Complete Guide to Building Your Vendor Risk Management Program

SecurityScorecard

Introduction

Security professionals know what they're up against when it comes to securing their organizations' digital footprints. They—and their boards—have all seen statistics like the 630% increase in attacks on cloud services from January through April 2020[1] and are on the front lines managing an expansive attack surface.

Accelerated digital transformation, driven by the work-from-home boom, is making third-party networks more complex and straining security operations (SecOps) teams operating with limited resources. Yet even as chief information security officers (CISOs) and their teams are working above capacity, most are still deploying and tracking vendor assessments via Excel spreadsheets—a time-consuming manual process that provides limited point-in-time security data, does not scale, and hinges on full vendor cooperation and disclosure.

In a world where zero-days happen every day, relying on static assessments exposes organizations to visibility gaps that can prove costly—to the tune of $3.86 million on average according to IBM.[2] Recent high-profile breaches have boards and executive teams demanding more oversight to ensure that their data, brand, and customer privacy are protected. In a KPMG survey, three of the top five risks to growth identified by CEOs were cybersecurity risk, regulatory risk, and supply-chain risk.[3]

1 McAfee. (2020). Cloud Adoption and Risk Report.

2 IBM. (2020). Cost of a Data Breach Report.

3 KPMG. (2021). CEO Outlook Pulse Survey.

In order to demonstrate program results and prove regulatory compliance, teams must be able to produce security reports that frame risk as it pertains to the business's goals, strategies, and risk tolerance—on a timeline that doesn't impede business functions like vendor onboarding and M&A due diligence. So how can security teams gain the visibility they need and scale their resources to meet the demands of today's threat environment without increasing budget and staffing?

According to Gartner, teams that leverage automated and integrated cybersecurity platforms will be more effective in managing risk and demonstrating measurable results. Choosing the right technology is critical to maturing your vendor risk management (VRM) program, and in a dynamic threat landscape in which your critical assets reside in interconnected cloud environments teeming with unmanaged digital devices, rogue web applications, and sophisticated adversaries, visibility is paramount.

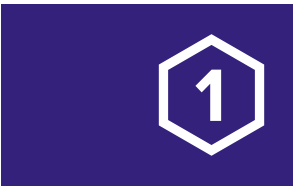
Next-generation security ratings platforms are providing a unified, objective, comprehensive view of a company's security posture by combining external data on security hygiene with intelligence signals and automated vendor questionnaires.

4 Gartner. (2021). 2021 Planning Guide for Security and Risk Management.

Based on our experience providing security ratings on over 5 million organizations, these are a few of the top capabilities that drive a robust VRM program:

- Integrated, unified platform that provides a 360° view of security signals and intelligence via external cloud scanning, third-party sources, and surveys
- Automatically sends and manages questionnaire data and evidence of regulatory compliance
- Functions at enterprise scale so you can monitor more companies without adding headcount
- Identifies zero-days and CVEs in real time, allowing you to patch vulnerabilities before they are exploited by threat actors
- Leverages machine learning and continuous scanning of the global IP space to provide consistent, accurate, and transparent security ratings on demand
- Enables data sharing and self-certification for key regulatory reporting requirements such as NIST, ISO, and GDPR
- Integrates with security stack workflows, i.e. GRC and SIEM solutions
- Eliminates all manual tracking mechanisms such as Excel spreadsheets

In this ebook, you will learn about the strategies and technology that will take your VRM program to a mature state, ready to meet the modern risk landscape head on.



Part 1

You'll learn how to take on vendor risk assessments and ensure you're making the most of them from a risk management standpoint. It starts with identifying your organization's most critical risk factors and how third parties map to those factors. This is a foundational step necessary for understanding how risk pertains to your company specifically. The rest of Part 1 shows you how to use that information to better delegate assessments, ensuring that you're prioritizing assessments based on risk, rather than blindly assessing third parties.

Part 2

You'll learn how to establish a continuous monitoring process for your vendors to manage vendor risk on an ongoing basis, as many cybersecurity and regulatory standards mandate. It starts with establishing a central VRM office, a necessary step to VRM maturity. Afterward, we show you how to establish communication, third-party monitoring, and reporting.

