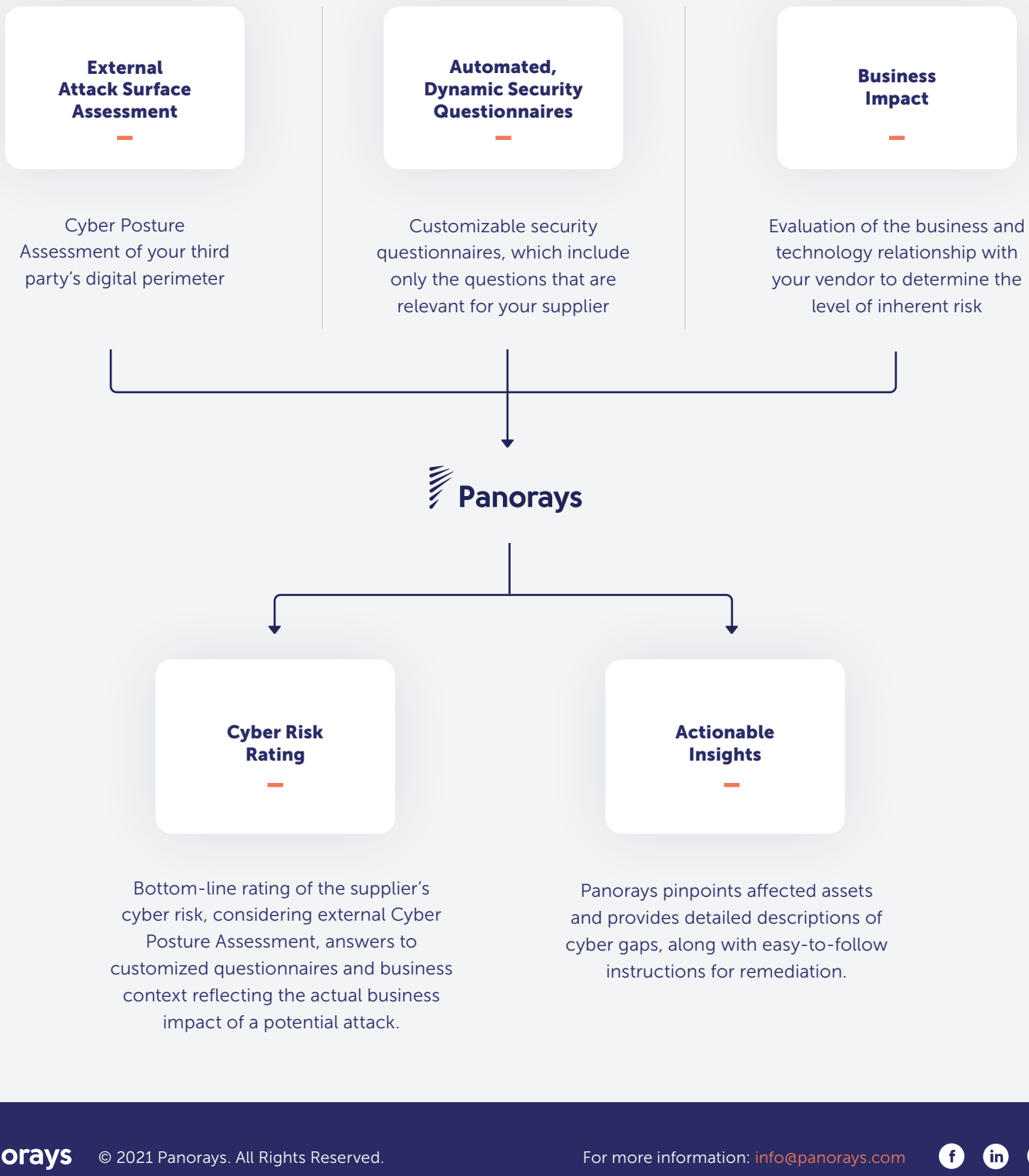
Panorays

A Deep Dive Into the Panorays Platform

Panorays automates, accelerates and scales the third-party security evaluation and management process so customers can quickly and easily manage, mitigate and remediate risk, reduce data breaches, ensure vendor compliance and improve their cybersecurity posture across the board.

Cyber Risk Assessment

Unlike other solution providers, Panorays combines automated, dynamic security questionnaires (Smart Questionnaires) with external attack surface assessments (known as our Cyber Posture Assessment) and takes business impact into consideration to provide organizations with a rapid, accurate view of supplier cyber risk.



For more information: info@panorays.com

Under the Hood
Cyber Risk Assessment

External Attack Surface Assessment

Automated Questionnaires

Cyber Risk Ratings

External Attack Surface Assessment

Panorays non-intrusively evaluates your vendor's attack surface through the analysis of externally available data. To ensure a comprehensive view of your third party's digital perimeter, Panorays performs hundreds of tests, such as collecting information on exposed assets or a lack of security best practices. Tests are performed to assess three different layers:

Network & IT
Web, e-mail and DNS servers, TLS protocols, asset reputation, cloud solutions and other exposed services.

