SecurityScorecard

EBOOK

TPRM PRACTITIONER GUIDE

The Questionnaire Trap

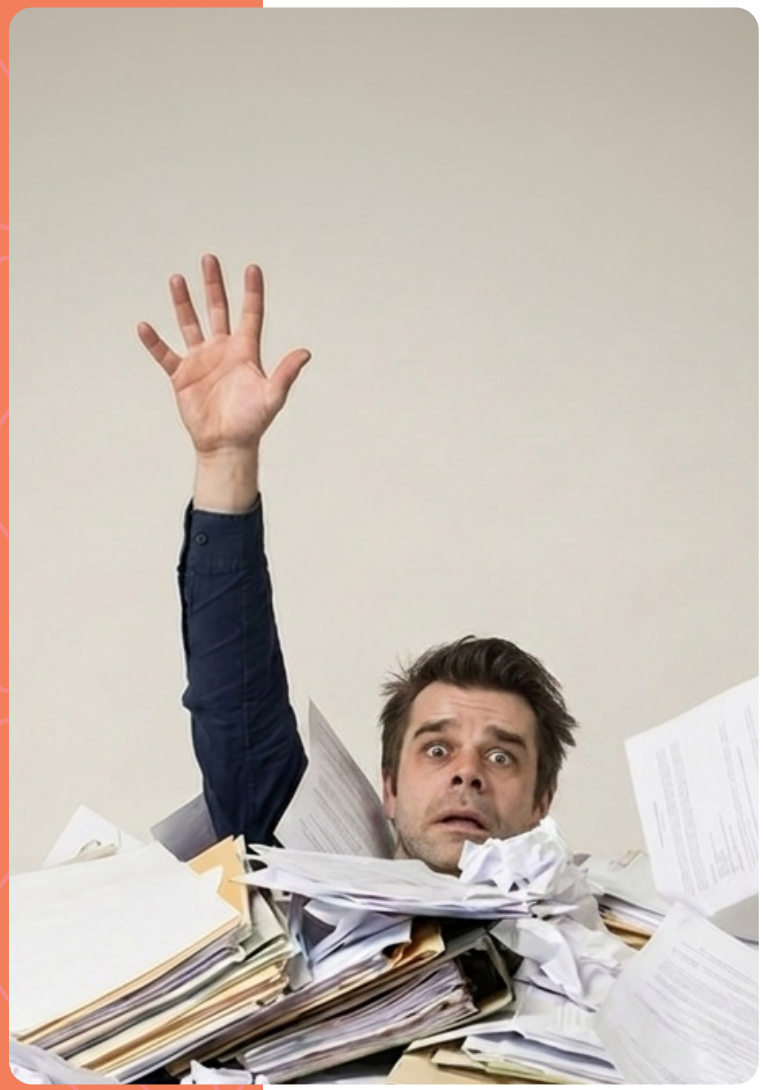
Why More Questions Mean Less Security, and What the Best TPRM Teams Do Differently

INSIGHTS FROM EXPERIENCED RISK MANAGEMENT PRACTITIONERS ON THE FUTURE OF VENDOR ASSESSMENTS

Contents

INTRODUCTION

We Built the Pool Ourselves



> *The questionnaire is not the enemy. The enemy is the unexamined questionnaire — the one that grew by accretion, was never pruned, and now exhausts everyone without protecting anyone."*

Third-party risk management programs were supposed to make organizations safer. Instead, many have become monuments to bureaucratic inertia: rooms full of spreadsheets, backlogs of unanswered questionnaires, and risk teams spending the majority of their time chasing vendors for responses rather than actually reducing risk.

The security questionnaire, in theory, is a sensible tool: ask vendors how they protect data, evaluate their answers, decide whether to work with them or hold them to higher standards. In practice, it has turned into something far less useful: a Frankenstein's monster of accumulated regulations, outdated standards, and well-intentioned additions that nobody has ever had the courage to remove.

This guide is for the TPRM leaders, risk managers, and security professionals who know something is wrong but have been too busy treading water to think about how to drain the pool. It draws on candid conversations with experienced practitioners and the latest research on what high-performing TPRM programs actually look like.

The good news: the path forward is clear. It requires letting go of some deeply held assumptions (that more questions mean more insight, that annual reviews are sufficient, that every vendor deserves the same level of scrutiny) and replacing them with a more intelligent, evidence-driven, and frankly more effective approach.

