SAFE ONE

Third-Party Cyber Risk Management (Cyber TPRM)

AUTOMATE, UNIFY, AND
RUN YOUR TPRM PROGRAM AT SCALE

SAFE Transforms the Cyber TPRM Game

SAFE TPRM is the industry's first AI-powered third-party risk management solution, equipping businesses with the benefits of outside-in security ratings, questionnaire-based assessments, zero-trust, and inside-out assessments. Using SAFE One's unified platform, enterprises can finally manage and mitigate their supply chain risk with confidence.

SAFE TPRM solution represents a major shift in how third-party cybersecurity risks are measured and managed. Unlike traditional methods, which provide a piecemeal view with static data, SAFE TPRM integrates diverse risk indicators into a single, clear perspective. This integration helps businesses not just see their entire third-party ecosystem but also actively manage and reduce risks in real time.

With SAFE TPRM, companies can proactively identify and address vulnerabilities and other security findings before they become critical threats. This means businesses can better protect themselves while also making smarter, more informed decisions by:

- Prioritizing Third Parties based on Risk
- Focusing on Critical Third-Party Controls
- Partnering with Third-Parties to Improve their Security Programs
- Managing Third-Party Risk Impact Using Zero Trust Controls
- Using a Fixed Pricing Model Independent of Number of Vendors
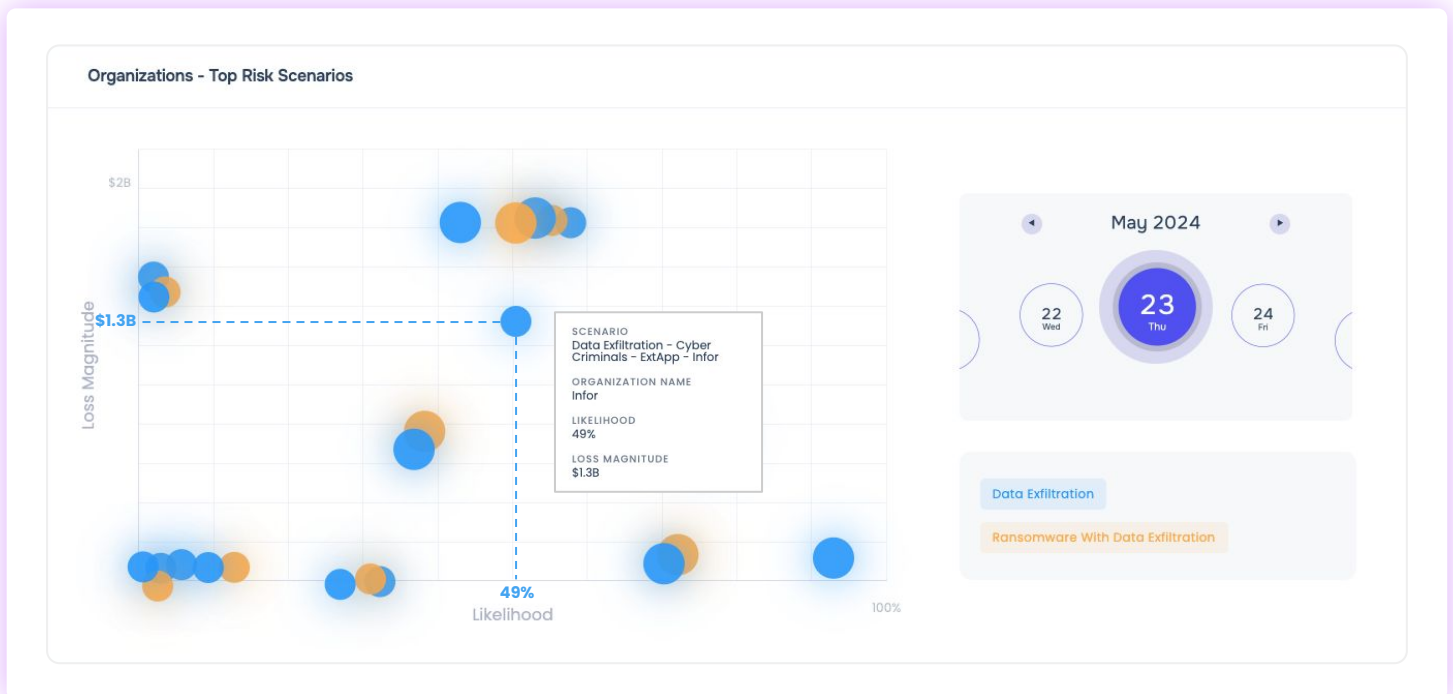
Solution Highlights

