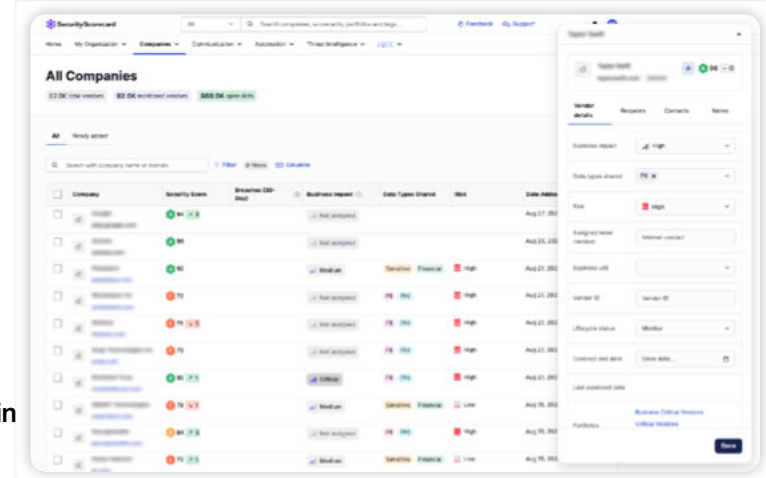
Security Scorecard

DATA SHEET

All Companies: Your Key to a Stronger TPRM Program

Reduce risk in your digital supply chain with deeper visibility from All Companies

Continuously monitor third-party risk, identify vulnerabilities, and work with vendors to remediate critical issues. With SecurityScorecard's All Companies view you can maximize TPRM efficiency. Store relationship details specific to your organization, better understand your vendors, the degree of risk they pose, and the potential impact to your organization in the case of a cyber event.



CREATE RULES FOR PARTIAL MONITORED AND FULL MONITORED COMPANIES

COMPLETE VISIBILITY INTO YOUR VENDOR ECOSYSTEM ON THE DASHBOARD

ACCESS VENDOR DETAILS DIRECTLY ON THE SCORECARD

Know Your Vendors on a Deeper Level

- Provide relationship details to better assess vendor security posture, how you're utilizing them in your ecosystem, and the risk they pose
- Following an incident or breach, leverage relationship details to quickly triage, and understand potential impact to your organization
- Easily track your organization's vendor requests (invitations, questionnaires, action plans, & evidence requests) in the details drawer

Insights at a glance for your entire vendor ecosystem

- Distinguish between vendors with a clear breakdown of your partial monitored vs. full monitored vendors
- Identify vendors who have reported breaches in last 30 days
- See vendors' scoring grade; view vendors by business impact
- Activity status; see if vendors have logged into the platform
- Demonstrate to stakeholders you're tracking all vendors in one place, with a holistic TPRM view

Vendor Details Tab

Requests: See evidence of all types of communication with a vendor from your organization

Contacts: Vendor recipients who respond to requests throughout the contract

Notes: Add comments to store important information about your vendors

Store vendor relationship details to more confidently assess risk

Business Impact: The potential consequence of a vendor's failure or disruption on your organization's operations, reputation, finances, and compliance. It evaluates how essential the vendor is to the business and the reliance on their services.

- Example: If a cloud service provider experiences downtime, it could disrupt operations, resulting in lost revenue, reduced customer trust, and legal issues, making the vendor critical.

Data Types Shared: Data types shared are the specific categories of information exchanged between an organization and its vendors.

- Example: A payroll vendor may receive employee PII, including names, addresses, and bank details, requiring strong data protection measures.

Risk: The probability of a negative event from a vendor's actions, services, or products, and its potential impact on the organization. It includes operational, financial, reputational, strategic, and compliance risks.

- Example: A vendor with inadequate security handling sensitive data poses a high risk, leading to potential breaches, financial penalties, legal issues, and reputational damage.

Internal Contact: The individual responsible for managing the vendor relationship within your organization, usually the stakeholder who initiated the vendor's entry into the platform.

- Example: The UX team uses Figma, therefore the individual responsible may be the Head of Design or VP of design.

Vendor ID: This field can be used to map the vendors in SecurityScorecard back to another system of record in your organization. This includes procurement, other GRC tools etc.

Business Unit: The business unit within your organization that owns the relationship with the vendor.

- Example: The UX team uses Figma, therefore the organization should be Product Design.

Status: The current status of the vendor at your organization.

Contract End Date: The date the contract with the vendor ends.

With SecurityScorecard's All Companies view, you can maximize the efficiency of your TPRM program by gaining deeper insights into your entire vendor ecosystem. Store relationship details, assess vendor security posture, and easily evaluate the risk and potential impact to your organization in the event of a cyber incident. With features like bulk actions, portfolio management, and the ability to distinguish between partial monitored and full monitored vendors, All Companies enables you to track and manage risk across all vendors, demonstrating a holistic approach to third-party risk management that goes beyond just your critical vendors.