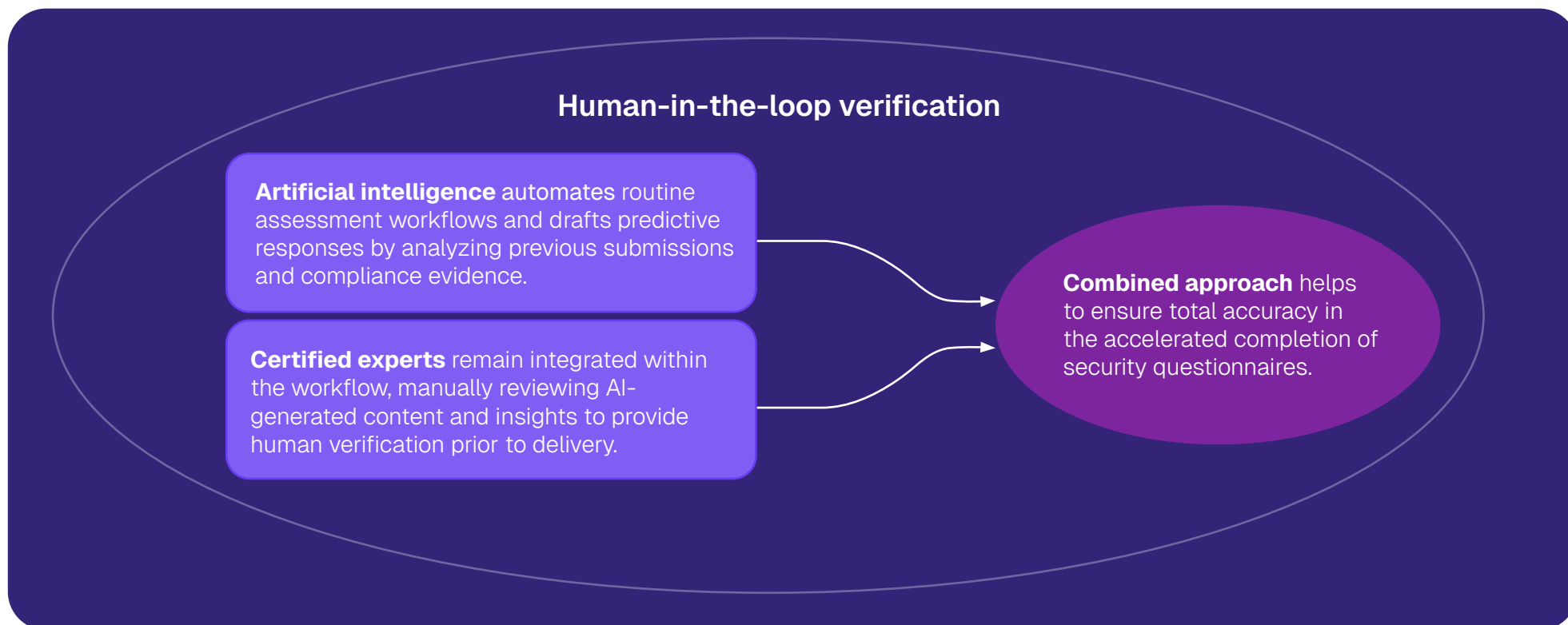
for 60% of organizations to remediate a high-severity issue once it has been identified.¹¹

Ultimately, AI is a key tool to bolster both TPRM compliance operations and SecOps threat response capabilities. With a centralized approach, both teams are better equipped to work together to establish a living, always-current source of truth across the entire vendor ecosystem. Automating workflows helps them significantly reduce manual delays and successfully transition from a reactive cybersecurity posture to proactive threat defense.

