Every vendor is a vector

A data-led guide to supply chain cyber risk and the case for modern TPRM

CybelAngel

The big picture

Supply chain cyber risk has moved from a niche concern to the **defining security challenge of 2026**.

Third-party breaches doubled as a share of all incidents this year. Regulations across Europe and the US now hold leadership personally accountable for vendor risk. And the organizations getting this right are pulling measurably ahead of those that aren't.

This report draws on the latest research from Verizon, SecurityScorecard, the World Economic Forum, BlueVoyant, Gartner, Forrester, and others to map where supply chain risk stands today and what a well-built TPRM program actually looks like in practice.

It is built for security teams evaluating how to strengthen their third-party risk posture, and for the people who need to make the case internally for better tools, better processes, and better visibility across the vendor ecosystem.

How to read this report

This report is structured in four parts:

Part 1

The threat environment map lays out where supply chain risk stands right now, with data across industries and geographies.

Part 2

The regulatory picture maps the compliance obligations reshaping how organizations manage vendor risk across France, Germany, Belgium, Switzerland, the UK, and the US.

Part 3

What good TPRM looks like makes the positive case for modern third-party risk management and what separates effective programs from checkbox exercises.

Part 4

The AI factor covers how AI is changing both the threat and the response, and what security teams should be planning for now.

Throughout, we have included data tables, comparison frameworks, and key stat callouts designed to be pulled out and used in internal presentations, board briefings, and business cases.

The threat environment map

What do the numbers actually tell us?

Let's start with the data, because it sets the context for everything that follows. The numbers this year aren't just bad; they represent a meaningful shift in how supply chain attacks are playing out.

According to Verizon's 2025 Data Breach Investigations Report, 30% of all data breaches this year involved a third party. That's double the prior year. BlueVoyant's State of Supply Chain Defense 2025, based on a survey of 1,800 executives, found that 97% of organizations experienced at least one supply chain breach, up from 81% in 2024. And when a breach does originate from a third-party system, Whistic's 2025 research puts the average remediation cost at $4.8M.

Perhaps most telling of all: according to the WEF Global Cybersecurity Outlook 2025, 54% of large organizations now say supply chain challenges are the single biggest barrier to achieving cyber resilience. This isn't a secondary concern anymore. For most large organizations, it's the primary one.

The vendor ecosystem itself is also expanding. The average organization now works with 286 third-party vendors, up 21% year over year. More vendors means more potential entry points and more relationships to monitor, assess, and manage.

Third-party share of all breaches

30%

in 2025, double the prior year

(Verizon DBIR 2025)

Average cost of a third-party breach

$4.8M

(Whistic 2025)

Organizations breached via supply chain

97%

up from 81% in 2024

(BlueVoyant 2025)

Large orgs citing supply chain as top resilience barrier

54%

(WEF GCO 2025)

Average vendor count per organization

286

up 21% year over year

(Industry data 2025)

Key headline metrics for 2025. Sources linked where publicly accessible.

So where are supply chain attacks actually hitting?

It's easy to assume supply chain risk is primarily an IT-sector problem. The data says otherwise. Attacks are distributed across industries, with some sectors taking consistently heavier hits because of the complexity and interconnectedness of their vendor ecosystems.

Let's look at where the exposure is most acute.

Manufacturing has been the number one ransomware target for four consecutive years. **With 38.9% of ransomware victims among companies over $1B in revenue**, and deep supplier interdependencies across tier-2 vendors, the sector saw multiple cascading production shutdowns via supplier compromise in 2024 and 2025.

Financial services carries DORA compliance pressure on top of high-value data and complex ICT third-party chains. Ongoing dark web trading of vendor credentials linked to major banks continues to surface in threat intelligence feeds.

Healthcare sits at the intersection of sensitive patient data, billing systems, connected devices, and cloud providers, with HIPAA exposure at every layer. The Episource breach alone affected 5.4 million individuals, and third-party billing compromises remain an ongoing pattern.

Retail operates extensive vendor networks for payments, logistics, and e-commerce. Marks & Spencer was among the notable third-party breach victims of 2025, alongside multiple POS vendor compromises affecting organizations across the sector.

