SUPPLY CHAIN RESEARCH

Independent · vendor-neutral research

Supply Chain Risk Management

The 2026 Buyer's Guide & Vendor Landscape

A practitioner's guide to evaluating, costing, and selecting supply chain risk and supplier risk software: what these systems do, how the market and vendors stack up in 2026, what they cost, how to run the selection, and how to de-risk the rollout.

Prepared by **Supply Chain Research** · June 2026 · Vendor-neutral: we take no payment from the vendors covered.

Contents

1. Executive summary

Supply chain risk management software exists to answer a question that has become a board-level concern: where is the next disruption coming from, and how exposed are we to it? The category spans multi-tier supplier mapping, continuous monitoring of financial, operational, geopolitical, cyber, and environmental risk, disruption detection and alerting, and supplier financial health. It is best understood as two related but distinct disciplines: supplier risk management, which is procurement-led and supplier-specific, and supply chain disruption monitoring, which is event-driven and network-wide. In 2026 the category is being propelled by a tariff and trade-war surge, by forced-labor and sustainability regulation, and by the first wave of agentic AI, against a backdrop in which global disruptions rose sharply in 2024.

This guide is written for procurement, supply chain, risk, and IT leaders evaluating a risk investment, and for the teams who must integrate it and act on its alerts. It is deliberately vendor-neutral: we accept no payment from the vendors covered, and we name no single best platform, because the right choice depends on whether your priority is supplier-specific risk or network-wide disruption, your industry, and your regulatory exposure. The pages that follow define the category and that central distinction, size the market honestly across its very different definitions, profile the n-tier, financial-health, ESG, and procurement-embedded tiers, lay out an evaluation framework, and explain why supplier-data quality and acting on the signal, not the dashboard, decide the return.

$1-20B	First MQ	+38%
range of 2025 estimates, from narrow risk software to broad supply-chain-plus-services definitions	Gartner published its first-ever Supplier Risk Management Magic Quadrant in April 2025	the rise in global supply chain disruptions in 2024, versus 5 percent in 2023 (Resilinc, vendor-reported)

What the evidence says

Supplier risk and disruption monitoring are different disciplines. Supplier risk management is procurement-led and supplier-specific; disruption monitoring is event-driven and network-wide. Most vendors lead in one and partner or extend into the other.

The category just got its first Magic Quadrant. Gartner published the inaugural Magic Quadrant for Supplier Risk Management Solutions in April 2025, naming four Leaders: Everstream, Exiger, Prewave, and Resilinc. It graduated from a prior Market Guide.

The market spread is one of the widest in this series. Estimates run from roughly $1.3B for narrow risk software to nearly $20B for the broadest supply-chain-plus-services definition, a roughly 15x spread, so always check the definition.

Disruption is rising and regulation is tightening. Disruptions rose sharply in 2024, with factory fires the leading cause for a sixth straight year, while tariffs and forced-labor and sustainability rules are pulling demand upward.

Acting on the signal, not the dashboard, drives ROI. Value comes from avoiding or responding faster to disruptions and meeting compliance obligations; the headline figures are vendor-sourced and should be tested against your own exposure.

2. What supply chain risk software is

Supply chain risk software gives an organization visibility into the risks in its supplier base and network, monitors those risks continuously, and alerts the business when something threatens supply. Getting the category straight starts with the distinction between supplier risk and disruption monitoring. The core capabilities are:

- **Multi-tier supplier mapping.** Discovering and mapping not just direct suppliers but the sub-tiers beneath them, where hidden dependencies and single points of failure often sit.
- **Risk monitoring across domains.** Continuously tracking financial, operational, geopolitical, cyber, environmental, and sustainability risk against suppliers and locations.
- **Disruption detection and alerting.** Scanning news, events, weather, and other signals to detect disruptions early and alert the affected parts of the business.
- **Supplier financial health.** Assessing the financial stability of suppliers to anticipate distress and failure.
- **Compliance and ESG risk.** Screening suppliers for forced labor, sanctions, and sustainability exposure against tightening regulation.
- **Resilience and response.** Quantifying exposure and supporting the response when a disruption hits, from alternate sourcing to business continuity.

