Prevalent

Prevalent Third-Party Risk Management Platform v3.19

Prevalent Vendor Threat Monitor v2.2

New and Enhanced Features

The Prevalent Third-Party Risk Management Platform is a SaaS solution that enables customers to automate the critical tasks required to manage, assess and monitor their third parties across the entire vendor life cycle. The solution combines the following integrated capabilities:

- Automated onboarding and offboarding
- Profiling, tiering and inherent and residual risk scoring
- Standard and custom risk assessments with built-in workflow, task and evidence management
- Continuous vendor threat monitoring and business risk intelligence from a multitude of sources
- Compliance and risk status reporting by framework or regulation
- Remediation management with built-in guidance

Prevalent Platform v3.19 introduces important new capabilities to deepen vendor intelligence insights, improve visibility, and further automate workflows.

Along with the Platform, **Vendor Threat Monitor v2.2** introduces significant new enhancements to business risk intelligence to enrich risk-based decision-making.

New Features Highlights

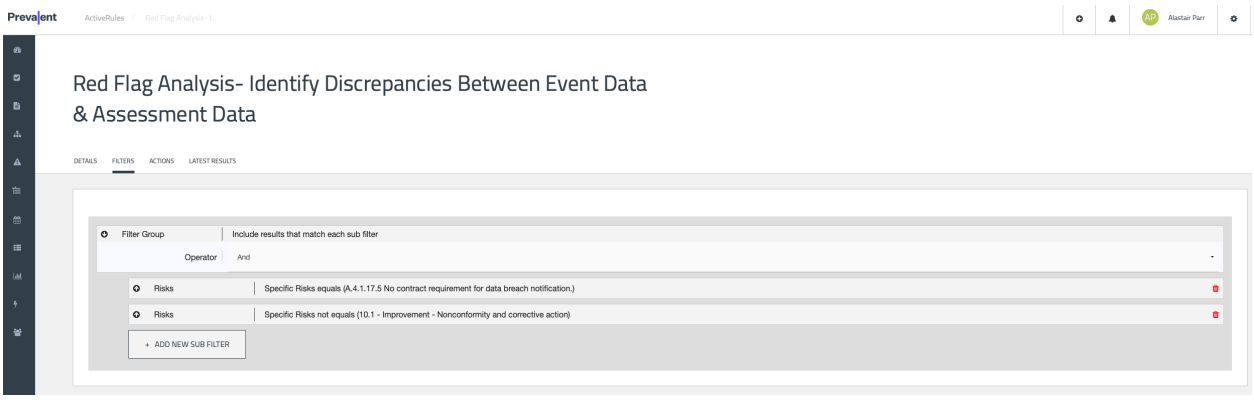
Unified Risk Register Correlates Cyber and Business Insights with Assessment Findings for Real-Time, 360-Degree Risk Visibility

While point-in-time, internal control assessments are central to third-party risk management, a lot can happen between these (usually annual) assessments. Business and cyber intelligence feeds can help to bridge these gaps and keep you out in front of emerging vendor risks. However, the value of monitoring a vendor is severely limited if you can't correlate their monitoring data and scores with their annual assessment results. And that's where other TPRM solutions typically drop the ball.

Prevalent Platform v3.19 solves this problem with a unified risk register that aggregates and correlates continuous, real-time monitoring data with the assessment results for each of your vendors. With intelligent rules and automation, the Prevalent TPRM Platform transforms vendor cyber and business event data into actionable risks that are recorded in the register. For example, with the Prevalent Platform, you can correlate a vendor's assessment responses revealing weak password management or patch management practices with associated vulnerabilities, breaches or leaked credentials on the dark web. This makes it easy to not only identify and prioritize issues, but also take clear steps for risk remediation.

info@prevalent.net
prevalent.net
Tel: 877.773.8253

Whether you combine Prevalent's vendor risk assessment data with intelligence from Prevalent Vendor Threat Monitor or another supported solution, our unified risk register makes it easier than ever to view, understand and act on risk. Actions can include sending notifications, creating tasks or flags to track remediation, or elevating risk scores to bring real threats into focus. You can do all of this either manually or automatically via rule-based triggers.

