Version 11/01/2022

BlueVoyant
Microsoft MDR for Microsoft 365 Defender

Powered by Microsoft XDR+Microsoft Sentinel

(Product Code - MSS-MDR-<CS, CB, S1,Defender>)

INTRODUCTION

This document ("Service Description") describes the BlueVoyant MDR service ("Service") being provided to you ("Client" or "you") by BlueVoyant.

Unless set forth in a writing signed by BlueVoyant and Client, or by you and a reseller authorized to market and resell BlueVoyant products and services, the Service is governed by this Service Description and the BlueVoyant Master Services Agreement available at https://www.bluevoyant.com/bvmsa (each an "MSA"), to the exclusion of all other terms. To the extent there is any conflict between this Service Description and the relevant MSA, this Service Description shall govern.

GENERAL OVERVIEW OF BLUEVOYANT SERVICES FOR MICROSOFT

BlueVoyant Services for Microsoft include consulting, onboarding, and implementation services called BlueVoyant Accelerators, BlueVoyant MDR (managed detection and response) services, and other services associated with MDR and Accelerators.

In the case of MDR Services, they include BlueVoyant's monitoring of Client's Microsoft environment as per the parameters set forth in a signed service order/proposal. MDR provides Client with 24 hours a day and 7 days a week security monitoring, detection, and response services across Microsoft products covered by the Service. The MDR Service utilizes the BlueVoyant platform ("Platform") which includes automation, case management, and threat intelligence enrichment in conjunction with security analysts in BlueVoyant's Security Operations Centers ("SOC"), as well as Client's Microsoft Sentinel instance, Microsoft 365 infrastructure, and other security products if covered by a BlueVoyant MDR Service.

BlueVoyant MDR Service is an ongoing subscription for managed detection and response which includes a full-time cloud-based 24x7 security operations center.

Standard MDR services are also referred to below as "Tier 1" MDR services. Certain MDR services can be purchased individually or bundled.

- MDR for Microsoft Sentinel
    - Monitoring and investigations of Sentinel incidents.
- MDR for Microsoft 365 Defender
    - Monitoring, investigations, and eradication where possible of security threats across Defender 365 suite of products.
- MDR for Defender for Endpoint

    - Can be purchased separately or as included with MDR for Microsoft 365 Defender

- MDR for Defender for Office 365
    - Can be purchased separately or as included with MDR for Microsoft 365 Defender
    - Includes Security Support Services for Email configuration and Business Email Compromise Investigation Services
- Advanced Threat Hunting, or Tier 2 MDR Services:
    - Proactive threat hunting and other advanced detections by BlueVoyant experts

General Notices about BlueVoyant MDR Services for Microsoft

Clients may opt into the complete BlueVoyant SOC service offerings or select only some of the abovementioned services. The price will change accordingly around selected services and the scope of service. Endpoint or Azure Active Directory response actions are not included unless the client is expressly covered by BlueVoyants MDR Microsoft 365 Defender service.

Client system onboarding for all MDR services above consists of a BlueVoyant Accelerator consulting service or onboarding service. The scope and pricing of the onboarding service will vary based on existing security readiness and configuration of the client environment and generally requires a scoping engagement prior to client onboarding. Please see separate BlueVoyant Accelerator documents for additional details.

The client is responsible for any license and consumption fees within its Microsoft environment, including fees associated with Microsoft Microsoft Sentinel ingestion, as well as Microsoft 365 licensing.

Please note that each service only covers services for one SIEM and tenant. Clients with multiple SIEMs and tenants may require a service agreement for each. Please review options with your sales representative.

BlueVoyant Accelerator Services -- that is, onboarding and baseline configuration services for implementing specific Microsoft security solutions are offered separately, as are various other add-on services.

All the Services will be executed according to this service description unless stated differently in the accompanying statement-of-work (SOW).

Version 11/01/2022

MDR for Microsoft 365 Defender - Service Description

(See Appendix for Additional Service Details)

BlueVoyant's Managed Detection and Response (MDR) for Microsoft 365 Defender service combines the power of Microsoft's Defender product suite with an elite 24x7 security operations team to identify, investigate and eradicate today's most sophisticated and advanced cyberattacks. This service requires the activation of Microsoft Sentinel.

