Third-Party Risk Management Strategies

SEE RISK, SOLVE PROBLEMS, REPORT RESULTS.

SecurityScorecard

Contents

Introduction

Third-party risk management (TPRM) is a top business concern—not only as a regulatory requirement but as an operational necessity for organizations working to keep pace with unprecedented change related to digital transformation, the continued evolution of remote work, and interdependencies within supply chains. McKinsey's 2020 Global Survey of executives found that organizations are accelerating the digitization of their internal, vendor, and customer-facing operations more rapidly than before the pandemic.[1]

As CISOs and their teams adapt quickly to digital transformation accelerated by the shift to remote work, threat actors are capitalizing on a growing attack surface. Organizations across industries are seeing an uptick in phishing, malware, and ransomware events. Regulators and executive boards are putting new pressure on security teams following recent high-profile supply-chain attacks on SolarWinds, Microsoft Exchange, and Pulse Secure VPN—increasing the need for a more comprehensive view of the expanding ecosystem of partners.

This need goes beyond simple point-in-time surveys. At present, manual exchange of Excel spreadsheets—an onerous and time-consuming effort—is still how most teams deploy vendor questionnaires and verify security performance over time. To fill in the gaps that arise between assessments and make the questionnaire cycle less resource-intensive, IT and security operations (SecOps) teams can leverage artificial intelligence (AI)- and machine learning (ML)-driven tools to continuously monitor their digital footprint, and auto-populate and validate vendor questionnaires.

[1] McKinsey. (2020). How COVID-19 has pushed companies over the technology tipping point—and transformed business forever.
https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-f2021orever#

Top TPRM challenges for security teams

- Excel is still the #1 tool used for deploying and tracking vendor assessments
- Threat actors upping their attack vectors and frequency
- Digital transformation creating an expanded third-party ecosystem
- Remote workforce expanding the attack surface
- Escalating compliance requirements
- Increased executive oversight

Most teams do not have the time, talent, or budget to build effective, scalable technology solutions in-house. Those who are successfully pivoting with the pace of change are moving beyond fragmented, manual processes and investing in security ratings platforms to automate and streamline their TPRM programs. These flexible software-as-a-service (SaaS) products are setting a new standard for the tools that drive TPRM programs by helping CISOs and their teams scale their resources and provide deeper insight for boards, compliance reports, and auditors—all while lowering cost.

Cybersecurity ratings platforms allow organizations to rate the security posture of their third and fourth parties by assessing their digital footprint.

According to Forrester research, SecurityScorecard can reduce the vendor assessment cycle by up to

83%.[2]

[2] Forrester 2021 - The Total Economic Impact™of SecurityScorecard

In this ebook, we will highlight three principles that are key to implementing a world-class TPRM program. Taken together, these practices will move your organization toward a full 360° view of organizational risk—both internally and across your ecosystem:

SEE RISK

Understand, identify and manage risk in your digital ecosystem. Gain a more comprehensive understanding of your risk portfolio with a 360° view of the threat landscape with inside-out and outside-in data so you can quickly remediate security issues.

SOLVE PROBLEMS

Create an effective, scalable, and accurate TPRM environment by leveraging purpose-built technology designed to boost team capacity, automate workflows, and manage your entire vendor ecosystem.

REPORT RESULTS

Support compliance, cyber insurance, and executive reporting demands to avoid regulatory penalties, optimize insurance premiums, and drive effective board-level decision-making around security.

See risk

Understand, identify and manage risk in your digital ecosystem. Gain a more comprehensive understanding of your risk portfolio with a 360° view of the threat landscape with inside-out and outside-in data so you can quickly remediate security issues.

See risk

SecOps teams are fighting an uphill battle to identify the most relevant risk vectors among the growing number of vendors, SaaS providers, Cloud vendors, and IOT cloud-connected devices that support digital transformation initiatives and remote operating models. A recent McAfee report found that attacks on cloud services increased by 630% from January through April 2020.[3] The gap between known and unknown assets, devices, and endpoints—known as shadow IT—has also grown due to the introduction of connected IoT devices used for tracking and data exchange purposes across industries.

Security teams working to secure a growing attack surface must gain a complete view of the IT estate and leverage actionable intelligence to respond to emerging threats. Most teams receive event data from a variety of sources which, when not properly tuned, result in a barrage of alerts that don't represent actual threats. In order to optimize the signal-to-noise ratio, security teams should prioritize findings that have the greatest impact on their security posture.

