

MANAGED DETECTION, RESPONSE, AND REMEDIATION (MDR+)

Small-to-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.

MDR+ provides comprehensive endpoint protection that detects, blocks, and contains malware, ransomware, zero-days, non-malware and file-less attacks. Using a combination of automation and human analysis, BlueVoyant identifies the root cause of your breach and remediates for you.

Our technology platform, matched with a team of cybersecurity experts within our Security Operations Centers (SOCs), allows us to move quickly, 24x7, to monitor, detect, and respond with actionable intelligence. Our threat intelligence data helps us to predict, detect, investigate, and contain attacks before they impact your business.

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. BlueVoyant relieves alert and product fatigue by simplifying the information you receive while also managing your security for you.

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.

Right-Sized Solutions

Reinforced service offerings like MDR+ work in concert with DaaSSM or Managed SIEM, as well as Vulnerability Management Services. BlueVoyant is a cybersecurity force multiplier that is robust, relevant and right sized for your needs.

Why Clients Choose Us

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.

KEY FEATURES & BENEFITS

ROBUST TECHNOLOGY PLATFORM

Detect, block, and/or contain malware, ransomware, zero-days, non-malware and file-less attacks automatically. **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. Our SOC experts reduce the mean-time-to-resolve (MTTR). **Faster resolutions and no more alert fatigue.**

24/7 SECURITY OPERATIONS CENTERS

BlueVoyant SOC's monitor the collection of cyber security data and are ready to respond to anomalies. **The SOC can respond to security events 24/7, giving you peace of mind that breaches can't spread unnoticed.**

CUSTOM CORRELATIONS

BlueVoyant experts help you to generate custom correlations and content. **Our fully trained and certified experts set your IT staff up for success and allow you to make sense of all the data.**

WAVELENGTH™, CLIENT PORTAL

Our web-based portal has an easy to understand representation of your security program. **You have full event visibility and access to at-a-glance insights and compliance reports.**

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. **Greater threat intelligence translates into faster identification and remediation of security events.**