ESG

Enterprise Strategy Group | **Getting to the bigger truth.™**

First Look

BlueVoyant Managed Security Services

Date: April 2020 **Author:** Jack Poller, Senior Analyst

Cybersecurity Challenges:[1]

44%

Have a problematic shortage of cybersecurity skills

67%

With a cybersecurity skills shortage have been targeted by ransomware in the last year

73%

With a cybersecurity skills shortage will increase their usage of third-party professional services

Protecting an organization from a cyber-attack has become more difficult due to the rapidly changing and evolving threat landscape, the growing attack surface as organizations shift to support mobile and remote workers, and the increased volume of alerts. These challenges are exacerbated by the global cybersecurity skills shortage, making it harder for small to medium organizations to appropriately staff cybersecurity teams. Attackers are increasing in sophistication, gaining knowledge through experience, and developing stealthy attacks targeting key personnel in weakly protected organizations. Attackers are also threatening smaller organizations with automated tools, reducing the adversary's cost and effort and enabling them to target a larger population at scale.

BlueVoyant

BlueVoyant Business Units

The founders of BlueVoyant were cognizant of three cybersecurity truths: organizations' cybersecurity budgets are not infinite; they cannot acquire all the tools they need; and they can't find the people to run the requisite tools to protect their organizations. Thus, BlueVoyant was created to provide cybersecurity protection using the best-in-breed cybersecurity technology operated efficiently and effectively by experienced and knowledgeable staff.

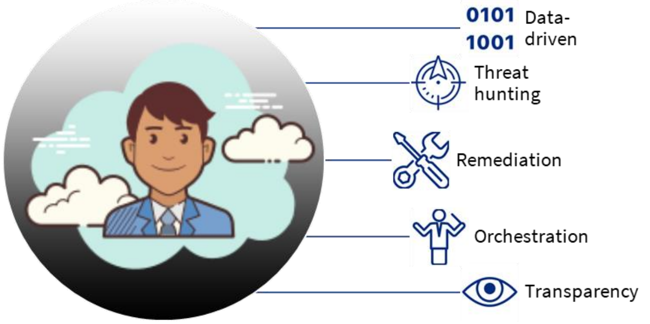
The threat intelligence team develops proprietary threat intelligence using the world's largest passive DNS database, propriety tools, and a team of threat researchers. BlueVoyant customizes threat research to deliver timely, actionable intelligence specific to each customer and their supply chain. The professional services team is dedicated to helping organizations evolve their cybersecurity capabilities faster than they evolve their business operations, enabling organizations to proactively reduce risk.

BlueVoyant designed the managed security services team to help organizations achieve the same level of security as large, well-defended enterprises that have dedicated security teams and security operations centers (SOCs). BlueVoyant's team of experts are data-driven, using BlueVoyant's custom threat intelligence and cybersecurity telemetry to provide targeted security. The team remediates attacks and proactively hunts for preexisting threats; all activities are coordinated using security automation, orchestration, and response (SOAR) tools. And BlueVoyant is completely transparent, providing organizations with access to all cybersecurity data and activities through BlueVoyant's custom-developed user console.

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

ESG Demo Highlights

ESG evaluated Wavelength, BlueVoyant's client platform, and held in-depth discussions with BlueVoyant's managed security services experts.



BlueVoyant Managed Security Services

Managed Security Services

- BlueVoyant's managed security services (MSS) enable organizations to extend security coverage with full time 24x7 SOC data-driven analysts, threat intelligence researchers, threat hunters, and attack remediation staff.
- BlueVoyant recruited cybersecurity professionals from the NSA, FBI, GCHQ, US Airforce, Israel's Unit 8200, and other elite cybersecurity teams, enabling organizations to leverage the combined 600+ man-years of experience for the best defense and attack response.
- BlueVoyant starts with proactive security assessments, penetration tests, maturity assessments, and vulnerability assessments, developing the best programs to protect the organization "left of boom" (before the attack).
- The Threat Fusion Cell (TFC) analyzes threat intelligence and maps the organization's external attack surface to create a custom security profile providing for rapid identification of relevant or targeted emerging threats.
- BlueVoyant's MSS are data-driven, using threat intelligence, NextGen AV, EDR, and SIEMs from partnerships with Microsoft, Crowdstrike, Carbon Black, and Splunk, enabling rapid detection of active attacks.
- BlueVoyant's SOC analysts contain and remediate attacks, and update security controls to prevent future occurrences, while the threat hunting team investigates unknown threats based on adversarial behaviors detected by cybersecurity controls.
- BlueVoyant coordinates all "right of boom" activities using Demisto with custom-developed playbooks, providing consistent, orchestrated, targeted, rapid response.
- Wavelength provides the organization's security professionals and executive management with complete visibility into all cybersecurity activities, including threats, alerts, responses, and remediation efforts, along with routine summary reporting.
- Dedicated client experience managers periodically meet with each organization, help organizations fine-tune BlueVoyant services for their environment, advise in infrastructure and architectural weaknesses that help reduce the attack surface, and advocate for the organization within BlueVoyant.

First Impressions

Attackers never sleep, forcing organizations to respond to threats all day every day. Yet many organizations are unable to identify, afford, or acquire the appropriate cybersecurity tools, and are equally unable to recruit the requisite experienced staff to manage their cybersecurity operations 24x7. This leads to weaknesses or even holes in the organization's cybersecurity defenses, increasing the risk of compromise.

ESG's first impression is that BlueVoyant checks all the boxes. BlueVoyant prides itself on having a dedicated team of experts trained by elite cybersecurity agencies defending critical assets. BlueVoyant is both proactive, researching and applying the best defensive security controls for your environment, and reactive, responding to threats when they happen in your environment, 24x7, using the best and most appropriate tools. All activities are coordinated, tracked, and made completely visible to you at any time. All in all, a great first impression!