Your Questionnaire Won't Save You. Discover The Vendors Most Likely To Breach You Next.

2026

Whitepaper

elasticito
risk & threat specialists

A signed PDF from 2025 will not stop a 2026 exploit. This paper shows why questionnaire-led vendor risk keeps failing — and how continuous threat modelling finds the few vendors actually driving your breach risk, before they make the news.

Contents

I. Executive Summary

The vendors most likely to breach you next are the widely-shared software and SaaS providers carrying an actively-exploited vulnerability, leaking credentials into infostealer logs, or holding unrevoked privileged access to your data. Those are your breach candidates, and your annual questionnaire cannot see any of it. Across the 50 vendors most widely shared by the Forbes Global 2000, Black Kite found 70% carry an unpatched CISA Known Exploited Vulnerability and 62% have corporate credentials sitting in stealer logs.[1]

This paper explains why certification-led assessment misses them, names the four signals that predict a vendor breach, and shows how to rank your suppliers by real-world breach potential rather than contract value.

WHY YOUR QUESTIONNAIRE WON'T SAVE YOU

Vendor security questionnaires fail to prevent breaches because they capture what a vendor says on the day they fill in the form, not what their systems are doing every day after. They are point-in-time, self-reported, and easy to game, and the people who run third-party risk for a living already know it. Only 34% of TPRM professionals say they believe the answers their vendors give them, and 14% are highly confident a vendor actually meets requirements — yet 84% still use the questionnaire as their primary assessment method.[3]

The reflex is to send a longer questionnaire. That treats the symptom. The deeper problem is timing and trust: a form answered once a year cannot track a control that drifts the following week, and you cannot trust a self-report when the supplier itself often does not know what happened. ENISA found that in 66% of supply-chain attacks it analysed, suppliers did not know — or were not transparent about — how they had been compromised.[6] You are asking vendors to attest to controls they cannot see failing.

Certification does not close the gap. A certificate proves an audit happened; it does not prove the controls hold up the other 364 days. The contradiction is now coming from inside the audit profession: the AICPA's own Journal of Accountancy warned in 2026 that SOC 2 audit quality is degrading, with firms leaning too heavily on automation platforms and producing template reports.[7] The point landed hard when a whistleblower alleged that compliance-automation firm Delve had issued 494 SOC 2 reports, 493 of them near-identical templates — same paragraphs, same grammatical errors.[8] Questionnaire says: "We are SOC 2 Type II certified." Reality shows: 493 of 494 SOC 2 reports from one automation firm were near-identical templates (Corporate Compliance Insights, 2026); [8] the AICPA's own journal warns audit quality is slipping (Journal of Accountancy, 2026).[7]