Technology faces software supply chain risk, concentration in cloud providers, and cascading MSP/SaaS exposure. Exploitation of widely deployed vendor tools continued throughout 2025. Aviation and transport combines offshore call centers, complex global vendor chains, and real-time operational dependency. The Qantas third-party breach exposed six million customer records.

> "Supply chain attacks have become the ultimate force multiplier. Traditional threats target individual companies, but the most devastating attacks in 2025 exploit the few critical dependencies that connect thousands of organizations."
>
> — **SecurityScorecard**, 2025 Supply Chain Cybersecurity Trends Report

Sources: Black Kite 2025, Verizon DBIR 2025, public incident reporting.

Does geography change the risk profile?

It does, significantly. European organizations tend to operate more complex vendor networks spanning more countries, which creates both a larger attack surface and a more challenging compliance environment.

European companies

Vendors spanning 20+ countries

47%

Regulatory frameworks to track

4 to 6 overlapping
(NIS2, DORA, CRA, GDPR, national laws)

Foreign subsidiaries as breach sources

2x more likely than domestic

North American companies

Vendors spanning 20+ countries

22%

Regulatory frameworks to track

2 to 3
(SEC, sector-specific, state-level)

Foreign subsidiaries as breach sources

Baseline

Geographic comparison of vendor ecosystem complexity. Source: Supply Wisdom 2025, SecurityScorecard 2025.

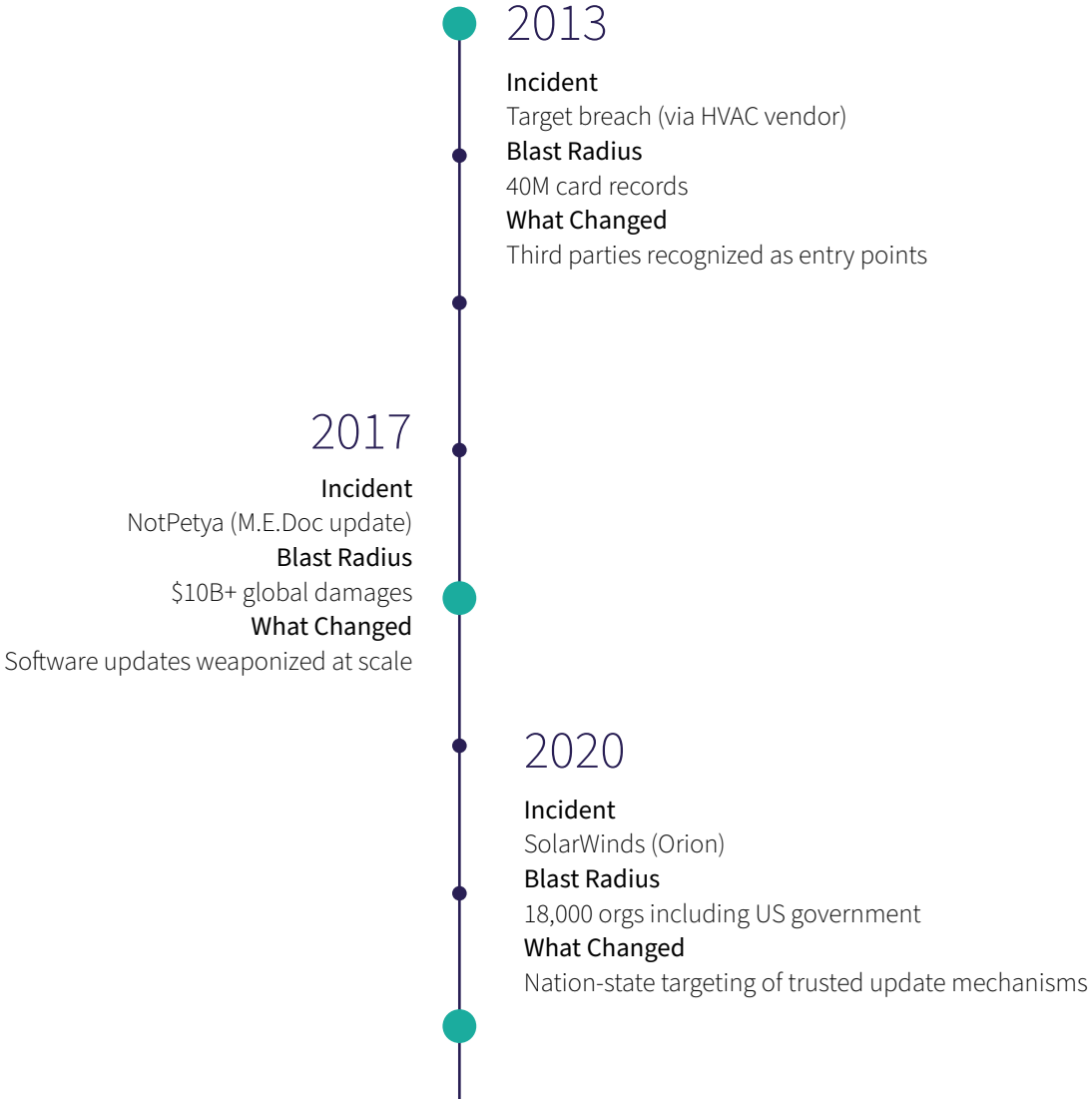
How did we get here? The attack timeline

