# BlueVoyant

An Expert-Driven Cybersecurity Services Company

# Detection-as-a-Service℠


BlueVoyant

BlueVoyant

"BlueVoyant utilizes technology and expertise employed by the largest and most well-defended organizations to deliver protection to resource-constrained security teams. We believe in democratizing security by making best-in-class services and technology accessible to organizations regardless of size."

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

- Incident Response
- Professional Services

## Who is 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 underserved. Through our advanced Threat Intelligence, Managed Security Services, and Incident Response 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.

BlueVoyant

# Detection-as-a-Service℠

## Democratized Cybersecurity

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

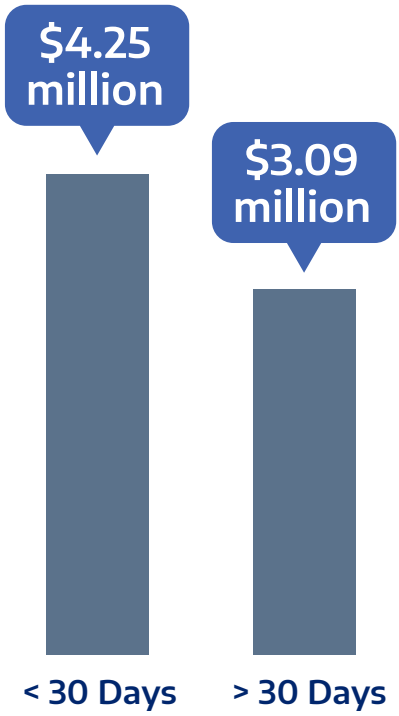
Detection-as-a-Service℠ from BlueVoyant provides a better, more cost-effective solution for IT teams who want SIEM-like capabilities without the expertise and expense required to do it themselves.

Our security analysts will 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 vs. those that took more than 30 days to resolve.**




| Data Aggregation | Synthesis | Reporting |
|---|---|---|
| Data from the client's internal environment and cloud environment are aggregated and processed | Collected Data is Correlated & Analyzed, then undergoes security orchestration and automation and compared against open source and proprietary threat intelligence | Information is triaged and presented within Wavelength™, the BlueVoyant Client Platform which reports on assets, vulnerabilities and threat intelligence updates so clients IT can take informed action |

BlueVoyant

# Detection-as-a-Service℠

Overview

**Log Collection:** Software agents will be 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 will be 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 will identify 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 will monitor installed endpoint agent communications using the Technology Platform. BlueVoyant will monitor log sources and will 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 will be 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.

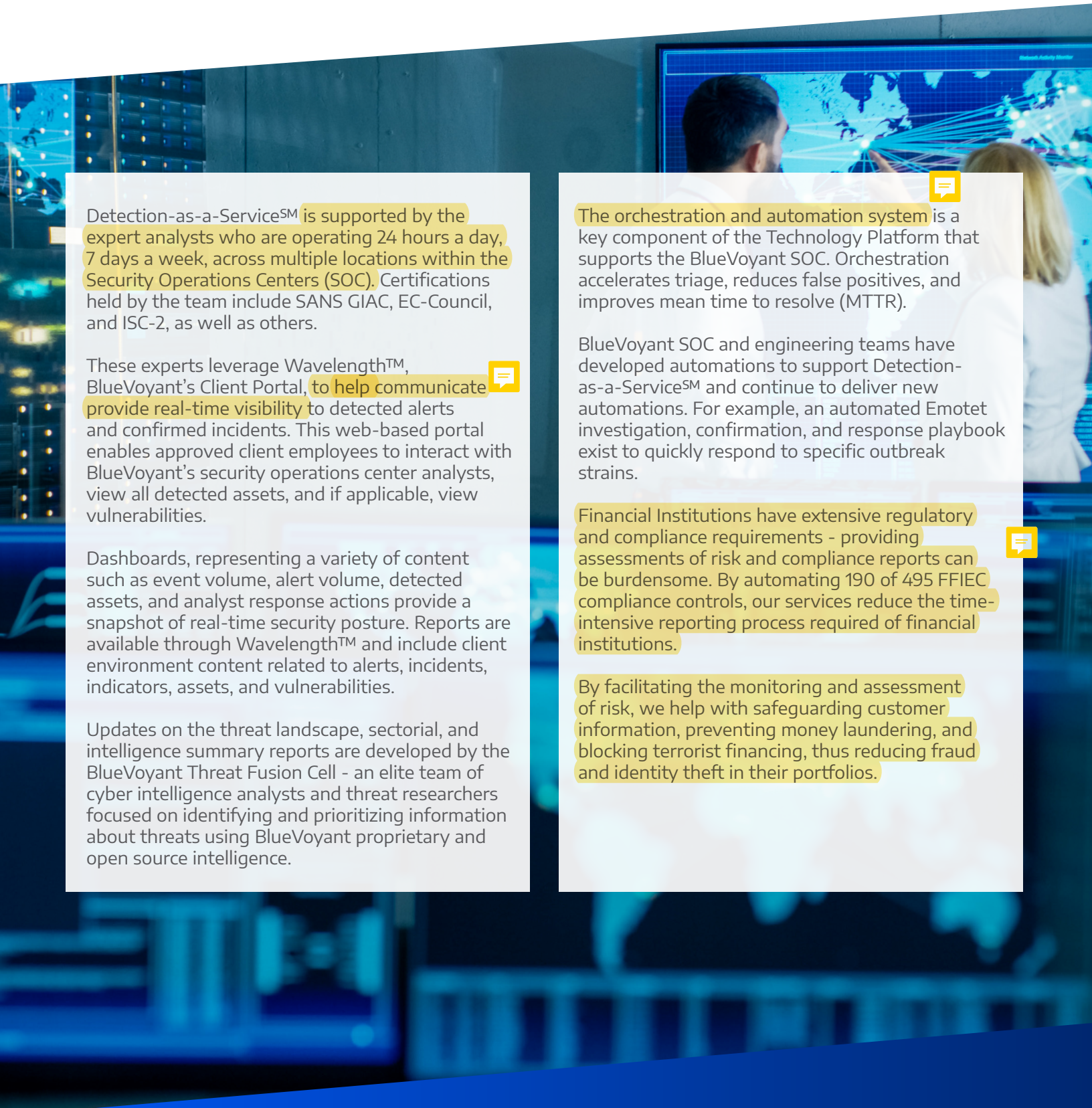
**Indicator Enrichment:** Indicators of compromise associated with detections within the monitored environment are automatically extracted, scored, and enriched leveraging open source and proprietary Threat Intelligence. Enriched indicators, assigned a reputation and classification, are visible within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


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

BlueVoyant

# Detection-as-a-Service℠

## Features



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

These experts leverage Wavelength™, BlueVoyant's Client Portal, to help communicate provide real-time visibility to detected alerts and confirmed 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 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.

The orchestration and automation system is a key component of the Technology Platform that supports the BlueVoyant SOC. Orchestration accelerates triage, reduces false positives, and improves mean time to resolve (MTTR).

BlueVoyant SOC and engineering teams have developed automations to support Detection-as-a-Service℠ and continue to deliver new automations. For example, an automated Emotet investigation, confirmation, and response playbook exist to quickly respond to specific outbreak strains.

