BlueVoyant

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 over 1,200 CIOs, CISOs, and CPOs 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. Your vendors, suppliers, and partner ecosystems are now critical components of your own attack surface.

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

BlueVoyant Third-Party Cyber Risk Management

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. We leverage the strength of these attributes to help businesses and government entities protect themselves against distributed risk.

> "It's continuous and collaborative, and fits into our way of working and importantly our priorities. BlueVoyant has built a service from the ground upwards that is an extension of our current TPRM program, giving us scale." - One of the UK's largest financial services institutions

About BlueVoyant

BlueVoyant is the only company that brings end-to-end internal and external cybersecurity into an integrated, modular solution. BlueVoyant's Ecosystem Cyber Defense (ECD) Platform™ is designed to protect organizations from sophisticated cyber threats targeting their infrastructure, applications, data, and executives. The ECD Platform is led by advanced machine learning, technology, and cutting-edge data collection and analytical capabilities, all enhanced by unrivaled cybersecurity expertise.

BlueVoyant

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

Get Started

Simply work with BlueVoyant's Risk Operations Center to determine digital assets and we'll begin discovering imminent cyber threats across your distributed ecosystem. To learn more about BlueVoyant Third-Party Cyber Risk Management platform or to schedule a demo please email us today at contact@bluevoyant.com

BlueVoyant

Solution Brief

BlueVoyant Digital Risk Protection

Take Fast Action to Identity and Mitigate Cyber Threats

Gaining visibility necessary to guard against external threats to your business requires ongoing monitoring and mitigation. Without extensive data sources including DNS data sets, clear, deep, and dark web, instant messaging, PII breach data, active scan data, and BGP data, it's impossible for organizations to guard against fraud campaigns, credential loss, data leakage, and threats to key executives.

BlueVoyant DRP

BlueVoyant provides organizations with the most comprehensive real-time visibility to external digital threats by continuously monitoring domains and websites, social media, apps in official and clandestine stores, clear, deep and dark web, and instant messaging. BlueVoyant's extensive global coverage, data science, and analyst expertise, enables identification of malicious "look-alike" attacks, live phishing pages, and more. A competitive differentiator, we have an unmatched ability to take action on your behalf to eliminate threats to your brand, employees, and customers.

Key Benefits

- Unmatched, comprehensive data sources including DNS data sets, instant messaging traffic, PII breach data, clear, deep, and dark web to monitor billions of threat actor sessions per month
- Exclusive, unlimited take-down capabilities due to cooperative agreements with domain registrars that no other providers have
- 24 hour take-downs of phishing sites/domain look-alikes, social media, and app stores
- Automated alerts, threat prioritization, and ongoing monitoring backed up by our expert analyst team, 24/7, in our Digital Risk Operations Center
- Product automation supported by expert analysts. Individual analysts assigned to customers
- Unique Executive Cyber Guard includes sentiment analysis

About BlueVoyant

BlueVoyant is the only company that brings end-to-end internal and external cybersecurity into an integrated, modular solution. BlueVoyant's Ecosystem Cyber Defense (ECD) Platform™ is designed to protect organizations from sophisticated cyber threats targeting their infrastructure, applications, data, and executives. The ECD Platform is led by advanced machine learning, technology, and cutting-edge data collection and analytical capabilities, all enhanced by unrivaled cybersecurity expertise.

Features and Capabilities

Digital Brand Protection

Monitors your external attack surface to protect against web, social media, and app impersonations in more than 230 official and illegitimate app stores. Proactive detection and unlimited takedowns of phishing sites and domain look-alikes as part of BlueVoyant's end-to-end solution. Monitors fake social media accounts in leading platforms including Facebook, Twitter, Instagram, and LinkedIn.

Account Takeover Monitoring

BlueVoyant monitors the clear, deep, and dark web for threat actor activity to prevent emails, usernames, and passwords from being compromised or sold by threat actors. With a 24/7 SLA, immediate notifications of exposed credentials enables organizations to minimize fraudulent activity and take immediate action.

Fraud Campaigns Discovery

Monitoring private groups in instant messaging applications including WhatsApp, Telegram, ICQ, and Discord, BlueVoyant defends against the use of stolen customer data, compromised payment cards and bank accounts, preventing the use of hundreds of newly stolen credit cards advertised and sold every day.

Data Leakage Detection

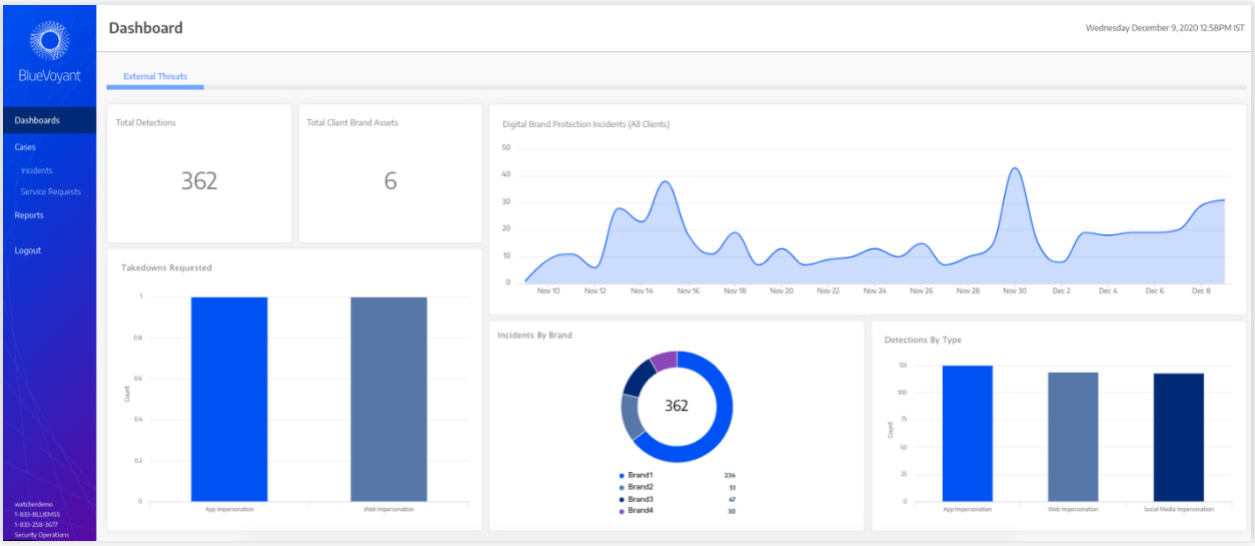
Our threat analysts scour the deep and dark web paste sites, code repositories, social media platforms, and instant messages, and through our avatars, interact with threat actors to provide proactive data leakage detection. BlueVoyant then provides detailed information about the event, the source, and suggested remediation.

Executive Cyber Guard

The threat of cyberattacks is not only the concern of large organizations, but also presents an ongoing threat to individuals in your executive suite. The resulting harm may be financial, reputational, and physical. BlueVoyant continuously monitors the exposure of personal information, stolen credentials, account hacking and takeover, online impersonation, identity theft, and more.

External Attack Surface Analysis

Extensive public and proprietary global internet data provides unmatched capabilities to assess customer network vulnerabilities. BlueVoyant maps customer network landscape by assessing hosting strategies, network dependencies, registration norms, and interactions between internal assets and external entities.



Get Started

To learn more about how BlueVoyant's DRP solution's best-in-class data, advanced analytics, and threat intelligence experts combine to provide the industry's leading detection, remediation, and cyber threat prevention, please visit www.bluevoyant.com/services/digital-risk-protection