RISK LEDGER

Every Link Matters:
The State of Supply Chain Security 2026 - US Edition

A Risk Ledger Data Insights Report

About this report

This report, "Every Link Matters: The State of Supply Chain Security 2026 - US Edition" provides a comprehensive analysis of supply chain security risks in the US, based on data collected from over 1000 cyber security and risk management professionals in the US, open source data from authoritative sources and governmental agencies, and proprietary risk intelligence.

About Risk Ledger

Risk Ledger was founded in 2018 by Haydn Brooks and Daniel Saul with a mission to shift the way organisations approach cyber security and risk management in the supply chain by building a global network of connected organisations.

Today, Risk Ledger is the cutting-edge Third Party Risk Management (TPRM) platform, dedicated to transforming supply chain security. We empower security and procurement teams to Defend-as-One, visualising their entire supply chain in real-time and providing unmatched transparency and collaboration. Our platform offers comprehensive, continuously updated risk assessments that reduce compliance burdens and enhance your organisation's cyber defences. By visualising and managing every link in your supply chain, Risk Ledger ensures you are always one step ahead of emerging threats.

Our commitment to asking the right questions and working closely with industry experts allows us to build a more secure, resilient future for all. With our Defend-as-One approach, we strengthen your organisation's ability to detect, respond to, and prevent cyber attacks. Risk Ledger isn't just about managing risk—it's about fortifying your entire supply chain because every link matters in cyber security. We're here to help you secure today's operations and safeguard tomorrow's reputation, creating a safer digital landscape for all.

Risk Ledger Ltd.
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com | marketing@riskledger.com | +44 1234 567890

Contents

Executive Summary

Supply chain security in the United States is at a pivotal moment, as evidenced by recent breaches that have exposed vulnerabilities in vendor networks. Incidents such as the SolarWinds compromise have demonstrated how weaknesses within extended supply chains can have sweeping effects. The "Every Link Matters" report draws on insights from 1000 US CISOs and risk leaders to distill the key trends and challenges reshaping Third-Party Risk Management (TPRM) today.

Organizations now recognize supply chains as core attack surfaces, driving TPRM up to board-level priority. In our survey, 42% report TPRM is a key focus for executive leadership, and a majority view supply chain risk as a top security—not just compliance—concern.

Yet, there remains a critical gap between recognition and capability. While 96% of CISOs know extended visibility is essential, over half lack the ability to monitor beyond their direct third parties.

Myth:
More questionnaire assessments lead to better risk management.

Reality:
Traditional approaches don't scale against exponential risk.

The fourth-party blind spot leaves organizations vulnerable to threats hidden deeper in the supply chain—risks static TPRM processes cannot address.

The 4th-Party Blind Spot: Risks Beyond Direct Oversight

The "fourth-party blind spot" is a tangible threat across all sectors. In financial services, unmonitored downstream processors have enabled data breaches beyond direct vendor controls. Healthcare and insurance organizations face similar exposures as attackers exploit indirect suppliers, impacting patient care and regulatory compliance.

Traditional TPRM falls short in illuminating these indirect dependencies. As a result, organizations are left with dangerous "unknown unknowns"—risks invisible until exploited.

Given the scale and intricacy of modern supply chains, organizations must move beyond periodic assessments and manual questionnaires. Sustainable risk management now demands a systematic, real-time approach that closes these persistent visibility gaps.

From Static Compliance to Active Supply Chain Security

Evolving from compliance-driven to Active Supply Chain Security requires structured implementation and organizational alignment.

Framework for Transitioning to Active Supply Chain Security:

- **Map Extended Relationships:** Identify direct and deeper-tier suppliers using contracts, attestations, and supply chain mapping tools. Embed ongoing mapping in governance.
- **Implement Continuous Monitoring:** Replace periodic reviews with real-time monitoring and automated threat intelligence. This shift enables prompt detection and response.
- **Foster Cross-Functional Alignment:** Unite security, procurement, legal, and compliance teams around supply chain risk objectives, ensuring shared accountability.
- **Automate Risk Detection and Response:** Deploy platforms for real-time alerts and automated workflow to accelerate remediation and reduce manual effort.
- **Measure and Communicate Outcomes:** Track metrics such as supplier coverage and incident response times. Report measurable improvements to leadership and the board.

Systematic mapping, monitoring, and rapid response transform TPRM into an adaptive, intelligence-led discipline.

CISO Priorities for Next-Generation TPRM

Our research reveals US CISOs are seeking TPRM solutions that provide:

- **Multi-Tier Visibility:** Transparent mapping and risk ranking of both direct and indirect supplier networks.
- **Automation:** Automated evidence collection, continuous scoring, and reminders for increased coverage with lean teams.
- **Integrated Compliance:** Platforms that align controls with multiple regulations (e.g., SEC, HIPAA, GLBA) and streamline audit readiness.
- **Real-Time Intelligence:** Actionable insights integrating live threat feeds and vulnerability databases, not just static reports.
- **User-Centric Reporting:** Intuitive dashboards and board-ready reporting to clearly communicate posture and demonstrate ROI.
- **Collaborative Features:** Tools fostering secure coordination and shared response during supplier-related incidents.

CISOs now view TPRM as a strategic function—seeking solutions that empower them to demonstrate competence, validate resilience, and achieve operational consistency.

Every link in your supply chain matters—unseen weaknesses can dictate your overall risk profile. Mapping and continuously monitoring those connections, even beyond direct partners, is essential. By benchmarking against industry peers and leveraging the insights in this report, organizations can identify capability gaps and focus on strategic investments.

Modern supply chain security hinges on continuous monitoring and automation. The adoption of advanced tools and frameworks not only enables teams to act on emerging risks but also provides concrete evidence of security improvements to leadership and regulators. Use this report as a roadmap for future-ready supply chain resilience: Active Supply Chain Security is a crucial, strategic advantage for anticipating threats, ensuring compliance, and strengthening your organization's reputation.

