
THRIVE THROUGH
TRANSFORMATION
BITSIGHT
The Standard in SECURITY RATINGS
EBOOK
3 Ways to Get the Most Out of Your Security Investments

INTRODUCTION

In today's competitive business climate, becoming a digital entity is no longer optional — it's essential to your success. Over recent years, organizations around the world have been investing in more and more digital transformation initiatives to ensure they're as efficient, agile, and flexible as possible. In fact, according to IDC's predictions, direct digital transformation investment spending is expected to approach $7.4 trillion between 2020 and 2023.[1]

Meanwhile, an analysis conducted by Accenture found that 79% of organizations are adopting new and emerging technologies faster than they can address related security issues.[2] And, in the end, this finding — though alarming — isn't necessarily all that surprising. While the ongoing wave of digital transformation opens up exciting opportunities for innovation, it also widens your attack surface — exposing you to new and evolving cyber risks, while making it increasingly difficult to gain continuous, broad visibility into your critical assets.

And getting this context into the cyber risk associated with your digital ecosystem has only become more challenging over recent months, as more employees are working from home than ever before. During the period of March 2020, we looked at a sample size of 41,000 organizations and found that up to 85% of the workforce in some industries had shifted to remote work. Of course, with this shift, employees are moving from working on secure corporate IPs to potentially flawed Work From Home-Remote Office (WFH-RO) networks.

From a cyber-risk perspective, residential networks exhibit their own unique attack surfaces and are increasingly susceptible to malware. In fact, we found that 61.2% of WFH-RO IP addresses that have one or more services open have an exposed cable modem control interface — and there's up to a 20x higher population of malware on remote office networks than corporate ones.

To make matters more complex, while security leaders are being challenged to mitigate the new and evolving cyber risks introduced through this new operating environment, security budgets are decreasing. As a result of the economic impact of the COVID-19 pandemic, Gartner estimates there will be a $6.7 billion decrease in global security spending in 2020, and Forrester warns security teams to expect lean budgets and the trimming of already-thin staff.[3]

In this ever-evolving cyber landscape, one thing remains clear: As security budgets decrease, businesses transform digitally, and teams continue to adjust to the "new normal" operating environment, it's increasingly critical for security leaders to find ways to do more with less. In order to get the most out of your investments in security tools *and* protect your data, you need to rethink traditional methods of mitigating risk and automate wherever possible.

That's where BitSight for Security Performance Management (SPM) comes in — empowering you to enrich the threat intelligence you're already collecting to maximize your cybersecurity ROI and prevent a potentially damaging breach or incident. Read on to learn three ways our suite of SPM solutions gives you the data-driven insights, context, and visibility you need to get the most out of your security investments.

[1]https://www.idc.com/getdoc.jsp?containerId=prUS45617519
[2]https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf
[3]https://www.darkreading.com/cloud/cybersecurity-spending-hits-temporary-pause-amid-pandemic-/d/d-id/1337970

1. IDENTIFY AND REMEDIATE CYBERSECURITY GAPS WITHIN YOUR EXISTING TECH STACK

In today's cyber risk landscape, new vulnerabilities are constantly being exploited and potential threats can escalate very quickly. Expectations and standards of care are always in flux — and what constituted "adequate" security yesterday may not be enough today. As the attack surface continues to grow, it's more important than ever for you to quickly identify and remediate cybersecurity gaps that exist within your infrastructure.

Do You Know Where Your Cybersecurity Gaps Are?

There's a lot that goes on behind the scenes between your network and the Internet — some of which your current security technology may not provide any insight or visibility into. Even if you have a Firewall, Intrusion Detection System (IDS), and other security controls in place, you likely do not have full context into all of the traffic occurring between various endpoints and your infrastructure across on-premise, cloud, and remote office environments.

From open ports to missing patches, there are a variety of potential cybersecurity gaps in your existing controls that you may not be aware of. In order to protect your data and maintain your desired security posture, you need to have a system in place to identify and address these flaws before they lead to a breach or other security incident.

This visibility is increasingly vital as Shadow IT, potentially unprotected applications being used without IT's knowledge, continues to pose a major threat to business operations. As your digital ecosystem expands, it's critical that you have the ability to discover hidden assets, assess them for risk, and bring them into line with corporate security policies.

Get More Out Of The Security Investments You've Already Made

Now, more than ever, organizations need to go beyond a static, compliance-oriented approach to cybersecurity. Checking a box in order to keep up with the latest regulations is not enough[4] and falling behind on implementing security updates or patching can lead to vulnerabilities that malicious actors can easily exploit. In fact, according to a recent Ponemon Institute survey, 60% of breaches involve vulnerabilities for which a patch was available but not applied.[5]

[4] https://info.bitsight.com/the-urgency-to-treat-cybersecurity-as-a-business-decision
[5] https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

Here's where BitSight's powerful data comes in. BitSight Security Ratings are calculated using externally observable data on compromised systems, security diligence, user behavior, and public disclosures. These four data categories are comprised of various risk vectors, including everything from botnet infections and exposed credentials to open ports and patching cadence. Through the Internet traffic insights we routinely collect, we can find evidence of where your existing security controls are failing and offer outside-in visibility into your company network. These insights into the vulnerabilities facing your organization empower you to understand the risk and likelihood of a breach.