Key Services Delivered:

- Onboarding of Microsoft 365 Defender products into Microsoft Sentinel and the BlueVoyant service (as provided by the Accelerator for MDR for Microsoft 365 Defender)
- 24x7 SOC investigation & response directly in Microsoft 365 Defender products
- Application of best practice policy and alert recommendations
- Close investigated alerts with classifications to see trends
- Enable cross-correlation of Microsoft 365 Defender signal to focus on MITRE coverage and informative responses
- Microsoft Cross Signal Threat Hunting (defined below) is included
- Advanced Threat Hunting (defined below) is included
- ServiceNow ITSM ticketing integration
- Wavelength Portal
- Includes support for: CloudStrike, Carbon Black, Sentinel One (support capabilities may vary - please review requirements with your representative)
- Clients can purchase variations of the MDR service for Microsoft 365 Defender. This service includes,

1. Complete coverage. This includes Managed Detection and Response (MDR) coverage for Microsoft 365 Defender as a whole.
    a. Defender for Endpoint
    b. Defender for Office 365
    c. Defender for Identity
    d. Defender for Cloud Apps

I. MDR for Defender for Endpoint

MDR for Endpoint provides remote endpoint threat protection, response, and mitigation. It protects data, assets, and business operations by detecting malware, including ransomware variants, zero-days, non-malware, and file-less attacks. The BlueVoyant SOC will investigate and neutralize threats on your behalf 24/7, based on requirements and rules of engagement agreed upon by BlueVoyant and the Client. Additionally, the client will provide access to and licensing for Microsoft Defender for Endpoint.

The MDR for Defender for Endpoint generally is deployed in conjunction with and as a component of MDR for Microsoft 365 Defender, and in this case, the client console to review security cases and other notes and updates from the BlueVoyant SOC returned to the client is Microsoft Sentinel with the Wavelength client portal. In client configurations where MDR for Defender for Endpoint is deployed in a stand-alone manner, and not as a component of MDR for Microsoft 365 Defender, Microsoft Sentinel may be an optional component, and may not be required.

Key Services Delivered:

- Investigation & Notification
- Indicator Enrichment
- Endpoint Response
- Additional Details
    - Supported Endpoint OS: Windows, macOS, Linux. Details on which operating systems are supported can be found at: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/tvm-supported-os
    - Standard Managed Prevention: Utilizing Microsoft Defender for Endpoint, automatically blocks malicious indicators of compromise (IOCs) and behaviors of compromise (BOCs) with an expert review of detections to ensure there is always human oversight on technology.

II. MDR for Defender for Office 365

MDR for Defender for Office 365 provides threat detection and investigation against malicious threats posed by email messages, external links (URLs) in files, and collaboration tools.

Key Services Delivered:

- Security Support Services: This is an ongoing subscription service from BlueVoyant's support team. The services include a quarterly assessment of the security configurations enabled for Defender for Office 365, including assessing external email forwarding statuses for new users and domains, review of DKIM, DMARC, and SPF records, and a review of in console Email reports for continuous improvement opportunities. In addition, the team provides Monday through Friday support service to support configurations, modifications, and change management within the Defender for Office 365 exchange admin console (EAC). This subscription service can be purchased after a successful accelerator engagement. Additional project hours can be purchased for extended team or project management use under a separate Statement of Work.

- Business Email Compromise Investigation Services: This is an ongoing subscription that includes a full-time cloud-based 24x7 security operations center that triages **non-user submitted** email alerts from Microsoft Defender for Office 365. The team will investigate the following alert types to identify the severity and blast radius of the attack and escalate accordingly:

    - Email messages containing phish URLs removed after delivery
    - Email messages containing malware removed after delivery
    - Admin triggered a manual investigation of an email
    - A potentially malicious URL click was detected
    - Suspicious email sending pattern detected
    - User restricted from sending email

III. MDR for Defender for Identity

MDR for Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) provides the ability to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization from on-prem domain controller vulnerabilities and brute force attacks. This service is purchased only as an included component of the MDR for Microsoft 365 Defender service, and is not purchased in a stand-alone manner.

