Recorded Future®

The Security Team's Guide to Supply Chain Threats

Why preventative security isn't enough to protect your supply chain

Executive Summary

Third-party vendors are a critical component for today's modern business, helping them to streamline supply chains, accelerate product deliveries, spur innovation, increase efficiency, and lower costs. In fact, the average company shares confidential information with 583 parties, according to a recent Ponemon Institute study.[1]

But there is a cost to these relationships and achieving these benefits. Organizations must grant third parties access to information systems that support core functions such as product design, manufacturing, logistics, order fulfillment, and finance. While critical to continued success, every vendor introduces potential threats to your organization, with more than 80 percent of organizations reporting a third-party related breach in the past year.[2] The consequences of a breach range from reputational damage and reduced competitive advantage to legal consequences and financial impact. These third-party breaches can be devastating to an organization. Today, the average cost of a third-party data breach is $4.33 million.[3] The stakes are far too high to ignore third-party risk.

Despite the magnitude of risk supply chain partners pose to an organization, most enterprises make third-party risk (TPR) management a low priority. Programs typically focus on preventative measures, relying on static outputs like self-reported questionnaires for protection. But our world is not static — it is changing every day. Your third parties' attack surface evolves continuously as new infrastructure is spun up, all while threat actors continue to wage attacks. To stay ahead of ever-evolving threats in our business world, you need a threat-focused approach to TPR management that reflects the dynamic world in which we do business.

Third-party intelligence continuously monitors critical data sources for signs that your supply chain partners have been compromised (even before they realize it) or may be targeted for an attack in the near future. As soon as a threat is detected, you are sent a real-time alert so you can take immediate steps to mitigate your risk.

In this ebook, we will explore:

- Why it's critical for organizations to start treating supply chain threats as part of their core attack surface
- What a threat-focused approach to TPR management is, and why you need one
- How to develop a successful proactive TPR program
- Recorded Future's approach to TPR
- How customers are using intelligence to achieve better business outcomes

1 https://hyperproof.io/resource/cybersecurity-risk-management-process/

2 https://www.darkreading.com/operations/identity-related-breaches-last-12-months

3 https://www.ibm.com/reports/data-breach

Businesses Aren't Prioritizing Third-Party Risk Management

Businesses today rely on third parties more than ever before. These relationships yield tremendous benefits but also open significant risk exposures. Cybercriminals and hackers know this and target your partners as potential pathways into your organization. Yet, for many, managing third-party risk falls as a low priority which can lead to costly consequences.