Supplier risk versus disruption monitoring

The most important distinction in the category is between supplier risk management and disruption monitoring. Supplier risk management is procurement-led and supplier-specific: it assesses and monitors the risk of individual suppliers, including financial health, compliance, and performance, and lives close to the sourcing process. Disruption monitoring is event-driven and network-wide: it watches the whole network for events, fires, floods, geopolitical shocks, that threaten supply, and maps the exposure across tiers. Some vendors do both, but most lead in one. Knowing which problem you are solving is the first step to choosing well, and it is a distinction this guide returns to throughout.

Discipline	Primary lens	Typical owner
Supplier risk management	Risk of individual suppliers	Procurement
Disruption monitoring	Network-wide events and exposure	Supply chain
Financial-health risk	Supplier solvency and distress	Procurement / finance
ESG and compliance risk	Forced labor, sanctions, sustainability	Compliance
Supplier information	Onboarding and master data	Procurement

Supply chain risk software is adjacent to procurement and source-to-pay, which Supply Chain Research covers separately, and to supply chain visibility and control towers, also covered separately. Risk is increasingly embedded in procurement suites, but the specialist platforms go far deeper on monitoring and n-tier mapping.

3. The risk software market in 2026

Supply chain risk is one of the most loosely defined markets in this series, and the published numbers reflect it, spanning more than tenfold. The spread comes from whether a figure counts dedicated risk software narrowly or the entire supply-chain-risk stack including services broadly. Treat the figures below as directional and always check the definition.

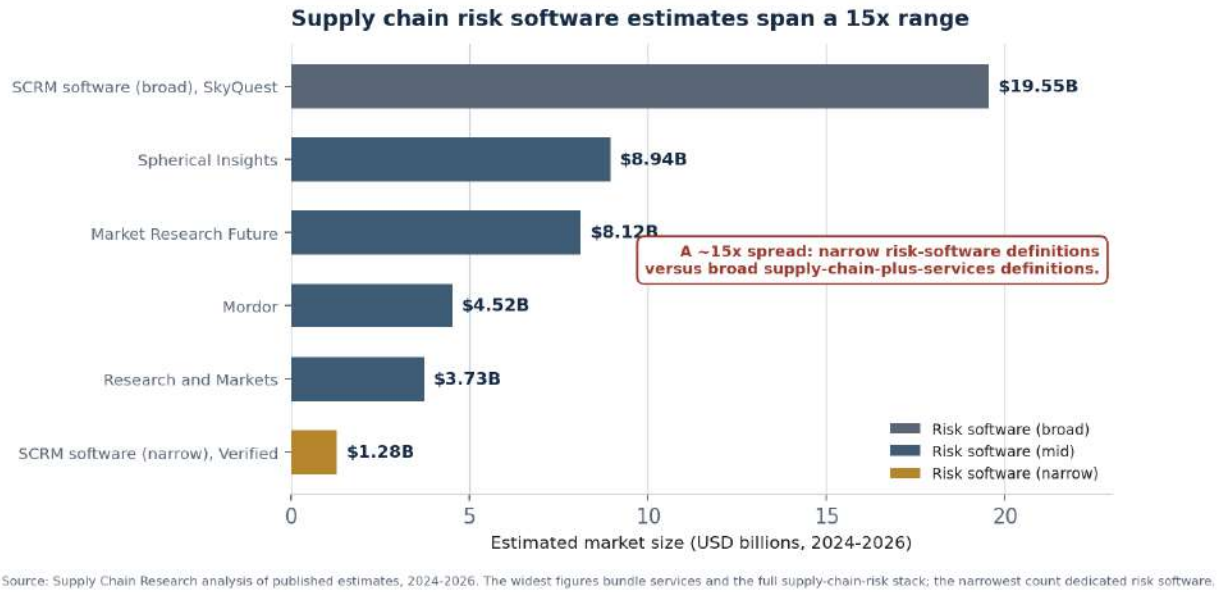

Figure 1. Published 2024-2026 estimates by definition. The roughly 15x spread reflects narrow risk-software definitions against broad supply-chain-plus-services ones.