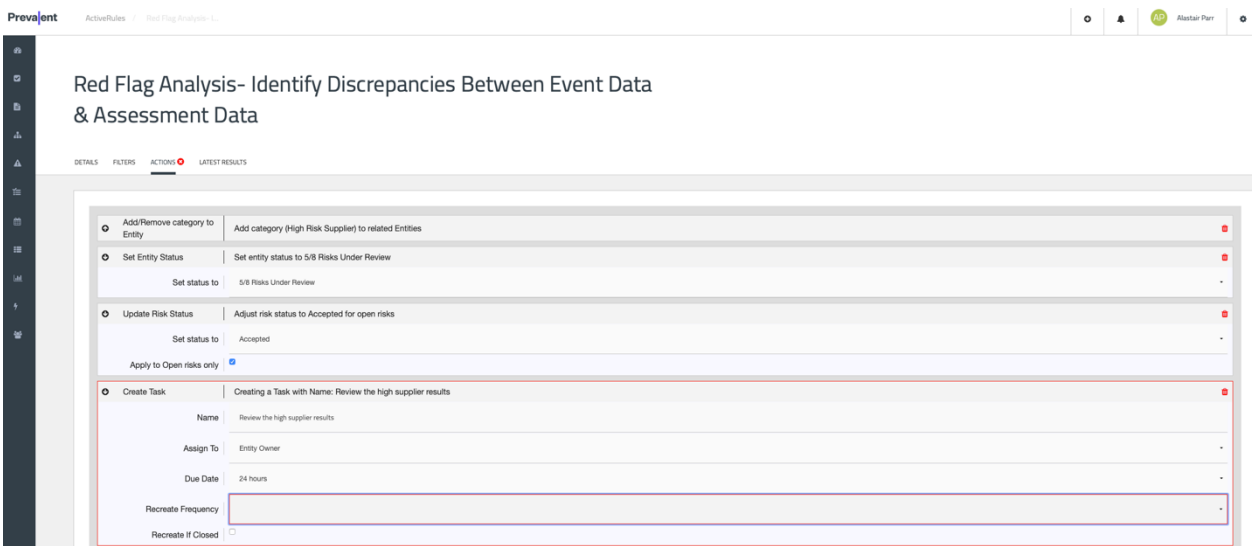


Prevalent's unified risk register enables organizations to correlate findings between assessments and monitoring to automate risk reviews, reporting and response.

New ActiveRules and Automation Playbooks Streamline Risk Response Tasks

Many organizations struggle with spreadsheet-driven vendor assessment processes that require dozens of manual steps to analyze and act on responses. While most TPRM solutions serve to simplify the process, many don't offer rules to further automate risk identification and management.

With Prevalent Platform v3.19, customers can leverage new ActiveRules capabilities for triggering risk response actions based on "If This, Then That" criteria for specific entities and risks. ActiveRules can automate a broad range of onboarding, assessment and review tasks – such as updating vendor profiles and risk attributes, sending notifications, and/or activating workflows. They also run perpetually to dynamically update the TPRM environment as new events and risks emerge.



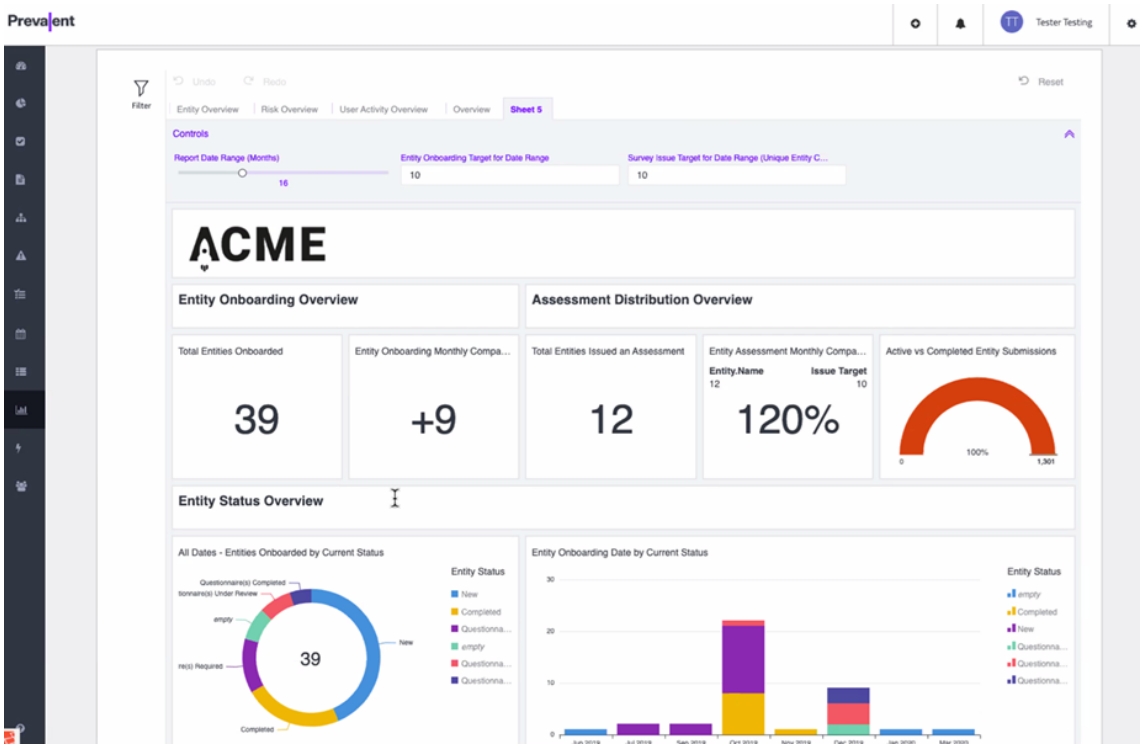
ActiveRules simplify and speed workflows for common risk response tasks.