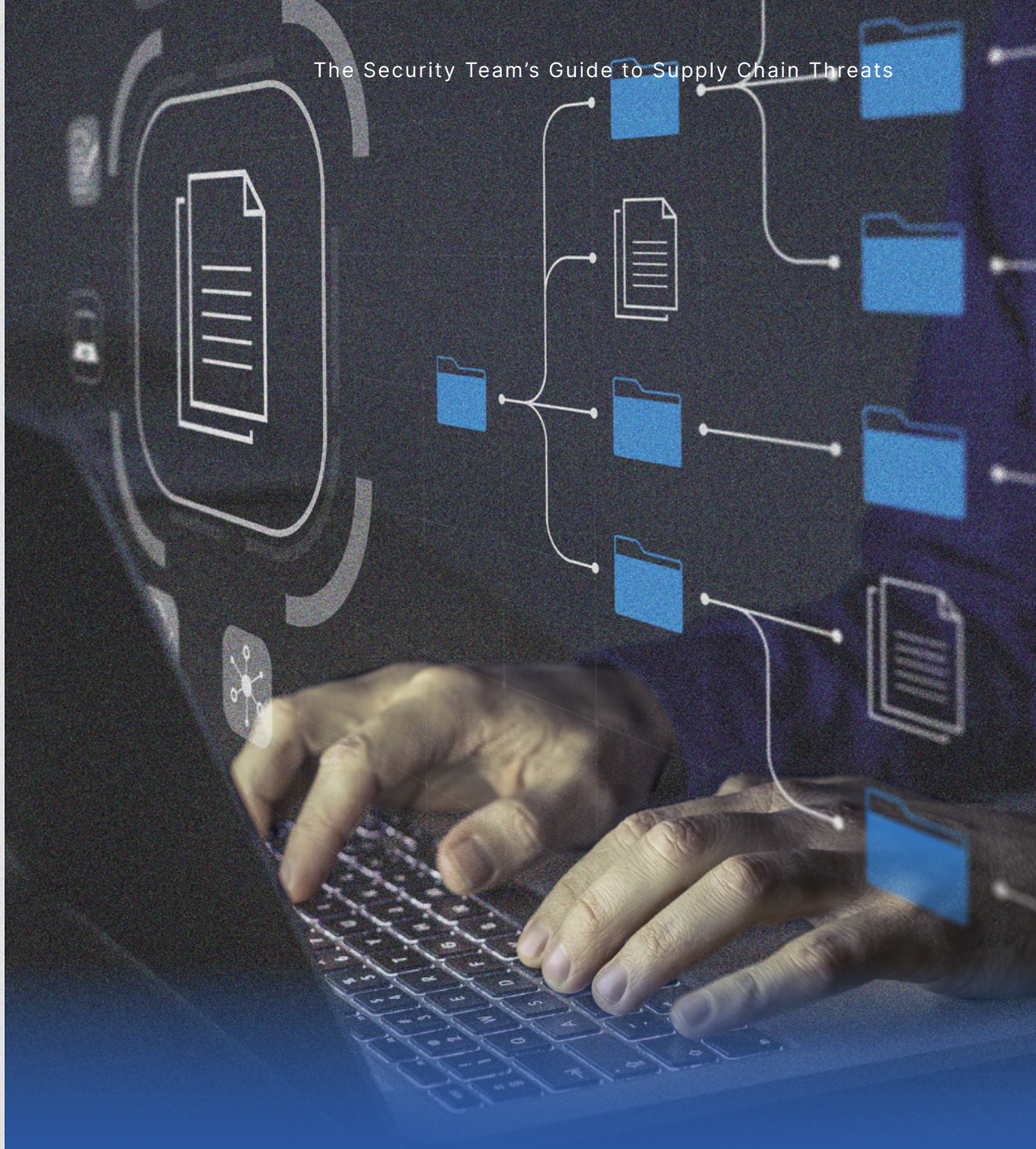
Third parties represent a massive part of your organization's attack surface, which is why security teams need to make monitoring for supply chain threats as high a priority as monitoring for first-party threats. Consider this: more than 80 percent of organizations have suffered a third-party related breach in the past year.[4] Statistically, your third parties will be breached; are you prepared for the fallout?

A threat actor who compromises one of your suppliers, contractors, service providers, or resellers has the potential to:

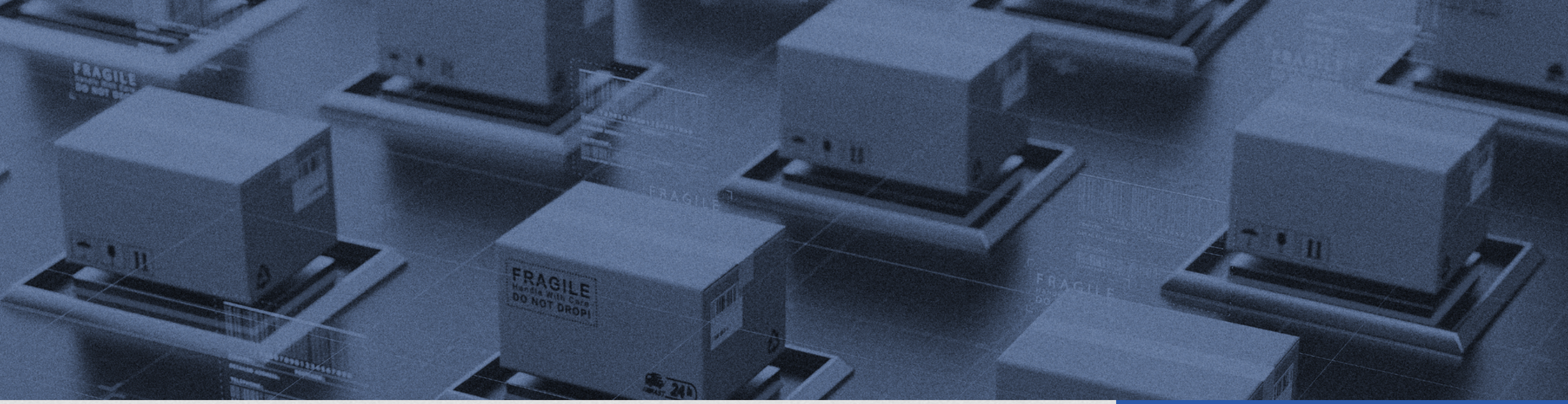
1. **Attack** your information systems using access or credentials acquired from the partner

