EVOLVE FROM RISK MANAGEMENT TO RISK INTELLIGENCE

Proven Strategies to Drive a Risk Intelligence Program in Your Organization

SecurityScorecard
The Power of Knowing

SecurityScorecard.com
info@securityscorecard.com

Tower 49 12 E 49th St Suite 15-001
New York, NY 10017
United States: (800) 682-1701
International: +1 (646) 809-2166

INTRODUCTION

The increasing volume and sophistication of ransomware and supply chain attacks in today's digitally transformed world mean that organizations must mature their cyber risk management practices. At the same time, the move to remote work and increased adoption of cloud technologies expands the attack risk surface. COVID-19 accelerated digital transformation by an average of six years between January and September of 2020[1]. In response to these challenges, more security teams need intelligence-led security.

Cyber resilience relies on being proactive rather than reactive. Organizations need to move beyond risk management strategies and embrace risk intelligence. Taking a 360° view of risk provides the intelligence required to protect the attack surface from every angle.

At the same time, threat actors continue to outpace organizations' ability to manage risk. With quickly shifting tactics and criminal operation groups that run like businesses, threats are ever more dangerous and persistent. Threat actors are continuously looking for both internal and external ways and means to infiltrate an organization's network. Their attacks are intended to steal data by leveraging an arsenal made up of phishing attacks, ransomware, malware, and other tactics and techniques.

Often, malicious actors use these credential-based and phishing attacks to deploy ransomware. According to Crowdstrike's 2022 Global Threat Report, ransomware-related data leaks increased by 80% in 2021 compared to 2020[2]. For example, a recent report[3] found:

- **17% increase in credential stuffing** attacks in 2021 compared to 2020
- **89% of organizations experienced a phishing attack** in 2021

[1] Koetsier, J. (2020, September 14). 97% Of Executives Say Covid-19 Sped Up Digital Transformation. Forbes. https://www.forbes.com/sites/johnkoetsier/2020/09/10/97-of-executives-say-covid-19-sped-up-digital-transformation/

[2] CrowdStrike. (2022, February 15). 2022 CrowdStrike Global Threat Report | CrowdStrike. Crowdstrike.Com. https://www.crowdstrike.com/resources/reports/global-threat-report/

[3] 2022 State of Passwordless Security Report | HYPR. (2022). Hypr. https://get.hypr.com/2022-state-of-passwordless-security

TABLE **OF CONTENTS**

WHAT DOES IT MEAN TO EVOLVE A RISK MANAGEMENT STRATEGY TO A RISK INTELLIGENCE-INFORMED PROGRAM?

While some organizations are more mature than others, most have a risk management program in place. Unfortunately, the traditional approach to managing risk no longer works as the world - and cyber risk - continue to evolve.

Moving from having a risk management program to one leveraging risk intelligence means:

- Creating alignment
- Integrating the right security tools to meet the organization's needs
- Up-leveling people, processes, and programs

From Risk Management to Risk Intelligence

Risk Management

Reactive
due to a basic and generalized view of risk

Cost center
that makes it difficult to secure necessary budget

One dimensional
approach to managing threats

Siloed workflows
due to lack of integrations and talent

Risk Intelligence

Proactive
data-driven action before vulnerabilities are exploited

Value creator
that propels business innovation and growth

Holistic
and integrated approach

Decisive action
with the right tools, people, and processes

WHAT IS RISK MANAGEMENT?

When risk and security professionals think about risk management, they may still focus on a legacy approach to threat mitigation. At the management maturity level, the organization may have processes that focus primarily on business-critical third-party vendors with mission critical data flows and availability dependencies.

This traditional approach views risk management as:

- **Reactive:** a basic, generalized understanding of risk in response to a point-in-time event
- **One-dimensional:** an approach to managing a single at a time, without a comprehensive view of risk
- **Costly:** a time-consuming and esource-intensive process
- **Siloed:** a one-dimensional view of individual risk indicators without correlating them

Some examples of this traditional risk management approach might be:

- Engaging in a risk assessment after adopting a new technology, then having to mitigate known vulnerabilities afterward, like updating default configurations. With risk assessments being an annual exercise, most teams implement new technologies within an environment without fully assessing the level of risk it introduces.
- Even with training and a strong security culture, sensitive information can leave an organization simply by accident, such as data stored in hidden rows in spreadsheets or included in external emails. Scanning an organization for sensitive data at rest and then removing any data stored where it does not belong dramatically reduces the risk of an accidental loss of sensitive data.