1 The Questionnaire Industrial Complex

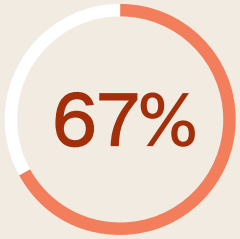
Before we can fix the problem, we need to understand its scale. The numbers tell a clear story: this is a system under serious strain.

Yet for all their ubiquity, questionnaires are struggling to keep up with the demands placed on them. Vendor ecosystems are growing. Regulatory requirements are multiplying. TPRM teams are not.

The result is a growing assessment gap: the difference between the number of vendors an organization has and the number it can realistically evaluate. For many organizations, this gap represents significant, unquantified risk hiding in plain sight.

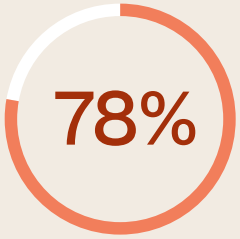
The burden falls on both sides of the questionnaire equation. TPRM teams are overwhelmed. So are the vendors they are trying to assess. Inbound assessment requests have risen sharply year over year, driving frustration, delayed responses, and lower-quality answers.

This is vendor fatigue at industrial scale. And it's getting worse. The tool meant to reduce risk has become a source of organizational strain, slowing down vendor relationships, generating resentment, and producing responses that are less thoughtful than they should be.



of organizations still rely on static, point-in-time security audits to assess their vendors, even as supply chain ecosystems expand rapidly and the threat landscape evolves daily.

Source: SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report



of organizations admit their internal cybersecurity programs cover less than 50% of their total vendor ecosystem, leaving the majority of third-party relationships effectively unexamined.

Source: SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report

Security teams now spend 47 or more hours every week analyzing third-party access risks alone, with nearly a third investing over 100 hours weekly. The average organization now manages 286 vendors, up from 237 just one year prior.

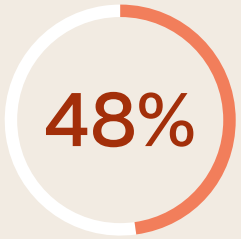
Source: Ponemon Institute, 2025 Third-Party Risk Report

The Risk Is Real, and Growing

While teams wrestle with questionnaire backlogs, the threat landscape is accelerating.

SecurityScorecard's own research finds that 12.7% of third-party breaches cascade into fourth-party incidents, showing how a single compromised vendor can ripple through an entire supply chain. When attackers get in through one door, they walk through many.

The status quo is not working. Annual questionnaires sent to every vendor, reviewed by overstretched teams, are not adequately protecting organizations from the risks they face. Something has to change.



of all breaches in 2025 were third-party related, according to the Verizon 2026 Data Breach Investigations Report. Supply chain compromise now ranks as the second costliest attack vector, averaging $4.91 million per incident.

Source: Verizon Business 2026 Data Breach Investigations Report; IBM Cost of a Data Breach Report 2025

2 The Frankenstein Questionnaire

Ask anyone who has spent time in TPRM how their organization's questionnaire was built, and you'll often hear the same story. It started with a reasonable baseline, often a SIG questionnaire or an internal adaptation of NIST. Then regulations changed, and five questions were added. Then a high-profile breach made headlines, and another 10 were appended. Then AI became a topic of concern, and a new section appeared almost overnight.

Nobody ever removed anything from the questionnaires.

of TPRM leaders say they would prioritize revisiting and refreshing their organization's TPRM methodology, yet most programs continue operating with questionnaires built years ago and never substantially updated.

Source: Deloitte, Third-Party Risk Management Survey 2025

> *"When third-party risk management really became a thing, organizations all started with the SIG. Then new regulations came into play, they added five more questions. Then AI came into play and they added ten more AI questions. It just became this Frankenstein of questions and controls — with no good flow and no real curation."*

Morgan Strobel
Third Party Risk Leader
Crowe

The result is questionnaires that are difficult to answer, difficult to evaluate, and that generate volumes of data teams simply don't have the capacity to address. Three specific failure modes show up repeatedly:

FAILURE MODE 1:

Irrelevant Questions

If a vendor's answer would never result in a finding being raised (because the team doesn't have time, doesn't have authority, or simply doesn't consider it material), asking the question wastes everyone's time. Every question in a questionnaire should be traceable to a potential action.