Germany's manufacturing sector is a particular hotspot. The country's dense network of Mittelstand companies, mid-sized manufacturers forming the backbone of European supply chains, creates a vast third-party attack surface that many organizations are only beginning to map systematically.

France faces a compliance timing gap, with NIS2 transposition still in progress while DORA is already in force for financial services. Belgian organizations have had more than a year of NIS2 enforcement experience.

Swiss companies, while outside the EU, face growing flow-down obligations from EU clients. And UK organizations are currently navigating the Cyber Security and Resilience Bill, which closely mirrors NIS2, with Risk Ledger's 2025 UK Supply Chain Security Report flagging monitoring gaps, poor visibility, and limited cross-industry collaboration as the biggest shortcomings.

The supply chain threat didn't emerge overnight. It built momentum over a decade, and each major incident expanded the playbook attackers use today. Understanding that progression matters because it explains why the tactics organizations relied on five years ago are no longer sufficient.



2021

Incident
Kaseya (REvil)
Blast Radius
1,500+ businesses
What Changed
MSP ecosystems as cascading attack vectors

2023

Incident
MOVEit Transfer
Blast Radius
2,700+ orgs, 93M+ people
What Changed
Single vendor tool compromising thousands

2024

Incident
CrowdStrike outage
Blast Radius
Airlines, banks, hospitals globally; Delta ~$350M loss
What Changed
Vendor concentration as operational risk

2025

Incident
M&S, Qantas, others
Blast Radius
Major retailers, airlines compromised via vendors
What Changed
Supply chain breaches become routine, not exceptional

That last shift, from exceptional to routine, is the one that should concern security teams most. Routine doesn't mean manageable. It means the baseline expectation has changed.

"What we're seeing now is a shift from supply chain attacks as headline events to supply chain attacks as background noise. That normalization is dangerous. It means organizations are absorbing the risk rather than resolving it."

— **Kevin Gaudichon,** Head of REACT, CybelAngel

Now that we've mapped where the threat stands, let's look at what regulation actually requires of you in response.

The regulatory picture

Why is the compliance landscape so complex right now?

The short answer: multiple major frameworks landed at roughly the same time, with different scopes, timelines, and enforcement mechanisms, and they all have explicit supply chain provisions.

Three EU frameworks, NIS2, DORA, and the Cyber Resilience Act, are converging. Layer in GDPR, SEC rules, CMMC, and sector-specific regulators, and most organizations are navigating a patchwork that demands real coordination across legal, security, and procurement teams.

The numbers reflect just how hard that coordination is proving to be.

