5 WAYS

To Secure Your Organization In Turbulent Times

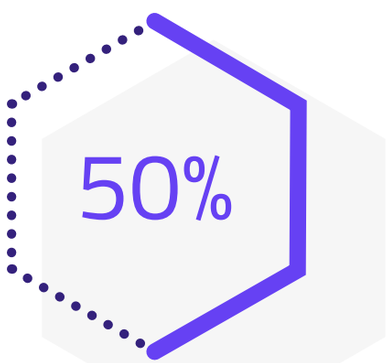
SecurityScorecard

Table of Contents

With this focus, security teams can **reduce risk** by up to

87%

Introduction



Around 50% of the risk companies face come by way of having multiple security vendors.

Source: Cisco

In times of economic uncertainty, improving your organization's security posture increases trust and enables business growth with both partners and customers. In addition, having the right security in place can greatly minimize the risk of a cyberattack and its associated expenses.

Even with these benefits to the bottom line, security spending is not immune from tough scrutiny. Any expenditure that does not show a clear Return on Investment (ROI) can be threatened. IT and security professionals need to understand what technologies and tactics are delivering value and which are just adding to the noise of alerts and warnings. SecurityScorecard is here to be your co-pilot and guide you through turbulent times. If you're reading this ebook, you're already taking the first step to preparing your organization!

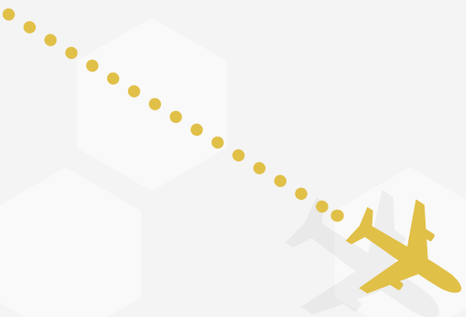
In this ebook, we will show you five key areas that every organization must prioritize now:

1. **Optimize and automate business ecosystem risk management**
2. **Consolidate and integrate vendor risk data into your existing security stack**
3. **Set Key Performance Indicators (KPIs), track ROI, and communicate clearly to stakeholders**
4. **Ruthlessly prioritize to keep your organization secure**
5. **Make your organization the vendor of choice**

With this focus, security teams can **reduce risk by up to 87%** while streamlining workflows and communicating metrics to stakeholders in a meaningful way — all while ensuring that security investments deliver value.

Quiz

This short quiz will give you a baseline of where your organization is in terms of understanding security investments and being able to justify security spend. Answer the multiple choice questions below.



1. My security team's daily operations have streamlined processes and are efficient, allowing us to maximize our resources.
   a. Agree
   b. Disagree

2. When a security issue arises, my security team receives an automatic alert and we are able to respond quickly.
   a. Agree
   b. Disagree

3. How would you describe your IT and security team's ability to pivot in response to changing business needs?
   a. Whether it's onboarding a new vendor or supporting a business technology initiative, we're in lock-step with corporate needs.
   b. My team struggles at times to keep up with the pace of procurement and digitization.
   c. My team is overwhelmed as we are not digital-first.

4. How has the complexity of your vendor ecosystem changed over the past two years?
   a. It hasn't changed.
   b. It has become more complex to manage.
   c. It has been a struggle to get a handle on who comes in contact with our data.

5. My organization monitors vendor risk...
   a. Continuously using a cybersecurity ratings platform.
   b. By conducting point-in-time vendor risk assessments.
   c. By hoping for the best.

6. How is your organization conducting remote vendor assessments?
   a. We invite our vendors into a cybersecurity questionnaire management platform which allows us to conduct assessments and validation off-premises.
   b. We manually exchange spreadsheets and questionnaires via email.
   c. My organization is not conducting remote vendor assessments.

7. My security team is getting the most value out of our security spending by using solutions that integrate well with each other.
   a. Agree
   b. Disagree
   c. Don't know

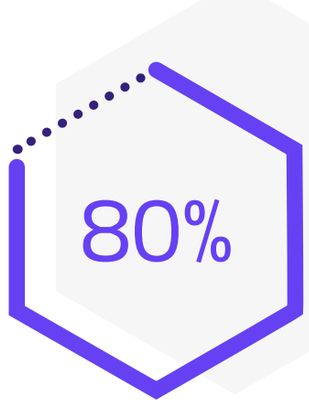
8. When reporting to the Board of Directors...
   a. I'm able to demonstrate ROI on cybersecurity spending with quantifiable data and KPIs that are understandable to executives with or without technical expertise.
   b. It's difficult at times to demonstrate the need for spending on cybersecurity initiatives.

