SecurityScorecard

ARAVO

Transforming Insights into Cyber Resilience via Technology Integration

FEBRUARY 2018

SECURITYSCORECARD.COM ARAVO.COM

Aravo and SecurityScorecard Partner to Persistently Assess Third-Party Cyber-health

Aravo, an industry leader third-party risk management solutions, and SecurityScorecard, the industry leader in security ratings, have partnered to integrate their solutions to provide today's global extended enterprises with a unique approach to assessing their third party ecosystem for cybersecurity vulnerability, and ensuring the appropriate remediation plans are in place.

This ability to take predictive insight and embed into action plans is a critical requirement for securing vulnerable vendor ecosystems that are evolving and expanding as rapidly as the modern cyberattack surface.

Overview

Enterprises continue to struggle with the increasingly difficult mandate to consistently improve, maintain, and document cybersecurity in order to protect and enhance brand reputation, customer trust, and the bottom line. Top of mind on the cybersecurity agenda is adopting a more agile approach to managing emerging risks across an organization's third-party portfolio.

The staggering cost of data breaches continues to escalate and is predicted to exceed $2 trillion by next year, according to Juniper Research. The average cost of a single breach is more than $4 million, estimates the Ponemon Institute. Industry analysts suggest that nearly two-thirds of data breaches can be attributed to third-party vendors.

Third parties are woven into the very fabric of the modern enterprise, and are intrinsically linked to business success and reputation. Today's complex and dynamic third-party networks, which can comprise thousands of suppliers, distributors, franchises, resellers, contractors, service providers, and other business partners, bring strategic advantages to a relationship; but they also bring vulnerabilities. Limited visibility of this vast, always-morphing environment populated with vendors that have may have access to sensitive corporate data can result in blind spots and weaknesses that hackers love to target. This has been evident in some of the largest data compromises to date, including the oft cited HVAC vendor weakness that resulted in the 2013 Target data breach that impacted 60 million customers. In Target's 2016 annual financial report they reported that the total cost of the breach was $292 million dollars. Regulators globally are also turning their attention to cybersecurity and cyber resiliency. They are increasingly expecting continuous monitoring of third-party ecosystems and evidence of expedited remediation processes. Enterprises need agile and defensible third-party risk solutions to continuously comply with evolving regulations, and they need advanced reporting capabilities to easily and transparently communicate and document high-level cyber-health status to executives and regulatory authorities.

In addition to cybersecurity, data privacy is also coming under increased attention – particularly from the European regulators. Increasingly stringent and far-reaching regulations like the General Data Protection Regulation (GDPR) are keenly focused on data privacy. This has implications for how third parties manage your data, and of course their own security measures. The expectation is that this focus on cyber risk in third party relationships will only continue to expand, and also extend into how companies are approaching their fourth party and n-tier risk.

