SecurityScorecard

Expand your Vendor Intelligence to Identify Active Threats

Third-party cyber risk is a business risk.

Manage your third- and fourth-party attack surface and be prepared to expect the unexpected.

EXPECT the UNEXPECTED

Table of Contents

EXPECT the UNEXPECTED

How to Manage Your Third- and Fourth-Party Attack Surface

Research by SecurityScorecard and the Cyentia Institute found that 98% of organizations have at least one vendor that's had a breach in the last two years, highlighting the scope of indirect exposure to risk. While third-party risk has been elevated to a key business risk, it is more challenging than ever. Even more alarming, only 34% of organizations are confident their suppliers would notify them of a breach that could put their business at risk.

As the global attack surface continues to expand, security teams are being asked to do more. They not only have to manage the security posture of their own organization, but that of their third-and fourth-parties too. Additionally, regulators around the world are putting a microscope on third-party risk management, demanding compliance. It's more important than ever to tighten and mature third-party risk management (TPRM) programs, also referred to as vendor risk management (VRM). Staying ahead of weaponized vulnerabilities and threat actors targeting your vendors' assets decreases the chances of a cyber disruption to your organization.

Staying ahead will ensure your organization is prepared to expect the unexpected.

Key Takeaways

1. Learn how to mature your third-party risk management program by incorporating threat intelligence to uncover true risk and threats across your vendor ecosystem.
2. Understand the difference between cybersecurity ratings and threat intelligence, and how they complement each other. Cybersecurity ratings identify potential risk. Threat intelligence surfaces active threats that put your vendors and your business at risk.
3. Evaluate how a large enterprise customer uses SecurityScorecard's Attack Surface Intelligence to proactively pinpoint risks, alert the vendor, and provide the incident response team with context and actionable next steps.

What is Third-Party Risk Management?

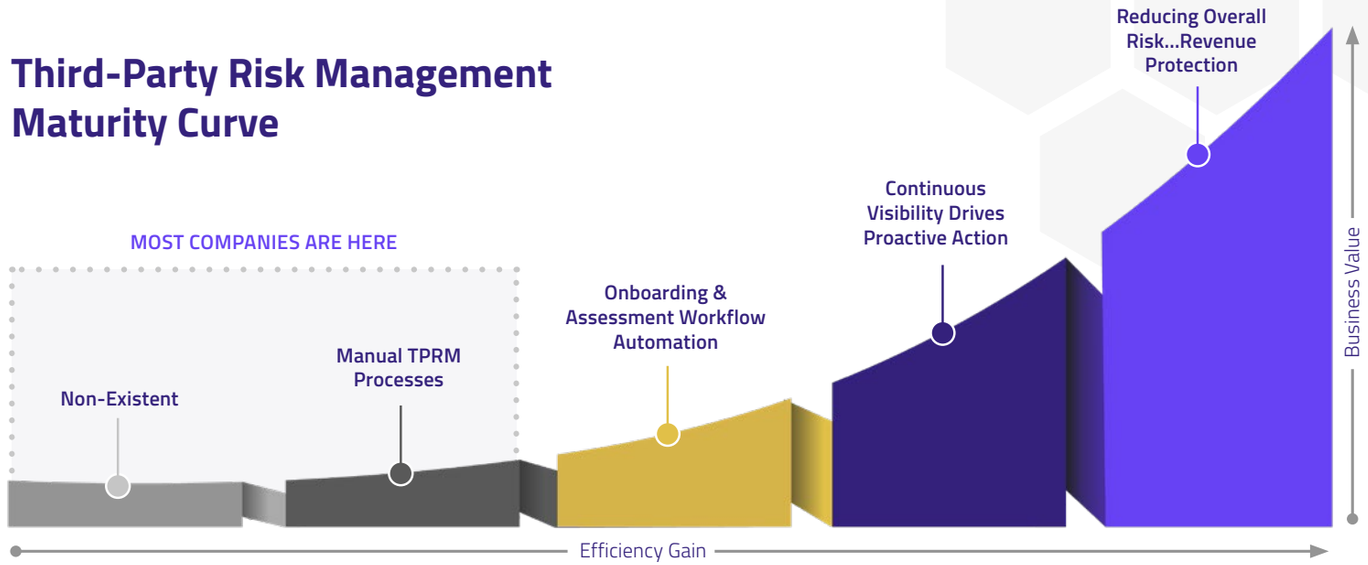
In addition to the evolving nature of cyber threats, technology stacks are expanding and the use of third-party vendors is growing at a high rate, introducing more risk into the environment. It is crucial for cybersecurity teams to know the level of risk to the organization from each of these business relationships.

TPRM is the process of monitoring your third-, fourth-, and even fifth-party relationships to ensure that they do not create unfavorable business outcomes, disrupt day-to-day operations, or expose your organization to a security risk. This is typically done through a third-party risk management program, which includes processes, procedures, and technology to help organizations assess, monitor, and manage risk exposure that stems from these relationships. Should there be a third-party risk event, TPRM programs also include comprehensive plans for risk mitigation to reduce the impact of legal liabilities and reputational damage.

How Mature is Your Organization's Third-Party Risk Management Program?

No organization's TPRM program is the same; however, most are at a level where they are moderately managing vendor risk. Let's take a look at the different levels of the TPRM maturity curve below and steps you can take to uplevel your program to mitigate third-party risk.

Third-Party Risk Management Maturity Curve



QUIZ Part 1

Determine Your Third-Party Risk Management Program's Maturity

01 **Does your organization have fully built-out and up-to-date TPRM policies and procedures?**
YES or NO

02 **Does your TPRM program have a dedicated person to manage vendors?**
YES or NO

03 **Are vendor questionnaires sent out and tracked through a platform, not spreadsheets?**
YES or NO

If you answered **YES** to a majority of the questions, skip to the next quiz. If you answered **NO** to a majority of the questions, read below to understand the next steps to mature your program.

NEXT STEPS:

Based on your answers, your organization's maturity level is in the **early stages with mostly manual processes.**

Recommended next steps are:

- Identify business goals and objectives of managing third-party vendors to create a more formal TPRM program.
- Develop or reevaluate policies and procedures based on best practices.
- Choose a process or platform for sending and receiving responses to questionnaires.
- Understand how and what to report to business leaders to show value and maintain the forward momentum of your TPRM program.