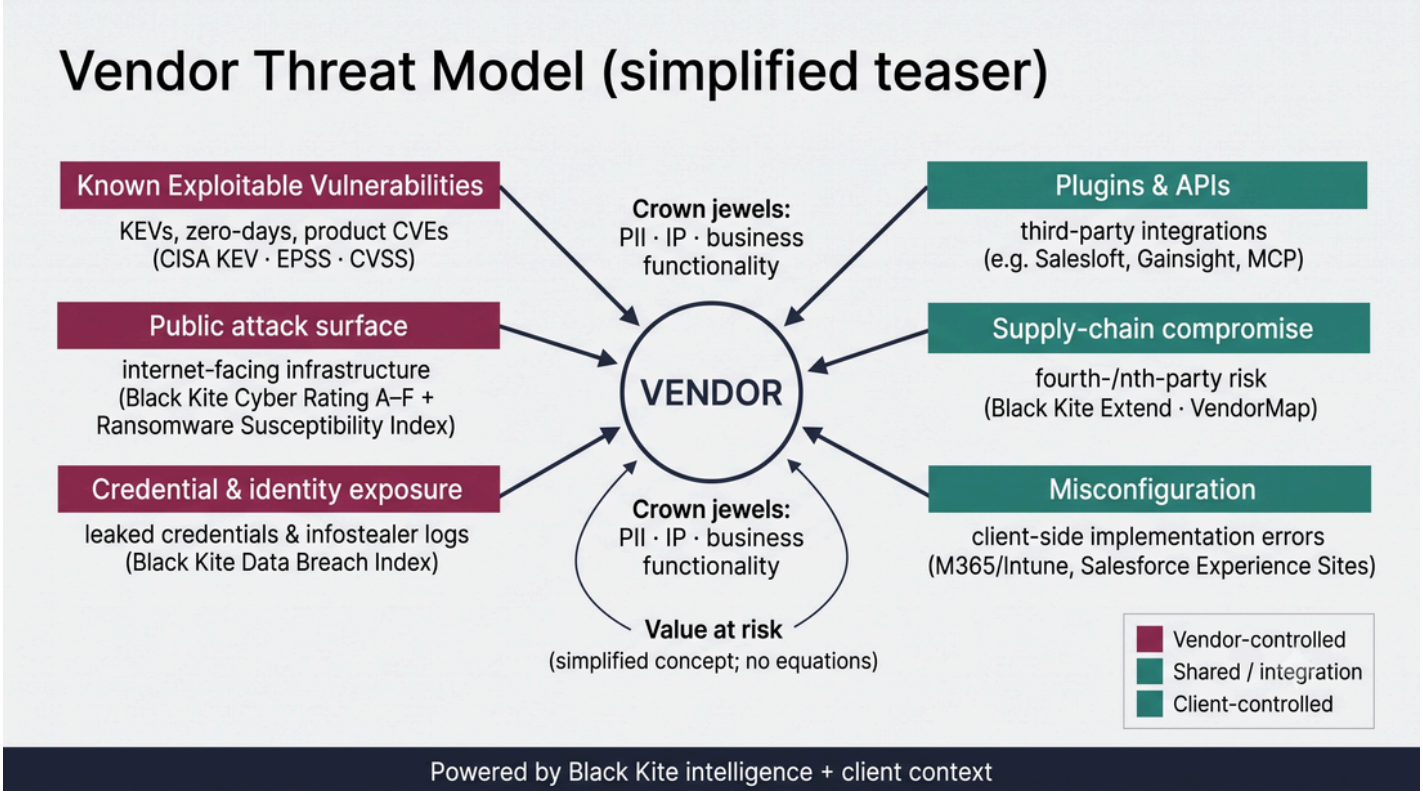
The cost of the gap is not theoretical. Change Healthcare was a HIPAA-covered organisation when attackers walked in through an internet-facing Citrix portal that had no multi-factor authentication, despite policy requiring it. The final figure filed with the US regulator: 192.7 million individuals notified — the largest healthcare data breach on record.[9] No questionnaire flagged the one portal that mattered.

> It is also possible to have AI auto answer questionnaires, providing the expected responses and producing the corresponding policy documents requested as supporting evidence, none which reflects the actual security controls that may be in place.

WHAT ACTUALLY DRIVES BREACH RISK: THE VENDOR THREAT MODEL

Breach risk is driven by what a vendor is doing in production today, across a handful of measurable signals — not by what they attested twelve months ago. A threat model makes those signals visible. Applied to your own stack, threat modelling is standard practice; the move this paper argues for is applying it to your supply chain, mapping each vendor's live exposure to the specific data and functions they can reach inside your organisation.

Elasticito builds that map as a Vendor Threat Model: a single view that pulls the vendor's external attack surface, known exploited vulnerabilities, exposed credentials, integration and API risk, fourth-party dependencies, and misconfiguration around one question: what can reach this vendor's crown jewels, and yours? It is powered by Black Kite intelligence combined with your business context, and it separates the risks the vendor controls from the ones you control. When a vulnerability like the MOVEit zero-day (CVE-2023-34362) is disclosed, the model shows at once which of your vendors run it, not which ones once filed a patching policy.



VALUE AT RISK, IN PLAIN WORDS (NO MATHS):

A vendor's value at risk is simply how much of your crown jewels they can reach multiplied by how likely they are to be compromised. You do not need an equation to act on it — you need to know which vendors can hurt you most and which are most likely to be hit. The Vendor Threat Model answers both.

