BITSIGHT
The Standard in SECURITY RATINGS

WHITE PAPER

Cybersecurity Risk Rating Solutions Buyers Guide and Recommendations

Buyer's guide for security ratings solutions as well as recommended requirements by use case.

Introduction

This guide has been developed to assist in identifying requirements for a security ratings solution for both third party and first party use cases. It outlines key questions that should be considered during a selection process to ensure that the chosen solution will address common requirements both from a business and operational perspective.

What is a security ratings solutions service?

Security ratings solutions are tools that continuously and non-intrusively collect data to create a quantitative, unbiased measure of an organization's cybersecurity performance. security ratings solutions are created by a trusted, independent organization and are utilized by a wide range of global market participants, including insurers, governments, enterprises, and investors. Security ratings solutions are derived from deep, broad, high-quality security performance data sets and use a repeatable, transparent model to provide meaningful, independently validated measurements of an organization's security performance.

Since security ratings solutions are created from data that is gathered non-intrusively in a systematic manner, it is an objective view of a company that can be normalized across a wide set of companies, industries, and even countries. In order to remain objective, this data should be gathered with no direct installation of agents or software in any individual company. It should also be able to address issues of "gaming" the system by vendors that choose to avoid fixing the infrastructure in favor of obfuscating their security issues.

Security ratings solutions are derived from deep, broad, high-quality security performance data sets

Why does my organization need a security ratings solutions service?

A security ratings solutions service lets an organization review and compare performance for themselves and their third party vendors, business associates, and supply chain partners as objectively as possible from a cybersecurity perspective. Using a common framework to explore security performance, a company can make an informed decision on what level of risk they are willing to assume or mitigate.

Many organizations today use point-in-time assessments and questionnaires to ascertain the security posture of their suppliers and vendors. The issue with this is that many organizations now use an automated answering process to provide "canned" answers for these assessments. When you send an assessment request to a company, your assessment response may be multiple years old. You need a way to objectively verify the answers you get and flag discrepancies.

Similarly, many organizations use a patchwork of tools and KPIs to try and determine the efficacy of their own security controls. Often organizations use overly technical or meaningless KPIs to communicate to business leaders how the security program is performing. A good security ratings solutions solution should use a range of externally observable risk events to determine the effectiveness of the security program over time, and translate that data into easily understandable numbers.

A security ratings solution that has been independently verified to correlate to risk can help facilitate discussions about business impact, prioritization, investment, and roadmap.

The solution should be able to identify and prioritize security issues that impact you and your suppliers

Recommended security ratings solution Platform Capabilities

Security ratings solutions will help your team identify security risk exposure across your ecosystem. Using a common methodology, your team can effectively measure security risk within your digital footprint and get insight into the organizations you are assessing.
The solution should be able to identify and prioritize security issues that impact you and/or your suppliers and communicate the risk in a common language across the supplier relationship consistently. Regardless of the industry of the supplier, the ratings and the data should be viewable by both parties.

Capabilities

The following capabilities will illustrate a best in class approach to security ratings solutions.

Data Collection

The ability to **continuously, non-intrusively collect data** for security controls as well as event data from incidents to include:

- **Certificates and their configurations** – Certificates identify authentic servers, and also may be used for access control as well as encryption of traffic.
- **System ports and protocols used** – Most companies have standard system hardening practices, this identifies if those practices are in force or adequate.
- **Email system configurations** – Knowing if email servers are permitted to send emails on behalf of a legitimate domain, as well as if emails were sent and authorized by that domain.
- **Domain Related Details** – This is observable data related to DNS, Domain squatting, Domain Squatting, use of DNSSEC or public key encryption for DNS server authentication.
- **Endpoint versions and vulnerabilities (Servers, Desktops, Mobile Devices and IOT)** - being able to detect commonly installed operating systems, server software, and browsers.
- **Observation of the use of peer to peer protocols** – peer to peer communications has been identified as containing malicious payloads, so it is recommended to either strictly control or not use.
- **Identification of Exposed Credentials** – If a company's employees credentials are compromised, seeing the disclosures extent and dates can help a company remediate.
- **Indicators of Compromise** – By having the capability to identify systems that have actually been compromised is a critical capability to improve detection and response.
- **Security Incident and Breach Monitoring** – Should have a research staff and process for identifying, categorizing, and presenting security incidents and breaches.
- **Domain Squatting and Spear Fishing details** – Threat intelligence of this nature provides a great amount of detail related to potentially malicious actors or resources they have created to facilitate attacks.

