WHITE PAPER

Is Your Security Ratings Provider Ready for Prime Time?

Four Questions to Consider Asking Your Security Ratings Partner

Is Your Security Ratings Provider Ready for Prime Time?

Four Questions to Consider Asking Your Security Ratings Partner

BitSight was recently named a Leader in The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q1 2021. As the creator and largest vendor by market presence in the category, we were honored to be recognized and to be the only vendor recognized for having differentiated product roadmap and go-to-market strategy.

For the report, Forrester evaluated seven cybersecurity risk rating solutions to appraise their efficacy and ability to address current market needs. Forrester offers the market important questions to consider when evaluating a Security Ratings provider. While we would encourage you to read the full report, this short analysis shares BitSight's perspectives on these critical issues.

We believe there are four things you should consider when choosing a security rating partner:

1. Is the rating independently verified to accurately reflect risk?
2. What data is included in the rating and how accurate is it?
3. How transparent is the ratings algorithm and the dispute resolution process?
4. How will a ratings provider fit into my ecosystem and how will it continue to evolve?

1. Is the rating Independently Verified?

Security Rating customers should ask their provider "what does your rating mean and what external evidence validates the rating?" At the end of the day, the most important characteristic of a rating is whether it has been verified to accurately reflect a firm's risk of cyber breach.

BitSight is the only Security Ratings provider who can provide a statistically-validated third party validation of their rating. The BitSight Security Rating is a meaningful, statistically significant rating correlated to real-life cyber-risk exposure and events. We've demonstrated through our own research that organizations with stronger security performance as measured by BitSight are less likely to experience a breach. Independent third parties, including catastrophe insurance modeler AIR Worldwide and information analytics firm IHS Markit have confirmed BitSight's analyses.

A strong security posture is good for business. BitSight partnered with financial index provider Solactive and together published research demonstrating a correlation between BitSight Security Ratings and financial performance. The conclusion was that a strong rating can lead to a market out-performance of up to 7% in certain sectors.

And we believe that our ability to create a meaningful, independently validated rating helps explain why so many organizations choose BitSight:

2,000+
customers

20%
of Fortune 500

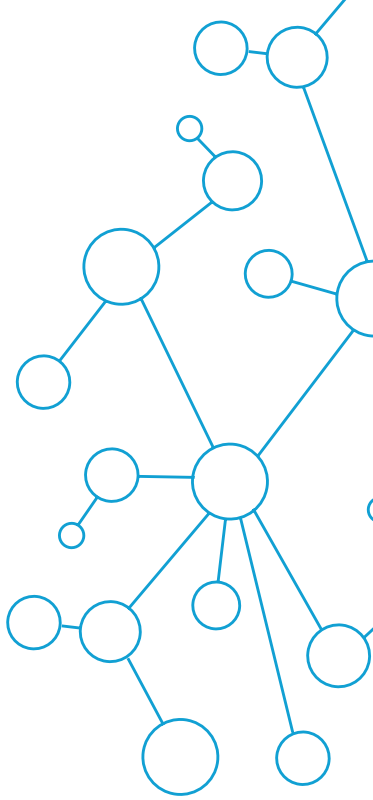
30+
insurance customers write 50% of global cyber insurance premiums

40+
40+ national governments (including the U.S. Department of Defense)

Companies and governments put BitSight's rating and underlying data to the test every day. We are proud of the unique partnerships we have formed with organizations such as the Department of Justice and the FBI. They leveraged BitSight data to disrupt the world's largest online criminal network).

You can't manage what you can't measure. Being in the security and technology world for over 20 years, I like how BitSight uses externally observable data and converts this insight into measurable values that can be transparently shared to get everyone across EPAM on the same page."

-YURIY GOLIYAD
GLOBAL IS HEAD, EPAM



2. What data is included in the rating?

Security Rating customers should ask their provider "what data do you collect and how do you ensure its accuracy?"

BitSight uses a 4 part process to drive accuracy

1. Automated collection

Models fundamentally have higher reliable predictability with more data inputs. BitSight's unique capabilities and partnerships with over 100 data providers allow us to observe 260B externally observable events with insight into critical issues across 300M companies

2. 500+ sources

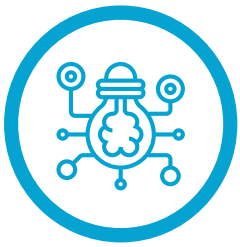
We catalog 500+ known cybersecurity issues and over 2,000 known vulnerabilities. This gives BitSight very broad and deep insight into everything from botnet infections to software services. These are segmented into 23 unique risk vectors such as malware, vulnerabilities, outdated systems, mobile and IOT.

3. Human review

We recognize that gathering data is only half the battle. That's why BitSight continuously invests in accurately building an organization's network footprint through patented automated processes that are continually tuned with human oversight. The result is that BitSight maintains an extremely low rate of IP/domain misattribution (0.00007%) when compared to the total number of mappings we've created.

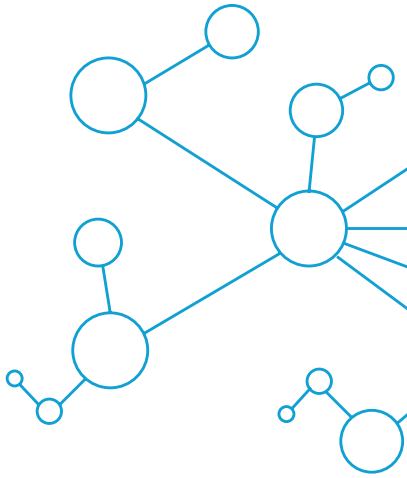
4. Entity Self-review

BitSight also allows organizations to add data and context based on their own internal knowledge. BitSight allows any rated entity to add context to their rating through self-published ratings. Self published ratings enable entities to create, publish a separate rating using their choice of a subset of their assets. In addition, we offer rated companies the option to create tags. With tag they can publish public comments including describing compensating controls. Support for self-published rating and tags opens our platform resulting in higher data quality and public scrutiny.