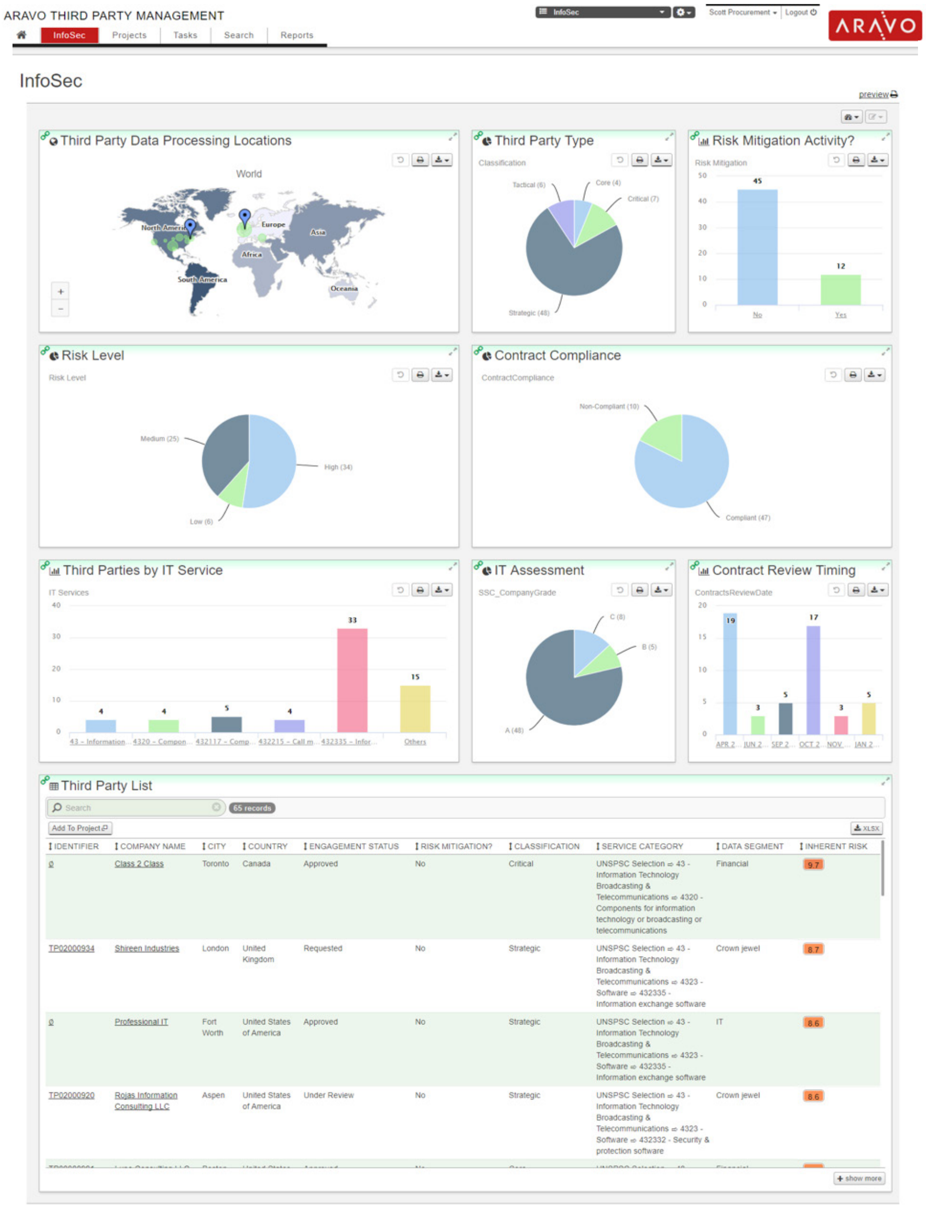
Integrated Solutions

Live integration of the Aravo and SecurityScorecard platforms enables companies to compare third-party point-in-time self-assessment data with dynamic security ratings to determine whether a recommended or current vendor's risk profile warrants additional due diligence prior to establishing or continuing a business relationship.

Aravo Third-Party Risk Management Platform

Aravo's third-party risk management platform features best-practice automated workflows and advanced reporting capabilities to manage third-party risk throughout the engagement lifecycle.

At the top level, the platform features a series of dynamic, customizable dashboards, co-branded with the customer's logo, that display an aggregated view of all of a company's third-party relationships. The risk dashboard, for example, features 1 to 10 numerical scores for inherent (overall) risk, country (geographical) risk, and service category (product or service) risk across all third parties in the organization's portfolio. A deeper dive reveals individual vendor scores in each of the three main categories, and deeper still you can see the risk of individual engagements



IDENTIFIER	COMPANY NAME	CITY	COUNTRY	ENGAGEMENT STATUS	RISK MITIGATION?	CLASSIFICATION	SERVICE CATEGORY	DATA SEGMENT	INHERENT RISK
∅	Class 2 Class	Toronto	Canada	Approved	No	Critical	UNSPSC Selection ⇨ 43 - Information Technology Broadcasting & Telecommunications ⇨ 4320 - Components for information technology or broadcasting or telecommunications	Financial	9.7
TP02000934	Shireen Industries	London	United Kingdom	Requested	No	Strategic	UNSPSC Selection ⇨ 43 - Information Technology Broadcasting & Telecommunications ⇨ 4323 - Software ⇨ 432335 - Information exchange software	Crown jewel	8.7
∅	Professional IT	Fort Worth	United States of America	Approved	No	Strategic	UNSPSC Selection ⇨ 43 - Information Technology Broadcasting & Telecommunications ⇨ 4323 - Software ⇨ 432335 - Information exchange software	IT	8.6
TP02000920	Rojas Information Consulting LLC	Aspen	United States of America	Under Review	No	Strategic	UNSPSC Selection ⇨ 43 - Information Technology Broadcasting & Telecommunications ⇨ 4323 - Software ⇨ 432332 - Security & protection software	Crown jewel	8.6