Part 3

You'll learn all about fourth-party insight, which concerns your vendors' third parties. Just as your third parties introduce risk, so do theirs, and it's important to keep your organization safe from any risk they may pose. Part 3 begins with establishing third-party relationships, a necessity for more advanced VRM programs as collaboration becomes increasingly important. After a robust third-party relationship is defined, you can start tracking any fourth parties and most importantly, use contracts as a tool to ensure that your exposure to the risk they introduce is mitigated.

While this ebook is laid out in parts and steps, you may find that certain aspects of your VRM program are already in place or that a specific part takes priority over others.

To make the most of this ebook, feel free to jump around to the step or part that is most important to your organization.

We've emphasized the key points of each section for you.

Stop spending your vendor risk management resources on the wrong security assessments

Most companies don't have a comprehensive process for vendor risk management in place.

Three quarters of VRM executives polled in a KPMG survey said they urgently need to make third-party risk management more consistent across the enterprise, and that their business's reputation depends on the security of its vendors.[5] Having an efficient process that can grow easily is essential for mitigating third-party risk and ensuring you're not exposed to unknown risks through your vendors.

A major challenge for vendor risk management is differentiating the various levels of risk among third parties when deploying vendor assessments. By identifying your risk factors, you can accurately prioritize third-party audits such as on-site assessments and penetration tests.

5 KPMG. (2020). Third Party Risk Management Outlook 2020.

Step 1
Identify and analyze specific risk factors

A Deloitte report found that many organizations are challenged with a lack of clarity in classifications of the vendors that are critical to the business.[6]

Not all risks are critical to your company.

Depending on your industry, you need to first identify potential risks specific to your company and then categorize them into low, medium, or critical risk buckets. This will help you prioritize vital security risks, ensuring you assess third parties based on the most important criteria to your organization.

6 Deloitte. (2019). Extended enterprise risk management survey 2019.

Ask yourself these questions when identifying your organization's risk:

If a third-party breach occurs, what information can cause the most harm if compromised?

Proprietary information

Customer's financial information

Employee's PII

Other third party data

Financially and strategically relevant information

Cyber business interruption

According to an Allianz study, business interruption following a cyber incident has emerged as the top business risk for mid-sized enterprises.[7] This is particularly concerning for companies with large supply chains (energy, utilities, manufacturing), where shutting down due to a cyber incident results in significant losses.

7 Allianz. (2021). Allianz Risk Barometer.

These risk factors need to be specific to the kinds of interactions and dependencies your third parties have.

In order to properly categorize these risks, think of potential consequences to your organization.

Will a third-party breach result in:

Reputational Damages?

Financial Penalties or Costs?

Regulatory Censure?

Litigation Possibilities?

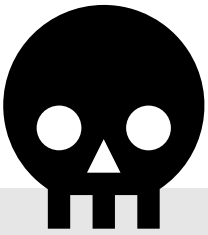
Negative Shareholder Reactions?

This risk identification and analysis will give you a comprehensive look into your own risk factors. Then, you can move on to your third parties.

Step 2
Rank your third parties' risk factors

In the same way that you defined risks specific to your company, you should define third-party service risks based on the type of relationship between your organization and the vendor in question.

- Do they have access to your employee or customer data?
- Will they implement systems within your networks?
- Will their third parties or subcontractors interact with your information?
- Does any of their access mean they are subject to compliance standards?



Did you know third-parties are a top source of security incidents?

A recent survey conducted by the Ponemon Institute and publicized by Security Boulevard found that 53% of organizations have experienced one or more data breaches caused by a third party, costing them an average of $7.5 million to remediate.[8] Maturing your VRM program will allow you to verify that your third parties have the right controls in place to react quickly when a security incident occurs.

8 Security Boulevard. (2020). Automation In Compliance: Why It's a Business Imperative and Where to Start

After defining your third partys' service risks, rank those risks by criticality. In our experience, it is best to use a four-factor vendor risk tiering system: low, moderate, high, critical. This gives you a standardized method for assessing existing and newly-onboarded third parties. This will allow you to make the most impact with your auditing budget by delegating assessments to the most critical vendors first.

Step 3
Map assessment types to your third parties

First take your assessment methods and segment them by the amount of resources necessary to perform each assessment. The three most important resources to consider are:

Financial Costs

Time Invested

Employees Needed

High-resource methods such as onsite assessments are costly, require multiple employees to be on-premises, and take time to produce results. You should only reserve these methods for high-risk third-parties. For other third-parties, you can delegate assessments that require fewer resources, such as questionnaires or self-assessments.