Even with due diligence, when an organization is unable to understand the post-integration risk or update configurations, the result can often be a time-consuming and isolated, point-in-time process.

UNDERSTANDING RISK INTELLIGENCE

Generally, intelligence is the process of collecting information that provides value, usually in a way that furthers a goal. When it comes to security, this means continuously collecting and correlating internal and external data about your digital footprint to enable proactive risk management.

Applying the common definition in the risk management context, risk intelligence is:

- **Proactive:** continuous activity, even without a triggering point-in-time event
- **Holistic:** data insights for informed decision-making through visibility and correlation across multiple vectors, such as internal and external threats
- **Value-driven:** information enabling all internal stakeholders across security, senior leadership, and Board of Directors
- **Decisive:** action informed by the right tools, people, and processes

An example of using risk intelligence might be: Continuously monitoring the Dark Web for leaked or weak credentials, reviewing user access, scanning for known vulnerabilities, and validating vendor security to create a complete risk profile.

With this level of well-defined insights, the organization can establish a proactive approach that allows it to apply consistent access policies that limit misconfiguration risk, unlike traditional risk management.

TRANSFORMING TO A RISK INTELLIGENCE-INFORMED PROGRAM

Digitally transformed environments and infrastructures incorporate dynamic data flows across various areas, meaning that static risk management lacks the ability to meet new security needs. Environments and infrastructures are multi-dimensional with on-premises, multi-cloud, and hybrid deployments, changing how data flows across integrations. These new environments enable organizations to grant more access to external users, like contractors and customers, creating another layer of risk.

The fundamental properties of a more sophisticated, risk intelligence-informed program include:

- Robust and scalable process
- Ability to consume more insights with less headcount
- Purposefully leveraging technology to achieve these goals

This holistic approach turns security into a value-provider by enabling the organization to make data-driven security decisions with visibility into multiple indicators across different vectors like:

- **External vulnerabilities:** Security patches installed to mitigate risk from common vulnerabilities and exposures (CVEs)
- **Threat intelligence:** Contextual business risk providing insight into targeted industries or vulnerability exploitability
- **Endpoint security:** Device attestation to prevent malware or ransomware
- **Authorization:** Secure passwords and multi-factor authentication (MFA) enabled
- **Containers:** Configuration review to ensure all cloud resources are properly configured
- **Cloud security:** Continuous monitoring of your cloud environment to detect identity and access management misconfigurations

With a risk intelligence-informed program, organizations can more effectively analyze, monitor, and mitigate risk, especially when they have the people, processes, and technologies they need.

WHY YOU NEED RISK INTELLIGENCE TO ENABLE A HOLISTIC SECURITY PROGRAM

With more sophisticated attacks, organizations need a more sophisticated approach to risk mitigation. Interdependencies lead to systemic risk, which is an emergent property of complex systems. While cybercriminals traditionally attack organizations through their core or “tier 1” third-party vendors, they also now leverage smaller providers.

A robust, value-driven security program revolves around understanding systemic risk that includes all vendors, not just those considered business-critical. Before setting security controls, an organization needs to understand all systems and networks that collect, store, process, and transmit sensitive data.

At a basic level, this means identifying and analyzing all risk arising from:

- Users
- Data
- Databases
- Access points
- Devices
- Networks
- Cloud services providers
- Third- and fourth-party vendors

In order to mitigate risk across all these different vectors, organizations establish various security controls. Often, each control comes with its own technology that needs to be managed, monitored, and fine-tuned, such as:

- Vulnerability scanners
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Security Information and Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR)
- Patch management systems
- Dark web monitoring tools
- Cloud Access Security Broker (CASB)

Gaining a single, unified view of security and risk across these different point products can be challenging. While the security team has the tools needed, without a holistic security program it may still struggle to seamlessly collaborate across the organization for rapid response and recovery.

This means that the organization finds itself in the difficult position of deciding whether to spend money on security or financing innovation.