01 | Focus on Critical Third-party Controls

SAFE TPRM simplifies third-party risk management by focusing on the most critical controls, derived from extensive research of current and past third-party cyber attacks. This eliminates duplication of effort and the need for third parties to respond to hundreds of questions, shifting the focus from quantity to quality of control assessments. By consolidating data from outside-in scans, questionnaires, and inside-out assessments, SAFE TPRM effectively assesses all controls and creates a laser focused prioritized list of critical controls.

Evidence-Driven Verification: SAFE TPRM supports the collection of direct evidence such as phishing reports, secured software documentation, and vulnerability assessment reports. This evidence collection is integrated into the control assessment process, significantly increasing the reliability and validation of security controls. Third parties can directly upload evidence, which is then reflected in the SAFE platform's Evidence Tab for each organization, showcasing the current state and completeness of evidence.

Actionable Insights and Reduced Workload: The prioritization of critical controls and the integration of direct evidence substantially reduce the administrative burden on third parties and first parties. This efficient approach minimizes unnecessary tasks and focuses efforts on high-impact areas, enabling vendors to improve security measures while the enterprise gains a clearer, more accurate understanding of third-party risks.
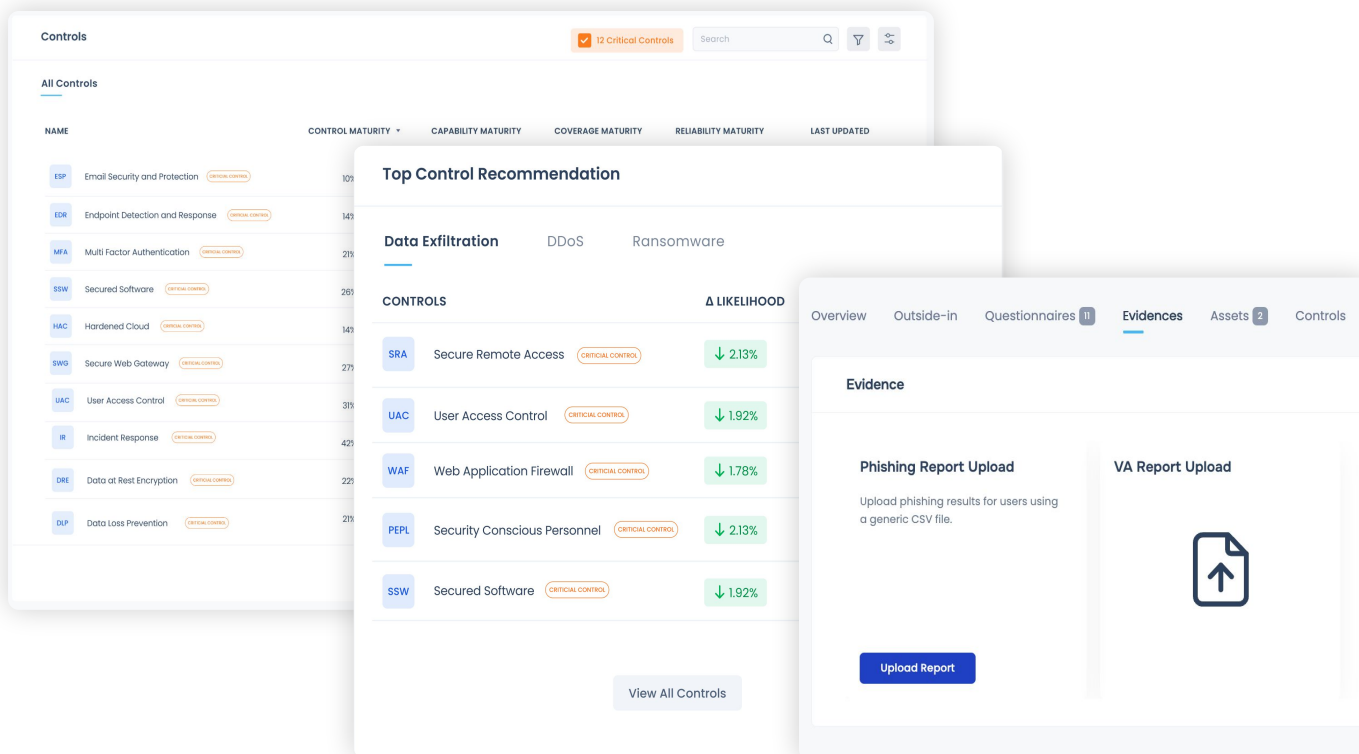
02 | Manage Third-Party Risk Impact Using Zero-Trust Controls