> **"While regulation forced organizations to act where they were doing nothing, it has also created bad decision making in the context of checking boxes... At worst, compliance forces us to spend money where we don't need it and keeps us from investing where we should."**
>
> - Gartner, The Urgency to Treat Cybersecurity as a Business Decision

Understand Your Attack Surface

It's become increasingly clear that a rigorous and ongoing approach to cybersecurity requires you to have this broad visibility into your growing attack surface — so that you can identify your risk exposure from outdated software, undetected malware, known and unknown vulnerabilities, unsecured access points, and misconfigured systems.

With BitSight Attack Surface Analytics and our suite of SPM solutions, you can continuously monitor, measure, and communicate the efficacy of the security controls you currently have in place, and gain insight into the inherent risk present throughout your expanding digital ecosystem. This unprecedented contextual data about your infrastructure makes it easier than ever to detect gaps in your current security controls, enrich the security analysis you're already conducting, and remediate issues faster.

And with our Work From Home - Remote Office solution, you can gain visibility into the risk present throughout the expanded operating environment caused by the widespread shift to remote work. This powerful offering enables you to import WFH-RO IP addresses and monitor them for open ports, malware traffic, out-of-date OS and browser software, and more — making it easier than ever to evaluate material findings that could pose significant risk and prioritize your remediation efforts.

Through BitSight's integrations with SIEM tools like Splunk, you can also extract more value from the security data you may already be collecting. With these integrations, you can pull your BitSight findings into existing security workflows and dashboards — so you can refer to all of your threat intelligence insights in one place. By streamlining this process of collecting and using cybersecurity data, you can optimize your risk management program and maximize your cybersecurity tech stack ROI.

2. AUTOMATE YOUR RISK DISCOVERY AND ASSESSMENT PROCESSES

Accustomed to working in a physical security operations center (SOC), where collaboration and teamwork are key, today's security teams must find ways to operate efficiently in our "new normal" environment. While this disruption has presented a challenge, it also offers an exciting opportunity for you to rethink how your infrastructure works — and find new operational efficiencies.

You can use this time to automate traditional security processes and help your team shift gears from a reactive, tactical, alert-based methodology towards a proactive, strategic, risk-based approach to security performance management.

Establish A More Strategic Risk Reduction Program

For years, security teams have been inundated with alerts, many of which were proven to be false negatives. In our "new normal" environment, it's much harder to cross-check and prioritize alerts with fellow team members. This leads to an escalation of alerts, delays in time-to-response, a greater consumption of manpower, a higher rate of staff burnout, new security risks, and the potential for threats to slip through the cracks as teams focus on remediating the false negatives.

Automating security processes can help teams become more proactive. Instead of responding to every alert in the same manner, today's security professionals must learn how to be more strategic by prioritizing their remediation efforts based on the areas of highest exposure and disproportionate risk. Essentially, they need to do more with less by moving from making cybersecurity decisions based on fear, uncertainty, and doubt to a risk-based, outcomes-driven approach.

Go Beyond Point-In-Time Assessments

Traditional cyber assessments only provide a point-in-time snapshot of security performance — making it increasingly difficult for you to perform truly comprehensive, real-time comparative evaluations. In today's ever-evolving cybersecurity landscape, it's critical that you continuously monitor your security controls — so that you can discover and mitigate vulnerabilities in a faster, more streamlined way.

BitSight Security Ratings, which are based on independent, objective, and comparable data — empower teams to better understand their organizations' security postures so they can prioritize resources based on the areas of greatest risk. Through this ratings data, you can continuously monitor your IT infrastructure for vulnerabilities such as unpatched systems, misconfigured software, open access ports, and compromised systems. With this detailed view, it's easier than ever to identify the security gaps across your attack surface and take swift action to mitigate risk.

> **"Societal perception is dominated by fear, uncertainty, and doubt. It results in poor engagement with executives, unproductive exchanges, and unrealistic expectations. Ultimately, it leads to bad decisions and bad investments in cybersecurity."**
>
> - Gartner, The Urgency to Treat Cybersecurity as a Business Decision

Gain Increased Visibility And Context Into Your Expanding Attack Surface

Without clear and continuous visibility into all the assets that comprise this ecosystem, it becomes difficult to identify hidden areas of risk lurking in the shadows. With BitSight Attack Surface Analytics, you can validate and manage your digital footprint across a complex environment involving cloud service providers, various geographies or business units, and remote office environments. This solution makes it easier than ever for you to discover Shadow IT and unknown risk hiding throughout your extended ecosystem — and continuously monitor the ongoing security posture of your cloud and remote office environments.