Financial Institutions have extensive regulatory and compliance requirements - providing assessments of risk and compliance reports can be burdensome. By automating 190 of 495 FFIEC compliance controls, our services reduce the time-intensive reporting process required of financial institutions.

By facilitating the monitoring and assessment of risk, we help with safeguarding customer information, preventing money laundering, and blocking terrorist financing, thus reducing fraud and identity theft in their portfolios.

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 organizational specific threat intelligence. BlueVoyant will collect information about you to better understand potential threats. The types of information we will be gathering will include public and private information; such as, the organization's industry, segment, key employees, key systems and what types of digital assets they own, including domains and IP address segments.

## 1 Introduction

Facilitates information gathering and begins with project kickoff.

## 2 Provisioning

Deploys software, sets configurations, and establishes connections.

## 3 Tuning

Establishes the baseline of activities and highlights anomalies.

### Your Client Experience Team

#### Client Advisor

The Client Experience Team is your primary support resource. You will be assigned an advisor who will act as your consultant and will enable the best experience interacting with BlueVoyant services. Your advisor will meet with you regularly to understand the goals of your security program and track results. Your advisor will also engage with 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. The Implementation Project Manager will help you establish timeline goals and select sources and devices that will be on-boarded with the appropriate priority that aligns with your goals.

#### Technical Account Manager

A BlueVoyant Technical Account Manager will also be assigned to you to serve as your main point of contact beyond direct calls to the SOC.

BlueVoyant

# Detection-as-a-Service℠

## Provisioning

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 connectivity of BlueVoyant virtual appliances.

Deployment of software agents to the identified endpoints and servers will enable log collection and configuration of devices and applications to facilitate collection of logs. 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.

### 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 anti virus 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. Analysis depth is determined by your unique statement of work with BlueVoyant.

### 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.


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


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

BlueVoyant

# Detection-as-a-Service℠

## Tuning

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 end-point or intermediary log sources.

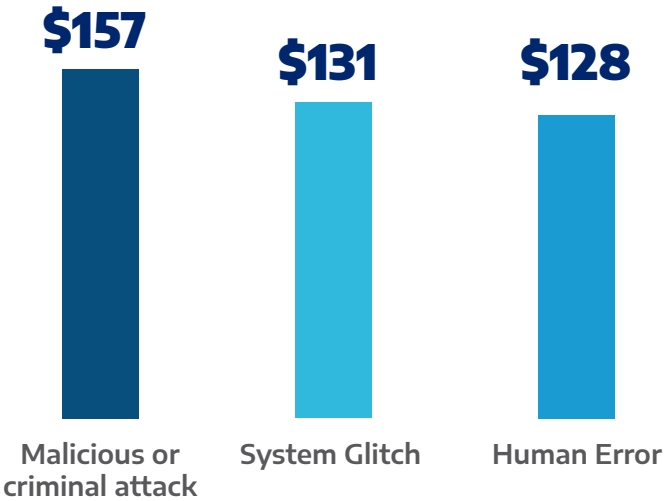
### Robust, Relevant, and Right-Sized Cybersecurity Options for Businesses of All Sizes

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.

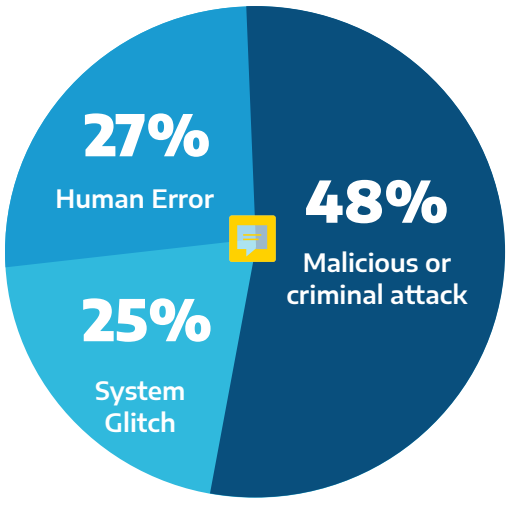
**Managed Detection and Response:** MDR+ relieves resource-constrained IT, allowing them to focus on the end-users while BlueVoyant provides the remediation and reports you need to stay informed. Our SOC analysts will respond to threat activities on the endpoints and intervene where applicable and appropriate.

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

Measured in USD




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



**Facing a Federal Financial Institutions Examination Council (FFIEC) assessment may feel like a daunting and insurmountable task for your organization to navigate. Financial institutions of every size face a growing number of security compliance management challenges that adversely impact their ability to successfully achieve FFIEC compliance.**

## TALE 1 - TYPICAL FFIEC COMPLIANCE MANAGEMENT CHALLENGES

| Security Expertise |
| --- |
| It is costly to hire and retain full-time specialized security experts to effectively deploy, integrate, and manage the numerous security products to meet ongoing control requirements. Additionally, your organization requires detailed security program documentation to effectively operationalize your security tools. |
| **Control Mapping** |
| With deployed security tools and policy documents defined, it can be difficult and time consuming to map existing tools to the 495 unique FFIEC CAT controls. Do you know if your current tools and documentation already satisfy the requirements or do additional gaps exist? |
| **Evidence Management** |
| Documenting evidence and preparing attestation content can make the audit process a difficult and time consuming endeavor. The process may also involve individuals and teams outside of IT and security that could introduce additional complexity and time. |

Instead of having the required information at their fingertips throughout the year, the majority of financial institutions struggle to gather required information, resolve previous findings, and shore up organizational security in the weeks and months leading up to the annual assessment.

Even if the institution has gathered documentation, and has implemented the previously recommended fixes, many remain unsure as to whether they will successfully pass their annual assessment.

The compliance enhancements to CyberProtect increase security and defense by delivering a global 24/7 managed security service (MSS) platform that eases compliance burdens and provides your financial institution with advanced managed detection and response, network monitoring, deception technology, around-the-clock SOC monitoring, remediation and threat intelligence so you can focus valuable resources on your business.

*"Fiserv and BlueVoyant are delivering a leading-edge cybersecurity solution that is both broader and deeper in its protection than any other solution we evaluated."*

**Elizabeth Macias, Chief Information Officer, Ponce Bank, New York, NY**

CyberProtect from Fiserv accelerates the maturity of your financial institution's security program and eases the FFIEC examination burden by providing approximately 100 of the required FFIEC controls assessed by the FFIEC Cybersecurity Assessment Tool (CAT). Future releases will provide support for additional controls.

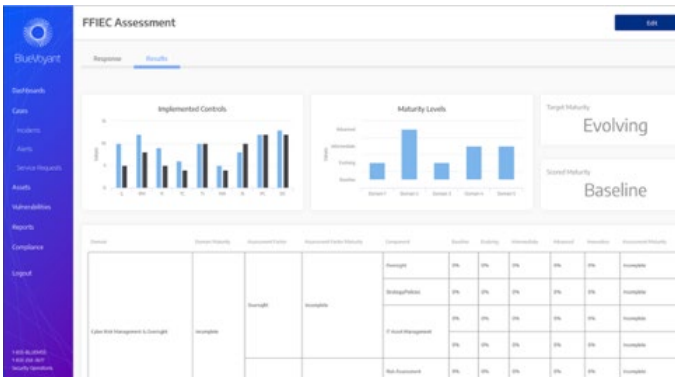
Unprecedented visibility and management of your cybersecurity program is now available through CyberProtect policy and process documentation, detailed scheduled reporting, and on-demand self-assessments.

