BITSIGHT®
The Standard in SECURITY RATINGS

TECH NOTE

BitSight Data

A commitment to quality, breadth and innovation

A DATA DRIVEN VIEW OF SECURITY PERFORMANCE

BitSight Technologies collects externally available internet data on security performance of companies worldwide. This data is gathered from over 100 sources looking for malicious activity, social chatter, vulnerabilities, and configuration diligence across the globe. With this data, BitSight produces daily Security Ratings by using a proprietary algorithm to process both diligence and event data. Then, within the BitSight portal customers can see a breakdown of security performance in each of the nine risk vectors that feed into the Security Ratings. Risk and security professionals in a wide variety of industries are using Security Ratings to mitigate cyber risks within their organizations and across their extended networks.

To ensure that BitSight provides the most relevant and comprehensive ratings on cyber security performance we are committed to continuously expanding the data quality, breadth and innovation used in Security Ratings. We do this by owning proprietary data streams and working closely with partners around the globe to ensure access to multiple and diverse data feeds. We do rigorous analysis on the quality, origin, and confidence of all collected data. Because of the breadth, we can cross-correlate and improve confidence based on multiple observation points and methods. In addition, we can provide historical data going back three years, giving organizations a long term view of security performance across the enterprise. By focusing on data quality, breadth and innovation, BitSight is committed to providing the industry standard of security ratings for businesses and organizations worldwide.

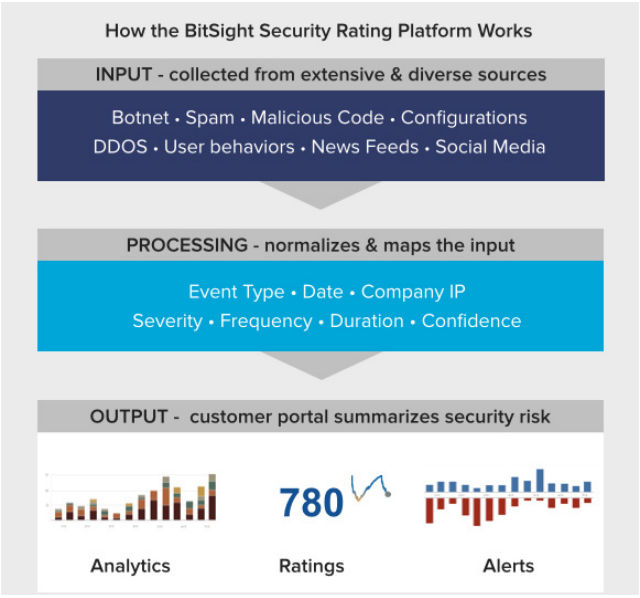
SECURITY RATINGS DATA

BitSight's Security Ratings are comprised of two main classes of data:

Event Data:
BitSight passively collects terabytes of publicly observable data about security events. We look for evidence of botnet infections, spam messages, malware servers, unsolicited communication, and other indications that a network has been compromised.

Diligence Data:
BitSight collects information about security diligence practices, such as SSL, SPF, and DKIM configurations.

This brief outlines the Event and Diligence data that are included in Security Ratings, with a breakdown of each individual risk vector and how we evaluate them.



The BitSight Security Ratings Platform

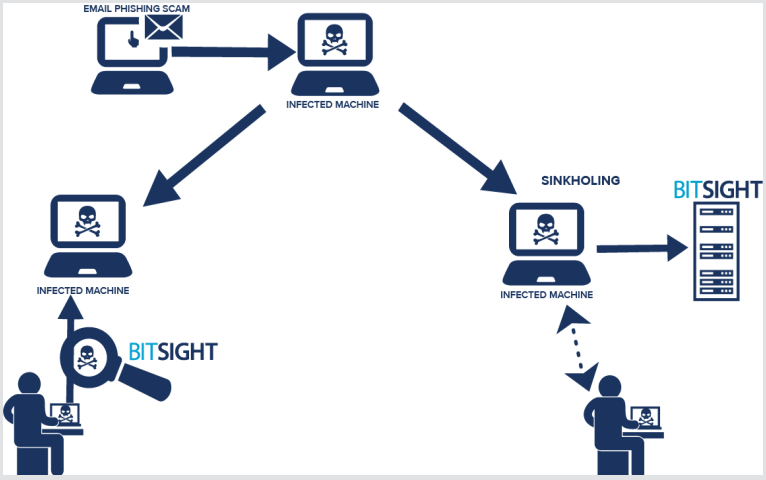
EVENT DATA

BitSight collects information about a wide range of security events. These events fall into the following categories:

Botnet Infections

A bot network, or botnet, is a collection of compromised devices, or bots, that an attacker can use together to carry out malicious activities such as sending spam messages or performing distributed denial of service (DDOS) attacks against a website or service. A botnet infection means that one or more devices on a company's network is acting as part of a botnet. Devices participating in botnets can drain resources from a company and/or steal sensitive data and send it back to a remote command and control server.

BitSight determines the presence of a botnet infection through evidence that one or more devices on a company's network are observed participating in a botnet. We identify botnet activity using honeypots and sinkholes that let bots communicate with us instead of (or in addition to) their command and control servers. BitSight operates some of these sinkholes, while others are operated by our data partners. For botnets using domain generation algorithms, we register a set of randomly generated domains and wait for devices to connect to them.



Identifying Botnet Activity

An attacker sends a phishing email to an employee who clicks the link, downloading harmful malware onto a company device. BitSight has multiple methods of detecting and intercepting traffic from a botnet and attributing it to a specific company's network. This illustration demonstrates two possible scenarios:

- BitSight can detect this infection by monitoring known bot networks and attributing the IP address of the connecting infected device back to a company (left).
- BitSight also detects this infection by intercepting communications between an infected device and a Command and Control server through sinkholing (right).

Spam Propagation

Unsolicited bulk email (spam) messages originating from a company's network indicate that one or more email addresses controlled by the company have been compromised in a way that allows an attacker to use an account. In most cases, the employee whose account has been compromised will continue to be able to send legitimate messages, so they may be unaware that the address has been compromised. If this activity persists, legitimate mail from the company may be flagged as spam and not reach its intended recipients.

BitSight is able to detect spam propagation using honeypots, spamtraps, and email addresses that are published in places where they will likely be harvested by spammers. These email addresses are not used to send mail or perform any useful services, so all mail received by them is considered spam. One type of spam propagation mechanism that we observe is a spam bot, which is a botnet used for sending out bulk email messages from multiple devices simultaneously.

Malware Servers

Malware servers are devices on a company's network hosting malicious software or websites used for phishing, fraud or scams. By hosting malware, these servers put visitors (including employees and customers) at risk and may make legitimate information inaccessible. Any company data stored on the server may also be compromised.

BitSight identifies malware servers by monitoring the traffic going to and from known malicious servers and by working with data sources that perform content analysis and scanning to locate malicious code. Malware servers can host a variety of different exploits, including fake antivirus software, drive-by downloads and phishing websites.

Potentially Exploited Hosts

A network may be exploited when a device is showing indications that it may be compromised, but a specific infection has not been identified. This can occur when the impact of an infection is limited to only a few applications, or when a device is infected by a difficult-to-diagnose problem.

We often identify potentially exploited hosts in the course of looking for other events. Typically, we will observe a device acting in a suspicious way that indicates it is either infected or misconfigured. One indication that a host may be exploited is adware, a type of software designed to display advertisements to the user. Adware is typically unwanted and is often accompanied by spyware that monitors computer usage for information that will help advertisers market toward the user.

Unsolicited Communication

Unsolicited communication occurs when a device infected with malware is attempting to communicate with a server that is not providing or advertising any useful services. We are able to discover this type of communication using data collected by software installed on edge devices across the globe as well as by monitoring traffic to darknets, blocks of IP addresses that are not hosting any useful services but passively collect information about devices that attempt to connect to them. Many of these communication attempts are detailed in firewall logs and aggregated.

