SOLUTION BRIEF

BlueVoyant Managed Detection and Response (MDR+)

Threat Actors are Increasingly Sophisticated, BlueVoyant Managed Detection and Response Can Help You Outpace Them

In a world of increasingly sophisticated cyber attacks, maintaining high quality defenses against constantly evolving threats is essential. Small and mid-sized businesses face the same fast-moving attackers as the largest enterprises, but with tighter budgets and fewer resources. Keeping up with well-financed threat actors on a limited budget is a monumental task for all organizations.

BlueVoyant Managed Detection and Response provides comprehensive endpoint protection that detects, blocks and contains malware, ransomware, zero-days, non-malware and file-less attacks automatically. We will identify the root cause of your breach and provide instructions on how to correct it.

Our Technology Platform matched with our team of cybersecurity experts within our Security Operations Centers (SOCs), allows us to move quickly, 24x7, to monitor, detect and send you actionable intelligence. Our Threat Intelligence data helps us to predict, detect, investigate, and contain attacks before they impact your business.

If a threat actor's sophistication allows them to infiltrate your network, BlueVoyant SOCs are prepared to respond immediately with remote endpoint incident remediation, led by investigators and cyber intelligence experts.

For more advanced threat detection, we offer Threat Hunting activities that are performed periodically to augment the automated detections with manual searches for suspicious activity.

Resource-constrained IT teams are overburdened trying to manage a variety of siloed cybersecurity products and respond to a constant barrage of alerts on all fronts.

Top of the line security tools are expensive to purchase and require a team of experts to install and manage.

BlueVoyant takes a unique approach that includes a sophisticated method of detecting threats faster with the ability to contain and remediate the incident in a timely matter.

Key Features & Benefits

Robust Technology Platform

BlueVoyant Technology Platform detects, blocks, and/or contains malware, ransomware, zero-days, non-malware and file-less attacks automatically.

Benefit: *You don't have to buy another technology or shoehorn in another layer of cyber security.*

Better Automation

Consolidated processes and workflows with orchestration and automation of security events and alerts is used to triage and reduce false positives. Reduces mean-time-to-resolve (MTTR) conducted by the SOC.

Benefit: *Faster resolutions and no more alert fatigue.*

Wavelength™ Client Portal

Our web-based portal has an easy to understand representation of your security program.

Benefit: *See the full context of incidents, assets, vulnerabilities and on-going investigations. In a world where other providers tell you what to do, we show you what we did.*

24/7 Security Operations Centers

Geographically diverse SOCs staffed by former government and leading private sector experts are supported by the BlueVoyant Technology Platform.

Benefit: *Experts are available and ready to handle alerts and attacks quickly long after your staff has gone home. SOCs minimize the impact of attacks and lower costs with real-time remediation and faster response times, continuously strengthening your security posture.*

Proprietary Threat Intelligence

Advanced Threat Intelligence is proprietary, open-source, and dark web intelligence leveraged to expedite triage and enrich investigations conducted by the SOC. Delivered as intelligence reports, new detections are outlined with classifications of threat indicators.

Benefit: *Greater threat intelligence translates into faster identification and remediation of security events. It also reduces the risk of data loss and business disruption due to successful attacks.*

Right-Sized Solutions

Reinforced service offerings like MDR+ work in concert with DaaS or Managed SIEM, as well as Vulnerability Management Services.

Benefit: *BlueVoyant is a cybersecurity force multiplier that is robust, relevant and right sized for your needs.*

Why Clients Choose Managed Detection and Response (MDR+)

The BlueVoyant team is led by cybersecurity experts from the some of the best defended organizations and government agencies around the world. We minimize the impact of attacks by utilizing pre-approved playbooks to automate threat response, reducing the time an adversary spends on your network. Every second counts when your network is under attack, we detect, investigate, and take action, so you don't have to.

About BlueVoyant

BlueVoyant is an expert-driven cyber security services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers and advanced threats.

Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry-leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials and headquartered in New York City, BlueVoyant has offices in Maryland, Tel Aviv, San Francisco, London, and Latin America.

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**