Prevalent Third-Party Risk Management Platform

Versions 3.15 & 3.16

Prevalent Vendor Threat Monitor

Version 2.0

New and Updated Features

The Prevalent Third-Party Risk Management Platform is a unified solution that combines automated standardized vendor risk assessments, workflow, remediation management, and continuous threat monitoring across the entire vendor life cycle to deliver a 360-degree view of vendor risks. With the platform, customers can:

- Automate the end-to-end process of collecting and analyzing vendor surveys, speeding and simplifying assessments, compliance, and due diligence review.
- Monitor vendors continuously, providing deep cyber and business threat visibility to inform risk assessments.
- Enable the sharing of completed standard vendor surveys and associated evidence to accelerate risk remediation efforts.
- Enable categorization of vendors based on risk and organizational importance, prioritizing remediation.
- Deliver clear reporting beyond a score, tying risks to business outcomes and helping to make better risk-based decisions, prove compliance, and prioritize resources.
- Meet industry standards and ensure third-party risk management regulatory compliance targets for cyber risk, InfoSec, and data privacy.
- Centralize TPRM functions, delivering a single view that provides single repository for effective reporting to satisfy audit and compliance requirements.
- Utilize a consistent, repeatable, proven methodology, enabling a scalable, more mature vendor risk management program.

Platform versions 3.15 and 3.16 introduce exciting new capabilities to enhance assessment scheduling, enable integration with additional solutions, improve workflow and automation, and offer new licensing options. Vendor Threat Monitor (VTM) 2.0 introduces new cyber scanning inputs to increase the depth of cyber risk insights. Please click on one of the links below to review specific features or continue reading to examine all new capabilities available in these releases:

New Features Highlights

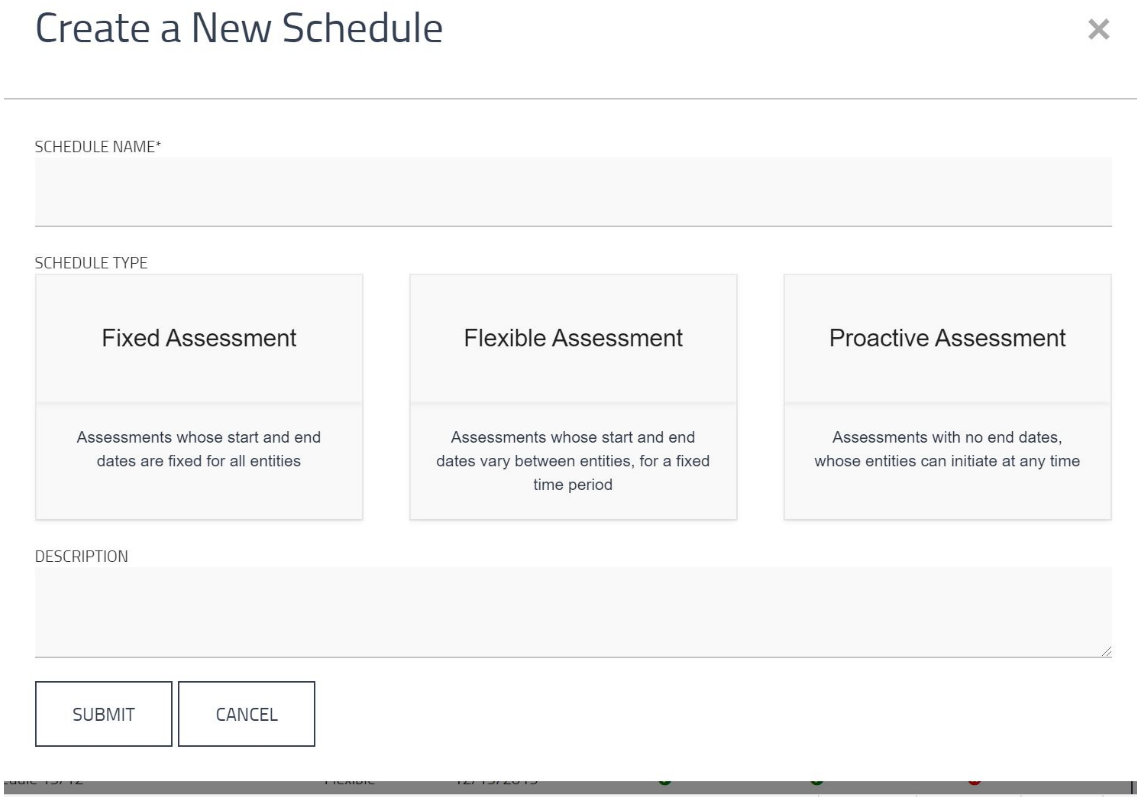
Scheduling Enhancements Add Flexibility to Assessments