Application
Web applications, CMS, domain attacks, etc.

Human
Employees' attack surface, social posture, presence of a dedicated security team, etc.

Example findings within the Network, IT and Application layers could include untrusted TLS certificates, a missing WAF on a significant asset, exposure of WordPress user data, an unpatched application version, etc. In addition, Panorays considers the effect of human behavior in a supplier's external attack surface assessment — and is the only platform that does so. Example findings here could include high employee attack likelihood based on social media presence, lack of employee security awareness or the absence of a dedicated security team.

Cyber Posture Rating

The analysis of a vendor's public-facing digital footprint is typically completed within hours and is continuously monitored and updated. Each supplier receives a Cyber Posture Rating from 0–100, representing a calculated average of ratings for each layer of the vendor's digital perimeter.

Fourth-Party Discovery

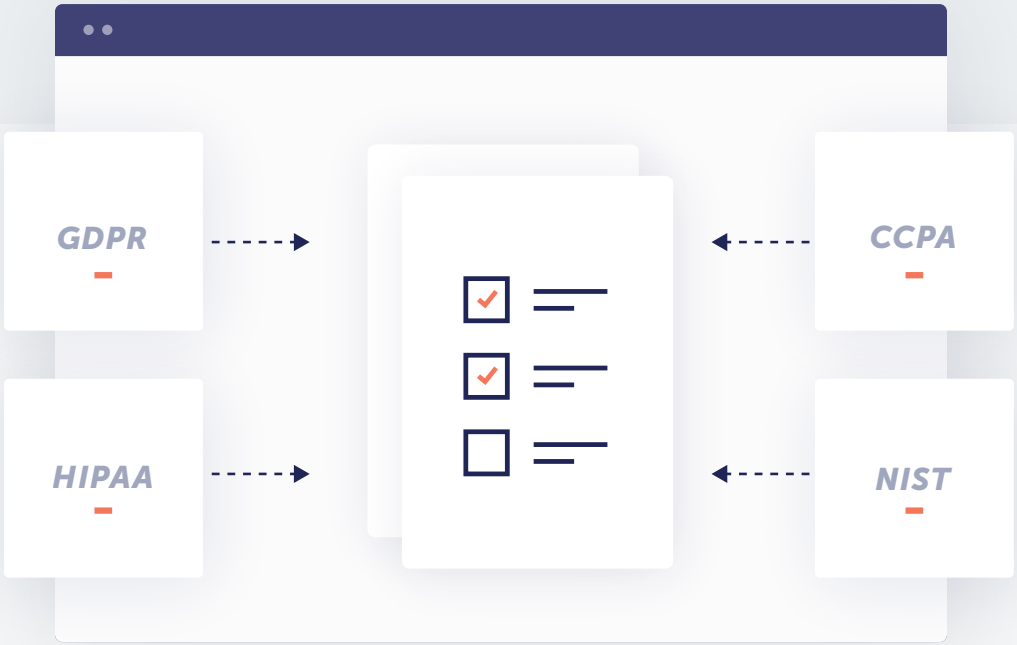
During the external attack surface assessment, Panorays automatically detects the third-party vendors of the supplier (the evaluator's fourth parties). This provides additional insights into the vendor's cyber posture, as it is affected by the cyber posture of its own suppliers.

Dark Web Insights

Dark Web Insights complement Panorays' context-based ratings in providing a comprehensive view of your third party's attack surface. Panorays checks mentions of the vendor on hacker forums and other dark web marketplaces, providing deep, real-time insight about in-the-wild threats to your supply chain. Companies automatically receive a notification when there is abnormal dark web activity regarding a third party.

Automated Questionnaires

Panorays' automated, dynamic questionnaires, known as Smart Questionnaires, are an essential part of assessing the vendors' cyber risk level. Panorays' questionnaires are completely customizable, enabling companies to select only the relevant questions for each third party evaluated, in the language they require.



