Publication date:
16 Jun 2021
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: Panorays offers third-party security risk management

Brought to you by Informa Tech

Table of Contents :

Summary

Catalyst

Panorays is a developer of third-party security risk management (TPSRM) technology, targeted primarily at midsize companies and delivered in software-as-a-service (SaaS) mode.

Omdia view

As trends such as business process outsourcing have taken off in the global economy, the need to detect and manage the risks posed to an enterprise by third parties (suppliers, contractors, and channel partners), and of course to remain compliant, has spawned an entire tech sector to meet those requirements. Those risks may come from lax or inappropriate behavior from those companies, resulting in financial, operational, or reputational damage to the enterprise dealing with them.

Within the field of third-party risk management (TPRM), however, it is only over the last decade or so that the cybersecurity dimension has come to the fore. As ever more business interactions and transactions have moved online, the ability to check that third parties' IT systems are secure and compliant is now an essential component of any company's governance, risk, and compliance (GRC) toolkit. As a vendor focused specifically on this segment of the broader TPRM market, Panorays is positioned to meet the needs of a growing number of businesses.

Why put Panorays on your radar?

Panorays supports both the questionnaire and security ratings approaches in its platform, factoring in the business impact of the relationship under analysis. It enables its customers to analyze the risk profile of partners and suppliers on an ongoing basis, determining the frequency with which checks are carried out, up to and including continuous monitoring. The platform also enables collaboration between customers and their vendor partners to improve the overall attack surface, thereby reducing risk and bolstering compliance. As such, it supports the whole flow of TPSRM as it is currently practiced.

Market context

TPSRM is a branch of the broader TPRM technology sector. While TPRM covers multiple dimensions of risk (financial, operational, compliance, reputational, etc.), TPSRM, as its name suggests, focuses specifically on the cybersecurity risks associated with third parties.

These may be suppliers of IT systems (software, hardware, or services) or other companies that interact with an enterprise, such as suppliers of goods and services, or downstream channel partners such as car dealerships and retail outlets. Essentially, it refers to any company that has access to the enterprise's IT infrastructure, whether in person (e.g., an IT contractor doing some development work) or programmatically (i.e., system-to-system, such as with a company's ERP system).

The importance of this aspect of TPRM has grown in tandem with the rise in business process outsourcing, e-commerce, and the general trend for interactions between commercial entities to move online. Panorays cites statistics suggesting that the average enterprise currently connects to 182 other businesses (partners, suppliers, tech, and service providers, etc.) every week and shares data with an average of 583 organizations generally. Furthermore, 58% of organizations believe they have incurred a data breach via a third party to which they are connected in this way.

There are countless high-profile examples of cyber risk, from the recent hack on SolarWinds's network monitoring software, which affected some 300,000 entities in business and government, to the infamous Target data breach of 2013, when a provider of HVAC services to the retailer was hacked by criminals, enabling them to steal details on 110 million customers' payment cards.

Among the types of cyber risks faced by enterprises engaging with third parties via their IT systems are:

- intellectual property theft
- credential theft
- spear phishing
- data exfiltration
- network intrusion
- fileless malware

To counter such attacks, TPSRM adopts two main approaches. First are manual questionnaires filled in by the companies, referred to as "vendors," that interact with its enterprise customers. While it represents a way of gathering a lot of information, this approach has limitations, in that it is time-consuming for both the company responding to the questionnaire and the TPSRM vendor rating the answers. As a result, there are scalability issues, even if efforts are made to streamline the process, e.g., via online delivery of the questionnaire. Lastly, and most seriously, such questionnaires are at best a point-in-time picture of a company's position, requiring repetition at least on an annual basis to remain vaguely up to date, which is clearly a sub-optimal situation causing friction in the vendor base.

Second are security rating services (SRS), providers of which use an external assessment engine. These engines scan the digital assets of the vendor that their customer is planning to onboard (or one that is already a business partner, supplier etc.), doing so over the public internet so as to be non-intrusive. The purpose of this exercise is to draw up a list of vulnerabilities, gaps in their security, and other issues, such as exposed assets, together with the concomitant security risks. They then score them by their severity, enabling the customer to decide whether to proceed with the business relationship, as well as to enable the assessed scanned vendor to fix any issues and improve their score.

Product/service overview

Panorays is a SaaS-based platform that is designed to integrate into existing organizational workflows and systems. It combines support for security questionnaires with an SRS capability, while considering the actual business relationship with each vendor when providing risk assessments.

Discovery

Once the initial list of vendors is supplied by the customer, usually by being exported from their CRM or ERP system, Panorays automatically discovers all third- and fourth-party relationships for a given vendor. It stresses that this discovery process does not require any consent from the vendor in question, though vendors can be invited to join the Panorays platform to collaborate in the discovery process if the customer so desires. Vendors can dispute findings and can follow Panorays' suggested mitigation steps to close cyber gaps and improve their rating.

Discovery is performed across domains, subdomains, the vendor's technology stack and its staff, as well as across its cloud infrastructure, with this last dimension considered something of a differentiator for its technology by Panorays.

