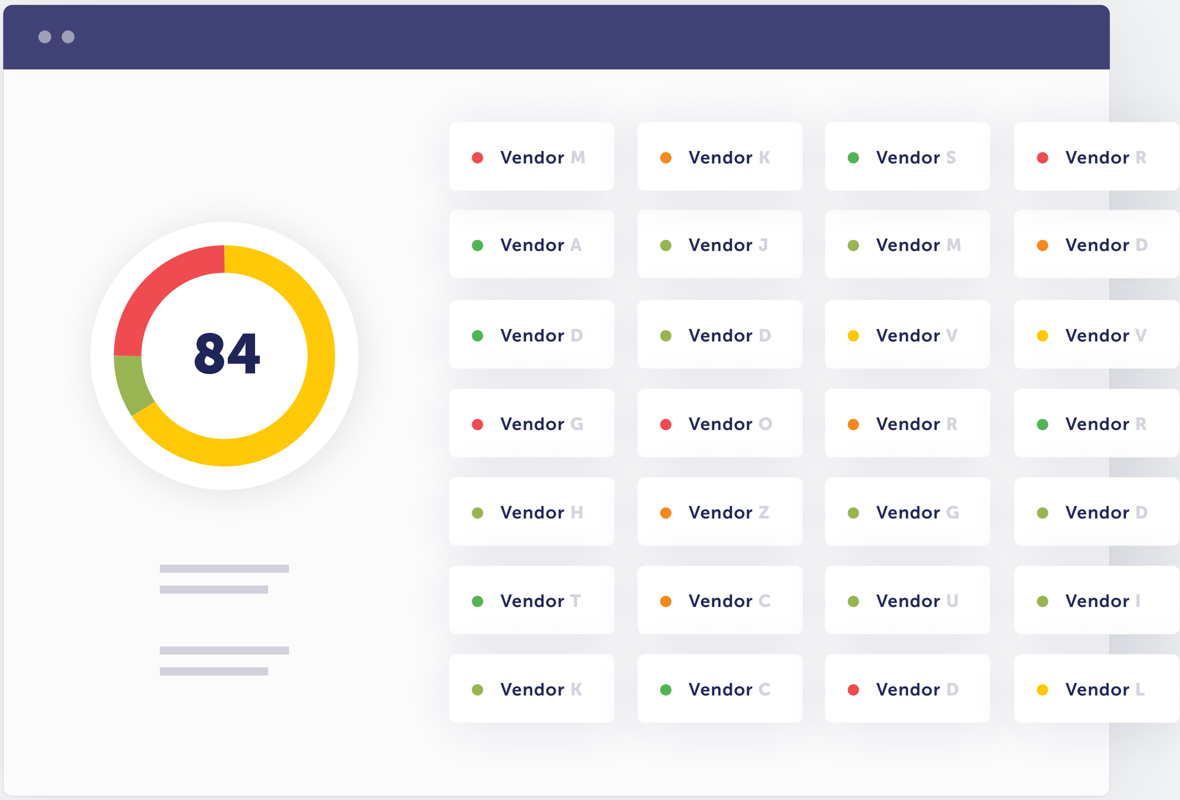
Panorays

The Critical Importance of Continuously Monitoring Third-Party Security

An Essential Part of Third-Party Security

Companies understand the importance of having a full due diligence process in place to assess the security of their third parties, such as vendors, suppliers, subsidiaries, partners, etc. But an essential part of the third-party security risk management process is what happens at the end.

Once you've finished assessing your third parties, you need to monitor them continuously for any potential or new risks that may require attention. That's because a point-in-time view doesn't keep up with the evolving risk landscape, as risk can change by the second and annual assessments are woefully ill-equipped for the task. Without that ongoing vigilance, an unknown change in a third party's security may result in a lack of compliance, heighten the risk of breach and exacerbate the associated fall-out.



As part of its mission to eliminate third-party cyber risk so that companies worldwide can quickly and securely do business together, Panorays continuously monitors and evaluates your third parties. You receive live alerts about any security changes or breaches. Let's take a closer look.

Four Key Benefits

To give customers ongoing visibility, insight and control over their third-party security, Panorays' monitoring is designed to be:

01. Rapid

When you are dealing with tens, if not hundreds, of third parties, time is of the essence. While monitoring is an essential part of managing third-party security, having to monitor your vendors/suppliers/partners manually is an arduous and time-consuming task, which is not sustainable. In order to scale, Panorays offers fast, automated monitoring.

02. Continuous

Performing a risk assessment of one of your third parties is essentially a snapshot of their security posture at a moment in time — even though organizations and technology are constantly changing. Panorays' continuous monitoring raises the awareness of third parties' changing vulnerabilities, processes and security posture through live alerts. This way, organizations can make effective decisions about their third-party security risk in real time.

03. Collaborative

Collaboration creates a common language among stakeholders. Conversely, when there isn't collaboration, the right hand doesn't know what the left hand is doing, which also increases risk. As the only solution that enables in-platform engagement, Panorays eliminates the friction between evaluator and supplier, enabling communication, collaboration and quick remediation.

04. Comprehensive

Organizations should have established processes to conduct comprehensive monitoring of third parties. Companies, as well as cyber threats, are constantly changing and evolving, making it imperative to keep up with the increased number of vendor threats. Panorays' comprehensive analysis includes performing hundreds of tests to evaluate your vendors' attack surface, investigating the dark web for anomalies that could indicate malicious behavior, as well as considering the impact of human behavior on your vendors. With knowledge comes power, so the more you know about your third parties, the better equipped you are to be proactive about mitigating risks as they are discovered.

Deep Dive on the Panorays Third-Party Security Platform

Panorays quickly and easily automates third-party security risk evaluation and management — handling the whole process from inherent to residual risk, remediation and ongoing monitoring. Companies using Panorays:

- Dramatically speed up their third-party security evaluation process
- Streamline collaboration and remediation between teams and suppliers, creating a transparent, efficient and effective process
- Eliminate the tedium and delay of manual questionnaires in assessing third-party security
- Gain continuous visibility and actionable insights into evolving supplier risk
- Manage and mitigate risk and implement security policies with the click of a button
- Prioritize risk remediation to better manage the security of their third parties
- Ensure vendor compliance with numerous industry regulations
- Optimize efficiency of their time, resources and budget
- Quickly and easily build trust within business relationships

Unlike other solution providers, Panorays combines automated, dynamic security questionnaires with external attack surface assessments and business context to provide organizations with a rapid, accurate view of supplier cyber risk. It is the only such platform that automates, accelerates and scales customers' third-party security evaluation and management process, enabling easy collaboration and communication between companies and suppliers, resulting in efficient and effective risk remediation in alignment with a company's security policies and risk appetite.

Panorays is a SaaS-based platform, with no installation needed, and is the missing link that creates an out-of-the-box process and security plan, which also easily integrates into existing organizational workflows and systems. It is trusted by organizations worldwide in industries such as financial services, banking, insurance and healthcare, among others.

Want to learn more about how to efficiently and comprehensively monitor your third-party vendors? Contact us to schedule a demo.

About Panorays

Panorays is a rapidly growing provider of third-party security risk management software, offered as a SaaS-based platform. The company serves enterprise and mid-market customers primarily in North America, the UK and the EU, and has been adopted by leading banking, insurance, financial services and healthcare organizations, among others. Headquartered in New York and Israel, with offices around the world, Panorays is funded by numerous international investors, including Aleph VC, Oak HC/FT, Imperva Co-Founder Amichai Shulman and former CEO of Palo Alto Networks Lane Bess. Visit us at **www.panorays.com**