After you've ranked your third parties and critical risks, you can begin mapping assessments.

This ensures you're focusing your resources on the vendors that are most relevant and most likely to impact you negatively should a breach occur. This flexible and scalable framework can be applied to all existing and incoming third-parties.

How SecurityScorecard helps

Prioritizing assessments can be challenging when you have a large backlog of uncategorized vendors. Did you know that our platform helps you prioritize assessments? With SecurityScorecard, you can rate any company on demand, allowing you to assess your critical vendors with weak security posture first.

Applying your new assessment methods continuously

Did You Know?

Thirty-five percent of organizations surveyed in EY's Global Third-Party Risk Management Survey 2019–20 revealed that they do not continuously monitor the cybersecurity posture of their third-party cloud vendors.[9]

Now you have the capabilities to assess third parties from a comprehensive, risk-first perspective. However, this is only the first step towards establishing a strong vendor risk management program.

Traditional VRM programs only assess third parties yearly or obtain point-in-time information that quickly becomes outdated. New vulnerabilities and threats arise everyday in your third-party ecosystem, but without continuous insight, you cannot react to security issues in real time.

9 Ernst & Young LLP. (2021). Data breaches and cybersecurity: managing third-party risk.

Security ratings in financial services

The American Banker's Association recently issued a report that recommends the use of security ratings and risk scores as part of an effective VRM program. As financial services firms work to more effectively understand their cyber risk, security ratings providers can offer an easy way to measure an organization's cybersecurity hygiene.

Replace point-in-time vendor risk assessments with continuous monitoring

Before implementing a continuous monitoring process, it's important to first identify and rank third-party risks that are critical to you as described in Part 1, allowing you to optimize assessment methods and properly manage third-party risk. Now, we're going to show you how to continually assess your third parties so your organization can manage risk on an ongoing basis, rather than just through point-in-time assessments.

The information collected through point-in-time assessments is often outdated and doesn't take into account changes in a third party's security posture between assessments. If the worst case scenario is realized and a third party is breached, you might not be aware until they alert you or until the next assessment. By that time, a hacker may have already entered your network.

Remote work driving third-party risk

The explosion of connected devices supporting remote work calls for more risk management and technology to protect sensitive data. If one of your vendors hasn't invested in the proper controls and policies, threat actors may be able to move up or down stream to access your critical data via a third-party device.

In a dynamic environment where vulnerabilities are exploited faster than ever, being aware of your vendors' security posture on an ongoing basis will give you the information and opportunity to react to and mitigate potential issues. According to EY, continuous monitoring via data from external sources is critical to understanding where the greatest third-party risk resides within your ecosystem.[10]

10 Ernst & Young LLP. (2021). Data breaches and cybersecurity: managing third-party risk.

The EY report referenced above predicts a future trend where technology moves TPRM management from manual to automated workflows. However, there is still significant ground to cover for organizations when it comes to tracking vendor security over time: Only thirty-five percent of organizations surveyed by EY indicated that they continuously monitor the cybersecurity posture of their third-party cloud vendors.[11]

These figures indicate that the current state of vendor risk management is exposing companies to unnecessary risk, which can prove to be costly.

In part 2 of this ebook, we'll show you how to incorporate continuous third-party monitoring as part of your vendor risk management program by establishing a centralized VRM office, defining monitoring controls and processes, and collaboratively engaging in tracking, reporting, and remediation processes with your third parties.

11 Ernst & Young LLP. (2021). Data breaches and cybersecurity: managing third-party risk.

How SecurityScorecard helps

At SecurityScorecard, one of our guiding principles is to make the world safer and provide a continuous, 360° view of risk. That's why we scan the global IP space daily and integrate signals from trusted partners, so you can identify vulnerabilities and zero-day exploits in real time, and leverage actionable cyber-risk intelligence.

Step 4
Establish a centralized VRM office

Half of the respondents in a Deloitte survey reported that their organizations underinvest in third-party risk management.[12]

Organizations are increasingly aware that if they are going to mature their VRM programs, they need to spend enough money to recruit leadership and full-time staff dedicated to this area.
A dedicated VRM office is essential for establishing a foundation for continuous third-party monitoring. A VRM office also provides a localized department for all aspects of third-party risk.