In order to gain visibility of your entire digital footprint, you'll need to automatically and continuously scan the global IP space. This will allow you to discover unmanaged assets and rate the security posture of any entity on demand so you can:

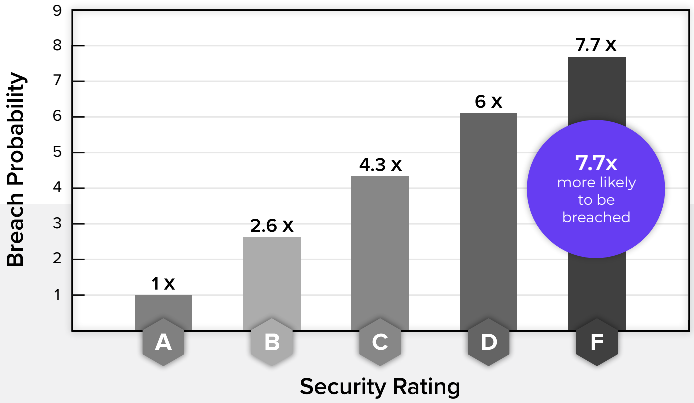
- scale your TPRM program to manage extensive vendor and IoT ecosystems.
- quickly see risk, access actionable information, and mitigate known exploits, which helps you keep up with emerging threats.
- prevent your security teams from becoming a bottleneck in the vendor onboarding process, reducing friction between business units.

[3] McAfee. (2020). Cloud Adoption and Risk Report
https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=3804edf6-fe75-427e-a4fd-4eee7d189265#form-download

Obtaining a complete view of your digital attack surface requires a combination of internal and external data sources. We recommend combining vendor questionnaires, external security ratings data, and additional third-party sources to gain a full view of risk from the outside-in and the inside-out. This 360° visibility provides a shared view of compliance backed by evidence, so both vendors and vendor risk managers can understand how they're being assessed. With 67% of third-party risk assessments being carried out by resources across departments, visual queues that enable at-a-glance confirmation of compliance help your organization's business units and vendors stay aligned.

To serve as a meaningful diagnostic data point, a security rating must provide attribution, granularity, and the ability to easily refute incorrect information in a score. Security ratings platforms should also have built-in transparency and resolution mechanisms so you and your vendors can know exactly how you're being scored and plan remediation resources accordingly.

4 KPMG International. (2020). Third-Party Risk Management Outlook 2020



How SecurityScorecard helps

SecurityScorecard allows companies to view their entire digital ecosystem, discover shadow IT, and instantly rate any entity with a digital footprint by continuously scanning the global IP space. SecurityScorecard's machine learning-tuned security ratings are maximally correlated with breach likelihood, making them more meaningful and actionable than human-generated ratings. To provide full transparency, SecurityScorecard publishes its scoring methodology and allows customers to dispute, correct, and appeal its findings. Users gain a 360-degree view of risk by validating vendor questionnaire responses with objective ratings data and by leveraging intelligence signals from trusted partners.

Solve problems

Create an effective, scalable, and accurate TPRM environment by leveraging purpose-built technology designed to boost team capacity, automate workflows, and manage your entire vendor ecosystem.

Solve problems

Unlike nation-state and criminal threat actors who have virtually unlimited time and resources at their disposal to wage unprecedented ransomware campaigns, SecOps teams' efforts are limited by budgetary and staffing challenges—and by tech stacks that do not function optimally at enterprise scale. Threat actors have many tools and resources at their disposal to discover known common vulnerabilities and exposures (CVEs) that may not have been patched, which puts security teams at a disadvantage when trying to discover and eliminate zero-day exploits before hackers do. According to IBM, the average time to identify and contain a breach in 2020 was 280 Days.[5]

In order to match the capabilities of their adversaries, security teams need automated tools to quickly identify and remediate vulnerabilities within their ecosystems. In this section, we'll show you the attributes of a fully integrated, automated, and scalable TPRM environment that will boost your team's capacity so you can discover and remediate risk without increasing budget or staff.