BENEFITS OF USING RISK INTELLIGENCE FOR A MULTI-DIMENSIONAL SECURITY APPROACH

Point solutions give organizations a way to detect and respond to threats. At the same time, organizations can leverage risk intelligence to optimize their security stack.

Threat intelligence provides visibility into the evolving nature of attack methods. While often considered the same as risk intelligence, organizations need to keep in mind that threat intelligence only provides visibility into attacks targeting:

- Specific technology vendors
- Business partners
- Industries

While risk intelligence incorporates threat intelligence, it also includes risks arising from:

- Excess access
- Compromised credentials
- Network traffic
- Application security
- Password hygiene
- Vulnerability scans
- Malware variants
- DNS health

Risk intellignece brings all these signals together, and then applies data analytics so that organizations can measure risk more quantitatively. This allows them to establish cyber resilient security programs with enhanced risk mitigation capabilities for:

- Prioritizing risk and remediation actions to enhance productivity
- Reduced Mean Time to Identify (MTTI)
- Faster vendor onboarding
- Increased security stack return on investment (ROI)

MATURING A MULTIDIMENSIONAL SECURITY PROGRAM WITH A CULTURE OF RISK INTELLIGENCE

Risk intelligence gives security teams the data and analytics they need for meaningful decision-making. Also, it acts as a bridge between security and business leaders to provide a robust security posture that also aligns with the organization's overarching strategies. Too often, organizations fail to integrate business objectives into their security programs, excluding key senior leadership decision-makers.

ALIGN

Organizations adopt technologies to further their business objectives. At the same time, the security risks that certain technologies can create may undermine strategic objectives and visions. With that in mind, security becomes a business initiative that everyone needs to discuss meaningfully.

Business and security leaders need to have a shared understanding of the organization's current security state. Since risk intelligence provides visibility across external and internal threats, it offers the

data needed to understand current risk.

Once everyone is aligned around potential security control gaps, security and business leaders can collaborate to take proactive steps.

INTEGRATE

A gap assessment during the alignment phase also helps determine whether the organization needs to integrate or add additional security tools. Risk intelligence enables a multidimensional security program here as well.

If the organization finds that its current risk data fails to provide the visibility and metrics needed for a robust, resilient cybersecurity program, then it needs a security tool to close that gap.

For example, many organizations use anti-virus tools to protect devices from malware. With risk intelligence, the organization gains visibility into gaps in its detection and response capabilities, enabling it to make the data-driven decision to integrate an EDR tool.

Integrating the security tech stack is key to driving a robust risk intelligence program. On average, organizations deploy 47 different cybersecurity solutions and technologies. Yet, 53% have no idea if their security tools are working[4]. By integrating the security tech, organizations benefit from data-driven workflows powered by disparate data, both external, threat intelligence, and internal, correlating with each other.

IMPROVE

Security is about more than technology. It's also about the people who use the security tools and processes to mitigate threats. Organizations need to have processes that ensure consistency across detection, investigation, and response activities.

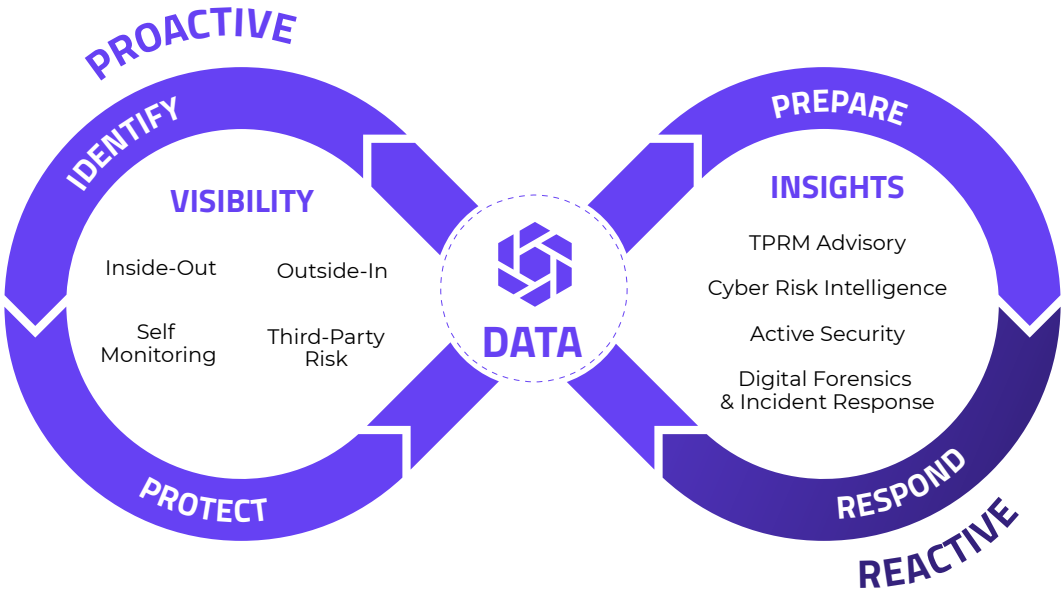
As threat actors continue to evolve their methodologies, organizations can use risk intelligence to provide security teams with the training they need. Risk intelligence creates hypothetical scenarios for