If you answered A to any of these questions, you are doing great in those areas!

If you answered B or C to any of these questions, this guide will help you get the most out of your organization's security, IT, and business ecosystem risk management (also known as third party risk management) program, so you can remain nimble and resilient in an uncertain environment.

FOCUS #1

Optimize and automate your business ecosystem risk management program



of legal and compliance leaders say that third-party risks were identified after initial onboarding and due diligence.

Source: Gartner

Your organization might have all of its cybersecurity ducks in a row, but you still face substantial risk if you rely on a vendor with security gaps. Your security posture is never just your security posture. A combination of yours, your vendors', and their vendors' make up the ecosystem of organizational risk.

Business ecosystem risk management (often referred to as third-party risk management) not only means threat actors getting into your system via third- or fourth-party connections; it also encompasses the impact that a third party system can have on how your business functions. In December 2021, Kronos, a workforce management organization that services over 40 million people in over 100 countries, was compromised by a ransomware attack. This attack meant that customers could not use the Kronos solution and as a result organizations failed to meet payroll, potentially being in violation of local laws and facing a fine. This one example shows how critical it is to accurately assess vendors' security postures and risks to protect your organization.

Building a scalable and sustainable business ecosystem risk program includes the following:

Identify Your Vendors

You must know who all your vendors are before you can perform a risk analysis. Since the number of third and fourth-party vendors can be significant, investing in a vendor detection system can speed up the process and give you a 360-degree view of your digital supply chain risk, allowing you to move into analysis and action sooner.

Analyze Risk for Each Vendor

Once discovered, all vendors' security posture needs to be assessed. Traditional questionnaires and self assessments are a good start, but they tend to provide only point-in-time snapshots. Implementing a rating software that can continuously monitor the security posture of your vendors will provide a more realistic view of risk.

Prioritize Vendors Based on Risk

Once you understand the risk associated with each vendor, you can categorize vendors based on their overall importance to your business and any potential threats they pose. This will help you address the most critical issues first or determine where a shift in vendor prioritization would be more beneficial.

Monitor Continuously

Just checking in with each vendor once a year is not enough. Technology, configurations, and the threat landscape are constantly evolving. Continuous monitoring of business ecosystem risk will alert you if something changes so you can act accordingly.

To be able to respond to market changes, it is critical to have a pulse on how things are working (or not working) at every moment. Implementing products that automate the continuous gathering of relevant security information will build the dashboard view that helps teams navigate change.

FOCUS #2

Consolidate and integrate vendor risk data into your existing security stack

The average security team uses 47+ different products yet only 39% of respondents said they are getting full value from their security investments.

Source: Helpnet Security

As budget pressure extends to the security team, a close look at security products should be part of the review of third- and fourth-party vendors. You should understand what products are in your stack, which are being used, and which may be sitting idle (and even forgotten), posing a huge security risk. In order to maximize investment in security products and minimize cyber risk, consider the following as you review your security stack.

Multiple Products for the Same Solution

As a result of quickly changing security needs and guidance, many organizations have redundant products. When prioritizing where to spend, evaluate which products get your organization the most functionality and which can be sunset.

Access to Actionable Data

A critical part of your security arsenal are products that identify security issues as they are discovered in the market. Products should be able to provide visibility into issues across any IP, domain, CVEs, ports, products, or threat actors to get ahead of them before they become a problem. With threats identified in near-real time, your team is able to prioritize appropriately and address them — whether it's opening an internal support ticket and resolving an issue, adding a comment to provide context to your Scorecard, or alerting a third party to the finding.

Integrating Data about Your Third Parties to Everything You Do

Your security posture is not just your own, it is also your vendors' that you rely on. In an inter-connected enterprise environment, it is more important than ever to incorporate the most up to date data about your vendors into your operations. Continuously monitoring the cybersecurity posture of your vendor ecosystem and gaining visibility into their security health across multiple products enables you to scale your vendor risk management and always have a clear view of your global attack surface.