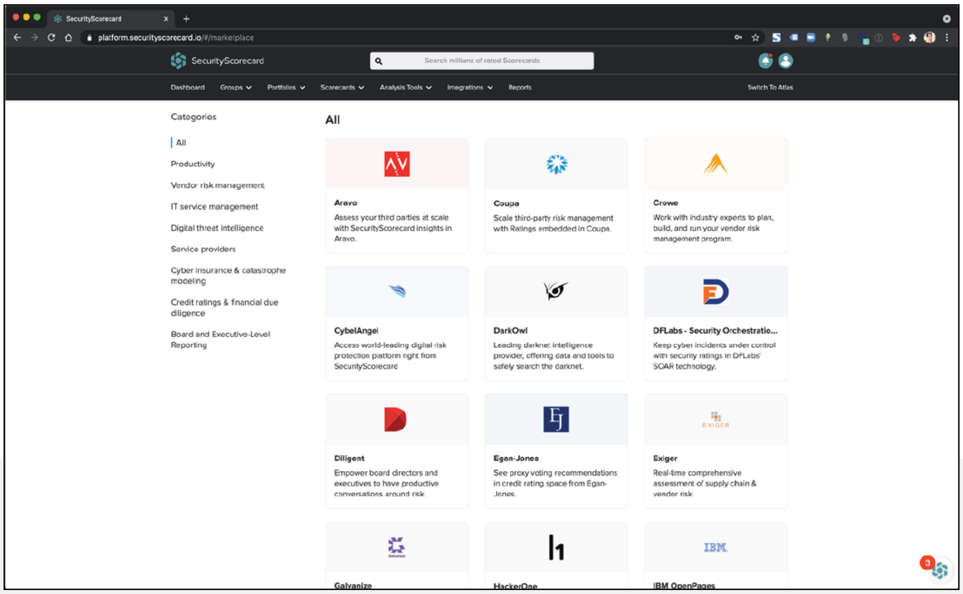
One of the key requirements for a modern TPRM platform is to reduce the burden of security ratings and assessments while gaining the ability to monitor more organizations. This is best achieved when you can feed and consolidate security signals from multiple sources into a centralized platform that allows you to prioritize and automate TPRM activities for your security team. A state-of-the-art TPRM platform goes beyond ratings and assessments:

- Integrates with your existing security stacks
- Discovers emerging threats across the ecosystem
- Ecosystem-wide visibility of CVEs
- Automates vendor assessments and tracks completion
- Drives proactive patch management to mitigate vulnerabilities
- Automates alerts through your organization's preferred communication channels

[5] IBM. (2020). Cost of a Data Breach Report.
https://www.ibm.com/security/data-breach

Security ratings platforms help your team keep pace with threat actors by allowing you to identify and remediate known CVEs before they are exploited. You can leverage these tools' monitoring capabilities to search your network for instances of zero-days and determine whether or not you or your vendors have been impacted by an active exploit.

We recommend continuously monitoring vendor security and enabling alerts that are triggered when a low score control limit is crossed to prevent security gaps from arising between assessments. When an issue is discovered and it's time to engage a third party for remediation, you'll also want to understand the factors that have the most impact on you and your vendors' security posture so you can prioritize remediation activities and create a custom-tailored plan to improve you and your vendors' ratings.


SecurityScorecard
platform.securityscorecard.io/#/marketplace
SecurityScorecard
Search millions of rated Scorecards
Dashboard
Groups
Portfolios
Scorecards
Analysis Tools
Integrations
Reports
Switch To Atlas
Categories
All
Productivity
Vendor risk management
IT service management
Digital threat intelligence
Service providers
Cyber insurance & catastrophe modeling
Credit ratings & financial due diligence
Board and Executive-Level Reporting
All

Aravo
Assess your third parties at scale with SecurityScorecard insights in Aravo.

Coupa
Scale third-party risk management with Ratings embedded in Coupa.

Crowe
Work with industry experts to plan, build, and run your vendor risk management program.

CybelAngel
Access world-leading digital risk protection platform right from SecurityScorecard

DarkOwl
Leading darknet intelligence provider, offering data and tools to safely search the darknet.

DFLabs - Security Orchestratio...
Keep cyber incidents under control with security ratings in DFLabs' SOAR technology.

Diligent
Empower board directors and executives to have productive conversations around risk.

Egan-Jones
See proxy voting recommendations in credit rating space from Egan-Jones.

Exiger
Real-time comprehensive assessment of supply chain & vendor risk.

