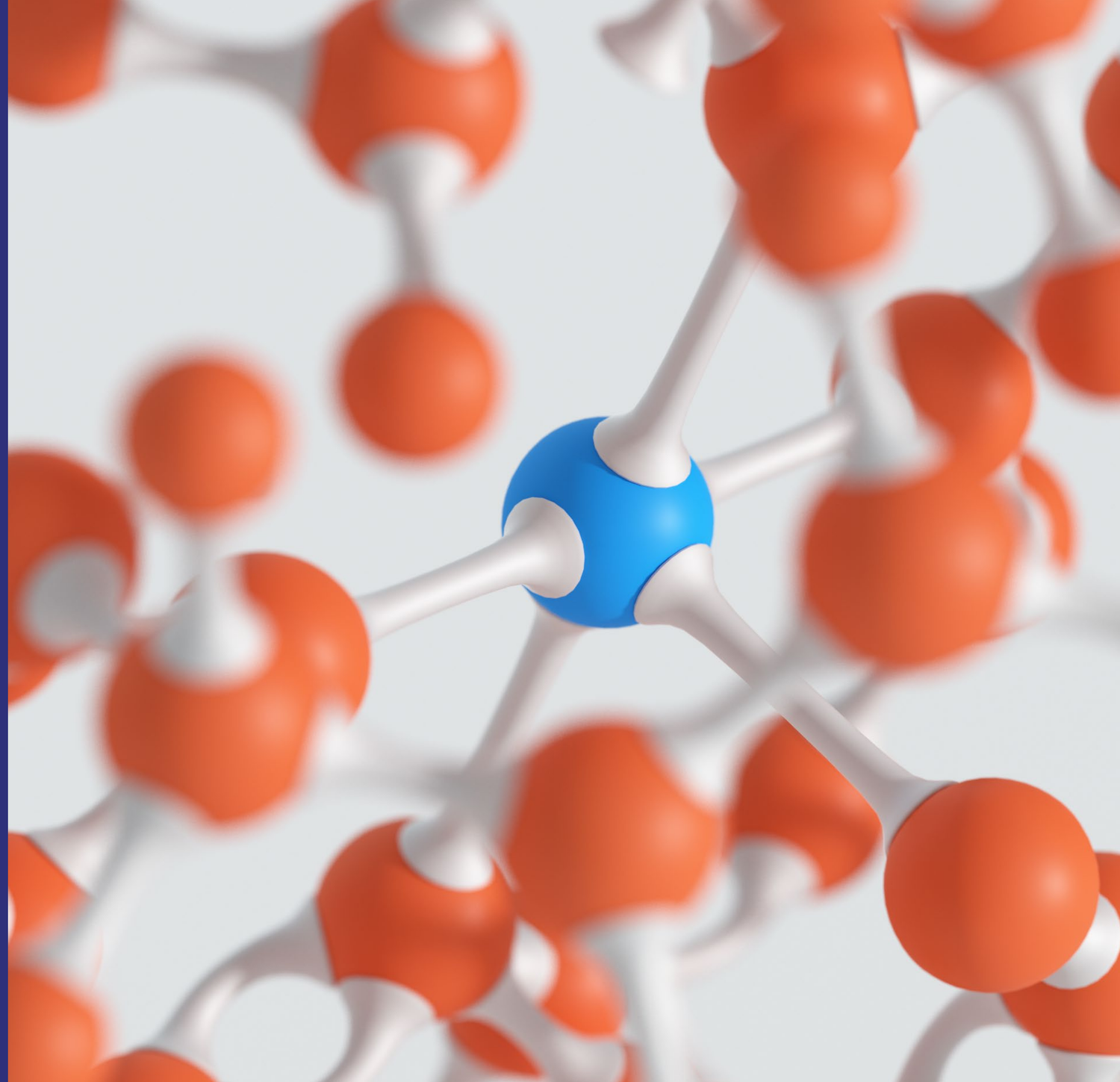
Panorays

Solution Brief

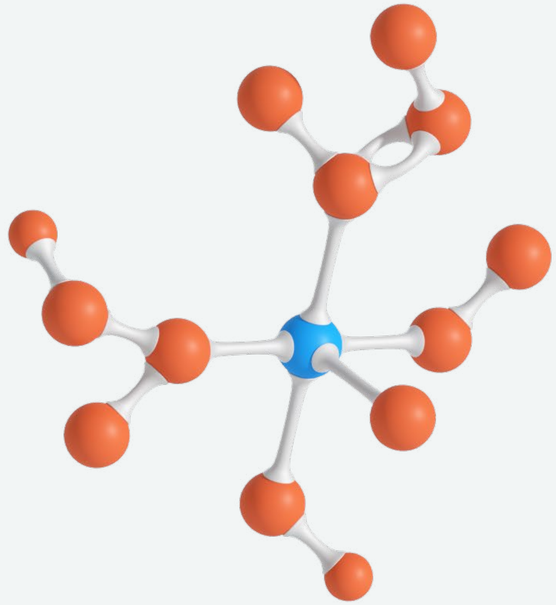
Digital Attack Surface Visibility



Introduction

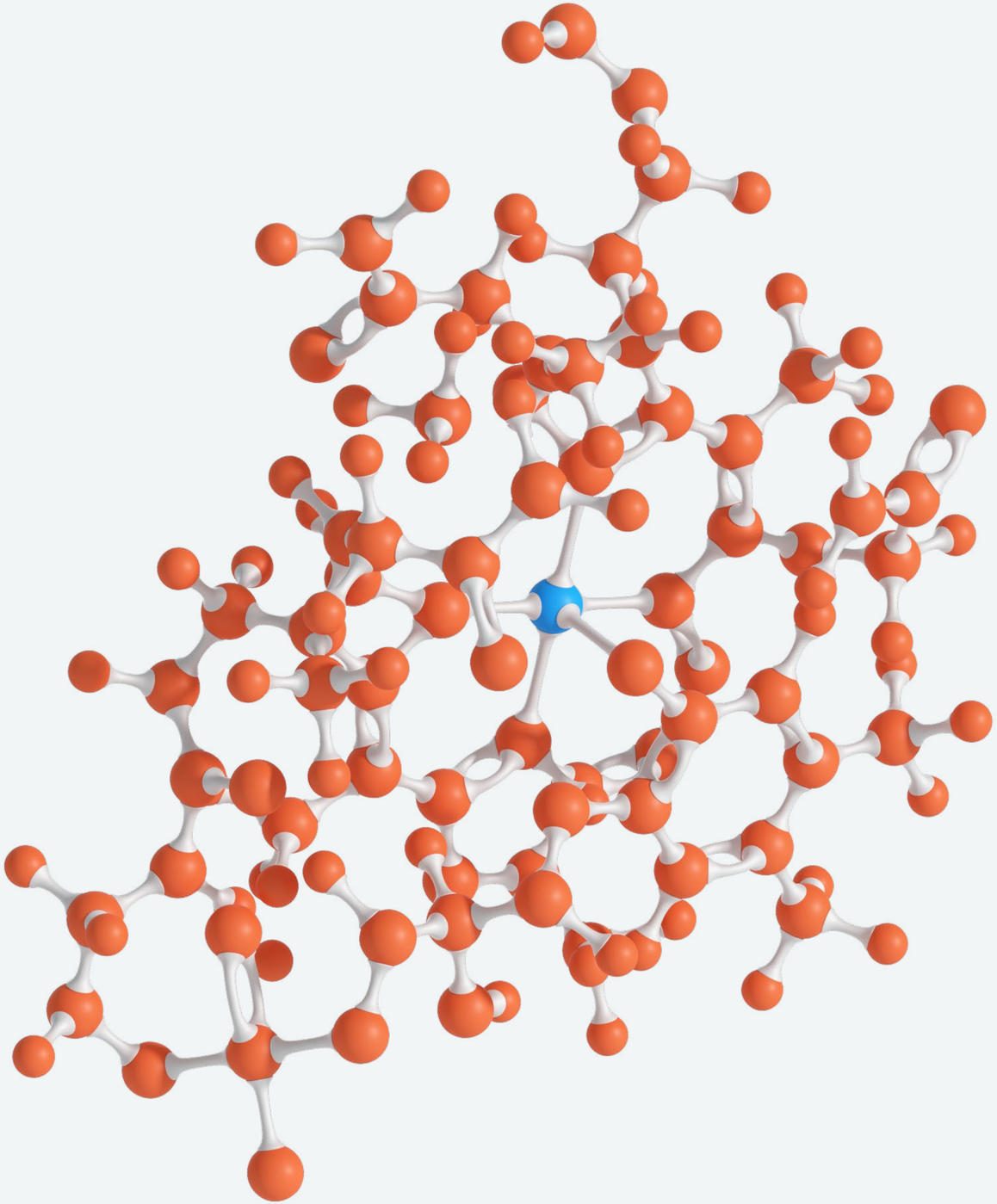
Your digital assets that previously sat within the perimeter of your network security have now moved to the cloud. Your own attack surface looks like a complex molecule, with each chemical bond providing threat actors a new opportunity to infect.