Assessment scheduling often brings different workflow requirements, depending on whether you're assessing a new vendor for the first time or are introducing a new assessment to an existing third party. When multiple assessment types are needed, you must have the flexibility in scheduling assessments to fit your specific workflow needs. The Prevalent Platform version 3.15 introduced two new schedule types to streamline the process:

- **Proactive assessment scheduling** where the vendor can complete an assessment when they choose, with no specific deadline or timeframe.

- **Flexible assessment scheduling** where an entity must fill out the assessment within a designated time frame at the time the entity is added to a schedule.

For a representation of the new schedules, please see the screenshot below.



Create a New Schedule

SCHEDULE NAME*

SCHEDULE TYPE

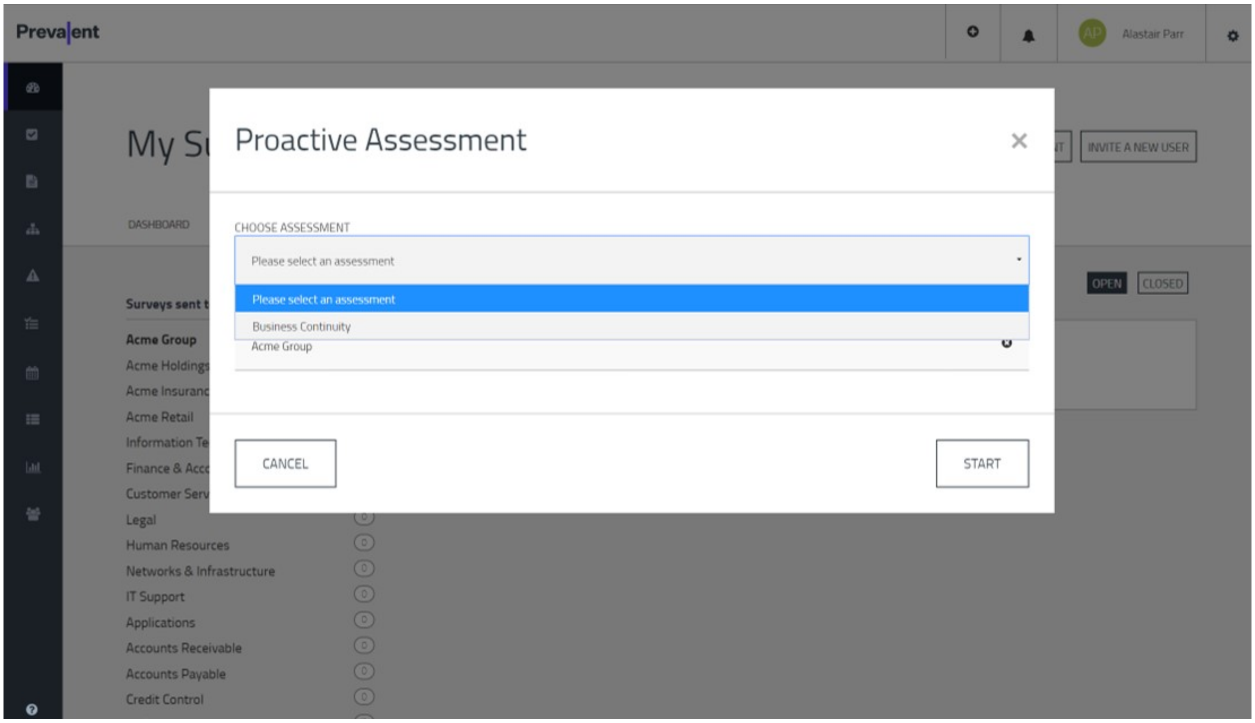
Fixed Assessment: Assessments whose start and end dates are fixed for all entities

Flexible Assessment: Assessments whose start and end dates vary between entities, for a fixed time period