Data Breach News Events

BitSight collects information about data breach events from a variety of news sources and data breach aggregation services. A breach event is attributed to a company when there is significant evidence that the company was at fault for the data loss, such as a company-issued disclosure notice or investigation from a credit card company. Similar to a security event, any data breach event attributed to a company detracts from its rating. BitSight also aggregates and files Freedom of Information Act (FOIA) requests to collect additional information about reported breaches.

DILIGENCE DATA

In addition to monitoring specific risk vectors, BitSight collects data about security configuration practices. We use this diligence data in conjunction with our risk vector data to determine a company's BitSight Security Rating. We currently observe the following types of diligence data.

Sender Policy Framework

SPF is a DNS (Domain Name System) record that identifies which mail servers are permitted to send email on behalf of a domain. SPF records help prevent spammers from sending emails with forged From addresses. Recipients can check the SPF record to determine whether an email claiming to have been sent from someone at a particular domain was indeed sent from a mail server authorized by that domain.

BitSight assesses each SPF record based on three criteria: syntactical correctness, effectiveness, and number of hosts authorized to send emails on behalf of the domain--the larger the number of hosts authorized to send emails on behalf of a domain, the higher the chances of a mail server becoming compromised. A record is syntactically correct if it conforms to the SPF RFC. An effective SPF record identifies a set of hosts that are allowed to send email on behalf of the domain. In addition, that record would state that email from all other hosts should either be assigned the state 'reject' or 'accept but mark'. A syntactically correct SPF record may still be ineffective if it contains conflicting elements or assigns the state 'accept' or 'neutral' to all other hosts. A domain must only have one SPF answer specified in the DNS TXT record and the SPF record of a domain. If both a TXT answer and SPF answer exist, they must match.

DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) is a protocol designed to prevent unauthorized servers from sending email on behalf of a domain. DKIM allows receiving mail servers to check if the sending domain is authorized by verifying a DKIM key located in the domain's DNS record against a DKIM signature located in the email.

BitSight evaluates DKIM records based on whether a company has a DKIM record for each of their domains and the key length of the public key found in their DNS record. For RSA keys, a length of 2048 bits is recommended; for elliptic curve keys, a length of 224 bits is recommended. BitSight assesses test records the same as not having a record on that domain.

Secure Sockets Layer (SSL)

Secure Sockets Layer SSL is a widely-used protocol to secure communications over the Internet. BitSight looks at a variety of criteria when determining the effectiveness of a TLS (Transport Layer Security) or SSL certificate. In order to be "good", an SSL certificate must adhere to the following rules:

- Today's date must fall within the valid dates for the certificate. If a certificate is expired or if it goes into effect in the future, any data sent to or from the host may be insecure.
- The key must be generated using a secure algorithm, such as RSA, DSA or elliptic curve.
- Keys must be the recommended length or longer. For RSA and DSA keys, a length of 2048 bits is recommended; for elliptic curve keys, a length of 224 bits is recommended.
- The certificate must be signed using a secure algorithm. MD2, MD5, and SHA-1 are considered insecure.
- The certificate must be issued by a trusted certificate authority. Self-signed certificates are evaluated as "warn".

CONCLUSION

BitSight's diverse set of data and wide array of risk vectors helps to produce the industry standard in cyber security performance ratings. By processing high quality data on security events and configurations, BitSight provides a comprehensive view of security posture on tens of thousands of companies across the globe. BitSight will continue to add breadth to our data sources and risk vectors to continuously expand the visibility of a company's performance.

For more information on BitSight data, please contact your BitSight representative or support@bitsighttech.com

BITSIGHT

ABOUT BITSIGHT TECHNOLOGIES

BitSight Technologies is a private company based in Cambridge, MA. Founded in 2011, BitSight is backed by Menlo Ventures, Globespan Capital Partners, Flybridge Capital Partners, Commonwealth Capital Ventures, and the National Science Foundation.

For more information contact us at:

BitSight Technologies
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com | sales@bitsighttech.com