Security Scorecard

BUYER'S GUIDE

Managed Services for Supply Chain Detection and Response

How to choose the right solution to secure your supply chain.

Table of Contents

Introduction

The Evolving Threat Landscape

AI isn't what's going to be the hot topic of the next year; it's going to be data breaches in the supply chain and the cost that companies face by not reacting quickly to this emerging threat.

The cyber attack on Change Healthcare, one of the world's largest health payment processing companies, illustrates this point. Change Healthcare was a clearing house for 15 billion medical claims annually—accounting for nearly 40% of all claims. A cyberattack knocked the company offline, resulting in a backlog of unpaid claims that left doctors' offices and hospitals with serious cash flow problems—threatening patients' access to care.

Rising geopolitical tensions spotlight cyber risk, as threat actors operate globally and are often supported by nation-states that understand the vulnerability of critical infrastructure and opportunities to disrupt it. Furthermore, a report by SecurityScorecard found an extreme concentration of cyber risk in just 15 major vendors, creating a single point of failure for countless businesses.

The time for action is now. A managed service for Supply Chain Detection and Response (SCDR) is the solution to identify and respond to these growing threats proactively.

The Current State of Supply Chain Cyber Risk Management

Supply chain or third-party risk management is a process and set of practices organizations use to identify, assess, and mitigate the risks associated with third-party vendors, suppliers, contractors, and other external entities that have access to or impact the organization's data, systems, and operations. TPRM is crucial because third parties can introduce significant organizational risks, including data breaches, compliance violations, operational disruptions, and reputational damage.

Supply chain risk management covers many risk areas, including cyber, financial, and ESG. Industry research has increasingly indicated that most TPRM professionals may underestimate or underinvest in the cyber pillar of supply chain risk management.

98%

of companies have a relationship with a third party that has been breached

SecurityScorecard

29%

of breaches have third-party attack vectors

SecurityScorecard

75%

of companies say their third-party risk program is still manual

Forrester

The cyber blind spot within most TPRM programs is real and driven by these factors:

Increasing size of supply chain dependencies

The proliferation and specialization of software tools, direct marketing to users, and the search for cutting-edge technologies have helped skyrocket the number of vendors that typical organizations depend on. It's no surprise that IT and security teams aren't 100% aware of the makeup of their vendor ecosystem. The growth in an organization's supply chain necessitates growth in the responsibilities of a TPRM program.

Exclusive reliance on single-point-in-time assessments

Typical TPRM programs are built around questionnaires sent to vendors to understand vendor security policies, practices, and controls. These questionnaires can't capture necessary nuances or maintain visibility of active threats and emerging vulnerabilities. As a result, the evidence provided in questionnaires can quickly become obsolete, and 100% reliance on them can foster a false sense of security.

Limited TPRM resources and capacity

Budgets under stress and staffing shortages force many TPRM programs to focus on a relatively small number of critical vendors if any at all. Yet organizations also have a long tail of vendors who provide more minor services that are ignored but can create meaningful attack vectors for threat actors. This issue is compounded in maturing TPRM programs that rely on labor-intensive spreadsheet management and other manual risk assessment processes.

Lack of cybersecurity expertise

TPRM programs tend to be driven by risk management professionals with skill sets better suited to manage financial, operational, compliance, strategic, and reputational risks. They work with IT or security professionals when in-depth assessments are required. Given the dynamic nature of cyber risk, the need for more expertise and dependence on security professionals can delay risk mitigation of active threats.

What is a Managed Service for Supply Chain Detection and Response?

As discussed before, teams in the Vendor Risk and traditional TPRM space aren't calibrated for the cyber risks they are now facing, and they find themselves unable to keep pace with breaches, CVEs, assessments, and more. A team to respond to dynamic cyber risks can be built, but that takes time and more money. That is where a managed service for SCDR comes in.

Managed services for SCDR are technology-enabled services that prevent third-party breaches. This type of service leverages artificial intelligence, risk and threat telemetry, and elite cybersecurity experts to improve an organization's supply chain cybersecurity posture.

Managed services for SCDR have three capability pillars, all delivered by a Vendor Risk Operation Center (VROC). A VROC comprises professionals with experience in cybersecurity investigations across government and private sectors and expertise in digital forensics, incident response, threat hunting, and third-party risk management.

Incident likelihood assessments

Snapshots of a vendor's security posture are needed during onboarding, renewal, and periodically in between. Incident likelihood assessments offer a quick perspective on a vendor's exposure to issues that can lead to a breach. Bringing incident response expertise to third-party risk management questionnaires ensures that the evidence collected is the most effective at mitigating the impact of supply chain incidents.