WHAT THE PAPERWORK PROVES VS. WHAT ATTACKERS EXPLOIT

WHAT YOU'RE SHOWN	WHAT IT ACTUALLY PROVES	WHAT IT DOES NOT PROVE	WHO CONTROLS THE GAP
SOC 2 Type II	An audit covered a 6–12 month look-back window, refreshed annually	That controls operate today, or that every critical system was in scope	Vendor
ISO 27001	An information-security management system exists (3-year cycle + annual surveillance)	Real-time control effectiveness or code-level vulnerabilities	Vendor
HIPAA / "compliant"	A statutory obligation applies	Nothing verifiable at procurement — the regulator investigates only after a breach	Vendor
Questionnaire response	The vendor answered on one day	Anything about the 364 days that follow	Shared
Integration / API grant	Access was approved at onboarding	That the token was ever rotated or revoked	Shared / client

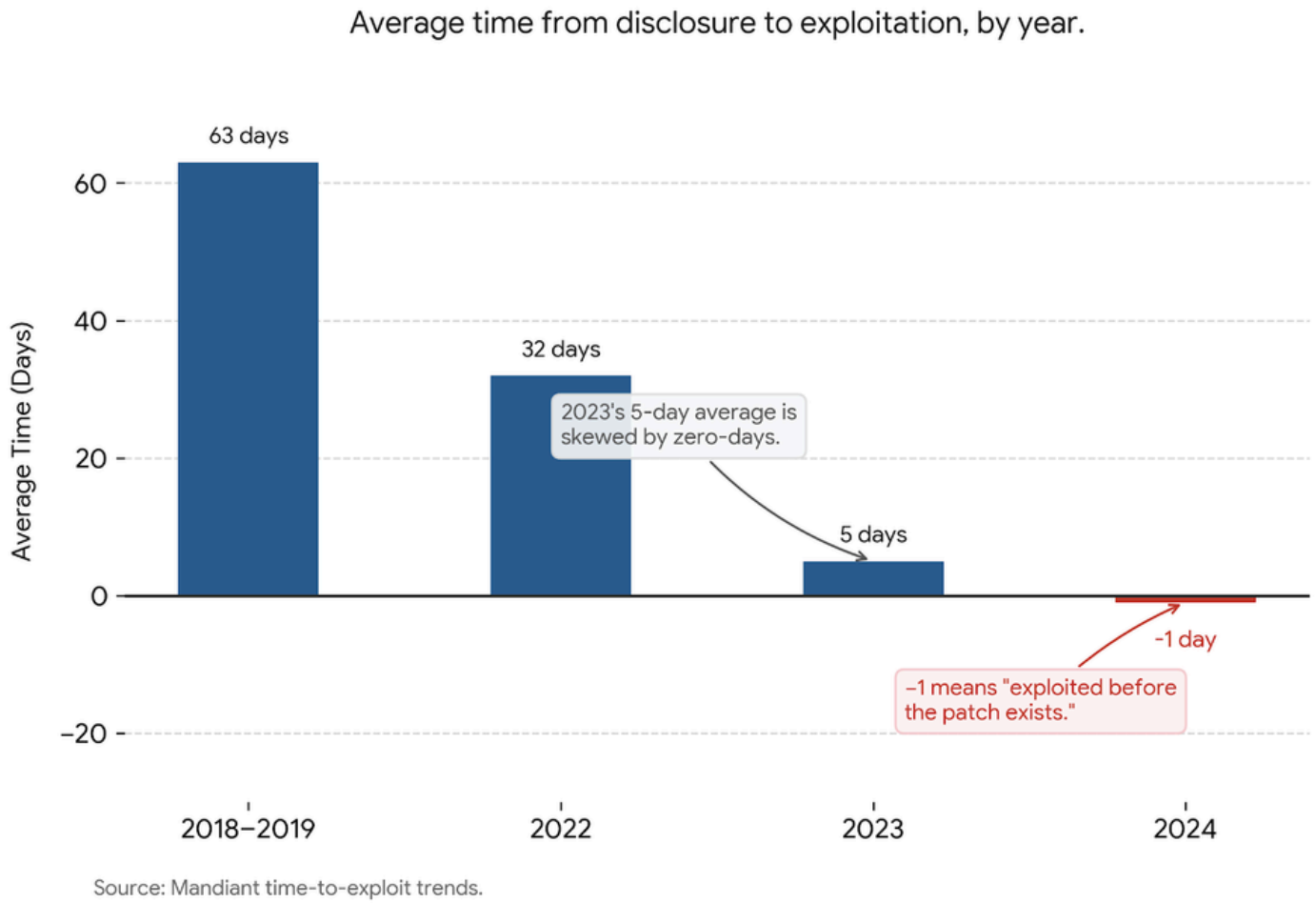
THE SIGNALS THAT PREDICT A BREACH

Ask an AI which vendors breach companies and it answers with categories: managed service providers, widely-shared SaaS platforms, file-transfer tools. The category is a clue, not a predictor. Four signals predict which vendors breach you next, and a vendor cannot fake any of them, because they are observed from the outside: unpatched known-exploited vulnerabilities, slow patching behaviour, exposed credentials and identity, and fourth-party sprawl. Each is measurable today. None appears on a questionnaire.

PATCHING BEHAVIOUR AND KEV EXPOSURE: WHAT THEY FIX, AND WHAT THEY LEAVE OPEN

The window between a vulnerability becoming public and attackers using it has collapsed, while vendor patching has not kept pace. Mandiant measured the average time-to-exploit falling from 63 days across 2018–2019, to 5 days in 2023, to minus-one day in 2024: attackers now exploit, on average, before the patch is public.[13]

Against that clock, vendor remediation is glacial: only 26% of CISA Known Exploited Vulnerabilities were fully remediated in 2025, down from 38%, while the edge-device patch median rose to 43 days.[14] The Cloud Security Alliance found **only 9% of organisations patch critical vulnerabilities within 24 hours — and those taking four to seven days reported a 97% rate of incidents involving known vulnerabilities**.[15]



