# Detection-as-a-Service℠


BlueVoyant

# INTRODUCTION

"BlueVoyant offers the private sector exceptional cyber defense capabilities through our unique data assets, world-class threat intelligence experts, and managed security services. Helping to defend businesses around the world against well-developed cyber attackers, we excel in delivering unparalleled visibility and insights for our customers. At our core, we believe in providing resource-constrained organization of all sizes with the same level of cybersecurity previously only available to the largest and most well-defended businesses and government agencies."

Jim Rosenthal, CEO | Former Chief Operating Officer of Morgan Stanley
Past Chairman of the Securities Industry and Financial Markets Association and its Cybersecurity Committee.

# OUR SERVICES

## Threat Intelligence

## Managed Security Services

## Professional Services

## About BlueVoyant

A first-things-first cybersecurity company focused on delivering best-of-breed technology and outstanding customer service to businesses around the world. We believe in the democratization of cybersecurity - offering robust solutions and tools to businesses previously ignored and under-served. Through our advanced Threat Intelligence, Managed Security Services, and Professional Services, we excel in intelligence gathering, cybersecurity defense, and detection of attacks with response coupled with remediation. With global SOCs, we are prepared to protect the world over from well-financed threat actors and their newest tools of attack. Learn more at www.bluevoyant.com

BlueVoyant

# Detection-as-a-Service℠

BlueVoyant democratizes next-generation cybersecurity by delivering services that offer the same level of protection enjoyed by large enterprises available to small-to-mid-sized businesses at a fraction of the cost.

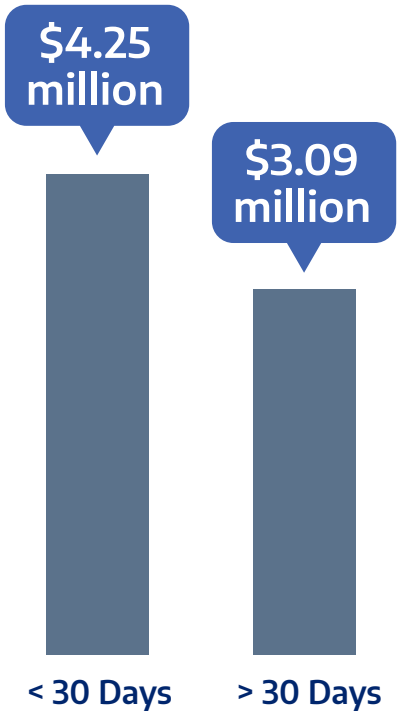
Detection-as-a-Service℠ from BlueVoyant provides a better, more cost-effective solution for IT teams who want SIEM-like capabilities without the expertise and expense required to do it themselves.

Our security analysts monitor network and security devices, track users, scan applications, and provide you with real-time, security event analysis across your monitored security infrastructure 24/7.

This service is supported by the BlueVoyant technology platform, a cloud-based ingestion, processing, and analysis system. This web-based platform generates reports based on the alerts that are analyzed by experts in BlueVoyant's geographically diverse security operations centers (SOCs).

Detection-as-a-Service℠ includes a proven implementation methodology which includes configuration necessary for provisioning of software agents; vendor software updates; collection, reporting, and notification of security events and device health events across your enterprise. Tools for self-service reporting and analysis are provided through Wavelength™, BlueVoyant's client portal.

**Companies that contained a breach in less than 30 days saved over $1 million versus those that took more than 30 days to resolve.**




Ponemon Institute 2018 Cost of a Data Breach Study sponsored by IBM

**Data Aggregation**

Data from the client's internal environment and cloud environment are aggregated and processed.

**Synthesis**

Data is indexed, correlated, and analyzed; the orchestration and automation of security events enhanced by our proprietary threat intelligence, filters background noise and identifies risks and security concerns.

**Reporting**

Information is triaged and presented within Wavelength™, the BlueVoyant client platform which reports on assets, vulnerabilities and threat intelligence updates so you can take informed action.

BlueVoyant

# Detection-as-a-Service℠

## OVERVIEW

**Log Collection:** Software agents are deployed on devices to enable collection of logs for security event monitoring. Using BlueVoyant virtual appliances, logs are aggregated and stored within Wavelength™, the BlueVoyant client portal.

**Security Event Monitoring:** Data is filtered, normalized, correlated, and analyzed to help identify anomalous, suspicious, or malicious behaviors indicative of threats in the monitored environment.

**Reputational Detection:** Utilizing proprietary and open source threat intelligence, BlueVoyant identifies threats based upon reputation by correlating inbound and outbound network traffic to monitor for suspicious and malicious domains and IP addresses.

**Investigation and Notification:** Once a suspicious event is detected or an automatic prevention activity occurs, an alert is generated and a security operations center analyst will investigate to determine whether or not there is a true positive, benign, or false positive and the client will be notified.