QUIZ
Part 2

01 Does your organization tier vendors by criticality to the business?
YES or NO

02 Does your organization continuously monitor vendor risk through a cybersecurity ratings solution that takes an outside-in view of multiple security controls?
YES or NO

03 Are vendor questionnaires tailored based on the cyber risk rating or recent security events that impact your third-party vendor?
YES or NO

04 Are you able to clearly articulate vendor risk to the board on a consistent basis?
YES or NO

05 Are cyber risk ratings used to make business decisions in regard to mergers and acquisitions, procurement, and contractual language in contracts?
YES or NO

If you answered **YES** to a majority of the questions, skip to the next quiz. If you answered **NO** to a majority of the questions, read more to understand the next steps to mature your program.

NEXT STEPS:

Based on your answers, your organization's maturity level is moving in the right direction with the **development of onboarding and assessment workflow automation.**

Recommended next steps are:

- Begin to develop and tier vendors based on impact to your business.
- Automate tedious vendor risk management duties to reduce the amount of time spent evaluating vendors and completing assessments.
- Work with your cybersecurity ratings provider to operationalize the platform with your business goals.
- Socialize your TPRM program with your vendors and customers to lay the foundation of trust and due-diligence in working together.

QUIZ
Part 3

01 **Does your organization evaluate risk posed by your fourth- and fifth-party vendors?**
YES or NO

02 **Does your organization automatically report cyber risk findings through easy-to-understand visualizations of the data to help the board and business leaders see solid ROI and understand TPRM efforts?**
YES or NO

03 **Are you able to measure the financial impact of a potential attack through a third-party vendor?**
YES or NO

If you answered **YES** to a majority of the questions, skip to the next quiz. If you answered **NO** to a majority of the questions, read below to understand the next steps to mature your program.

NEXT STEPS:

Based on your answers, your organization's TPRM program is close to delivering **continuous visibility to drive proactive action.**

Recommended next steps are:

- Continuously and easily provide key metrics to the board and key stakeholders.
- Measure the financial impact of a potential attack on your vendors to help quantify cyber risk.
- Automate the detection of all vendors in your digital ecosystem and create workflows to identify potential issues.
- Further mature your TPRM risk program through advisory services that focus on elevating your TPRM program beyond assessment completion and evaluation.

QUIZ
Part 4

01 Does your team know how to easily digest and use threat intelligence to understand, identify, and alert vendors of their threats and vulnerabilities that put your organization at risk?

YES or NO

02 Does your organization have a process to validate the vendors security posture with a deeper view into their attack surface?

YES or NO

03 Are you able to provide deep vendor intelligence insights to the incident response and vulnerability management teams to help them understand how to prioritize remediation?

YES or NO

04 Is your TPRM program advocated by the leadership team, building a risk-aware culture company-wide?

YES or NO

If you answered **YES** to a majority of the questions, congratulations! You are a leader among your TPRM peers. Check out how SecurityScorecard's expanded vendor intelligence helps find the unknown unknowns in your vendors' attack surface.

If you answered **NO** to a majority of the questions, read below to understand the next steps to mature your program.

NEXT STEPS:

Based on your answers, your organization's TPRM program is ready to build a deeper foundation to **reduce overall risk and protect revenue.**

Recommended next steps are:

- Identify how to add threat intelligence insights to your TPRM workflow. SecurityScorecard's Attack Surface Intelligence solution allows program owners to discern who in their vendor portfolio has active threats.
- Develop and set up workflows for proactive vendor notification or provide incident response teams with contextual information to take action.
- Prove the ROI of incorporating threat intelligence into your TPRM program to business leaders by sharing trending data.

No matter where your organization is in the process of managing vendor risk, you can't let your guard down or you could be the next victim of a cyber attack. **Reach out to experts to help you today.**

GET STARTED

How Intelligence Builds a Stronger and More Proactive Offense

A cyber attack through one of your third-party vendors could be prevented by using intelligence to track and alert you of your vendors' critical vulnerabilities and active threats that they may not be able to see themselves. Incorporating intelligence as part of your Third-Party Risk Management program helps you answer the following questions:

1. Have any third- or fourth-party vendors been part of a recent ransomware attack?
2. Which of my critical vendors in my portfolio have active threats and what is the severity of these threats to my business?
3. What vulnerabilities in my vendors' attack surface are at risk of being weaponized?
4. How do I provide deeper insights and context for my incident response team to investigate an at-risk vendor?

When threat intelligence is surfaced in an easily digestible fashion—for instance, when viewing your vendor portfolios—you catch your vendors' vulnerabilities in minutes and before they're exploited. Expanded vendor intelligence enables you to analyze your vendor-induced risk by exposing your vendor's vulnerabilities in minutes and collaborate with them to remediate before their vulnerabilities are exploited.

Not only can you identify threats, but you can ingest the intelligence data that is arranged contextually to alert your vendor to take action with a clear path to remediate and reduce the risk to your expanding attack surface.

Understand and Identify Risks in Your Vendors' Attack Surface Intelligence

SecurityScorecard's Attack Surface Intelligence allows everyone to be a threat researcher with the most contextualized global threat intelligence for you to drive actionable decisions to defend against attacks. SecurityScorecard provides a fully comprehensive solution to managing vendor risk including its cybersecurity ratings, vendor questionnaire engine, workflow capabilities through integrations and APIs, and more. SecurityScorecard Ratings help organizations view attributed cyber risk, providing a look into a vendor's security posture to give businesses a way to measure the probability of risk. Threat intelligence provided through SecurityScorecard's Attack Surface Intelligence module offers a unique capability to display real threats that are active in a 360-degree view by vendor portfolio or magnified at the individual vendor level. Malicious threats shown in your vendors' environments mean that the door is open for your organization to experience an attack.

Let's take a look at how SecurityScorecard's Attack Surface Intelligence helps TPRM teams advance their program and show proven ROI of how they've saved the organization time and money, and stopped potential disruption early.

How Attack Surface Intelligence Helped Oceano Industries Proactively Assess Vendor Risk

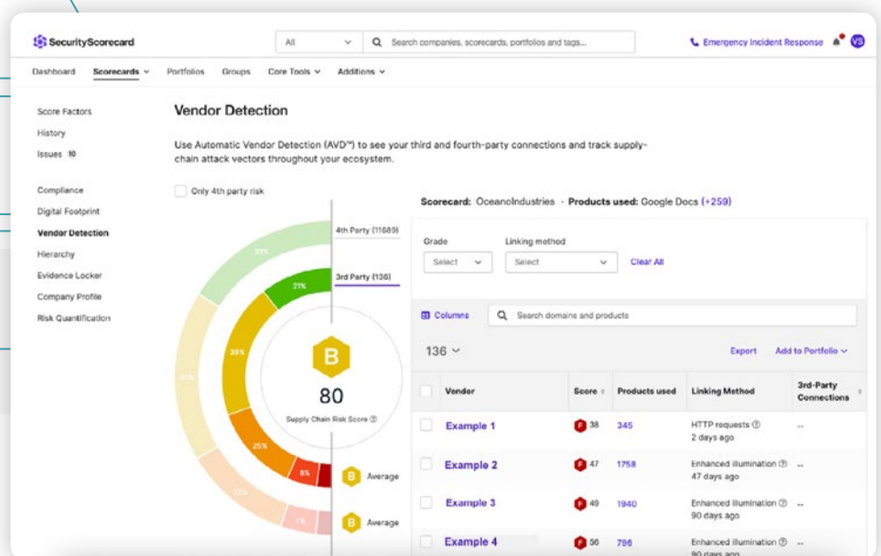
While Attack Surface Intelligence fits a variety of organization profiles in terms of size, maturity, and TPRM methodology, we will share a real- life example of one of SecurityScorecard's customers. For privacy purposes, the name of the customer has been altered.