Galvanize

HackerOne

IBM OpenPages

How SecurityScorecard helps

SecurityScorecard allows you to seamlessly manage your entire vendor network by automatically deploying and validating questionnaires, inviting vendors to collaborate, and generating remediation plans. With the largest integrated security ratings marketplace, you can use numerous apps to drive collaboration and fast resolution. Trigger automated alerts, tickets, and dedicated channels in your organization's product-management or business-communication platform based on signals from integrated VRM, SIEM, and threat intelligence solutions. Keep up with the threat landscape by searching your ecosystem for CVEs and zero-day exploits, so you can patch vulnerabilities before hackers act.

Report results

Support compliance, cyber insurance, and executive reporting demands to avoid regulatory penalties, optimize insurance premiums, and drive effective board-level decision-making around security.

Report results

After a number of recent noteworthy data breaches, boards of directors are demanding more and more oversight to verify that the appropriate practices are implemented to ensure data security. In Gartner's 2020 Board of Directors Survey, 49% of directors indicated a desire to reduce legal, compliance, and reputational risk associated with their digital investments. Modern TPRM platforms need to provide effective input to the overall corporate governance and risk portfolio management process. No single grade or data point should be used as the sole indicator of security posture, but they can provide board members and senior management the tools required to make informed decisions.

Constructive communication around cybersecurity issues with executive leadership requires customized reporting on vendor portfolio trends and program performance over time. With the functions listed below, you can demonstrate to the board where resources can be directed in order to protect the company's compliance posture, customer privacy, and brand:

- Use high-level dashboards to instantly pull data that frames risk as it pertains to the business's goals, strategies, and risk tolerance.
- Segment and rate the various business lines, subsidiaries, and departments within partner organizations that handle your data by using a platform to obtain a hierarchical view. This shows you exactly how your company's security is being impacted by providers with large digital footprints.

Effective reporting has critical strategic and compliance applications across the enterprise:

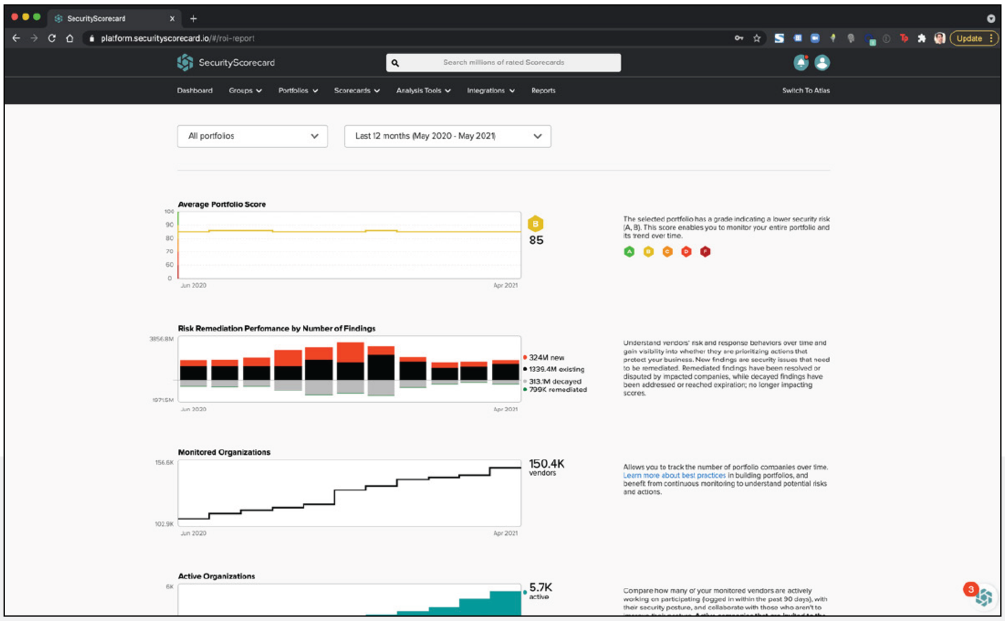
Board reporting/portfolio risk management	M&A due diligence	Cyber insurance
Public and other highly-regulated companies must provide boards with easy-to-understand information about strategic security posture as well as actionable intelligence on oversight and governance.	Rating an organization's security posture on demand allows CISOs to quickly determine whether a vendor, M&A target, or application poses an unacceptable risk to the organization, reducing friction between departments.	Many providers are leveraging security ratings to inform policy underwriting. Using ratings to continuously monitor your own cyber health can help you optimize your premium when purchasing a policy.

