BITSIGHT

TECHNICAL NOTE

# How BitSight Calculates Security Ratings

Building Security Confidence with a Transparent and Proven Approach to Mitigating Security Risk

## THE CHANGING THREAT LANDSCAPE

BitSight Security Ratings are used by over 1,000 companies across the globe to measure their own security risk and continuously monitor third party networks. Businesses use these ratings to screen and monitor third parties, underwrite cyber insurance coverage, monitor investment portfolios, benchmark their own security programs and more. Ultimately, BitSight is transforming the way organizations understand and manage cybersecurity risk.

BitSight continuously assesses new data and risk vectors to add into the product. In accordance with the Principles for Fair & Accurate Security Ratings, BitSight updates the algorithm that calculates BitSight Security Ratings, giving advance warning to customers. Algorithm updates are done in order to expand the breadth, depth and quality of data that go into the ratings. This provides customers with increased visibility into the security performance of their organization and third party organizations.

## BITSIGHT SECURITY RATINGS

BitSight Security Ratings measure the security performance of organizations. These ratings range from 250-900 with a higher rating indicating better security performance. All data collected by BitSight is externally observable. This means that we do not perform penetration tests or malicious attacks on any company network in order to collect information. To calculate these ratings, BitSight focuses on data breadth, depth, and quality - ensuring that customers gain the most accurate security ratings to make important business decisions. This data is processed daily using an advanced algorithm that is flexible to new inputs of data and produces accurate ratings of a company's network security performance over time.

## THE SECURITY RATINGS BREAKDOWN

BitSight Security Ratings are calculated by collecting and processing terabytes of security data collected from around the globe. Using proprietary data sources and exclusive contracts with data sources, BitSight provides users with the highest quality data.

### WHAT MAKES A SECURITY RATING?

Compromised Systems (55%)
+
Diligence (35%)
+
User Behavior (10%)
+
Public Disclosures*
=
BitSight® Security Ratings

*
(only publicly disclosed breaches impact ratings when they occur)

## ABOUT BITSIGHT TECHNOLOGIES

BitSight transforms how companies manage information security risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of external data on security issues. Seven of the largest 10 cyber insurers, 20% of Fortune 500 companies, and 3 of the top 5 investment banks rely on BitSight to manage cyber risks.

## FOR MORE INFORMATION

**BitSight Technologies**
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com
sales@bitsighttech.com

Security Ratings are calculated from data on Compromised Systems, Diligence, User Behavior and Public Disclosures. Using our network mapping process, this data is attributed to a specific entity and processed through BitSight's algorithm engine to produce a company's rating.

For a comprehensive list of risk vectors, visit www.bitsighttech.com/data.

## WHAT IS NOT IN SECURITY RATINGS?

BitSight Security Ratings are a strong quantitative indicator of a company's security performance. These ratings do not account for the following factors in a company's security performance:

- Budget: BitSight does not include qualitative factors such as security spend in the calculation of Security Ratings. Since Security Ratings reflect improvements in security controls, a change in budget may affect quantitative factors over time.
- Franchise Locations: BitSight intentionally leaves out franchise locations for specific retail operations since these locations are outside the control of the corporate entity. Through our advanced network mapping process we determine whether every IP address should be attributed to the host company based on a set of comprehensive criteria.
- Beta Risk Vectors & Informational Only Feeds: data collected in categories such as DNSSEC and Dark Web are informational only and will not impact rating calculations.
- Compliance: BitSight provides reports that indicate an organization's alignment to security frameworks such as NIST CSF and ISO27001, but these reports do not impact rating calculations.

## HOW TO IMPROVE RATINGS OVER TIME

Security Ratings are a measurement of security performance based on historical data - over years - meaning they won't change dramatically overnight. There are some steps you can take right now to improve your company's ratings over time:

- Ensure security configurations are up to industry standards
- Enable continuous monitoring of compromised systems your network
- Remediate issues as soon as you discover them
- Verify your network infrastructure and ensure that all addresses are properly attributed