76% of CISOs say regulatory fragmentation greatly affects their ability to maintain compliance.
(WEF Global Cybersecurity Outlook 2025)

69% find existing regulations too complex to verify third-party adherence.
(WEF Global Cybersecurity Outlook 2025)

75% of the world's population will have personal data covered by privacy regulations by the end of 2025.
(Gartner)

The complexity isn't going to ease. But understanding what each framework actually requires, and where your organization sits within it, is a manageable starting point.

The supply chain compliance map

Here's how the major frameworks compare across the dimensions that matter most for vendor risk management.

	Covers	Supply chain requirements	Leadership accountability	Maximum penalties
NIS2	Critical and important entities across 18 sectors	Vendor risk assessment; explicit supply chain security	Personal liability; possible leadership bans	€10M or 2% global turnover
DORA	Financial entities and critical ICT providers	ICT third-party risk framework; register of information; critical provider designation	Mandatory resilience training for management	€5M or 2% turnover; daily penalties for critical providers
Cyber Resilience Act	Digital product manufacturers	Security-by-design; vulnerability management across product lifecycle	Manufacturer liability	Product bans, recalls, safety-level fines
GDPR	Data controllers and processors	Processor obligations; breach notification flow-down	Controller accountability	€20M or 4% global turnover
SEC Rules	US public companies	Material incident disclosure including supply chain	Board-level governance disclosure	SEC enforcement; shareholder litigation
CMMC	US defense contractors	Third-party control verification; subcontractor flow-down	False Claims Act exposure for misrepresentation	DOJ prosecution; contract loss

Regulatory framework comparison across the six dimensions most relevant to vendor risk. Correct as of Q4 2025.

Where does each country actually stand?

Let's look at the current state of play country by country, because the picture varies considerably.

France

NIS2 transposition is in progress, with European Commission infringement proceedings underway. DORA is already in force. CRA applies from December 2027. Enforced by ANSSI and CNIL. France's strong GDPR enforcement track record suggests NIS2 follow-through will be serious when it arrives.

Germany

NIS2 was transposed in April 2025. DORA is in force. CRA applies from December 2027. Enforced by BSI and BaFin. The manufacturing sector is heavily exposed, and Mittelstand supply chain mapping remains a significant gap for many organizations.

Belgium

NIS2 was transposed in April 2024, giving Belgium the longest enforcement runway of any EU member state covered here. DORA is in force. CRA from December 2027. Enforced by CCB. Audits are already underway.

Switzerland

NIS2 doesn't apply directly, but the ISG creates parallel obligations. DORA applies via flow-down for financial services. CRA impacts EU-sold products. Enforced by NCSC.ch. EU client contracts are increasingly driving Swiss companies toward effective NIS2-equivalent postures.

UK

Aligned with NIS2 via the Cyber Security and Resilience Bill. FCA has its own third-party risk framework for financial services. Enforced by NCSC, FCA, and ICO. The expectations are clear and getting sharper.

US

EU-serving companies face NIS2 and DORA flow-down obligations. CRA impacts EU-sold products. Enforced by SEC, DOJ, and sector regulators. SEC four-day materiality disclosure is in force and CMMC third-party verification requirements are tightening.

Why has this become personal for CISOs?

Regulation has always been part of the CISO's job. What's genuinely different now is the personal accountability dimension, and it's worth understanding exactly what that means in practice.

Under NIS2, management bodies are explicitly responsible for compliance. Failures can lead to temporary bans or disqualification from leadership roles, not just organizational fines. DORA requires senior leadership to complete digital operational resilience training and maintain segregated ICT risk management. The SEC requires board-level cybersecurity governance disclosure, which means the board, not just the security team, has skin in the game.

Forrester predicts that breach-related class-action costs will surpass regulatory fines by 50% in the coming year. When you add regulatory fines, litigation, insurance premium increases, and customer churn together, the total financial exposure from a single supply chain breach compounds fast.

What does enforcement actually look like?

Rather than dealing in hypotheticals, let's look at what has already happened in 2025.

MORSECORP (US defense, 2025)
Self-reported compliance score of 104. An independent review found -142, with only 22% of controls actually in place. Settlement: $4.6M. The lesson: self-reported posture means nothing without external verification.