2. **Steal** your sensitive information that resides on the partner's systems

3. **Disrupt** your business operations by shutting down the partner's operations



4 https://www.darkreading.com/operations/identity-related-breaches-last-12-months



Case in point, Kaseya, an information technology (IT) solutions developer for managed service providers (MSPs) and enterprise clients, announced that it had become the victim of a supply chain ransomware attack on July 2, 2021. The attackers leveraged a vulnerability in Kaseya's Virtual System Administrator (VSA) software against multiple MSPs — and their customers. Estimates suggest that 800 to 1500 small- to medium-sized companies were affected.

A physical supply chain risk can also impact your business. For example, the Russian-Ukraine war has severely impacted the global supply chain, "impeding the flow of goods, fueling dramatic cost increases and product shortages, and creating catastrophic food shortages around the world.[5]"

The reality is that most cyber and physical attacks currently in planning or execution are likely leaving cyber breadcrumbs that we can trace back to digital sources: be it through breach disclosure databases, the dark web, the criminal underground, news coverage, social media, or even compromised corporate networks. The key is to identify those breadcrumbs and make the necessary contextual connections before the attack occurs or soon after to mitigate the risk to your business.

5 https://mitsloan.mit.edu/ideas-made-to-matter/ripple-effects-russia-ukraine-war-test-global-economies

6 80% of Firms Suffered Identity-Related Breaches in Last 12 Months https://www.darkreading.com/operations/identity-related-breaches-last-12-months

MORE THAN

80%

of organizations have suffered a third-party related breach in the past year.[6]

Traditional Third-Party Risk Management Methods Are Broken

Traditional approaches to third-party risk management have value, but the problem is: they don't stop breaches. Why? Most programs are only preventative, relying on static outputs like self-assessments, financial audits, monthly reports about new vulnerabilities discovered in the systems an organization uses, and occasional reports on the status of security control compliance. These methods don't present a complete picture of an organization's security posture because they cannot reflect quickly changing conditions or report real-time insights; this traditional approach is unlikely to protect you from a third-party attack like the one Kaseya experienced.