Oceano Industries is a large manufacturer. Their customer base includes cruise lines, shipping companies, and even the U.S. Government. With this variety of clientele they are heavily regulated and required to comply with multiple frameworks, such as CMMC, PCI, NIST, and others. Oceano is also affiliated with an industry-based, information sharing and analysis center (ISAC).

Given the complexity of their operations, Oceano has more than 800 vendors in their SecurityScorecard Portfolios. The sheer volume of third-party risk has driven Oceano to invest in a mature TPRM program with a well-staffed team and even an incident management "sub-team".

Expanded Capabilities

Oceano's parent TPRM team typically monitors vendors and vets potential vendors at an administrative level, focusing more on questionnaire assessments. Upon learning about significant security events, such as drastic score drops or breaches, they engaged their incident response team to contact affected vendors to investigate these events, provide remediation recommendations, set remediation expectations, and track progress. SecurityScorecard's Platform and Services suite supports this TPRM model in a number of ways.



Prioritizing Threats with Existing Vendors

Oceano's TPRM team is tasked with monitoring their 800-plus vendors and identifying risks on an ongoing basis.

At an administrative level, this means sending each vendor an annual, quarterly, or even monthly review-assessment, depending on the vendor's criticality to Oceano's operations and their level of system permissions or exposure to sensitive information. Sending questionnaires from SecurityScorecard, the TPRM team inquires about any changes affecting the vendor's security posture, such as deployment of new cyber-defense products, renewed compliance with key frameworks, and breaches.

At a tactical level, the TPRM team uses SecurityScorecard's Rule Builder to generate automatic alerts on any significant changes to vendor Scorecards, such as significant score drops or breaches. This ensures that they never miss a change or potential critical vulnerability that could affect one of their vendors.

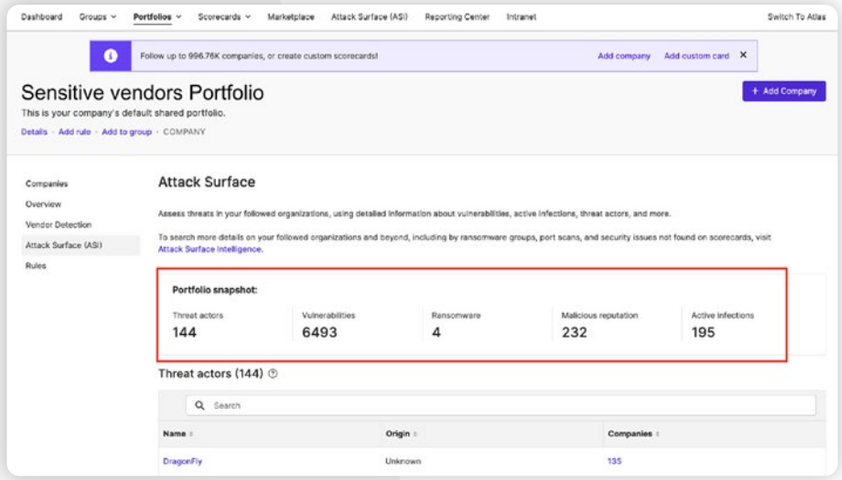
Additionally, they use Automatic Vendor Detection to identify their vendors' third- and fourth-party ecosystems for low scores, the products their vendors use, and other items of concern.

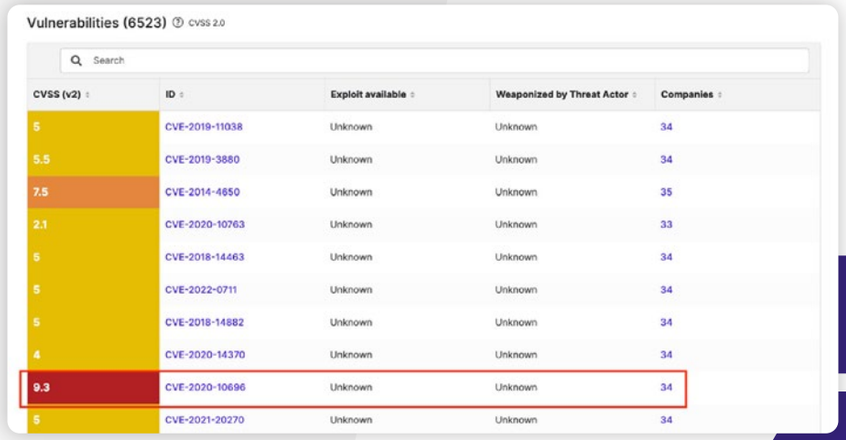
Zeroing in on Actionable Threats with Attack Surface Intelligence

This broader coverage keeps Oceano apprised of their vendors' cyber-health on a continuing basis. With Attack Surface Intelligence, the TPRM team can quickly scan their portfolios for threats that demand immediate attention.

Clicking the Attack Surface Intelligence tab of any portfolio, the team immediately sees tallies of actionable threats, such as:

- Detected **ransomware events**
- **Threat actors** known to have weaponized vulnerabilities found on vendors' assets
- Vendor IPs with **malicious reputations**, which indicate that they may have been breached and controlled by threat actors to launch attacks on other internet targets
- Detected active **malware infections**





Scrolling down the Attack Surface Intelligence landing page, they can drill into these actionable threats to determine which vendors are implicated and gain more critical details and context to pass on to their incident response team.

