
BITSIGHT
The Standard in SECURITY RATINGS
EBOOK
Using Continuous Monitoring Technology to Revolutionize Vendor Risk Management

INTRODUCTION

In the past, the job of a cybersecurity or third-party risk professional included a workflow that went a little like this: Spend the workday reviewing as much data as you can get your hands on; Analyze that data manually for common themes and ideas; Draw conclusions based on these ideas; Make or suggest decisions based on these conclusions.

The data on these vendor risk managers' desks might have come in the form of monthly, quarterly, or annual reports. Depending on the risk category, perhaps they were financial reports, or maybe strategic analyses from major consulting firms, but either way the data was aggregated over the long-term, analyzed using time-consuming processes, and deliberated over in order to reach decisions.

Modern business no longer allows for this kind of slow-and-steady risk management workflow. With the takeover of big data and adoption of artificial intelligence, organizations are able to assess and respond to risks faster than ever before.

Now, data is aggregated from millions of devices, sensors, and users every second. This unprecedented volume of data is often combined with other vendor data sources, then analyzed by software employing machine-learning algorithms to produce conclusions that are constantly updated based on real-time changes to the data set. Vendor risk management professionals then review the conclusions for trends and anomalies, weighing the information against their company's risk tolerance to make strategic decisions.

A process which once took weeks or months is now happening in a second — and beyond that, it's happening every second, so that the most up-to-date information is always just a click away.

Continuous monitoring represents a shift in vendor risk management that has brought TPRM leaders new power when handling their cybersecurity programs.

This strategy is called continuous monitoring, and it represents a shift in vendor risk management that has brought TPRM leaders new power when handling their cybersecurity programs. In this Ebook, we'll explore why continuous monitoring has changed vendor risk management, how security professionals can implement this approach into their programs, and why continuous monitoring is a transformation you should care about.

First, we'll briefly explore what it means to continuously monitor, and where you might have seen examples of companies relying on continuous monitoring in the past.

GAINING THE COMPLETE PICTURE

Continuously monitoring risks and your supply chain is not a new concept, and in some areas of risk management it's already left its mark. Take cybersecurity for example. In this field, continuously monitoring risk has become no less than necessary. Many businesses have internal cybersecurity operations centers where personnel are monitoring the network for incoming threats, then deciding on appropriate remediation measures and neutralizing them as soon as possible. With these monitoring processes turning automated, the time saved in both recognizing and remediating threats is exponential.

2020 exposed businesses to new risks as networks moved remote and at-home employees expanded the threat landscape for organizations across all industries.

Cyber risk professionals, specifically third-party risk managers, rely on continuous monitoring solutions to keep tabs on cyber threats and incidents on their expanding vendor networks — networks which are becoming increasingly complex thanks to the proliferation of internet of things (IoT) devices and malicious actors continuing to take more sophisticated approaches to assessing important data. On top of that, 2020 exposed businesses to new risks as networks moved remote and at-home employees expanded the threat landscape for organizations across all industries.

In most areas of business, the idea of continuous monitoring risks to prevent detrimental business outcomes is nothing new. What is new to many organizations, however, is the ability to use continuous monitoring to identify and remediate risk effectively when managing their third-party cybersecurity networks. The reason? Continuous monitoring requires massive data sources, and now big data and cloud technology has brought vast amounts of cybersecurity data from a variety of sources to third party security and risk professionals for management purposes.

With a continuous view into your program's data, vendor security managers can begin to fill in gaps where they were previously unable to have visibility due to manual processes.

THE BUSINESS IMPACT: EXPANDING MONITORING TO EXPAND YOUR BUSINESS

Cybersecurity professionals are constantly bombarded with changing risk environments, whether they come in the form of updated technology or unpredictable global pandemics. Finding processes that work, and sticking to them, help security leaders stay consistent. So why do we want you to consider a potentially new change to your cyber security practices?

Continuous monitoring is a strategy your organization will only benefit from over the course of your relationships with your vendors. By providing your organization with a consistent, wider view into your risk portfolio, totally monitoring your vendors shrinks the exposure to risk through better, systemic third-party risk management. Instead of gathering point-in-time assessment data during the audit lifecycle, security managers can gain total visibility through complete cyber risk monitoring and reduce the risk their business takes on through working with vendors.

Your Vendors Have Access To More Than You Think

According to Gartner, "Vendor risk management (VRM) is the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance."

In other words, whenever vendors, suppliers, or other third parties have access to your data, there is a risk that something bad might happen to it. This risk is very real — according to Deloitte, 20.6% of business leaders report having dealt with a situation where sensitive customer data has been breached through third parties.

For a long time, questionnaires were one of the only ways to gather IT security information about third party vendors. Now, many companies rely on aggregating and analyzing externally observable cybersecurity risk factors that finally enable the continuous monitoring of vendor risk.