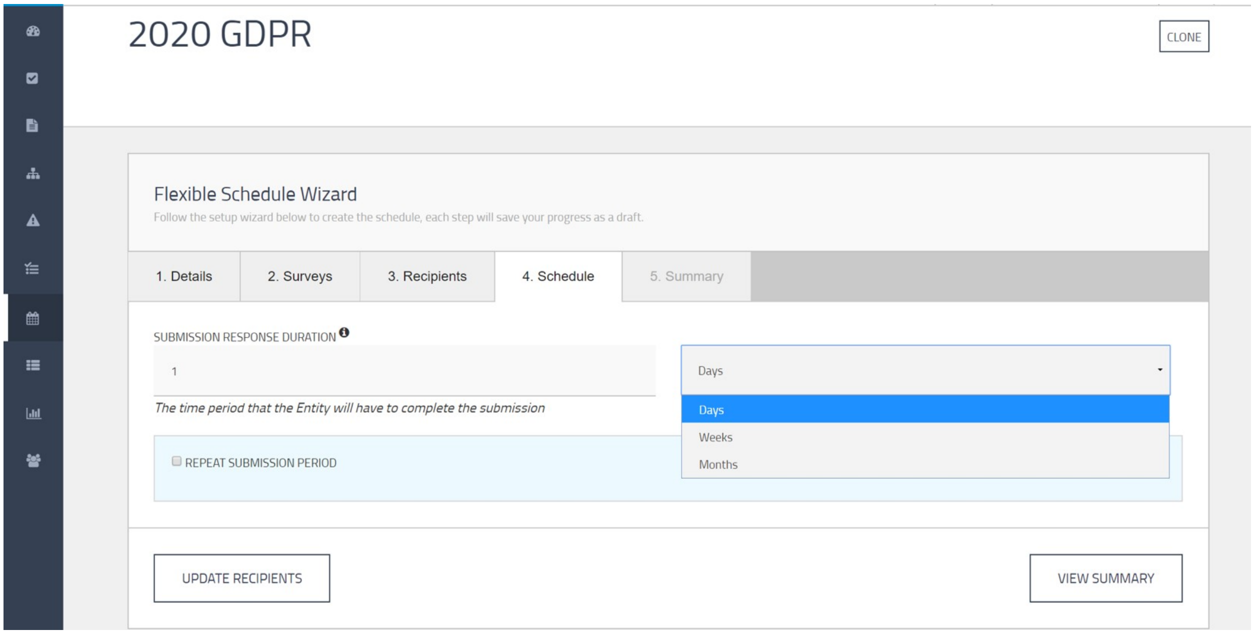
Proactive Assessment: Assessments with no end dates, whose entities can initiate at any time

DESCRIPTION

Proactive scheduling ensures vendors can proactively complete an assessment to update customers on improved compliance and risk management measures:



With flexible assessment scheduling, Prevalent customers can add vendors to an existing schedule instead of creating a new schedule, reducing time to create schedules:


2020 GDPR
CLONE
Flexible Schedule Wizard
Follow the setup wizard below to create the schedule, each step will save your progress as a draft.
1. Details
2. Surveys
3. Recipients
4. Schedule
5. Summary
SUBMISSION RESPONSE DURATION
1
Days
Days
Weeks
Months
The time period that the Entity will have to complete the submission
□ REPEAT SUBMISSION PERIOD
UPDATE RECIPIENTS
VIEW SUMMARY

API Enhancements Centralize Risk Management Information

Sound, risk-based decision making usually requires you to analyze data from multiple sources across the organization. Unfortunately, it's common for organizations to fall into a siloed approach to enterprise risk management, with collections of disparate tools making it difficult to reveal, interpret and act on risk.

API enhancements added in version 3.15 make it easier to collect and interpret data from multiple risk vectors. With the API's new read/write capability, you can now centrally manage and analyze Prevalent third-party risk data in concert with information from your IT service management and enterprise risk management solutions.

ServiceNow Connector Enables Central Management of Third-Party, IT Service, and Risk Data

Organizations standardized on ServiceNow for IT service management (ITSM) often seek integration with other enterprise solutions to optimize workflows and productivity. It’s no different with risk management. Building on API enhancements announced in version 3.14 and 3.15 (see below), v3.16 introduces a connector that enables ServiceNow to consume and manage Prevalent platform data, enabling you to:

- Centrally manage third-party risk management, IT service management, and other enterprise risk management activities
- Analyze third-party risk data with other risk data
- Reduce the number of credentials and platforms you need to manage

This integration is essential for organizations that run their businesses on ServiceNow.