## POLICY AND PROCESS DOCUMENTATION

A major cornerstone of any FFIEC-compliant organization is the creation, management, and measurement of the policies and processes that comprise the institution's security program. CyberProtect will produce a comprehensive document that explains what controls BlueVoyant MSS supports along with sample evidence to support the assessment process throughout the calendar year.

## DETAILED REPORTS

In order to measure the success and maturity of your FFIEC-compliant cybersecurity program, CyberProtect provides robust data collection, searches, and detailed reports mapped to specific FFIEC control areas. Provide your partners with the information they need from a single authoritative source to streamline all FFIEC assessment information requests.




## SELF-ASSESSMENT WIZARD

The self-assessment wizard enables institutions to manage their program and gain visibility into the organization's security risk, program maturity, and FFIEC assessment readiness throughout the year and, more importantly, leading up to the scheduled audit.

The continuous security and privacy of your financial institution's customer data is no longer a desired state, but an expected one. For more information on CyberProtect, call Fiserv at 800-872-7882.

## ABOUT BLUEVOYANT

BlueVoyant is an analytics-driven cybersecurity company whose mission is to protect businesses of all sizes against agile and well-financed cyber attackers by providing unparalleled visibility, insight, and responsiveness. BlueVoyant provides Advanced Threat Intelligence, Managed Security Services and Professional Services from offices in the United States, the United Kingdom, Israel, and Spain. Learn more at www.BlueVoyant.com.

## ABOUT FISERV

Fiserv, Inc. (NASDAQ: FISV) enables clients worldwide to create and deliver financial services experiences in step with the way people live and work today. For 35 years, Fiserv has been a trusted leader in financial services technology, helping clients achieve best-in-class results by driving quality and innovation in payments, processing services, risk and compliance, customer and channel management, and insights and optimization. Visit Fiserv.com and follow on social media for more information and the latest company news.

**Facing a National Credit Union Administration (NCUA) assessment may feel like a daunting and insurmountable task for your credit union to navigate. Credit unions of every size face a growing number of security compliance management challenges that adversely impact their ability to successfully achieve NCUA compliance.**

## TALE 1 - TYPICAL NCUA COMPLIANCE MANAGEMENT CHALLENGES

| Security Expertise |
| --- |
| It is costly to hire and retain full-time specialized security experts to effectively deploy, integrate, and manage the numerous security products to meet ongoing control requirements. Additionally, your organization requires detailed security program documentation to effectively operationalize your security tools. |
| **Control Mapping** |
| With deployed security tools and policy documents defined, it can be difficult and time consuming to map existing tools to the 495 unique FFIEC CAT and NCUA ACET controls. Do you know if your current tools and documentation already satisfy the requirements or do additional gaps exist? |
| **Evidence Management** |
| Documenting evidence and preparing attestation content can make the audit process a difficult and time consuming endeavor. The process may also involve individuals and teams outside of IT and security that could introduce additional complexity and time. |

Instead of having the required information at their fingertips throughout the year, the majority of financial institutions struggle to gather required information, resolve previous findings, and shore up organizational security in the weeks and months leading up to the annual assessment. Even if the institution has gathered documentation, and has implemented the previously recommended fixes, many remain unsure as to whether they will successfully pass their annual assessment.

The compliance enhancements to CyberProtect increase security and defense by delivering a global 24/7 managed security service (MSS) platform that eases compliance burdens and provides your financial institution with advanced managed detection and response, network monitoring, deception technology, around-the-clock SOC monitoring, remediation and threat intelligence so you can focus valuable resources on your business.

*"Fiserv and BlueVoyant are delivering a leading-edge cybersecurity solution that is both broader and deeper in its protection than any other solution we evaluated."*

**Elizabeth Macias, Chief Information Officer, Ponce Bank, New York, NY**

CyberProtect from Fiserv accelerates the maturity of your financial institution's security program and eases the NCUA examination burden by providing approximately 100 of the required NCUA controls assessed by the NCUA the Automated Cybersecurity Examination Tool (ACET). Future releases will provide support for additional controls.

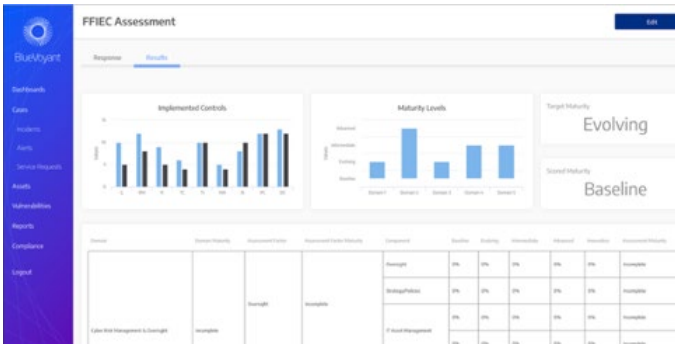
Unprecedented visibility and management of your cybersecurity program is now available through CyberProtect policy and process documentation, detailed scheduled reporting, and on-demand self-assessments.

## POLICY AND PROCESS DOCUMENTATION

A major cornerstone of any NCUA-compliant organization is the creation, management, and measurement of the policies and processes that comprise the institution's security program. CyberProtect will produce a comprehensive document that explains what controls BlueVoyant MSS supports along with sample evidence to support the assessment process throughout the calendar year.

## DETAILED REPORTS

In order to measure the success and maturity of your NCUA-compliant cybersecurity program, CyberProtect provides robust data collection, searches, and detailed reports mapped to specific NCUA control areas. Provide your partners with the information they need from a single authoritative source to streamline all NCUA assessment information requests.




## SELF-ASSESSMENT WIZARD

The self-assessment wizard enables institutions to manage their program and gain visibility into the organization's security risk, program maturity, and NCUA assessment readiness throughout the year and, more importantly, leading up to the scheduled audit.

The continuous security and privacy of your credit union's member data is no longer a desired state, but an expected one. For more information on CyberProtect, call Fiserv at 800-872-7882.

## ABOUT BLUEVOYANT

BlueVoyant is an analytics-driven cybersecurity company whose mission is to protect businesses of all sizes against agile and well-financed cyber attackers by providing unparalleled visibility, insight, and responsiveness. BlueVoyant provides Advanced Threat Intelligence, Managed Security Services and Professional Services from offices in the United States, the United Kingdom, Israel, and Spain. Learn more at www.BlueVoyant.com.

## ABOUT FISERV

Fiserv, Inc. (NASDAQ: FISV) enables clients worldwide to create and deliver financial services experiences in step with the way people live and work today. For 35 years, Fiserv has been a trusted leader in financial services technology, helping clients achieve best-in-class results by driving quality and innovation in payments, processing services, risk and compliance, customer and channel management, and insights and optimization. Visit Fiserv.com and follow on social media for more information and the latest company news.

