SOLUTION GUIDE

Visualize and Assess Cyber Risk Across Your Digital Ecosystem

With BitSight Attack Surface Analytics, part of the BitSight Security Performance Management solution suite.

BITSIGHT®
The Standard in SECURITY RATINGS

Managing Cyber Risk In An Expanding Digital Ecosystem

As data breaches continue to grab headlines and create significant business challenges, companies actively are seeking ways to identify and manage cyber risk. Traditional onsite cybersecurity assessments are time-consuming and only provide a point-in-time snapshot of performance.

Organizations need a way to assess the ongoing state of their security posture in order to identify and detect unknown risk hiding throughout their digital ecosystems.

They also need information that helps them prioritize their limited security resources and focus remediation efforts on the areas that can have the biggest impact.

Cyber threats are constantly evolving, and vulnerabilities are always emerging, so it is incumbent upon companies to protect themselves by monitoring and tracking their security performance continuously over time.

Security ratings help organizations do just that.

BitSight Security Ratings — which are based on independent, objective, and comparable data — empower organizations to assess their current security postures and set achievable targets for improvement.

The robust data set that feeds the BitSight platform provides much-needed broad visibility into an organization's attack surface — and business context to help security leaders and their teams make risk-based decisions about remediation and program investments.

Security ratings have become a common indicator of an organization's overall cyber risk reputation, which is important particularly to board members, executives, and customers. As cyber attacks continue to have a profound impact on businesses, these groups are becoming increasingly concerned about potential vulnerabilities.

In fact, Forrester[1] found that more than one-third of companies agree that they have lost business due to either a real or perceived lack of security rigor. And 82 percent of decision-makers agree that increasingly, the way customers and partners perceive security is important to the way their firm makes decisions.

1 Forrester. Better Security and Business Outcomes with Security Performance Management, A Forrester Consulting Thought Leadership Paper. September 2019.

As the digital ecosystem expands, so does the attack surface.

As security ratings provide an easy-to-understand cyber risk analysis, this data can be used to communicate program effectiveness with key stakeholders.

Ratings are essential to assessing and communicating the status of an organization's security posture, but ratings platforms can provide even more insights beyond just the top-level rating itself. With greater context and visibility, companies can get an even better grasp of where they stand and truly fortify their risk management processes.

Staying Ahead Of Threats Is Challenging

In today's evolving threat environment, cybersecurity is never static. As more organizations embrace digital transformation initiatives to become increasingly agile and boost productivity, they also transform the number of digital touchpoints employees interact with on a day-to-day basis dramatically.

Unfortunately, as the digital ecosystem expands, so does the attack surface. This makes businesses increasingly vulnerable to cyber risk, as bad actors are looking to exploit unmonitored and unknown websites and infrastructures, and putting tremendous pressure on security leaders who don't have a handle on the risk hidden across digital assets in the cloud, geographies, subsidiaries, and a remote workforce. After all, you can't secure what you can't see. As the attack surface expands, security leaders struggle to improve their security rating because they lack a holistic, continuous view of the risks that drive that rating.

Businesses must get a handle on the cyber risk hidden within their growing digital ecosystems — in the cloud, and across geographies, subsidiaries, and the remote workforce. Ignoring this risk opens organizations up to the increased likelihood of a breach.

Using BitSight Attack Surface Analytics To Improve Visibility

BitSight Attack Surface Analytics, part of the BitSight Security Performance Management suite of products, allows an organization to validate its digital footprint, assess high areas of cyber risk exposure, and identify how to improve its cyber risk reputation quickly. This additional context around the organization's BitSight Security Rating, makes it easier than ever to make informed, comparative decisions about where to focus cybersecurity efforts.

In this guide, we will explore the challenges that security and risk leaders face while managing risk across an ever-broadening digital ecosystem. Then, we will look at how they can leverage BitSight Attack Surface Analytics to better understand and manage risk in their expanding digital ecosystems, thereby improving their security ratings and earning their customers' trust.

The Hidden Cyber Risk In Today's Broad Digital Ecosystem

An expanding digital ecosystem can make it difficult to achieve and maintain a strong security posture.

Common obstacles to achieving a high security rating include a lack of visibility across deployed assets including those stored in the cloud; and a lack of tools for asset discovery, management, risk reduction, and a remote workforce.

Let's break down those challenges in more detail.

1. Organizations Can't Secure What They Can't See

As companies seek new opportunities for innovation and expansion, a variety of cybersecurity considerations come into play. The cloud, mergers and acquisitions, and geographically dispersed business units can grow the corporate digital footprint substantially, far beyond its usual perimeter.

Yet organizations often lack visibility into the inventory of critical assets that comprise these ecosystems, and the risk associated with those assets.

In this scenario, managers have an incomplete view of overall security performance and potentially expose their businesses and customers to unnecessary cyber risk.