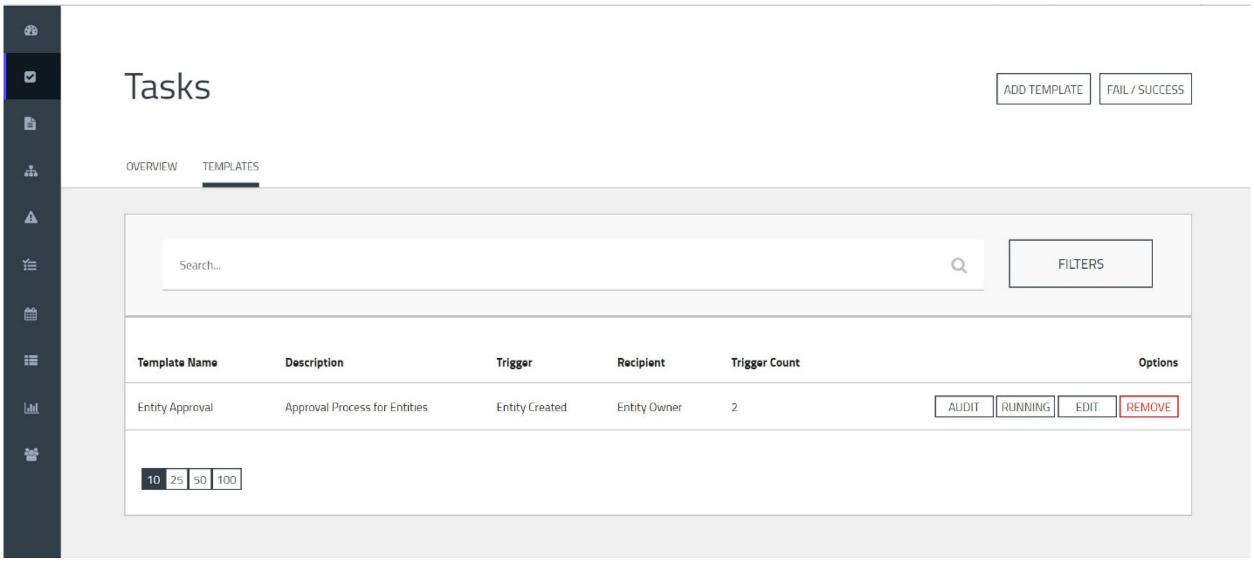
Task Templates Advance Workflow for Vendor Lifecycle Management Automation

Managing the vendor lifecycle can involve many complex steps – from creating entities and changing statuses, to alerting relevant parties about certain actions – making it difficult to scale your third-party risk management program. Prevalent addresses this challenge by introducing task templates in v3.16. Task templates leverage triggers (e.g., entity creation or assessment completion) to generate new workflow tasks. You can use task triggers for workflow actions such as:

- Notifying the entity owner to review a newly created entity
- Automatically changing the entity status upon task completion
- Alerting survey reviewers upon assessment completion

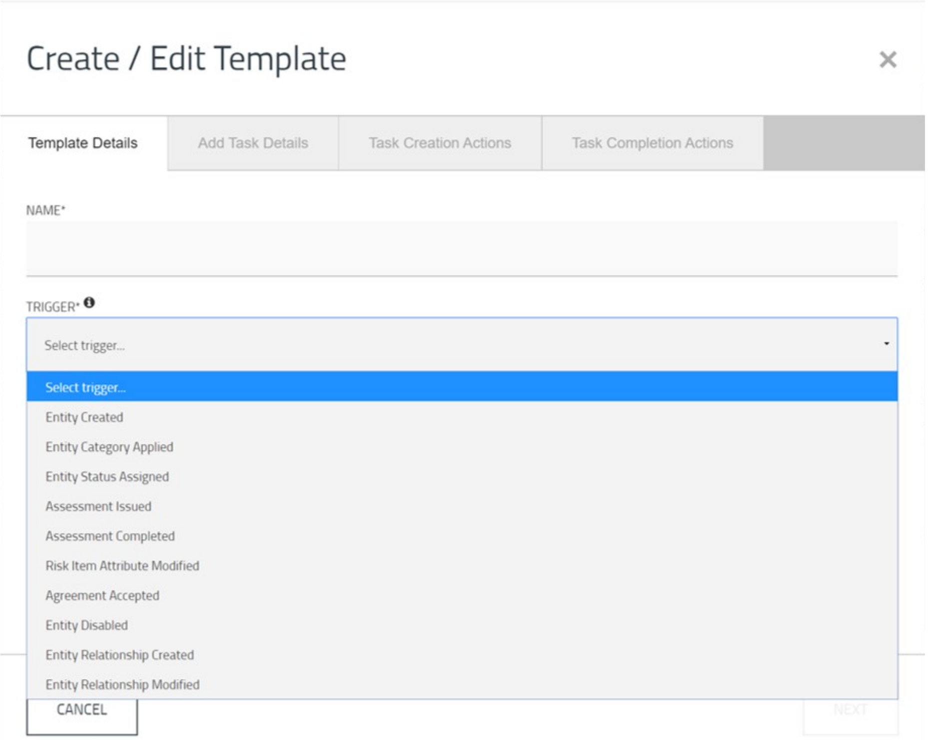
By automating workflow actions, you eliminate manual steps, reduce errors, and are able to focus on priority issues that require your direct intervention. For a representation of a task template, please see the screenshot below.