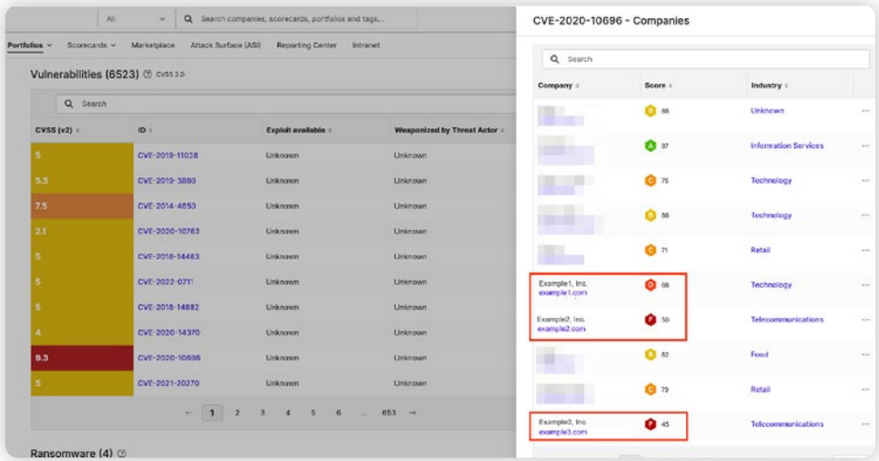
Noting four ransomware events, they scroll to the Ransomware section of the page and see which of their vendors are affected.

Sorting common vulnerabilities and exposures (CVEs) by severity, Oceano brings the highest-severity CVEs to the surface and clicks the number of companies affected by these vulnerabilities...

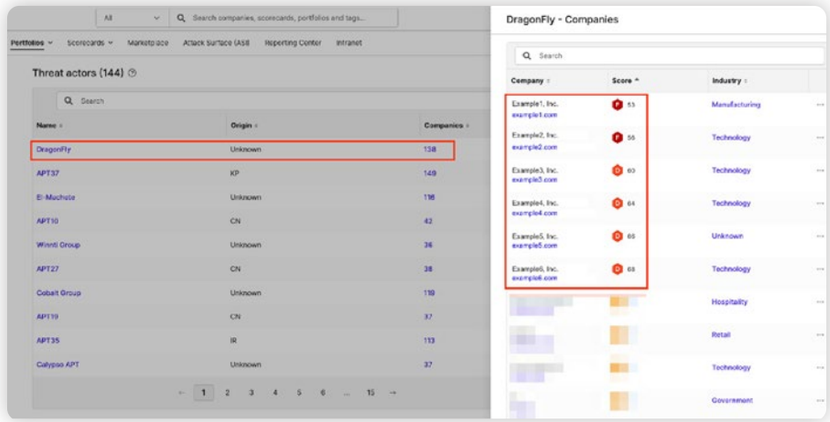
...and then notes the l highest-scoring companies as requiring the most urgent attention.

USE CASE

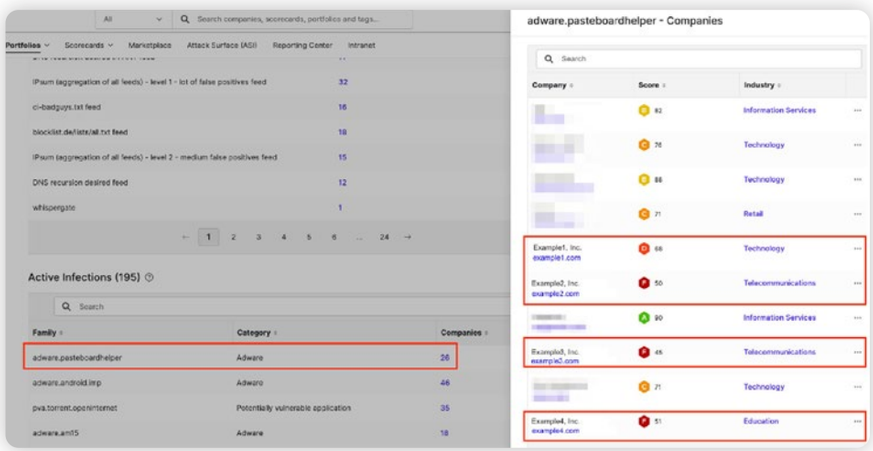
How Attack Surface Intelligence Helped Oceano Industries Proactively Assess Vendor Risk



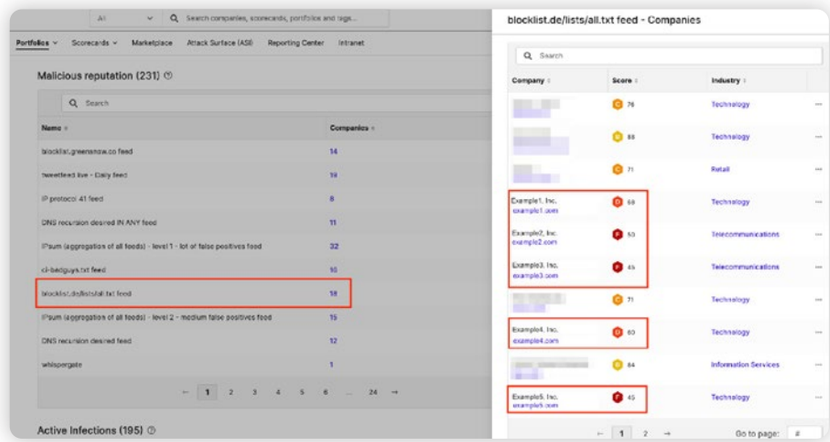
Oceano's TPRM team does the same with active infections...



...and malicious reputation posts.



...threat actor connections,...



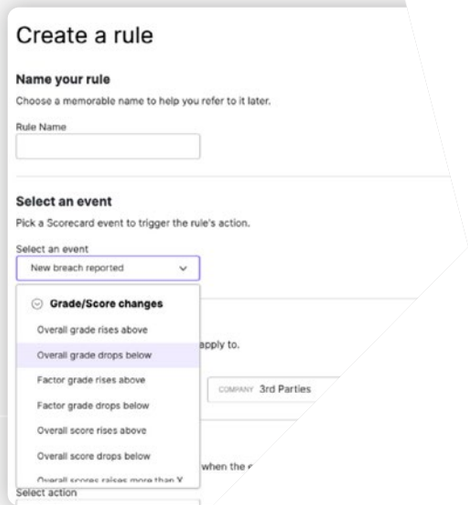
Create Automated Rules for Vendor Event Notifications

Using the Rule Builder, the TPRM team is able to automatically add or remove a vendor from a portfolio, create a report, send a vendor an alert, or send a questionnaire.

Rules are triggered by various changes in a vendor scorecard including:

- Change in score
- High-severity issue
- CVE detected
- Breach detected

Producing a list of at-risk companies helps Oceano's incident response team engage the vendors without much effort on their part.



Supporting Vendor Outreach

Oceano's incident response team reviews the TPRM team's list and uses Attack Surface Intelligence throughout its outreach operations.