**Health Monitoring:** BlueVoyant monitors installed endpoint agent communications using the technology platform. We monitor log sources and generate an alert when a log source's output has not been received in a specified interval.

**Log Retention and Archiving:** All log data collected is stored for a period of 30 days for security event analysis and retained in archive storage for a period of one year, or as uniquely specified.

**Indicator Enrichment:** Indicators of compromise associated with detections within the monitored environment are automatically extracted, scored, and enriched leveraging open source and proprietary Threat Intelligence. Enriched indicators, assigned a reputation and classification, are visible within Wavelength™.


**The average cost for each lost or stolen record containing sensitive and confidential information has increased by 4.8% year over year to $148.**

Ponemon Institute 2018 Cost of a Data Breach Study sponsored by IBM

BlueVoyant

# Detection-as-a-Service℠

## FEATURES

Detection-as-a-Service℠ is supported by expert analysts who operate 24 hours a day, 7 days a week, across multiple locations within Security Operations Centers (SOC). Certifications held by the team include SANS GIAC, EC-Council, and ISC-2, as well as others.

Our experts leverage Wavelength™, BlueVoyant's client portal, to provide real-time visibility into detected alerts and to confirm incidents. This web-based portal enables approved client employees to interact with BlueVoyant's security operations center analysts, view all detected assets, and if applicable, view vulnerabilities.

Dashboards (representing a variety of content such as event volume, alert volume, detected assets, and analyst response actions) provide a snapshot of real-time company security posture. Reports are available through Wavelength™ and include client environment content related to alerts, incidents, indicators, assets, and vulnerabilities.

Updates on the threat landscape, sectorial, and intelligence summary reports are developed by the BlueVoyant Threat Fusion Cell - an elite team of cyber intelligence analysts and threat researchers focused on identifying and prioritizing information about threats using BlueVoyant proprietary and open source intelligence.

Orchestration and automation is a key component of our technology platform; it allows the BlueVoyant SOC to accelerate triage, reduce false positives, and improve mean-time-to-resolve (MTTR).

BlueVoyant's SOCs and engineering teams have developed automations to support Detection-as-a-Service℠ and continue to deliver new automations to improve the system daily. For example, an automated Emotet investigation helps with threat confirmation and faster response, which allows quicker triage to specific outbreak strains.

We have custom FFIEC and NCUA-ACET automations to assist financial institutions of every size. The growing number of security compliance management challenges adversely impact compliance. The mandatory risk assessments and compliance reports can be burdensome, but BlueVoyant has automated many of the FFIEC and NCUA-ACET compliance controls to reduce the time-intensive reporting process that is crucial.

Through a single-pane-of-glass view of your endpoint and network environment, you can address the need for access control, configuration control, and protective control compliance in order to reduce the risk of data breaches and malware attacks. You can help safeguard customer information and reduce fraud and identity theft.

# GETTING STARTED

During Introduction, key BlueVoyant and enterprise staff will engage you to learn your priorities, expectations, and deadlines. It is at this juncture that project timelines are established for both parties.

To begin, we will collect information specific to your business. This information will help us to provide organization-specific threat intelligence.

## Introduction

Facilitates information gathering and begins with project kickoff.

## Provisioning

Deploys software, sets configurations, and establishes connections.

## Tuning

Establishes the baseline of activities and highlights anomalies.

BlueVoyant will collect information about you to better understand your potential threats. This will include public and private information; such as your organization's industry, segment, key employees, key systems, and what types of digital assets you own, including domains and IP address segments.

## Client Experience Team | Primary Support

### Client Advisor

At Introduction you will be assigned an advisor who will act as your personal consultant and will help you as you interact with and navigate BlueVoyant services.

Your advisor will meet with you regularly to understand the evolving goals of your security program and will track key results. Your advisor will engage you should you have any significant security events occur.

### Implementation Project Manager

At the beginning of your DaaS℠ deployment, a BlueVoyant Implementation Project Manager will be assigned to you to assist you through the on-boarding process.

He or she will help you establish timeline/benchmark goals and select the sources and devices that will be on-boarded. His/her advice will help with matching and prioritizing work needed with your specific goals.

### Technical Account Manager

A BlueVoyant Technical Account Manager will be assigned to you to serve as your main point of contact beyond direct calls to the SOC. The technical account manager will assist with specific technology inquiries.

The Provisioning Phase focuses on the deployment of software to enable log collection and the configuration of devices and applications to deliver logs to the BlueVoyant technology platform for storage and analysis.

This phase includes the installation of BlueVoyant virtual appliances and establishes connectivity to BlueVoyant. Deployment of software agents to the identified endpoints and servers enable log collection and configuration of devices and applications to facilitate collection of logs.