A centralized VRM office allows a singular team (whether cross-departmental or made up of one department) to communicate with third parties, establish standardized practices, track and report, take ownership and responsibility, and provide a point of contact for other business unit owners that have relationships with third parties. The central VRM office will make critical decisions, quickly inform business unit owners, and escalate priorities should any critical issues arise.

12 Deloitte. (2020). Extended enterprise risk management survey 2020.

Establishing a VRM office begins with hiring an in-house VRM team, transitioning existing employees to move into a TPRM position, or assigning VRM responsibilities to existing information security stakeholders. The VRM office is a highly specialized department that aids information security across the enterprise:

Contract Management

Financial and Commericlal Management

Issue and Dispute Management

Service Performance Management

Governance

Multi-Service Provider Integration

Transition and Trainsitional PMO and Oversight

Document Manangement

Service Request Management

Risk Management and Third Party Compliance

After a central office is set up, you can start defining what you will be monitoring.

Step 5
Define controls and processes to monitor and establish third-party reporting methods

According to PwC, less than half of business and tech/security executives are confident that their cyber spending is aligned with their organizations' most critical risks.[13]

Because continuous monitoring requires more resources than most VRM processes, optimizing the resources involved is crucial. You have to define which aspects of your vendors (whether data, assets, processes, or controls) you will be monitoring based on various criteria. These criteria include:

Risk criticality

If you followed step one of this ebook, then you've already defined and identified your risk factors. Defining what is most risk-critical to your company will inform you on what you should be monitoring. If a third party is processing or storing sensitive information, then you should be monitoring the security controls or systems in place that protect your vendor's network and endpoints.

13 PwC. (2021). Rethink your cyber budget to get more out of it.

Likelihood of information/status change

Categorize your risk-critical third-party services and systems by frequency of change over time. If a vendor is hiring rapidly, that means the number of endpoints are increasing, and you should pay more attention to endpoint security. However, for systems that are not likely to change over a long period of time, such as a hosting or CMS provider, you may decide that annual reviews are sufficient.

Compliance posture

When it comes to your vendors', and by extension your compliance posture, what's true today may not be true tomorrow, and regulators are increasingly pursuing enforcement actions against companies that are unable to demonstrate implementation of effective risk management programs. The evolving threat landscape requires continuous monitoring of enterprise and partner security posture to ensure sustained compliance with shifting regulations. Leveraging a platform that automates the vendor questionnaire process and continuously tracks issues that pertain to specific regulatory frameworks will help your organization mitigate the risk of regulatory penalties and reputational damage that can result from a public data breach.

Automating the assessment process

A mature VRM program incorporates technology to aid in the identification of risk. Leveraging a security ratings platform allows you to automatically deploy and track vendor questionnaires mapped to regulatory standards and verify the results with objective outside-in data, so you can monitor more vendors without additional resources.

Step 6
Establish communication, tracking, and reporting processes collaboratively

Third-party collaboration and communication is key to successful vendor monitoring. Your VRM office should clearly communicate with your third parties what will be monitored and tracked in order to improve the security posture of all parties involved.

Ideally, you are already engaging in continuous monitoring of your own security posture through automated tools, solutions, and other processes. One option is to use these same tools and processes to monitor any integrated systems that your third parties own. Keep in mind that even if you are using tools that won't alert your third parties, you should reach out to them to begin remediation if any issues arise.

According to a Ponemon Institute study, 59% of respondents experienced a third-party data breach, and only 16 percent said they effectively mitigate third-party risks.[14] If you identify with the 59%, here are some elements to build into your process to with effectiveness and consistency of your VRM program:

Metrics

Monitoring and tracking must be accompanied by the development of key performance indicators (KPIs) specifying how any data change over time is relevant to security. Mark goals like lowering the average number of days passed between a patch being released and a patch being applied or increasing the frequency of open port scans. Setting concrete goals will allow you to identify vendors who aren't meeting your standards.

Tracking and monitoring

While your VRM office should begin monitoring and tracking your third parties using any existing technologies or tools in place, you should consider using a new tool or technology that will sit on top of your existing technology. Leveraging a unified, API-driven platform that centralizes communication around security issues with vendors allows you to optimize your workflows, drive collaboration with your third parties, and accelerate risk mitigation.

