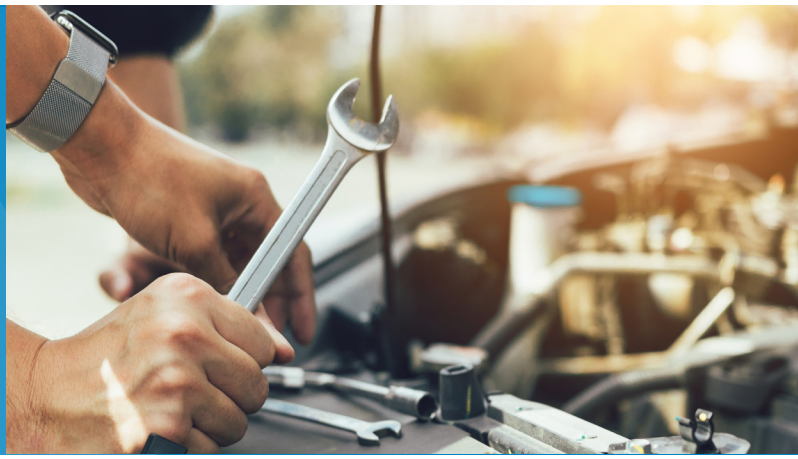
CUSTOMER SUCCESS STORY

How a Fortune 500 Automotive Aftermarket Retailer Solves Third-Party Risk Management Challenges with OneTrust Vendorpedia™ + BitSight Security Ratings

The Retailer's Key Takeaways

By leveraging OneTrust Vendorpedia and BitSight, this retailer is making third-party risk management a more fundamental aspect of their business operations. Not only can the retailer evaluate vendor's in a more automated and efficient manner, but their business units are more engaged in the third-party risk management processes, which will continually elevate the overall quality and drive down risk across their portfolio of vendors.



For one Fortune 500 automotive aftermarket retailer, the OneTrust Vendorpedia™ and BitSight Security Ratings integration was the right combination to support their 2,500+ vendor landscape and a growing list of third-party risk management challenges.

How Vendorpedia Supports Third-Party Risk Management

By implementing OneTrust Vendorpedia's centralized third-party risk management platform, the retailer can leverage aggregated research for vendor due diligence, identify and mitigate associated vendor risks or breach-related incidents, link vendors to multiple engagements, IT systems, and business processes, all while offloading assessment-related work and maintaining regular vendor oversight. With Vendorpedia, the retailer's third-party risk management team can work alongside business owners to collaborate in real time, using a single system of records for internal as well as external third-party vendors and business operations.

"It is essential, with over 2,500 vendors in our ecosystem, that the business be engaged in helping the third-party risk team maintain a centralized database of information, but it isn't a guarantee of our success. So, what's the next step? Having the confidence to make faster, more strategic third-party risk management decisions, so we can not only onboard vendors quickly, but still ensure that we are conducting sufficient and adequate data privacy and security risk assessments to both maintain customer trust and compliance," said the retailer's Third-Party Risk Manager.

How the Vendorpedia and BitSight Integration Works

Along with the Vendorpedia platform, the retailer wanted the integrated value of having security ratings to improve their efficiency and risk reduction efforts. By adding immediate risk data about their vendors' security posture they were able to help the organization make more transparent and rapid third-party risk management decisions. This is where the OneTrust Vendorpedia and BitSight Security Ratings integration came into play.

The retailer leverages BitSight to gain a better understanding of third-party risks and monitor changes as new risks arise, such as when systems are compromised. These ratings enhance the retailer's decision-making capability related to assessment depth, risk prioritization, as well as informing purchase decisions.

With the Vendorpedia and BitSight integration, the retailer can seamlessly (and securely) ingest data insights between both platforms while maintaining a consistent and up-to-date vendor inventory that serves as a single source of truth for all third-party risk management operations. The retailer uses BitSight to identify a third party's risks, while adding context to each vendor by tracking processing activities and operations in the Vendorpedia platform. Leveraging the integration, the retailer can automate their vendor's lifecycle actions, flag risks, trigger reassessments and track mitigation efforts in the event a third party's BitSight Security Rating changes.