Source and definition	Size	Forecast	CAGR
SkyQuest (broad)	$19.55B (2024)	$20.91B / 2032	10.4%
Spherical Insights	$8.94B (2025)	$62.74B / 2035	21.51%
Market Research Future	$8.12B (2025)	$56.06B / 2035	21.31%
Mordor Intelligence	$4.52B (2025)	$9.22B / 2030	15.31%
Research and Markets	$3.73B (2026)	$5.03B / 2030	7.8%
Verified Market Research (narrow)	$1.28B (2024)	$2.98B / 2031	12.29%

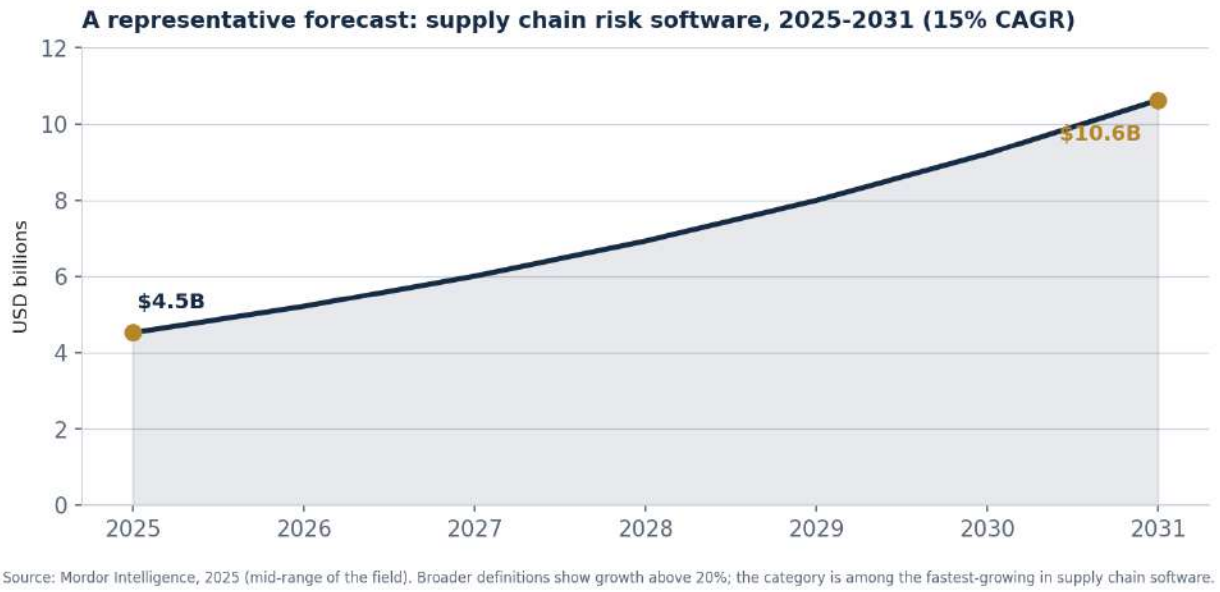

Figure 2. A representative trajectory for supply chain risk software at about 15 percent CAGR (Mordor Intelligence).

Why the estimates diverge

The spread is a definition problem. The narrowest figures count only dedicated risk software; the broadest count the entire supply-chain-risk stack, including services, consulting, and adjacent categories. Growth is rapid by any definition, in the mid-teens to low twenties, making this one of the faster-growing areas in supply chain software. Cloud deployment dominates at roughly 71 percent, and North America leads, with significant public-sector demand. For planning, the mid-range figures, roughly $4B to $5B in 2025, are the most consistent baseline for a dedicated risk-software purchase.

The disruption surge driving demand

Demand is anchored in a measurable rise in disruption. According to Resilinc, global supply chain disruptions rose 38 percent in 2024, against just 5 percent growth in 2023, with factory fires the leading cause for a sixth consecutive year, labor disruptions up 47 percent, and cyberattacks on supply chains up roughly a third (figures vendor-reported, drawn from Resilinc's monitoring of millions of sources). Layered on top are the tariff and trade-war volatility of 2025 and tightening forced-labor and sustainability regulation. Those forces explain why risk has moved from a periodic assessment to a continuous, board-level concern.