14 Business Wire. (2018). Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks.

Reporting

The central VRM office should establish reporting methods for third-parties and also relay them to the respective business unit owners. The VRM office is responsible for alerting both third-parties and business unit owners of any potentially critical issues that arise in reports.

Engaging in remediation

The foundational work performed in previous steps will help the VRM office more clearly identify issues and abnormalities. When any third-party security issues pop up, the VRM office should work in tandem with business unit owners and third parties in order to remediate issues.

Engaging in third-party continuous monitoring takes some effort but produces compounding results, improving not only your vendor risk management but your own security posture as well.

How SecurityScorecard helps

SecurityScorecard helps teams centralize and streamline VRM activities by offering a security ratings platform that integrates with GRC, SIEM, and other security stack workflows. Our industry-leading marketplace is a one-stop shop where you can discover and deploy trusted partner solutions and pre-built integrations to get maximum value from your VRM program.

Looking ahead toward fourth-party insight

Given that third parties can represent a significant risk to your business, then their third-parties should also be considered. This is important for understanding vendor security when initially assessing them, and also when engaging in continuous monitoring in order to see if your third parties have recently started to work with a company you have previously identified as risky.

Managing third- and fourth-party risks

If you have prioritized your third-party assessments and established a centralized vendor risk management program to engage in continuous monitoring as we discussed in the first two parts of this ebook, you're well on your way to having a strong risk mitigation plan in place. You may, however, still be ignoring a major risk factor—your third parties' third parties.

In the era of digital transformation, we rely on software-as-a-service (SaaS) and other cloud-based services to deliver critical applications. As we've seen many times, fourth parties can impact the delivery of third party companies, as was the case when the content delivery network Fastly experienced an outage in June 2021, which caused dozens of sites to go offline—including Amazon, Twitch, Reddit, and the New York Times. This is why having a VRM program that monitors fourth-party risk is an important part of your strategy.

The OCC's Bulletin on Third-Party Relationships offers a number of guidelines and standards focused on subcontractor assessment visibility, such as making risk-based decisions to ensure that critical third-party service providers are the best available.[15]

15 Office of the Comptroller of the Currency. (2020.) Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29.

Additionally, KPMG's Outsourcing and Third-Party Risk Management report includes key considerations regarding fourth-parties and subcontractors.[16]

These include:

- ensuring the vendor's risk assessment and controls are proportionate to the services provided and data handled by a fourth party.
- managing concentration risk—i.e. multiple vendors within close geographical proximity or relying on a common fourth party.
- ensuring your due diligence process documents any outsourcing arrangements and verifies third-party governance of those fourth parties.

These next steps give some direction on how to establish more control over fourth-party monitoring and reporting.

16 KPMG. (2021). Outsourcing and third-party risk management.

Step 7
Establish third-party relationships to manage fourth-party risk

Fourth-party monitoring is a collaborative effort and requires a strong relationship with your third parties in order to gather data around your fourth parties' security posture. By working with your third parties to facilitate and engage in fourth-party monitoring, you'll not only improve your cyber health, you'll be helping your partners improve their VRM processes as well. Making this a point of emphasis in security conversations with your partners can help you drive buy-in when addressing third-and fourth-party security issues.

Because fourth-party monitoring is an intensive effort, a blanketed approach is not recommended. While you should be monitoring all of your third parties in some capacity, you don't necessarily need to be monitoring all your fourth parties.

First, identify your most risk-critical third parties as recommended in step one of this ebook. After identifying your risk-critical third parties, work with these vendors to produce a list of their suppliers mapped to their responsibilities to define the services your fourth parties provide.

You should know the following about your fourth-parties:

- What services they provide and how?
- Do they have access to your sensitive data?
- Do they have access to your third-party's sensitive data?
- If they were breached, what are the attack vectors that would lead to your data being compromised?
- Are there degrees of separation or deliberate network segmentation implemented to prevent connection between your organization and your fourth-parties?
- Where are your fourth-parties located?

82% of respondents to a Forrester/RSA survey indicated that they still use spreadsheets to inventory, assess, and manage third parties.[17]

17 RSA. (2020). 82 Percent of Organizations Still Use Spreadsheets to Manage Third Parties.

After compiling a list of third parties and the services they provide, you must now understand their third-party monitoring capabilities. Do they have a mature VRM program in place? Are they engaged in continuous vendor risk monitoring? What is their incident response plan should one of their partners suffer a data breach? Understanding the security posture of your fourth parties is a key element of a mature vendor risk management program, and also encourages your third parties to implement VRM best practices.