With continuous monitoring, risk and IT professionals can maintain a real-time understanding of the risks they're being exposed to by every vendor in their portfolio. Organizations can monitor and protect the data living outside their network in nearly the same way they monitor and protect internally stored data.

Threats Now Happen Faster, And At Greater Scale

Threats to businesses through cybersecurity avenues have adapted greatly in the last five years. Malicious actors understand the technology, and can access data quicker and wreak greater havoc than ever before. Deloitte reports that "the financial impact of [cybersecurity] failure by a third-party has at least doubled over the past five years... one in five respondents believe the financial impact has multiplied tenfold".

Danger has always lurked on internal and third-party networks, but the scale and speed at which those threats can become financial hits and blows to business operations is now incredibly fast. Taking the right steps to find efficient solutions to mitigate these evolving threats might be what saves an organization when a threat arises.

Deloitte reports that "the financial impact of [cybersecurity] failure by a third-party has at least doubled over the past five years... one in five respondents believe the financial impact has multiplied tenfold".

Take the large-scale cyber breach of shipping giant Maersk in 2017. The Danish company, the largest shipping organization in the world, spent billions of dollars dealing with damage caused by Russian malware NotPetya. The attack originated on the network of Maersk's third-party tax-filing software based out of Ukraine, and within 2 hours had caused enough damage within the network of almost 80,000 employees that the majority of the stunned workforce was asked to turn their computers off and leave for an undetermined period.

After two weeks of 24/7 remediation efforts, the Maersk employees started returning to work, but only after the company experienced financial loss and extreme delays in their shipping operations. Some subsidiaries turned to manual management of shipping operations where they could, but the speed and severity of the breach prevented operations from returning to normal for months, all of which could have been avoided, or remediated more efficiently with continuous monitoring third-party risk management.

Mature Your Program Faster

Committing to a continuous cyber risk monitoring strategy for managing your vendors not only reduces the risk associated with working with more and more vendors, but also helps mature your TPRM program to handle more with less. A mature TPRM program operates efficiently and proactively mitigates risk, instead of waiting for risks to present themselves.

With the maturity that a continuous monitoring approach brings to managing third party risk, organizations do not need to rely on their vendors for **visibility into their entire threat landscape**. Without a continuous monitoring approach, security managers are stuck basing their third party risk management decisions on the subjective data and responses their vendors submit.

Besides of the time-management pressure to follow up with vendors and receive the needed responses with enough time to make business decisions, there is inherent risk associated with trusting point-in-time data to be reflective of a vendor's total risk portfolio outside of the assessment period. It also can be time-consuming to verify vendor assessment responses, so most third-party risk managers rely on subjective assessment responses without knowing their real level of accuracy.

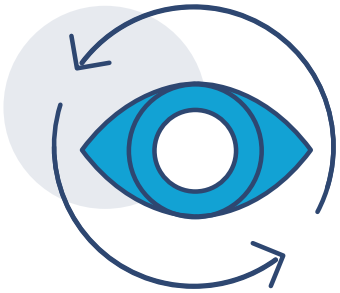
There is no longer a need to rely on subjective vendor data when security leaders have access to their own data pool through **continuously monitoring objective security indicators**. This can be true during the early stages of onboarding a vendor, as well as during the assessment and offboarding phases. Where TPRM leaders used to need vendor reports throughout the vendor lifecycle, they can mature their program through continuously monitoring their vendor pool and removing the need for customer-reliance during the entire vendor lifecycle.

"Total Portfolio" Third Party Risk Management

Deloitte reports in their 2020 third-party risk management global survey that "senior executives are extending their focus beyond risk to include a broader view of third-party management, enabling synergies in the long term…" representing the growing focus on tackling cybersecurity from the portfolio management perspective.

The ultimate goal of implementing a continuous monitoring strategy is not just to follow a cyber risk best practice, but to help create more efficient processes through developing a **total portfolio perspective of managing third party vendors.** When treating your organization's vendor risk as one big portfolio where each piece is vital to the overall success and is handled the most efficient way, organizations:

1. See better alignment between all parties involved in third party risk management, including security leaders, your board, and your vendors.
2. Have broad visibility into every aspect of their TPRM programs, instead of facing roadblocks where manual processes might still be used, or ignore parts of the program completely.
3. Create a sense of consistency across the vendor lifecycle. Continuous monitoring and other efficient vendor management strategies are useful when applied at different parts of the TPRM process, but value is truly found when these approaches are used across the board with your entire third party program.



By reaching a point where you can approach your third party risk management program in a way that applies efficient processes across the portfolio, organizations can get the most value out of the resources they put into managing their vendors. Finding how to implement continuous monitoring where you were previously relying on more manual, or point-in-time assessments, is a critical piece of reaching a total portfolio vendor risk management point.