A new “Templates” tab has been added in the Tasks menu:

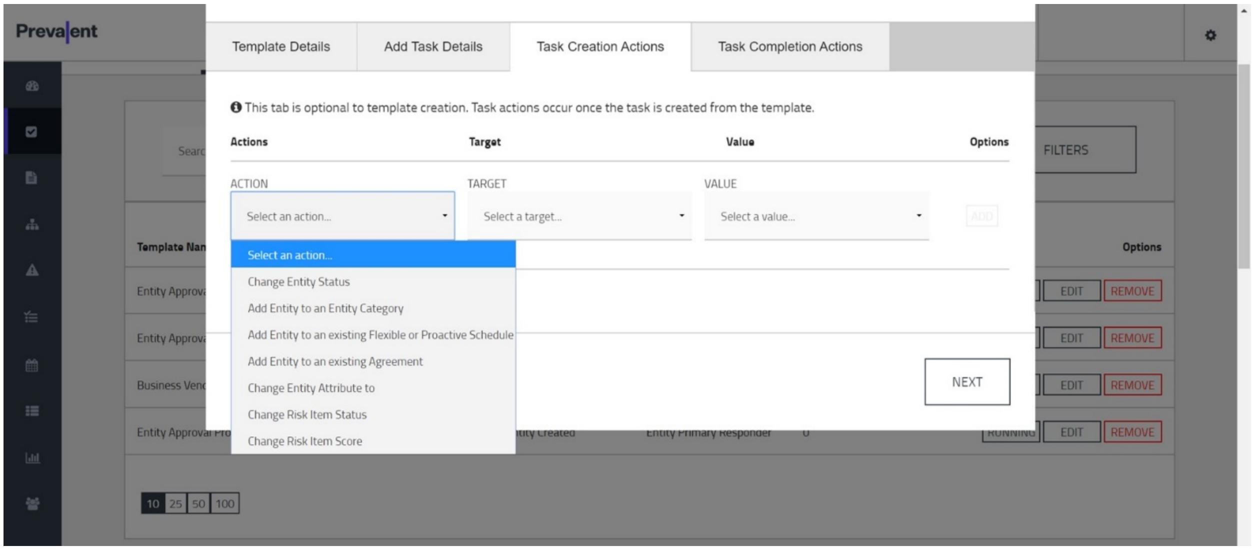


Template Name	Description	Trigger	Recipient	Trigger Count	Options
Entity Approval	Approval Process for Entities	Entity Created	Entity Owner	2	AUDIT RUNNING EDIT REMOVE

The Prevalent platform provides several template options for establishing workflow triggers:



Once it has been selected, you can customize actions per your organization’s relevant parties and processes:



This tab is optional to template creation. Task actions occur once the task is created from the template.

New Licensing Options – From a Starter Kit to Enterprise TPRM

Overtaxed vendor management teams struggle every day with everything from defining who their vendors are, to understanding how much risk they present to the business. Building on our expertise in helping organizations establish and grow their third-party risk management programs, Prevalent now offers new options for vendor teams to manage, assess and monitor their third parties wherever they are in their program maturity.