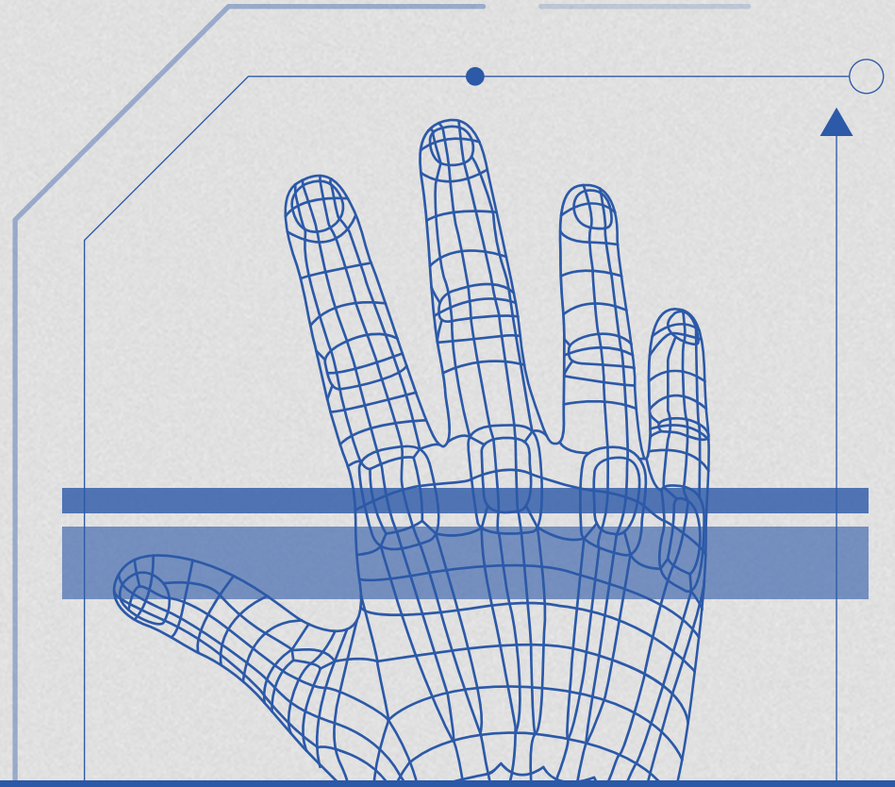
You Need a Threat-Focused Approach to TPR Management

Potential security threats are cropping up all the time. A security rating won't do you any good if you are breached. Even more critical, many partners lack the knowledge and resources to discover holes in their defenses. As long as they remain in ignorance, they jeopardize your security. Finally, as partners try to manage the potential fallout from a breach, some may choose to wait weeks, even years, to notify their customers about breaches. That delay could be devastating for your organization.

You don't have time to waste. You need the same level of real-time monitoring for your third-party relationships. Third-party intelligence provides critical risk indicators that enable you to spot shortcomings in your supply chain partners' defense and determine significant third-party risks to your organization.

To accurately evaluate supply chain threats, you need immediate context and visibility into the wider threat actor landscape and the ability to detect threats in real time that need to be acted on quickly. Third-party intelligence enables you to accurately assess the risk posed by those organizations and keep assessments current as conditions change and new threats emerge.

For example, if a French-language local news station reports that one of your key providers is hindered or shut down due to a cyberattack, you need to know about that as soon as possible. A third-party Intelligence solution should monitor for this information and notify you in real-time so you can take appropriate and immediate action to reduce your own risk.



Essential elements of a third-party intelligence solution

- Access to a diverse range of threat data from the open web, criminal underground, and technical sources
- Automation and analytics to distill massive amounts of data into actionable intelligence
- Transparent evidence for faster threat analysis and mitigation
- Real-time alerts on changes and newly emerging risks

Organizations need to continuously be monitoring their existing third-party vendors while also vetting new vendors.

How To Get Started in Developing a Proactive TPR Program

The following steps and questions will help you formulate a proactive TPR program that you can customize for your organization's needs.

1. Identify your key risks.

- These will be your priority intelligence requirements (PIRs).
- What kind of risks are you most concerned about? What risks could have the most significant impact on your business and your customers?

2. Identify your third parties.

- Who are your business partners, solution providers, vendor management software companies, and technical vendors?

3. Tier and tag the third-party vendors that could pose the most risk.

- You may have thousands of third-party vendors within your supply chain, but they don't all pose the same threat. Ask yourself, who has direct access to your network? How would a natural disaster or political unrest affect a key supplier?
- Do they have VPN or remote access? Can they access your intranet, shared files, digital access management (DAM), or other apps and systems?

4. Identify how intelligence can pinpoint and address gaps that need to be filled by information, technology, or people to make insights effective in closing these gaps.

