PREVALENT®

Cyber & Business Monitoring Service

IMMEDIATE, ACTIONABLE INSIGHTS INTO VENDOR DATA AND BUSINESS RISKS

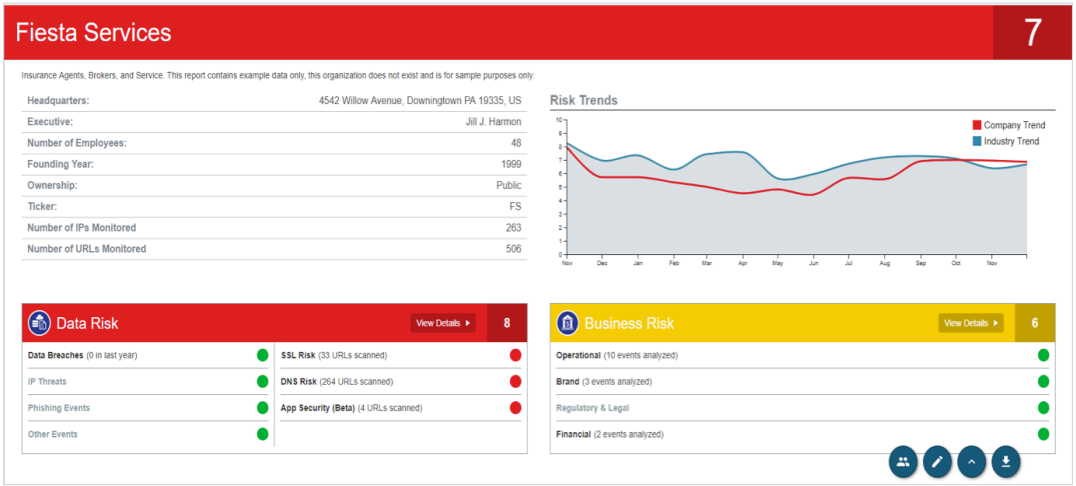
Vendors represent a significant attack surface that cyber criminals can exploit to gain access to your network. While periodic assessments are essential to provide an understanding of how vendors govern their information security and data privacy programs at a point in time, how do you validate vendor responses to surveys and gain more frequent, unbiased insights into their potential cyber vulnerabilities or relevant business risks that can negatively impact your business?

Gain a Strategic View of Vendor Information Security Risks

Delivered as part of the industry's only purpose-built, unified platform for third-party risk management, the cloud-based Prevalent Cyber & Business Monitoring Service provides both snapshot and continuous vendor monitoring with immediate notification of high-risk issues, prioritization, and remediation recommendations. Data security and business risk monitoring ensures that you are looking beyond tactical vendor health and gaining the strategic business view that drives a vendor's overall information security risk.

Key Benefits

- Improves visibility by filling the gaps between point-in-time assessments
- Provides a holistic view of both vendor data and business risks
- Delivers a comprehensive, trusted and transparent scoring methodology
- Offers prescriptive guidance and remediation recommendations
- Helps teams to focus on and prioritize the most significant risks



The Prevalent integrated Third Party Risk Management Platform uniquely combines cyber and data threat intelligence with business-level risks for an optimal view of your vendors' risk posture.

Toll Free: (877) PREVALENT • **info@prevalent.net** • **www.prevalent.net**

Cyber Threat Intelligence

Prevalent combines native vulnerability scanning with multiple external sources for cyber threat intelligence, including from internet sensor networks, global threat databases, dozens of collaborating security partners, and anti-virus users. In tracking more than 27 billion URLs, four billion IPs, 600 million domains, and all public IPv4 addresses – along with collecting data on IP threats, phishing events, and data breaches globally – Prevalent delivers deep insights into the cyber risks of your vendors.

Business Intelligence

Prevalent implements an industry-unique combination of technology, data analytics, and human analysts to deliver business risk assessments. Prevalent analysts collect, categorize, and score based on rules derived from a combination of methods including commercial due diligence, financial analysis, and cyber threat intelligence. With backgrounds in national security and cyber threat intelligence, Prevalent cyber analysts provide geopolitical context and fluency in seven languages.

Key Features

AI-Powered Media Analytics Platform: Analysts partner with the industry's leading AI-powered media analytics platform to collect and monitor open-source intelligence on vendors from 450,000 global sources.

OSINT Collection: Prevalent employs a proprietary-based OSINT collection method to collect business intelligence information, including corporate demographic information via API used for inherent risk scoring.

Risk Scale: Each element is scored on a scale of 0 (low risk) to 10 (high risk) and derived from risk events scored low, medium, or high.

Customizable Risk Relevance Rules & Weights: Set importance of risk types to reflect the nature of the service provided and assessed.

Inherent Industry Risk: For vendors with sparse data, industry risk data is used as a proxy for inherent risk of the vendor.

Alert Notifications: Tailor alerts based on risk types, thresholds, and vendors or portfolios of vendors managed.

Stakeholder-specific Reporting: Create multiple notification groups for different internal stakeholders, including data breach alerts for the executive team and vendor-specific alerts for assessors, in multiple formats including email, Excel, pdf, or in the application itself.

Filtering: Filter and sort on risk types, score, date, vendor, criticality, and group.

Tiering: Categorize vendors by risk tier enabling prioritization by criticality and severity.

Remediation with Actionable Recommendations: Identify risks and share results with vendors via PDF export or direct sharing links. SSL, DNS, and AppSec risks have remediation recommendation associated with each event.

Integrated Monitoring & Survey Scores: Risk scores at the vendor- and event-level are used for alerting to complement survey-based risk scoring for a complete 360-degree view of vendor-based risks.

The Prevalent Third Party Risk Management Platform

The Cyber & Business Monitoring Service is part of Prevalent's integrated third-party risk management platform, a unified solution that provides a 360-degree view of vendors risks. With integrated data from assessments and ongoing monitoring, organizations will improve the reliability of risk scores while simplifying compliance, reducing vendor-based risks, and improving efficiency of third-party risk management.

Prevalent, "leads the pack with a third party risk management platform... best for companies that want one TPRM tool with integrated cyber-risk ratings."

The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018.
Nick Hayes and Trevor Lyness.
November 13, 2018