Key Services Delivered:

- Protect user identities and credentials stored in on-premises Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage
- The following alert types are supported use cases:
    - Security Principal Reconnaissance
    - NMAP Reconnaissance
    - DC-Sync Attacks (Directory Services Replication)
    - Suspected Pass the Ticket (Identity theft)
    - Kerberos and NTLM brute force attacks
    - SMB User and IP address reconnaissance

IV. MDR for Microsoft Defender for Cloud Apps

MDR for Microsoft Defender for Cloud (formerly Microsoft Cloud App Security) Apps provides protection powered by Microsoft's MCAS solution. This service is purchased only as an included component of the MDR for Microsoft 365 Defender service, and is not purchased in a stand-alone manner.

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes, including log collection, API connectors, and reverse proxy. In addition, it provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all your Microsoft and third-party cloud services.

All of these techniques and monitors provide a rich level of events and incidents to the BlueVoyant SOC that enable rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all your Microsoft and third-party cloud services.

While Microsoft Cloud Application security offers DLP and compliance features, these features are out of scope for detection and response services.

Alerts with category: 'Threat Detection' within MCAS offer the highest quality detections for MDR, and are in scope for the service:

- Impossible Travel
- Multiple Failed Logon attempts to a service
- Activity from TOR IP address
- Multiple failed login attempts
- Suspicious OAuth app file download activities
- Data exfiltration to an unsanctioned app
- Discovered app security breach
- Multiple powerBI sharing report activities
- Malware detection
- Misleading OAuth app name
- Mass download by a single user
- Cloud discovery anomaly detection
- File shared with personal email addresses

- Data exfiltration to an app that is not sanctioned
- Activity from an anonymous proxy
- Activity from infrequent country
- Externally shared source code
- Logon from risky IP address
- New high volume app
- External user added to Teams
- Investigation priority score increase
- Ransomware activity
- Suspicious inbox manipulation rule
- New high upload volume ap

Key Services Delivered:

- 24x7 Cloud App Monitoring and response: Monitors suspicious behavior and provides detailed visibility of alerts and their responses within the Sentinel integration.
- On-going MCAS policies tune-up: BlueVoyant SOC will adjust all MCAS policies to reduce the number of false positives alerts
- Centralized SIEM Alerting, Automation, and Remediation: Through Sentinel integration, BlueVoyant SOC will provide advanced playbooks to automate the response for several built-in Threat Detection policies provided by Microsoft
- Support and remediation of security incidents related to users with high investigation scores: BlueVoyant SOC has developed a set of Sentinel alert rules and playbooks to actively remediate incidents related to high investigation priority score users (score>100)
- Conditional Access App Control apps: BlueVoyant team will assist the Client with setup and monitoring of new SAML application (subject to the scope of Consulting Concierge Services)

Microsoft Cross Signal Threat Hunting

Cross Signal Threat Hunting is bundled with the MDR for Microsoft 365 Defender offering. This detection-driven, CI/CD model of threat hunting includes additional cross signal detections across the Microsoft ecosystem that take advantage of cross-system attribution capabilities within the Microsoft 365 Defender hunting tables. Examples of these hunting scenarios include identity and email detections in addition to traditional endpoint hunting use cases.

Advanced Threat Hunting

BlueVoyant's Tier 2 Managed Detection and Response (generally referred to as "Threat Hunting", but also includes additional capabilities as described below) includes all detection and service delivery components of Tier 1 (Standard MDR), with additional detection capabilities and techniques, as listed below and described further in the Appendix.

- Anomaly Detection
- Threat Hunting
- Forensic Artifact Analysis
- Attacker Abuse Insights
- Ad-hoc IOC Discovery

BlueVoyant Threat Hunting services are designed to identify adversary activity that has bypassed prevention and detection technologies, malware-less attacks, Advanced Persistent Threat actors, and historical compromises. Through continuously updated queries and hunting hypotheses, BlueVoyant Threat Hunters execute automated, and manual queries against raw telemetry from endpoints, network devices, and other sources to drastically reduce the risk of detection bypasses and hands-on-keyboard adversary activity.

Some of the areas investigated include, but are not limited to, Persistence Mechanisms, Webshells, Malicious Scripts, Malicious Documents, Administrator Tool Use, Reconnaissance, Remote Access Solutions, privilege escalation, and manipulation, among other elements.

Reactive hunting is performed on an ad-hoc based on intelligence tippers, new OSINT (open-source intelligence) on threat actor TTP (tactics, techniques, and procedures), client requests, and ongoing research. The BlueVoyant Threat Hunting team is constantly adding new leads and retro-hunting and/or adding scheduled queries based on BlueVoyant research, publicly shared research, intelligence tippers, and the like.