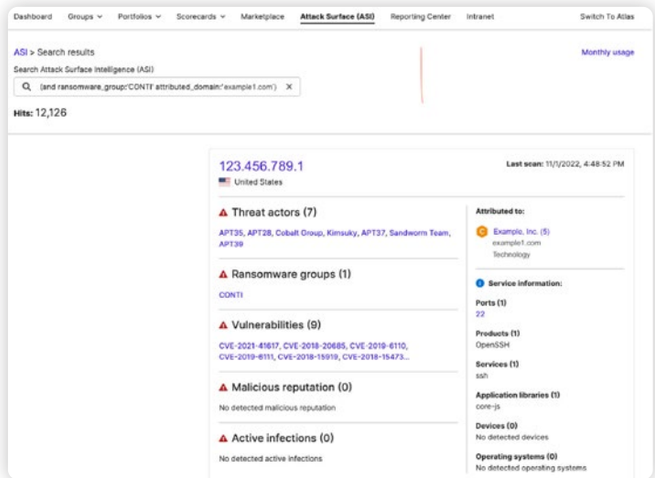
For each vendor, the incident response team queries Attack Surface Intelligence for key, threat-related details. Running a vendor query from the portfolio is as simple as selecting an Attack Surface.

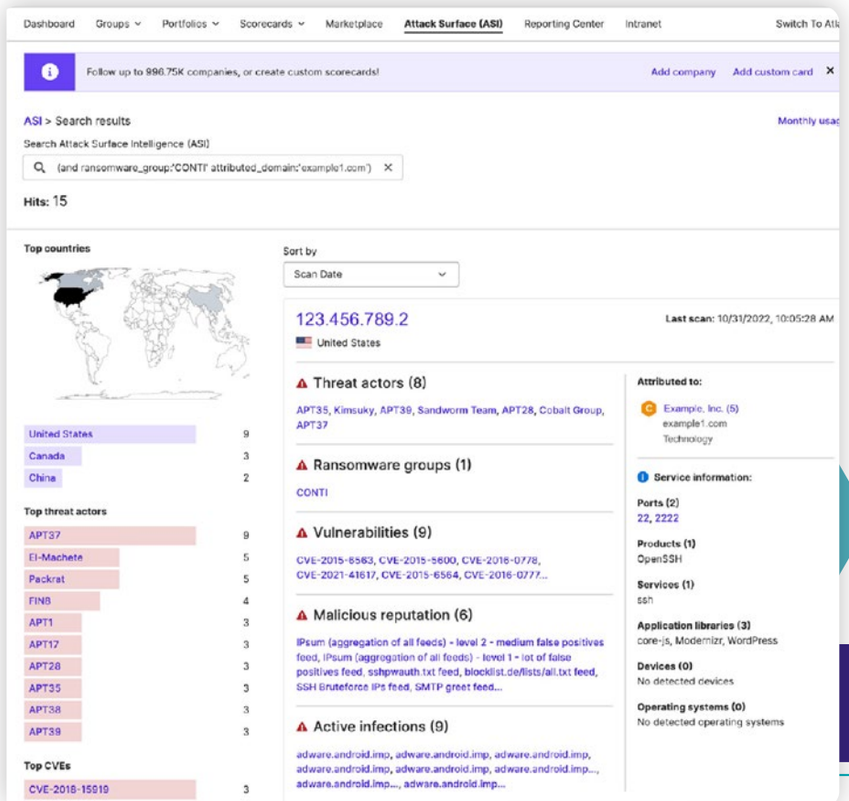
Intelligently search for a given vendor in any of the threat-related views where they appear:

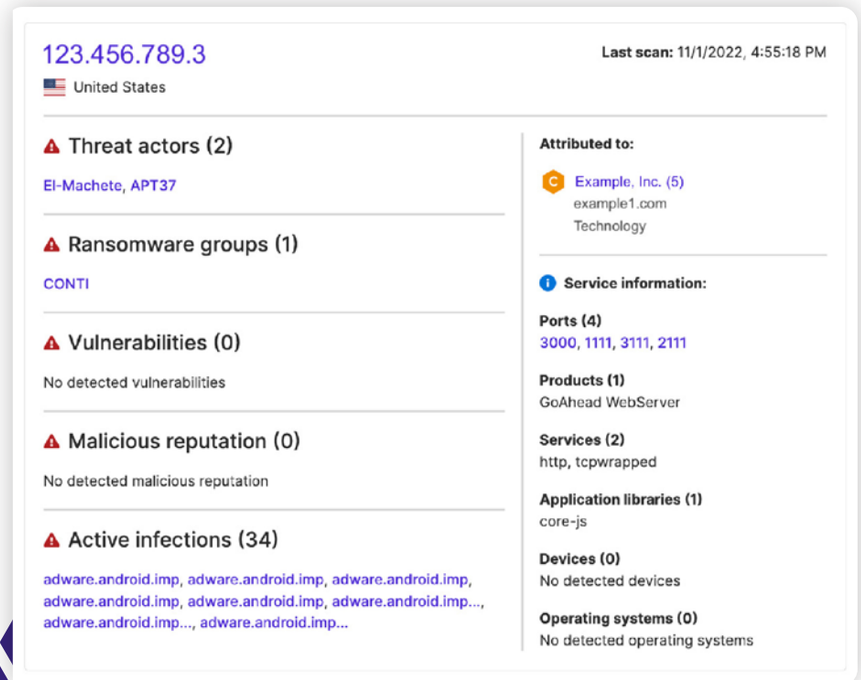
- Threat actors
- Malicious reputation
- Vulnerabilities
- Ransomware (as in the following screenshot)
- Active infections

The queries bring up details about each IP address attributed to the vendor, such as all detected vulnerabilities and threat-related data points. The details also include geographic location and comprehensive data about processes running on open ports.

Using this intelligence, Oceano's incident response team can put together a deeply contextual understanding of the risks these vendors carry.