> *"If you're asking the question and the vendor says no — and you're not going to create a finding about it — then maybe think about why you're asking this question at all."*
>
> **Kassi Wilson**
> Senior Manager, Third Party Risk Consulting
> Crowe

FAILURE MODE 2:

Questions Nobody Understands

Ambiguous questions and compound questions (two questions rolled into one with only a single yes or no answer available) are more common than most teams realize. They generate noise rather than signal, and put vendors in the impossible position of giving an accurate answer to a poorly formed question.

> *"We regularly see questions that are vaguely and ambiguously written. When I ask the customer what they mean, they often say they're not really sure. Someone threw the question in and nobody questioned it. If the customer doesn't know what a good answer looks like, the vendor certainly won't either."*
>
> **Simon Jones**
> Senior Director, Partner Delivery
> SecurityScorecard

FAILURE MODE 3:

One Size Fits All

Sending the same 500-question questionnaire to a critical SaaS provider and a minor office supplies vendor is not risk management; it is checkbox compliance. The questions that matter for a managed service provider with deep data access are different from those relevant to a hardware vendor with no network presence. Tailoring assessments to the actual risk profile of the vendor and service is fundamental, and many organizations still aren't doing it.

Beyond these structural problems, questionnaires often fail at the review stage. Because a questionnaire is a self-assessment, it is only as reliable as the validation performed on top of it. Many organizations accept vendor responses at face value and move on, which means the entire exercise generates a false sense of assurance rather than genuine risk reduction.

3 Beyond the Annual Audit: The Case for Trigger-Based TPRM

The most fundamental problem with the traditional questionnaire model is the calendar. Most TPRM programs send questionnaires on an annual schedule, regardless of what has actually changed in the relationship, the vendor's security posture, or the threat landscape. This is risk management driven by convention, not by actual risk.

Trigger-based assessment works by monitoring for events that signal a real change in vendor risk and escalating assessment activity in response. These triggers can be external (a cyber incident in the news, a change in security posture indicators, a zero-day affecting the vendor's technology stack) or internal (a change in the scope of services, a new integration, an acquisition).

> *"I would like to see us move away from the calendar as the driver of risk activity and really replace it with actual risk events as the trigger. The annual questionnaire doesn't go away entirely — it just becomes the entry point. Everything after that should be driven by data, not dates."*
>
> **Morgan Strobel**
> Third Party Risk Leader
> Crowe

What a Trigger-Based Model Looks Like

In a mature trigger-based program, a vendor goes through a comprehensive initial assessment during onboarding. If that assessment reveals no critical or high-risk findings, the vendor moves into a lighter monitoring phase, with continuous data collection replacing the intensive annual questionnaire.

When a trigger fires (a security incident, a financial event, a change in ownership), the assessment engine activates. Analysts review the relevant question set for that trigger type, determine whether additional outreach is warranted, and document their reasoning. This creates a defensible audit trail that regulators increasingly expect.

> *Regulators are specifically looking for continuous monitoring. What they really want is documentation and explainability — an appropriate audit trail that shows what the trigger was, what actions you took, and when. As long as you have that, this model meets regulatory requirements."*
>
> **Morgan Strobel**
> Third Party Risk Leader
> Crowe

Concentrating Resources Where They Matter

A trigger-based model lets teams redirect human expertise toward the vendors that pose the greatest actual risk. Critical vendors, particularly those representing single points of failure or those with the deepest access to sensitive systems, may warrant something more intensive than even a detailed questionnaire. Tabletop exercises, resiliency assessments, and deeper technical reviews become possible when the team is no longer buried in low-signal annual reviews.

> *For critical vendors, you're now considering going back to on-sites or doing something more substantial — tabletop exercises, resiliency-focused assessments. The trigger-based model gives you the flexibility to spend less human time on lower-risk vendors and redirect that capacity to the ones that really matter."*
>
> **Morgan Strobel**
> Third Party Risk Leader
> Crowe

The point isn't doing less. It's doing the right things for the right vendors at the right time. A 500-question annual questionnaire sent to every vendor is not more rigorous than a targeted, evidence-driven assessment of your highest-risk partners. It is just noisier.