### Log Collection

We collect all network traffic entering or leaving the environment, which is typically provided by means of access to firewalls (or equivalent) and all activities occurring on your endpoints including behavioral detections. This visibility can be provided either through Bluevoyant's managed detection and response services (available as a separate service), or by means of allowing us access to your deployed, next-generation antivirus agents or endpoint detection and response agents.

The BlueVoyant virtual appliance is a software package that enables log collection from external sources and delivers it to the BlueVoyant Technology Platform. It enables log collection and monitoring for devices and systems in which deployment of a log collection agent is not possible, such as a router or firewall.

We also use collection agents - software that is installed directly on client endpoints and servers to enable log collection and delivery to the BlueVoyant technology platform. This information is automatically aggregated and then BlueVoyant analysts provide a set of correlations and detections for commonly supported sources and platforms.

Nonstandard log sources may require our consultants or engineers to work with you to understand your unique set up, important event criteria and any custom reporting or real-time alerting requirements. If you require nonstandard log sources, Managed SIEM may be a better option for you. Our consultants and engineers can work with you to define important event criteria and any custom reporting or real-time alerts you need.

This most often includes configuration of network devices, such as firewalls, to direct Syslog content to a BlueVoyant virtual appliance for log collection.

Once all collection software has been deployed and sources have been appropriately configured to enable detection, an audit is performed to ensure system readiness.

### Correlation Development

BlueVoyant Engineering implements and delivers new correlations on a regular basis; requests for new correlations are prioritized by our product management process. If you have urgent correlations that you would like BlueVoyant to prioritize, we would be happy to provide pricing for this additional service.

## INDUSTRY AVERAGES


**The mean time to identify (MTTI)**


**The mean time to contain (MTTC)**

Ponemon Institute 2018 Cost of a Data Breach Study sponsored by IBM

BlueVoyant

# Detection-as-a-Service℠

During Tuning, BlueVoyant will use the first 14-30 days post installation to identify a baseline of the environment and familiarize ourselves with your technology set and its alerts. Tuning is a process of factoring out some of the expected noise of the client's environment and optimizing our service to provide better visibility and anomaly detection.

Once the collection and agent software has been deployed onto your environment, identification and contextualization of assets can occur. This includes identifying "Key Terrain" devices and applications as well as tagging assets and assigning asset criticality.

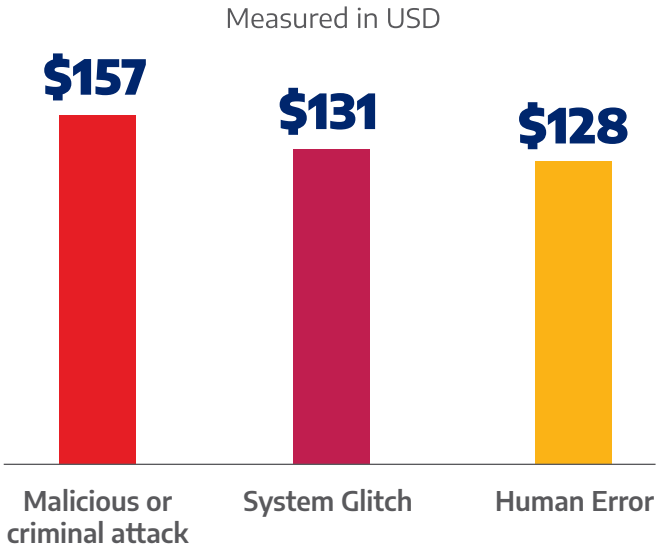
Please note, Detection-as-a-Service℠ is limited to monitoring the devices and sources subscribed for service as defined in detail in your Service Order. It does not include management or monitoring of any unsubscribed endpoint or intermediary log sources.

## Robust, Relevant, and Right-Sized Cybersecurity Options for Businesses of All Sizes

As part of our commitment to democratizing cybersecurity, BlueVoyant's services are designed to be mutually reinforcing but do provide significant value as stand alone solutions. Many clients choose additional services that are designed to work together to enhance and strengthen their security posture; this decision is generally based upon the size and expertise level of their IT staff. The addition of our Managed Detection and Response (MDR+) service adds protection to your DaaS℠ - no longer just detecting, but protecting your enterprise.

**Managed Detection and Response:** MDR+ relieves resource-constrained IT, allowing them to focus on the end-users while BlueVoyant provides the remediation and reports you need to stay informed. Our SOC analysts will respond to threat activities on the endpoints and intervene where applicable and appropriate.

## Per capita cost for three root causes of the data breach




Ponemon Institute 2018 Cost of a Data Breach Study sponsored by IBM

## Distribution of the benchmark sample by root cause of the data breach