When paired with a security rating, this additional context can eliminate much of the tactical, manual groundwork involved in responding to every alert and sifting through potential threats. Your busy security team can make more informed, comparative decisions about where to focus your cybersecurity efforts, rather than fixing issues as they arise. In addition, you can prioritize remediation efforts based on areas of disproportionate risk, and report on improvement using a standardized, easily understandable KPI.

3. MAKE STRATEGIC, DATA-DRIVEN CYBERSECURITY DECISIONS

Data can be the key to making more informed security decisions — and ensuring you're spending your security dollars effectively. In order to get the most out of your increasingly limited security resources *and* meet or surpass industry benchmarks, you need visibility into the relative performance of your security program — and insight into the cyber risk present across your ecosystem.

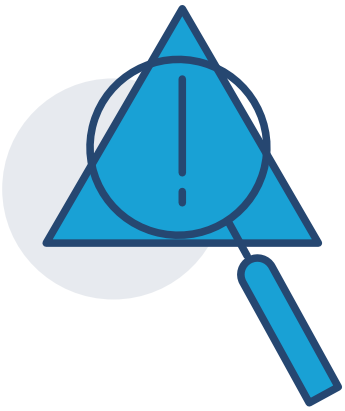
Understand And Meet Rapidly Changing Standards Of Care

It's never been more important for security and risk leaders to know their industry's security performance standards — and conduct peer and sector-wide security benchmarking. A failure to meet customer requirements and industry-wide standards of care for cybersecurity can result in legal, financial, and reputational repercussions. But, due to the ever-evolving nature of the cybersecurity landscape, expectations and standards of care are constantly in flux.

With BitSight Peer Analytics, you can gain unprecedented visibility into the security benchmarks that exist in your industry, sector, and peer group — based on the security performance data of hundreds of thousands of global organizations. Armed with these insights, you can determine the security posture your company should strive to attain to win new business and remain competitive in your market. This solution empowers you to uncover gaps in your cybersecurity program based on a comparison of risk vectors within your peer group — and prioritize investments for the areas that can have the greatest security performance impact.

Gain Visibility Into Security Performance Across Business Units And Subsidiaries

As cyber threats evolve and your digital ecosystem expands, knowing where to prioritize cybersecurity investments and resources for the greatest impact can be difficult. Large enterprises typically consist of multiple distinct organizational groups, including business units, subsidiaries, mergers, acquisitions, and disparate geolocations. Each group has a unique structure, function, and ecosystem of digital touchpoints — and this level of complexity often makes it difficult to pinpoint where the greatest cyber risk exists across your distributed organization.



BitSight Enterprise Analytics takes the guesswork out of identifying risk concentration throughout and enhances security performance across distributed enterprise groups. This solution empowers you to get insight into the impact of risk introduced at the organizational group level so that you can identify and prioritize the areas of highest risk concentration. Use real-time, meaningful, and objective data and metrics to uncover the factors within each enterprise group that most significantly impact overall security performance, such as unpatched systems, insecure access points, and existing malware infections. And then drive progress with an automatically created action plan, which includes the rating impact on the parent from subsidiary improvements.

Identify Paths To Reduce Cyber Risk And Better Allocate Resources

Now, more than ever, your board and senior leadership team want to ensure you have a strong security program in place. Oftentimes, the challenge is deciding which adjustments to that program will deliver the fastest and most significant results. To present a clear and confident plan of action to business leaders, you need to weigh different strategies and outcomes.

With BitSight Forecasting, you can assess your current security performance based on historical analysis plus qualitative and quantitative data about weaknesses in your security program. Armed with this information, you can make more informed decisions about the strategy and resources needed to improve your security posture. Explore a variety of security scenarios to identify immediate opportunities for security performance improvement and project how changes to processes, technologies, and culture will impact your environment over time. And then track your progress to determine the impact of program changes, update executives and the board, and ensure your organization hits its goals.

Building these data-driven action plans will empower you to guide your organization down the road to continuous process improvement. While addressing the issues that require fixing, you can also identify key areas of weakness across the organization. With this big-picture view and focus on process failure and improvement, you can increase operational efficiency and achieve better alignment with business initiatives.

DO MORE WITH LESS

The role of the cybersecurity professional has been evolving for years, and now, as the industry continues to adapt to the "new normal" operating environment, this transformation is happening even more rapidly. As security leaders face continued pressure to meet the shifting requirements of their role, they must also learn to work effectively with shrinking budgets, limited resources, and an increasingly remote workforce that opens corporate networks up to new and evolving cyber threats.

Given these conditions, it's never been more important for you to rethink traditional methods of mitigating risk in an effort to find new operational efficiencies and do more with less.

With the BitSight for Security Performance Management suite of solutions, you have the tools and data-driven insights necessary to optimize the ROI of your existing cybersecurity technology, prioritize limited resources to achieve the greatest impact, and drive operational efficiency in your risk management processes.

Interested in learning more about how BitSight empowers you to get the most out of your security investments?

Go to www.bitsight.com/security-performance-management or contact sales@bitsight.com.

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.