Asset Mapping

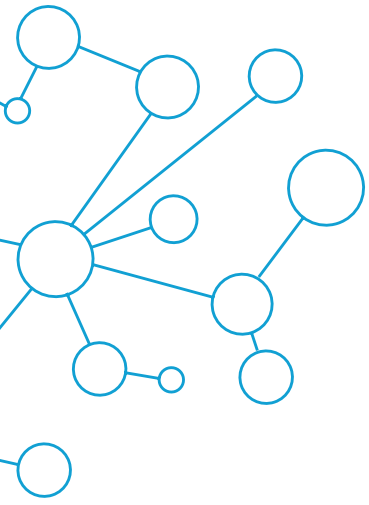
The ability to **map a company accurately and identify the attack surface** of that organization is critical to ensure you are monitoring the right assets.

- Leverage **visual maps** to quickly see where assets within a company fall.
- **Attribute incidents** to specific portions of a company to help remediation.
- **Detect changes** in that infrastructure for both static and dynamic assets.
- **Identify** assets based in **hosted environments versus dedicated company data centers**.
- The ability to **detect service providers** of a given company.
- The ability to **detect products used by a company** via their service providers.

Rating Calculation Methodology

An easy to understand **weighting of risk based on detections** and classification of behaviors that come from an organization's network assets.

- Make it easy to **identify risk** by providing a distribution of ratings from good to bad.
- Identify **indicators of risk** since past performance often indicates future compromise.
- Use risk indicators to **determine monitoring posture and assessment practices.**
- Identify thresholds for vendor tiers, as well as alerts using the weighting metrics.



Integration and API

The solution should include the ability to **tightly integrate** with other tools in your environment to provide their data in a way that enriches and enhances other decision-making processes.

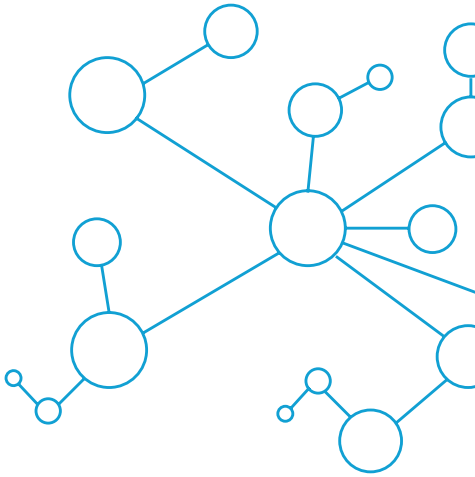
- Out of box integrations with **vendor risk management** platforms.
- Out of box integrations with various **incident response tools.**
- Out of box integrations with **ticketing systems.**
- Out of box integrations for **reporting tools.**
- **Flexible API** to help integrate to systems not already built, or for custom applications.

Discovery of service providers and products

A security risk solution should have the ability to discover technology providers and products in an organization's infrastructure. These data points can be used to identify internal business practice maturity through observations of various service providers or products used.

- Identifying if a company has a **mature governance model** by identifying if they actually have tools in place for: IT Governance, IT Operations, Performance Management, Facility Management, etc.
- Identify **single points of failure** for critical services such as: DNS, CDNs, Telephony, Hardware Platforms, Network Management, Commerce Platforms, and Middleware Platforms, etc.
- See what **dependencies** exist for your third party by seeing their cloud providers and identify where those providers are providing that hosting.

A security ratings solutions service lets an organization review and compare performance for themselves and their third party vendors



Use Cases for security ratings solutions

A Cyber Ratings platform can support multiple use cases in a business environment depending on your requirements. Some of these use cases should include:

Third Party Security Risk Management

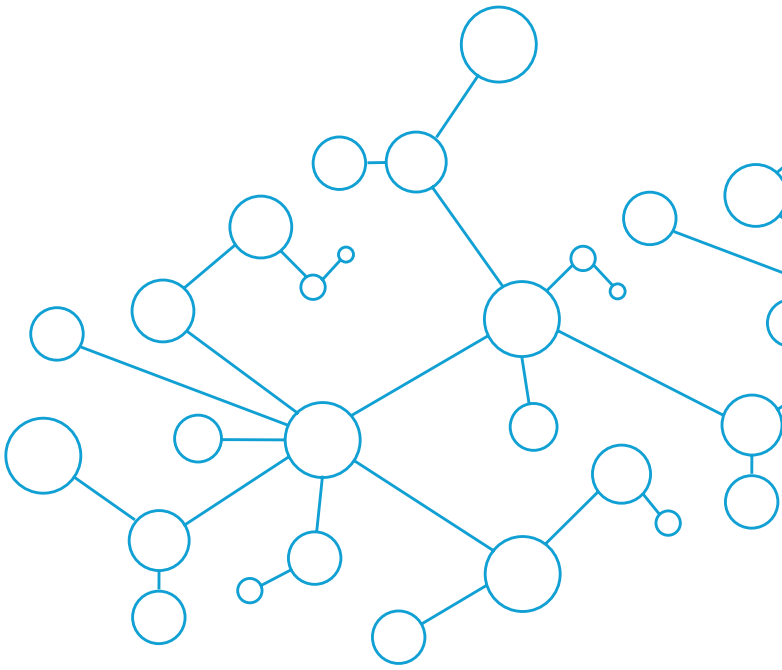
Provide a way to explore risks presented by your vendors in a portfolio view, as well as for each individual vendor, and manage the portfolio efficiently. Provide free access for my supplier to view this data with a minimum of features that enable them to see and address issues noted.