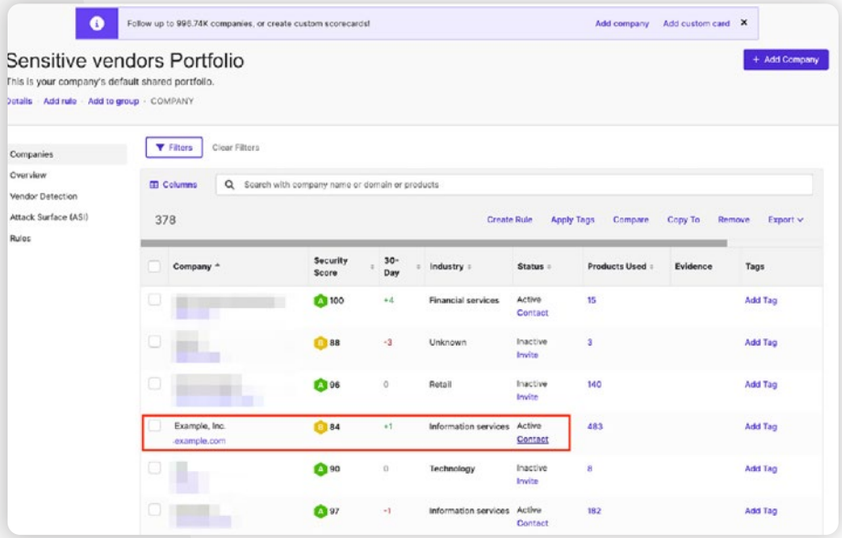


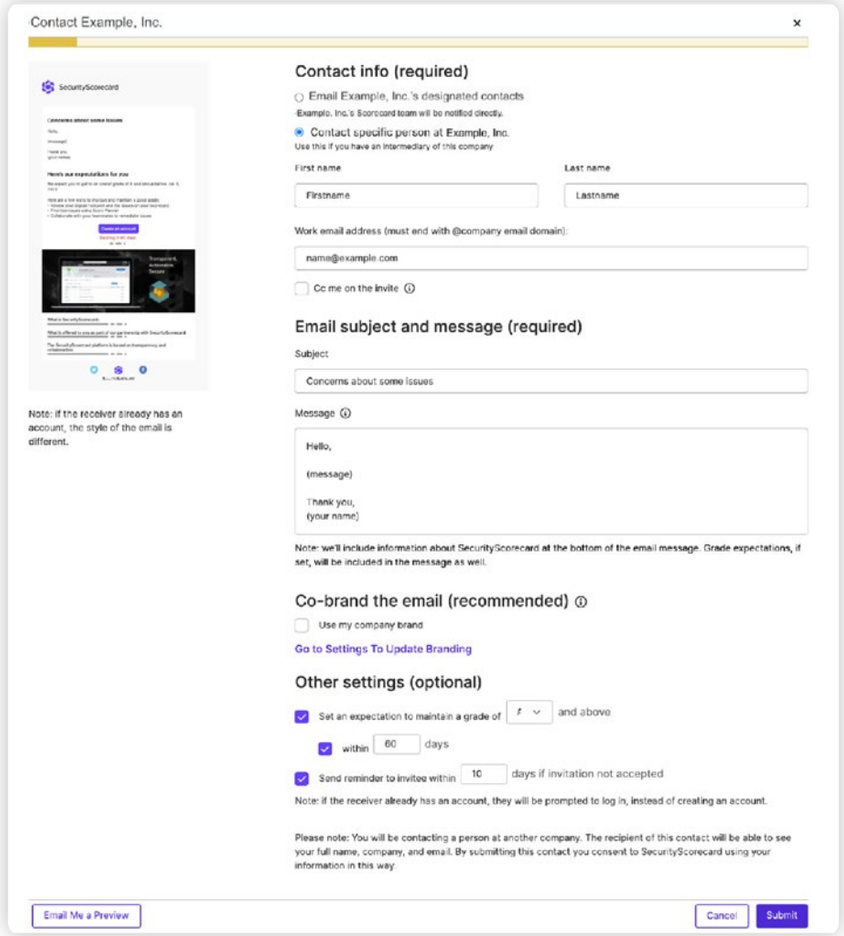
When they reach out to vendors about these issues, they use their Attack Surface Intelligence findings to answer any vendor disputes about the raised issues and to help the vendors in their own remediation efforts.

Reaching Out to Vendors Right From the Ratings Platform

When they're ready to engage with vendors to address concerning issues, Oceano's team contacts them directly from the Portfolio...

...and sends them a personalized message with the option to set expectations for score improvement within a certain timeframe.