Source: Mandiant time-to-exploit trends.

IDENTITY: THE UNMANAGED LAPTOP IS THE FRONT DOOR

The most common modern path into your data is not a flaw in the vendor's product — it is the vendor's identity. Stolen credentials, unrotated for months and never protected by MFA, are now an industrial-scale entry point. In 2024, the group UNC5537 used infostealer-harvested credentials to reach around 165 Snowflake customer tenants with no MFA enabled; 79.7% of the leveraged accounts had appeared in prior infostealer dumps, some valid since 2020.[16] A year later, attackers abused OAuth tokens from one SaaS integration to pull data from more than 700 organisations via the Salesloft Drift connection — Cloudflare, Palo Alto Networks and Zscaler among the victims. [17]Even security vendors were caught.

This is the pattern the original supply-chain breach established: attackers stole credentials from Target's HVAC vendor and pivoted to point-of-sale systems across 1,797 stores, exposing 110 million individuals.[18] The vector has only industrialised since — Microsoft reports that 80–90% of successful ransomware attacks originate from unmanaged devices.[19]

Questionnaire says: "All access requires MFA; credentials are rotated every 90 days." Reality shows: in the Snowflake campaign, credentials sat unrotated for 18 months with no MFA, and 165 tenants were breached (Mandiant, 2024).[16] In the 2026 Verizon DBIR, only 23% of third parties had fully fixed known MFA gaps on cloud accounts.[14]

FOURTH PARTIES: THE BREACH YOU NEVER CONTRACTED FOR

Your risk does not stop at the vendors you signed. It extends to their vendors — a layer that sits outside your register and outside every questionnaire you have ever sent. In June 2023, the BBC, British Airways and Boots had staff data exposed even though none of them used MOVEit; their payroll provider Zellis did, and attackers exploited a zero-day in Progress MOVEit to reach them.[20] The blast radius of that one file-transfer flaw reached roughly 2,773 organisations and 95 million individuals.[21] Yet only about one in three organisations collects any risk information on its fourth parties at all.[25]