Supply Chain Risk in the US: Why Now?

In the United States, supply chain security has rapidly become a strategic, board-level imperative—driven by escalating geopolitical tensions, high-profile breaches, and tightening regulations. While internal defenses have improved, third-party dependencies now represent the most dynamic area of risk exposure. Attackers are targeting these extended webs of suppliers, exploiting trusted connections to penetrate otherwise secure environments.

Recent data highlights the shift: 42.1% of organizations now consider Third-Party Risk Management (TPRM) a critical board-level priority, and over half of CISOs (51.4%) identify limited visibility beyond immediate suppliers as a primary risk. This "fourth-party blind spot"—lack of insight into deeper supply chain tiers—remains a widespread vulnerability, impacting both operational resilience and compliance.

As security leaders seek actionable ways forward, it is crucial to recognize the consequences of insufficient visibility. Without it, organizations face:

- **Regulatory Risk:** Potential penalties and enforcement actions for lack of oversight.
- **Operational Disruption:** Incidents deep in the supply chain can halt critical operations.
- **Reputational Damage:** Breaches involving sensitive supply chain partners quickly erode market and stakeholder trust.
- **Delayed Response:** Slow detection and unclear accountability hinder timely incident mitigation.

Evolving Threat and Regulatory Drivers

Federal agencies and regulators have responded decisively. Initiatives from CISA and new SEC rules have established clearer accountability, while incidents like SolarWinds and MOVEit proved a single supplier breach can cascade across thousands of organizations and agencies. Compliance frameworks alone are no longer sufficient: legacy checklists and annual assessments are ill-suited to today's rapidly shifting risk landscape.

Myth vs. Reality

Myth: More assessments equal better risk management.

Reality: Assessment volume cannot match the exponential complexity and speed of modern supply chain threats.

The path forward hinges on three principles:

- **Visibility:** Achieve insight across all supply chain tiers—not just direct vendors.
- **Proactivity:** Move from periodic assessment to continuous monitoring and intelligence-led defense.
- **Alignment:** Ensure security priorities are shared at board, operational, and ecosystem levels.

Transitioning from Compliance to Active Supply Chain Security

Modernizing supply chain security demands a risk-driven, automated approach. Moving beyond annual assessments, leading organizations are adopting real-time monitoring and data-driven response. AI-powered platforms now support automated alerting and shorten incident response times—delivering measurable improvements in resilience.

Operational and Governance Framework

A focused, stepwise framework for building resilience includes:

1. **Map the Ecosystem:** Catalog all third, fourth, and nth party supplier relationships using automated discovery where available.
2. **Implement Continuous Monitoring:** Adopt tools for real-time oversight of vendor status, risk indicators, and cybersecurity posture.
3. **Prioritize Critical Suppliers:** Identify and escalate due diligence and response plans for relationships supporting key operations or handling sensitive data.
4. **Integrate Threat Intelligence:** Augment risk profiles with external data to enable anticipatory mitigation.
5. **Automate Assessments:** Streamline data collection, scoring, and remediation workflows to optimize team capacity.
6. **Strengthen Collaboration:** Align internal teams and work actively with key suppliers and industry peers to standardize security expectations and response.

Collaboration and Peer Networks

Effectively managing systemic supply chain risk requires shared responsibility across the ecosystem. Key actions include:

- **Engagement:** Join ISACs and sector forums to exchange timely intelligence and practices.
- **Supplier Partnership:** Establish transparency and set clear expectations for downstream risk management.
- **Industry Standards:** Advocate for and adhere to common frameworks that drive coherence and elevate sector resilience.

Collective action is essential—no organization can address complex supply chain threats in isolation. Sustained collaboration and proactive alignment are what will define resilient enterprises and sectors.

Empowering your team with actionable intelligence and direct engagement will strengthen both your individual and sector-wide security posture. Leverage peer networks and data-driven solutions now to secure every link in your supply chain and drive lasting resilience.

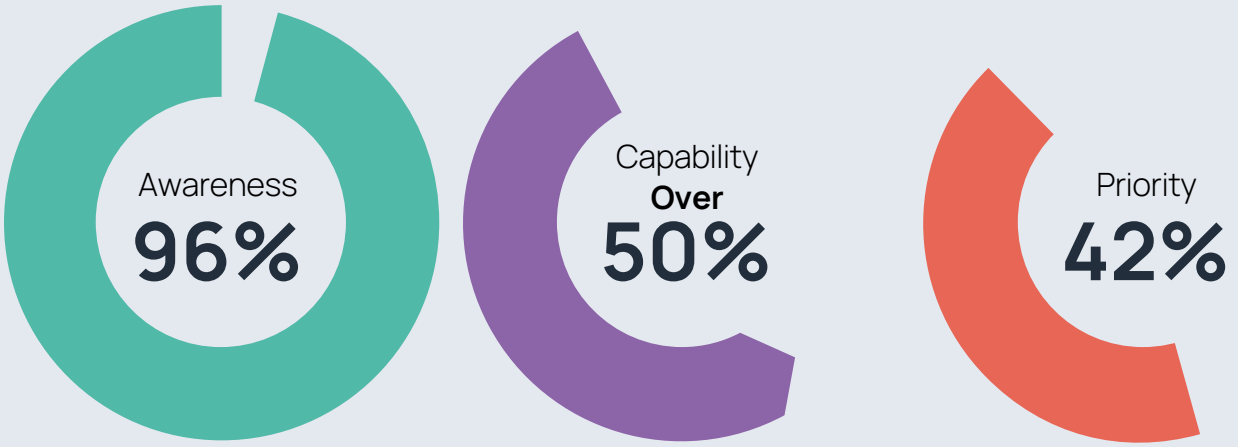
Is TPRM Fit for Purpose in 2025?