Next, we will walk through how to implement a continuous monitoring strategy in your vendor risk management program, from different levels of continuous monitoring to where BitSight can support your program.

SO NOW, HOW CAN YOU START CONTINUOUSLY MONITORING YOUR VENDORS?

Maturing your TPRM program by implementing a continuous monitoring vendor management strategy doesn't have to be complicated. Monitoring technology has adapted to meet the needs of security managers by easily merging with their processes at every stage of vendor management and producing immediate, meaningful results.

Three key steps to start using a continuous monitoring approach to manage your organization's third party risk include:

1. **Integrating your vendor risk landscape with a monitoring technology**, such as the BitSight for TPRM product, to give the monitoring platform complete access to your endpoints both internally and across your vendor network. Instead of focusing just on the most obvious points of risk in your program, integrating a continuous monitoring capability gives visibility into each vendor's risk landscape.

   Your vendor risk profile might include more than you think. It is important, and more efficient, to keep an eye on each vendor's cybersecurity posture with continuous monitoring automation because you **get visibility into critical external vulnerability data like**:

   - On premise cyber data
   - SIEMs
   - Firewalls
   - Shadow IT
   - Remote office network accessed by employees
   - Subsidiaries & GEOs
   - Cloud data
   - Your expanding digital footprint, and more

More informed, data-driven decisions can be made once vendor security manager's have full-access to their vendor's endpoints, instead of just manually monitoring the areas of their vendor's program that they deem the most important, or have the time for.

2. Bringing the continuous monitoring technology to your **entire vendor risk management program**. With total program integration, security leaders can benefit from automated, data-driven processes during the vendor onboarding and assessment stages, all the way through the end of the vendor lifecycle.

   Becoming extremely efficient in one area of vendor lifecycle management is great, but if you're bogged down with manual and outdated processes in other stages than your progress might be useless. When continuous monitoring is combined with other efficient vendor management processes, including tiering your pool of vendors based on criticality to the business, your entire program can run more efficiently. When you tier your vendors, and then can continuously monitor those tiers, the alerts and data you receive from your monitoring software is more impactful and leads to better informed decision making.

Using a solution like security ratings, executives can track changes in actual cyber risk against the timelines of certain solution implementations.

3. **Satisfy your board with reliable metrics and improved ROI**. The final step to secure your complete value from implementing a continuous monitoring strategy is when you're communicating your vendor management results and status with the board. Continuous monitoring allows for more updated metrics that your internal team can pull whenever they need to put together a security presentation for the board. Third party security leaders no longer have to rely on the most recent audit period as the vendor-representation the board sees.

   You can also trust that your data and updated cybersecurity metrics represent your complete vendor portfolio, instead of just the pieces that you were able to manually pull. With the real time data-access security leaders gain from continuously monitoring their third parties, companies can make quicker third-party risk decisions, reducing the time it takes for the board to see the return on investment for their cybersecurity spend.

TPRM managers no longer need to perform as many assessments when reassessing vendors with continuous access to vendor data, saving time and money spent on assessments each year. Onboarding vendors can also be done quicker with the accuracy provided by a continuous view into potential third-parties. Organizations don't have to wait for new vendors to provide subjective security data, they can monitor and make third-party decisions efficiently on their own terms.

Continuous Monitoring With BitSight for Third Party Risk Management

BitSight helps security managers implement the most efficient processes throughout their vendor lifecycle. BitSight for Third Party Risk Management includes continuous monitoring technology that gives vendor risk managers a complete and trusted view into their risk portfolio. Instead of relying on yearly assessments or security information that is collected and reported out by the vendors themselves, BitSight's continuous monitoring software presents each vendor's security status with the BitSight Cybersecurity Rating.

For managers, much of the work of risk-based reporting comes down to choosing the most relevant performance indicators.

The BitSight rating reflects the cybersecurity posture of a third party organization based on risk factors like botnet infections, out-of-date devices, TLS/SSL certificates, file sharing behavior, and more. With our continuous monitoring technology scanning vendor's risk vectors for changes in behavior or potential concerns, the rating is an updated, total view into each of your vendor's cybersecurity posture.

The Only Independently Verified Continuous Monitoring Database

Not all continuous monitoring technology is the same, and in a cybersecurity industry growing crowded with solutions claiming to solve security managers' problems, it's important to find a reliable continuous monitoring program that is worth spending your resources on.

BitSight Cybersecurity Ratings have been proven to correlate with the risk of data breaches. AIG research shows a company's overall BitSight rating, as well as their grades in given risk categories, can reliably predict future security performance if they remain unchanged.