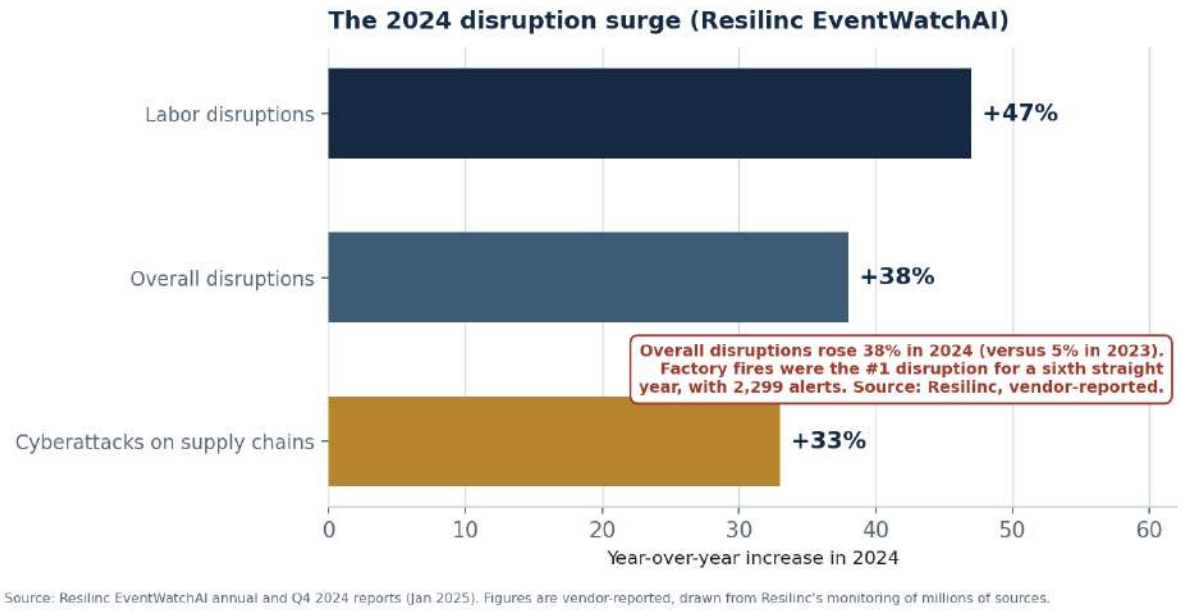

Figure 3. The 2024 disruption surge (Resilinc EventWatchAI). Figures are vendor-reported; factory fires were the leading disruption for a sixth straight year.

4. The vendor landscape

The risk market is crowded and newly mapped by analysts. We group vendors into four tiers by what they do best, not by size. No vendor leads every tier, and the supplier-risk and disruption-monitoring worlds, though converging, remain distinct.

What the analysts say

This is a category whose analyst coverage changed materially in 2025, when supplier risk received its first dedicated Magic Quadrant. The essentials:

- **The first-ever Magic Quadrant for Supplier Risk Management Solutions.** Published by Gartner in April 2025, it evaluated nine vendors and named four Leaders: Everstream, Exiger, Prewave, and Resilinc. It graduated from a prior Gartner Market Guide.
- **A procurement-context quadrant, distinct from other risk research.** This is a supplier-risk quadrant, separate from Gartner's Market Guide for third-party risk management technology and from broader supply-chain-risk research. There is no separate supply-chain-risk Magic Quadrant.
- **Several prominent vendors were not in the inaugural quadrant.** Names such as Craft, Avetta, and Sayari are significant in the market but were not among the nine vendors Gartner evaluated, so the quadrant is not a complete map of the category.

Figure 4. Supply Chain Research's directional map, structured after the first-ever Supplier Risk Magic Quadrant; these positions are our interpretation, not analyst coordinates.

N-tier mapping and disruption monitoring

These vendors lead on network-wide disruption and sub-tier visibility, and several are the new quadrant's Leaders. Everstream Analytics is a predictive risk-analytics Leader. Resilinc, established in 2010, runs the EventWatchAI monitoring engine across millions of sources and deep sub-tier mapping, though Gartner has flagged slower-than-expected progress on agentic AI. Interos provides automated multi-tier risk scoring, has reached unicorn valuation with a strong federal footprint, and has been noted by Gartner for longer support-resolution times. Prewave, the quadrant's only European Leader, covers many languages and is strong in Europe, with a lower average deal size. Sayari and Exiger, the latter strong in defense and government with an agentic roadmap, round out the tier. Strengths: real-time, network-wide monitoring and n-tier mapping. Limitations: data and mapping effort, and varying maturity on the newest AI.