Integration Between Products

Even in consolidating products, some new solutions will have to be added to the stack. Any product added must have a specific purpose that's not currently being fulfilled by another product. It must integrate with existing products for automated security workflows with your GRC, SIEM, ITSM, SOAR, CASB, and vulnerability management solutions in order to correlate data and take immediate action.

By streamlining the security stack and automating workflows, the noise and swivel chair activity that haunt the dreams of security professionals are greatly reduced. A focus on business ecosystem risk management ensures that decisions about security products are data-driven rather than reactionary, stemming future creep of the security stack.

FOCUS #3

Set KPIs, track ROI, and communicate clearly to your stakeholders

62%

of global organizations cannot claim that they are equipped to handle a cyber attack.

Source: IBM

With a full view of risk, both internally and from third-parties, you can measure progress in protecting against threats and minimizing risks. Proving the value and effectiveness, or even showing the ineffectiveness, of your cybersecurity efforts to date builds a strong case for further investment to meet the evolving threat landscape.

Striking a balance between meaningful metrics and efficient data gathering is critical, so you can get the information you need while keeping your team focused on their primary responsibilities.

Quantify Financial Risk

Model and test different scenarios and potential financial impact for your organization. Risk in the form of monetary values is the language of executives and the board. Once a threshold is set, you then have an at-a-glance view of the most critical issues that need to be addressed.

Effective Board Reporting

As boards put a lens on business ecosystem risk management, security and vendor risk management teams need ways to clearly and effectively report what's working and where they need help. The boards and C-suite are most interested in showing the value of security while measuring costs — as well as being assured that investments are happening in the right places. Automated systems can reduce the time it takes to issue reports from hours to seconds.

Metrics that Matter

More than just threat avoidance, business ecosystem monitoring impacts operations and the bottom line. An effective business ecosystem monitoring system with automated questionnaires can result in **83% less time onboarding new vendors and 83% less time on compliance validation.**

As regulations increase, this will help you get ahead of any potential vulnerabilities that could put you at risk for non-compliance.

83% less time onboarding new vendors

83% less time on compliance validation

FOCUS #4

Ruthlessly prioritize to keep your organization secure

Security organizations are scanning applications approximately three times a week — up from three times a year in 2010. **69% of businesses** find the cost of staying ahead of cyber criminals unsustainable.

Source: TechJury.net

Lack of data is not an issue for security professionals. Alert fatigue is a real problem with teams drowning in too much information, all of which appears on the surface to be "blinking red." IT teams should look at ways to quickly highlight the most critical threats to calm the noise and allow security professionals to quickly focus on areas that will make the biggest impact to securing the enterprise.

IMPROVE DATA UTILIZATION

Security and third-party risk management teams collect a lot of information across multiple sources, but are not sure how to best prioritize and utilize it. Ratings products help you detect your digital footprint to help get a sense of where threat actors can access your organization. With this information you can better classify the most critical areas in need of attention first.

DO MORE WITH LESS

Fully staffing security teams with qualified individuals will continue to be a challenge. Arming those who are on staff with a way to cut through the noise of alerts and prioritize remediation based on threat and risk is not only more effective; it also improves the morale of overworked security professionals.

Especially in lean times, having the right data to make decisions on spending—both time and money—allows you to spend time on the most pressing issues and justify spending on products that make a tangible difference. **This is key to improving security even as budgets decrease.**

STAY AHEAD OF BAD ACTORS

Savvy cyber criminals know that cuts will be made and they will be planning to exploit this. Ensure that your cyber toolkit includes intelligence on the latest threats and match those against your security architecture and plans.

GROUP VENDORS INTO PORTFOLIOS BASED ON RISK AND CRITICALITY TO YOUR BUSINESS

In addition to products, looking at business ecosystem risk and prioritizing assessments is also critical. By grouping vendors into portfolios, you can prioritize assessments. Those with access to customer data or intellectual property—or that face regulatory scrutiny—require more oversight.

FOCUS #5

Make your organization the vendor of choice

Every vendor, regardless of business focus, must see cybersecurity as a key offering. A organization can have the best tactical solution, but if their security posture is weak or their reputation is tarnished with a breach, customers will not trust them. Similarly, incumbent vendors can quickly disappear as organizations look to make cuts in tough times, starting with the vendors posing the greatest risk to the organization. Strengthening cybersecurity posture means strengthening market position.