To deliver a fast time-to-value, Prevalent has packaged sets of ActiveRules into a series of Automation Playbooks that enable customers to address common risk management scenarios.

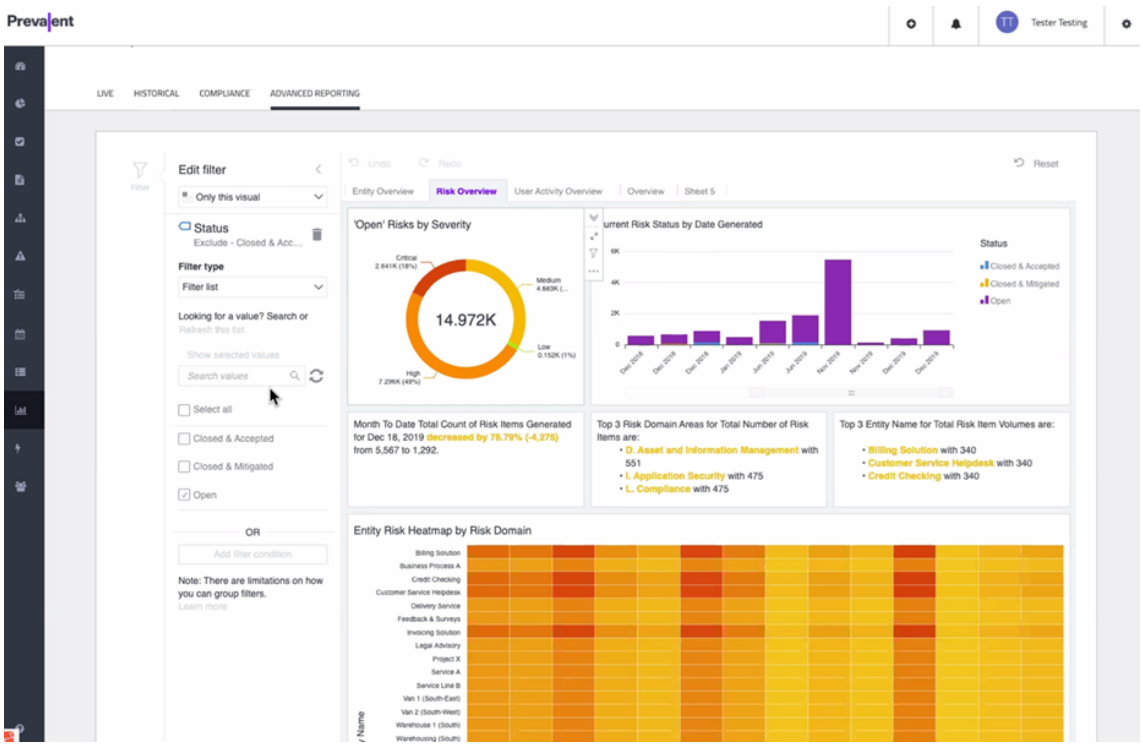
Machine Learning Brings More Clarity to Enterprise Reporting and Analytics

As threats become increasingly sophisticated, so too is the need for sophisticated reporting to better interpret risk and enable response activities. That's where machine learning comes in.