Comprehensive analysis of your organization's attack surface is the first step towards a holistic and effective cybersecurity program.



Third-party software and applications that connect to your core systems and data rapidly expand your digital attack surface. Without a way to see, assess and scale the security of that expanded perimeter, your company is vulnerable to third-party breaches.

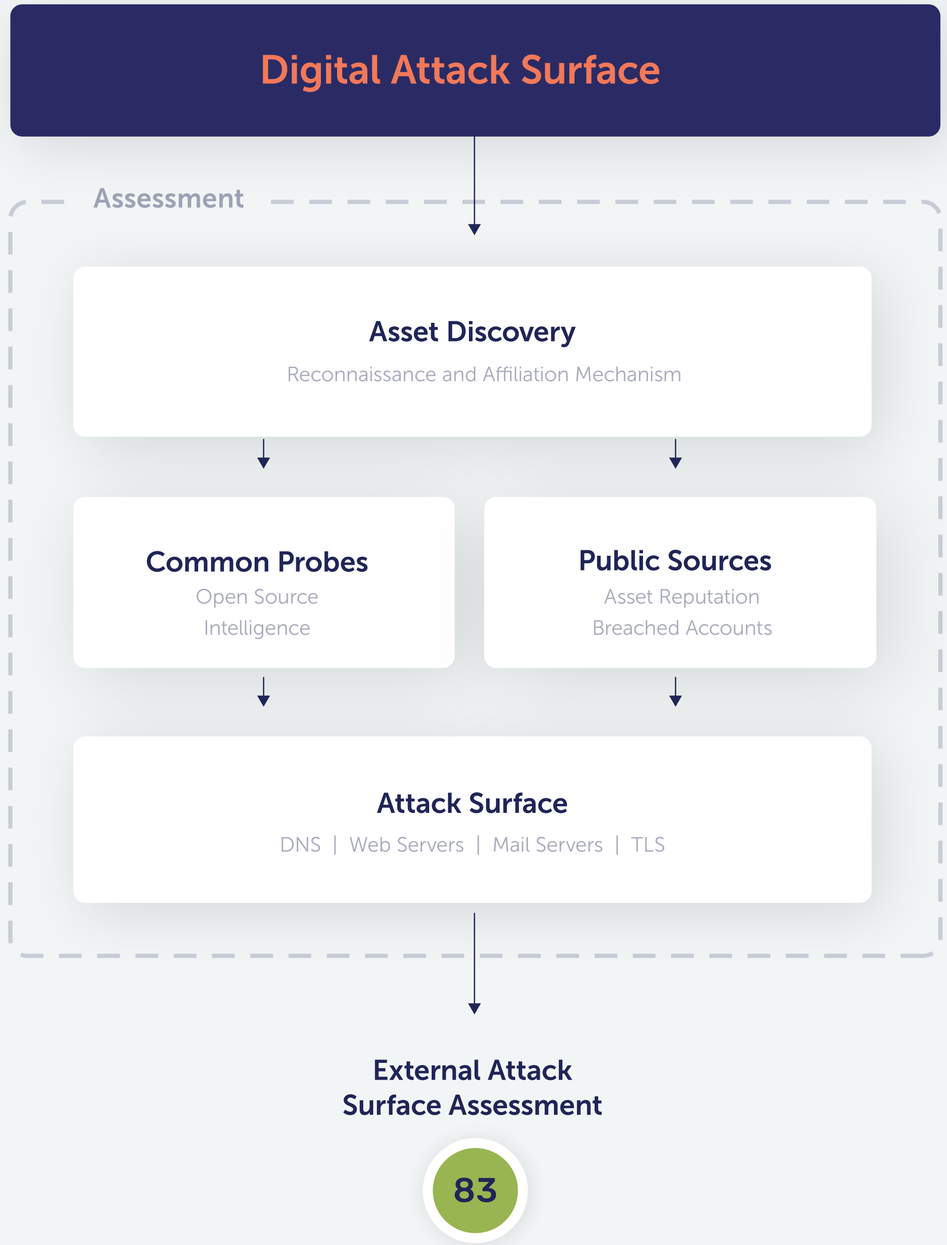
You must understand how your third parties' assets impact your business: who owns them and in which business processes they are used. Panorays evaluates the attack surface of both you and your vendors by performing hundreds of tests, such as collecting information on exposed assets or checking for lack of security best practices. Let's take a closer look.