To grow and scale confidently, organizations must achieve continuous visibility into assets and the risk that may be hiding throughout their ecosystems. Only with this understanding can businesses make strategic decisions about prioritizing their remediation efforts and moving their cybersecurity programs forward.

2. Understanding Cyber Risk Context Is Hard

In order for businesses to get the greatest return on investment (ROI) for their cybersecurity initiatives, they must allocate resources based on the criticality and level of risk associated with each asset. For instance, a top priority could be remediating any incidents that involve a critical asset with a high risk of being breached.

Of course, if these organizations have an extensive digital footprint and lack the right tools to gain visibility into cyber risk, this often means filtering

through massive amounts of data and likely multiple technology solutions to identify the most severe or potentially severe security events.

Without enough information to give context to their current security postures, it can be challenging to prioritize remediation efforts to improve their security rating.

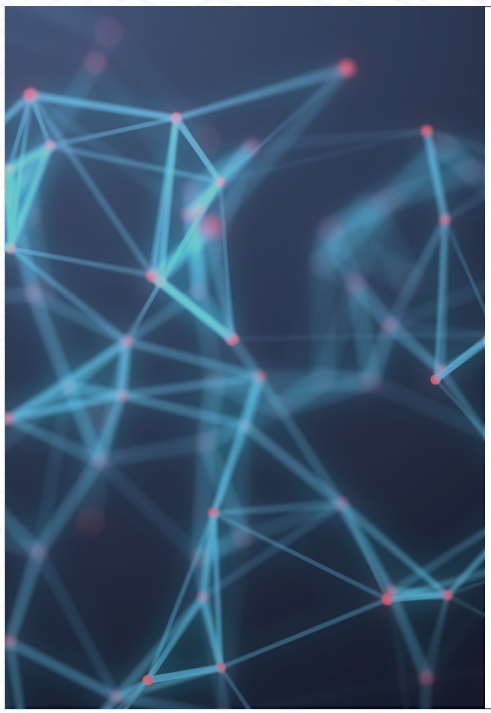
3. Security Teams Lack A Common Language To Quantify Risk

Organizations must be working continuously to improve security performance over time to get the most out of the money and effort they invest in their cybersecurity programs.

Yet too often, disparate systems and teams lack a common language of KPIs, vulnerabilities, and issues. This makes it hard to work towards an organization-wide understanding of security performance and cyber risk.

Only by quantifying risk through a common frame of reference, such as a standard set of KPIs, can organizations track improvement and determine whether they are using their resources effectively, and on those program areas that will lead to the biggest ROI.

Such a framework also will ensure that appropriate teams are held accountable for security performance over time.



More than one-third of companies agree that they have lost business due to a real or perceived lack of security rigor.

-Forrester[1]
Better Security and Business Outcomes with Security Performance Management

Mitigating Risk In An Expanding Digital Ecosystem

Despite these challenges, it is more crucial than ever that organizations achieve broad and continuous visibility into all of their assets across their digital ecosystems. They also need to understand the context for their security rating (the contributing factors) so they can make informed, comparative decisions and focus on what to improve.

Here is how BitSight Attack Surface Analytics makes it possible for IT and security teams to quickly validate their organizations' digital footprints, assess their security postures, reduce risk exposure, enhance their cyber risk reputations — and drive higher security ratings.

Gain Visibility Into Digital Assets So They Can Be Secured

With BitSight Attack Surface Analytics, security teams can gain unprecedented insight into digital assets across their ecosystems.

Instead of manually tracking asset inventory via a spreadsheet, teams can discover all of their assets automatically and identify where they are located for quick remediation. A centralized dashboard outlines the location of all assets — broken down by cloud provider, geography, and business unit — and the corresponding cyber risk associated with individual assets.

If a manager is looking to lead and streamline remediation efforts based on assets, BitSight Attack Surface Analytics provides a way to identify, filter, and organize assets by type more easily; visualize the digital landscape quickly; and identify previously unknown outliers. The manager even can learn which cloud providers the organization is using to store assets in, across subsidiaries and/or recent acquisitions.

Furthermore, teams can leverage additional context to make informed, comparative decisions in order to prioritize and focus cybersecurity efforts. BitSight Attack Surface Analytics leverages the power of the BitSight platform to allow security teams to overlay asset views with objective, quantifiable cybersecurity insights. From here, they can understand better which groups and types of assets are secured properly — and which ones represent the greatest potential for cyber risk.

Based on a view of their digital assets, teams can gauge which assets represent the greatest proportion of risk.

Gaining visibility into an organization's attack surface is the first step to establishing an effective security program.

For instance, if a company has 120,000 records stored in an Amazon Web Services (AWS) cloud environment, but the BitSight Security Ratings platform identifies 120 severe material findings, such as vulnerabilities or infections, this may indicate a significant amount of risk is present and the asset should be prioritized for mitigation efforts. If only three material findings are identified among a million stored records, however, these scenarios can be de-prioritized if other, more material findings are found.