Log Collector Virtual Appliance service

The BlueVoyant Log Collector Virtual Appliance is a software package deployed into a virtual machine that enables log collection from on-premises networks, other commercial clouds, or

other external sources, and delivers it to the customer's Microsoft Sentinel instance(s). The log collector is used when deployment of a log collection agent is not possible, such as gathering logs from a device or appliance where a log collector agent cannot be installed (ex. router or firewall). The BlueVoyant log collector is designed to receive log items in Syslog file formats. Upon receipt of the package by the client, the log collector must be installed in a virtual environment of the customer's choosing and be connected to the networks that are being monitored.

BlueVoyant will remotely manage the virtual appliance, and it will be dedicated to this purpose. In addition, customers will provide internet access and manage firewall rules.

This log collector virtual appliance does not support guaranteed delivery of logs. Therefore, it should not be used for compliance purposes when logs are required to be collected and stored for purposes other than as required by the BlueVoyant SOC.

Key Services Delivered:

- A BlueVoyant Ubuntu-based image containing the software stack required for the Log Collector Virtual Appliance, including Remote Access for management, patching, AV detection, and monitoring
- Log Collector virtual appliance health monitoring, administration, updates, and patching
- Log Source and log file receipt monitoring

General Services Included in All MDR Services

- Security Operations Centers (SOC): BlueVoyant's managed detection and response service is delivered through a cloud-native SOC, which operates 24 hours a day, 7 days a week. The BlueVoyant SOC is SOC II TYPE II certified and staffed with security experts with technical certifications including, but not limited to, Microsoft (MS-500, AZ-500, SC-200), SANS (GCFA, GCFE, CDIA, GCIA, GCIH), and CISSP.
- Wavelength™ (BlueVoyant's Client Portal): Wavelength is a web-based portal that provides real-time visibility to detected alerts, confirmed incidents, enables approved Client employees to interact with BlueVoyant's SOC analysts, view all detected assets, and if applicable, view vulnerabilities.
    - Dashboards: Available through Wavelength, dashboards representing a variety of content including but not limited to event volume, alert volume, detected assets, and analyst response actions.
    - Reports: Available through Wavelength, reports include Client environment content related to alerts, incidents, indicators, assets, and vulnerabilities.

- If needed, the Client can request specific reporting on events be delivered as a report on an automated basis. Extensive customization of report templates and or creation of custom reports are not included in the service and can be performed on an engagement basis subject to the mutual agreement of a separate signed Statement of Work.

  - Threat Intelligence Reports: Threat landscape and intelligence summary reports are developed by the BlueVoyant Threat Fusion Cell.

    The BlueVoyant Threat Fusion Cell (TFC) is a dedicated team of intelligence analysts and threat researchers operating within our SOC that identifies, prioritizes, and operationalizes information about threats that pose risks to our Clients. The TFC collects and curates feeds from 37 sources of data to include BlueVoyant's proprietary dataset, as well as an open-source, partner, and paid intelligence to operationalize and contextualize malicious activities that could pose a risk to you. Threat intelligence includes all atomic indicator types such as SHA256, SHA1, and MD5 hashes, email addresses, URLs, domains, IP addresses, and CVE vulnerabilities. In addition, threat intelligence indicators may also include unstructured indicators on the dark web from web forums or data leaks.

    Our process enables curated threat intelligence to improve detections using a guided course of action with the SOC. Focused on zero-day and emerging threats, the service recommends mitigation efforts for successful incidents. Curated threat intelligence is key to any strategic threat hunt missions and, once detected, is used for reputation scoring and detection efficacy.

- Unlimited Live Remote Response: A core component to BlueVoyant's MDR service includes unlimited remote investigations and response services for all activities consistent with remote SOC capabilities and visibility and response capabilities of managed security tools. This will include day-to-day remote level 1 through 3 investigations and response to all events requiring ongoing coordination and communications with the Client via telephone, email, or conferencing with BlueVoyant security operations personnel. However, remote SOC services do not include on-site support, information technology configuration management, and traditional post-mortem endpoint or network forensics.

  - Traditional incident response services are available from BlueVoyant's incident response team through a separate professional services engagement. A professional services (PS) engagement is necessary for scenarios where endpoint security tools (such as Defender for Endpoint) cannot provide enough insights to determine the root cause or the extent of any data exfiltration that may have occurred. As an example, this can occur when incidents involve devices without sensors or during heavily obfuscated activities.