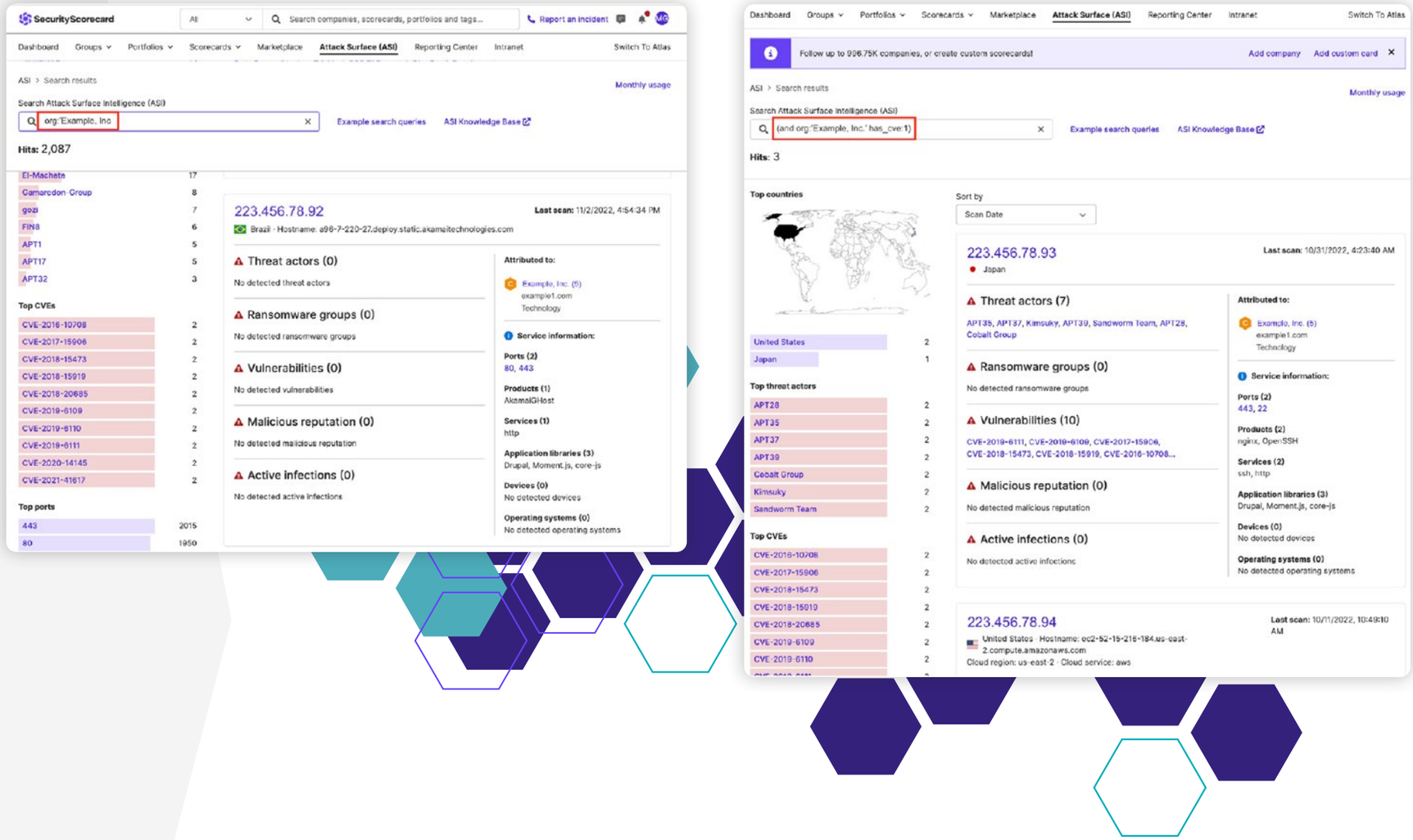
Assessing Risk with Potential Vendors

By running queries through Attack Surface Intelligence, Oceano's TPRM team can vet potential vendors for risk at different levels of depth and breadth. Queries return detailed threat-relevant information about every internet-facing asset a vendor has deployed.

They can simply query on an organization's name to get a comprehensive view.

They can narrow the query to only IPs that have vulnerabilities...

...or ransomware events.



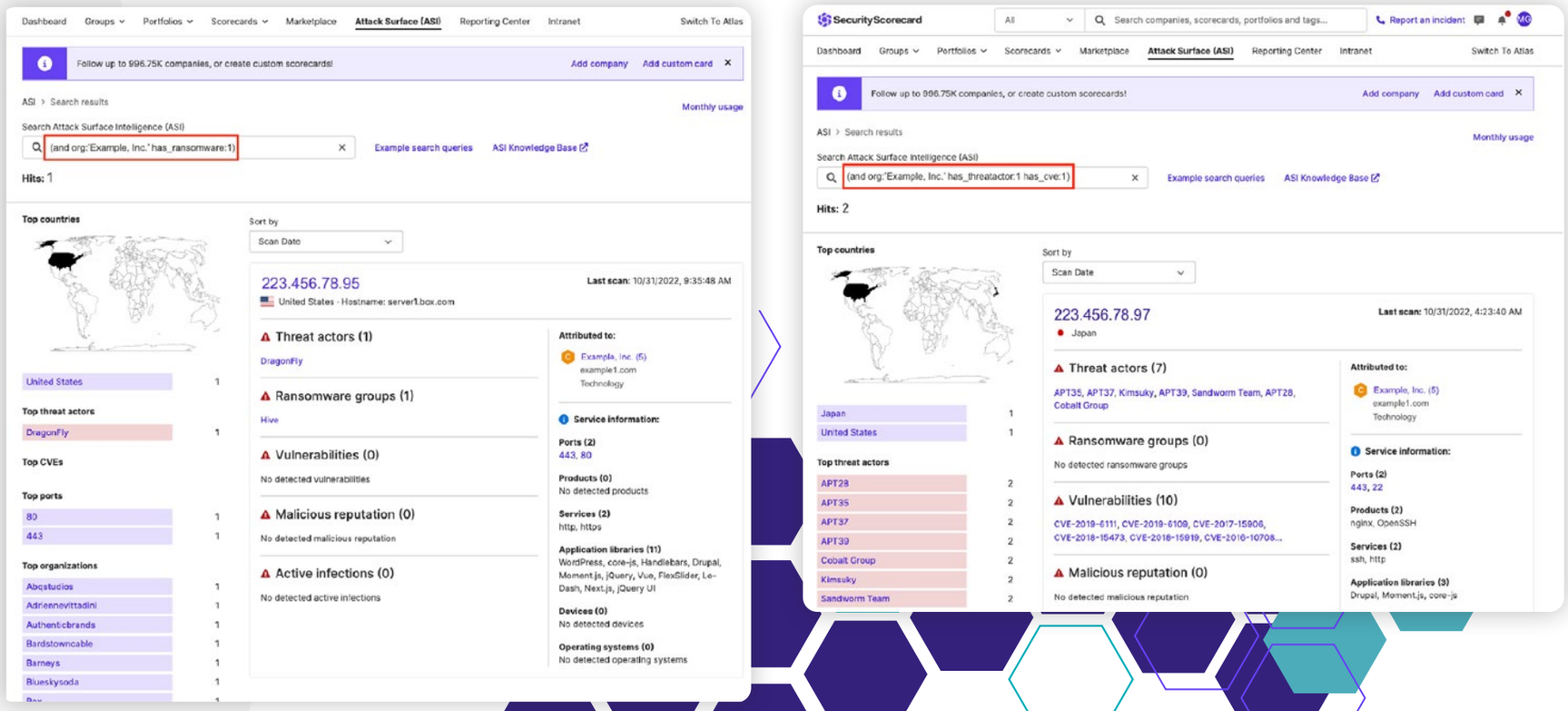
And they can combine data facets to refine results, for example, finding IPs with CVEs and threat actor connections.

This level of detail is especially relevant for prospective vendors who would have higher network permissions or access to sensitive data, such as a database host provider.

Assessing Risk of Mergers and Acquisitions (M&A) Targets

Attack Surface Intelligence queries provide Oceano a discreet way to study prospects for mergers and acquisitions. Oceano can avoid adding these organizations to portfolios that might be visible across the organization, preventing unwanted attention early on in the M&A process.

Leverage Attack Surface Intelligence as part of your due diligence process for M&A and start collaborating internally on the level or risk to accept or address.



Conclusion

With threat intelligence incorporated into your TPRM program, finding the unknown unknowns in your vendor's attack surface is a whole lot easier. Schedule a demo of Attack Surface Intelligence or reach out to our Cyber Risk Intelligence team to learn how our threat hunting experts can support your efforts and help you gain cyber clarity on your vendors' attack surface.

Drive Confident Decision Making

SecurityScorecard is proud to support over 50,000 organizations with a platform to integrate, leverage, and present security data for security teams, non-technical audiences, and the board to understand and act upon.

SecurityScorecard's platform expands its offerings beyond traditional security ratings capabilities so, organizations can gain needed insights to help mitigate these new risks.

PROFESSIONAL SERVICES

Proactive Security

Defend your organization with a range of proactive services, including: penetration testing, red teams, and tabletop exercises. Battle-test your security controls, identify gaps in your attack surface, and enhance your ability to defend against cyberattacks.