- **Prevalent Platform Essentials:** Ditch the spreadsheets and upload your global vendor population into the Prevalent Platform to centralize entity management, and perform profiling, tiering and inherent risk assessments using standard content.
- **Prevalent Assessment Standard – PCF Option:** Address the requirements of multiple regulatory mandates and security frameworks by performing assessments using the standard Prevalent Compliance Framework (PCF) content. The PCF is a comprehensive assessment containing 175+ questions mapped to common frameworks and regulations such as GDPR, CCPA, NYDFS, NYMITY, SOX, HIPAA, ISO27001, NIST and SSAE18 (SOC and SOC II). Completing a PCF assessment enables an organization to review, report and remediate across multiple regulations greatly streamlining the compliance process.
- **Prevalent Assessment Standard – Custom Option:** Ideal for customers that want to use their own questionnaire and import it into the Platform, have specific custom questionnaire requirements, or need help building a customized questionnaire.
- **Prevalent Assessment Professional:** Leverage all assessment capabilities in the Prevalent platform, including complete access to standard library content and the ability to create custom content. Ideal for customers that support a mature enterprise-wide risk management program and require flexibility in using both standard and custom content.

With these new options, risk management teams can mature and scale their TPRM programs with automation and greater visibility.

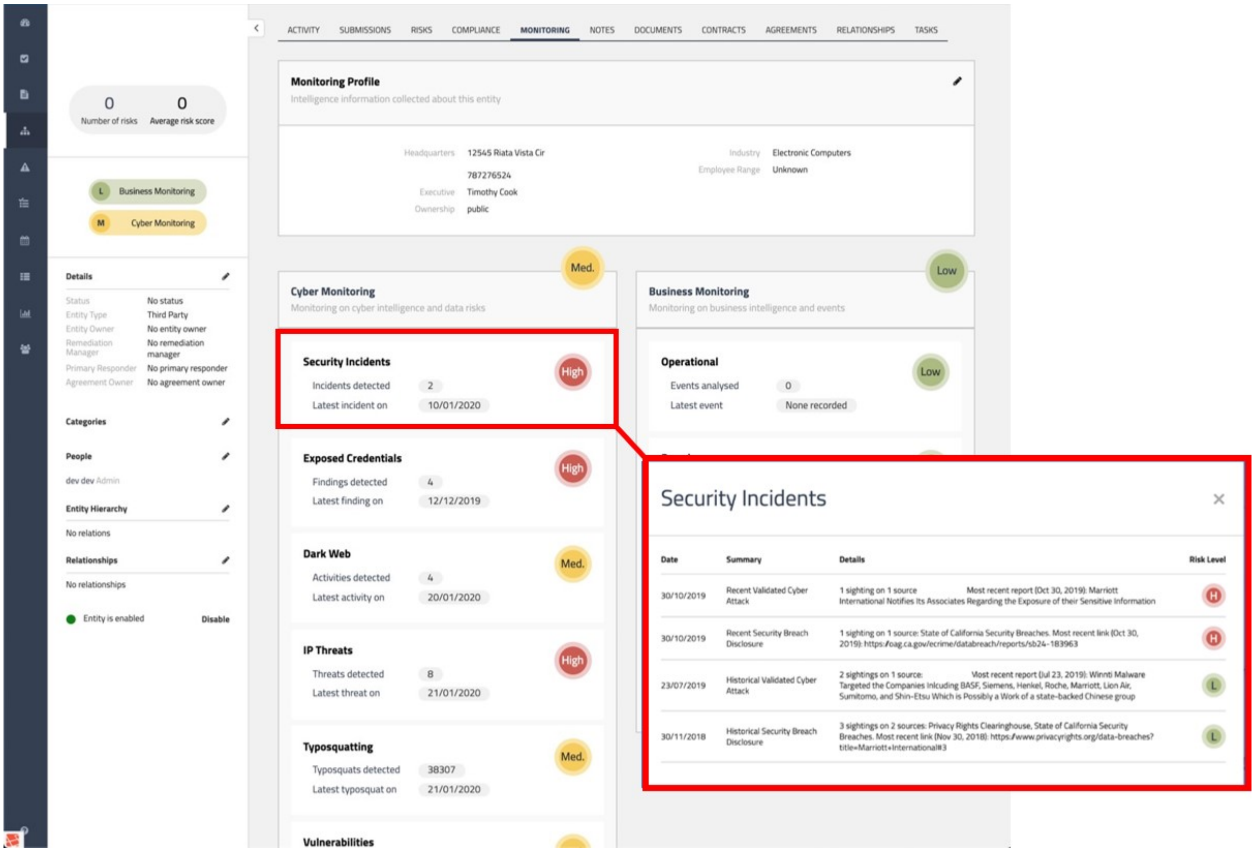
Enhanced Monitoring in Vendor Threat Monitor 2.0 Exposes More Cyber and Business Risks

A complete third-party risk management program requires a combination of inside-out, internal controls assessments and outside-in, monitoring for cyber and business risks. However, without the proper level of integration with their assessment solutions scoring tools provide little visibility into whether a vendor's activities could be a risk before, after, or between assessments. Organizations must be able to leverage continuous monitoring that provides visibility in the business activities and cybersecurity landscape of their vendors to better inform ongoing assessments.

