BITSIGHT
The Standard in SECURITY RATINGS

POLICY REVIEW BOARD

Ensuring Fair and Accurate Security Ratings

BitSight is committed to creating the highest quality and most accurate security ratings in the industry. We are also committed to allowing all rated organizations—not just customers—the opportunity to challenge the assets, findings, and interpretation of those findings used to determine a BitSight Security Rating, and to provide corrected or clarifying data. As a signatory and contributing author, we are firmly committed to upholding the U.S. Chamber of Commerce's Principles for Fair and Accurate Security Ratings.

The BitSight Policy Review Board (PRB) is a committee created to govern the ratings algorithm and associated policies, and to ensure that they are aligned with our principles. As the highest level of ratings governance, the PRB also adjudicates appeals related to data accuracy and evaluation methodology. It is charged with providing a consistent, transparent, and systematic dispute resolution process that is available to all rated entities. BitSight seeks accurate and prompt remediation for any dispute.

SCOPE

The PRB's scope includes the following areas:

- The ratings algorithm, including:
- The overall Security Rating
- Risk vectors and grades
- Criteria for interpreting and grading findings
- Criteria for inclusion of assets within a company's network map
- Policies for addressing appeals and disputes
- Acceptable use of security ratings

COMPOSITION

The PRB currently consists of nine BitSight staff, including the CEO, CTO, General Counsel, and heads of relevant departments. To avoid conflicts of interest and to maintain commercial independence, it does not include representation from the company's commercial functions.

PRINCIPLES FOR FAIR AND ACCURATE SECURITY RATINGS

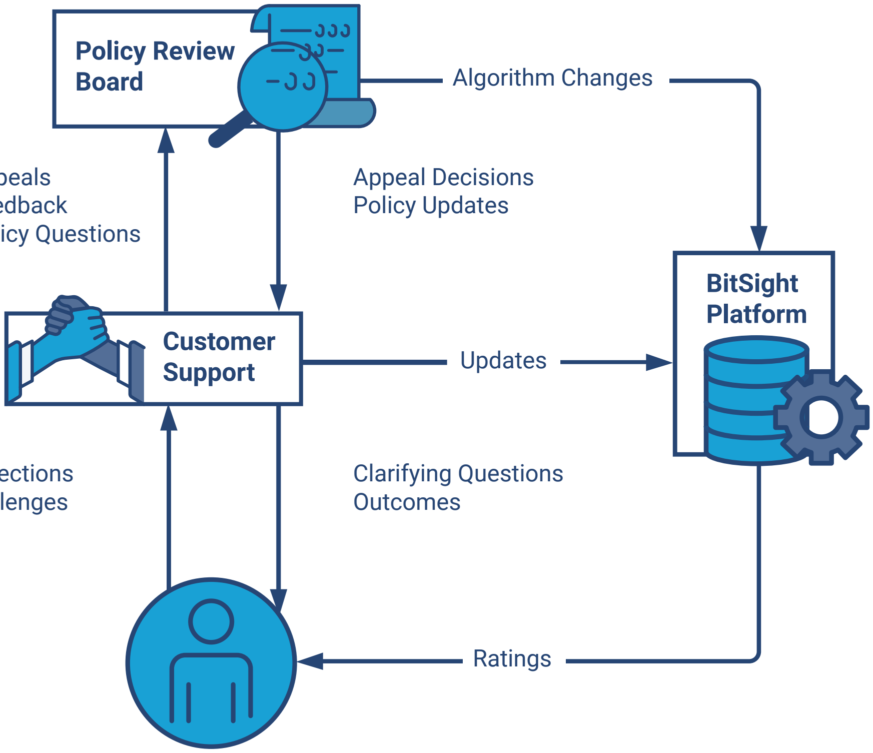
- Transparency
- Dispute, Correction, and Appeal
- Model Governance
- Independence
- Confidentiality

TYPES OF DECISIONS

Model Governance and Algorithm Changes

From time to time, BitSight updates its ratings algorithm, to further increase its accuracy and breadth, and to reflect the evolving threat landscape and security best practices. Algorithm changes are driven by BitSight research, ongoing feedback from customers, and guidance from industry experts. We make these changes in a deliberate and considered manner, however.

Significant changes to the algorithm are first proposed internally to the PRB to be thoroughly reviewed. Following PRB approval and algorithm research and development, a preview of the changes is made available to rated organizations. During the preview period, we invite comments and feedback on the proposed changes. Finally, the algorithm changes are released and become effective.



DISPUTE RESOLUTION PROCESS

While we strive for the utmost in accuracy in our ratings and data, we also have a robust and transparent dispute resolution process. A rated organization may challenge the assets, findings, and interpretation of those findings, used to determine its security rating. In many cases, there are options within the product itself to submit corrections for, e.g. assets included in the organization's network map. When those are insufficient, however, the organization may follow the process below. Furthermore, all rated organizations—not just customers—have the right to challenge their ratings.

1. CUSTOMER SUPPORT

The first step in the process is for the rated organization to contact Customer Support.

Support will make every effort to to work with the organization to clarify the matter or to make corrections where necessary. During this process, Support may ask for additional material related to the dispute; e.g. network logs or screenshots of the system in question. These materials are treated with strict confidentiality. In the vast majority of cases, Support is able to facilitate a successful resolution of the issue. Our support team responds to most inquiries within two business days.

If Customer Support cannot satisfactorily resolve the issue, or if the rated organization disagrees with Support's decision, the rated organization may petition for escalation to the Policy Review Board.

2. PRB REVIEW

The Policy Review Board is designed to address issues raised by rated organizations that may require a change to the overall ratings policy or where a rated organization feels that a policy decision provides an inaccurate description of their security posture and performance. This may include changes to the ratings algorithm, inclusion of assets within a company's network map, and the acceptable use of security ratings.

Prior to review, the PRB may invite additional input and supporting material from the organization making the dispute. All of the material is treated as confidential. The PRB decision draws upon existing policy, prior case decisions, input from subject matter experts, and advice from independent industry experts.

3. COMMUNICATION AND DOCUMENTATION

The outcome of the review, and the reasons for the decision, are communicated to relevant stakeholders, including the rated company who made the appeal, if applicable. We also publish a short summary of PRB decisions on our website on a quarterly basis.

ABOUT BITSIGHT

BitSight transforms how organizations manage cyber risk. The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third party risk; underwrite cyber insurance policies; conduct financial diligence; and assess aggregate risk. With over 2,000 global customers and the largest ecosystem of users and information, BitSight is the Standard in Security Ratings.

FOR MORE INFORMATION

BitSight Technologies

111 Huntington Ave, Suite 2010 • Boston, MA 02199 • www.bitsighttech.com