Financial-health and ESG risk

Two specialist tiers address specific risk domains. Financial-health providers, RapidRatings, Dun and Bradstreet, Moody's, Craft, and apexanalytix, assess supplier solvency and distress, the risk most directly tied to procurement and finance. ESG and compliance providers, EcoVadis, IntegrityNext, Sphera, Assent, and Avetta, screen suppliers for forced labor, sanctions, and sustainability against tightening regulation. Sphera, which acquired the risk specialist riskmethods, brings a broad environmental and risk portfolio, though Gartner has noted lower customer interest in its supplier-risk solution specifically. Strengths: depth in their domain. Limitations: narrower than the network-wide monitors.

Procurement-embedded risk

Finally, the procurement suites, Coupa, SAP Ariba, Ivalua, and Jaggaer, embed supplier risk into the broader source-to-pay process. This suits organizations that want risk inside procurement rather than in a separate platform, accepting less depth than the specialists in exchange for one system and one supplier record.

Vendor summary

Vendor	Tier	Best fit	Notes
Everstream / Resilinc	N-tier monitoring	Network-wide disruption	Both 2025 MQ Leaders
Interos	N-tier monitoring	Automated multi-tier scoring	Unicorn; strong federal footprint
Prewave	N-tier monitoring	European coverage	Only European MQ Leader
Exiger	N-tier monitoring	Defense and government	MQ Leader; agentic roadmap
RapidRatings / D&B	Financial health	Supplier solvency	Distress and failure risk
EcoVadis / IntegrityNext	ESG and compliance	Sustainability and forced labor	Regulatory-driven screening
Sphera	ESG and risk	Environmental and risk	Acquired riskmethods
Coupa / SAP Ariba / Ivalua	Procurement-embedded	Risk inside source-to-pay	One system, less depth

Positions and notes are Supply Chain Research's interpretation from public information and the first-ever Supplier Risk Magic Quadrant, current to mid-2026. Several significant vendors were not in that quadrant. Ownership and scope change quickly; verify current details directly with each vendor.

5. How to evaluate a risk platform

The right platform depends first on which problem you are solving, supplier-specific risk or network-wide disruption, and then on data, coverage, and your ability to act. We use five dimensions.

The five evaluation dimensions

1. **Risk-domain fit.** Is your priority supplier-specific risk, network-wide disruption, financial health, or ESG and compliance? Match the platform's core strength to it rather than buying a generalist for a specialist need.
2. **Coverage and data quality.** How deep is the supplier and sub-tier coverage, how many sources and languages does it monitor, and how accurate and timely are its data and alerts?
3. **N-tier mapping.** Can it map beyond direct suppliers to the sub-tiers where hidden risk concentrates, and how much effort does that mapping require from you?
4. **Integration and workflow.** How cleanly does it connect to your procurement and supplier systems, and does it turn alerts into action rather than just dashboards?
5. **Regulatory fit and viability.** Does it cover the forced-labor, sanctions, and sustainability rules you face, and is the vendor stable in a fast-consolidating market?

Making the decision

Map your need before you shortlist. If the priority is network-wide disruption and sub-tier exposure, start with the n-tier monitors such as Everstream, Resilinc, Interos, Prewave, and Exiger. If it is supplier solvency, start with the financial-health providers. If it is forced labor and sustainability compliance, start with the ESG specialists. And if you want risk inside procurement, the suite-embedded options may suffice. Then run a proof of value on your own supplier base.

A selection process that works

6. Define which risk problem you are solving and the suppliers and tiers in scope.
7. Match that to a tier, and shortlist within it rather than across all four.
8. Run a proof of value on your own supplier base, testing coverage, alert accuracy, and sub-tier mapping.
9. Test integration with your procurement and supplier systems, and confirm alerts drive workflow.
10. Confirm regulatory coverage and weigh vendor viability as the market consolidates.