Building on its first-to-market native integration between assessments and monitoring originally announced in version 3.14, Prevalent platform version 3.16 extends coverage to now include the dark web monitoring, as well as additional IP threat intelligence. New threat indicators include:

- Deep/dark leaked credential scanning and alerting
- Asset activity (e.g., hosting a TOR network; asset hosting command and control; communicating with a command and control server; IP detected in malware sample analysis; etc.)
- Dark Web activity (e.g., criminal chatter forums; criminal attention on Dark Web markets, etc.)
- DNS Typosquat notifications and DNS suspect activity events
- Infections recently reported (e.g., external threat lists, external honeypots, etc.)
- Data breach disclosures
- Cyber-attacks recently validated by our global threat research team

Available via a straightforward upgrade path for existing VTM customers, this solution delivers deeper insights into potential third-party risks, enabling your security and risk management teams to be more proactive. For a representation of how these new risk types and incidents influence risk scoring, please see the screenshot on the following page.



0 Number of risks
0 Average risk score

Details

Status	No status
Entity Type	Third Party
Entity Owner	No entity owner
Remediation Manager	No remediation manager
Primary Responder	No primary responder
Agreement Owner	No agreement owner

Categories

People

dev dev Admin

Entity Hierarchy

No relations

Relationships

No relationships

Entity is enabled

Monitoring Profile

Intelligence information collected about this entity

Headquarters	12545 Riata Vista Cir	Industry	Electronic Computers
	787276524	Employee Range	Unknown
Executive	Timothy Cook		
Ownership	public		

Cyber Monitoring

Monitoring on cyber intelligence and data risks

Security Incidents
Incidents detected 2
Latest incident on 10/01/2020

Exposed Credentials
Findings detected 4
Latest finding on 12/12/2019

Dark Web
Activities detected 4
Latest activity on 20/01/2020

IP Threats
Threats detected 8
Latest threat on 21/01/2020

Typosquatting
Typosquats detected 38307
Latest typosquat on 21/01/2020

Vulnerabilities

Business Monitoring

Monitoring on business intelligence and events

Operational
Events analysed 0
Latest event None recorded

Security Incidents

Date	Summary	Details	Risk Level
30/10/2019	Recent Validated Cyber Attack	1 sighting on 1 source Most recent report (Oct 30, 2019): Marriott International Notifies Its Associates Regarding the Exposure of their Sensitive Information	H
30/10/2019	Recent Security Breach Disclosure	1 sighting on 1 source: State of California Security Breaches. Most recent link (Oct 30, 2019): https://oag.ca.gov/ecrime/databreach/reports/sb24-183963	H
23/07/2019	Historical Validated Cyber Attack	2 sightings on 1 source: Most recent report (Jul 23, 2019): Winnti Malware Targeted the Companies Inlcuding BASF, Siemens, Henkel, Roche, Marriott, Lion Air, Sumitomo, and Shin-Etsu Which is Possibly a Work of a state-backed Chinese group	L
30/11/2018	Historical Security Breach Disclosure	3 sightings on 2 sources: Privacy Rights Clearinghouse, State of California Security Breaches. Most recent link (Nov 30, 2018): https://www.privacyrights.org/data-breaches?title=Marriott+International#3	L

Additional Enhancements

Please see the Release Notes for a complete list of all enhancements in Platform versions 3.15 and 3.16, and VTM 2.0.

About Prevalent

Prevalent helps enterprises manage risk in third party business relationships. It is the industry's only purpose-built, unified platform that integrates a powerful combination of automated assessments, continuous monitoring, and evidence sharing for collaboration between enterprises and vendors. No other product on the market combines all three components, providing the best solution for a highly-functioning, effective third-party risk program. To learn more, please visit www.prevalent.net.