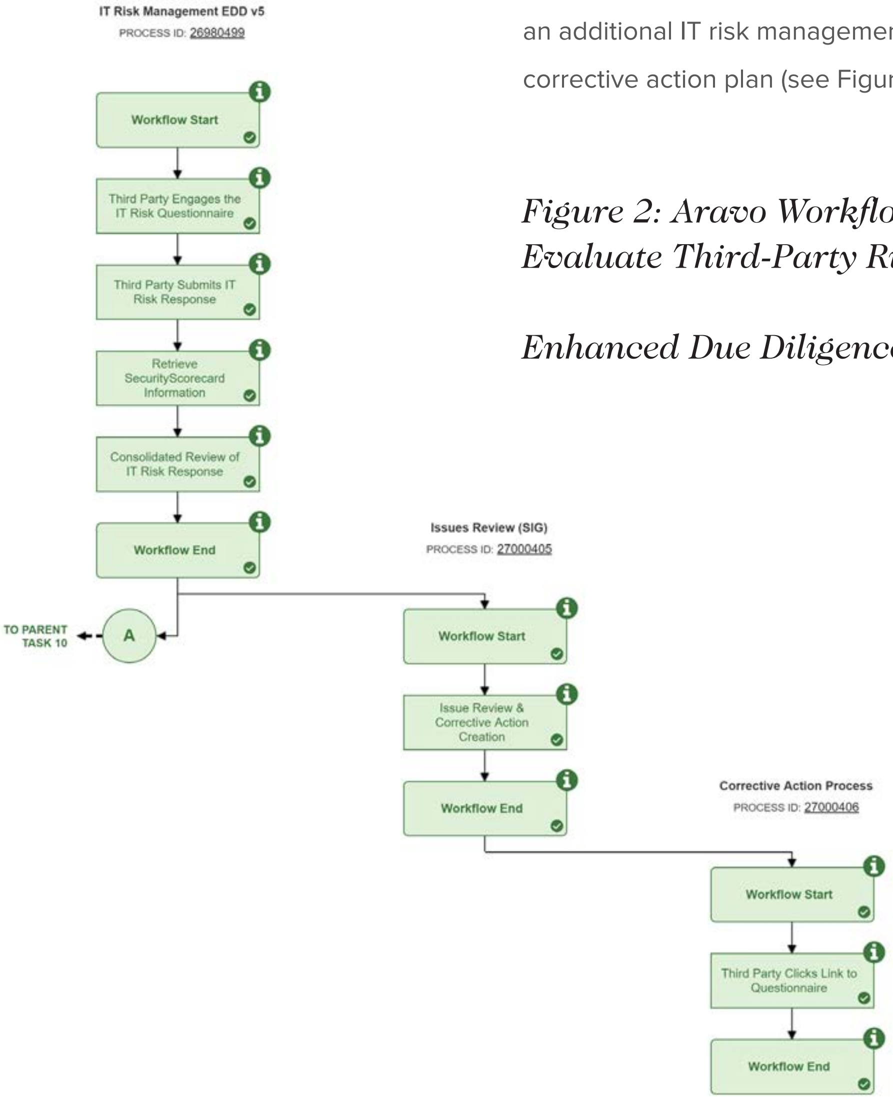
Figure 1: Aravo Risk Dashboard

Everything that happens within the Aravo environment is driven by embedded process automation. Every workflow step includes specific role accountability and if require, documented issue resolution. If mandated actions are not completed within defined timelines, the system triggers reminders that if ignored increase in severity, eventually resulting in warnings about vendor contract deactivation and termination.

The Aravo third-party management workflow navigates the required steps for automated risk assessment prior to an organization's procurement team making a decision about whether to initiate or continue a business relationship with a particular vendor. The steps orchestrated by the Aravo workflow include internal reviews and approvals, third-party data security questionnaire completion, and validations from external sources (Dunn & Bradstreet, Google, the IRS... and now, SecurityScorecard). All of this data is collected, contribute to risk scores and if certain pre-defined risk thresholds are approached or exceeded, routed to internal stakeholders who then determine if enhanced due diligence is required, such as an additional IT risk management workflow or the initiation of a corrective action plan (see Figure 2).

