Recorded Future® | DATA SHEET

Third-Party Risk

Detect third-party cyber threats before they disrupt business operations, expose data, or damage trust

Third-party risks keep increasing

Security and GRC teams are responsible for monitoring hundreds to thousands of third-party relationships, but visibility into risk is often self-reported, point-in-time, and disconnected from real-world threats. Assessment cycles leave long gaps where new issues and active attacks go undetected.

When incidents happen, it's difficult to quickly see which vendors are affected, how critical they are to the business, and what to do next – slowing response and increasing risk.

Why Recorded Future?

Recorded Future Third-Party Risk combines security ratings with threat intelligence to show which of your vendors pose material risk to your business today. Instead of relying on point-in-time questionnaires and surface-level scores, security and GRC teams get a clear view of which vendors are putting the business at risk and how to reduce exposure.

You get visibility into each vendor's external security posture, which issues matter, and when a third-party or key fourth-party is tied to breaches, ransomware activity, or dark web exposure. This makes it easier to prioritize vendors and findings, and detect incidents before formal notification.

Understand vendor-specific risk

Gain a consistent, evidence-based understanding of cyber risk across your third-party ecosystem with standardized ratings and clear insight into weaknesses and exposures that could be exploited.

Detect incidents before vendors disclose

Identify breaches and campaigns early instead of being kept in the dark or waiting for formal notification. Continuous monitoring for ransomware extortion site mentions, dark web exposure, credential leaks, and breach indicators drives timely alerts so you can quickly scope exposure and respond.

Prioritize what actually matters

Focus limited resources on vendors and issues most likely to impact your business, rather than low-impact hygiene fixes. Issues are prioritized by severity and impact, and vendor-specific threat intelligence can be layered on to identify active threats.

Scale monitoring without scaling headcount

Monitor more vendors with the same team. Extend coverage across your vendor portfolio with automated discovery, security posture scoring, and intelligence collection. Integrated workflows and questionnaires reduce manual research, duplication, and spreadsheet-driven tracking.

Make vendor risk easy to explain

Turn complex vendor risk into clear, actionable insights for stakeholders. Executive-ready summaries show top risks, key incidents, and trends across vendors and categories. Vendor comparisons and portfolio views support executive and board conversations.

> **"Threat intelligence-driven security is vital. It's the eyes and ears of a security team. You can't protect yourself against what you don't know.**
>
> **A couple times now, Recorded Future has alerted us to something prior to the third-party vendor. That's huge when we're trying to protect our data."**
>
> *Natalie Salisbury - Strategic Threat Intelligence Analyst, Novavax*

Third-party risk management is an intelligence operation. Vendor-specific threat intelligence is the critical input for understanding when third parties have been compromised and how that impacts your business.

Top benefits:

- **Quick detection of third-party incidents:** Detect vendor breaches and ransomware events days or weeks before formal notification.
- **Cut manual vendor research:** Replace hours of manual investigation and spreadsheet work with on-demand vendor profiles and reports.
- **Confident go/no-go vendor decisions:** Use objective risk scores and evidence to support third-party decisions.
- **Cover more of your portfolio:** Extend monitoring beyond tier-1 vendors, without increasing noise or headcount.
- **Strengthen board and regulator conversations:** Show measurable improvements in third-party risk with context-rich data.

Who it's for and how it works:

For teams responsible for third-party cyber risk across large vendor portfolios, Recorded Future Third-Party Risk provides continuous monitoring that ties externally observed security posture evidence to real-world threat activity.

- **Map risk:** Uncover exposures and weaknesses across your vendor ecosystem.
- **Detect early:** Flag vendor-linked threat activity as it emerges.
- **Act fast:** Prioritize remediation and response, document evidence, and report outcomes.

Feature	Description
Asset-based cyber risk ratings	External, independently validated ratings across nine security domains with asset value built in for effective prioritization.
Real-time threat intelligence overlay	Ransomware, dark web, and breach insights layered onto vendor profiles to highlight active threats and compromises.
High-impact third-party alerts & playbooks	Portfolio-wide alerts for high-impact vendor events (e.g., breaches, extortion site mentions, credential leaks) with recommended response guidance and remediation tracking.
Third- and fourth-party mapping	Visualize cyber risk across your third- and fourth-party ecosystem, including technology dependencies and concentration risk.
Risk priority matrix & vulnerability exposure	Combines issue severity, asset value, and exploitability to show which vulnerabilities and vendors matter most right now.
Vendor action plans and collaboration portal	Select issues to share with third parties using the collaboration portal, and track remediation status for each vendor.
Executive-ready reports & comparisons	One-click summaries and comparisons that non-technical stakeholders can understand and use in vendor, M&A, and board discussions.
GRC & workflow integrations	Integrate with platforms like ServiceNow and Archer to embed intelligence into existing TPRM and procurement workflows.
AI-powered assessments & questionnaires	Automate questionnaire generation and vendor response analysis to shrink assessment cycles from weeks to minutes.