01

Assess your attack surface

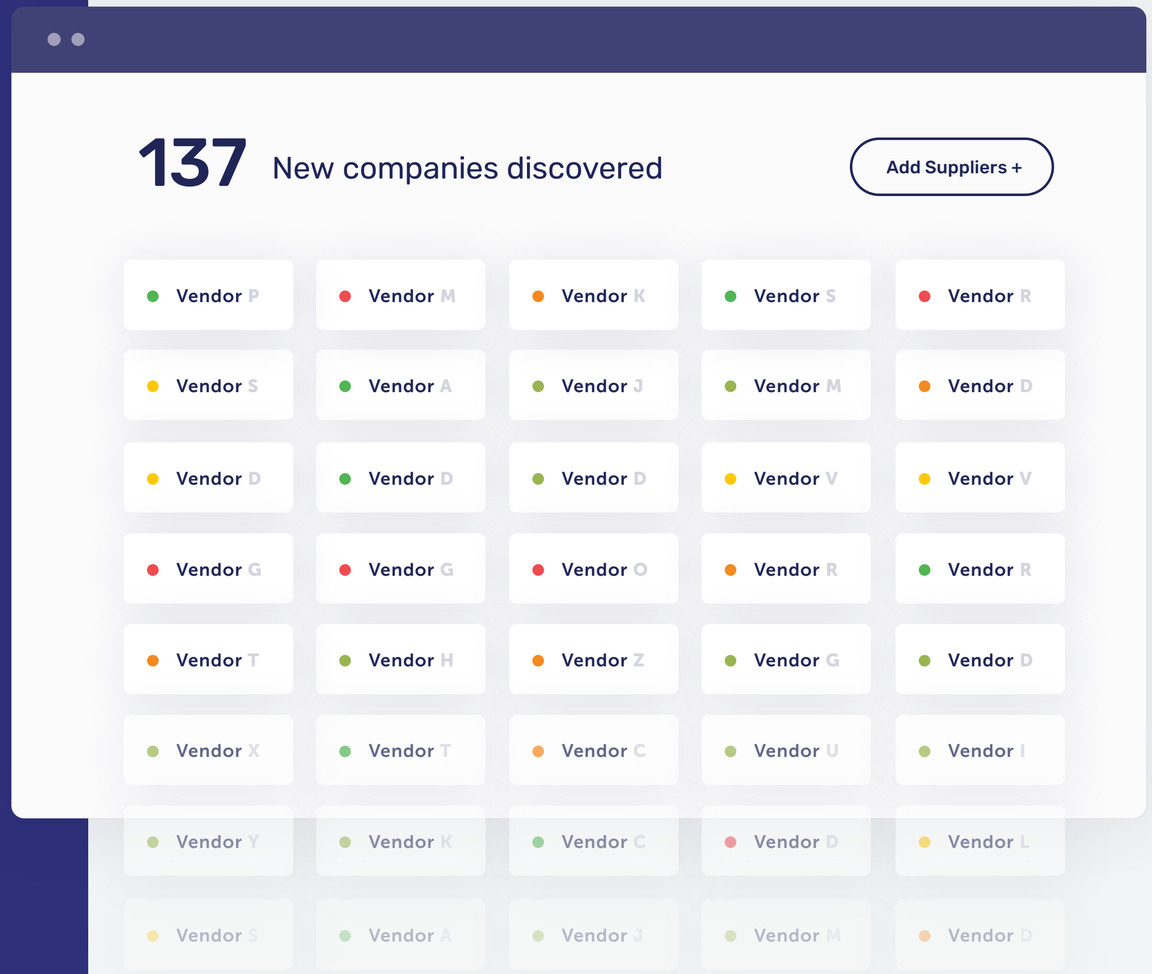
Unknown, incomplete, or inaccurate view of your digital attack surface can result in breaches, fines, lawsuits and loss of customer trust. Panorays' non-invasive enterprise risk assessments provide an overview of your organization's digital perimeter by mimicking the actions of thousands of threat actors. Panorays pinpoints your organization's vulnerabilities, explains their severity and then provides mitigation strategies so you can address them. As you improve your security, the changes are automatically reflected in your enterprise risk assessment.