6. Cost and pricing

Risk-software pricing scales with the number of suppliers monitored, the depth of monitoring, and the modules selected. The models you will encounter:

Pricing model	Typical basis	Notes
Subscription	Annual platform fee	Tiered by scope and modules
By supplier count	Usage-based	Scales with suppliers monitored
By tier of monitoring	Depth-based	Deeper sub-tier mapping costs more
Module-based	Per capability	Financial, ESG, and disruption priced apart
Implementation	Project fee	Supplier data, mapping, integration

What drives the number

The number of suppliers monitored, the depth of sub-tier mapping, and the range of risk domains covered are the main cost drivers. The largest hidden effort is supplier data and n-tier mapping: building an accurate picture of who supplies your suppliers takes work, and platforms vary in how much of that they automate. Procurement-embedded risk can be the least expensive route if you already own the suite, while the specialist monitors are priced on the breadth and depth of coverage. Model the full cost, including the mapping effort, not the subscription alone.

Risk-platform pricing is typically gated behind a sales process, so published figures should be treated as starting points. Build a proof of value and a reference check into the buying process to validate both cost and the disruption-avoidance and compliance benefits the vendor projects.

7. Implementation: where programs succeed or fail

Risk programs fail in predictable ways, and almost none of the failure modes are about the monitoring engine. They are about data, integration, and acting on the signal. The recurring causes:

- **Incomplete supplier data.** Without an accurate supplier and sub-tier map, the platform monitors the wrong things or misses the dependencies that matter most.
- **Alert fatigue.** A flood of undifferentiated alerts trains the business to ignore them; risk scoring and prioritization are what make monitoring usable.
- **No response process.** Detecting a disruption is worthless if there is no defined process to act on it; the value is in the response, not the alert.
- **Treating risk as a procurement silo.** Risk that does not connect to sourcing, planning, and business continuity stays an interesting dashboard rather than a decision tool.

Three principles that separate success from failure

Invest in the supplier map. Build an accurate supplier and sub-tier picture first, because monitoring is only as good as the network it watches.

Prioritize, do not just alert. Use risk scoring to surface what matters and suppress the noise, so the business trusts and acts on the signal.

Define the response. Decide in advance who acts on an alert and how, and connect risk to sourcing and continuity, because the response is where the return lives.

A phased rollout

Sequence the program to retire risk early. Begin by mapping your most critical suppliers and the tiers beneath them, and stand up monitoring on that core. Add risk scoring and a defined response process so alerts drive action, and integrate with procurement and planning. Then extend coverage across the supplier base and into deeper sub-tiers and new risk domains. Treating these as sequential stages, rather than a single switch, is what separates a smooth rollout from a stalled one.

8. Trends shaping 2026

AI for risk detection and n-tier mapping

The clearest shift is AI used to detect risk earlier and to map sub-tier supplier relationships automatically, work that was once slow and manual. Machine learning across vast numbers of sources is what lets the leading platforms watch the whole network in near real time.

The tariff and trade-war surge

The tariff volatility of 2025 has pushed supply chain risk up the executive agenda as companies scramble to understand their exposure to shifting trade policy. Tariffs and trade restrictions have become a first-order risk domain, and a major driver of new demand for these platforms.

Forced labor and sustainability regulation

Tightening regulation, forced-labor enforcement and corporate sustainability due-diligence rules, is making supplier compliance a legal as well as a reputational matter. This is pulling ESG and compliance risk from a voluntary exercise toward a mandatory one, and expanding the role of the screening specialists.

Generative and agentic AI for risk intelligence

Generative AI is being applied to summarize and explain risk, and the frontier is agentic AI that can investigate alerts and trigger workflows with less human effort. Exiger and others are moving in this direction, though maturity varies, and buyers should weigh demonstrated capability over roadmap promises.

Real-time, multi-tier visibility

The strongest structural trend is the move toward continuous, real-time visibility across multiple supplier tiers, rather than periodic assessment of direct suppliers. As that capability matures, risk monitoring is converging with broader supply chain visibility, and today's risk purchase should be weighed for how well it fits that wider picture.

9. Segment-specific guidance

The right approach depends on your industry and exposure. The table summarizes where each segment usually starts; the prose adds the nuance.