As supply chain threats intensify in scope and sophistication, traditional Third-Party Risk Management (TPRM) is under unprecedented pressure to evolve. Today's TPRM programs, while foundational, are being outpaced by regulatory demands, escalating boardroom expectations, and the sheer scale of supplier ecosystems.

Inescapable Drivers: What's Forcing Change

- **Geopolitical and Cyber Risk:** High-profile incidents like SolarWinds and Kaseya have demonstrated the ripple effect of attacks originating from a single supplier, impacting entire sectors and critical infrastructure.
- **Regulatory Escalation:** Rules from bodies such as the SEC, GLBA, and sector-specific agencies now require organizations to evidence security controls across all tiers of their supply chain, not just the immediate vendors.
- **Market Demands:** Boards and clients increasingly expect real-time visibility and continuous monitoring, making annual or periodic assessments insufficient.

The TPRM Visibility Gap



of CISOs know extended visibility is essential.

lack the ability to monitor beyond direct third parties.

report TPRM is a key focus for executive leadership.

Where Traditional TPRM Falls Short

The combination of more demanding oversight and increasingly complex supply chains are exposing the limitations of legacy TPRM models. Manual workflows, focused only on direct suppliers, are inadequate for today's distributed threat landscape. High-profile incidents like MOVEit reinforce the urgency for change.

Key challenges with traditional approaches include:

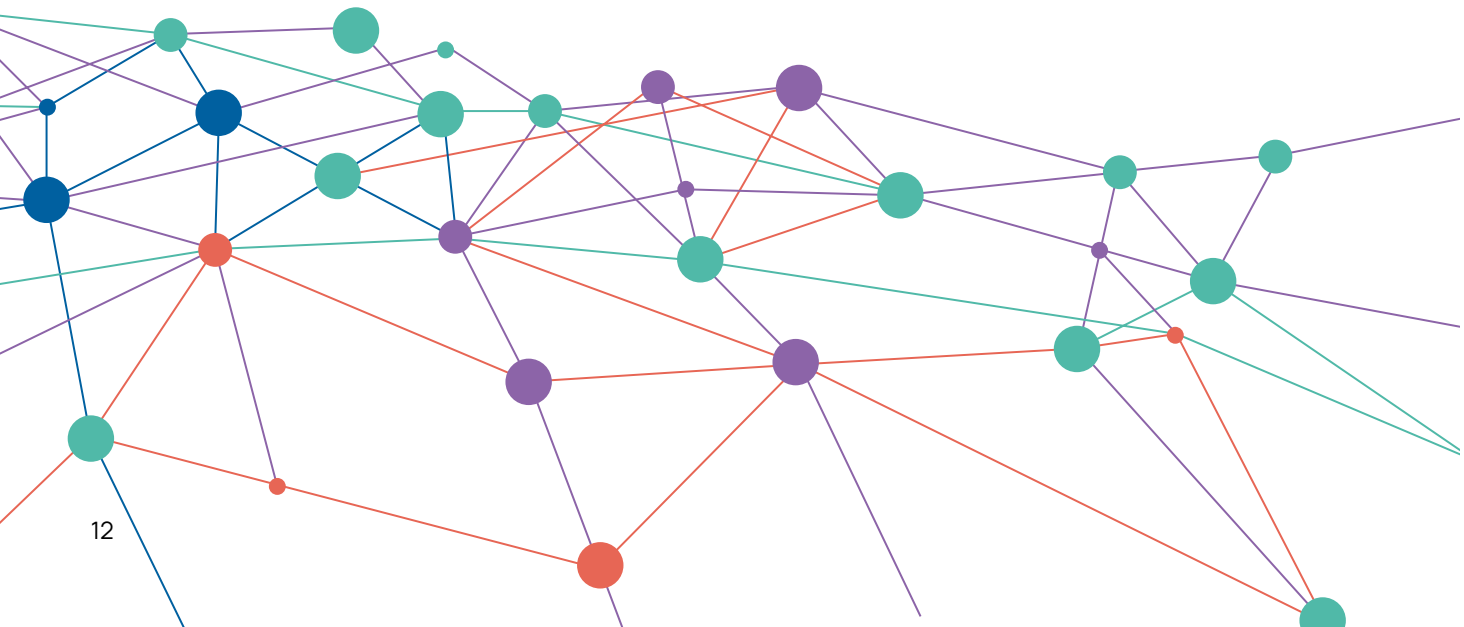
- **Limited Visibility:** Over **51%** of organizations lack insight beyond tier-one suppliers, leaving downstream risks undetected.
- **Manual, Siloed Workflows:** Spreadsheet-based processes delay detection and are difficult to scale.
- **Static Point-in-Time Assessments:** Infrequent reviews fail to capture ongoing changes in the threat landscape.

Survey data validates this: **41%** of US security leaders cite automation as the top TPRM improvement needed.

Modernizing TPRM: Technology as a Catalyst

The next generation of TPRM leverages technology to replace static processes with real-time, intelligence-driven risk management:

- **AI-Driven Analytics:** Automates assessment and monitoring, providing predictive insights and early alerts for emerging vendor risks.
- **Continuous Monitoring:** Enables adaptive workflows and integration with incident response, ensuring prompt detection of changes in supplier posture.
- **Collaborative Platforms:** Centralize data exchange and benchmarking, enhancing transparency and speeding up remediation across the entire supply chain.