SAFE TPRM promotes using zero-trust principles to handle third-party interactions safely. By assuming that all third parties could be potentially compromised, it urges enterprises to prioritize strengthening their internal defenses. This approach is akin to securing one's own house in a rough neighborhood before acting on the broader area. Implementing strict resilience controls within your operations minimizes the risks to your business.

- **Navigate Risk Control Focus**: Shift from merely trying to reduce the likelihood of third-party breaches to strengthening controls within your own scope to minimize both likelihood and potential loss. This approach ensures you're not just reacting to threats but proactively managing them.

- **Third-Party Risk Exposure Likelihood Reduction**: Implement security gates within your organization that act as the first line of defense in protecting your network and data should a breach occur at a third party. Such controls could be multi-factor authentication, endpoint detection and response, etc.

- **Third-Party Risk Loss Magnitude Reduction:** Enhance your security monitoring capabilities to act as a layered defense. These capabilities are crucial in minimizing the impact of any security incident, ensuring that potential damages are contained. These include incident response and recovery, data backup, cyber insurance, etc.

By implementing a zero trust architecture towards third parties, CISOs can confidently answer a fundamental question: "Assuming all vendors are compromised, what are our resilience controls to minimize risk to the business and how effective are they?"
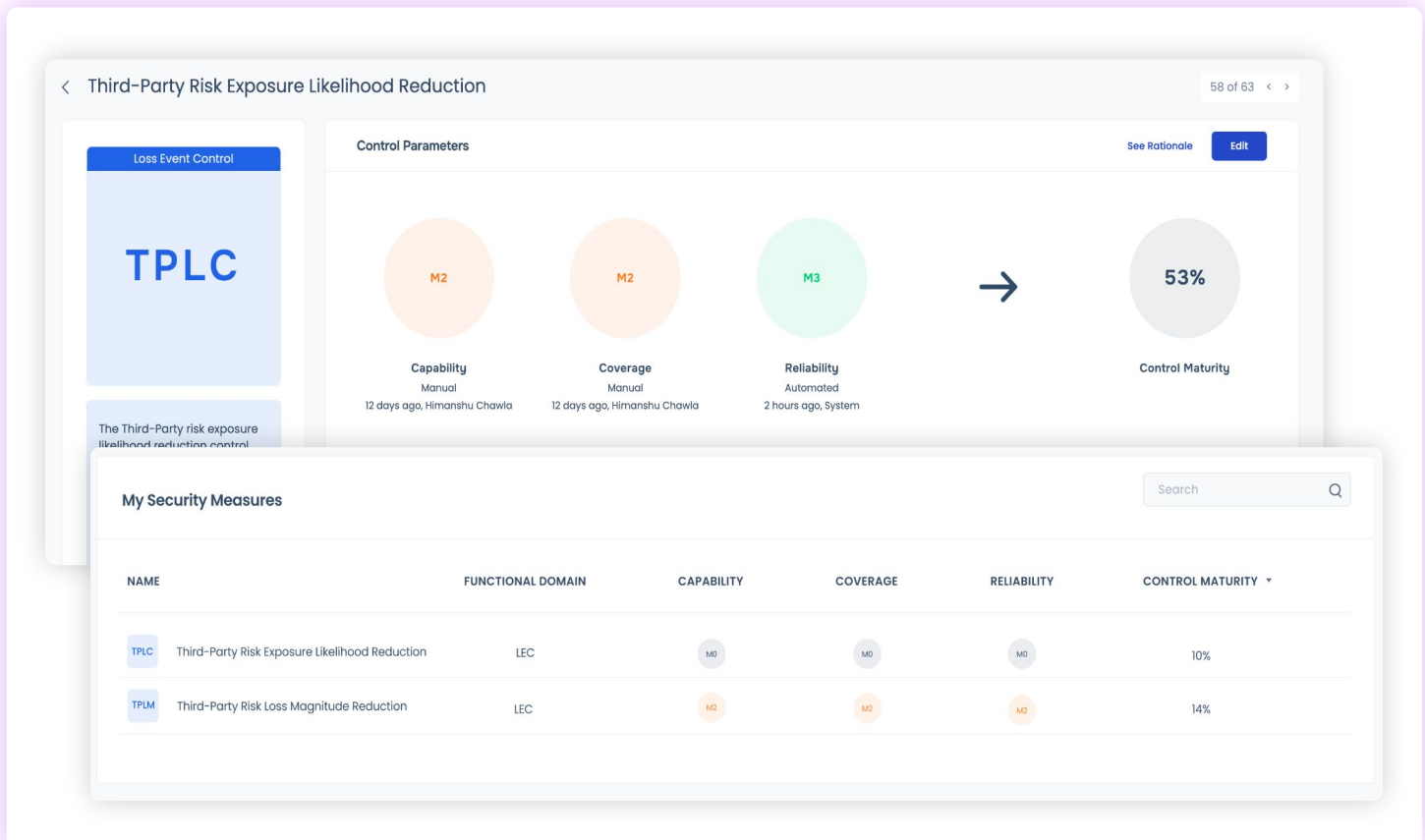
03 | Partner With Third Parties to Improve Their Security Programs