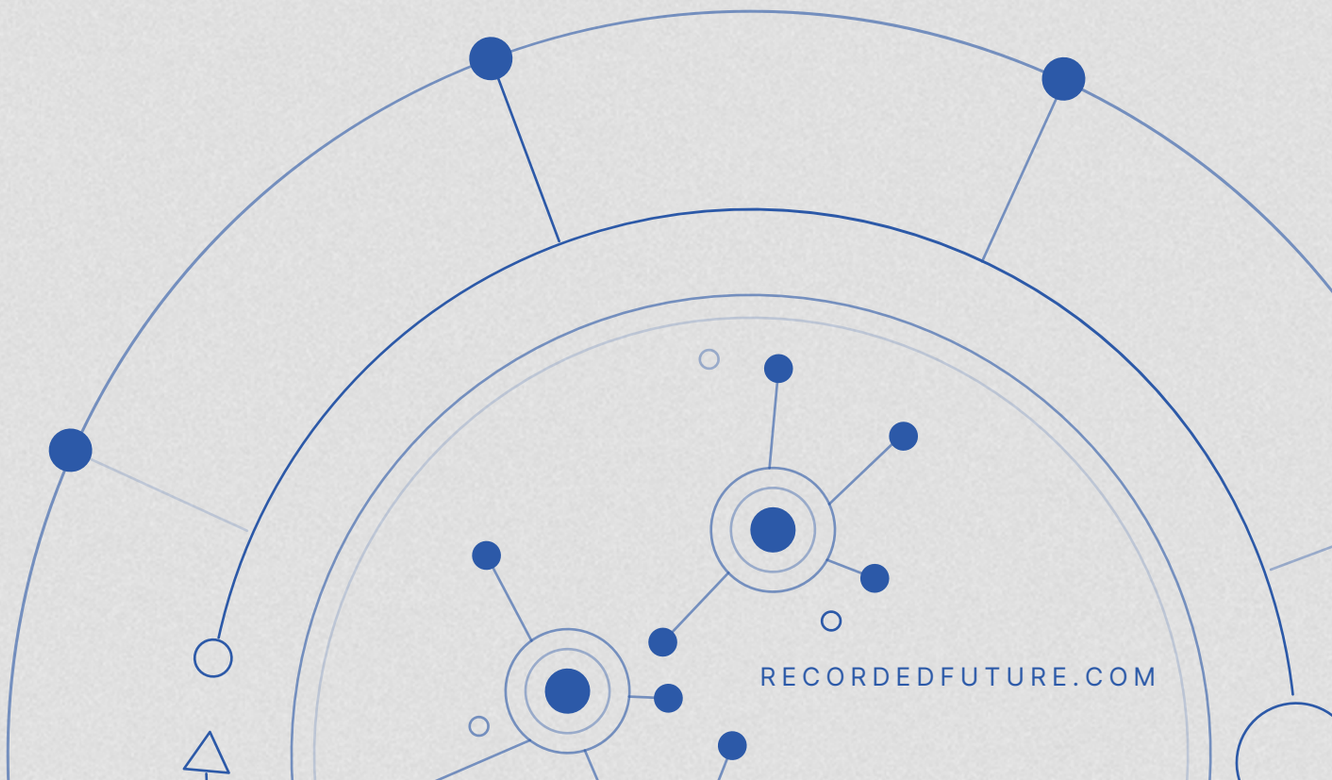
- How can intelligence address some of those risks? What information would you need to address those risks?

5. Identify who, aside from your own team, would benefit from access to intelligence on your third-party partners and vendors. Collaborate with them.

- Which teams can help react to real-time threats? Which teams are responsible for third-party relationships?

6. Establish how your team will collaborate with Governance, Risk, and Compliance (GRC).

- How can you align your intelligence collection and sharing with GRC priorities to help reduce risk?



