

## Solution Brief

# Third-Party Cyber Risk Management

Identify, validate, prioritize, and confirm mitigation of cyber threats and vulnerabilities

### Distributed attack surface

Managing distributed risk associated with hundreds and even thousands of vendors, suppliers, and partners is quickly becoming the defining cybersecurity challenge in today's increasingly complex environment. As organizations have increased the number and variety of third parties they work with, they have simultaneously exposed their enterprises to the vulnerabilities of those partners. The ugly truth is that 93% of 1,200 chief information officers (CIO), chief information security officers (CISO), and chief procurement officer (CPO) surveyed in the 2021 Global Supply Chain Cyber Risk Report suffered a breach at the hands of a third party in the past 12 months. Vendors, suppliers, and partner ecosystems are critical components organizations' own attack surfaces.

### BlueVoyant Terrain: 3PR

BlueVoyant identifies and mitigates cyber threats and vulnerabilities in third-party ecosystems – not just by identifying risk, but by validating, prioritizing, and confirming mitigations have taken place through direct relationships with third parties. BlueVoyant's Risk Operations Center (ROC) is staffed by our team of world-class cybersecurity experts, has access to the largest globally distributed private and open-source datasets, and automates previously manual mitigation processes. BlueVoyant leverages the strength of these attributes to help businesses and government entities protect themselves against distributed risk.

### Key benefits/differentiators

- Gain visibility, prioritization, and remediation action plans for events and vulnerabilities
- Enact mitigation via direct engagement with third parties on the customer's behalf
- Identify all third parties impacted by zero-day vulnerabilities and guide mitigation efforts at each impacted vendor within hours - not days
- Map findings against multiple regulatory and specific control frameworks
- Reflect extended digital ecosystem needs with tailored proprietary and commercially available data

# Key features and capabilities

## Scalability

- Continuous monitoring of the complete third-party ecosystem with existing resources
- Deployment takes place in weeks rather than months

## Remediation with Vendor Collaboration

- Platform delivers visibility, evidence, prioritization, and specific remediation action plans for events and vulnerabilities
- Analysts work directly with third parties on the company's behalf to resolve issues

## Proactive Threat Hunting

- Proactive reviews of newly identified cyber risks and Zero-days across the third-party ecosystem
- Analysts contact vendors directly to remediate in advance of any escalation resulting from a potential incident

## Advanced Cyber Risk Identification Capabilities

- Superior data collection and machine learning enabled analytics result in complete view of the distributed third-party attack surface
- Analysts curate the findings to remove false positives

## Real-Time Data

- Incorporates proprietary threat intelligence that can expose active targeting and identify imminent threats
- Provides real-time visibility into third-party risk status with alerts, confirmed incidents, and remediation status

## Alignment with Control Frameworks and Risk Appetite

- Maps findings against multiple regulatory and company-specific control frameworks
- Sets risk appetite in line with desired thresholds to manage and drive risk reduction to agreed threshold



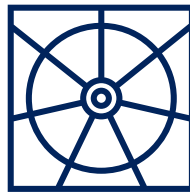
### Easily deployed

Monitoring begins by loading third party's name and domain



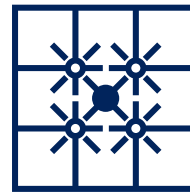
### Continuous monitoring

For existing and new externally visible critical vulnerabilities



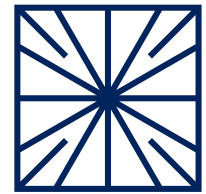
### Risk operations center

Quickly responds and directs remediations



### Fully scalable

Scales to easily cover tens of thousands of suppliers continuously



### Immediately actionable

All escalated findings include immediate actions necessary

Contact Spirity Enterprise Zrt. to learn more.

Éva Szunomár | [hello@spirity.hu](mailto:hello@spirity.hu) |

**BlueVoyant**