[4] The Cybersecurity Illusion. (2019, July). Ponemon Institute. https://go.attackiq.com/PR-2019-PONEMON-REPORT_LP.html

tabletop exercises that test processes. After completing the exercise, the security team can discuss areas for improvement, including fine-tuning security tools or updating processes.

CRITICAL ELEMENTS FOR EVOLVING A RISK MANAGEMENT PROGRAM TO A RISK INTELLIGENCE-INFORMED MANAGEMENT PROGRAM

Traditional risk management focuses on potential external threats. Evolving to a risk intelligence-informed program is a multipronged process. In this section, we will review the critical elements of building a holistic risk intelligence program that empowers you through every step of the cyber risk life cycle.



OUTSIDE-IN VIEW: UNDERSTANDING YOUR SECURITY POSTURE FROM THE HACKER PERSPECTIVE

Data breaches arise because external actors gain unauthorized access to a company's systems and

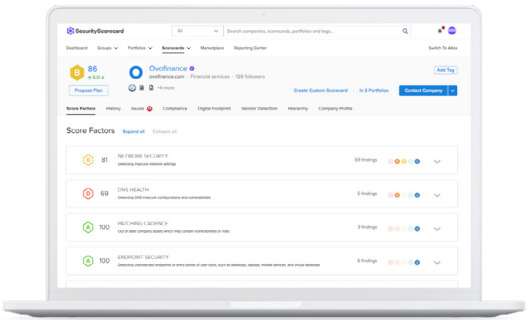
[4] The Cybersecurity Illusion. (2019, July). Ponemon Institute. https://go.attackiq.com/PR-2019-PONEMON-REPORT_LP.html

[5] Stats Report. (2022, March 7). Edgescan. https://www.edgescan.com/stats-report/

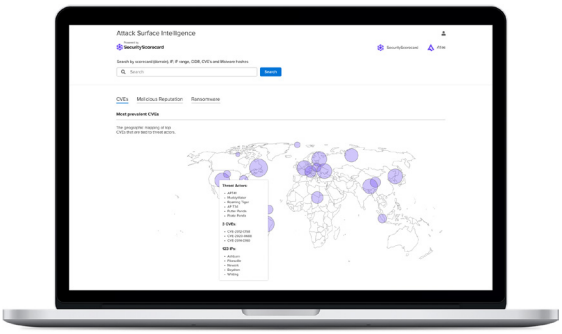
networks. The first step in any attack is reconnaissance. During this phase, malicious actors may scan networks looking for security vulnerabilities. For example, according to the 2022 Vulnerability Statistic Report[5], 20.4% of all vulnerabilities discovered in 2021 across an enterprise stack were either High or Critical. In order to mitigate supply chain attack risks, organizations need outside-in visibility for their third parties as well.

Organizations need to start with the outside-in visibility so that they can slow down attackers during this initial phase.