How To Be Successful

Short of fending off an immediate supply chain attack, it's not easy to prove immediate value when building out a TPR program. Here are several ways to generate quick wins:

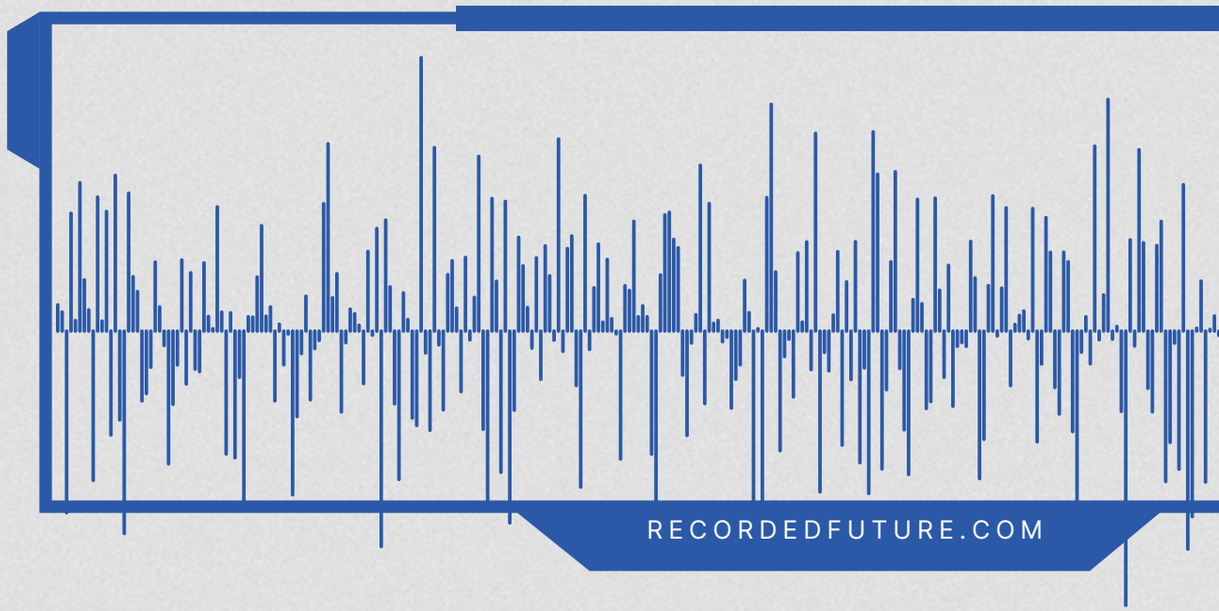
1. **Start with tier-1 vendors.** When first building your TPR program, it is best to start small and focused. Narrow your initial actions to tier-1 vendors. This allows you to identify more significant, impactful wins. It also enables you to test your investigation and response workflows.
2. **Expand your TPR program over time.** Once you have some wins with tier-1 vendors, it's time to expand to tier-2 and tier-3. Build up your process with an eye on scalability. For example, many organizations will monitor all possible threat types for their tier-1 vendors (for example, with systems access), and only worry about breaches for tier 3.
3. **Share intelligence with your third-party vendors.** Those leveraging intelligence (with visibility into third-party exposure, vulnerabilities, dark web plotting, etc.) can easily find a surprising number of breaches, exposures, and other supply chain threats. When your team uncovers gaps, risks, or attacks on one of your third-party partners, be sure to share that information with them quickly so they can take action, to protect you and others.
4. **Concentrate your monitoring on specific data types that prove value quickly.** While there is a countless number of data sources to monitor for threats to your third parties, it is best to start with high-value sources that look for:

Ransomware

If you monitor ransomware extortion websites, you will get early notice that the partner has been compromised. Speed of response is critical. If you can take action while the negotiations between the attacker and the victim are still going on, you may be able to harden your defenses before the attackers turn their attention to you.

Evidence of Data Breaches

Websites on the open internet and dark web can provide evidence that your partners have been compromised, even before they know it has happened. The information can turn up on dark web marketplaces, hacker forums, paste sites, and code repositories. Also, many breaches are disclosed on news sites on the open web and on social media.