Gaining visibility into an organization's attack surface is the first step in establishing an effective security program. With this insight, organizations can justify actions or investments more effectively, and improve their current security postures and teams' ability to communicate the status of their organizations' security performance levels.

See What's Lurking In Shadow IT

To have a full grasp on an organization's exposure to risk, security teams need a strategy in place to discover shadow IT — those technology solutions that are procured or spun up by functional teams and individuals without IT's knowledge or approval.

Because these information assets don't fall within the control of the IT or cybersecurity departments, security managers lack a complete view of the assets' malware infections, failures, and other weaknesses that can expose the organizations to cyber risk. After all, it is difficult for administrators to secure what they don't know exists.

With BitSight Attack Surface Analytics as the core of a security performance management program, teams can discover unknown assets attributed to their organization and the risk or threats associated with those assets.

For example, managers can uncover unauthorized cases of a server spun up in the cloud, such as an AWS instance in China that previously was not on their radar. They also can discover if multiple cloud instances are at play, perhaps as the result of an acquisition, such as an instance of Google Cloud in a business unit — a surprising find for IT managers who thought their cloud footprint was limited to AWS.

BitSight Attack Surface Analytics can discover cloud providers or cloud-based applications that are not listed in the organization's inventory of contracted vendors.

With these new insights, security teams can pinpoint where the breakdown of control lies, and leverage geographic and IP address information to track

BitSight Attack Surface Analytics gives security teams continuous, broad visibility and context into their attack surface in the cloud.

down the user in question and find out what they are using the asset for. They also can identify if there is any associated cyber risk and enforce the appropriate security practices to mitigate that risk.

Monitor Risk Hidden In Cloud Environments

Cloud migration can make maintaining a desired security posture increasingly complex. Organizations must understand the shared responsibility model for every cloud vendor they work with, and configure each cloud instance securely. If they don't, they open themselves up to cyber risk.

Unfortunately, as their cloud and multi-cloud strategies evolve, many organizations believe that they must also relinquish visibility and control. Traditional security assessment practices can be difficult to scale. And they make it hard for security teams to discover and determine how well they are securing their cloud-hosted assets across various cloud environments, and the portion of the risk *they* own and manage versus their cloud providers.

BitSight Attack Surface Analytics gives security teams continuous, broad visibility and context into their attack surface in the cloud and across hosting providers so they can understand the risk profile of all cloud-hosted assets.

For instance, BitSight Attack Surface Analytics shines a spotlight on the security of cloud-hosted assets based on the number of material/severe findings. These findings can reveal unknown vulnerabilities, infections, and misconfigurations that could expose the organization to the risk of a cyber breach.

BitSight Attack Surface Analytics also layers in additional context such as geographic location. There is no more guessing about security risk locations — the BitSight dashboard provides a map-based view. Security teams can determine the precise location of a vulnerable asset, such as whether an AWS instance in China or Germany is misconfigured, and quickly move to remediate that risk. They can also prioritize remediation efforts by ranking asset importance by cloud provider.

Enterprises with multi-cloud environments also can realize significant benefits from BitSight Attack Surface Analytics. Teams can compare the security posture of multiple AWS instances, or the security of AWS in comparison to a Google Cloud or Oracle instance so that they know where to focus their remediation and training efforts.

If each cloud in a certain geography, or all clouds from a certain vendor have security issues, then there clearly is a training problem. Or, perhaps

one cloud is harder to secure and the organization may want to think about switching providers. Security teams also can identify cloud instances that fail to adhere to corporate security policies so they can take steps to bring them into alignment.

With BitSight data, organizations benefit from a common frame of reference that allows them to achieve true comparative analysis of security across clouds and multi- or hybrid cloud environments.

BitSight Attack Surface Analytics makes it possible for IT and security teams to validate their organization's digital footprint and reduce exposure.

Boost Cybersecurity ROI

In today's threat climate, a key factor in improving any organization's security performance is the ability to have broad and continuous visibility into its digital footprint.

This context empowers IT and security teams to detect unknown risk hiding throughout their digital ecosystem, identify weak areas of their security program, and find failed security controls that require improvement.

These are the types of insights organizations need in order to use their tools and resources most effectively.

Once they have the necessary visibility into their ever-evolving digital ecosystems, these teams can feel confident that they are allocating their limited resources to the program areas that will lead to the biggest ROI — making it easier than ever to align security to the business, reduce cyber risk, improve security ratings, and maintain customer trust.

Achieve Continous Visibility Into Your Digital Ecosystem With BitSight Attack Surface Analytics

Learn more:

www.BitSight.com/attack-surface-analytics

BITSIGHT®
The Standard in SECURITY RATINGS

BitSight
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. Seven of the top 10 largest cyber insurers, 25 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.