Trust in the age of AI adoption

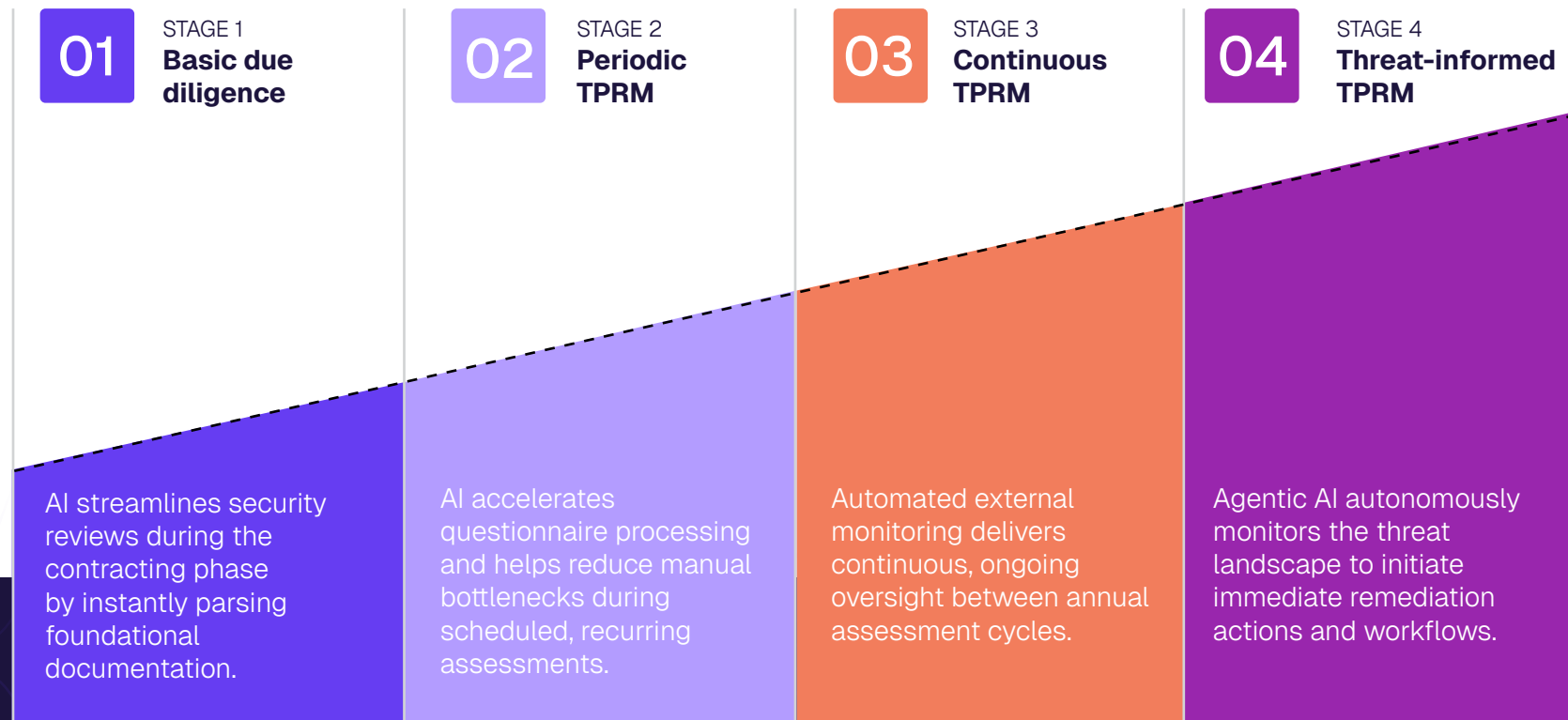
CISOs face immense pressure to integrate AI into their threat defense strategies. But a lack of clear return on investment can hinder this mandate. Many organizations also harbor legitimate concerns regarding data privacy and the AI governance policies of their partner providers.

Safely navigating the evolving threat landscape requires strong internal AI policies as a starting point. Proactively addressing trust also helps to ensure that AI empowers teams instead of simply adding to the existing alert noise. A “human-in-the-loop methodology”—where humans are the ultimate decision-makers and AI is a tool that facilitates their work—delivers critical benefits to alleviate concerns and bridge the evolving gap between automated speed and total reliability.



Applying AI across the TPRM maturity curve

The maturity stage of a TPRM program dictates which AI capabilities an organization can choose to implement to empower its TPRM and SecOps teams. Examples of those capabilities, depending on the maturity stage, include:



The end result is a transformation of TPRM from a manual compliance chore that uses reactive tools into a proactive threat defense built on a continuous strategic advantage.

SecurityScorecard's TITAN AI autonomously connects threat intelligence with third-party data to continuously detect and respond to risk. By prioritizing real risks and engaging vendors effectively, organizations can use TITAN AI to evolve from compliance-driven programs to operational, threat-informed TPRM.

To learn how you can proactively address risks in your vendor ecosystem, [read more about how continuous threat intelligence powers TPRM.](#)

SecurityScorecard is the global leader in threat-informed third-party risk management (TPRM), securing the world's supply chains. The company delivers a threat-informed approach to TPRM that enables organizations to drive out risk at the source. The platform uses continuous visibility and AI-accelerated workflows to help organizations reduce third-party risk before incidents occur and respond with confidence when they do.

Trusted by over 3,300 organizations, including 70% of the Fortune 100, and recognized as a trusted resource by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, Google Ventures, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity.

Protect the supply chain behind your business. Learn more at securityscorecard.com.

SOURCES

- ¹ SecurityScorecard, [2026 Supply Chain Cybersecurity Trends Report](#)
- ² Ibid.
- ³ Verizon Business, [2026 Data Breach Investigations Report](#)
- ⁴ Ibid.
- ⁵ SecurityScorecard, [The TPRM Evolution: From Checkbox to Continuous Intelligence](#), 2026
- ⁶ SecurityScorecard, [TITAN Assess: AI-Powered Security Questionnaire Automation & Compliance](#), 2026
- ⁷ Ibid.
- ⁸ Ibid.
- ⁹ SecurityScorecard, [The TPRM Evolution: From Checkbox to Continuous Intelligence](#), 2026
- ¹⁰ SecurityScorecard, [2026 Supply Chain Cybersecurity Trends Report](#)
- ¹¹ Ibid.