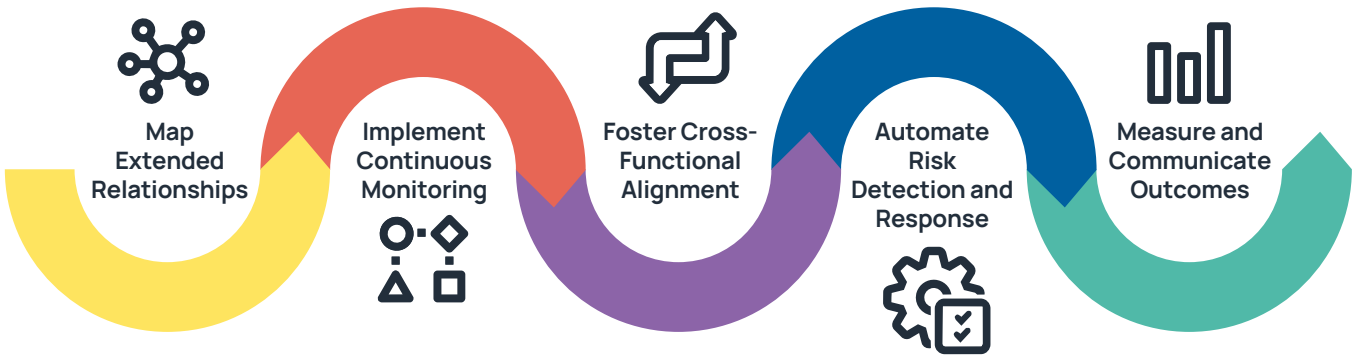


A Structured Path: Transitioning to Active Supply Chain Security

Moving from reactive compliance to active, risk-based security requires a systematic approach:

1. **Assess Current Maturity:** Benchmark visibility and automation; identify manual gaps.
2. **Align Board & Stakeholders:** Present industry data to justify change; set unified metrics.
3. **Map Critical Dependencies:** Inventory strategic suppliers and hidden dependencies using automated discovery.
4. **Adopt Automation & Continuous Monitoring:** Replace static assessments with dynamic tools and integrate threat intelligence.
5. **Extend Incident Response:** Build plans and exercises that include lower-tier vendors.
6. **Iterate & Report:** Use metrics and feedback to refine, reporting progress in board-ready formats.

Framework for Active Supply Chain Security



The Imperative: Rethinking TPRM for 2025

Legacy TPRM leaves enterprises exposed to rapidly evolving risks and visibility gaps that attackers exploit. To achieve resilience, organizations must embrace automation and adopt a continuous, intelligence-led approach. Every connection in the supply chain matters—the standard is rising, and leadership means transforming TPRM from passive oversight into active defense.

Organizations that act now will define the new standard for trust and security. The time for incremental change is over; the shift to Active Supply Chain Security is imperative.

The 4th-Party Blind Spot

Effective risk management begins with visibility. For CISOs, understanding the extended supply chain ecosystem is essential to anticipating and mitigating risk. As digital ecosystems expand, most programs mature their direct vendor oversight yet remain exposed to deeper-tier, less visible threats—the fourth-party blind spot.

Why the Fourth-Party Gap Matters

Today's supply ecosystem functions as an interconnected web, not a linear chain. Each third-party supplier brings its own set of dependencies, increasing complexity and risk propagation potential. Traditional frameworks rarely account for this depth.

Consider the following:

- **Pharmaceuticals:** A direct supplier managing clinical trial data relies on a cloud analytics subcontractor (fourth party). If compromised, your data and compliance position are impacted.
- **Insurance & Financial Services:** Incidents from downstream partners or subcontractors have led to millions in remediation and operational disruption. In 2023, 68% of CISOs in regulated industries experienced a supply chain incident originating beyond direct suppliers.

The Leadership Gap in Visibility

Our 2025 US CISO survey found **96% believe visibility beyond direct suppliers is vital**, yet **51% lack this capability**. Enhanced SEC disclosure rules and shifting frameworks like GLBA further drive the need for extended insight.

Industry Impact: Key Scenarios

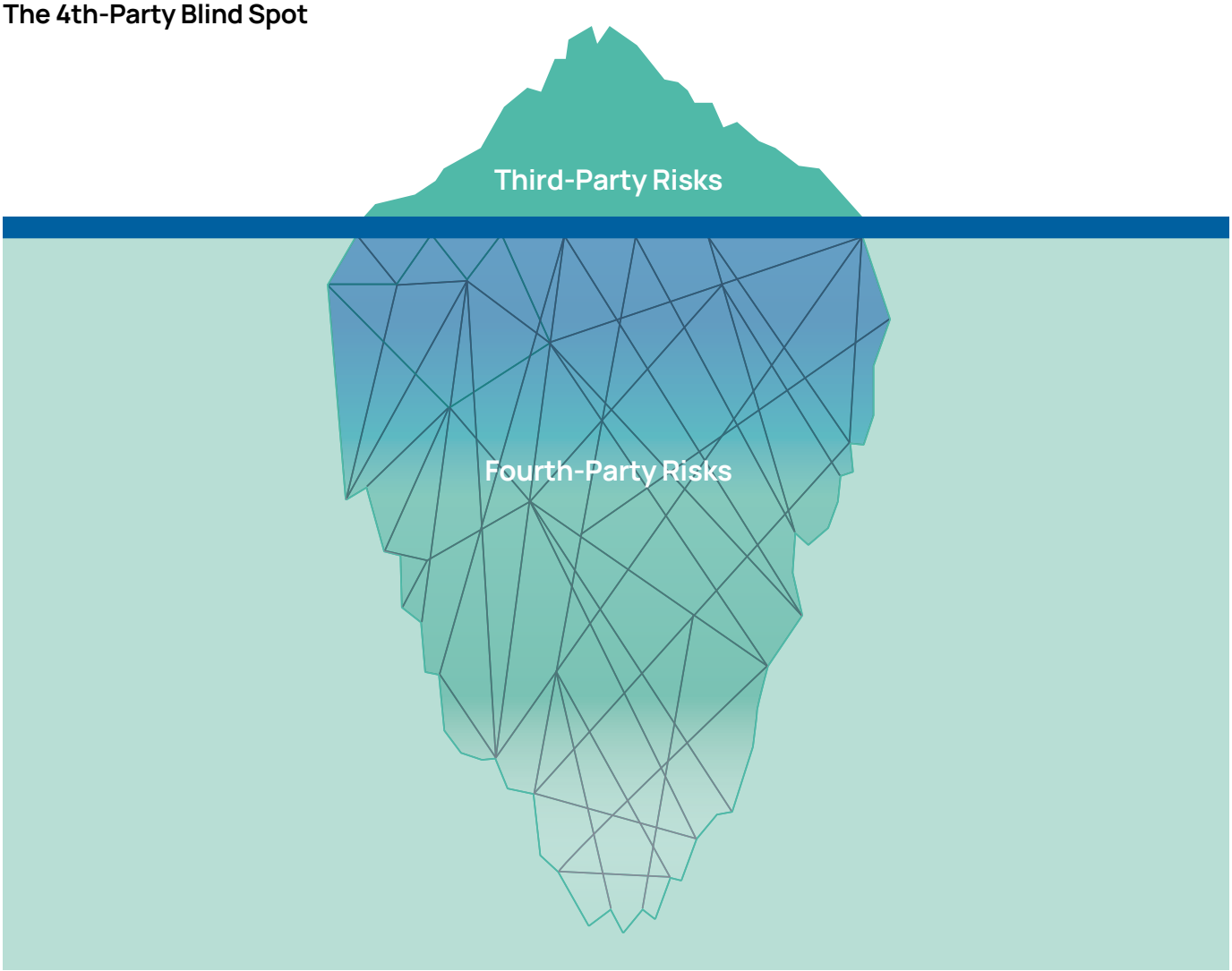
- **Financial Services:** Breaches in niche analytics providers have exposed sensitive customer data—often only detected post-incident.
- **Insurance:** Compromised automation scripts by offshore agencies put customer information and compliance at risk.
- **Pharmaceuticals:** Vulnerable fourth-party IoT systems halted production and triggered regulatory intervention.