BlueVoyant

# EXTERNAL VULNERABILITY ASSESMENT
# PROFESSIONAL SERVICES

## EVOLVING BUSINESS OPERATIONS EXPAND THE VULNERABILITIES OF ORGANIZATIONS

**The business landscape has transformed to include cloud storage and remote workers. While these advancements have significant advantages, they also open networks to increased vulnerability to cyber attacks. With networks no longer static, IT professionals must plan for the inevitability that threat actors will look for opportunities to target organizations with sensitive data.**

It's easier with so many connected devices for threat actors to gain access that may go unnoticed by internal scanning. From proxies for malicious traffic to dynamic redirects on compromised websites, threat actors are monetizing unauthorized access at the expense of customers and the organizations that work to serve them.

## LOOK IN FROM THE OUTSIDE

The business landscape has transformed to include cloud storage and remote workers. While these advancements have significant advantages, they also open networks to increased vulnerability to cyber attacks. With networks no longer static, IT professionals must plan for the inevitability that threat actors will look for opportunities to target organizations with sensitive data.

It's easier with so many connected devices for threat actors to gain access that may go unnoticed by internal scanning. From proxies for malicious traffic to dynamic redirects on compromised websites, threat actors are monetizing unauthorized access at the expense of customers and the organizations that work to serve them.

## HOW EXTERNAL ASSESSMENTS HELP

Many small to mid sized organizations have previously opted out of external assessments because they were cost prohibitive. By ignoring these attack surfaces, threat actors have successfully compromised the integrity of business protections, often going undiscovered for astonishingly long periods of time or until they disrupt operations. By proactively scanning and assessing your risks beyond your network perimeter, you can resolve issues before they become a problem and reduce the possibility of threat actors interfering with your organization.

External assessments are an investment towards solidifying and maintaining your reputation. Several highly publicized incidents have caused severe harm to the trust customers have in large businesses, (Equifax 2017 and Facebook breaches 2019). Small to mid-sized organizations are held to the same standard for customer data privacy but often don't perform the assessments needed to identify weaknesses.

BlueVoyant

# EXTERNAL VULNERABILITY ASSESMENT
# PROFESSIONAL SERVICES

## WHAT WE ASSESS

BlueVoyant's External Vulnerability Assessment serves to give you unparalleled visibility into your organization's web presence. We will scan your web properties and report our findings in a digestible, action-outlined format for easy application. We will assess:

- ***Servers:*** scan for server vulnerabilities, unsecured management scripts and sites sharing the same IP
- ***Network:*** identify default credentials, firewall configuration gaps, and all listening devices
- ***Web:*** search all applications in use, listing unauthenticated areas, SQL investigations or cross-site scripting as well as insecure configurations

We will leverage both open-source intelligence, testing for reputation and blacklisting, and the BlueVoyant proprietary global cyber threat data set. By combining both manual search and machine-learning, clients are able to holistically improve their cyber hygiene.

•

## OTHER WAYS WE CAN HELP

External Vulnerability Assessments can add additional value when conducted alongside the deployment of our Managed Security Services offerings. By working in parallel, our Professional Services team can provide greater context for your risks.

Whether you're looking to safeguard your business image, encourage financial investment, or simply create a more robust plan, this assessment can help you expedite smarter cybersecurity improvements.

If you need more robust cybersecurity insights, our incident response team is comprised of field-experienced analysts who can help you in the event of a breach. If you need help investigating or remediating, our team of BlueVoyant cybersecurity experts can help you throughout the entire threat cycle, from scanning to identification and prioritization to remediation.

## ABOUT US

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 underserved. 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.

**Discover the BlueVoyant Difference**

www.bluevoyant.com | Contact@bluevoyant.com

# Managed Detection & Response


BlueVoyant

BlueVoyant

"Business disruption is a major concern of both large and small enterprises today. As the world of cyber criminals continues to grow, companies will continue to deploy more and more defenses and layers of protection to defend themselves from losses. No single form of defense is sufficient - you have to take a multi-layered approach."

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

## Who is 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 underserved. 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.

BlueVoyant

# Managed Detection & Response

## Democratized Cybersecurity

BlueVoyant democratizes next-generation cybersecurity by creating 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.

Managed Detection and Response from BlueVoyant consists of monitoring and management of endpoint software deployments and the performance of incident response actions as needed. Monitoring Services include 23/7 collection, storage, reporting, and client notification of security events and device health events.

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).

Managed Detection and Response includes a proven implementation methodology and tools for simple reporting and analysis that are provided through Wavelength™, BlueVoyant's client portal.

MDR+ can be tailored to fit your needs with additional services like custom advanced threat detection.

### Security Monitoring

Event classification is part of the process that BlueVoyant analysts perform when investigating security alerts. Depending on the severity, clients will be notified by email, phone call, or through the client portal.

| LOW | MEDIUM | HIGH | CRITICAL |
|---|---|---|---|
| **Minimal Threat** \| Adware or other potentially unwanted programs (PUPs) | **Potential Threat** \| malware bots or spyware that are not as dangerous | **Significant Threat** \| rootkits, keyloggers, trojans, ransomware, confirmed suspicious privilege escalation, confirmed social engineering-based attack | **Eminent Threat** \| data destruction, encryption, exflitration, or malicious interactive attackers. |

### Services Activation:

Advanced endpoint software will be deployed. Client applications will be whitelisted to reduce the likelihood of unintended business disruption. Remote intrusion response activities pre-approval guidelines will be established.

### Investigation and Notification:

When 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.

### 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™.

### Endpoint Response:

BlueVoyant will take a specific set of actions at the completion of an investigation: quarantine, delete, whitelist, monitor, or blacklist. Depending on your services, if an advanced investigation with live/real-time response is needed, BlueVoyant may perform intrusion remote intrusion response activities.

### Threat Detection:

Advanced endpoint software will be used to expand enrichment and enhanced behavioral correlations. Depending on your services, BlueVoyant will vproactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions.

### Malware Prevention:

Deployed endpoint software will automatically prevent the execution of suspicious or known malicious software, often preventing the outbreak or spread of malware. Through blacklist policy management, delivery of unique signatures and threat intelligence indicator matching, BlueVoyant can deny, terminate and block operations remotely.

### Health Monitoring:

BlueVoyant will monitor installed endpoint agent communications using the Technology Platform. BlueVoyant will monitor log sources and will generate an alert when a log source's output has not been received in a specified interval.

### Outage Prevention:

All third-party vendor patches and upgrades will be assessed for their security, stability, and functionality by BlueVoyant prior to client deployment to ensure they are supported and won't cause outages.

# Managed Detection & Response

## Features

Managed Detection and Response is supported by the expert analysts who are operating 24 hours a day, 7 days a week, across multiple locations within the 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 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 SOC and engineering teams have developed automations to support Managed Detection and Response and continue to deliver new automations. For example, an automated Emotet investigation, confirmation, and response playbook exist to quickly respond to specific outbreak strains.

**During Introduction,** key BlueVoyant and enterprise staff will engage you to learn your priorities, expectations, and deadlines. You will meet your BlueVoyant Project Manager as well as the Client Experience Team. We will establish your Threat Profile which helps us identify potential threats. We will create an Approve Response Plan as well as a list of Pre-Approved Response Actions that will be used to inform the SOC which response actions they may perform under what conditions.

## 1 Introduction

Facilitates information gathering and begins with project kickoff.

## 2 Provisioning

Deploys software, sets configurations, and establishes connections.