02

Discover your third parties

Before you can assess your third parties, you need to know who they are, what their digital assets are and how they connect to your network. Panorays automatically discovers your technology relationships—some of which may be third parties—and their technology relationships as well. Panorays needs only a single asset, usually the company's main domain, to discover all of the company's attack surface, domains, subdomains and IP addresses. Panorays will uncover old suppliers and freemium subscriptions that you may not have used for years, but that still have access to your data.

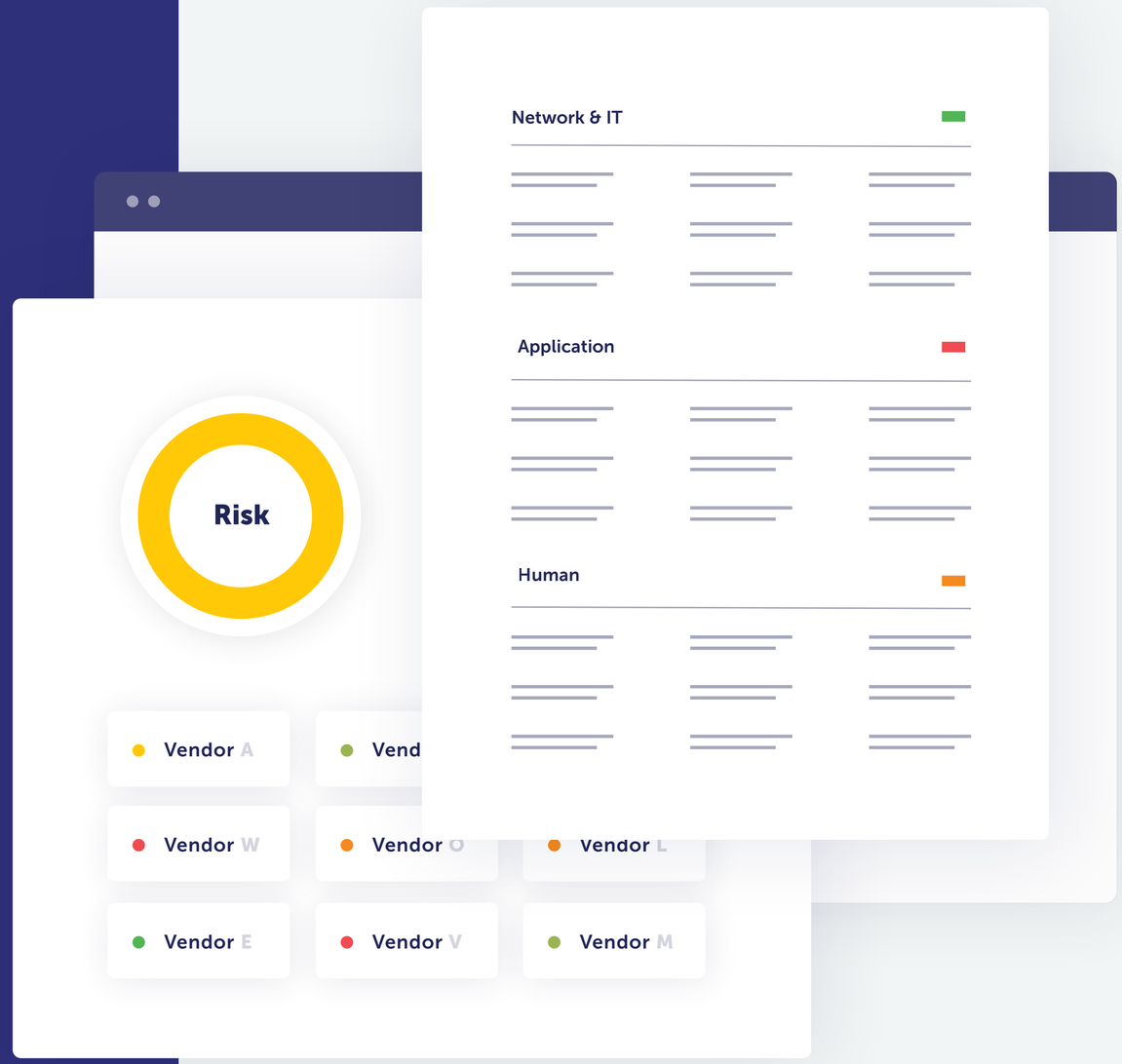


03

Assess your vendors

Panorays non-intrusively evaluates all your vendors' attack surfaces, assessing how they are connected to your infrastructure, across network & IT, application and human layers, including web, email and DNS servers, web applications and employees' social posture.

