Keep it Fair
Security Ratings and Reviews

KEY POINTS

- What We Do
- Transparancy
- Dispute, Correct, and Appeal
- Accuracy and Validation
- Model Governance
- Independence
- Confidentiality

In 2017, the US Chamber of Commerce developed the Principles for Fair and Accurate Security Ratings with a number of industry representatives, to bring consistency and credibility to the emerging security ratings market.

The need arose to provide more insight and validation into the nature of how scores are developed and represented, to increase the public's confidence in security ratings as a whole.

BlueVoyant's Cyber Risk Management Services platform and services were purpose-built to adhere to these principles and ensure fair and accurate representative risk scores for customers and the vendors within their ecosystem.

What We Do

BlueVoyant utilizes a combination of public and proprietary data sources, analytical strategies, and machine learning algorithms to create a **single source** of truth that is associated with a target company. BlueVoyant combines this information with behavioral analytics and proprietary IP intelligence to obtain a complete view, further incorporating machine learning to measure the confidence of those relationships to deliver accurate insights into an organization's security risks.

BlueVoyant's main objective is to identify and remediate cyber risk for our clients, not to rate organizations. We provide a managed risk service to triage risks and prioritize those that need investigating, to empower risk professionals as opposed to inundating them with ratings data.

As with other solutions, our services utilize a risk scoring system to make it easier to identify and mitigate serious vulnerabilities faster. Scores are constantly refreshed and updated near real-time to provide the most accurate representative risk scores for organizations.

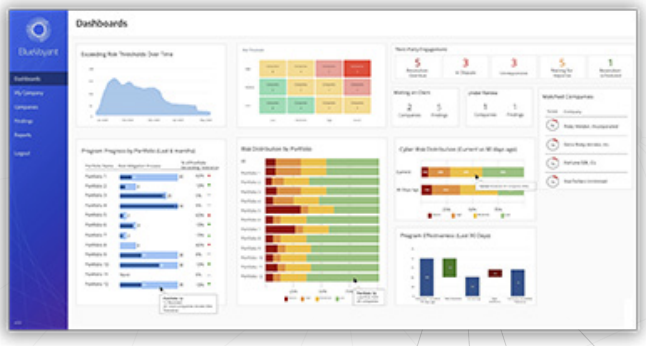
BlueVoyant's Cyber Risk Management Services adhere to the Principles for Fair and Accurate Security Ratings as follows:

Transparency

Rating companies shall provide sufficient transparency into the methodologies and types of data used to determine their ratings, including information on data origination as requested and when feasible, for customers and rated organizations to understand how ratings are derived. Any rated organization shall be allowed access to their individual rating and the data that impacts a change in their rating.

BlueVoyant is committed to complete transparency with our customers and their third-party vendors.

Clients can monitor an entity's adversarial and risk scores through the Cyber Risk Management Services portal where they can view detailed data on how a particular score was derived.



BlueVoyant utilizes a combination of public and proprietary data sources, analytical strategies, and machine learning algorithms to create a single risk score which is comprised of five risk categories:

- **Email Security:** Identification of correct configuration and best practices for Email Security including use of spoofing and spam protection.
- **IT Hygiene:** Identification of misconfigured network infrastructure and proper internal IT best practices, including exposed ports that are easily breached, administration, or unauthenticated. Additionally, detection of the internal use of peer-to-peer (P2P) file sharing and torrent software indicators lack proper IT governance and controls.
- **Vulnerability Detection:** Identification of exposed vulnerabilities that could potentially be exploited, including proper use of certificates.
- **Malicious Activity:** Identification of malware, phishing, and ransomware emanating from the third party's environment. Detection of a company's interactions with adversarial infrastructure, including darknet and botnet infrastructure.
- **Adversarial Threat:** Monitoring of adversarial attacks directed at the third party company, including inbound phishing and attacker infrastructure targeting the third party.

BlueVoyant can provide reporting or work with our client and their vendor directly to review all data associated with their assigned rating.

Dispute, Correct, and Appeal

Rated organizations shall have the right to challenge their rating and provide corrected or clarifying data. Rating companies should have an appeal and dispute resolution process. Disputed ratings should be notated as such until resolved.

BlueVoyant's Cyber Risk Management Services incorporate entity feedback into its scoring process. Whether through written questionnaires or direct engagement, BlueVoyant works directly with clients and organizations to refine, amend, and correct data discovered.

As mentioned above, BlueVoyant Risk Analysts will review findings with an organization to demonstrate how the data was collected and the score was derived. This interaction provides them the opportunity to work directly with us to ensure the risk level rating is portrayed correctly or the issues discovered are effectively remediated.

Accuracy and Validation

Ratings should be empirical, data-driven, or notated as expert opinion. Rating companies should provide validation of their rating methodologies and historical performance of their models. Ratings shall promptly reflect the inclusion of corrected information upon validation.

BlueVoyant takes a continuous, iterative approach to effectively analyze data to help fill in the blanks and deliver more accurate results. We believe that to ensure the accuracy of a score, data needs to be evaluated over a set period of time, not a single instance. When determining an accurate score, changes in data access, data gaps, company footprint, and even changes in cybersecurity risk are factored in.

Clients are able to view historical risk data for their vendors and review their performance over the previous 12 month period.

Model Governance

Prior to making changes to their methodologies and/or data sets, rating companies shall provide reasonable notice to their customers and clearly communicate how announced changes may impact existing ratings.

BlueVoyant utilizes a combination of public and proprietary data sources, analytical strategies, and machine learning algorithms to create a single source of truth that is associated with a target company.

The speed and accuracy of BlueVoyant's Cyber Risk Management Services algorithms allow for entity score updates in near real-time and thus, to alert when a specific entity deviates from its cyber risk profile.

Any changes in methodologies would be used to enhance the level of information provided and will always be communicated to our customers.

Independence

Commercial agreements, or the lack thereof, with rating companies shall not have direct impact on an organization's rating; any rated organization will be able to see and challenge their rating irrespective of whether they are a customer of the rating company.

Foundational to BlueVoyant's Cyber Risk Management Services is providing clients with actionable information that will assist them with understanding and lowering the cyber risks in a vendor's environment. Driving out errors is essential to assure an accurate profile of the entity - and the entity alone, regardless of agreements or affiliation. As mentioned, BlueVoyant Cyber Risk Analysts will review findings with an organization to demonstrate how the data was collected and the score was derived in the hopes of rectifying any concerns and improving upon any issues identified.

Confidentiality

Information disclosed by a rated organization during the course of a challenged rating or dispute shall be appropriately protected. Rating companies should not publicize an individual organization's rating. Rating companies shall not provide third parties with sensitive or confidential information on rated organizations that could lead directly to system compromise.

BlueVoyant's Cyber Risk Management Services platform is built on our core capabilities and expertise in cybersecurity. We believe in complete transparency and confidentiality. We do not perform or disclose ratings on individual organizations unless contracted by our customers. That data is only available to our client and can be shared with their vendors on an as-needed basis.

BlueVoyant is committed to improving the relationships between our customers and their supply chain while enhancing the security and risk posture of all organizations in the process.

For more information visit: www.bluevoyant.com
Secure your business today: contact@bluevoyant.com