## 3 Tuning

Establishes the baseline of activities and highlights anomalies.

### Your Client Experience Team

#### Client Advisor

The Client Experience Team is your primary support resource. You will be assigned an advisor who will act as your consultant and will enable the best experience interacting with BlueVoyant services. Your advisor will meet with you regularly to understand the goals of your security program and track results. Your advisor will also engage with 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 onboarding process. The Implementation Project Manager will help you establish timeline goals and select sources and devices that will be onboarded with the appropriate priority that aligns with your goals.

**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 connectivity of BlueVoyant Virtual Appliances. You will also gain access to the client portal, Wavelength and we will configure multi-factor authentication which will be followed by training for client users. Security monitoring will begin once 80% of the target deployment has been met and an audit has been performed to ensure software has been properly deployed.

**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. We will develop endpoint policies to help with whitelisting applications which will be refined through steady-state operations as your IT infrastructure changes.

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.

## Service Tier Comparison

| Managed Detection and Response | MDR+ | MDR+ with Advanced Threat Hunting |
|---|---|---|
| MDR Service Activation | ✓ | ✓ |
| Investigation & Notification | ✓ | ✓ |
| Indicator Enrichment | ✓ | ✓ |
| Endpoint Response | ✓ | ✓ |
| Threat Detection | ✓ | ✓ |
| Malware Prevention | ✓ | ✓ |
| Health Monitoring | ✓ | ✓ |
| Software Upgrades | ✓ | ✓ |
| Access to Wavelength™ | ✓ | ✓ |
| Threat Hunting | | ✓ |
| Remote Intrusion Response | | ✓ |

BlueVoyant

# Managed Detection & Response

## Layered Security Protection

### 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.

Our Managed Detection and Response (MDR) service is the foundation of a robust cybersecurity program. Adding additional layers of protection as your need grows helps reduce risk to your enterprise.

**73%** of breaches are perpetrated by outsiders

**60%** of breaches are conducted by organized crime

**92%** of breaches originated through email

Companies that contained a breach in under 30 days saved over **$1M USD**

### Additional Managed Security Services Available:

**Detection-as-a-Service** (SM)

Collects logs from applications and on-premise and/or cloud infrastructure to enable advanced threat detection. BlueVoyant leverages proprietary, open-source, and dark web intelligence to expedite triage and enrich investigations conducted by the SOC.

**Managed SIEM**

Maximize existing platform investments with access to a BlueVoyant hosted Splunk® Enterprise environment that will enable hands-on access to data and a team to help you perform searches, develop correlations and execute analysis.

**Vulnerability Management Services**

Takes the guesswork out of identifying potential weaknesses such as missing patches, malware, and misconfigurations. Vulnerability Management Services help organizations prioritize vulnerabilities so that they can reduce risk.

BlueVoyant

# FISERV BIN WATCHER
# POWERED BY BLUEVOYANT

## CATCH THREAT ACTORS USING STOLEN CREDENTIALS & IMPROVE CUSTOMER PROTETIONS

**Organizations invest great amounts of time, energy, and resources into technology that protects their customers from credit card fraud.**

They verify the legitimacy of transactions by monitoring spending habits and are fairly proficient at catching abnormal trends; however, threat actors are becoming more sophisticated in their approach, which is leaving some organizations struggling to respond and remediate in a timely way. Slow response leaves organizations vulnerable and customers unhappy.

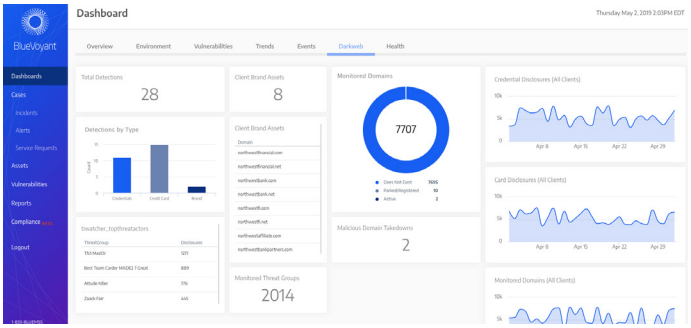
BIN Watcher, part of BlueVoyant's Threat Intelligence Solutions, helps organizations to identify freshly stolen credit cards and facilitates proactive protection for your customers. You can take immediate action on compromised credit cards and prevent cyber-criminals from monetizing them on underground groups and forums.

## PROTECT YOUR REPUTATION

Brand loyalty is fleeting in today's marketplace and customers don't need any incentives for changing brands. You can protect your organization's reputation and loss of consumer confidence by extensively monitoring your customers' credit cards.

## HOW BIN WATCHER WORKS

BIN Watcher, powered by BlueVoyant Threat Intelligence, constantly searches for mentions of Bank Identification Numbers (BIN) within instant messaging applications as well as the Deep and Dark Web. By searching for mentions, we can proactively identify if threat actors are trafficking in debit or credit cards belonging to your customers. When the bank's BIN is detected, an alert is provided including all the details to lock the account.




BIN Watcher is deployed alongside our team of expert cybersecurity analysts. These elite, field-seasoned, human intelligence professionals are able to leverage their knowledge of the Deep and Dark Web as well as their deep understanding of threat actor behaviors and languages, to role play and gain cyber criminals' trust. We can think, talk, and act like attackers, engaging threat actors in investigative conversations which reveal fraudulent activities and reveal attacker trends.

BlueVoyant

# FISERV BIN WATCHER

## THE CHANGING THREAT UNDERGROUND ECONOMY

Cyber-criminals have created their own underground economy. They have shifted communication to popular instant messaging applications to exchange stolen banking information and evade authorities.


BIN Watcher is the only cybersecurity solution that monitors closed groups in four distinct instant messaging applications: WhatsApp, Telegram, ICQ and Discord. Hundreds of freshly stolen credit cards are advertised and sold on these channels each day. Protecting your customers from the ever-increasing risk of credit card fraud builds trust and protects your brand.

## WHY BLUEVOYANT

BIN Watcher, powered by BlueVoyant Threat Intelligence, currently serves the top global financial organizations. We also democratize cybersecurity so that organizations of any size can leverage our expertise and investigative capabilities. Our access to the deepest corners of the web allows us to defend your bank by employing some of the same methods and tactics used by threat actors.

Our experience across market sectors, including private and government organizations, allows our field-seasoned analysts to more accurately identify when fraudulent activity is about to occur. Our technology, exclusive data set, and team of elite cybersecurity professionals positions us as industry leaders and set us apart from our contemporaries.

## 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 underserved. Through our advanced Threat Intelligence, Managed Security Services, and Incident Response 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.

**Discover the BlueVoyant Difference**

www.bluevoyant.com | Contact@bluevoyant.com

BlueVoyant

# INCIDENT RESPONSE PLANS
# **PROFESSIONAL SERVICES**

## REDUCE RISK WITH PLANNED RESPONSES TO CYBERSECURITY EVENTS

**Today's threat landscape is evolving at an unprecedented rate because threat actors have become agile, well-financed, and motivated to target organizations of all sizes. These cybercriminals have found new ways to evade law enforcement using the Deep and Dark Web to monetize stolen information. In response to this increase in criminal activity, organizations are ramping up their cybersecurity protections.**

Despite increased efforts and investments in defense tools, no organization is immune from a breach. What you do when this security incident occurs can have serious repercussions for both your organization and your customers.