4 Trust, But Verify: The Documentation-First Revolution

The most effective change most TPRM teams can make is to start with evidence rather than questions. The documentation-first approach inverts the traditional model: instead of asking vendors to self-attest to their controls and then requesting supporting documentation, you request the evidence first and only ask questions about what that evidence does not answer.

That means requesting SOC 2 reports, relevant policies, certifications, and trust portal access before sending a questionnaire. A reviewer (or an AI assistant) works through the documentation and maps it to the question set. Questions go out only for what the evidence doesn't cover.

> *Think about it from the vendor's perspective: you may not be the first person who has contacted them this week, this month, or even today about an assessment. Meeting vendors where they are — accepting their existing documentation, using trust portals, receiving pre-packaged evidence — is a sign of respect and dramatically accelerates the process."*

Simon Jones
Senior Director, Partner Delivery
SecurityScorecard

Five Principles of Effective Questionnaire Design

Beyond the documentation-first approach, practitioners consistently point to five principles that separate effective questionnaire programs from exhausting ones:

1. **Be ruthless about purpose.** If a negative answer would not generate a finding, remove the question. Every question must be traceable to a potential action.
2. **One question, one control.** Compound questions produce compound confusion. Each question should address a single control with a clear, unambiguous answer.
3. **Tailor for relevance.** Use conditional logic to skip sections that do not apply to the vendor's actual service. Do not ask hardware security questions of a SaaS-only provider.
4. **Write for the reader.** Avoid jargon, ambiguity, and open-ended free-text fields wherever possible. If you cannot articulate what a good answer looks like, the question is not ready.
5. **Keep it current.** Review your question set regularly against the compliance standards you are measuring against. Standards evolve; your questionnaire must too.

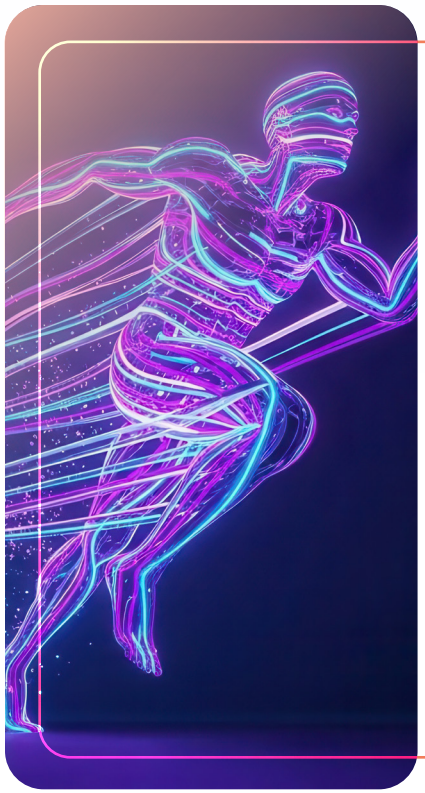
Validation Is Not Optional

A questionnaire is a self-assessment. Vendors report on their own controls, their own policies, their own practices. Without validation, you are trusting but not verifying. For higher-risk vendors, validation might mean cross-referencing questionnaire responses with external security posture data or reviewing a sample of evidence in depth. For lower-risk vendors, a lighter spot-check may suffice. The key is that some form of validation is always present, and always documented.

> *A questionnaire is only as good as the validation the assessor performs on top of it. A lot of organizations make the mistake of trusting what's in the responses — and that will not appropriately identify risks. You need to verify responses through the documentation and artifacts you collect as part of the assessment."*
>
> **Morgan Strobel**
> Third Party Risk Leader
> Crowe

5 AI Is Already at the Table, on Both Sides

Artificial Intelligence is rapidly changing the security questionnaire from both directions at once. Vendors are increasingly using AI to generate questionnaire responses. Assessors are using AI to analyze them. Understanding how both dynamics work, and where human judgment remains irreplaceable, is critical for any TPRM team.



AI on the Vendor Side: Faster Answers, Same Accountability

Many vendors are now deploying AI tools to help respond to incoming questionnaires. These tools ingest the vendor's own policies, certifications, and documentation and generate question-by-question responses based on their internal knowledge base. For a vendor receiving 37+ assessment requests per month, this is a rational response to an unsustainable workload.