For example, a major provider of mobile recording for the finance sector needed to prove their security posture since protecting customer data is crucial. The team had relied on point-in-time questionnaires to assess risk, but these provided limited visibility and uncertain recourse in the event of an incident. Instead, they implemented a continuous monitoring solution that gave visibility into the risks posed by third- and fourth-party vendors, ensuring cyberhealth and reducing the need for time-consuming yearly or bi-annually assessments. Their confidence in this data could then be communicated to customers, allowing them to tell potential and current customers that all of the digital assets and business communications going through their system are being continuously monitored.

Trust badges improve consumer confidence by 48%.

Source: Yieldify.com

Being able to show proof of your security claims and posture eases onboarding to new customers. Showing your security up front shortens the questionnaire process, getting deals to close quicker and your solution into customer environments faster.

Show off your positive security posture

Similar to how the Good Housekeeping Seal of Approval gave consumers confidence in a cleaning product, security ratings, badges, and seals work to engender confidence from enterprise IT buyers. According to a global telecom customer, a public rating gives them an "unfair advantage" over their competitors.

Embed cybersecurity into operations

Much like security should be an offering of every organization, maintaining security should be a responsibility within every department. Solutions that provide a granular, dashboard view into systems that matter to each operational team empower non-security teams to track vulnerabilities within their systems – spreading security responsibility and management across the organization.

Securely showcase your certifications

Highlight your industry certifications and compliance badges in a secure repository. With a single source of truth, sharing and validating your organization's security posture simplifies the vendor risk assessment process.

Security deserves—and needs—a seat at the executive table now more than ever. Security promises are just as important as other operational promises that product and service teams are focused on. The right data showing security posture, application stability, and more prove that good security equals good business.

Security is a critical enabler of business success.

Focusing on business ecosystem risk management at scale, consolidating security products that work, and enabling effective reporting can make your offerings both secure and attractive to customers.

Think of the focus areas defined in this book as your safety instructions:

1.
Optimize and automate business ecosystem risk management

2.
Consolidate and integrate vendor risk data into your existing security stack

3.
Set KPIs, track ROI, and communicate clearly to your stakeholders

4.
Ruthlessly prioritize to keep your organization secure

5.
Make your organization the vendor of choice

If you implement products and processes to carry out these tactics, you will be ready for any turbulence you face.

Confidently navigate risk with SecurityScorecard as your trusted co-pilot

SecurityScorecard is proud to support over 30,000 organizations providing a platform to integrate and leverage security data and present it in a way that can be understood and acted upon by security teams, non-technical audiences, and the board alike. SecurityScorecard's platform expands its offerings beyond traditional security ratings capabilities so that organizations can gain needed insights to help mitigate these new risks.

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 (CRQ)

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

Attack Surface Intelligence (ASI)

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. ASI 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 (AVD)

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. AVD instantly gives you a view of your entire business ecosystem, enabling you to visualize and take active steps to mitigate risk.

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 60+ integrations, apps, and digital risk intelligence data.

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.

SecurityScorecard 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. We give your team the products to fill knowledge gaps and gain the skills they need to take control of your organization's cybersecurity.

SERVICES

Additionally, SecurityScorecard has a team of seasoned threat intelligence and incident response experts **available 24/7** to deliver proactive and reactive services to strengthen your security posture and cyber resilience. Our services include:

Third-Party Risk Management Program Development

Build and optimize your Third-Party Risk Management program by partnering with our subject matter experts to reduce your overall risk across your entire vendor ecosystem. We'll partner with you to align people, processes, and technologies to mature your current business ecosystem risk management program or build a new one.