SAFE TPRM makes it simple, swift, and efficient to collaborate with your supply chain using AI-assisted training and onboarding modules. These modules provide 24x7 support to vendors who have a direct SAFE One platform access. They can leverage the platform to visualize their cyber risk exposure and effectively prioritize their critical controls to reduce risk. This unique partnership enables third parties to manage cyber risk more effectively with security profile visualization, self-assessments, and training materials, and shrinks your third-party risk assessment cycle from weeks to days,

Direct Access to Safe One Platform: Vendors can directly access the Safe One Platform via role-based access control. This direct access enables them to manage their security profiles, perform self-assessments, and access training materials directly, which encourages proactive management of their security in alignment with the standards expected by your organization.

Effortless Collaboration: Creates an environment that makes it easy for third parties to engage and share information. Utilizing user-friendly platforms and clear communication channels simplifies interactions and enhances cooperative efforts towards better security practices.

AI-Driven Automation: Automates routine tasks, allowing you and your vendors to focus on critical security issues.
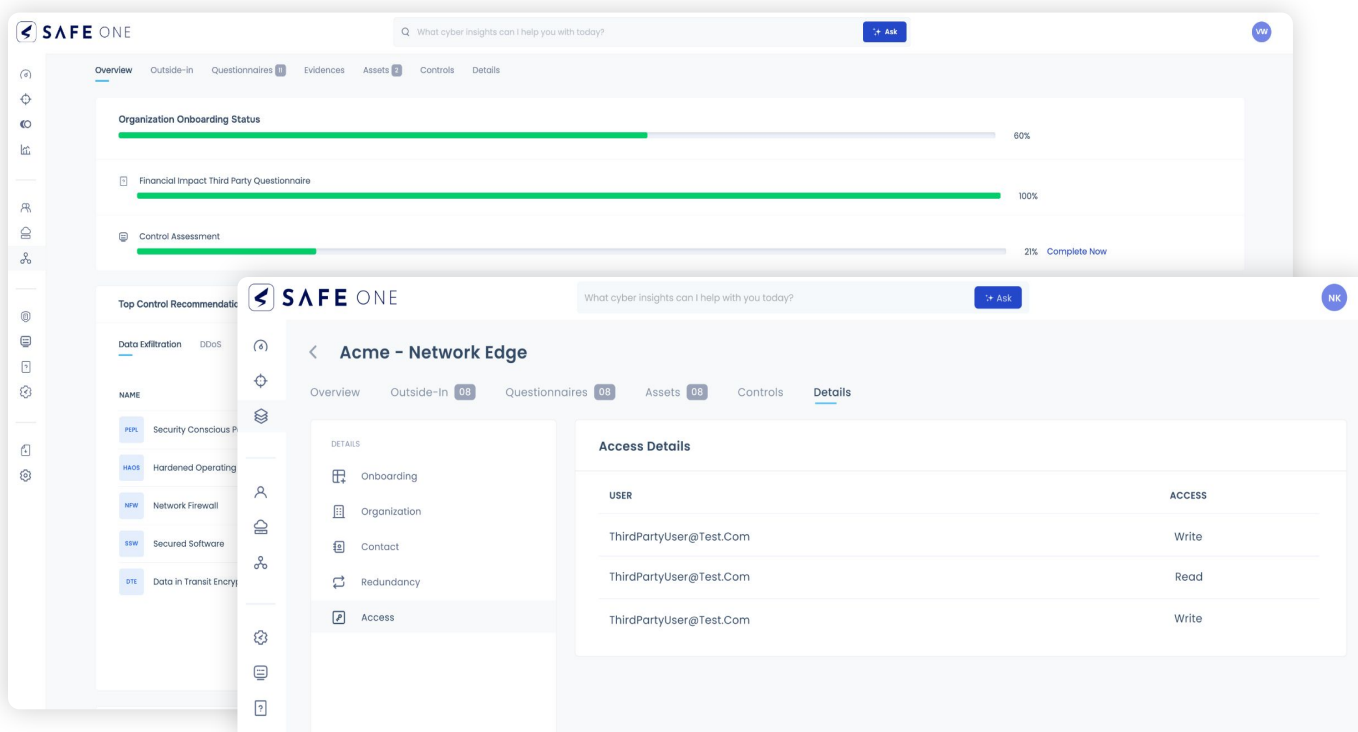
04 | Prioritize Third Parties Based on Business Risk

SAFE TPRM assesses the dollar risk and likelihood of occurrence of the most frequent cyber risk scenarios such as ransomware and data breach attacks based on third-party data access, network access, and resultant business interruption. This enables CISOs to tier their most critical vendors based on loss exposure instead of values such as size or revenue. SAFE TPRM enables enterprises to prioritize the most impactful controls to mitigate and reduce third-party risk.

SAFE TPRM transforms qualitative risk assessments into quantitative data that can be easily analyzed and acted upon. This process involves:

- **Breach Likelihood**: Each third party is evaluated based on their exposure to various risk scenarios such as ransomware and data breach attacks. These scenarios are prioritized based on their likelihood and potential impact on business operations.

- **Financial Impact Analysis:** The platform quantifies the potential financial loss from each risk scenario. This quantification takes into account direct costs such as operational disruption, legal fees, and regulatory fines, as well as indirect costs like reputational damage and loss of customer trust.