The accountability does not change because the answer was generated by an algorithm. An AI tool that extrapolates from an outdated document or confidently reports a control that does not exist in practice produces responses that are wrong in a way that is harder to detect. Assessors who know that AI is likely involved on the vendor side should be more disciplined about evidence validation, not less.

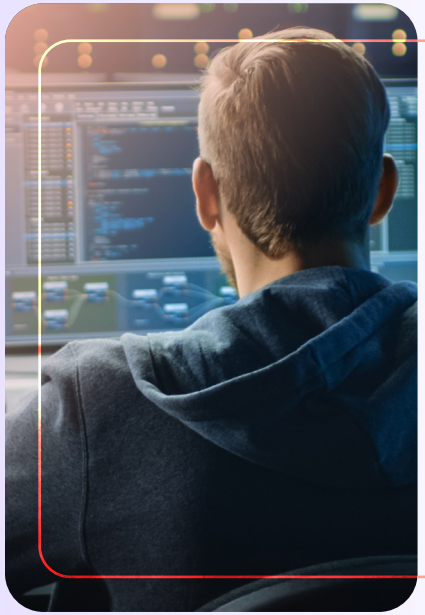
> *If AI is responding versus a person, you're probably getting better answers in some respects — the AI is actually pulling from the vendor's policies and procedures. But you're still going to be validating with evidence, whether it's AI or a person responding. The same standard applies."*

Kassi Wilson
Senior Manager, Third Party Risk Consulting
Crowe

AI on the Assessor Side: Force Multiplier, Not Replacement

On the assessor side, AI offers significant opportunities to close the coverage gap. It can review incoming documentation and auto-populate questionnaire responses. It can flag inconsistencies between a vendor's stated controls and their externally observable security posture. It can prioritize follow-up questions and surface responses most likely to warrant deeper review.

For teams managing hundreds of vendor relationships with small headcounts, these capabilities are a real force multiplier. Organizations using AI-assisted assessment workflows report reductions in vendor onboarding time of 40-50% and cuts in manual effort of 70-80%. Assessments that once took weeks complete in under 10 days.



The Human-in-the-Loop Imperative

Human judgment remains essential to effective TPRM. AI can process data faster, identify patterns, and dramatically reduce the administrative burden of questionnaire management. But understanding the specifics of a vendor relationship, evaluating the credibility of a claim in context, and making defensible risk decisions requires expertise that no current AI system can fully replicate.

The goal is to automate the parts of TPRM that don't require a human expert, so that human experts can spend their time on the things that actually do.

> *"AI is an incredibly valuable tool. But nothing is going to replace human judgment. We absolutely need full oversight and understanding of what a vendor has provided to us — what it means, what risk it represents, what we should do about it. AI is a force multiplier, not a substitute."*

Simon Jones
Senior Director, Partner Delivery
SecurityScorecard

6 Your Quick Win Playbook

Theory is useful. But what can you actually do this quarter to start moving your program toward a smarter, more effective approach? Practitioners consistently point to three actions that deliver immediate, measurable improvements.

QUICK WIN 1

Audit Your Questionnaire

Take your current questionnaire and go through it question by question with a simple test: if a vendor answers this question poorly, are we actually going to do something about it? For every question where the honest answer is “probably not,” either fix the question or remove it.

Check for compound questions. Remove or rewrite anything ambiguous. Flag open-ended free-text fields where you cannot articulate what a good answer looks like. And review the question set against your current compliance standards. If your questionnaire is based on a framework version that’s two or more years out of date, you’re missing key controls.

> *“It’s time to go back and look at your questions, your control set, and make sure you’re really curating it. No compound questions. No open text fields. No ambiguous questions. Questions that you need answers to — that you will actually make issues out of. Especially now, with AI in the mix, this is the moment to get your questionnaire right.”*
>
> **Morgan Strobel**
> Third Party Risk Leader
> Crowe

QUICK WIN 2

Pilot a Documentation-First Intake

Select a cohort of upcoming vendor assessments and run them with a documentation-first approach. Request SOC 2 reports, relevant policies, and any existing trust portal access before sending a single question. Document how many questionnaire items are answered by the evidence, and send questions only for the rest.

Track cycle time, vendor friction, and the quality of findings against a comparable cohort that went through your standard process. The results will make the business case for broader adoption more compellingly than any slide deck.

