BITSIGHT

BitSight Security Ratings

Empowering businesses with the insight needed to seamlessly identify and measure cyber risk.

INPUT

Collected from extensive & diverse sources

- Botnet
- Spam
- Malicious Code
- Configurations
- DDOS
- User behaviors
- News Feeds
- Social Media

PROCESSING

Normalizes & maps the input

- Type of Compromised System
- Date
- Company IP
- Severity
- Frequency
- Duration
- Confidence

OUTPUT

Customer portal summarizes security risk

Analytics   Ratings   Alerts

BITSIGHT SECURITY RATINGS

BitSight Security Ratings are a measurement of an organization's security performance. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data. Armed with daily ratings, organizations can proactively identify, quantify and manage cyber security risk throughout their ecosystem.

Unlike existing security assessment tools that examine a company's policies or conduct periodic scans, BitSight continuously measures security performance based on evidence of compromised systems, diligence, user behavior, and data breaches to provide an objective, evidence-based measure of performance. This data-driven, outside in approach, requires no information from the rated entity. With BitSight Security Ratings, organizations can shift from time and policy based security risk management towards a continuous outcome based model that is both effective and efficient.
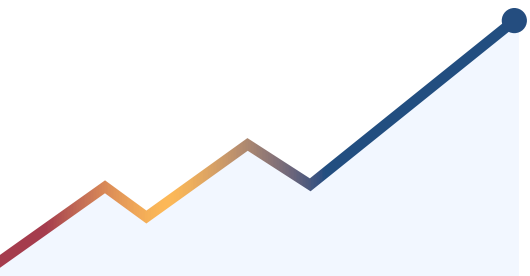
HOW ARE BITSIGHT SECURITY RATINGS CALCULATED?

BitSight Security Ratings range from 250 to 900. The higher the rating, the more effective the company is in implementing good security practices. BitSight Security Ratings are calculated using a proprietary algorithm that analyzes and classifies externally observable data. The ratings are generated based on four classes of data -– compromised systems, diligence, user behavior, and data breaches.

Compromised Systems observed by BitSight represent evidence of successful cyber attacks. Examples of compromised systems include communication with known botnets, spam, malware and more. Although a compromised system may not necessarily equate to data loss, each one is an indication that the organization has been compromised in some manner.

Diligence data points are an indicator of whether a company has taken steps to prevent an attack. BitSight analyzes security configurations such as SSL, SPF, DKIM, DNSSEC and more to measure a company's effectiveness in implementing these controls. Proper email server configuration, for example, can help prevent email related attacks and indicates that a company has employed good risk management practices.

Security Ratings are updated daily and accessible through the BitSight platform and via the API. In addition to ratings, historical trends, compromised systems and diligence details, industry and peer comparisons and more are available on the platform.

HOW ARE COMPANIES USING BITSIGHT SECURITY RATINGS?

Benchmark Security Performance

BitSight Security Ratings for Benchmarking enables organizations to quantify their cyber risk, measure the impact of risk mitigation efforts, and benchmark their performance against industry peers. BitSight provides a detailed view into a company's own compromised systems and diligence data. These details can be used to better identify the sources of risk and take swift action to mitigate it. BitSight Forensics can provide a company with specific information on communications with Command and Control servers to remediate potentially harmful infections. By benchmarking security peformance, organizations can better communicate key performance indicators to the board while simultaneously providing risk and security teams with actionable information to address serious issues.

Manage Risk Posed by Third Parties

Whether an organization has to manage an abundance of third party vendors, potential new clients, business partners or acquisition targets, continuous visibility into their security performance is crucial. BitSight Security Ratings for Third Party Risk Management help organizations quickly and cost effectively mitigate risk within third party networks. With these ratings, businesses can proactively identify issues within their extended network ecosystem, prioritize and streamline further assessment and drive conversations about security controls. A wealth of data on current and historical performance of different compromised systems and diligence risk vectors allows organizations to better understand potential vulnerabilities and engage with third parties before data loss.

Underwrite Cyber Insurance

Cyber insurance is a fast growing industry, with demand outstripping supply. With a lack of actuarial data, insurers need actionable insights into the security posture of applicants. BitSight Security Ratings for Cyber Insurance provides insurers with a historical record of an applicant's security performance along with the ability to continuously monitor companies beyond the application process. Insurers and brokers can gain insight into the relative performance of a company's security program in relation to peers and industry averages. In addition, BitSight has specialized features designed for underwriters such as policy notes and folder dashboards. For companies looking to purchase cyber insurance, Security Ratings can be used to demonstrate a proven track record of security performance and negotiate comprehensive coverage and lower premiums.