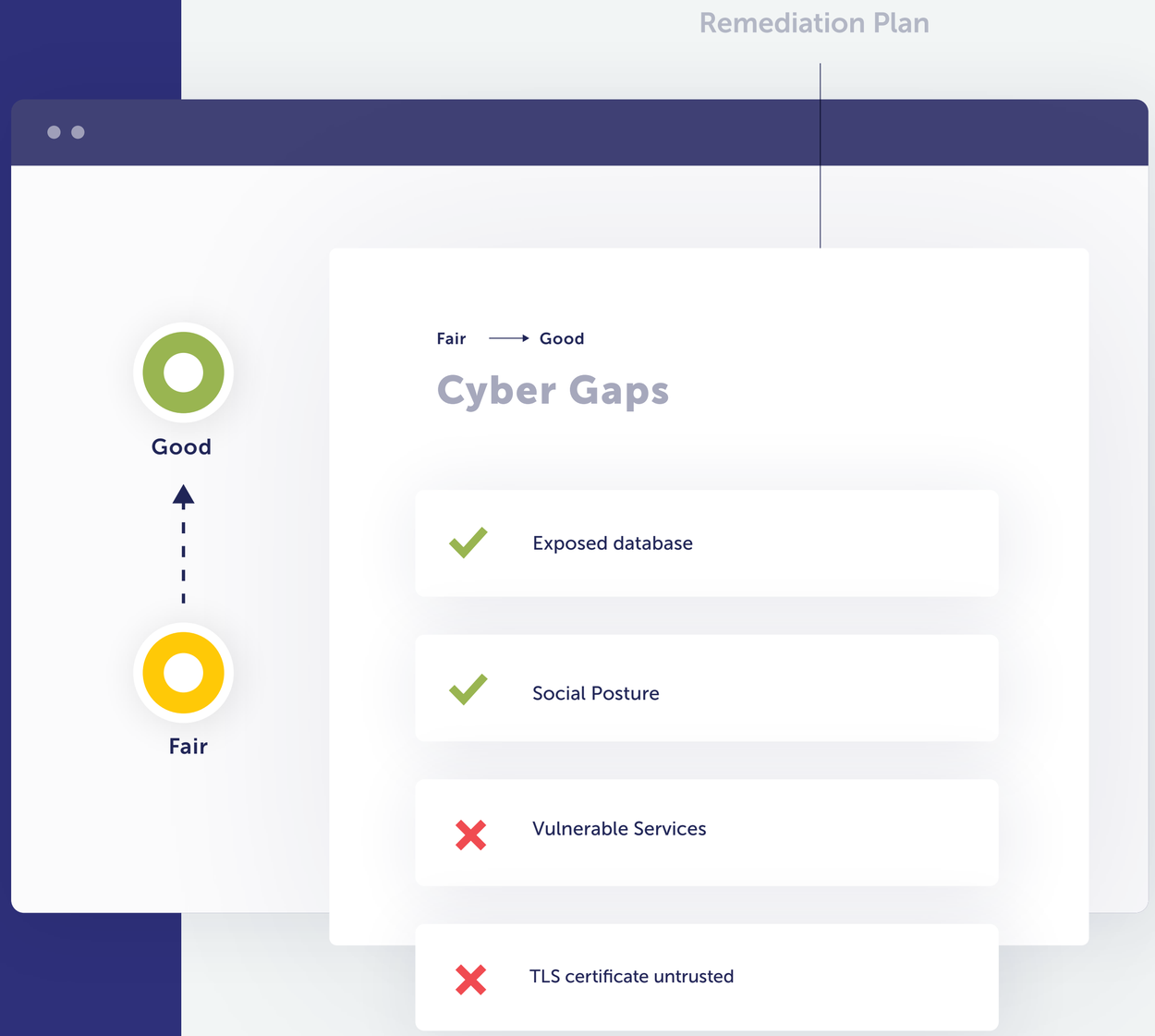
This external mechanism delivers quick results, typically within hours, while maintaining an extremely high accuracy rate. Assessment data is collected from both public sources, such as asset reputation feeds; and common probes, such as sending an empty email to see whether a destination actually exists. Example findings 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, such as breached credentials of employees or responsiveness of the security teams to patching vulnerabilities—and is the only platform that does so.