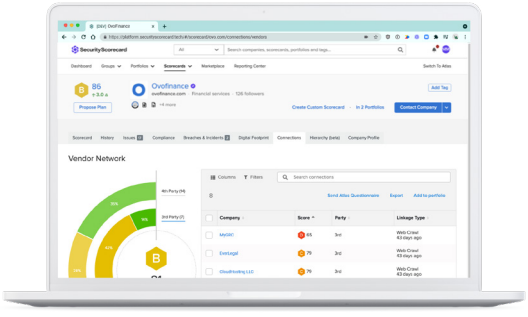
HOW SECURITYSCORECARD HELPS



SecurityScorecard's platform gives organizations the outside-in visibility they need to continuously monitor security controls. Our platform's external monitoring capabilities include:



- **Security Ratings:** Continuously monitor your security posture and that of your vendors with easy-to-understand, transparent security ratings. Tens of thousands of organizations leverage security ratings to communicate and collaborate on security risk for their own organization, with their third- and fourth-party vendors, to report to the board, and much more.



- **Attack Surface Intelligence (ASI):** ASI is the first platform to automate and integrate attack surface management, threat intelligence, and attribution intelligence into one platform that is designed to detect your entire threat landscape with actionable threat information. We combine threat intelligence, IP scanning, domain attribution, third-party risk management, and CVE/malware trackers into a single console.

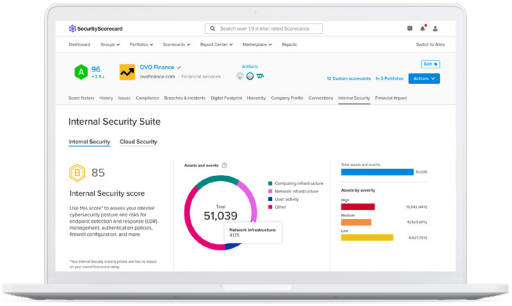
- **Automatic Vendor Detection (AVD):** Automatically visualize your entire third- and fourth-party supply chain. AVD leverages SecurityScorecard's continuous monitoring

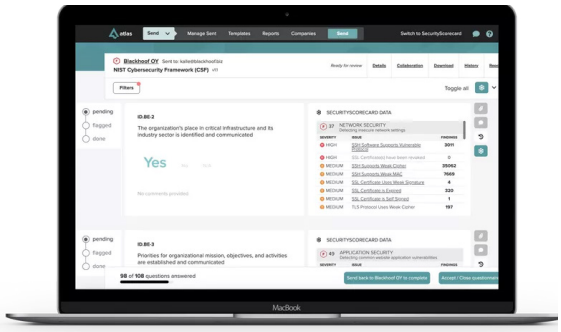
to detect your digital third parties and their vendors and consolidates it into a single Supply Chain Risk Score. Pinpoint supply chain risk and automate workflows to streamline your vendor risk management process.

- **Security Data:** Our proprietary scanners continuously scan over 12 billion IPs across more than 2,000 ports globally. Go beyond what you can access in the SecurityScorecard platform with our security data APIs so you can leverage and analyze security data within your daily workflows to build actionable insights.

INSIDE-OUT VIEW: QUANTIFYING AND COMMUNICATING YOUR INTERNAL RISK

Distributed workforces mean that users connect to cloud-based resources from anywhere, requiring organizations to have visbility into and control of devices, user access, and cloud security. With new compliance mandates focusing on zero trust architectures, they need to augment their external security monitoring with solutions that enable them to mitigate internal risks, like those arising from credential-based attacks or data leakage.



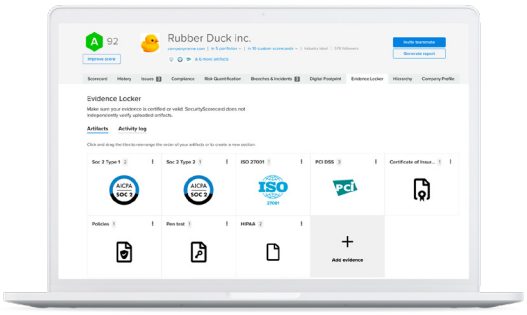


HOW SECURITYSCORECARD HELPS

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

- **Internal Security Suite (ISS):** Complement the outside-in view of risk by seamlessly integrating your internal security solutions to consolidate your internal risks. Quickly identify, prioritize, and effectively communicate their impact on your overall security posture.