Health Net Federal Services (US defense, 2025)
Falsely certified compliance with 110 NIST controls for three consecutive years, while running vulnerability scans but taking no action on the results. Settlement: $11M. The lesson: running assessments without acting on them isn't a process gap, it's a compliance failure.

Multiple NIS2 infringement proceedings (2025)
The European Commission is actively pursuing 13 member states including France, Germany, and Spain for late transposition. Status: ongoing. The lesson: even governments are struggling with the timeline. Waiting for regulatory clarity before acting is not a viable strategy.

With the threat and regulatory landscape clear, let's turn to the more practical question: what does a TPRM program that actually works look like?

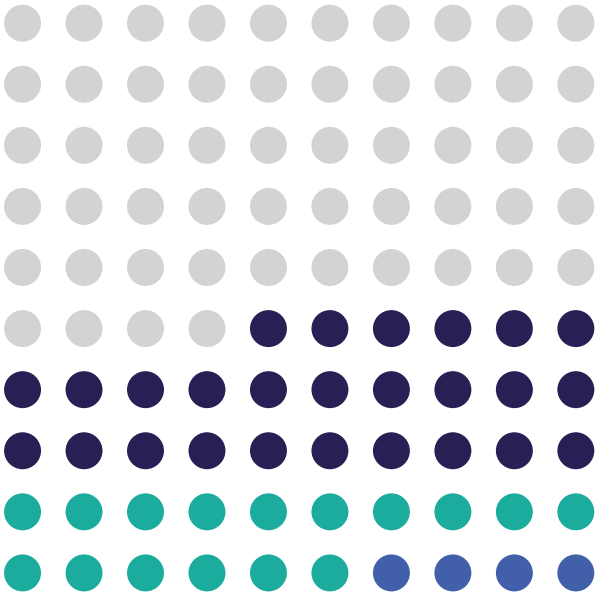
What good TPRM looks like

Why isn’t more spending solving the problem?

This is the question that deserves a straight answer. 95% of organizations increased their TPRM budgets this year. 97% still got breached through their supply chain. If investment isn’t solving the problem, something more fundamental needs to change.

The answer, when you look at how most programs are actually built, becomes clear. The problem isn’t TPRM as a discipline. It’s that most organizations are running compliance-driven programs in a risk environment that requires something different.

Consider where most programs stand today.



Only **26%** integrate incident response into their TPRM program. (SecurityScorecard 2025)

Only **16%** of organizations cite risk reduction as the primary driver of their TPRM program. (BlueVoyant State of Supply Chain Defense 2025)

Only **4%** have high confidence their questionnaires reflect vendor security reality. (Industry survey 2025)

These aren’t small gaps. They represent a fundamental mismatch between what most programs are designed to do, satisfy compliance requirements, and what the threat environment actually demands.

What's broken vs. what works

The difference between compliance-driven and risk-driven TPRM shows up across every dimension of how a program operates.

What most organizations do (compliance-driven TPRM)	What leading organizations do (risk-driven TPRM)
Annual vendor questionnaires	Continuous external monitoring and periodic deep assessments
Assess all vendors the same way	Tiered assessment based on business criticality and data access
Self-reported vendor posture only	External threat intelligence validates vendor claims
TPRM sits in procurement or compliance	TPRM embedded in security operations with cross-functional input
Point-in-time snapshots	Real-time alerting on vendor posture changes
Measure compliance status	Measure actual risk reduction and time-to-remediation
React to breaches after disclosure	Detect vendor exposures before exploitation
1 to 2 FTEs managing 300+ vendors	Right-sized team supported by automation and AI tools
Brief leadership quarterly at best	Monthly or event-driven reporting tied to business risk
Nth-party risk is a blind spot	Extended supply chain mapping with flow-down obligations

Compliance-driven vs. risk-driven TPRM: how the two approaches differ across every dimension of program operation.

The organizations in the right column aren't doing anything exceptional. They've made a deliberate decision to treat TPRM as a security function rather than a compliance function. And the data consistently shows it pays off.