These real-world examples highlight how invisible dependencies can escalate into tangible, high-impact events.

51%

of CISOs admit their organizations lack visibility beyond direct suppliers

The 4th-Party Blind Spot



Closing the Blind Spot: Action Framework

To mitigate the fourth-party blind spot, organizations should adopt the following structured approach:

1. **Map the Ecosystem**
   - Document all third-party relationships and require disclosure of their own critical third parties utilising new tooling to map deep-tier supplier dependencies.
2. **Continuous Monitoring**
   - Implement real-time monitoring and integrate threat intelligence for third-, fourth-, and nth-party risks.
3. **Risk Segmentation**
   - Focus due diligence on high-criticality, high-impact relationships; deploy enhanced controls for core suppliers.
4. **Incident Response Alignment**
   - Extend protocols and exercises to account for incidents beyond direct suppliers.
5. **Stakeholder Alignment and Reporting**
   - Provide board-level reporting and coordinate with procurement, compliance, and continuity teams.

A stepwise **framework diagram** can clarify this process for both executive and operational audiences.

Strategic Value of Deeper Visibility

By closing the fourth-party blind spot, organizations reduce risk exposure, strengthen audit readiness, and enhance stakeholder confidence. Proactive, multi-tier visibility in TPRM programs empowers teams to focus on critical threats.

Key Takeaway:

Addressing the fourth-party gap is no longer optional—focused visibility and structured response are now the foundation of modern supply chain resilience.

From Static Compliance to Active Supply Chain Security

The transition from static, compliance-centered models to an active, intelligence-driven security posture is now critical for supply chain resilience. This section presents a structured framework to help CISOs align operations, governance, and board engagement toward proactive risk management.

The Limits of a Compliance-First Mindset

Traditional supply chain risk management is rooted in compliance measures, often centered on supplier questionnaires, certifications, and annual reviews. Although these activities satisfy audit requirements, they capture only historical assurance and do not address evolving threats or enable real-time risk mitigation. Recent breaches—including those involving fourth-party vendors—highlight the inadequacy of static, review-based models, which lag behind dynamic adversary tactics.

Key Insight: Compliance processes are often reactive, providing a limited snapshot of supplier security. In our 2025 US CISO survey, over 61% of insurance CISOs and 54% of financial services CISOs identified static reviews as a major barrier to true risk visibility.

Actionable Recommendation:

- Shift from periodic reviews to frequent, risk-tiered engagements.
- Supplement questionnaires with ongoing validation and verification.
- Integrate board metrics to track the cadence and effectiveness of supplier oversight.

Embracing Active Supply Chain Security: A Framework for Modern Operations

Active Supply Chain Security reframes TPRM beyond paper compliance to continuous readiness, embedding resilience through a people, processes, and technology approach.

Operational Benefits:

- **Continuous Monitoring:** Automated, ongoing risk assessments deliver up-to-date visibility and enable early risk detection. In financial services, 68% of CISOs now mandate live monitoring for critical vendors.
- **Real-Time Intelligence:** Combining threat intelligence with supplier telemetry allows prioritization based on evolving risks, distinguishing true exposures from superficial compliance gaps.
- **Automation:** Automated platforms streamline supplier data collection, risk scoring, and incident escalation at scale. 41% of CISOs in our survey prioritized automation improvements in TPRM; over half of healthcare organizations have active pilots.

Action Steps:

- Map critical supply chain dependencies and flag visibility gaps.
- Invest in solutions that deliver real-time intelligence.
- Establish automated workflows to escalate high-risk findings promptly.

Enabling Strategic Value Through Board Communication

Active Supply Chain Security doesn't just reduce risk—it creates business value and should be communicated as such to executive leadership.