- **Assessments:** SecurityScorecard Assessments enable you to cut through the questionnaire noise by empowering users to send, complete, and auto-validate questionnaires at scale. Leverage machine learning to

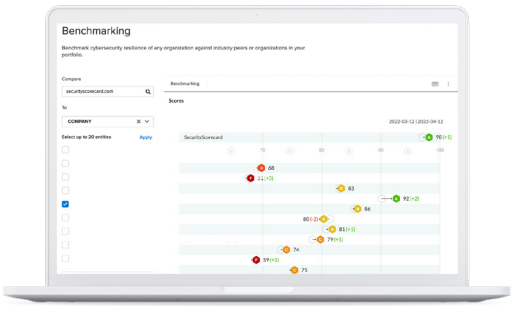


automatically respond to newly received questionnaires based on previous responses and to map security ratings data to individual questions, so you can trust and verify your vendors.

- **Evidence Locker:** Showcase your security posture on your Scorecard to build trust, accelerate the vendor onboarding process, and securely store your compliance attestations. Manage compliance artifacts, track artifact history, and monitor the compliance initiatives that your customers care about most.

CYBER RISK REPORTING: COMMUNICATE RISK MEANINGFULLY

With cyber risks becoming increasingly prevalent, boards of directors and executives need to evaluate those risks and become more involved with cybersecurity. Effectively reporting to the board is a key component of every security leader's job. In Gartner's 2022 Board of Directors survey, 69% of respondents said they view digital as the top business challenge for 2020 and 2021. Not only that, but 49% of directors cite the need to reduce legal, compliance, and reputation risk related to digital investments [6].

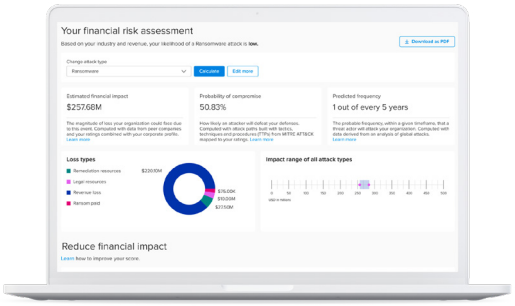


Having the right tools to automatically build reports and communicate risk will make it easier, faster, and more impactful.

HOW SECURITYSCORECARD HELPS

- **Reporting Center:** Show the impact of your security programs and secure more budget with the persona-based reports that give you the data you need. Choose from over ten reports that help you interpret

[6] 88% of boards now view cybersecurity as a business risk - from the 2022 survey https://www.gartner.com/en/articles/6-key-takeaways-from-the-gartner-board-of-directors-survey?source=BLD-200123&utm_medium=social&utm_source=bambu&utm_campaign=SM_GB_YOY_GTR_SOC_BU1_SM-BA-SWG-CONF



SecurityScorecard findings with prepared reports that are easily accessible and shared with stakeholders across the business.

- **Cyber Risk Quantification:** Demonstrate the impact of your security program by translating cyber risk into dollars, assisting you in a cost-benefit analysis of different cyber investment options.

PROFESSIONAL SERVICES: OPTIMIZING AND UP-LEVELING YOUR HOLISTIC SECURITY ORGANIZATION

Security teams struggle with staffing because the demand for security professionals continues to outpace the supply of experienced analysts. A holistic cyber resiliency program requires having the right people and resources for incident response.

At the same time, people can work from anywhere, often with their own devices, which increases the risk that a social engineering attack will be successful. A successful security program is a collective effort, meaning everyone - from security and IT to senior leadership and employees - need to collaborate effectively.

To mature their cybersecurity posture, organizations may need to augment their teams either through managed services, professional services, or training.

HOW SECURITYSCORECARD HELPS

SecurityScorecard offers more than a platform so that organizations can understand, mitigate, and communicate cybersecurity risk more effectively to internal and external stakeholders. SecurityScorecard's Cyber Risk and Resilience Services bring team augmentation to help customers achieve:

- **Digital Investigation, Forensics, and Incident Response:** Be ready to respond to any threat with a team of experts on hand. Integrate data forensics and incident response (DFIR) capabilities to augment your security team's capabilities with SecurityScorecard LIFARS on-demand.

- **Third-Party Risk Management Program Development:** Align people, processes, and technologies to mature your current third-party risk management program or build a new one. third-party risk management (TPRM) consulting services help bring visibility of the TPRM program to the organization by identifying how to mature the program and improve efficiencies while reducing risk.

- **Active Security Services:** Test and strengthen your organization's defenses with our suite of offensive security services, including penetration testing, tabletop exercise, and red team.