04

Receive actionable insights

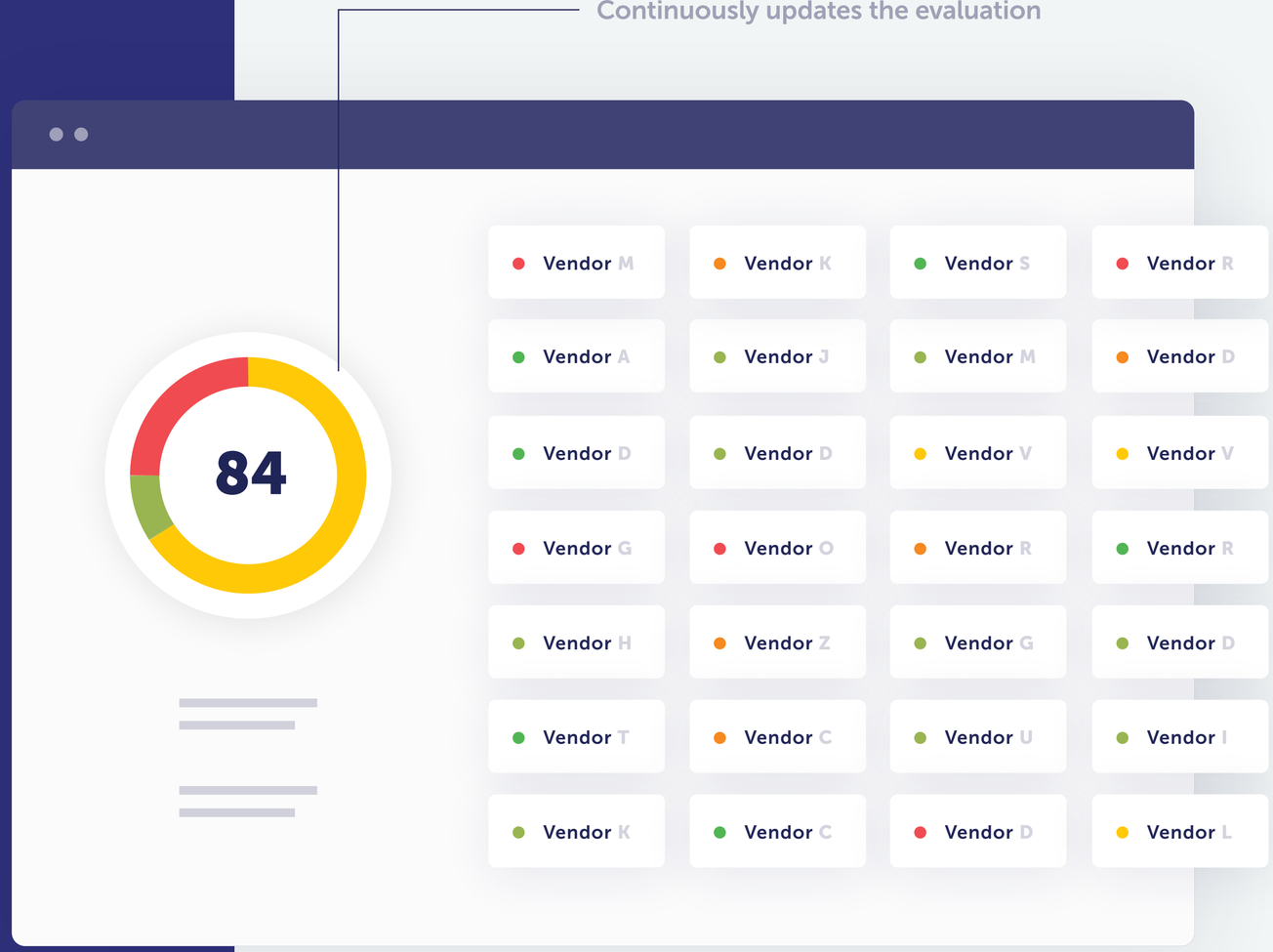
Panorays provides these insights so you can be proactive about remediating them and gain control of your third-party security risk. Panorays aggregates the data about your third parties' security into an easy-to-understand framework, so you can correctly identify how each third party is integrated into your environment, how they can mitigate cyber gaps, and if they don't, what type of compensating controls you can implement. These action items enable you to quickly move business forward securely. Lastly, Panorays' business context function allows you to prioritize vendors in terms of inherent risk.



05

Monitor continuously

A point-in-time view of suppliers doesn't keep up with the evolving risk landscape and attackers are waiting to jump on new opportunities. A sudden change in a supplier's attack surface, such as a new mail server or public cloud provider, can rapidly expand their attack surface faster than they can protect it, leaving your organization at risk. Panorays continuously monitors and evaluates your suppliers, and you receive live alerts about any security changes or breaches to your third parties, giving you ongoing visibility, insight and control.



The Panorays difference

Panorays offers an automated, comprehensive and easy-to-use third-party security platform that manages 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.

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, Greenfield Partners, BlueRed Partners (Singapore), StepStone Group, Moneta VC, Imperva Co-Founder Amichai Shulman and former CEO of Palo Alto Networks Lane Bess. Visit us at www.panorays.com

Panorays

Any questions about getting started with Panorays?
We are happy to help. info@panorays.com