- **Regulated Sectors:** Enables rapid compliance with regulations (e.g., GLBA, OCC, SEC), enhances audit outcomes, and reduces exposure to evolving cyber threats.
- **Operational Metrics:** Organizations adopting Active Supply Chain Security report significant reductions in third-party incident response times and increased board confidence in risk programs.

Key Advantages:

- Uncover hidden risks in multi-tier supply chains.
- Accelerate response when incidents occur, minimizing business impact.
- Equip executive teams with actionable, data-driven insights for strategic decisions.

Board-Focused Actions:

- Regularly update executives with tailored dashboards showcasing live supplier risk.
- Present real-world scenarios to validate and improve incident response readiness.

Invest in Proactive Security

The data is clear: static, compliance-only TPRM is inadequate in the face of modern supply chain complexity and regulatory scrutiny. Forward-looking CISOs are shifting from basic compliance to strategic risk management, measured by KPIs such as time-to-detect supplier breaches and the percentage of suppliers with validated controls.

Next Steps:

- Assess current TPRM maturity and identify visibility gaps.
- Prioritize investment in continuous, automated monitoring.
- Foster cross-functional stakeholder engagement to drive adoption.

Conclusion:

In today's interconnected landscape, your security depends on every link in your supply chain, visible or not. Taking an active approach means minimizing blind spots and building resilience beyond compliance—a strategic imperative for organizations seeking to stay ahead of risk.

What US CISOs Want in 2025

Understanding CISO priorities is essential to effective supply chain security. This section distills the expectations and decision drivers shaping strategic investments in 2025.

Key Investment Drivers

CISOs prioritize supply chain security for four central reasons:

- **Regulatory Requirements (50.9%):** Compliance mandates are continuous. New frameworks like SEC disclosure rules, GLBA, and state-level laws now require audit-ready transparency beyond tier-one suppliers. Non-compliance can lead to operational risk, regulatory penalties, and lost board confidence.
- **Industry Standards (44.9%):** Adhering to benchmarks such as NIST SP 800-161 or ISO/IEC 27036 is a strategic differentiator. Mapping supplier relationships beyond direct vendors can expose and remediate overlooked risks, supporting successful certifications.
- **Client & Customer Demands (43.9%):** Clients and partners require evidence of proactive risk management. Failing to show supply chain oversight can result in lost business opportunities and reputational damage.
- **Board & Executive Oversight (43.8%):** Boards increasingly demand real-time, data-driven reporting. Security leaders must demonstrate measurable improvements, driving investments in automated, intelligence-led platforms.

CISOs seek solutions that directly align with these drivers—delivering compliance, differentiation, trust, and actionable oversight.

Solution Priorities for 2025

CISOs are focusing investment in three core areas:

1. **Enhanced Supply Chain Visibility (54.3%):** Full visibility into supplier dependencies is foundational. Platforms that illuminate hidden risks and support mitigation planning are prioritized.
2. **Real-Time Monitoring (51.0%):** Continuous monitoring is now essential, enabling proactive responses to supplier threats and reducing incident response times.
3. **Automation (41.3%):** Automating assessments and evidence collection enables scale, supports compliance, and frees security teams for higher-value strategic work.

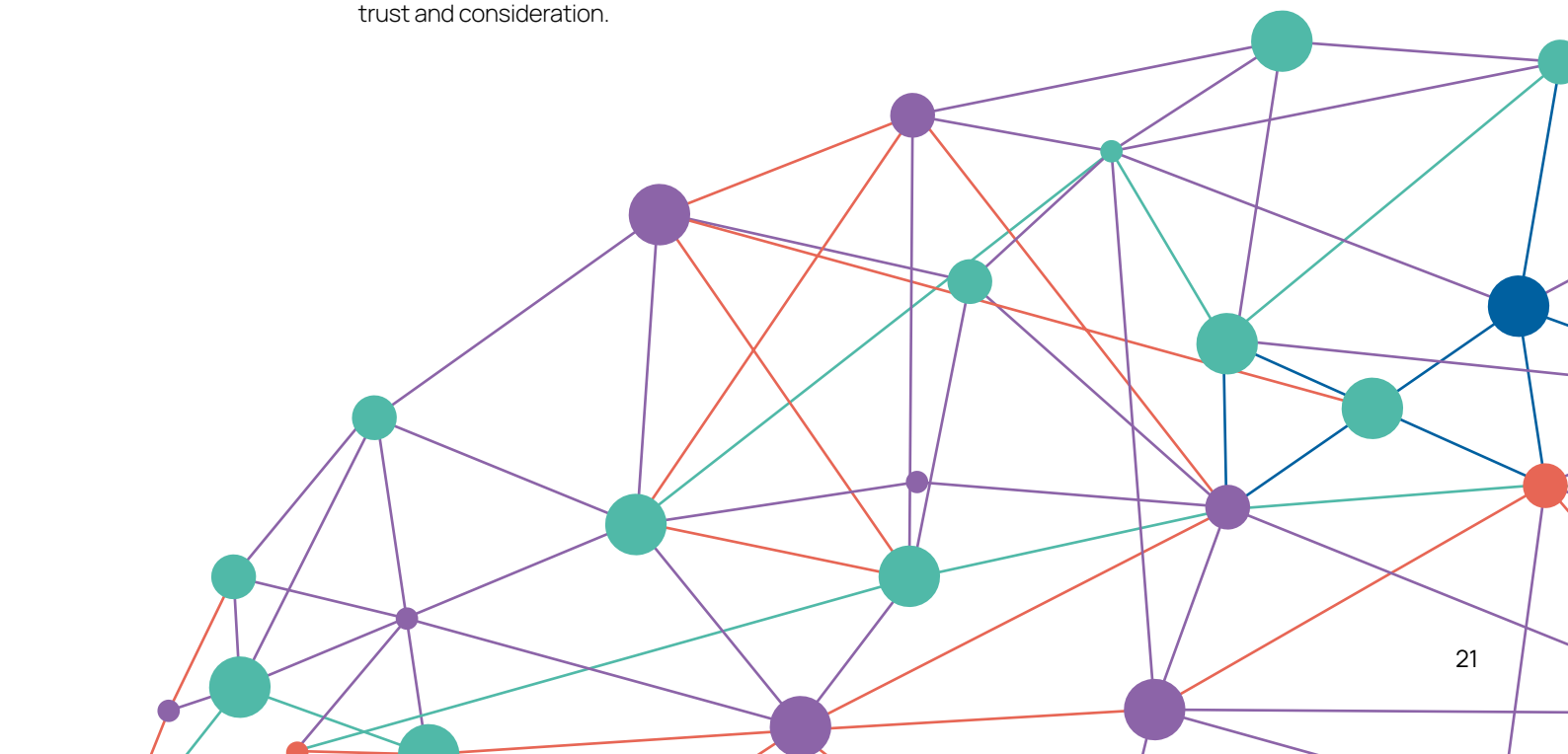
Targeted investment here delivers measurable gains in resilience, speed, and operational efficiency.