Figure 2: Aravo Workflow to Evaluate Third-Party Risk

Enhanced Due Diligence Workflow


IT Risk Management EDD v5
PROCESS ID: 26980499
Workflow Start
Third Party Engages the IT Risk Questionnaire
Third Party Submits IT Risk Response
Retrieve SecurityScorecard Information
Consolidated Review of IT Risk Response
Workflow End
TO PARENT TASK 10
A
Issues Review (SIG)
PROCESS ID: 27000405
Workflow Start
Issue Review & Corrective Action Creation
Workflow End
Corrective Action Process
PROCESS ID: 27000406
Workflow Start
Third Party Clicks Link to Questionnaire
Workflow End

SecurityScorecard Security Ratings

SecurityScorecard continuously identifies, monitors, and assesses vulnerabilities to build and update an organization’s security risk profile. SecurityScorecard’s patented sensors collect 80 percent of the data ingested by the platform, non-intrusively observing millions of security signals and gathering critical data points from every addressable IP across the internet. The remaining 20 percent of data is collected from trusted open-source and commercial threat intelligence feeds. All of this input is analyzed, normalized, and attributed by advanced machine learning algorithms in SecurityScorecard’s proprietary ThreatMarket engine.

Companies with poor overall SecurityScorecard ratings experience a 500+ higher likelihood of a data breach .

Our proprietary software gathers as much threat intelligence data as possible using non-intrusive methods.

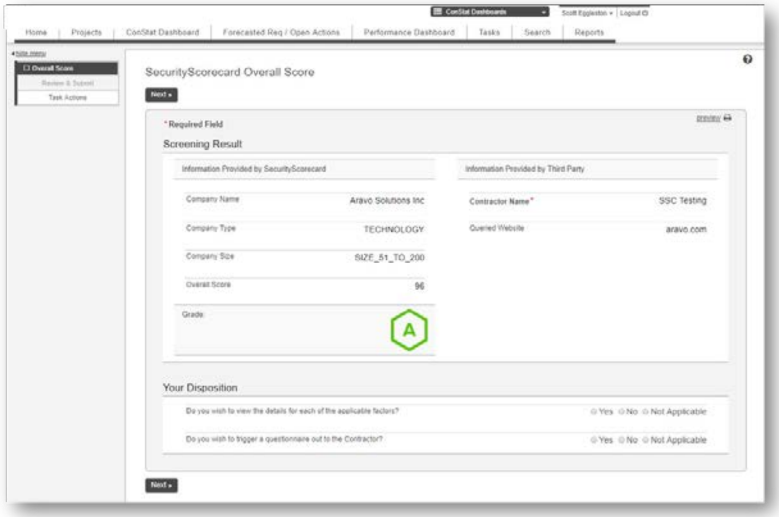
The threat intelligence data is normalized and scored using patented machine learning algorithms.

Based on the threat data, businesses are graded and benchmarked against each other.

Accurate real-time security ratings (A-F letter grades) for organizations (including third parties) are calculated by evaluating ten predictive risk factors (web application security, DNS health, endpoint security, IP reputation, cubit score, patching cadence, network security, hacker chatter, social engineering, and leaked credentials) and the severity of issues and probability of a data breach associated with each category. The end result is a comprehensive view of an organization’s cybersecurity posture.

The Power of Integration

Once a third party submits its risk assessment to Aravo, the workflow engine automatically sends the company's website domain to SecurityScorecard to retrieve the security risk profile, which the internal buying organization then uses to validate the supplier's questionnaire. SecurityScorecard ratings factors can be mapped and filtered according to specific sections of the vendor's self-assessment questionnaire. In fact, the SecurityScorecard dashboard view (featuring the vendor's numerical score and grade) (see Figure 3) serves as the cover page for the questionnaire that's uploaded to the Aravo platform for the customer's procurement subject matter experts. Here the SMEs can drill down for granularity about the factors underlying the vendor rating.



SecurityScorecard Overall Score

* Required Field

Screening Result

Information Provided by SecurityScorecard	
Company Name	Aravo Solutions Inc
Company Type	TECHNOLOGY
Company Size	SIZE_51_TO_200
Overall Score	96
Grade	A

Information Provided by Third Party	
Contractor Name*	SSC Testing
Queried Website	aravo.com

Your Disposition

Do you wish to view the details for each of the applicable factors? ○ Yes ○ No ○ Not Applicable