How SecurityScorecard helps

In a world where core business functions are supported by third-party SaaS platforms that serve numerous vendors, one outage can result in service interruptions across an ecosystem. Tracking your third parties and the fourth parties that support them helps you identify interdependencies that represent a risk to your business in the event of an adverse event. SecurityScorecard helps organizations track fourth-party security data via API calls, security ratings data, and automated questionnaire exchange and validation.

Step 8

Utilize contracts to safeguard against high-risk third and fourth parties

Leveraging contracts is a good way to ensure that your most critical services are not being outsourced. When drafting a contract with an incoming third party, or if you're making any amendments to an existing contract, make sure you specify the services that cannot be outsourced or subcontracted. This can be implemented now for your most critical third parties and moving forward as new third parties enter your ecosystem.

You can incorporate fourth-party insight into your vendor risk management process by tailoring questionnaires to find out if your vendors outsource any of the services they provide to you.

At $8.64 million on average, the United States continues to experience the highest data breach costs in the world, followed by the Middle East at $6.52 million in 2020. The global average cost per data breach is $3.86 million million.[18]

When drawing up contracts, you can include language that will require notifications when your third parties partner with new subcontractors, even if it's later in the engagement.

Leveraging contracts is even more important for highly regulated industries such as the healthcare or finance industry. Because of the strict scrutiny these organizations are subject to, these organizations should act like regulators themselves when it comes to managing their vendors.

By taking a structured approach to fourth-party insight, regulated companies can be proactive and adhere to VRM-focused guidelines and regulations.

18 IBM. (2020.) Cost of a Data Breach Report 2020.

Roadmap to success

At SecurityScorecard, our experience rating the security posture of millions of organizations has shown us that when companies adopt the right strategies and technology, they can keep up with the pace of change and set themselves apart from their industry peers. Now is the time to make your company's security posture an asset so you can be a sustainable strategic partner.

By implementing the practices and tools outlined in this ebook, you'll cut time spent on rote, manual processes so you can increase your team's capacity and bring value to your entire organization. To help you select a best-in-class VRM solution, we provided this checklist as part of your process and evaluation criteria:

General:

Accuracy of data. Highly accurate and reliable from an outside-in security perspective. Scores should be created and updated automatically as new security issues are detected.

Scores correlate to breach likelihood. Scoring algorithms should have a direct correlation to breach likelihood. Scoring methodology should be transparent, refutable, and validated by third parties.

Integrated questionnaire management. Provides an integrated and automated questionnaire management solution for deploying and tracking third-party risk assessment questionnaires.

Speed and scalability:

Scoring new organizations. If an unrated company is found, the solution should be able to produce a new scorecard on demand without relying on human intervention.

Scalability. Rates the entire global supply chain. Both small and new companies should already be in the ratings platform to derive meaningful value.

Scorecard details:

Score improvement & remediation plan. Generates a score improvement plan to improve a company's security posture. The score improvement plan should clearly show how much the score will change when specific issues are remediated.

Transparency of data. Provides details around adverse findings and what the recommendations are to mitigate the risk. The ratings provider should disclose the full IP details and a timestamp of when an issue was last observed.

Digital footprint. Segments all IPs that belong to an organization, discloses full IP details with sources for attribution, and self-corrects the digital footprint in the event the IP attribution is incorrect. Interface should allow an organization to self-correct its digital footprint by requesting that IPs be added or removed.

Creating a custom scorecard. Creates custom scorecards of large organizations by using filters such as IP ranges, domains, sub-domains, and geographic location.

Compliance mapping. Provides compliance mapping to conduct a gap analysis of commonly used frameworks such as CMMC, NIST, and ISO.

Continuous monitoring and alerts:

Continuous monitoring with daily score updates. Scores are updated daily as new security issues are detected and made visible in the platform.

Alerts & notifications. Configurable alerts & notifications for individuals and teams based on score change, risk factor change, and new issues and breaches detected.

Remediation and false positives:

Remediation workflow. Provides an interface for submitting remediated issues for review as well as a tracking mechanism and documented SLA for the process.

Score change after remediation. Scoring should be updated within 72 hours of remediation activity.

False positives. Provides an interface for refuting detected security issues that are believed to be false positives. Accepted refutations should be reflected in scoring within 72 hours of submission.

