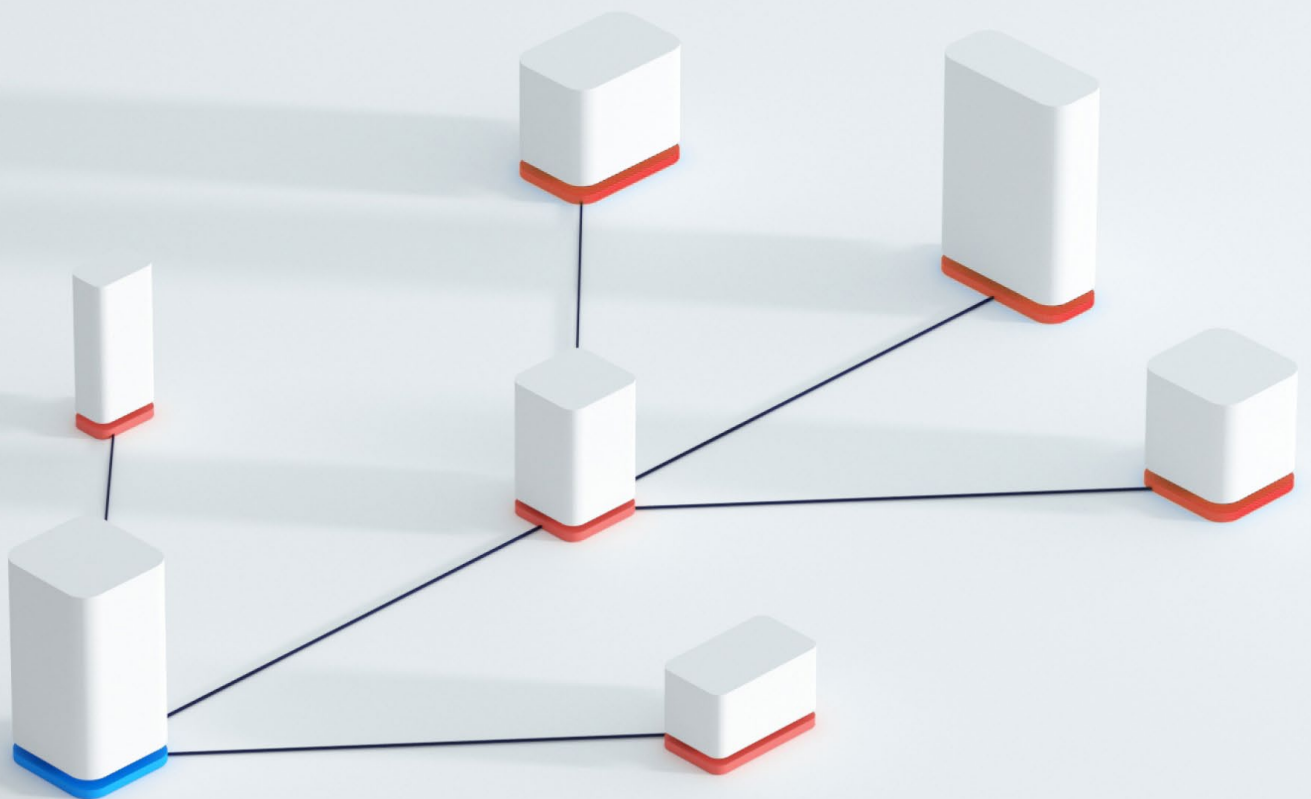


# Third- and Fourth-Party Discovery

Failing to adequately screen suppliers' security can lead to data breaches, which can shut down operations, damage customer trust and incur hefty regulatory penalties. For these reasons, third-party security must be comprehensive, efficient and scalable.

Panorays provides a feature to automatically detect your third-party vendors. As an evaluator, this is a useful tool to verify that all your third parties are known and managed with Panorays.

Additionally, Panorays automatically detects the third parties of the suppliers added to the platform, also known as your fourth parties. This gives you additional insights into the cyber posture of a certain supplier, as each supplier is affected by the cyber posture of its suppliers, and so on.



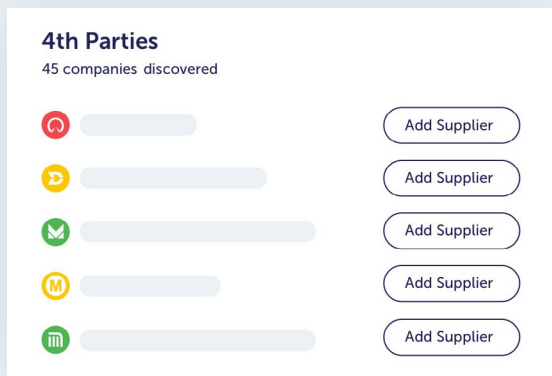


# Methodology

During the cyber posture assessment of a company, Panorays discovers all of the company's digital assets, including domains and IP addresses. Panorays then collects information about each asset; for example, the technologies that are in use.

The data collection includes common methods such as technology fingerprinting and DNS record mining. Panorays also has undisclosed discovery methods that are part of its intellectual property. All discovery methods are either passively obtained from public sources or non-intrusive common probes.

By the end of the assessment, Panorays has collected a considerable amount of data, from company assets and mappings to external assets and technologies. Since Panorays has such a large database of hundreds of thousands of companies, it can correlate the external assets to real companies and automatically detect many vendors used by the assessed company.



All of the third- and fourth-party vendors discovered by Panorays are companies that have been identified and assessed in the Panorays platform. Therefore, they provide immediate insight into the cyber posture of the company using them.

It is important to note that Panorays does not just assess technology vendors. Although there is a strong bias toward discovery of technology vendors due to the digital assets being assessed, Panorays has additional proprietary methods for discovering non-tech vendors in the discovery process as well.

# About Panorays

---

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. 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.

The company is offered as a SaaS-based platform and serves enterprise and mid-market customers primarily in North America, the UK and the EU. It 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](http://www.panorays.com)

Any questions about getting started with Panorays?

[Please click here to get in touch >](#)