CyberGRX vs. Competitors

CyberGRX brings a revolutionary approach to Third-Party Cyber Risk Management. Using sophisticated data analytics, real-world attack scenarios, and real-time threat intelligence, we provide a complete portfolio analysis of your third-party ecosystem, helping you to prioritize your risks and make smarter decisions.

With a growing digital ecosystem, companies are increasingly relying on third parties to succeed. With this, many turn to third-party risk management solutions to help with ingestion and management of third-party risk.

We see three main approaches to the problem, with none of them suited to solve the issue alone.

VRM PROVIDERS

Strengths

Often seen as the "true" solution to third-party risk management

Typically provide some sort of workflow capabilities

Multiple assessment types including customizable and drag-and-drop

Weakness

Exchange capability is truly data gathering & storage with little to no analytics

Focused on broader TPRM areas including privacy instead of cyber

Examples

OneTrust - Prevalent - UpGuard

GRC/WORKFLOW TOOLS

Strengths

Helps resources organize and prioritize assessment programs across multiple teams and third parties

Some have specific third-party risk management modules

Weakness

Simply an automated spreadsheet that doesn't provide analytics nor remediation prioritization

No data analysis nor focus on security

Expensive and resource-intensive

Examples

Archer Suite (RSA) - IBM OpenPages MetricStream

SECURITY RATINGS

Strengths

Does not require participation from third-party which means quick results

Often have many integrations that can be used with other tools in place

Emphasis is on security

Weakness

Limited visibility with outside-in scanning

Exchange capability is truly data gathering & storage with little to no analytics

No inherent or residual risk elements, meaning it's not reflective of actual risk posture

Examples

Bitsight - Security Scorecard

So how is CyberGRX different?

- True Exchange model built on standardized data that allows for rich analysis and actionable insights
- Both inside-out and outside-in data sources to provide contextualized 360-degree data and broad visibility that accurately reflects actual risk posture
- Portfolio-wide coverage that allows you to see, measure and reduce the overall risk across your entire portfolio within a single platform
- Security focus combined with third-party risk management expertise to provide only cyber-centric risk management program that helps to protect from emerging and existing cyber threats

	CyberGRX	VRM Providers	GRC/Workflow Tools	Security Ratings
A dynamic Exchange approach shared between customer and third party	Yes	No	No	No
Portfolio-wide view of risk surface	Yes	Yes	Yes	No
Mineable, structured data for analysis	Yes	No	No	No
Ability to produce continuous, near-real time results	Yes	No	No	Yes
Ability to manage domains of risk outside of security, privacy, and business continuity	No	Yes	Yes	No
Advanced kill chain analytics based on machine learning	Yes	No	No	No
Custom & Standard Control Framework Mapping	Yes	No	No	No
Automated Risk Ranking and Remediation Prioritization	Yes	No	No	No

Selecting an effective TPCRM program can be a daunting task. While there may be similarities between the different solutions on the market, it's the differences that you should focus on when evaluating. In order to secure digital ecosystems, companies need a methodology that combines a wide range of security safeguards with a modern approach to third-party cyber risk management, including threat intelligence and comprehensive data analytic capabilities.

A CyberGRX representative can walk you through how our solution ranks against the others. Contact us today at **Sales@CyberGRX.com** or visit our website at **www.CyberGRX.com** for more information