QUICK WIN 3

Define Your Trigger Criteria

You do not need to rebuild your entire program to start thinking trigger-based. Begin by defining: what events, if they happened to one of your vendors, would cause you to take immediate action? A high-severity breach? A significant drop in security posture indicators? A change in ownership or a financial event?

Document those triggers. Set up whatever monitoring is available to alert you when they occur. Start tracking how often you are responding to triggers versus waiting for the annual cycle. Over time, that data will tell you exactly how to evolve your program.

"One decision you can make today: take a step back and ask, 'What do we actually want to get out of our third-party risk program? What is the point of it for our organization?' Then make sure everything you're doing — every question you're asking, every assessment you're running — is in service of that goal."

Morgan Strobel
Third Party Risk Leader
Crowe

CONCLUSION

What Good Looks Like in 3-5 Years

The best TPRM programs of the future will look significantly different from those of today. The annual questionnaire cycle (the backbone of most current programs) will give way to a more dynamic, intelligence-driven model in which continuous data collection triggers targeted assessments, and human expertise is concentrated on the relationships and moments where it matters most.

Questionnaires will not disappear. They will evolve into a more focused instrument: shorter, smarter, and better aligned to the specific risk profile of each vendor. The documentation-first approach will become standard practice, with AI handling the heavy lifting of evidence review and response analysis while human analysts focus on validation, judgment, and the things that cannot be automated: understanding context, building vendor relationships, and making defensible decisions under uncertainty.

The organizations that will fare best in this transition are those that start now. Not by investing in technology alone, but by getting clear on what their TPRM program is actually trying to accomplish, curating their assessment content to match that purpose, and putting the right processes in place to move from reactive, calendar-driven assessment to proactive, risk-driven assurance.

Traditional TPRM	Future-Ready TPRM
Calendar-driven (annual)	Trigger-based and event-driven
Same questionnaire for all vendors	Risk-tiered, tailored assessments
Questions first, evidence requested second	Evidence first, questions for the delta
Manual review with low coverage	AI-assisted review with high coverage
Responses accepted at face value	Trust but verify, always
Risk accepted by default	Risk tracked and actively remediated

Organizations that invest in this transformation will do more than save time and money. By curating their questionnaires, adopting documentation-first processes, and building the infrastructure for trigger-based monitoring, they will build TPRM programs that actually reduce risk, satisfy regulators, and protect their business from the supply chain threats already reshaping the cybersecurity landscape.

The questionnaire trap is real. But it is escapable. And the way out starts with a single decision: to measure what matters, ask only what you will act on, and trust, but always verify.

Sources & Citations

67% of organizations still rely on static audits.
SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report.
https://securityscorecard.com/resources/research/2026-supply-chain-cybersecurity-trends-report/

78% cover less than 50% of their vendor ecosystem.
https://securityscorecard.com/resources/research/2026-supply-chain-cybersecurity-trends-report/

Security teams spend 47+ hours weekly on third-party risk analysis, with nearly a third investing over 100 hours weekly.
https://www.kiteworks.com/cybersecurity-risk-management/third-party-access-risks-manufacturing-2025-ponemon-report/

Average vendor inventory now 286 vendors.
https://dynamicbusiness.com/topics/technology/one-misconfigured-vendor-one-lost-deal-one-lesson-too-late.html

36% of all breaches in 2024 were third-party related
Link

Supply chain compromise identified as the second costliest attack vector at $4.91 million average.
IBM, Cost of a Data Breach Report 2025.
https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

63% of TPRM leaders want to revisit their methodology.
Deloitte's 2023 Third-Party Risk Management Survey

48% of all breaches in 2025 were third-party related
Verizon 2026 DBIR
https://www.verizon.com/business/resources/reports/dbir/

About SecurityScorecard

SecurityScorecard is the global leader in threat-informed third-party risk management (TPRM), securing the world's supply chains. The company delivers a modern, threat-informed approach to TPRM that enables organizations to drive out risk at the source. Through continuous visibility, AI-accelerated workflows, and predictive insights, the platform transforms third-party risk into a competitive advantage, empowering organizations to proactively reduce risk before incidents occur and respond with confidence when they do, delivering measurable supply chain resilience.

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, NGP Capital, Intel Capital, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity.

SecurityScorecard