Panorays

How to Avoid an Inaccurate View of Supplier Risk

Why Accuracy is Essential for Assessing Supplier Risk

Data breaches. Fines. Loss of reputation and customer trust.

That's what you could be facing if you have an unknown, incomplete or inaccurate view of supplier risk. Not knowing the extent of your supplier risk leaves you vulnerable, but the process of gathering and effectively analyzing data can be daunting—especially when you are working with hundreds or thousands of vendors.

Panorays provides you with a rapid, accurate view of supplier and fourth-party cyber risk, so you get comprehensive in-depth visibility and control and can make rapid decisions about whether to work with suppliers.

Here's how.

01 360-Degree Ratings

Some platforms assess third parties using security questionnaires, but they only provide a snapshot of a moment in time. Other platforms perform external attack surface assessments to detect cyber gaps, but these don't consider a third party's internal policies or security posture. In addition, they don't necessarily consider the context of the business relationship between the organization and supplier to understand the level of risk.

Panorays' 360-degree ratings combine automated, dynamic security questionnaires with external attack surface assessments and business context, providing organizations with the most comprehensive and accurate view of supplier and fourth-party cyber risk.

02 Customizable Questionnaires

Security questionnaires are essential to assessing third-party security controls, but it can be difficult to create the right questionnaire based on your unique relationship with each supplier.

The Panorays platform lets you select the best option for your organization's needs with its Smart Questionnaire™. You can use built-in SIG and CAIQ questionnaires, allowing you to derive the most relevant set of questions quickly, or customize your own. By ensuring that each of your suppliers receives a tailor-made questionnaire, you can cut down on time spent reviewing irrelevant questions and receive the most accurate data to make decisions about supplier risk.

03 Attack Surface Assessment

Comprehensive analysis is necessary for assessing the security of your third parties, but many companies lack the resources to accomplish this quickly and effectively.

Panorays non-intrusively evaluates your vendor's attack surface by performing hundreds of tests, such as collecting information on exposed assets or a lack of security best practices. Tests are performed to assess network & IT, application and human layers, including checking web, email and DNS servers, web applications and employees' social posture. Panorays also checks mentions of vendors on dark web hacker forums and other web marketplaces, providing deep insights into supply chain threats.

04 Context-Based Ratings

Not all risk is the same, but companies have no easy way to contextualize risk according to the business relationship. For example, a supplier that brings paper to the office should not be rated the same way as one that connects to your mail systems. If suppliers are not assessed correctly, risk can be portrayed inaccurately, leading to wasted effort in remediation when risk is incorrectly overweighted, and lack of urgency in mitigating when it is falsely underrated.

Only Panorays rates according to context by considering the business and technology relationship with your suppliers. Companies get an accurate picture of risk according to actual business impact, enabling them to prioritize efforts correctly to truly control risk.

05 Ratings Accuracy

Often, third parties receive low cybersecurity ratings because of an erroneous finding or a problematic asset that they may not even own. These "false positives" can wreak havoc for both third parties and organizations.

Panorays' cybersecurity ratings consist of numerous tests that are checked against a large dataset for distribution, as well as a trusted dataset for validation, resulting in an accuracy rate of 99.4%. All tests and results are made available to organizations and their third parties. Moreover, third parties may easily dispute findings and assets, and Panorays validates the data internally within 24 hours, accepts or rejects the claim and updates the findings accordingly.

06 Ratings Visibility

To perform a comprehensive evaluation of third-party security, it's necessary to combine data from many different sources, which can be confusing. In order to fully understand this evaluation, organizations and their third parties must receive a clear explanation of how cyber risk is assessed, including the methodology used to calculate ratings.

The Panorays platform provides complete visibility into the elements that make up the vendor's ratings. For example, in the attack surface assessment, the user can see which tests were performed, whether there were findings or not, and drill down to the asset level so the finding can be validated. In addition, CVE information is attached to each relevant finding, which provides information on how the finding severity level was derived.

07 Continuous Monitoring

A point-in-time view of suppliers doesn't keep up with the evolving risk landscape. Risk can change by the second, and annual assessments are woefully ill-equipped for the task. An unknown change in a supplier's security posture can result in lack of compliance, additional risk to the company, heightened risk of breach and associated fallout such as fines and lawsuits.

Panorays continuously monitors and evaluates the supplier, and you receive live alerts about any security changes or breaches to your third parties. That way, you gain ongoing visibility, accuracy and insight into, and control over, third-party security risk.

Conclusion

Isn't it time you received a comprehensive and accurate view of supplier risk?

Find out how easy it is to bring your third-party cyber risk assessment to the next level with in-depth visibility and control. Breathe easier knowing that you are getting the most accurate view of your vendors' cyber posture.

Request a Panorays demo today >

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**

For more information: info@panorays.com