

Third-Party Incident Response Service

Many organizations struggle to get timely information about data breaches affecting their supply chains. Delays between a vendor incident and your own risk identification, analysis and mitigation leave your organization exposed to operational disruptions, fines and customer losses. However, manual event notification processes only slow risk assessment and remediation at a time when speed is essential.

Fast, Programmatic Breach Response

The Prevalent™ Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.

Delivered either as a managed service or as a self-service platform, the solution helps security teams automate the critical tasks required to quickly discover, score and remediate risks from vendor data breaches.

Key Benefits

- Automate the collection and analysis of vendor incident information, enabling your team to focus on risk mitigation
- Speed critical response time by enabling third parties to proactively submit event notifications and updates
- Be well prepared for board and executive questions regarding the impact of supply chain incidents
- Demonstrate proof of your third-party breach response plan with auditors and regulators

Package Options

	Self-Service Your team manages assessment collection and analysis.	Managed Service Prevalent manages assessment collection.
# of Vendors to Manage	Unlimited	Unlimited
# of Vendors to Assess	Unlimited	Up to 2,500
Frequency of Assessments	Unlimited	4x per year

Prevalent offers flexible options to accommodate your organization's budget and resources.

Key Features



Unlimited Vendor Onboarding and Management

Build a centralized vendor repository using an API connection to existing tools, a comprehensive intake form, or bulk upload from a spreadsheet. Requires Prevalent Platform Essentials.



Flexible Collection Options

Manage an unlimited number of vendors and assessments yourself, or have Prevalent experts perform incident response collection on your behalf.



Assessment Scheduling & Management

Monitor real-time questionnaire completion progress, assign risk owners, and set automated chasing reminders to keep surveys on schedule.



Incident Management Assessment

Leverage Prevalent’s continuously updated and customizable event and incident management assessment questionnaire to determine the impact of incidents affecting your vendors.



Risk Scoring

Quickly quantify third-party risk levels with consolidated views of risk ratings, counts, scores, and flagged responses for each vendor.



Proactive Vendor Assessments

Enable third parties to proactively report incidents using a standardized event reporting assessment.



Automated Response Actions

Leverage a library of workflow rules to trigger automated playbooks that enable you to act on risks according to their potential impact to the business.



Central Risk Register

Normalize, correlate and analyze information across assessment results for unified reporting and remediation.



Built-in Remediation Guidance

Get guidance from built-in remediation recommendations to reduce risk.



Central Risk Reporting Dashboard

Identify, alert and communicate exceptions to common behavior with built-in report templates.



Data & Relationship Mapping

Identify relationships between your organization and third parties to visualize information paths and determine at-risk data.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors and suppliers throughout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.