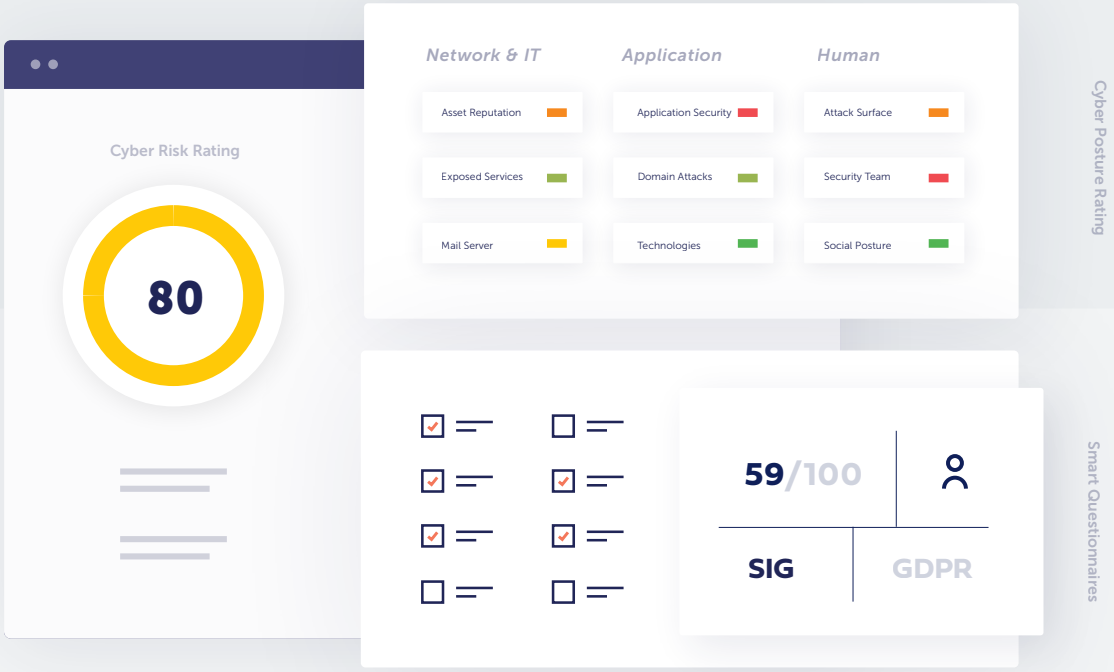
You can either choose from a built-in Panorays template, customize a standard questionnaire such as SIG or CAIQ or create your own questionnaire based on internal company policies. Companies can also decide on which specific frameworks, standards and regulations should be reflected in each questionnaire. As an example, a supplier with access to customers' private data will probably need to adhere to GDPR, CCPA and/or other privacy regulations.

Automated Questionnaires Rating

A rating from 0–100 is calculated based on the third party's responses to the customized questionnaire. You can decide on how your questions should be calculated in the rating, according to your company's internal policies and risk appetite. Companies can also flag important "deal-breaker" questions, to quickly identify vendors that don't comply with internal policies.

Cyber Risk Ratings

In addition to providing a detailed description of cyber gaps with a suggested remediation plan, Panorays also generates a Cyber Risk Rating for each third party. Cyber Risk Ratings empower security professionals to make quick decisions regarding a potential or existing vendor. In the supplier's vetting process, the evaluator can establish a threshold that vendors need to meet in order to do business with the company. For existing vendors, a drop in the Cyber Risk Rating can indicate a significant change in risk, requiring the company to take immediate action. Cyber Risk Ratings also serve as an input for higher-level risk management platforms.



Ratings by Context

The Cyber Risk Rating has five levels, calculated by a risk matrix based on impact and likelihood. Impact score takes into consideration the business and technology relationship with your suppliers, reflecting the potential damage to the company in case of a third-party cyber breach. The likelihood of an attack is determined based on the results of both the external attack surface assessment and internal security questionnaire. Context-based ratings provide you with an accurate picture of risk according to actual business impact, and the ability to prioritize efforts correctly to control risk.

Working With the Panorays Platform

Managing third-party security risk involves many different stakeholders within the evaluator and vendor organizations. Panorays is an automated, easy-to use, comprehensive platform that unites different departments within a company as well as all of their suppliers — providing a single, unified place to communicate, collaborate and remediate third-party security risk.

Evaluators and vendors can easily manage the third-party security risk process using Panorays:

01

Assessment

Panorays combines automated, dynamic security questionnaires with external attack surface assessments and takes business impact into consideration to provide organizations with a rapid, accurate view of supplier cyber risk.

02

Engagement

In-platform engagement eliminates the friction between evaluator and supplier, enabling communication and collaboration.

03

Remediation

Companies can customize Panorays' suggested remediation plan and monitor progress using the platform. Suppliers easily dispute or validate findings to achieve accuracy.

04

Approval

Companies quickly onboard suppliers which are in alignment with the organization's security policies, regulations and risk appetite.

05

Continuous Monitoring

Panorays continuously updates the risk assessment based on changes to the supplier's external footprint, responses to questionnaires and the feedback loop between the supplier and evaluator. Security teams receive live alerts about any security changes or breaches to third parties.

Why Panorays?

360-Degree Ratings

Collaboration

Smart Questionnaires

Continuous Monitoring

Context-Based Ratings

Dark Web Insights

Human Factor

Vendor Compliance

For more information: info@panorays.com

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