[6] Gartner. (2020). Digital Risk is Primary Focus for Corporate Boards in 2020 & Beyond. https://blogs.gartner.com/john-wheeler/digital-risk-is-primary-focus-for-corporate-boards-in-2020-beyond/?_ga=2.224157661.735546658.1608749611-1027403403.1575939693

Industry-specific compliance and regulatory demands

Organizations need to be able to produce proof of compliance with industry-specific regulatory frameworks. Security teams can use technology to store and produce evidence without manually poring over disparate documents and findings when an audit takes place.

Public company compliance:	Critical infrastructure:	Customer protection/privacy:	Operational regulatory standards:
• SOX • SEC Regulatory Board	• NIST • CMMC • FedRAMP	• GDPR • CCPA	• PCI DSS • HIPAA • Hitrust • ISO



All portfolios

Last 12 months (May 2020 - May 2021)

The selected portfolio has a grade indicating a lower security risk (A, B). This score enables you to monitor your entire portfolio and its trend over time.

Understand vendors' risk and response behaviors over time and gain visibility into whether they are prioritizing actions that protect your business. New findings are security issues that need to be remediated. Remediated findings have been resolved or disputed by impacted companies, while decayed findings have been addressed or reached expiration; no longer impacting scores.

Allows you to track the number of portfolio companies over time. Learn more about best practices in building portfolios, and benefit from continuous monitoring to understand potential risks and actions.

Compare how many of your monitored vendors are actively working on participating (logged in within the past 90 days), with their security posture, and collaborate with those who aren't to

How SecurityScorecard helps

SecurityScorecard allows you to report on and show evidence of you and your partners' adherence to the policies and practices mandated by regulatory frameworks such as NIST, CMMC, GDPR, and others. When reporting to the board, you can instantly pull high-level reports that show vendor portfolio trends over time to align TPRM strategy with your company's business goals and risk tolerance. To further customize reporting, you can drill down into the exact business units, geographies, and domains within partner organizations that process your data.

Roadmap to success

The present represents a sink-or-swim moment in which companies can either adopt next-generation tools and practices to remain competitive, or take on significant operational and reputational risk. At SecurityScorecard, our experience rating the security posture of millions of organizations has shown us that when companies focus their efforts on the right areas, they can keep up with the pace of change and set themselves apart from their industry peers. Now is the time to own your security rating to make your company a sustainable strategic partner.

As digital transformation becomes a greater part of every organization's operations, having a fully automated, integrated, and scalable TPRM program is essential to effectively assessing and monitoring your entire third-party network. Choosing a platform with pre-built integrations and flexible APIs allows you to build out workflows within your unique environment—without ripping and replacing.

Leveraging comprehensive scanning technology allows your team to accelerate the speed at which it gathers intelligence and rates the security of your company's vendors. This optimizes incident response time and reduces friction between internal departments by providing full, objective visibility of your attack surface on a timeline that doesn't impede business initiatives.

By implementing the practices and SecurityScorecard 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.

In conclusion, we'd like to leave you with a checklist of the top 12 attributes you should be looking for in a modern TPRM platform to meet your needs—today, and in the future:

1. Scans the global IP space daily
2. Security ratings reports on demand
3. Machine learning-driven scoring
4. Ecosystem-wide visibility of CVEs
5. Customized board and compliance reporting
6. Automated third-party security assessments
7. Continuous vendor-ecosystem monitoring
8. Simple and automated vendor invitation process
9. API-driven interface for integrations
10. Segments and rates subsidiaries within partner organizations
11. Accurate ratings and rapid refutation process
12. Score-improvement planning

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.

[7] Forrester 2021 - The Total Economic Impact™of SecurityScorecard

- **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.

According to Forrester research, SecurityScorecard users recovered their investment after three months and saw an **ROI of 198%.**[8]

> ***"Using SecurityScorecard has clearly improved the speed of our response to security incidents in our supply chain, as well as our ability to take preventative actions in areas that really matter."***

ANTERO PÄIVÄNSALO

CHIEF INFORMATION SECURITY OFFICER, NOKIA

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.

SecurityScorecard

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