What does the business case actually look like?

For security teams making the internal case for better TPRM investment, the numbers are worth putting side by side.

Average cost of a third-party breach

$4.8M

Non-compliance cost

Typically $3M to $5M+ in fines and litigations

(Ponemon estimate: approximately 3x the cost of compliance)

Average US breach cost (all types)

$10.22M

Average annual investment in a mature TPRM program

$500K to $1.5M depending on org size

(platform and headcount)

Platform consolidation savings

30 to 40% cost reduction

(replacing 5 to 10 point solutions)

Breach and program cost comparison. The math is clear: a mature program costs a fraction of what a breach does.

Beyond the direct cost comparison, organizations with mature TPRM programs consistently report a 60 to 80% reduction in alert volume through better signal-to-noise ratio, 30 to 50% faster incident response when vendor compromises occur, and measurably better relationships with regulators who can see evidence of genuine oversight rather than paper compliance.

Six things effective TPRM programs do differently

So what specifically separates programs that work from those that don't? Let's look at the six practices that consistently show up in effective programs.

1. They monitor continuously, not periodically

Annual assessments were built for a threat landscape that no longer exists. Automated attackers scan the internet constantly, and data shows that critical cloud misconfigurations can be exploited in under 10 minutes. Effective programs pair periodic deep assessments with continuous external monitoring that tracks vendor posture changes in real time, so that a vendor whose credentials appear on a dark web forum on a Tuesday night doesn't stay undetected until next quarter's review cycle.

2. They tier vendors by actual risk, not contract size

Not every vendor deserves the same level of scrutiny, and treating them all equally wastes the resources you need for the vendors that actually matter. Effective programs ask four questions about every vendor: How much data do they touch? How deeply are they integrated into your systems? How operationally dependent are you on them? And what's the regulatory exposure if they're compromised? The answers determine how much attention each relationship deserves.

3. They validate vendor claims with external intelligence

Questionnaires capture what vendors choose to tell you. External threat intelligence, including dark web monitoring, leaked credential detection, and exposed asset discovery, reveals what they can't or won't disclose. Security teams with integrated external threat intelligence are twice as likely to catch a major incident before it causes widespread damage. The two inputs aren't alternatives; they're complementary.

4. They integrate TPRM into security operations

In most organizations, TPRM sits in procurement or GRC. In effective programs, it feeds directly into the SOC. When a vendor's credentials surface on a dark web marketplace, the response shouldn't start with a questionnaire. It should start with containment. That speed of response is only possible when TPRM is wired into the broader security function rather than operating as a separate process.

"The most effective supply chain defense programs treat vendor risk the same way they treat internal threats, with real-time detection, validated intelligence, and incident response workflows that move at the speed of the attack, not the speed of a procurement cycle."

— **Kevin Gaudichon,** Head of REACT, CybelAngel

5. They measure outcomes, not activity

Counting vendor assessments completed is an activity metric. Measuring mean-time-to-detect a vendor exposure, or the percentage of critical vendors with validated security posture, is an outcome metric. Boards and regulators increasingly want the latter, and rightly so. Activity metrics tell you how busy your team is. Outcome metrics tell you whether the program is actually working.

6. They plan for nth-party risk

Your vendors' vendors are part of your attack surface, whether you're tracking them or not. Effective TPRM programs require primary vendors to disclose material subcontractor dependencies, include flow-down obligations in contracts, and use external scanning to identify concentration risks in the extended supply chain. This is where most programs have the biggest blind spot, and where some of the most significant recent breaches have originated.

The good news is that all of these practices are achievable. None of them require exceptional resources; they require deliberate choices about how the program is structured and what it's optimized for. With that foundation in place, let's look at the factor that's reshaping TPRM faster than any other: AI.

The AI factor

How is AI changing the supply chain equation?

AI is simultaneously creating new categories of supply chain risk and providing the most promising tools for managing that risk at scale. Both things are true at the same time, and the organizations navigating this well are the ones planning for both sides of that equation.