- **Tier Vendors** – Provide the ability to tier vendors in a way that lets you categorize vendors by criticality and recommend an action plan based on their rating.
- **Categorize Vendors** –Include a way to use categorization to cross reference vendors in the context of various other tools in the platform.
- **Vulnerability Catalog and Remediation Instructions** – Ensure that the platform includes a list of vulnerabilities as well as remediation instructions for each.
- **Advanced Filtering of Portfolio Vendors & Findings** – Provide advanced filtering in order to hunt for specific risks, as well as to view findings in a variety of methods.
- **Scheduling and Timers** – Ensure that there are multiple ways to use timers and scheduling for report delivery as well as vendor lifecycle management.
- **Risk Ratios** – Provide multiple ways to identify risk using ratios in a number of contexts. Ratios could be a "findings against assets" or ratio of cloud vs on prem assets, etc.
- **Rating Change Analysis** – Identify rating changes over time, and also track the movement of vendors across various thresholds.
- **Provisional vs Complete Ratings** – When a new company is added to the service library, provide a provisional rating up front in a matter of hours.
- **Vendor Lifecycle Management** – Provide a method to bring vendors through a multi-step process and include recommendations for activities at each stage.
- **Risk Summary Reports** – Provide risk summary reports for the overall portfolio, as well as for each individual vendor in the portfolio.
- **Identify Compromised Event Resolution Timing** – If a vendor has compromised systems, identify how long it takes to resolve issues.
- **Remediation Strategy Details** – When a vendor is analyzed, provide details on how many points they might recover if they remediate specific issues.
- **Network Geographic Footprints** – Show the geographic footprints of vendors individually and as a whole, in order to spot operations in other countries.
- **Rating Details and Findings** – Show all rating details and findings current status, as well as their status over time. Always provide at least one year of history for all data.
- **Vendor Collaboration** – Provide vendors access to the platform so that they can review their own ratings for free. Track and report these engagements and outcomes.
- **Service Providers and Products** – Provide a way to identify vendor service providers and products by type in their infrastructure.

First Party Risk Management

Provide a solution that will allow your organization with the ability to measure, monitor and manage your own cybersecurity performance.
The solution should provide deep analytical capabilities including the ability to understand your organization's relative performance in the context to peers. This solution should also provide deep forensics to analyze possible issues, as well as a tool to forecast changes to your rating should certain mitigation steps be taken. The forecasting tool should provide the ability to prioritize remediation based on severity, making it easy to select the best starting point in remediation.
The features recommended include:

- **First Party Cyber Benchmarking** – Provide licensing and tools necessary to compare your own company to subsidiaries, peers, an industry, or competitors.
- **First Party Peer Analytics** – Provide an anonymized approach to comparing ratings to a peer group with similar sized companies, employee base and industries.
- **Remediation Impact Analysis** – Provide details on recommended approaches to remediating issues found.
- **Remediation Task Management** – Provide a ticketing like tool for internal process management related to remediation steps taken. This tool should provide guidance, reporting, and the option to request a refresh scan for anything remediated. Ideally this should integrate with external ticketing systems.
- **Identify Issues in Cloud Assets** – Be able to identify external hosting providers, locations of issues, findings for those assets and the ability to assign asset importance.
- **Identify Service Providers and Products** – When an issue is identified for an IP address, or domain, ensure that the forensic details provide the service provider, host, and products that are in use behind a specific asset
- **Tag and Assign Importance** – Provide a tagging mechanism to self-identify various assets, as well as to designate importance of assets yourself.
- **View Subsidiary Details in Depth** – Provide a tool to review subsidiaries side by side, and create a report for all subsidiaries using a lens for all risk elements.
- **Easy Searching and Filtering of Findings** – Provide a way to quickly search through, filter, and ultimately report out any findings for your organization.
- **Customizable Dashboard** – Provide a customizable dashboard so that individuals can organize their own tasks, alerts, notifications, and areas of focus in their own way.



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. Fifty percent of the world's cybersecurity premiums are underwritten by BitSight customers, and 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.