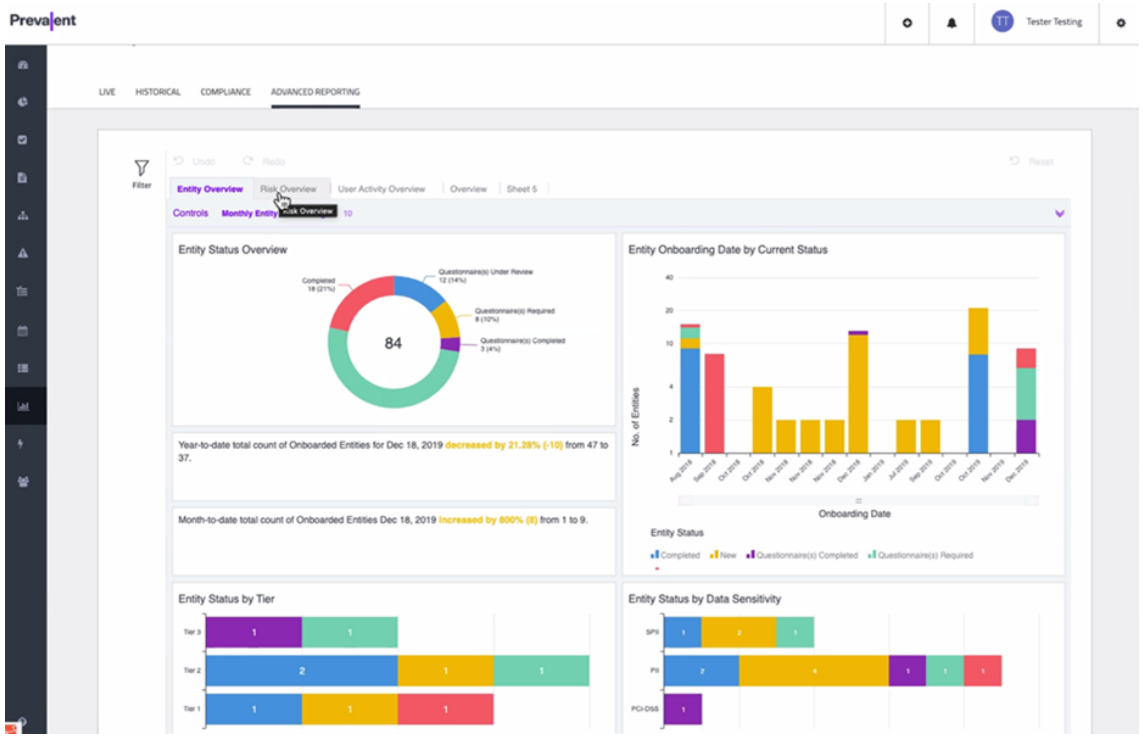
Prevalent Platform v3.19 introduces significant reporting enhancements that incorporate machine learning analytics to identify exceptions in common behavior – for example outliers across assessments, tasks, risks, etc. – that could warrant further investigation. Built directly into the Prevalent Platform, the new capability also includes templates for communicating exceptions arising from threat and business monitoring, SLAs and user behavior tracking, and other activities.



Review the onboarding process and your assessment metrics against targets.



Analyze risk data from assessments, threat monitoring, and events in one consolidated report, including machine learning insights of noteworthy trends.



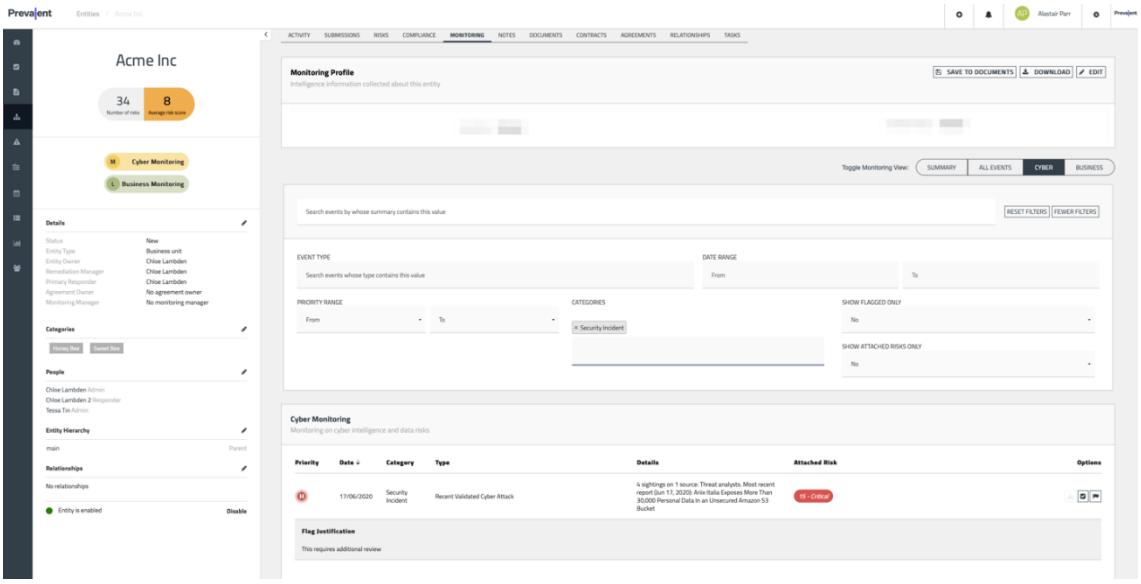
Review the profiling and tiering results of your third parties based on common attributes and categories.