The adoption numbers are striking. According to Zscaler's ThreatLabz 2026 AI Security Report, enterprise AI/ML activity grew 91% year over year in 2025, spanning more than 3,400 applications. Yet the WEF Global Cybersecurity Outlook 2025 found that only 37% of organizations have processes in place to assess the security of AI tools before deployment. And according to Proofpoint's Voice of the CISO 2025, 72% of CISOs worry that generative AI could cause a significant breach at their organization.

The gap between adoption speed and governance maturity is where the risk lives. Let's look at what that means in practice.

What is shadow AI doing to your supply chain?

The biggest AI risk for most organizations isn't their own AI deployment. It's the AI their vendors are deploying without telling them, and the data flowing through it that nobody has reviewed or consented to. Here's how that plays out across common scenarios.

Scenario	What happens to your data	Can your TPRM program see it?
Vendor enables AI features in your SaaS tool	Data fed into AI model; may be used for training	Unlikely; often enabled by default
Subcontractor uses ChatGPT to process deliverables	Confidential documents uploaded to third-party AI	No; happens at individual user level
Cloud provider adds AI analytics layer	Metadata analyzed by AI partner; data residency risks	Rarely; buried in updated terms of service
Vendor's vendor uses AI for quality assurance	Test data containing real customer info processed through AI	No; beyond typical TPRM scope
AI translation of sensitive communications	Text processed and potentially retained by AI model	No; rarely disclosed

Common shadow AI scenarios and their visibility to existing TPRM programs. Most represent blind spots today.

Adversarial techniques add another layer of concern worth understanding. Data poisoning, injecting malicious data into AI training sets, is growing more sophisticated. Techniques like ConfusedPilot specifically target RAG-based enterprise AI systems. When these techniques hit a vendor's AI pipeline, the blast radius extends to every organization that vendor serves.

And then there's the nth-party AI problem. Your vendor's vendor may be running your data through AI models you don't know about, hosted in jurisdictions you haven't evaluated, with retention policies nobody has reviewed. This is an emerging blind spot that most current TPRM frameworks simply aren't designed to address.

How does AI help on the defense side?

Here's where things get genuinely useful for security teams evaluating their tooling. The core TPRM challenge, assessing hundreds of vendors with limited staff, maintaining visibility across an expanding ecosystem, connecting fragmented threat signals, is exactly the kind of problem AI is built to help solve.

Let's look at what changes when AI is properly integrated into a TPRM program.

	Manual TPRM	AI-augmented TPRM
Vendor assessment throughput	40% of vendors assessed on average	80 to 100% coverage through automated initial scoring
Time to detect vendor posture change	Months (next assessment cycle)	Hours to days (continuous monitoring)
Alert quality	High false positive rate; analyst time wasted on noise	Pre-filtered, enriched alerts with contextual risk scoring
Questionnaire processing	Weeks per vendor; manual review	Days; AI extracts and cross-references responses
Nth-party visibility	Effectively zero for most programs	Automated supply chain mapping and concentration analysis
Scalability	Linear; more vendors means more headcount	Non-linear; same team covers expanding ecosystem

Manual vs. AI-augmented TPRM: the operational difference across six program dimensions.

Agentic AI takes this further still. Unlike traditional tools that augment human workflows, agentic AI systems make decisions, adapt to new information, and run complex workflows with minimal human input.

In TPRM, that means AI agents that continuously monitor vendor ecosystems, flag posture changes automatically, kick off enrichment workflows when anomalies appear, and escalate to humans only when confidence thresholds aren't met. Gartner forecasts that agentic AI will enable at least 15% of day-to-day work decisions to be made autonomously by 2028, up from effectively zero in 2024.

That said, automation without validation creates its own problems. The organizations getting the most value from AI-augmented TPRM are pairing AI's scale and speed with human judgment, using automation to surface signals faster, and analysts to interpret what those signals mean in context.

"The way we think about it is straightforward: AI handles the volume, analysts handle the complexity. You need both. An automated system can flag that a vendor's credentials appeared on a dark web forum at 3am. But understanding what that means for your specific risk posture, your contractual obligations, and your incident response — that still takes a person who knows the context."