Continuous risk monitoring

Periodic incident likelihood assessments are complemented with real-time analysis of the threat landscape and the security posture of supply chains. This proactive approach helps protect the organization's cybersecurity against evolving threats and maintain regulatory compliance. Managed services for SCDR maintain pace with dynamic cyber risks by leveraging accurate and scalable data collection methods.

Supply chain engagement and remediation

With insights about a vendor's real-time cyber risk exposure, the managed services for SCDR ensure that issues are remediated. This involves engaging with vendors to help them meet security standards and mitigate the impact of incidents in the supply chain. By sharing threat intelligence and collaborating on security improvements with vendors, organizations can enhance the overall security posture of the supply chain.

What isn't a Managed Service for Supply Chain Detection and Response?

As discussed, managed services for SCDR offer multiple value propositions. Given the pace of innovation and investment in the security industry, other solutions may provide overlapping capabilities, but none of them constitute a complete solution.

Managed security services

Like managed services for SCDR, managed security services offer outsourced security program management. The difference is in their scope. Managed security services focus on protecting internal assets and remediating issues within the customer organization, while managed services for SCDR focus on remediating an organization's attack surface, which includes its own digital footprint and that of its third-party ecosystem.

Managed questionnaire services

Specialized firms can handle the creation, distribution, collection, and analysis of risk assessment questionnaires sent to third-party vendors. However, these only gather evidence using questionnaires. Managed services for SCDR go beyond these services since they review attack surface data that can't be captured in questionnaires and work directly with vendors to explain findings and drive remediation.

Technology onboarding services

Managed services for SCDR are built on a technology platform, and other vendors offer similar technology platforms. These vendors also have services designed to accelerate the platform deployment, but once deployment is complete, the customer is fully responsible for managing the platform's use. Unlike technology onboarding services, managed services for SCDR can also configure technology for deployment and fully administer the platform on the customer's behalf.

Evaluating Your Supply Chain Security Needs

Understanding Your Vendors

Strengthening your supply chain security starts with a clear understanding of your vulnerabilities. Evaluating your supply chain security needs involves pinpointing critical points where a breach could cause significant disruption. This could be identifying vendors with access to sensitive data or those managing crucial infrastructure. Once you understand your weak spots, getting to know your vendors better is essential. Assessing their security practices, data handling procedures, and incident response plans helps identify potential risks they may introduce. By prioritizing vendors based on their role and security maturity, you can focus resources on shoring up vulnerabilities and building a more resilient supply chain.

Critical Questions for Vendor Security

Here are some key questions to ask your vendors to gain a deeper understanding of their security practices:

Data Security:

- How do you secure sensitive data (customer information, intellectual property) at rest and in transit? (Encryption standards?)
- What access controls do you have to restrict access to sensitive data? (Least privilege principle?)

Security Practices:

- Do you have a documented security policy outlining your data protection and incident response approach?
- Do you regularly conduct security assessments and penetration testing of your systems?
- How do you update your software and systems with the latest security patches?

Incident Response:

- Do you have a documented incident response plan?
- How will you notify us of a security breach involving our data?
- What steps will you take to contain and remediate a security incident?

Vendor Management:

- Do you have security requirements for your third-party vendors?
- How do you ensure the security of your supply chain?

Visibility into Your Supply Chain Risk

Achieving robust supply chain security hinges on clear visibility into the potential risks lurking within your network. Imagine a complex map – without a complete picture, blind spots can harbor vulnerabilities. Evaluating your supply chain security needs requires gaining visibility into your entire chain, from raw material suppliers to final product distributors. This includes understanding every vendor, subcontractor, and logistics partner's security practices. You can pinpoint potential weaknesses by mapping your supply chain and assessing each player's security posture. This newfound visibility allows you to prioritize vendors based on risk and allocate resources to fortify the most vulnerable areas. With a clear view of your supply chain landscape, you can proactively address risks and build a more secure and resilient network.