Validation & Procurement

CISOs rely on trusted sources to select solutions:

- **Analyst Reports (54.4%):** Industry-standard assessments (e.g., Gartner, Forrester) provide independent validation for solution shortlisting.
- **Security Media (47.9%):** Publications and peer interviews inform ongoing awareness.
- **Consultants (43.2%):** Advisory partnerships contextualize best practices and tailor strategies.
- **Industry Events (43.0%):** Peer insights and real-world demonstrations build confidence in solution fit and impact.

Peer validation, analyst recognition, and industry presence are essential to earning trust and consideration.



Toward Resilience: Moving Beyond Compliance

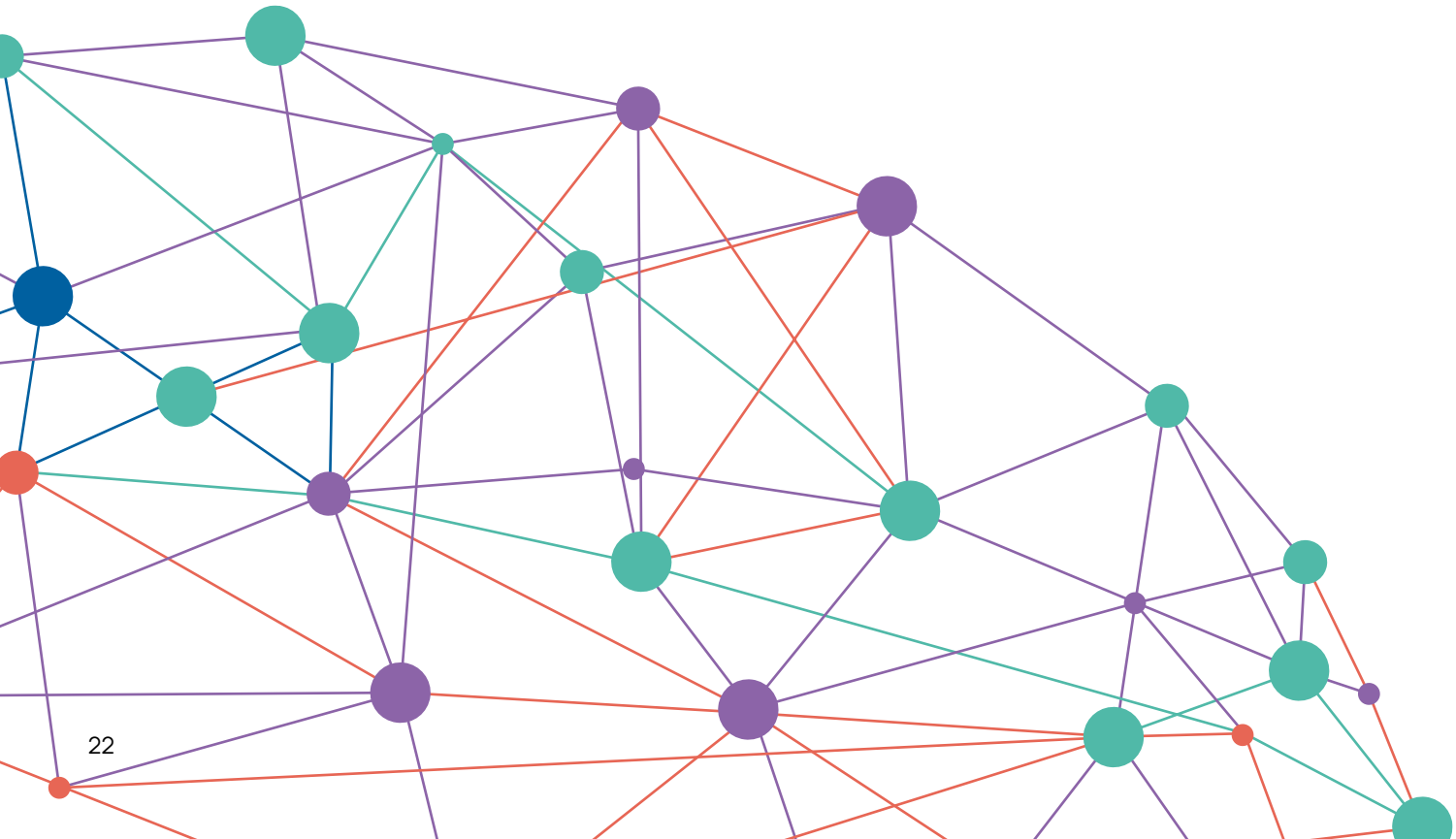
US CISOs want platforms that deliver more than compliance—they expect continuous, intelligence-driven visibility and the ability to communicate risk in board-level language. To align:

- Deliver real-time, multi-tier visibility powered by automation and integrated intelligence.
- Equip leaders with data that supports board reporting and secures budgetary support.
- Ensure solutions are flexible and scalable across growing supplier ecosystems.