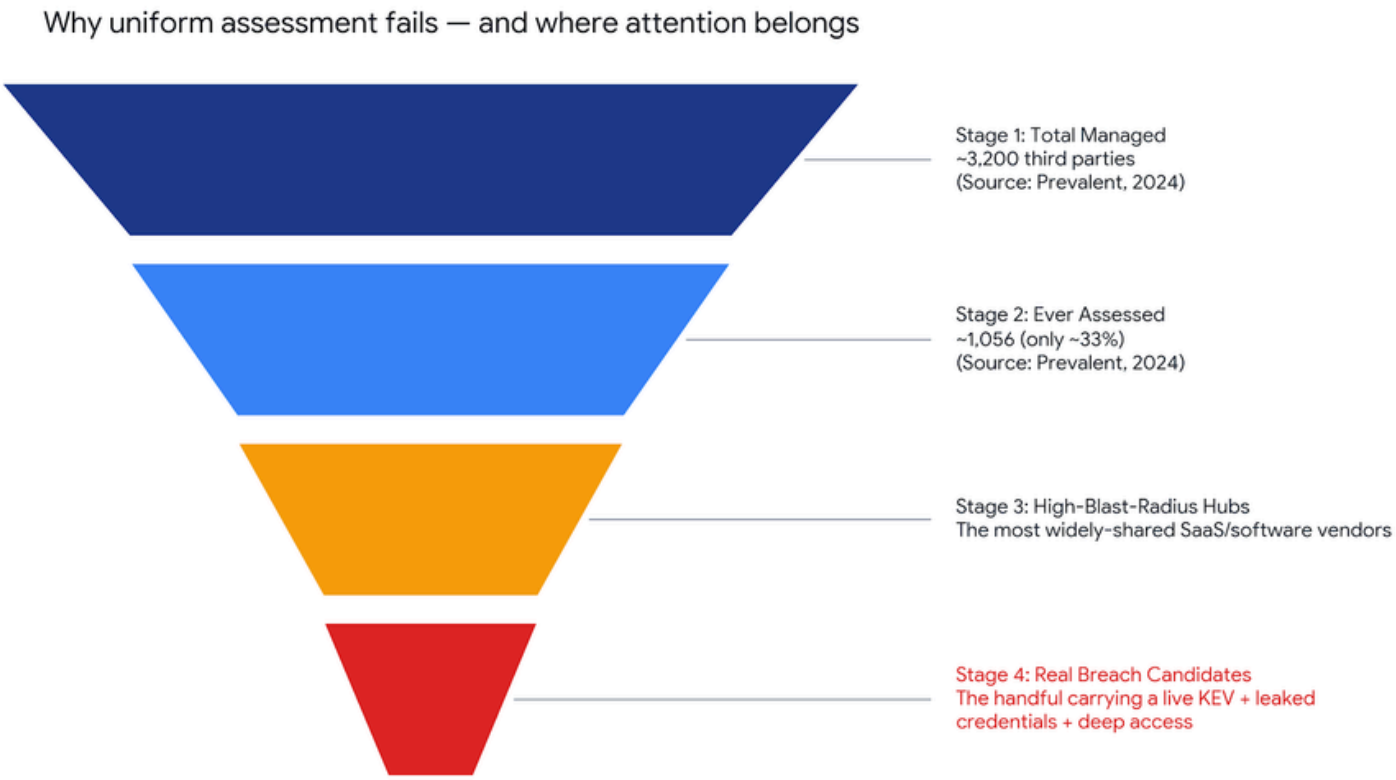
Liability, meanwhile, does not travel down the chain. Under UK GDPR Article 28(4), the original processor stays fully liable for its sub-processor's performance,[23] and DORA requires financial entities to map and oversee the whole sub-contracting chain for critical functions.[24] A breach you did not cause, through a vendor you never met, is still your problem.

Questionnaire says: "We vet all of our sub-processors." Reality shows: BA, the BBC and Boots were breached through the Zellis/MOVEit fourth-party chain — a vendor they never contracted with (The Register, 2023)[20] — and only about 1 in 3 organisations can see their fourth parties at all.[25]

FROM 400 VENDORS TO THE FEW THAT MATTER

Most of your breach risk concentrates in a small subset of suppliers, so the goal is not to assess every vendor equally — it is to find the few that can actually hurt you and watch them closely. Tier by blast radius: how much of your data and how many of your functions a vendor can reach, and how many of your downstream customers a breach of that vendor would touch. Contract value is a poor proxy; a small, deeply-integrated SaaS provider can carry more blast radius than your largest supplier.