Enhanced Business Risk Intelligence Sources Add Context to Continuous Monitoring

Prevalent Vendor Threat Monitor (VTM) is the only continuous monitoring solution to truly integrate business and cyber risk monitoring for more informed decision-making. Business risk monitoring complements cyber monitoring with both qualitative and quantitative insights into vendor financial information, legal actions, executive leadership changes, violations on OFAC lists, and more – all of which provide early indicators of potential cybersecurity or compliance issues.

Vendor Threat Monitor v2.2 includes vastly expanded business monitoring capabilities that collate information from over 567,000 new sources, including:

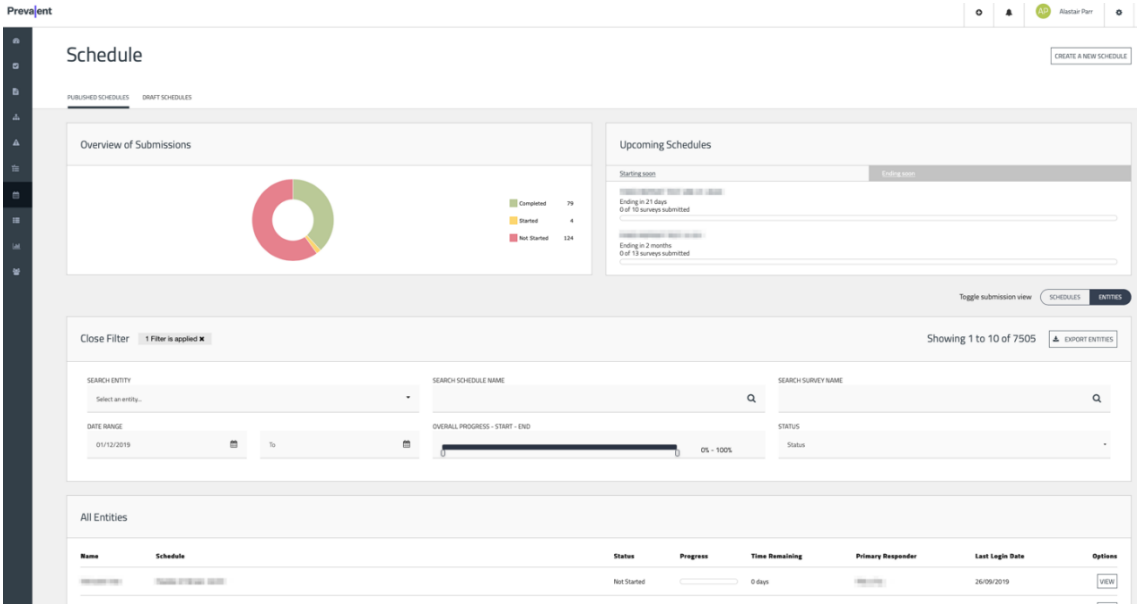
- Data breach sites
- Corporate sites
- Regulatory portals
- Review websites
- Job boards
- Trade publications
- Industry sites
- News feeds
- Social media



With Prevalent Vendor Threat Monitor, you can automatically associate events with risks, create tasks for further risk review, get remediation guidance, and generate reports for communicating progress.

Enhanced Schedule Filtering Simplifies Assessment Cadences

Scheduling can become more complex as the number of vendors requiring assessments increases. Prevalent Platform v3.19 has improved the user experience in the Define Schedules page, making it easier to review any emerging, ongoing and completed schedules. Customers are now able to sort and filter their schedules by a range of fields to for insights into which vendors to chase or what work is upcoming. This data can also be exported into an Excel file for offline analysis.



Apply filters to identify exactly which third party or entity requires chasing or is due to complete an assessment in a given timeframe.

Additional Enhancements

Please see the Release Notes on the Prevalent Customer Portal for a complete list of all enhancements in Platform v3.19 and VTM v2.2.

About Prevalent

Prevalent takes the pain out of third-party risk management. Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties. Our customers benefit from a flexible, hybrid approach to TPRM, realizing a rapid return on investment. Regardless of where they start – our Global Vendor Intelligence Network, Vendor Risk Assessment Services, or our award-winning Third-Party Risk Management Platform – we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time. To learn more, please visit www.prevalent.net.