## PREPARE FOR THE UNPREDICTABLE

The threat landscape is ever-changing and the tools threat actors are employing to breach your organization are also evolving. Due to the complexity of most security environments, resource-constrained IT professionals have to focus on emerging priorities and often can't afford the time, or allocate the resources, to develop an incident response plan.

## PLAN FOR THE FUTURE

While no organization wants to believe they are susceptible to security incidents, the reality is that an incident will occur and you have to be prepared with a robust, relevant and right-sized solution for responding.

Time is a crucial factor for reducing the impact of a security incident. Unfortunately, most internal incident response teams are already multi-tasking and many organizations don't have the resources to support this function. When time is consumed by business operations, it's crucial for your organization to have a plan for responding to incidents.

## STREAMLINE YOUR RESPONSE

BlueVoyant's Incident Response Plans come into play the minute you have identified suspicious or malicious cyber activity that could impact your business through:

- Disruption of information systems, networks or digital services
- Manipulation and/or destruction of information and infrastructure
- Unauthorized access to infrastructure and sensitive data

The plan will help streamline the response your team makes to classify events based on overall impact to the organization.

BlueVoyant

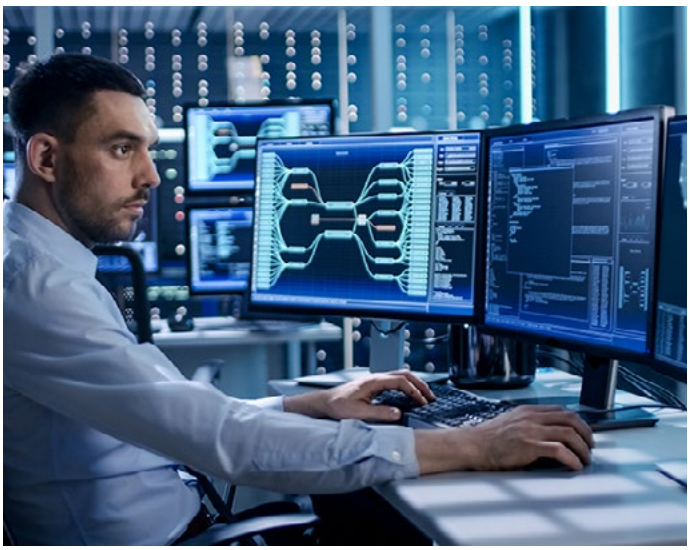
# INCIDENT RESPONSE PLANS
# PROFESSIONAL SERVICES

## HOW WE WORK

BlueVoyant will create a plan that is flexibly built to address multiple breach types and severities. We will help you to identify personnel needed based on the unique threat incidents possible. We will define and outline breach responses based on the event (internal/external threat actor, PII or proprietary data theft). We will provide a tailored checklist of prioritized action items and help you to audit legal obligations of your organization and assess third-party compliance.

Your plan will include ways to:

- Determine scale of impact and escalation protocol
- Assign roles and responsibilities post notification
- Communicate internally when responding to the incident



## BLUEVOYANT ADVANTAGE

The services of BlueVoyant's Threat Intelligence, Managed Security Services and Professional Services are mutually reinforced. Our proprietary, global cyber threat data set provides threat intelligence unparalleled to our contemporaries.

As a BlueVoyant client, you can amplify your cybersecurity by engaging our team for additional services, such as:

- ***Incident Response:*** BlueVoyant Incident Response Team and SOCs are available for increased insights and incident investigation and reporting
- ***Managed Security Services:*** From endpoint and vulnerability awareness to a complete robust technology suite to address evolving threats, MSS solutions address a variety of common cybersecurity challenges
- ***Threat Hunting:*** BlueVoyant's team of experts provide human and machine-learning to execute threat hunting
-

## ABOUT US

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 underserved. 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.

**Discover the BlueVoyant Difference**

www.bluevoyant.com | Contact@bluevoyant.com

BlueVoyant

# NIST CYBERSECURITY ASSESSMENT
# **PROFESSIONAL SERVICES**

## ASSESSMENT BASELINES HELP PRIORITIZE CYBERSECURITY IMPROVEMENTS

The National Institute of Standards and Technology (NIST) through the U.S. Department of Commerce has developed a guide for assessing the security controls within federal information systems and organizations. This NIST Guide establishes common assessment procedures to evaluate the effectiveness of security controls and ensures that companies are using consistent, comparable and repeatable security assessments of cybersecurity systems. It is considered an industry standard for comprehensive security posture assessment.

## HOW NIST HELPS

BlueVoyant uses NIST in conjunction with our own carefully developed proprietary framework. We use it as part of a larger, holistic plan to help clients develop awareness of their existing deficiencies and recommended improvements. As a starting point for developing more specific assessment procedures and targeted plans, BlueVoyant works with IT teams to create organization-specific recommendations that are robust, relevant and right-sized.

## PREPARE FOR UNIQUE CHALLENGES

While the NIST Guide provide best practice standards, BlueVoyant's Professional Services team uses their field-experience to augment our cybersecurity assessment of your organization. We see NIST assessment as a way to quantitatively measure your effectiveness across the incident response lifecycle.


## BENEFITS: UNDERSTAND, JUSTIFY, OUTLINE

Some of the key benefits to engaging BlueVoyant for cybersecurity assessments include:

- Understanding your cybersecurity risks, infrastructure gaps, and external vulnerability blindspots
- Justifying your security investments for key stakeholders by articulating the urgency, relevance and applicability of your threat posture
- Outlining your roadmap for security initiatives by prioritizing risks and measuring your effectiveness in present and future state

BlueVoyant

# NIST CYBERSECURITY ASSESSMENT
# PROFESSIONAL SERVICES

## HOW WE WORK

When you engage BlueVoyant, we will assess the current state of your cybersecurity posture and maturity by comparing your current state against industry-standard frameworks (like NIST) and best practices. After evaluating your technology and interviewing your key staff, we will provide a report on your exposure points. Our report will include counsel on your unique challenges and will outline tailored improvements you should employ. These recommendations will help you to plan using your unique risk profile, budget, resources, policies, and compliance needs.

## ENGAGE ADDITIONAL SUPPORT

When conducted alongside the deployment of our Managed Security Services offerings, our Professional Services team can help provide greater context for your risk level. Whether you're looking to safeguard your business image, encourage financial investment, or simply create a more robust plan, the Cybersecurity Assessment can help you expedite smarter cybersecurity improvements.

## BLUEVOYANT THREAT INTELLIGENCE ADVANTAGE

The services of BlueVoyant's Threat Intelligence, Managed Security Services and Professional Services are mutually reinforced. Our proprietary, global cyber threat data set provides unrivaled threat intelligence. As a BlueVoyant client, you will have access to our experts who will employ this data to guide our recommendations.

Our team of field-seasoned experts have deep experience in both the public and private sectors and use their knowledge to inform clients on the most applicable threats. From Fortune 500 company leadership to global intelligence communities, our team has seen the threat landscape and is prepared for the constant changes. We plan for the evolving threat horizon and create recommendations that help you to be better prepared for the future.