Malicious Network Activity

Just like you monitor your own IT infrastructure, you also need to monitor the network traffic of your suppliers, contractors, service providers, and others who have access to your systems. Malicious network activity provides insight into planned and ongoing attacks on third parties.

Freshly Stolen Credentials

While a vast supply of stolen credentials is available to cybercriminals, your focus should be on freshly stolen credentials that are still valid. You want to monitor malware stealer logs, dark web forums, dark web marketplaces, criminal underground forums, paste sites, dump sites, and the many other places where stolen credentials are exposed.

Plotting on the Dark Web

If you monitor dark web forums, you can uncover plots against your partners (as well as your enterprise). Observing activity on these forums provides early warning of attacks and information about the tactics, techniques, and procedures that will be used.

Recorded Future Provides Real-time Intelligence To Detect Supply Chain Threats

Recorded Future's Intelligence gives you comprehensive visibility into the supply chain threat landscape so you can detect threats earlier. Our solution empowers security teams and business leaders to make fast, informed decisions about the companies in their supply chain and reduce the overall risk of business disruption, data breaches, and reputational damage.

Recorded Future eliminates the guesswork and hassle of traditional vendor risk assessment by providing deep visibility and real-time insights into suspicious activity and alerts on rapidly accelerating risk assessments. What makes Recorded Future different is our comprehensive visibility into threat actors, their infrastructure, and the attack surface of organizations, which allows us to see more than anyone else. Our platform uses patented machine learning and natural language processing to automatically collect and analyze information from more than one million technical, open web, and dark web sources.

How We Deliver

Continuous monitoring: Recorded Future continuously monitors your vendors to provide early warning of impending and ongoing attacks and risks, including ransomware extortion, data breaches, malicious network activity, exposed credentials, and cybercriminal chatter. We watch and analyze a variety of sources, including closed dark web forums, ransomware extortion sites, malware logs, network intelligence, data breach reporting databases, and local language news sites.

Detailed context and actionable recommendations: We go beyond finding problems — we provide detailed context on the incident and recommend appropriate actions for your organization so you and your team can respond quickly and protect your enterprise.

Threat profiles for faster risk assessment: Get insight into hundreds of thousands of third-party organizations. With Recorded Future, you can rapidly assess the cybersecurity risk of new vendors, streamline procurement, and negotiate (enforceable) security compliance standards into your purchasing agreements.

Finished intelligence: Recorded Future's threat research team Insikt Group® regularly publishes detailed human-finished intelligence reports on cyber and physical supply chain risks and incidents. This research goes the extra mile, providing in-depth analyses on significant events with actionable recommendations for mitigations so you can protect your organization.