Reporting:

Reporting functionality. Provides a variety of reports on a company's security posture, including summary reports (simplified view) and detailed reports (all detected security issues with full IP details).

Side-by-side comparison. Allows for side-by-side comparison of various organizations for competitive benchmarking.

Board reports. Provides board-friendly reports that frame risk as it pertains to the business's goals, strategies, and risk tolerance.

Invited vendor collaboration:

Inviting vendors. Allows for permanent third-party access at no charge so partners can see their ratings.

Invited vendor dashboard. Provides a dashboard to track remediation activities among invited vendors.

Integrations:

Integrations & API library. Provides an extensive API library to integrate with SIEM, ticketing systems and GRC solutions. API should support custom integrations in multiple languages such as Python and Javascript.

SecurityScorecard for third-party risk management

We mentioned earlier that a security ratings provider can help you manage your increasingly complex third-party ecosystem and digital footprint. SecurityScorecard simplifies your daily operations and extends the value of your investments with automated tools and features that integrate with your existing workflows.

- SecurityScorecard **Sentinel** scans the global IP space daily so you can:
    - continuously monitor you and your vendors' security posture.
    - keep pace with threat actors and search your ecosystem for CVEs to determine whether or not you've been impacted by a zero-day exploit.
- Rate any company on demand with **FastScore** to enable rapid due diligence and vendor onboarding.
- **Digital Footprint** provides a complete view of the IT estate—including all endpoints, apps, and web domains—to prevent shadow IT from becoming a security threat.
- **Integrate 360° Marketplace**, the largest security ratings marketplace for integrating and automating workflows, allows you to leverage signals from trusted intelligence partners like **CybelAngel**, **HackerOne**, and **DarkOwl**. These signals augment your view of the threat landscape without impacting your score.
- With **Rule Builder**, you can trigger alerts in **Slack**, **Jira**, **ServiceNow**, and **Zapier** to streamline communication and remediation when there's a third-party breach or change in vendor security posture.
- **Atlas** allows you to automatically map vendor cybersecurity questionnaire responses to SecurityScorecard data, cutting the vendor assessment cycle by 83%.7 Using **Custom Issue Mapping** to create or edit a questionnaire in Atlas, you can choose which security ratings data points validate each question. This brings more customization and transparency to the cybersecurity assessment process, providing a true 360° view of risk.

- SecurityScorecard's robust **APIs** offer direct access to actionable data that allows businesses to power their workflows, save time, and gain more value from their tech stacks. Any company can leverage the **SecurityScorecard Ratings API** to develop custom solutions or integrate existing services with our platform. Additionally, SecurityScorecard offers over **20 out-of-the-box integrations** with leading industry SIEM and VRM solutions that customers can instantly use to support their daily operations.

- **Score Planner** provides full transparency into how specific issues impact scores and automatically generates a remediation plan to achieve a target letter grade. If the recommendations do not fully align with your company's security priorities, the plan can be easily customized with SecurityScorecard's simple user interface.

- Automate and accelerate your vendor risk assessments with **Atlas**, our questionnaire exchange and validation platform. The **Evidence Locker** acts as a single source for TPRM documentation, allowing teams to automatically populate vendor and compliance questionnaires with stored data by exchanging this information between **Atlas** and **Ratings**.

- **Custom Scorecard** creates an individualized, hierarchical view of third-party organizations so you can rate the security posture of the specific subsidiaries, geographies, and domains that are most relevant to your organization.

- SecurityScorecard's **Board Trends Reports** instantly provide real-time executive-level insight to track compliance and strategic TPRM performance—and its impact on the business over time.

About SecurityScorecard

SecurityScorecard is the global leader in cybersecurity ratings and the only service with over five million companies continuously rated. SecurityScorecard's patented rating technology is used by over 1,000 organizations for self-monitoring, third-party risk management, board reporting, and cyber insurance underwriting, making all organizations more resilient by allowing them to easily find and fix cybersecurity risks across their externally facing digital footprint. SecurityScorecard is the only provider of instant risk ratings that automatically map to vendor cybersecurity questionnaire responses—providing a true 360-degree view of risk.

To learn more, request a demo.

SecurityScorecard

info@securityscorecard.io
United States: **(800) 682-1707**
International: **+1 (646) 809-2166**