- **Transfer Liability to Third Parties**: SAFE TPRM helps you set up agreements that shares risk with third parties if a breach occurs.
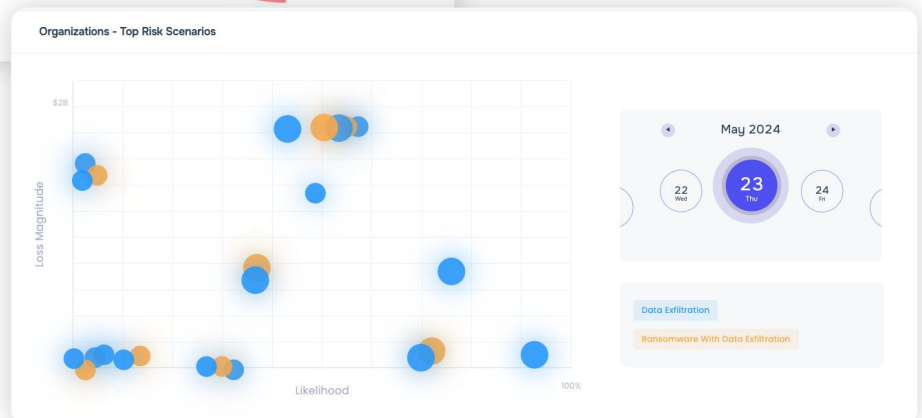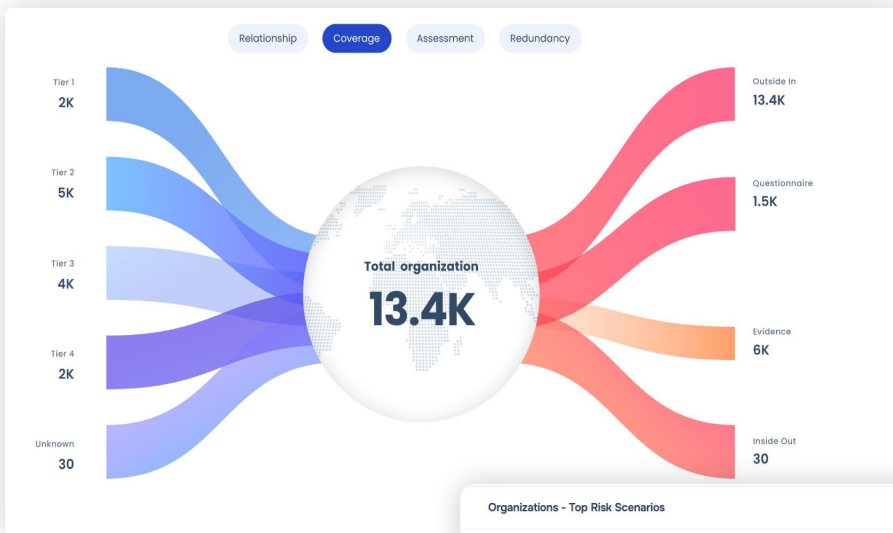
05 | Reduce Cost While Covering All Your Key Third Parties

SAFE TRPM acknowledges the dynamic nature of vendor risk management and its associated costs. Users of the platform can add an unlimited number of vendors at a fixed price since SAFE TPRM pricing is independent of the number of vendors – ensuring 100% of vendors are assessed. This scalable pricing model makes it practical to manage expenses of your growing third-party portfolio as the business expands.

- **All-Inclusive Pricing**: Pay one fixed price for access to all features, regardless of how many vendors you manage.
- **Add Unlimited Vendors:** Expand your network without worrying about increased costs.

SAFE Helps You With Key Third-party Questions

☑ **Who are your riskiest third parties in $ terms?**

Risk-based Third-Party Tiering: Focus on crucial vendors with tiering based on potential loss from their data access, network use, and any related business disruptions

☑ **How can I look at all telemetry from threat feeds and third parties?**

Comprehensive TPRM Approach: Integrates outside-in, questionnaire-based, and inside-out assessments with evidence and external threat intel to get a singular risk view

☑ **How can I efficiently manage my own security controls?**

Zero-Trust TPRM: Offers real-time insights into the effectiveness of first-party controls to minimize the impact of third-party breaches

☑ **What can I do? What can my third parties do to mitigate risk?**

Prioritized, Actionable Insights: Provides prioritized, ROI-focused insights to mitigate financial risks posed by critical vendors

☑ **How can I automate our enterprise third-party risk management program?**

Gen-AI-Powered Automation for TPRM: Automates data collection and security analysis to increase precision and speed

☑ **How can I visualize first-party and third-party cyber risks?**

Simple, One-Platform Solution: Manages both third-party and first-party risks on a unified platform for holistic risk oversight

☑ **Is it defensible and tunable?**

Open Standards and Defensible: Leverages FAIR, FAIR-TAM, FAIR-CAM, FAIR-MAM, MITRE ATT&CK, MITRE D3FEND, and NIST CSF

☑ **How can I manage my costs?**

Fixed Pricing Model: Features predictable, inclusive pricing that covers unlimited vendors, helping optimize TPRM costs

SAFE ONE