Active Security Services

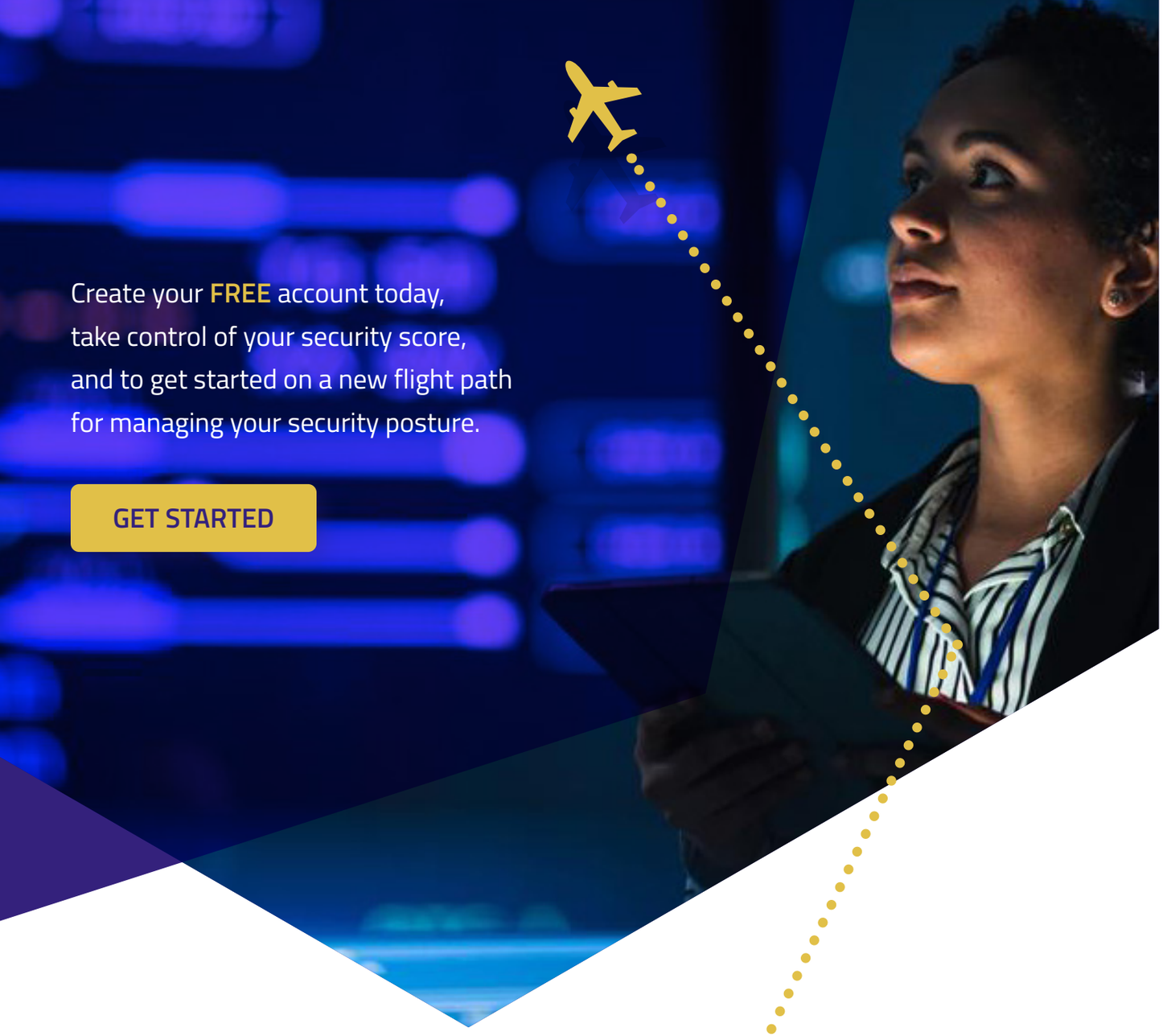
Is your organization's incident response plan up to date? How easy is it to get into your organization? Answer these questions, and more, with our active security services that test and strengthen your organization's defenses with penetration testing, tabletop exercises, and red team.

Cyber Risk Intelligence

Get customized deep threat intelligence about emerging threats that are attacking or targeting your organization, third-party vendors, and executives from SecurityScorecard's threat intelligence team. We partner with security teams identify the cyber threats that require immediate attention by sorting through the volumes of information and identifying where and how to prioritize security resources.

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 on demand.



Create your **FREE** account today, take control of your security score, and to get started on a new flight path for managing your security posture.

GET STARTED

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 30,000 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**.

SecurityScorecard
The Power of Knowing

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1701
International: +1(646) 809-2166