Segment	What matters most	Where to start
Complex global manufacturer	N-tier disruption exposure	Everstream, Resilinc, Interos
Defense and government	Sub-tier and integrity risk	Exiger, Interos
Regulated / ESG-exposed	Forced labor, sustainability	EcoVadis, IntegrityNext, Assent
Finance-sensitive supply base	Supplier solvency	RapidRatings, D&B, Moody's
Procurement-led organization	Risk inside source-to-pay	Coupa, SAP Ariba, Ivalua

Complex global manufacturers with deep, multi-tier supply chains reward the n-tier disruption monitors. **Defense and government organizations** need sub-tier and integrity risk, the strength of Exiger and Interos. **Regulated and ESG-exposed companies** need forced-labor and sustainability screening from the compliance specialists. **Companies with finance-sensitive supply bases** need supplier solvency monitoring, and **procurement-led organizations** may reward risk embedded in their source-to-pay suite. The unifying rule is to match the platform to the risk domain that matters most, not to buy a generalist for a specialist need.

10. ROI and the business case

The business case for risk software is straightforward in structure and easy to overstate in practice. The levers are disruption avoidance, faster response, reduced revenue-at-risk, and compliance. The discipline is refusing to bank the vendor's headline figure before you have tested it against your own exposure, and remembering that the value lands only when the business acts on the signal.

Avoidance	Response	Compliance
early warning lets the business act before a disruption bites	faster, better-informed response reduces the cost of disruptions that do hit	screening avoids penalties and protects the brand under tightening rules

Where the value comes from

Most of the return is in a few places. Disruption avoidance is the headline lever: early warning of a supplier failure, a factory fire, or a geopolitical shock lets the business secure alternate supply before the disruption bites. Faster response reduces the cost of the disruptions that do occur, with one vendor citing a customer that cut risk-response times by three days (a vendor-stated figure). Reduced revenue-at-risk follows from seeing and mitigating exposure across tiers, and compliance screening avoids penalties and brand damage under tightening forced-labor and sustainability rules. The crucial caveat is that all of this value is contingent on acting on the signal; a platform that produces alerts no one responds to returns nothing. Build the case on your own exposure and response capability, and use vendor figures only to size the opportunity.

11. Frequently asked questions

What is supply chain risk management software?

Software that gives visibility into the risks in a supplier base and network, monitors them continuously, and alerts the business to threats. It spans multi-tier supplier mapping, financial, operational, geopolitical, cyber, and ESG risk, disruption detection, and supplier financial health.

What is the difference between supplier risk and disruption monitoring?

Supplier risk management is procurement-led and supplier-specific, assessing the risk of individual suppliers. Disruption monitoring is event-driven and network-wide, watching the whole network for events that threaten supply and mapping exposure across tiers. Some vendors do both, but most lead in one.

Is there a Gartner Magic Quadrant for this category?

Gartner published its first-ever Magic Quadrant for Supplier Risk Management Solutions in April 2025, naming Everstream, Exiger, Prewave, and Resilinc as Leaders. It is a procurement-context quadrant, distinct from third-party-risk research, and several significant vendors were not in it. There is no separate supply-chain-risk Magic Quadrant.

Who are the leading vendors?

It depends on the tier. N-tier disruption monitors include Everstream, Resilinc, Interos, Prewave, and Exiger; financial-health providers include RapidRatings, Dun and Bradstreet, and Moody's; ESG and compliance specialists include EcoVadis and IntegrityNext; and the procurement suites embed risk into source-to-pay.

How big is the market?

It depends on the definition, ranging from roughly $1.3B for narrow risk software to nearly $20B for the broadest supply-chain-plus-services definition, a roughly 15x spread. The mid-range figures of about $4B to $5B in 2025 are the most consistent baseline for a dedicated purchase.

What is n-tier supplier mapping?

Mapping not just your direct suppliers but the suppliers beneath them, the sub-tiers, where hidden dependencies and single points of failure often sit. It is one of the hardest and most valuable capabilities, and platforms vary widely in how much of the mapping they automate.

What is driving demand right now?

A measurable rise in disruptions, the tariff and trade-war volatility of 2025, and tightening forced-labor and sustainability regulation. Together these have moved risk from a periodic assessment to a continuous, board-level concern.

What does it cost?

Pricing scales with the number of suppliers monitored, the depth of sub-tier mapping, and the risk domains covered. The largest hidden effort is building an accurate supplier and sub-tier map; procurement-embedded risk can be the least expensive route if you already own the suite.

How is AI changing risk software?

AI is detecting risk earlier and automating sub-tier mapping, generative AI is summarizing and explaining risk, and agentic AI is beginning to investigate alerts and trigger workflows. Maturity varies, so demonstrated capability should be weighed over roadmap promises.