## ABOUT US

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 underserved. 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.

**Discover the BlueVoyant Difference**

www.bluevoyant.com | Contact@bluevoyant.com

BlueVoyant

# FISERV THREAT INTELLIGENCE
# POWERED BY BLUEVOYANT

## IDENTIFY THREATS, ENHANCE YOUR INSIGHTS AND PROTECT YOUR ORGANIZATION

**Resource-constrained IT departments work hard to protect company assets by incorporating multiple layers of technology to detect, defend, and remediate threats.**

At the end of the day, they rest easy believing that the enterprise is secure. However, threat actors well outside their perimeter are busy devising meticulous, pre-planned attacks that, by their very nature, go unnoticed by the excellent security measures the enterprise has in place.

Insight into the activity occurring well outside your perimeter is no longer a "luxury". It is a necessity. Data theft, impersonation, and the construction of malicious infrastructures for fraudulent activity are realities that companies of all sizes must acknowledge and defend against.

## KEEP WATCH BEYOND YOUR PERIMETER

BlueVoyant Threat Intelligence solutions are the only cyber defense services that monitor threat actors throughout the entire cyber-crime lifecycle. We scan the deep recesses of the web to help you prevent these kinds of threats before they reach your perimeter and disrupt your business.

BlueVoyant is able to alert you to the advanced indicators such as stolen credentials and sensitive data for sale, malicious IPs and domains targeting your organization and customers and other distinctive markers that warn of impending attacks or an existing compromise.

## HOW THREAT INTELLIGENCE SOLUTIONS WITH BLUEVOYANT WORK

The difference between Threat Intelligence with BlueVoyant and other providers is the depth of our investigations, the breadth of data that we are able to ingest, and the actions we take to help you protect and salvage data loss.

BlueVoyant is monitoring threat actor activities outside your perimeter. From locating malicious infrastructures, to identifying phishing attacks on your employees and customers, to uncovering the sale of your stolen sensitive data on the Dark Web, our solutions can be used independently or in conjunction to give full visibility and status on your security posture.

## WHAT WE DO

Instead of alerts and unrefined data feeds, Threat Intelligence puts threat data within the context of your organization. By monitoring your perimeter, we can provide a more complete and relevant threat landscape that is customized to your organization. Our feed shows your unique environment and highlight where you need to focus your energy.

Depending on the service you choose, we can stop threat actors from using tools that could be used to confuse and steal data from you and your clients, like fake websites, phishing schemes, and misleading domain names. And/or we can monitor threat actors within the deep and dark web to alert you to when your information, or your customers' information, are being sold.

BlueVoyant

# FISERV THREAT INTELLIGENCE

## WHY BLUEVOYANT

Threat Intelligence, powered by BlueVoyant, currently serves the top global financial organizations. We also democratize cybersecurity so that organizations of any size can leverage our unique machine and human-generated intelligence to defend against threats that lurk well outside their perimeter.

Our access to the deepest corners of the web allows us to defend your enterprise by employing some of the same methods and tactics used by threat actors.

Our experience across market sectors, including private and government organizations, allows our field-seasoned analysts to more accurately identify, assess, and triage potential malicious activity no matter where it occurs. Our technology and our exclusive data set, positions us as industry leaders and set us apart from our contemporaries.

## THREAT INTELLIGENCE SOLUTIONS

**BlueVoyant BIN Watcher**
See when someone is selling your credit or debit card data on the underground market.

**BlueVoyant Credentials Watcher**
Know when someone is selling your personally identifiable information (PII) on the underground market.

**BlueVoyant Brand Watcher**
Be informed when malicious fraud infrastructure is set up to target your customers.

## CYBERPROTECT + THREAT INTELLIGENCE = END-TO-END CYBER PROTECTION

When you combine Threat Intelligence with other BlueVoyant Managed Security Services, you are able to achieve an end-to-end solution that vastly improves your security posture, saves time, and allows you to focus on growing your business.

## ABOUT US

BlueVoyant is an analytic-driven cybersecurity company whose mission is to protect organizations of all sizes against agile and well-financed cyber attackers. Founded and led by experts in the cyber security and government security sectors, BlueVoyant's offerings are built with real-world insight and applicability, plus an eye on the threat horizon.

Through our Advanced Threat Intelligence, Managed Security Services, and Incident Response Services, we excel in intelligence gathering, cyber security defense, detection of attacks and response coupled with remediation.

Our SOCs around the world keep us on top of developing and established threat actors and the well-financed tools they are developing to out-smart traditional security measures. Our 24/7 SOCs, offices around the world, and our security analytics platform positions us to best help our customers defend against emerging cyber threats.

**Discover the BlueVoyant Difference**
www.bluevoyant.com | Contact@bluevoyant.com

# Vulnerability Management Services

BlueVoyant

BlueVoyant

"The latest industry reports estimate that 92 percent of attacks originate from spear-phishing, where employees unwittingly click on malicious malware. No company is immune from a smart threat actor with spoofing capabilities, but BlueVoyant helps reduce your risk of cyber attack and is here to remediate attacks that have already occurred through our layered security protection products and services."

Milan Patel, Chief Client Officer

## OUR SERVICES:

### Threat Intelligence

### Managed Security Services

### Professional Services

## Who is 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 underserved. Through our advanced Threat Intelligence, Managed Security Services, and Incident Response 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.

BlueVoyant

# Vulnerability Management Services

## Democratized Cybersecurity

**BlueVoyant Vulnerability Management Service (VMS)** delivers vulnerability assessments of your environment to let you know where there are weaknesses that threat actors could potentially exploit.

From missing updates and patches to software bugs and operating design flaws, weaknesses in your system leave you open to possible risk. BlueVoyant VMS offers automated, recurring vulnerability scanning and utilizing the BlueVoyant Technology Platform in conjunction with a team of elite, highly-certified security analysts to help you catalogue and prioritize vulnerabilities within your system.

BlueVoyant accomplishes this by installing a software appliance on your endpoints in order to perform the vulnerability assessments.

VMS is an additional layer of protection that we offer to current BlueVoyant Managed Security Services clients.Your vulnerability assessments will inform and improve the quality of your current BlueVoyant service protection.

We offer three tiers of the VMS service exclusively to our MDR, DaaS and Managed SIEM clients: Vulnerability Import, Internal Scanning and Full Service.

**Vulnerability Import,** the first service tier, works with you to enable the automatic import of vulnerabilities into the BlueVoyant platform utilizing support third-party vendor assessment software. Vulnerabilities will be visible to the expert analysts in the Security Operations Center.

**Internal Scanning**, our second tier, expands upon the first tier by deploying the BlueVoyant Virtual Appliances and conducting vulnerability assessments and asset discovery internally in your environment.

**Full VMS,** our third and most comprehensive tier, combines all the service features and most notably adds external scanning.

**Wavelength™,** the BlueVoyant client portal gives you visibility into your network vulnerabilities and allows you to track them and generate reports. It is a feature of all three tiers of service.

**65%** of companies have more than **500** users who are never prompted to change their passwords

- Varonis 201

**Vulnerability Assessment:** VMS works to perform a variety of vulnerability assessments utilizing best-of-breed vulnerability detection software to discover well known weaknesses in software. It proves recommendations for managing or resolving the vulnerabilities through the BlueVoyant Portal and through custom reports.