Inherent Risk

The discovery process enables Panorays to provide an assessment of the vendor's external attack surface, or as it refers to it, the "third-party digital perimeter." More specifically the score awarded to a vendor as a result of this process is for its inherent risk, defined as the risk level a Panorays customer faces when nothing is done. By specifying this risk level, it enables customers to work on reducing inherent risk, leaving only so-called residual risk in the third-party relationship, which is defined as the risk that still exists after security measures have been implemented.

In addition to the assessment process, Panorays also operates automated questionnaires that can be adapted to the customer's security policies, with the customer itself providing the tiering and criteria for which tier a scored vendor should appear in. The cadence of vendor assessments can vary from quarterly all the way to continuous.

Once the assessment is completed, Panorays users can share a prioritized remediation plan with their vendors, which includes issues raised by both the security questionnaires and the external attack surface assessment. The assessed vendor can take remedial action, after which the platform can again perform an assessment and enable the customer to approve of the changes made or request further action. The customer can communicate with the vendor from the platform itself, for example commenting on specific questions and requiring additional information. Finally, the customer can approve or reject a vendor from the platform itself.

Company information

Background

Panorays was founded in 2016 by CEO Matan Or-El, COO Meir Antar, and CTO Demi Ben-Ari, who had all met while working in IT for the Israeli Air Force. Prior to starting the company, Or-El spent nearly five years at Imperva, the last two of which as R&D platform and infrastructure team leader. Antar had previously founded Cloud Memory Analytics (CMA), which provided endpoint detection and response (EDR) based on the analysis of big data, while Ben-Ari's previous role was senior data engineer at Windward, a predictive intel platform provider.

Panorays has raised a total of $20m in two funding rounds, most recently announcing a $15m Series A round in December 2019, led by Oak FC/HT, an Israeli VC fund focused on healthcare information services and financial service technology.

Current position

Panorays targets midsize companies, which it defines as those between 200 and 1,999 employees. Within those entities, it sells to line-of-business owners, as well as security, compliance, and third-party risk managers. It also aims to foster closer relationships with the vendors on which it reports, signing them up so that both sides of the TPSRM audit process can be on the same platform. This also enables them to cite Panorays whenever they are negotiating relationships with other companies in future.

Panorays says the average vendor audit takes around eight days and highlights the fact that there is no obligation for customers to take its entire platform, i.e., they can just use it for questionnaires or for ratings if they prefer. That said, the company reckons around 85% of its customers are currently using the platform in its entirety. It says its customer base currently runs into the hundreds and spans multiple vertical markets. The majority of its customers are located in the US.

While it relies heavily on the viral effect of customers involving other companies in its orbit by sending them its questionnaires, Panorays also has partners in the managed security services provider (MSSP) segment, since its platform can be readily employed to deliver a TPSRM service with their brand.

As for its charging mechanism, Panorays customers purchase a subscription, the scope size of which is based on the number of vendors to be monitored.

Future plans

Panorays' technology roadmap for 2021 and 2022 comprises a number of enhancements to the platform, such as:

- Workflow automation, i.e., streamlining the evaluation process with automation and integrations with systems from other vendors.
- Expert review, which will require the integration of various information points to enable a more comprehensive evaluation.
- The creation of security profile kits, which will enable vendors to share their cyber posture privately or publicly with customers and prospects, thereby further spreading the Panorays name.
- More self-service features and the kind of capabilities required of an enterprise-grade platform, thereby enabling Panorays to target larger organizations.

Key facts

Table 1: Data sheet: Panorays

Product/Service name	Panorays	**Product classification**	Third-party security risk management
Version number	1	**Release date**	May 2018, with monthly updates
Industries covered	All	**Geographies covered**	Global
Relevant company sizes	Mid-market (200–1,999 employees)	**Licensing options**	Per vendor assessment

URL	https://www.panorays.com/	**Routes to market**	Direct and channel
Company headquarters	New York, NY, US	**Number of employees**	60

Source: Omdia

Analyst comment

Panorays’ competitive landscape is a fragmented one, in that it faces different competitors in each market segment. Thus, there are a number of companies offering SRS, such as BitSight, Black Kite, and RiskRecon, but they do not offer security questionnaires. Conversely, it encounters the likes of OneTrust, Whistic, and CyberGRX on the questionnaire side of the market, but they don’t offer a ratings service. Any threat to Panorays from such companies would require them either to develop the missing part of their portfolio or to partner/merge with companies in the other part of the market for a complete TPSRM offering.

There are, of course, companies that aspire to span both worlds in the broader TPRM market, such as SecurityScorecard, UpGuard, and Prevalent, but Panorays questions their ability to provide a true 360-degree view of vendor cyber risk. Should any of them seek to double down on cyber with a view to addressing the growing requirement specifically for TPSRM, they might be tempted to acquire one or other of the specialist vendors, which could impact the overall competitive environment.

As for moving beyond cyber risk to the wider world of TPRM, while Panorays’ customers might urge such a move, Omdia suspects that it has enough market potential and competitive challenges in the narrower realm of security risk for the time being.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com