The maths of attention is already against most teams. The average enterprise manages around 3,200 third parties but assesses only 33% of them,[25] and 94% of programmes admit they cannot assess all the vendors they would like to.[25] Spreading thin effort evenly across thousands of vendors guarantees the dangerous few get the same glance as the harmless many.



Concentration is what makes this work. One vendor breach now cascades to an average of 5.28 downstream organisations, the highest multiplier on record,[1] and just two file-transfer vulnerability clusters drove 63.5% of vulnerability-driven third-party breaches in 2024.[2] The most-shared vendors are measurably worse than the field: 70% carry a KEV against a ~54% platform-wide baseline.[2] Susceptibility is even rankable — organisations in the top band of Black Kite's Ransomware Susceptibility Index are 96× more likely to suffer a ransomware attack[28] than those in the lowest.

Regulators are pushing the same way. DORA Articles 28–31,[24] the UK FCA's Critical Third Parties regime,[29] and NIS2 Article 21[30] all require risk-based, proportionate treatment of suppliers — tiering by criticality, not uniform questionnaires.

HOW ELASTICITO SURFACES THE VENDORS MOST LIKELY TO BREACH YOU

Elasticito builds a live Vendor Threat Model so you see which vendors are exposed today, not which ones looked acceptable at last year's review. The method combines continuous, OSINT-based monitoring — powered by Black Kite intelligence — with your own business context about which data and functions each vendor can reach. No agent is installed on the vendor; nothing depends on the vendor self-reporting.

The engine grades each vendor A–F from 306 controls across 20 categories, built entirely from open-source intelligence.[31] When a high-profile vulnerability breaks, Black Kite FocusTags flag every exposed vendor within 24–48 hours[32] — carrying CVSS, EPSS exploitation probability, CISA KEV status and threat-actor attribution — so you act inside the exploit window, not at the next annual cycle. Black Kite catches leaked credentials and infostealer logs across 400+ OSINT feeds, including dark-web sources.[33] Black Kite Extend and VendorMap[34] discover fourth- to sixth-party dependencies with no vendor-supplied list required.

The silent window is long. Black Kite found that once a breach is detected, organisations wait an average of 117 days before disclosing it publicly[12] — and a supply-chain breach takes 267 days on average to contain.[12] Continuous validation closes that gap; the direction of travel is clear, with Gartner finding (2019) iterative monitoring delivers 2× better remediation and 1.5× earlier identification[11] than point-in-time review.

ANNUAL QUESTIONNAIRE VS. CONTINUOUS VENDOR THREAT MODEL

	ANNUAL QUESTIONNAIRE	CONTINUOUS VENDOR THREAT MODEL
Cadence	Once a year	Continuous; zero-days tagged in 24–48h
Evidence	Vendor self-report	OSINT-observed, 306 controls / 20 categories
Catches a new KEV?	At next review, if ever	Within the exploit window
Sees fourth parties?	No	To 6th-party depth, auto-discovered
Sees stolen sessions & credentials?	No	Across 400+ feeds, incl. dark web
Ranks by blast radius?	No	Yes — tier by reachable data + downstream impact

FREQUENTLY ASKED QUESTIONS

WHICH VENDORS ARE MOST LIKELY TO CAUSE A DATA BREACH?

The vendors most likely to cause a breach are the widely-shared software and SaaS providers carrying live, observable exposure: an unpatched CISA Known Exploited Vulnerability, corporate credentials in infostealer logs, and privileged access to customer data. Black Kite found 70% of the 50 most-shared vendors across the Forbes Global 2000 carry an unpatched KEV and 62% have leaked credentials, and that 26% of 2024 third-party breaches originated with software-services vendors — the largest single category. Contract size does not predict breach risk; technical exposure and blast radius do.

