

REPORT REPRINT

# BlueVoyant looks to bring enterprise cyber defense capabilities to all size organizations

**OCTOBER 30 2019**

**By Aaron Sherrill**

Armed with capital, expertise and unique partnerships, BlueVoyant is bringing together threat intelligence, managed security services and professional services to help organizations gain access to technology, intelligence and expertise that would otherwise be unattainable or cost-prohibitive.

---

THIS REPORT, LICENSED TO BLUEVOYANT, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.



### Introduction

As reliance on technology continues to grow, organizations of all sizes are discovering that cybersecurity risks and threats are impacting almost every aspect of their operations. Each year the number and impact of data breaches and security incidents continue to increase as an organization's IT ecosystem becomes increasingly dispersed and disparate. Although organizations are spending an increasing amount on securing critical infrastructure and data, many organizations lack the combination of resources, technology, expertise, capabilities and processes to protect sensitive data and business operations. Armed with capital, expertise and unique partnerships, BlueVoyant is bringing together threat intelligence, managed security services and professional services aimed at helping organizations expand their cybersecurity capabilities and gain access to technology, intelligence and expertise that would otherwise be unattainable or cost-prohibitive.

### 451 TAKE

BlueVoyant is taking on a highly competitive security services market that remains confusing and frustrating for midsize enterprises. Faced with many of the same threats and security challenges as large enterprises, midmarket security teams are tasked with protecting and securing the enterprise with a fraction of the expertise, tools and budgets of their larger counterparts. Many of these turned to managed security services to help them improve their cybersecurity posture, but found most providers were either too small to address their complex needs at scale or too large to understand their business and provide cost-effective services. Designed for scale, transparency and the midmarket from the start, BlueVoyant should find the midmarket to be a greenfield opportunity for its managed security services.

### Context

Headquartered in New York, BlueVoyant was founded in 2017 by CEO Jim Rosenthal and executive chairman Thomas Glocer. Before cofounding BlueVoyant, Rosenthal served as the chief operating officer at Morgan Stanley, and Glocer as CEO of Thomson Reuters. The privately held company touts a robust management team that has served in a variety of cybersecurity leadership roles at well-known large enterprises and government organizations, including the NSA, FBI, the United Kingdom's GCHQ and Israel's Unit 8200.

Along with offices in New York, San Francisco, Washington DC, London, Madrid, Tel Aviv and Manila, the company also has two 24/7 global cybersecurity operations centers located in College Park, Maryland, and Tel Aviv. Since its launch, BlueVoyant has added over 300 managed security service customers spanning 15 verticals, including financial services, municipalities, manufacturing, and energy and utility providers, among others.

In May the company announced that it had closed an \$82.5m series B funding round at a valuation of over \$430m. The investment included participation from Fiserv, a financial services technology provider and original investor in BlueVoyant, as well as participation from new investors. The company has raised over \$207m to date.

BlueVoyant says its goal is to democratize cybersecurity and protect organizations of all sizes against agile and well-funded adversaries. While the company has developed some of its own IP, it largely partners with well-known cybersecurity technology vendors like Carbon Black, Claroty, CrowdStrike, Illusive, IronNet, Splunk, and others to deliver threat intelligence, managed security services, and professional services like incident response, cyber forensics and risk assessments.

### Managed security services

According to BlueVoyant, its managed security services enable organizations to achieve the same level of security as the largest and most well-defended enterprises. The company says it provides resource-constrained security teams with access to the technology, expertise and 24/7 services to solve complex security problems at scale.

BlueVoyant's cloud-based managed security services are designed for midmarket organizations that have identified their critical assets and security needs, but lack the resources and funding to address security at the scale needed to adequately protect the organization's digital assets. However, the company says its customer base spans from organizations with as few as 50 employees to enterprises with over 60,000 employees.

Built around technologies from key security vendors, the company has developed a client cybersecurity portal and platform to integrate, automate and orchestrate its security services stack; report on risk posture and compliance status; and provide customers visibility into BlueVoyant's SOC operations and investigations. The company's core managed security services include managed detection and response (MDR) and detection as a service (DaaS). BlueVoyant's endpoint-centric MDR service provides the technology and services to detect, block, contain, and investigate and remediate attacks and threats. BlueVoyant says its cloud-based automation and orchestration capabilities correlate multiple logs and threat intelligence sources, enabling faster MTTD and MTTR.