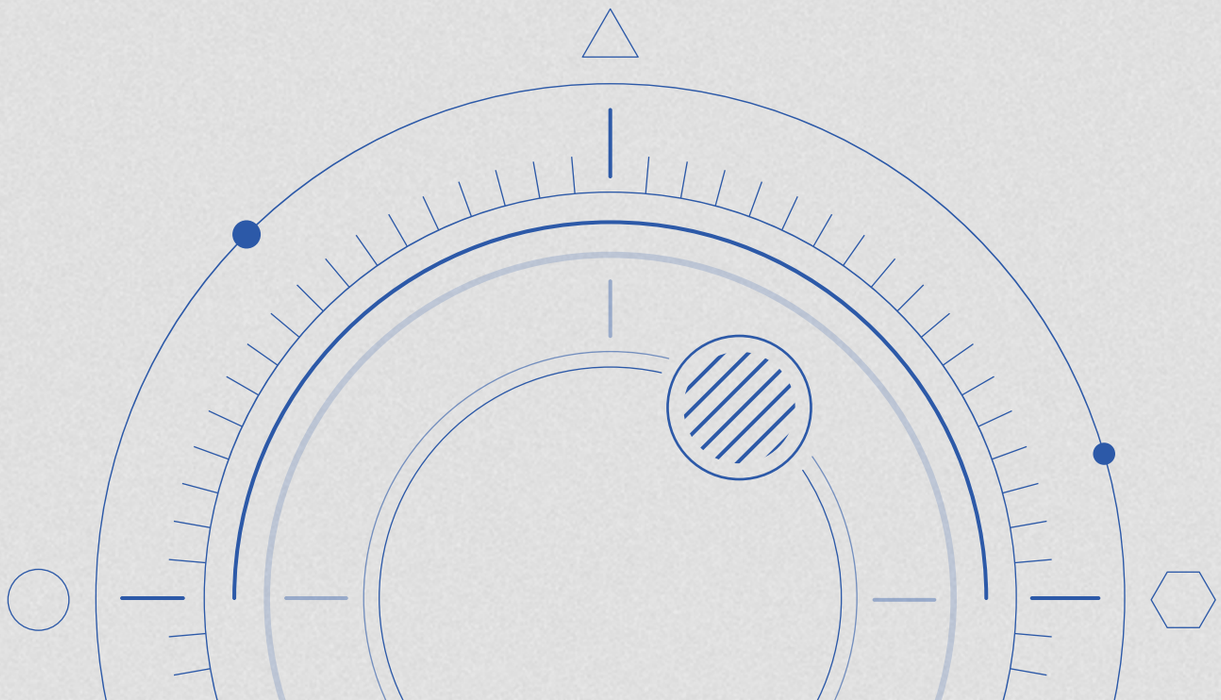
Business Outcomes With Recorded Future

Benefits

- Identify supply chain threats in real time
- Respond quickly with the detailed evidence and research required to act
- Assess vendor risk 50% faster with an external view of your third parties' threat landscape
- Align risk with the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Improve cross-team efficiency across security, risk, compliance, and legal

"Recorded Future has helped us better prioritize third-party risk information and incorporate that into our broader cyber threat intelligence perspective."

– Risk Management Lead, National Insurance Company



CASE STUDY:

Hughes Federal Credit Union

Over $1.9 billion in assets

CHALLENGES

- 70%+ of business is working with third-party vendors
- Rapid business growth but a small security team

RESULTS

- Automated, real-time alerts and insight into potential threats
- Reduces risk with faster reaction and remediation
- Pinpoints and notifies when vendors are compromised
- Decisions now based on quantifiable evidence

SEE THE FULL CASE STUDY

Conclusion

With continued investment in digital transformation and the adoption of cloud-based services, everyone's attack surface continues to grow, including your third-party vendors' ecosystem. Traditional third-party risk management methods cannot stop all breaches because they only provide you with a static and incomplete picture of your partners' security posture. While some of that static information can be useful in your overall periodic analysis of a partner, it won't alert you in real-time to immediate or impending threats.

You need to be better prepared. Your business requires a modern solution built for the digital age. Recorded Future Intelligence automatically monitors and programmatically analyzes hundreds of thousands of threat sources so you can detect supply chain threats early.

Recorded Future invests in skills and resources to draw information from sources across the internet, including websites, forums, and marketplaces on the open web and dark web, ransomware extortion sites, paste and dump sites, news sources, blogs, social media accounts, and threat intelligence databases. In addition, many important sites on the dark web are invitation-only, and it can take years of effort to develop personas that will be accepted by cybercriminal communities. Our staff of experts with extensive knowledge of cybercriminal and hacker communities, and fluency in languages, such as Russian, Chinese, and Arabic, can monitor corners of the web that few enterprises can ever find.

None of this is possible with a traditional third-party risk management solution. Data shows that it is just a matter of time before your third parties are breached. With access to real-time intelligence, you can quickly identify these attacks and take immediate action to protect your customers, employees, and business.

Want To Know More?

For more information, request a demo of Recorded Future Third-Party Intelligence or talk with your customer success representative.

Recorded Future®

About Recorded Future

Recorded Future is the world's largest intelligence company. Recorded Future's Intelligence Cloud provides complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,500 businesses and government organizations across more than 64 countries.

Learn more at recordedfuture.com.