ARE VENDOR SECURITY QUESTIONNAIRES EFFECTIVE?

Questionnaires are useful for setting a baseline and recording contractual commitments, but they are weak as a standalone security control. They are point-in-time and self-reported: only 34% of TPRM professionals believe the answers they receive, and ENISA found that in 66% of supply-chain attacks the supplier did not even know how it was compromised. A questionnaire cannot detect a control that drifts the week after it is filed. Use it for the paperwork; use continuous monitoring for the risk.

WHAT IS CONTINUOUS RISK MONITORING?

Continuous risk monitoring is the ongoing, automated tracking of a vendor's real-world risk posture — vulnerabilities, leaked credentials, attack surface, and fourth-party exposure — rather than a single annual snapshot. In practice it means a new exploited vulnerability flags the affected vendors within 24–48 hours, not at the next review cycle. Gartner found (2019) iterative, continuous approaches deliver roughly twice the remediation effectiveness and identify risks 1.5× earlier than point-in-time due diligence.

DOES A VENDOR REMAIN MY RESPONSIBILITY IF THEIR SUB-PROCESSOR IS BREACHED?

Yes. Liability does not transfer down the supply chain. Under UK GDPR Article 28(4), your original processor remains fully liable for its sub-processor's performance, and DORA requires financial entities to map and oversee the entire sub-contracting chain for critical functions. Practically, the BBC and British Airways were exposed through the Zellis/ MOVEit chain despite never using MOVEit themselves — and the legal and reputational exposure was still theirs.

IS A SOC 2 OR ISO 27001 CERTIFICATE PROOF A VENDOR IS SECURE?

No. A SOC 2 Type II report attests that an audit covered a 6–12 month look-back window; ISO 27001 attests that a management system exists on a three-year cycle. Neither proves controls are operating today or that every critical system was in scope. The AICPA's own Journal of Accountancy has warned that SOC 2 audit quality is degrading. A certificate tells you an audit happened — not that the vendor is secure right now.

CONCLUSION: YOU CANNOT QUESTION YOUR WAY TO VENDOR SECURITY — YOU HAVE TO WATCH

A questionnaire records what a vendor claimed on one day; a breach happens on a different one, and the vendors most likely to breach you are visible right now in signals no form captures. Watch the full webinar here to see the live Vendor Threat Model and how Elasticito and Threatplane surface those vendors.