What is the most common reason these programs fail?

Incomplete supplier data, alert fatigue, and the absence of a defined response process. Almost none of the common failures are about the monitoring engine. The value is in acting on the signal, so the supplier map and the response process matter most.

12. Recommendations

A practical path for buyers, drawn from the analysis above:

11. **Decide which risk problem you are solving.** Separate supplier-specific risk from network-wide disruption, because they call for different platforms and the distinction shapes the whole decision.
12. **Use the first-ever Supplier Risk Magic Quadrant, with its limits.** Lean on the April 2025 quadrant and its four Leaders, Everstream, Exiger, Prewave, and Resilinc, but remember several significant vendors were not evaluated.
13. **Match the tier to the risk domain.** N-tier monitors for network disruption, financial-health providers for solvency, ESG specialists for compliance, procurement suites for risk inside source-to-pay.
14. **Invest in the supplier map first.** Build an accurate supplier and sub-tier picture, because monitoring is only as good as the network it watches.
15. **Design the response, not just the alerts.** Define who acts on an alert and how, and connect risk to sourcing and continuity, because the response is where the value is realized.
16. **Treat vendor ROI claims as a ceiling.** Run a proof of value on your own supplier base, and prove disruption-avoidance and compliance benefits before scaling.

13. Methodology and caveats

- This guide synthesizes public market-research estimates, the first-ever Gartner Magic Quadrant for Supplier Risk Management Solutions, vendor disclosures, and trade reporting, current to mid-2026. Supply Chain Research is independent and accepts no payment from the vendors covered.
- Market-size figures diverge by roughly fifteen times by definition, from about $1.3B for narrow risk software to nearly $20B for the broadest supply-chain-plus-services definition. We present a range and separate the definitions rather than asserting a single number.
- The April 2025 Supplier Risk Magic Quadrant is a procurement-context quadrant evaluating nine vendors; it is distinct from third-party-risk research, and several significant vendors, including Craft, Avetta, and Sayari, were not in it. The map in Figure 4 is our directional interpretation, not analyst coordinates.
- The disruption figures in Figure 3 are vendor-reported by Resilinc, drawn from its monitoring of millions of sources. Response, avoidance, and compliance ROI figures are vendor-stated and treated as a ceiling, and depend on the business acting on the signal.
- Vendor ownership, valuations, and scope change quickly, including Sphera's acquisition of riskmethods and Interos's unicorn valuation. Validate current details directly with vendors before any purchasing decision.

14. Sources

[1] Everstream Analytics (2025). Named a Leader in the first-ever Gartner Magic Quadrant for Supplier Risk Management Solutions.

[2] Exiger (2025). A Leader in the first-ever Gartner Magic Quadrant for Supplier Risk Management Solutions.

[3] Prewave (2025). Recognized in the Gartner Magic Quadrant for Supplier Risk Management Solutions.

[4] Resilinc / GlobeNewswire (Jan 2025). EventWatchAI annual report: 2024 supply chain disruptions.

[5] Mordor Intelligence (2025). Supply Chain Risk Management Market. $4.52B (2025), 15.31% CAGR.

[6] Market Research Future (2025). Supply Chain Risk Management Software Market.

[7] SkyQuest (2024). Supply Chain Risk Management Software Market. Broad definition $19.55B (2024).

[8] Research and Markets (2026). Supply Chain Risk Management Market Report.

[9] Verified Market Research (2024). Supply Chain Risk Management Software Market. Narrow definition $1.28B (2024).

[10] CB Insights (2025). riskmethods (acquired by Sphera) company and funding profile.

Additional figures drawn from: Spherical Insights (market sizing); Gartner Critical Capabilities for Supplier Risk Management Solutions and the 2026 edition (analyst perspective); Tradeverifyd and DevOpsSchool (vendor comparisons); and vendor and trade reporting on Interos, Exiger, and Overhaul funding. Disruption, response, and ROI claims are vendor-stated unless otherwise noted, and the April 2025 Magic Quadrant did not evaluate every significant vendor.

Supply Chain Research is an independent, vendor-neutral research platform for supply chain and IT leaders. We accept no payment from the vendors covered. Figures should be validated against your own requirements before any purchasing decision.