**Scanning:** Scans will be conducted on a regular basis at weekly, monthly, or quarterly intervals. External scanning includes the detection of vulnerabilities that are exposed beyond your network perimeter and are therefore visible and possibly exploitable by attackers. Internal scanning includes vulnerabilities within your organization that may not be externally facing but could be exploitable by attackers within the environment. BlueVoyant can also conduct on-demand vulnerability scans on a need basis.

**Asset Discovery:** As part of the service, you can request BlueVoyant to conduct regular asset scanning to identify new devices in their environment or to update any identifying information on previously detected assets such as hostname or IP address. Asset Prioritization: Through the BlueVoyant Portal, you can assign criticality to asset records to indicate which assets are the most important in their environment. Asset Tagging: Through the BlueVoyant Portal, you can apply “tags” to asset records. This enables grouping of assets to support dashboards and reports.

**Vulnerability Verification:** By comparing new vulnerability scan results against previously identified vulnerabilities our experts will determine which vulnerabilities have been appropriately remediated. Vulnerabilities will remain in an active state within the BlueVoyant Portal until a vulnerability scan occurs, rather than when a patch or upgrade was applied in order to confirm any remediations.

**Policy Selection:** As part of Service Activation, BlueVoyant staff will work with you to understand what your compliance and risk goals are to help you select one of the approximate twenty (20) vulnerability scan policies.

**Vulnerability Tracking:** Through the BlueVoyant Portal, you are able to see all active vulnerabilities that have been detected. These vulnerabilities are mapped to asset records which are mapped to any security alerts or incidents (detected through other BlueVoyant Managed Security Services) to support traceability of the activity of assets and vulnerabilities.

**Software Upgrades**: As software patches, upgrades, and new vulnerability signatures are released for the supporting vulnerability assessment software BlueVoyant will assess the release for security, stability, and functionality before certifying it as a supported version. BlueVoyant will perform software upgrades automatically for deployments leveraging the BlueVoyant Virtual Appliance.

# Vulnerability Management Services

## Features

Vulnerability Management Services are supported by expert analysts who operate 24/7 across multiple locations and within 2 global Security Operations Centers (SOCs). Certifications held by the team include SANS GIAC, EC-Council, and ISC-2, as well as others.

Wavelength™, the BlueVoyant portal is a web-based portal that provides real-time visibility into detected alerts, confirmed incidents, all detected assets, and vulnerabilities. Locate dashboards representing a variety of content including but not limited to event volume, alert volume, detected assets, and analyst response actions inside Wavelength™.

Access vulnerability reports containing content such as new and resolved vulnerabilities and high-risk vulnerabilities on critical assets through Wavelength™.

Orchestration and automation, a key component of the Technology Platform, synchronizes security tools and helps maintain the proper balance of machine automation and human intervention. Orchestration and automation accelerates triage, reduces false positives, and improves mean time to resolve (MTTR).

BlueVoyant SOC and engineering teams have developed automations to support Managed Detection and Response and continue to deliver new automations. For example, an automated Emotet investigation, confirmation, and response playbook exist to quickly respond to specific outbreak strains.

The Client Experience team is your primary support team. Your advisor will meet with you on a regular basis (most often monthly) to understand your security program goals and will advise how BlueVoyant services can best meet your needs.

**During Introduction,** key BlueVoyant and enterprise staff will engage you to learn your priorities, expectations, and deadlines. You will meet your BlueVoyant Project Manager as well as the Client Experience Team. The Client Experience team is your primary support team. Your advisor will meet with you on a regular basis (most often monthly) monthly) to understand your security program goals, to offer advice, and to help you select BlueVoyant services to best meet your security needs.

BlueVoyant works with you to understand your network environment and the best deployment locations for BlueVoyant Virtual Appliances to ensure proper vulnerability assessment coverage. Our team will work with you to understand your risk and compliance goals and select the best vulnerability scan policies and scan frequency to meet those vulnerability assessment needs. During the introduction phase, you will identify infrastructure that is hosted with a cloud provider and BlueVoyant will work with you to obtain prior approval for the scan frequency of that infrastructure.

## 1 Introduction

Facilitates information gathering and begins with project kickoff.

## 2 Provisioning

Deploys software, sets configurations, and establishes connections.

## 3 Tuning

Establishes the baseline of activities and highlights anomalies.

### Your Client Experience Team

#### Client Advisor

The Client Experience Team is your primary support resource. You will be assigned an advisor who will act as your consultant and will enable the best experience interacting with BlueVoyant services. Your advisor will meet with you regularly to understand the goals of your security program and track results. Your advisor will also engage with you should you have any significant security events occur.

#### Implementation Project Manager

At the beginning of your MDR deployment, a BlueVoyant Implementation Project Manager will be assigned to you to assist you through the onboarding process. The Implementation Project Manager will help you establish timeline goals and select sources and devices that will be onboarded with the appropriate priority that aligns with your goals.

**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 connectivity of BlueVoyant virtual appliances. You will also gain access to the client portal, Wavelength™ and we will configure multi-factor authentication which will be followed by training for client users. Security monitoring will begin once 80% of the target deployment has been met and an audit has been performed to ensure software has been properly deployed.

**During Tuning,** we establish the baseline of activities and highlights anomalies. Once the BlueVoyant Virtual Appliance(s) have been deployed, the environment will be scanned to detect all assets. The asset list will be reviewed with you. This includes the identifying "Key Terrain" devices and applications as well as asset tagging and assigning asset criticality.

## Service Tier Comparison

| Vulnerability Management | Vulnerability Import | Internal Scanning | Full VMS |
|---|---|---|---|
| Vulnerability Assessment | | ✓ | ✓ |
| Internal Scanning | | ✓ | ✓ |
| External Scanning | | | ✓ |
| Asset Discovery | | ✓ | ✓ |
| Vulnerability Tracking | ✓ | ✓ | ✓ |
| Reports | ✓ | ✓ | ✓ |
| Software Upgrades | | ✓ | ✓ |
| Integration with MSS | ✓ | ✓ | ✓ |

## 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.

### Additional Managed Security Services Available:

### Managed Detection and Response (MDR)

Our Managed Detection and Response (MDR) service is the foundation of a robust cybersecurity program. Adding additional layers of protection as your need grows helps reduce risk to your enterprise.

### Detection-as-a-Service

Collects logs from applications and on-premise and/or cloud infrastructure to enable advanced threat detection. BlueVoyant leverages proprietary, open-source, and dark web intelligence to expedite triage and enrich investigations conducted by the SOC.

### Managed SIEM

Maximize existing platform investments with access to a BlueVoyant hosted Splunk® Enterprise environment that will enable hands-on access to data and a team to help you perform searches, develop correlations, and execute analysis.

**The average cost top companies spend on a malware attack is $2.4 million** -Accenture, 2017

**Malware and web-based attacks are the two most costly attack types** -Accenture, 2017

**In 2017, 2.7 billion records were stolen, or twice as many as were stolen in 2016** -Wipro, 2018

**87% of surveyed CEOs are investing in cybersecurity to build trust with clients** -PwC, 2018

# BlueVoyant

An Expert-Driven Cybersecurity Services Company