Works Cited

1. Black Kite, 2026 Third-Party Breach Report — https://blackkite.com/reports/third-party-breach-report-2026
2. Black Kite, 2026 Third-Party Breach Report press release — https://www.prnewswire.com/news-releases/black-kites-2026-third-party-breach-report-identifies-risk-concentration-as-the-primary-catalyst-for-global-cascading-failures-302701211.html
3. Cyentia / RiskRecon, The Problem with Security Questionnaires — https://blog.riskrecon.com/the-problem-with-security-questionnaires
4. Verizon, 2025 Data Breach Investigations Report — https://www.verizon.com/about/news/2025-data-breach-investigations-report
5. SecurityWeek, Verizon DBIR 2026: Vulnerability Exploitation Overtakes Credential Theft — https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/
6. ENISA, Threat Landscape for Supply Chain Attacks — https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
7. Journal of Accountancy, Promises of "fast and easy" threaten SOC credibility (2026) — https://www.journalofaccountancy.com/issues/2026/feb/promises-of-fast-and-easy-threaten-soc-credibility.html
8. Corporate Compliance Insights, SOC 2 Is Broken: What the Delve Scandal Shows (2026) — https://www.corporatecomplianceinsights.com/soc-2-broken-delve-scandal-shows/
9. HIPAA Journal, Change Healthcare cyberattack — https://www.hipaajournal.com/change-healthcare-responding-cyberattack/
10. Gartner, More Than Eight in 10 Organisations Discover Third-Party Risks After Due Diligence (2019) — https://www.businesswire.com/news/home/20190815005199/en/Gartner-Says-More-Than-Eight-in-10-Organizations-Discover-Third-party-Risks-After-Due-Diligence-Period
11. Help Net Security, A more proactive approach to third-party risk management (Gartner, 2019) — https://www.helpnetsecurity.com/2019/08/20/approach-to-risk-management/
12. Black Kite, Silent Breaches Lurking Within Interconnected Ecosystems (2025) — https://www.globenewswire.com/news-release/2025/02/11/3024215/0/en/Black-Kite-Research-Exposes-The-Silent-Breaches-Lurking-Within-Interconnected-Ecosystems.html
13. Mandiant / Google Threat Intelligence, Time-to-Exploit Trends 2023 — https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023
14. Tenable, Key Findings from the Verizon 2026 DBIR — https://www.tenable.com/blog/key-findings-from-the-verizon-dbir-2026
15. Cloud Security Alliance, Over 80% of organisations that miss the 24-hour patch window report incidents (2026) — https://cloudsecurityalliance.org/press-releases/2026/06/02/over-80-of-organizations-that-miss-24-hour-patch-window-report-security-incidents-involving-known-vulnerabilities
16. Mandiant / Google, UNC5537 Snowflake data theft and extortion — https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
17. Mandiant / Google, Data theft from Salesforce via Salesloft Drift — https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift
18. Krebs on Security, Target Hackers Broke in Via HVAC Company — https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
19. Microsoft, Digital Defense Report 2023 — https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2023
20. The Register, British Airways, Boots and BBC hit by MOVEit breach (2023) — https://www.theregister.com/2023/06/05/british_airways_boots_moveit/
21. Emsisoft, Unpacking the MOVEit breach: statistics and analysis — https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/
22. Black Kite, Solving nth-party cyber risk press release — https://blackkite.com/press-releases/black-kite-gives-organizations-the-power-to-solve-nth-party-cyber-risk-with-new-cyber-third-party-risk-management-bridge/
23. UK GDPR Article 28 — https://www.legislation.gov.uk/eur/2016/679/article/28
24. Digital Operational Resilience Act, Article 28 — https://www.digital-operational-resilience-act.com/Article_28.html
25. Prevalent, 2024 Third-Party Risk Management Study — https://www.prevalent.net/content-library/2024-third-party-risk-management-study/
26. Venminder, State of Third-Party Risk Management 2025 — https://www.venminder.com/blog/highlights-state-of-third-party-risk-management-2025-survey
27. SecurityScorecard, 2025 Global Third-Party Breach Report — https://securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/
28. Black Kite, Ransomware Susceptibility Index — https://blackkite.com/platform/ransomware-susceptibility-index
29. UK FCA, PS24/16 Critical Third Parties — https://www.fca.org.uk/publications/policy-statements/ps24-16-operational-resilience-critical-third-parties-uk-financial-sector
30. NIS2 Directive (EU) 2022/2555 — https://eur-lex.europa.eu/eli/dir/2022/2555/oj
31. Black Kite, Knowledge Base Controls (306 controls / 20 categories) — https://help.blackkitetech.com/hc/en-us/articles/360009413120-Knowledge-Base-Controls
32. Black Kite, FocusTags for High-Profile Incidents — https://help.blackkitetech.com/hc/en-us/articles/14127474253340-How-does-Black-Kite-apply-FocusTags-for-High-Profile-Incidents
33. Black Kite, Data Breach Index Overview (400+ feeds) — https://help.blackkitetech.com/hc/en-us/articles/4621905814556-Data-Breach-Index-Overview
34. Black Kite, nth-Party Visibility / Extend — https://blackkite.com/platform/nth-party-visibility

elasticito
risk & threat specialists

Let Elasticito's team of cyber risk experts handle your vendor risk assessments

We have not yet come across a cyber risk or information security team that is not under-resourced and has time on their hands. Assessing third parties for the cyber risks that they might pose to your business is a critical, but additional task to add to the already full job-list of security and risk teams.

We combine the use of world-class technology tools and our team of cyber risk specialists to streamline the assessment and monitoring of vendor cyber risk assessments so that our customers can focus on delivering value back to their business stakeholders through accurate and up to date vendor cyber risk metrics.

+44 (0) 3330428268 information@elasticito.com www.elasticito.com