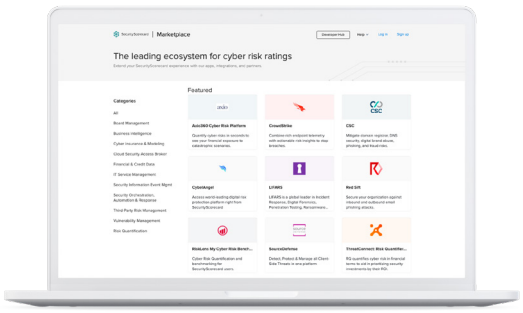
- **Cyber Risk Intelligence as a Service:** Get customized deep threat intelligence about emerging threats that are attacking or targeting your company, third-party vendors, and executives from our threat intelligence team. Sample questions answered include: Are we being attacked? Was the attack successful? Who is targeting my organization?

- **Academy:** Up-level 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.

MARKETPLACE OF INTEGRATIONS: ACT DECISIVELY

Leveraging security tools that speak to each other is key to driving a risk intelligence program. When evaluating security solutions, leaders should be thinking about building a tech stack that works together to drive decisive action through connected data flows. This will enable more efficient collaboration by integrating all business-critical applications across security, IT, compliance, and vendor risk management.

HOW SECURITYSCORECARD HELPS



- **Marketplace:** Integrate SecurityScorecard data into your tech stack to drive integrated workflows, mitigate risk faster, and augment security data through our ecosystem of 60+ integrations, apps, and digital risk intelligence data. SecurityScorecard's integrations extend the value of adjacent solutions by integrating security ratings into those tools. Save time through integrated workflows and creating a 360° view of risk.

• **Developer Hub:** Leverage SecurityScorecard data to power your organization's workflows leveraging our powerful APIs. Build custom integrations and apps using our easy-to-use developer guides in the Developer Hub and drive smarter workflows in your organization.

GO BEYOND RISK MANAGEMENT USING RISK INTELLIGENCE

SecurityScorecard continues to evolve its platform and capabilities to ensure customers can respond to shifts across the cybersecurity threat landscape. Security ratings - for external and internal risk - remain a valuable tool for ensuring cyber resiliency.

However, organizations need more than visibility. They need the data analytics that drives informed decision-making. Augmenting the SecurityScorecard platform with new capabilities provides customers with a 360° view of risk that can help them move beyond reactive risk management practices.

Attack Surface Intelligence (ASI) is the gateway to our rich data lake, scanning billions of data sources to provide deep threat intelligence and visibility into correlated attack surface risk data. This helps you identify all of your internet-connected assets, expose unknown threats, and prioritize remediation.

With **Automatic Vendor Detection (AVD**), organizations gain at-a-glance visibility into the overall health of their vendor ecosystem instead of focusing on individual vendor risk. Then, you can focus on the individual vendors impacting the overall risk score.

Internal Security Suite (ISS) enables organizations to aggregate and enrich the security data necessary for mitigating new threats associated with cloud technologies, like credential-based attacks. This provides you with a 360° view of your risk, a better understanding of your security posture, and the ability to make informed decisions about how to best protect your organization.

However, these proactive measures only tell one half of the cyber resiliency story. Many organizations also need to ensure that they have the appropriate people, processes, and technologies in place to help them mitigate a security incident's impact. SecurityScorecard now enables this post-incident resiliency through **digital forensics and incident response (DFIR)** and active security services. The suite of full cyber risk and resilience services help strengthen your organization's defenses to prevent an attack and respond right away with a team available to you 24/7.

These new products and services augment existing tools to provide the data analytics and support to effectively mitigate risk and respond to incidences for a holistic cyber resiliency program.

READY TO EVOLVE FROM RISK MANAGEMENT TO RISK INTELLIGENCE?

Request a demo today to try our capabilities for yourself. Learn more about how our holistic cyber risk and intelligence response platform enables you to drive your security program forward and establish a culture of risk intelligence.

SecurityScorecard
The Power of Knowing

SecurityScorecard.com
info@securityscorecard.com

Tower 49 12 E 49th St Suite 15-001
New York, NY 10017
United States: (800) 682-1701
International: +1 (646) 809-2166