BitSight Security Ratings help our information security team translate complex cybersecurity issues into simple business context that enables our board of directors to make intelligent decisions.

-DIRECTOR OF INFORMATION SECURITY
Large Telecom Company and BitSight Customer



3. How transparent is the ratings process and resolution process?

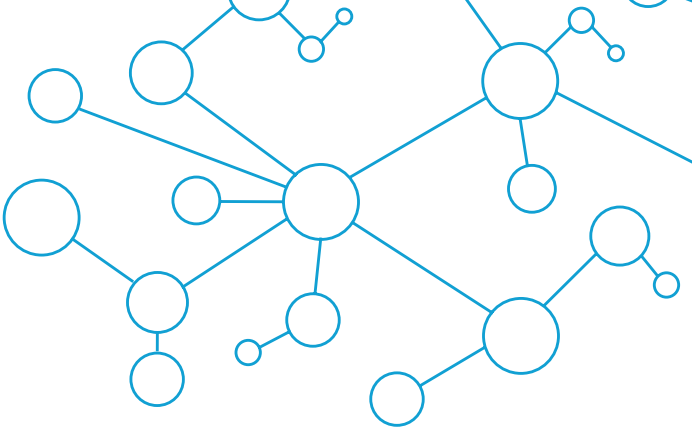
Security Ratings customers should ask their provider "how do you address challenges and disputes to the rating?"

BitSight's rating and dispute resolution process is designed to be rigorous, while allowing for any rated entity to challenge their rating and methodology.

BitSight seeks accurate, prompt remediation of disputes. The dispute resolution process is governed by the Policy Review Board and follows the Fair and Accurate Principles laid out by the US Chamber of Commerce. BitSight responds to inquiries within 48 hours, evaluates data submitted, helps the impacted organization understand our conclusions, and creates an audit trail of supporting evidence.

Policy Review Board decisions are published with findings along with case summaries. If satisfaction is not achieved, final resolution can be pursued through the industry's first independent Ombudsman.

BitSight's dispute resolution process is unique among Security Rating Service providers, with a focus on transparency, and empiricism.



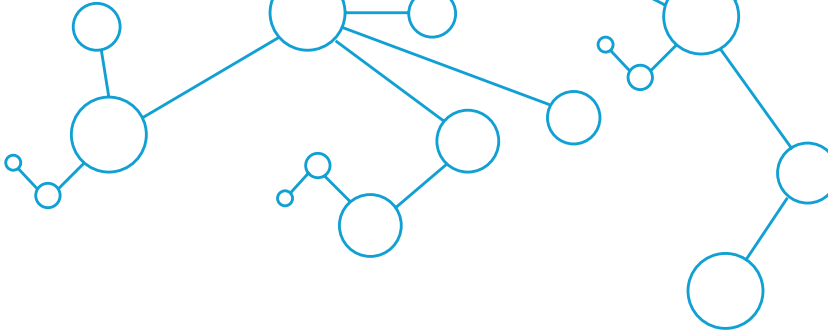
4. A partner for the future

Security Ratings customers should ask their provider "how do you plan on being a good partner to our business?"

Customers don't just want to buy data. They want to know that their Security Ratings provider will be a partner for the future. BitSight has proven to be a trusted partner, and we're here for the long haul.

We've worked hard to address several aspects of managing cybersecurity risk. It's one of the reasons that Forrester recognized us as being, "Best suited for firms with a wide range of use cases and reporting requirements." We are the only vendor offering a full suite of capabilities for the first party use case, including Enterprise Analytics, Forecasting, and Peer Analytics. Our competitors offer some functionality, but do so via their third party offering. We recognized much earlier that first party was important, and we built a suite of capabilities specific to the first party use case.

These are challenging times for security and risk professionals. From increased risks and unprecedented attacks on third party supply chains, to growing demands from executives and board members for better security program measurement and efficacy, BitSight has demonstrated an ability to help our customers confidently engage in the most critical and difficult challenges facing security teams and organizations. Whether adding new WFH capabilities to give broader insight into expanding risks, helping our customers improve their third party risk program through hundreds of consultant-led workshop, or offering free subscriptions to customers to help provide enhanced visibility during the onset of COVID-19, BitSight is committed to being a strong partner now and for the future.



Summary

BitSight is honored to have been named a leader by Forrester. While some Security Ratings Service providers may not be ready for prime time, BitSight certainly is!

Our goal was to tackle three critical questions every provider should be asked. The answers reveal critical differences between providers.

1. A rating or score's correlation to breach events should independently be verified to be statistically correlated. Please read the conclusions reached by AIR and Solactive.

2. The data set and process applied to calculate ratings should be transparent and it's accuracy measured.

3. A clear governance process is a market must have. Our process is anchored in the FAIR Principles, complemented with a Dispute Resolution Process for any rated entity along with the industry's only independent Ombusdperson.

As a provider we are committed to constantly improving our offering. We appreciate Forrester's recognizing the strength of our product roadmap, the breadth of supported use cases and

go to market strategy. We believe these are critical elements of how we deliver differentiated value to the market.

BitSight is proud of the partnership we have created with companies and governments to improve how third party risk is managed and overall security posture is maintained. The value of objective, statistically correlated data measuring security effectiveness over time is helping organizations make better risk informed decisions every day.

Choosing a Security Ratings provider is an important decision. We hope that you will consider BitSight as your partner now and for the future.

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.