DaaS collects logs from applications and on-premises and cloud infrastructure, enabling BlueVoyant's security analysts to monitor network and security devices, track users, scan applications and analyze security-event analysis for advanced threats across the entire IT ecosystem. The company also offers managed SIEM services, network threat analysis, vulnerability management services and deception services.

### Threat Intelligence and professional services

BlueVoyant's Threat Intelligence Services monitor the external attack surface of each customer to assess emerging risks and deliver enriched, contextual and actionable intelligence. The company says the service leverages large proprietary data sets that combine traditional threat data with deep and dark web sources to identify vulnerabilities and risks specific to each customer's business. The service provides in-depth investigative support into attacks such as data theft, brand impersonation and phishing schemes, including providing advanced warning of impending cyber attacks.

BlueVoyant's professional services are designed to arm organizations with insight and expertise to improve their cybersecurity posture, address compliance requirements, and mitigate risks in the event of a security incident or breach. The company provides a range of professional security services, including incident response and remediation services, cyber forensics, risk assessments, consulting and proactive services.

### Partnerships

Strategic partnerships with Fiserv and IronNet have been a catalyst in BlueVoyant's growth. Fiserv, a global provider of financial services technology to banks, credit unions, securities brokers and other financing companies, teamed with BlueVoyant in 2018 to provide advanced cyber defense capabilities to banks and credit unions of all sizes. The service, called CyberProtect, delivers a managed security platform that addresses the unique needs of financial institutions and provides threat detection, response and remediation; regulatory compliance; and reporting capabilities.

## REPORT REPRINT

In March BlueVoyant announced a strategic partnership with IronNet to deliver advanced, collective cyber defense and threat-detection capabilities to small and medium-size energy providers in the United States. The service combines IronNet's IronDefense Network Threat Analytics Platform and IronDome Collective Defense Platform with BlueVoyant's threat intelligence, managed detection and response service, and global security operations center to ensure that critical services remain secure and uninterrupted.

### Competition

The midmarket is a prime target for managed security service providers. Local and regional MSSPs focused on small and medium-size enterprises will compete directly with BlueVoyant, and often have a perceived advantage because of their locality. Large and midmarket MSSPs such as Avertium, Masergy, N-Dimension, the Herjavec Group, Delta Risk, Vigilant, NuSpire, ReliaQuest and others are pursuing many of the same customers as BlueVoyant. Large global MSSPs and systems integrators like NTT, Unisys, EY, Trustwave, Verizon, BT and BAE are also moving downstream to pursue customers in the midmarket. BlueVoyant also competes with specialized MSSP and MDR providers that address specific security needs within the enterprise, such as ArcticWolf, Red Canary, Cyberint and eSentire.

### SWOT Analysis

#### STRENGTHS

Scaling operations and platforms and building trust can be a challenge for most any type of managed service provider. However, these capabilities often prove to be even more difficult for MSSPs, especially in the face of rapid growth. BlueVoyant's platform and business were designed from the start with scale and full transparency in mind. These capabilities should prove to be vital as the company looks to continue to build trust and rapidly grow into new industries and markets.

#### WEAKNESSES

The security services market is intensely competitive, with competition ranging from well-funded startups to large incumbents. As a relative newcomer to the market, the company will need to build brand recognition and demonstrate its competitive differentiation to stand out in the highly competitive and crowded security services space.

#### OPPORTUNITIES

The company has shown its vertical focus in areas such as finance and utilities to be advantageous. BlueVoyant should continue to build out partnerships and go-to-market strategies for specific verticals, bringing specialized managed security service offerings to the marketplace to meet nuanced needs and demands.

#### THREATS

BlueVoyant is ramping up to accelerate growth across Europe and Asia. Expansion will bring many new challenges to the company as it addresses security and service delivery demands in a complex, global landscape.