Core Capabilities Of A Managed Service for Supply Chain Detection and Response

What to Expect

INCIDENT LIKELIHOOD ASSESSMENTS

What to look for	Why it's needed
Non-intrusive and automated evidence collection from vendors	Vendors may not be available or willing to complete questionnaires
Use of incident likelihood model to identify the specific issues that drive risk	Perfect vendor security hygiene is not possible, and remediation should be focused on the most impactful issues
Prioritization of vendors by business impact and incident likelihood	There is no one-size-fits-all approach to TPRM, and the most critical vendors deserve the most attention
On-demand reports of any vendor's incident likelihood	Meet security and compliance requirements set by the business or risks management team

CONTINUOUS RISK MONITORING

What to look for	Why it's needed
Ability to monitor an organization's entire supply chain ecosystem at the same time	Security issues can emerge at any time for any vendor
Detection and alert security incidents within the supply chain	Meet regulatory or internal incident response requirements
Proactive discovery of unknown vendors within the organization's supply chain	Vendors can be adopted without consent from IT or security, which creates visibility gaps
Early warning and detection of exposure to zero-day vulnerabilities	Zero-day vulnerabilities can be exploited quickly, and immediate attention is required to remediate
Visibility of threat actor behavior across deep and dark web	Prevent incidents by identifying which vendors are being actively targeted

SUPPLY CHAIN ENGAGEMENT AND REMEDIATION

What to look for	Why it's needed
Vendor invitation and onboarding	Vendors need to understand their customer's security needs and the TPRM program's expectations
Expertise in discussing a vendor's specific cybersecurity posture and developing a remediation plan	The TPRM team or vendor team may not know how to solve security issues
Ability to engage directly with vendors to execute remediation plans	The TPRM team may not have the capacity to contact and meet with vendors
Capacity to respond to one security threat per vendor per day	Cyber risk has no constraints, and it's possible that a single systemic issue can impact an entire supply chain

VENDOR RISK OPERATION CENTER

What to look for	Why it's needed
Technology platform configuration	Every organization has unique requirements that need to be captured as rules and processes that govern a TPRM program
Technology platform administration	TPRM resources can be limited and are best utilized for strategic decision-making
Regular risk management reporting	Monitor the impact of risk management strategies and report performance to executives
On-demand customer dashboard	Access to the VROC team and visibility of their actions eliminates obstacles to collaboration
Dedicated advisory service team	TPRM programs require consistency and familiarity with customers to achieve results

How To Use A Managed Service for Supply Chain Detection and Response At Your Organization

Managed services for SCDR are ready to meet any organization where it is in its TPRM journey. Its flexibility allows organizations to choose precisely how to do this.

Ad-hoc or inexistent TPRM

For organizations without a formal TPRM program, a managed service for SCDR creates a foundation or the organization to begin taking action to secure its supply chain.
A TPRM program can quickly be established by leveraging well-defined best practices that have been proven to work in organizations of similar backgrounds.

Labor-intensive TPRM

At organizations where a TPRM program is built on manual processes and crushed under the weight of a growing number of vendors and assessments, a managed service for SCDR can create the efficiencies necessary to close security gaps and ensure compliance.
A TPRM program can gain the agility needed to tackle challenging new threats while maintaining a consistent operating model for managing known and ordinary risks.

Standardized and repeatable TPRM

Even organizations with smoothly operating TPRM programs are not immune to budget pressures and must prioritize limited resources. In these cases, a managed service for SCDR can be brought in to shift focus toward strategic risk management efforts while an independent team administers the TPRM aspects.

How To Measure Success

Metrics to Look At

Risk reduction can be challenging to measure since the goal is to prevent something bad from happening. If nothing bad happens, is it because of actions taken, or was it never going to happen? Despite this characteristic of risk, the performance of a managed service for SCDRcan be effectively measured through metrics proxies for risk reduction.

Number of vendors monitored

Describes the size and scope of the program.

Vendor response rate

Percentage of vendors who accept the TPRM program onboarding invitation.

High-risk vendor decrease rate

Percentage of vendors that move from high to low or medium risk.

Low-risk vendor increase rate

Percentage of vendors moving to low risk from high to medium.

Vendor patching compliance

Percentage of vendors who remediate issues after notification.

How to Prioritize Improvements

1. **Identify high-risk areas:** Analyze your supply chain to pinpoint areas most vulnerable to cyberattacks. This could include suppliers with weak security practices, critical infrastructure points, and systems handling sensitive data (e.g., intellectual property).
2. **Prioritize based on threats:** Evaluate the types of cyber threats most likely to target your supply chain. Consider common attacks like ransomware, phishing scams, and supply chain infiltration attempts. Focus improvements on addressing these specific threats.
3. **Scalability:** Ensure your managed service can scale to accommodate future growth and changes in your supply chain.
4. **Integration:** Consider how your managed service for SCDR integrates with other security tools and systems within your organization. Seamless integration helps streamline threat detection and response efforts.
5. **Regulatory Compliance:** Factor in relevant industry regulations or data privacy laws that may impact your requirements.

Ready to take supply chain cyber risk management to the MAX?

Learn more today at securityscorecard.com/max

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, 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 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io