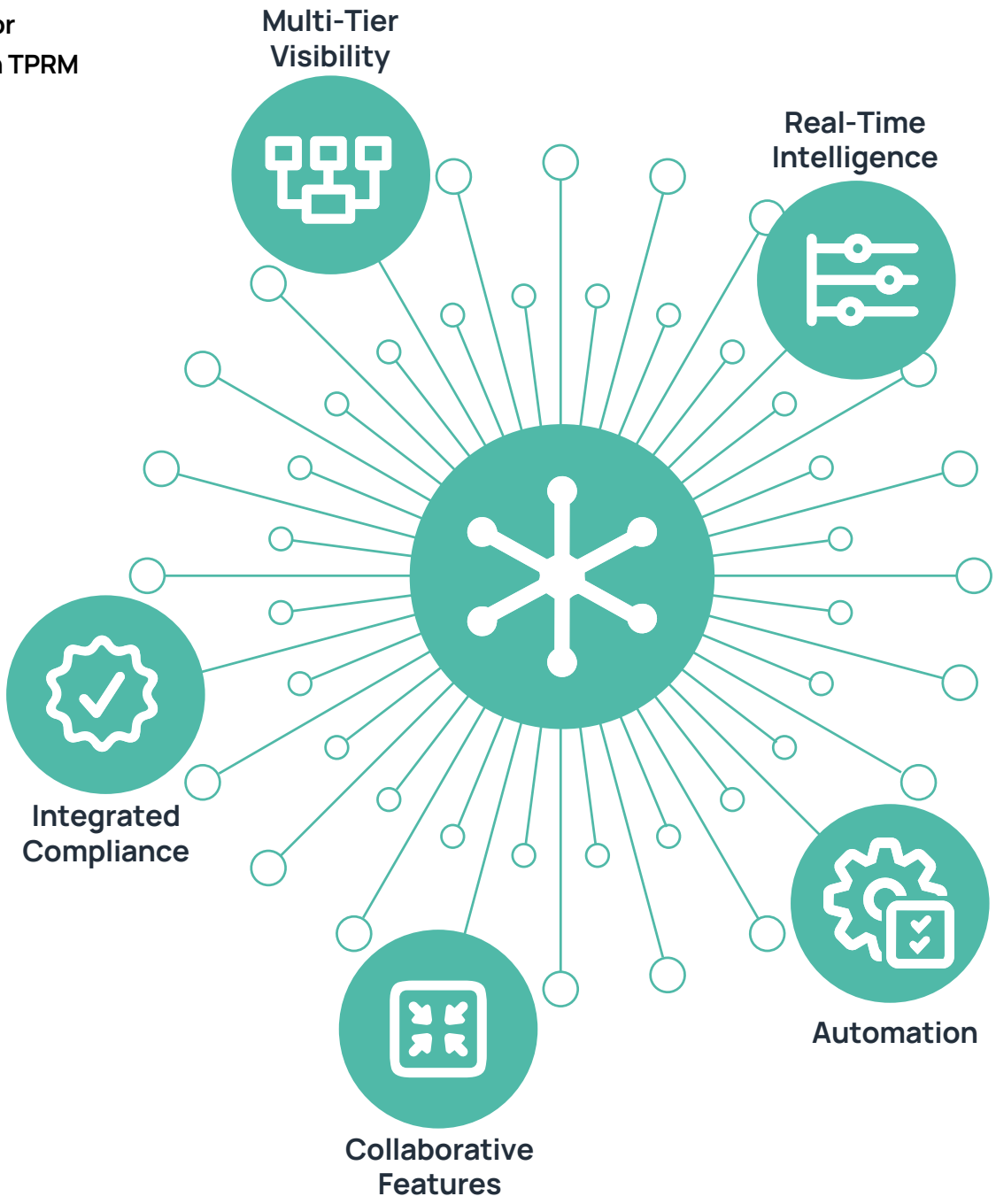
Summary

- Investment is driven by compliance, market differentiation, client trust, and executive oversight.
- Visibility, continuous monitoring, and automation are central to scalable, effective strategies.
- Solution credibility relies on independent and peer validation.
- Strategic alignment empowers CISOs to transition from basic TPRM to enterprise resilience.

Every link in the supply chain matters—and resilience depends on unified, intelligence-led approaches that empower security leaders to anticipate and withstand evolving threats.



CISO Priorities for Next-Generation TPRM



Closing Insight: You're Not Alone—Shared Risks Demand Collective Defense

This report makes one point clear: supply chain security threats are systemic and deeply interconnected. No organization operates in isolation—your digital supply chain often overlaps with peers and partners. This reality means vulnerabilities, especially with common vendors, can cascade across industries.

Traditional, siloed approaches to Third-Party Risk Management (TPRM) are no longer sufficient. Our 2025 CISO survey shows 96% of security leaders recognize the importance of visibility beyond direct suppliers, yet over half lack this capability. To close this critical gap, organizations must shift to collaborative models.

Actionable Steps for Collective Resilience:

- **Share Supplier Intelligence:** Collaborate to map extended supply chains and flag concentration risks.
- **Streamline Assessments:** Reduce duplication by sharing assurance data, enabling automation, and reallocating resources to strategic risk mitigation.
- **Coordinate Responses:** Exchange threat intelligence and best practices to accelerate and strengthen collective responses.

Adopting a network-based, community defense platform transforms risk management from a solitary effort into a strategic, sector-wide advantage. The challenges—from blind spots in the supply chain to static compliance—can be overcome when organizations choose to defend as one. Shared risk becomes shared strength when you act together.

RISK LEDGER

Risk Ledger Ltd.
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com | marketing@riskledger.com | +44 1234 567890