Digital Forensic and Incident Response

Be ready to respond to any threat confidently and mitigate business interruptions from a cyberattack by partnering with industry-leading experts in digital forensic and incident response services. Integrate data forensics and incident response (DFIR) capabilities to augment your security team's capabilities with SecurityScorecard on demand.

Zero-Day-as-a-Service

Available as part of Managed Cyber Risk Services or individual offering, Zero-Day-as-a-Service is an early warning and detection service, alerting organizations to new and emerging potential zero-day vulnerabilities across their third-party vendor landscape.

Managed Cyber Risk Services

Delivered by our Risk Operations Center (ROC) of cybersecurity professionals, Managed Cyber Risk Services helps organizations operationalize their third-party cyber risk management program to stop attacks before they happen using the platform's powerful risk signals, predictive intelligence, and expert-led breach response capabilities.

Cyber Risk Intelligence

Delivered by SecurityScorecard's STRIKE Threat Intelligence team, Cyber Risk Intelligence fills critical intelligence gaps and illuminates cyber risk trends, enabling cyber security teams to deploy limited cyber resources to the most efficient areas.

PRODUCTS

Security Ratings

Consistent and data-driven cybersecurity scores enable our customers to understand the vulnerabilities in their own environment as well as their third- and fourth parties. A standard A-F grading scale streamlines cyber risk communication and empowers risk mitigation across the entire vendor ecosystem.

Cyber Risk Quantification

Put cyber risk into monetary values so that all investments are justifiable and aligned with broader business goals.

Security Data

Power your existing business workflows with the industry's most trusted security data about your organization and business ecosystem.

Questionnaires

Save time and gain a 360-degree view of your vendors with the only customizable questionnaire to automatically validate responses against.

Attack Surface Intelligence

Most threat hunters find it challenging to stay up to date on current threats as threat adversaries become more sophisticated and the global attack surface continuously evolves. Attack Surface Intelligence aids threat hunters in collecting thorough and essential data on the global attack surface for faster, more effective risk mitigation and threat prioritization.

Automatic Vendor Detection

Security and third-party risk management teams are struggling to keep up with the growing ecosystems of third- and fourth-party vendors supporting their business. Automatic Vendor Detection instantly gives you a view of your entire business ecosystem, enabling you to visualize and take active steps to mitigate risk.

Evidence Locker

Vendor Risk Managers spend countless hours, even days, chasing down answers and validating questionnaires. With SecurityScorecard, organizations can openly exchange security artifacts to simplify the vendor risk assessment process. Save time by managing compliance artifacts, track artifact history, and monitor the compliance initiatives in a single view.

Marketplace

Security, IT, and VRM teams deploy an average of 47 different cybersecurity technologies and solutions, and many don't integrate with each other. The SecurityScorecard Marketplace helps you maximize and integrate investments in your security stack with out-of-the-box integrations with leading technology organizations, and the ability to build your own custom solutions with our Rule Builder and SecurityScorecard's APIs.

Integrate SecurityScorecard data into your tech stack to drive integrated workflows, mitigate risk faster, and augment security data through our ecosystem of 90+ integrations, apps, and digital risk intelligence data.

Reporting Center

Contextualize and communicate cyber risk into business problems with a flexible reporting dashboard that tailors to your business needs.

SecurityScorecard Academy

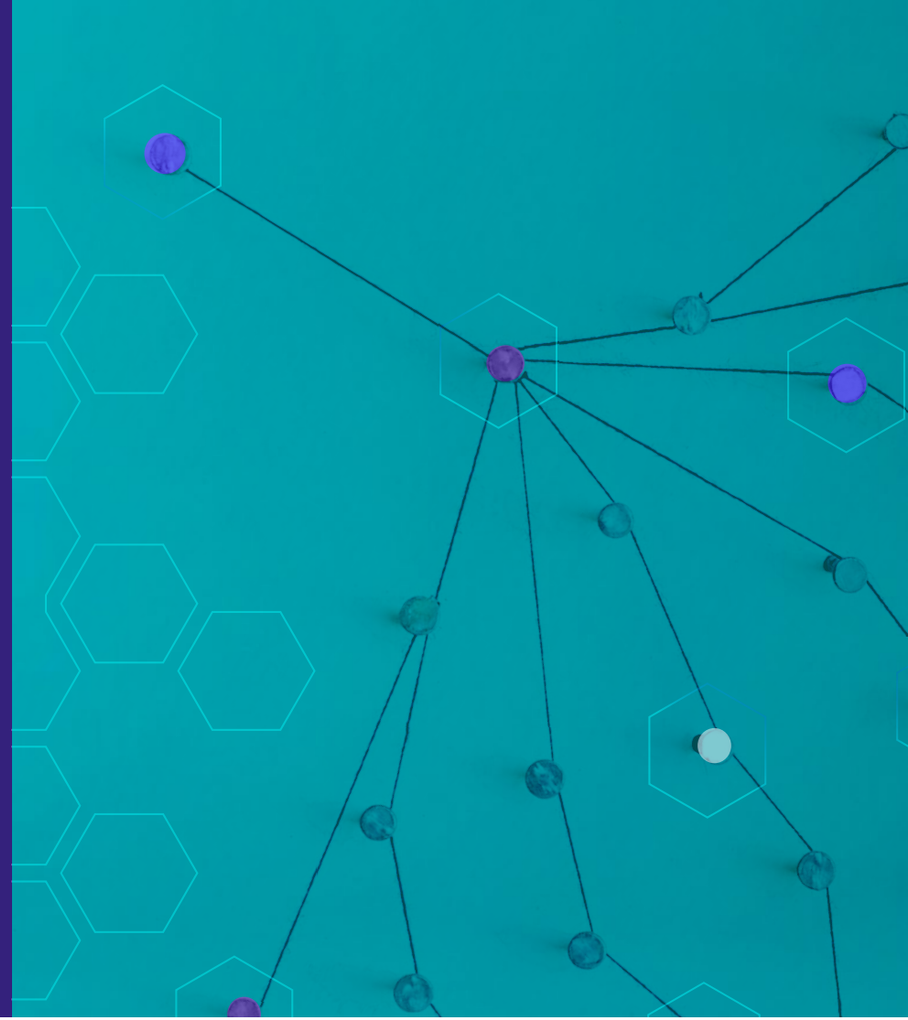
Uplevel internal stakeholders with certifications and knowledge to augment your security program, with courses ranging from cyber insurance, board reporting, third-party risk management, and more. We give your team the products to fill knowledge gaps and gain the skills they need to take control of your organization's cybersecurity.

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 50,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.



Talk to an Expert

10X your security performance with the world's most complete security ratings platform.

GET STARTED

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166