BITSIGHT®
The Standard in SECURITY RATINGS

OneTrust Vendorpedia™
THIRD-PARTY RISK SOFTWARE

BITSIGHT®
The Standard in SECURITY RATINGS

> *"Vendorpedia and BitSight's integration not only automates what was once an increasingly complex and time-consuming third-party risk management process, but it helps visually demonstrate third party cyber risk in a way that senior executives and board members can easily digest. The ability to overlay BitSight Security Ratings on Vendorpedia's lineage diagrams has opened up more conversations about enterprise risk management which will positively influence all vendor-related operations."*
>
> **Fortune 500 Automotive Aftermarket Retailer**
> THIRD-PARTY RISK MANAGER

Unique Value for Third-Party Risk Management Use Cases
Real life example scenarios where the Vendorpedia and BitSight integration worked in practice for this retailer include:

Scenario 1: The Third-Party Provided Inconclusive Evidence

- **Problem:** A long-term, local vendor's contract was up for renewal and had a BitSight Security Rating which indicated a high-level of risk. Additionally, the vendor was unable to provide evidence that they were adhering to the retailer's security best practices including a remediated Penetration Test and SOC2 (3rd Party) Application assessment.
- **Outcome:** Utilizing the Vendorpedia system of records, in combination with BitSight's Security Rating, the retailer evaluated the vendor's rating against their inability to provide standard assessment documentation for a retailer of their size. This was the first successful case where the retailer had an enterprise conversation with members of their leadership and Legal teams about the privacy and security risk of a vendor. Ultimately, the third-party risk team made recommendations to renew their vendor while including language for risk mitigation within the contract. Furthermore, BitSight was leveraged to not only continuously monitor this vendor, but to engage in perpetual remediation, driving their cybersecurity rating up.

Scenario 2: The Third-Party Provided No Evidence

- **Problem:** A vendor was unable to supply any privacy or security assessment information, however the niche offering of the vendor made it advantageous to onboard.
- **Outcome:** The Vendorpedia platform and the vendor's BitSight Security Rating allowed the retailer to demonstrate a level of due diligence from a legal perspective. This was the first example of an exception process where the retailer's leadership team leveraged the vendor's rating against the cost of not implementing the vendor and determined they should move forward with onboarding.

Scenario 3: A Third-Party Breach was Discovered

- **Problem:** The retailer was conducting discovery on an existing CRM vendor because they were looking to implement a third one. During discovery, the third-party risk team pulled a Vendorpedia report comparing the existing vendors use cases and BitSight Security Ratings against the prospective vendor. In doing so, the retailer discovered an existing vendor had suffered a 100 point decrease in their BitSight Security Rating due to a breach which was not proactively reported to the retailer.
- **Outcome:** Vendorpedia and BitSight jointly suggested remediation options. The retailer worked with the business owner and existing vendor, as well as their InfoSecurity team, to understand what happened, the impact, and next steps for remediation, so the vendor could stay onboarded.

Scenario 4: Third-Party Vulnerabilities during an RFP:

- **Problem:** While evaluating vendors during the RFP process, the retailer's third-party risk and executive management teams pulled a report from Vendorpedia to review each option and narrow considerations. The third-party risk team made a recommendation to move forward with the options that had the highest BitSight Security Rating. A few days after giving this recommendation, the retailer received a notification that one of these vendor's parent companies had a breach and the BitSight score dropped. This highlighted an area for improvement within the vendor selection process.
- **Outcome:** Initially, the retailer eliminated all but two of the prospective RFP vendors based on their BitSight ratings as well as their ability to provide specific documentation. This saved time and effort spent during the evaluation process. Because one of these vendors had a breach, the retailer required a Vendorpedia risk assessment to move forward with the evaluation process.

> *"From a tactical level, our company implemented Vendorpedia and BitSight to better position ourselves against regulations like PCI DSS, GDPR, and CCPA, however the gains we've made with these technology solutions far surpass compliance. Now we are more empowered than ever to leverage our third-party risk management operations as a competitive advantage and a key to building on our enterprise risk program."*
>
> **Fortune 500 Automotive Aftermarket Retailer**
> THIRD-PARTY RISK MANAGER