— **Kevin Gaudichon,** Head of REACT, CybelAngel

What should you do about AI risk in your supply chain now?

The good news is that this is a manageable problem if you start building the right foundations now. Here's where to focus.

PART 4

Add AI-specific questions to vendor assessments.

Do they use AI to process your data? What models? Where does data go? What governance exists? If they can't answer clearly, that's a signal worth flagging.

Extend your AI governance to third parties.

Internal AI policies that stop at your organizational boundary miss the biggest risk surface. Make vendor AI usage policies contractually binding, not just advisory.

Evaluate AI-powered TPRM tools.

The scale of modern vendor ecosystems is past what manual processes can cover. Look for platforms that combine automated detection with human validation. The goal is fewer false positives, not more noise.

Require nth-party AI disclosure.

Contractually require primary vendors to disclose material subcontractor AI usage. If they can't tell you whether their subcontractors are processing your data through AI models, you have a gap worth closing.

Start tracking post-quantum readiness.

It's early, but including post-quantum cryptography in vendor assessment criteria positions your program ahead of the curve. For your most sensitive data relationships, this should already be on the agenda.

The organizations that treat these steps as foundational rather than aspirational are the ones that will be best positioned as both the threat and the tooling continue to evolve.

Key findings at a glance

Finding	Data point	Source
Supply chain breaches are now routine	**97%** of organizations breached via supply chain in 2025, up from **81%** in 2024	BlueVoyant 2025
Third-party compromise is a top attack vector	**30%** of all breaches involved a third party, 2x vs. prior year	Verizon DBIR 2025
Vendor ecosystems are expanding fast	286 vendors per organization on average, up **21%** year over year	Industry data 2025
Most TPRM programs aren't focused on risk	Only **16%** cite risk reduction as primary TPRM driver	BlueVoyant 2025
Assessment coverage is inadequate	Organizations assess only **40%** of vendors on average	Mitratech 2025
TPRM teams are undersized	**73%** have 2 or fewer FTEs managing 300+ vendors	Ncontracts 2025
Regulation is creating personal liability	NIS2, DORA, and SEC all include management accountability provisions	Multiple
European supply chains are especially complex	**47%** of EU companies report vendors in 20+ countries	Supply Wisdom 2025
AI is creating new blind spots	Only **37%** assess AI tool security before deployment	WEF Global Cybersecurity Outlook 2025
AI-powered TPRM delivers measurable results	**60 to 80%** alert reduction; **30 to 50%** faster incident response	Industry benchmarks

Summary of key findings. All data points sourced from publicly available 2025 research.

METHODOLOGY AND SOURCES

- Verizon 2025 Data Breach Investigations Report
- SecurityScorecard 2025 Supply Chain Cybersecurity Trends
— survey of approximately 550 CISOs
- BlueVoyant / Opinion Matters State of Supply Chain Defense 2025
— survey of 1,800 executives
- World Economic Forum Global Cybersecurity Outlook 2025
- Gartner: Volatile Environment Driving TPRM Market Growth and Maturity
- Gartner: Intelligent Agents in AI — agentic AI forecast to 2028
- Gartner: Top Cybersecurity Trends for 2026
- Forrester 2026 Cybersecurity Spending Analysis
- Black Kite 2025 Supply Chain Vulnerability Report
- Mitratech 2025 Third-Party Risk Management Study
- Ncontracts 2025 Third-Party Risk Management Survey
- Whistic 2025 TPRM Report
- Risk Ledger 2025 UK Supply Chain Security Report
- Supply Wisdom Global TPRM Benchmarking Data 2025
- Zscaler ThreatLabz 2026 AI Security Report
- Proofpoint 2025 Voice of the CISO
- ECSO NIS2 Directive Transposition Tracker
- ISACA NIS2/DORA White Paper 2025
- Ponemon Institute / IBM Cost of a Data Breach 2025

CybelAngel perspectives are drawn from the REACT threat intelligence team's operational observations across deep, dark, and open web monitoring.

The external threat intelligence platform that **secures your business**