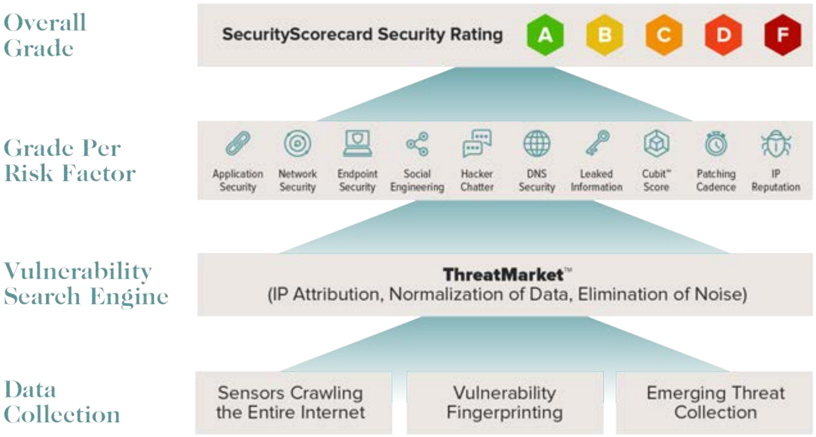
Do you wish to trigger a questionnaire out to the Contractor? ○ Yes ○ No ○ Not Applicable

Figure 3: SecurityScorecard Dashboard View for Internal Buying Team

Aravo’s flexible rules-driven workflow engine makes it easy for nontechnical users to specify the ratings information buyers want to see. For example, users can choose to see grades for all or just some of SecurityScorecard’s ten security factors, and they can set control thresholds to automatically view factors that score below a certain grade. Procurement practitioners can selectively retrieve and store precisely the data they need to make smarter decisions about third-party contracts and renewals.

The gathered intelligence and insights also inform prioritization of critical issues. C, D, and F scores, for example, can automatically escalate issues and trigger notifications and requests to suppliers for triage and remediation. After the enterprise embraces, understands, and operationalizes the ratings data and shares it with the vendor, Aravo drives interaction and collaboration between the two parties, which, in turn, accelerates remediation. Actionable contextual data delivered with guidance directs enterprises to vendors and issues that require immediate attention, leading to measurably improved cybersecurity outcomes.

For current vendors, security ratings can be used to instantly visualize and quantify risk across the third-party ecosystem, prioritize remediation workflows, and report progress to executives and the board of directors. While vetting new vendors, security ratings can supplement risk assessment activities and facilitate faster contracting and onboarding processes. Users gain an aggregated view of risk across the third-party portfolio as well as the ability to drill down into the data that supports risk ratings for individual vendors, resulting in a 360-degree view of risk for strategic decision-making.



Benefits of Integrating Automated Workflows and Security Intelligence

The direct link between Aravo automated business workflows and SecurityScorecard security ratings empowers organizations to better understand and manage risk across the entire spectrum of third parties. The powerful and scalable integrated platform enables organizations to gain operational command of partner and vendor security posture, and reduce risk across their third-party ecosystems, an especially valuable capability considering the critical and expanding shortage of cybersecurity talent resources.

Continuous Compliance

Proactively monitoring third-party cyber-health and enforcing consistent vendor adherence to security frameworks and guidelines facilitate enterprise regulatory compliance due care. The integrated Aravo/SecurityScorecard platform's advanced automated reporting capabilities enable organizations to demonstrate due diligence across their third-party ecosystems. Organizations can meet or exceed regulatory mandates while simplifying compliance audits. Platform users can automatically verify compliance adherence to common standards and frameworks including SIG, SIG Lite, ISO, and PCI.

Streamlined Collaboration

Vendors seamlessly collaborate directly with their customers on the Aravo platform to accelerate remediation processes and leverage opportunities to improve their cybersecurity performance and ratings—a win-win equation for the enterprise and the service provider.

Today, the Aravo/SecurityScorecard integrated solution offers a high-level view of a vendor's security risk rating based on ten factors, providing valuable insights for validating the supplier's self-assessment. As the platform's capabilities mature to become more comprehensive and sophisticated, users will be able to drill down further into third-party findings. Aravo customers will soon be able to access many of the same views as SecurityScorecard clients: the security ratings of all third parties via a single dashboard, average ratings across vendors, best and worst performers, scorecards of industry peers for benchmarking, high-risk suppliers with poor and declining ratings, the most critical and common issues, and more.

Contact SecurityScorecard & Aravo

SecurityScorecard

www.securityscorecard.com

1 (800) 682-1707

info@securityscorecard.com

@security_score

SecurityScorecard HQ

214 West 29th St
5th Floor
New York City, NY 10001

ARAVO

www.aravo.com

1 (415) 835 7600 (US)

+44 20 3866 2682 (UK)

info@aravo.com

Aravo Solutions Inc.

555 California Street
Suite 350
San Francisco, CA 94104