- Companies with a BitSight Security Rating of 400 or lower are five times more likely to experience a breach than those with a rating of 700 or higher.
- Organizations have a 3x higher chance of suffering a data breach if 50% of your computers run outdated operating systems.

- If your Botnet grade is B or lower, or the file sharing grade is B or lower, or the grade for open ports is an F, you have 2x more likelihood of suffering a breach.

Not only can organizations use BitSight ratings to protect against vendors who have a higher likelihood of experiencing a cyberattack, but BitSight customers can also trust that relying on BitSight for continuous monitoring technology is a profitable business solution.

Solactive research shows that companies with strong cybersecurity performance, including organizations with higher BitSight ratings, financially outperform their market peers by up to 7%. Only BitSight ratings have been used by organizations to link their cybersecurity performance to overall company governance resulting in higher financial performance. Cybersecurity actions, including monitoring your vendors with BitSight's continuous monitoring technology, can enable your business and create measurable value.

Personalized Monitoring Options

Finding the right level of continuous monitoring technology that meets the needs of your organization will help promote efficiency across your TPRM program without overspending or underutilizing the opportunity to gain visibility into your vendor risk. BitSight's TPRM product promotes efficiency and successful TRPM management with our customers by allowing for flexible, personalized continuous monitoring packages where organizations can select the best level of monitoring for their business needs.

Each customer has unique needs for monitoring their vendors, which is why BitSight offers customers the ability to customize their continuous monitoring packages. Customers can select different levels of monitoring for each vendor, prospect, or other organization, based on their specific relationship with that organization:

1. **Total Risk Monitoring** - Some third-party program managers get more out of focusing their resources and attention on a handful of highly critical vendors. Total Risk Monitoring provides an encompassing continuous monitoring view into a selected vendor, usually critical vendors and business partners connected to the most sensitive company information and critical operations. This all-inclusive monitoring option gives vendor risk managers:
    - Daily ratings and data updates
    - Access to historical data on the vendor or business partner for the past year
    - Constant visibility into a vendor's risk posture

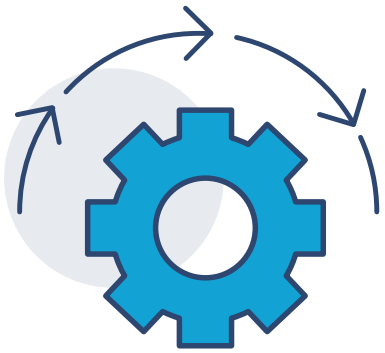
2. **Risk Monitoring** - Following cyber risk best practices for a mature TPRM program, organization's shouldn't ignore the cybersecurity status of their non-critical vendors. With a risk monitoring selection in the BitSight platform, vendor security and risk professionals will be notified only when critical updates occur for the selected organizations, usually lower tier or early prospective vendors. The risk monitoring level gives security leaders:
   - Notifications only when the security posture of a third-party becomes critical and needs attention
   - A sense of security and visibility over lower-tiered vendors, instead of sacrificing knowledge on non-critical vendors for visibility into the top-tier

3. **Risk Assessor** - If a customer isn't fully ready to assign a specific level of monitoring to a vendor, or if they are onboarding a new vendor and aren't sure of the vendor's historical cybersecurity performance, the risk assessor tool within the BitSight portal can be utilized to help guide a monitoring selection. Risk assessor subscriptions can also be applied to vendors that the organization needs more information on as they are working to fix vulnerabilities within their portfolio.

Full Coverage Packages

BitSight offers users suggested continuous monitoring packages based on their organization's third-party security needs.

Where continuous monitoring using a Total Risk Monitoring approach for all vendors can provide a solid defense against cyber threats, organizations are using vendors more and more. Monitoring a pool of 5,000 vendors with updates every time there's a change in a vendor's BitSight rating might get overwhelming, but finding the best package that gives security managers the right level of visibility into each vendor is possible with BitSight's continuous monitoring options. Users can also change their level of vendor monitoring at any time to better meet the needs of a vendor, or to monitor a vendor thoroughly during a critical use period.



CONCLUSION

Finding the time and motivation to make process changes to your TPRM program is hard. Doing away with your current vendor monitoring processes to adopt a continuous risk monitoring approach is worth making the change. Bring your third-party risk management program into the next level of maturity by tackling your inherent vendor risk with a continuous monitoring approach such as the different offerings included in BitSight's TPRM product. See effective results today when you introduce continuous monitoring to your program, and expand it to integrate with your entire program.

We are already faced with a world of change, it is time to start implementing changes that will further your business for the better.

Request a personalized demo with a BitSight representative today to learn more about applying a continuous monitoring approach to your third party risk management program.

GET STARTED

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. Seven of the top 10 largest cyber insurers, 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.