- BlueVoyant's incident response services (separate add-on) include conducting forensic analysis on endpoint devices utilizing multiple industry-standard tools such as Encase, FTK, Axiom, and X-ways. This analysis is performed in scenarios where additional evidence may be required to solidify conclusions regarding the root cause or data exfiltration, such as passwords, PHI, PII, or other sensitive data from a compromised device. With the help of these tools, BV's professional services can more thoroughly understand the impact of even a brief compromise and identify future risks to the environment.

- BlueVoyant's incident response services will also perform investigations in a forensically sound manner for proper transitioning between investigative services and law enforcement.

- Security Orchestration and Automation: Security orchestration and automation are key system components of the Platform that support the BlueVoyant SOC. BlueVoyant has multiple methods to bring SOAR platforms to security operations centers to accelerate event triage, reduce false positives, and improve mean time to resolution (MTTR).

  - MDR Playbooks: BlueVoyant SOC and engineering teams have developed automation to support services and continue to deliver new automation as part of the service. These playbooks support service implementation, delivery, assessment, and operational data gathering and are not configurable by the Client.

  - SOAR Playbooks: Additional response action automation that requires privileged access to execute or SOAR playbooks extensions of custom requirements are deployed within the Client's Microsoft Sentinel environment during Accelerator packages. The MDR Service will use customer-specific SOAR playbooks in escalation recommendations but ensure access to invoke this automation stays within the Client's jurisdiction. These are configurable but managed by BlueVoyant.

- BlueVoyant Client Experience Team: BlueVoyant's Client experience team is the primary support team for the Client. The assigned Client Success Manager (CSM) will meet with the Client regularly to understand the Client's security program goals and advise how BlueVoyant services can best meet their needs. The CSM is also engaged in any significant security events that occur for the Client. In addition, the CSM will deliver any requested feedback to the BlueVoyant product and service delivery teams. The CSM may also encourage the participation of a BlueVoyant Security Advisor (SA) where appropriate.

Concierge Services

- Standard Concierge Services: Standard Concierge Services is a service that allows the Client to request modifications to the operation of the MDR Service or management of the SIEM. This may include maintaining and tuning data sources to adjust to changes in source systems or to keep up with platform updates. Standard Concierge Services are intended to describe services that modify the existing configuration of BlueVoyant services for a customer and include such services as grouping alerts together into a single response, adjusting thresholds for an automatic response, alert tuning, and threat eradication or adding and removing columns in response arrays, etc.

- Consulting Concierge Services: Consulting Concierge Services is a paid service for the creation of customized content and for Client requests that are out of scope for Standard Concierge Services. Generally, this occurs after the Client has reached a "steady state" with live monitoring services. Prior to work being initiated, BlueVoyant will provide a Consulting Concierge Service statement of work (SOW), including a price quote, and will review this for approval with the Client. Depending on the work effort required, a project manager may also be assigned as part of the work effort. BlueVoyant has the right to refuse the development of custom content for the Client based upon the effort or scope of the request. Consulting Concierge Services will be billed in 30 minute increments.

- Scope of Requests: The scope that the Concierge will support includes (but is not limited to) the development of customized dashboards, widgets, reports, alerts rules, playbooks based on the event and/or available threat intelligence data, and informal user training of the Sentinel software.

- Submitting a Concierge Request. Client requests for Concierge Services are submitted as a concierge service ticket or to the CSM via a service request. The Concierge desk will determine when a Client request qualifies as a Standard Concierge Service or when it is out of scope and must be classified as a Consulting Concierge Service request. This may be when a Client request is too complex or would take too many hours to be completed using the standard level of service.

- Concierge Work Hours. Concierge work hours are determined by "work effort", or the time it takes a Concierge Content Engineer ("CCE") to build, test, and deploy the requested content to your environment. Standard Concierge Services work hours are not charged to the customer, but Consulting Concierge Services work hours are charged against the Client Work Hour Account.

- Client Work Hour Accounts. Each request for Consulting Concierge Services is charged against the client account for Concierge Work Hours. Generally, a BlueVoyant MDR Contract will include an initial quantity of twenty (20) Concierge Work Hours. If a

Concierge request is estimated to require more hours than are available in the client account, the client will be asked to purchase sufficient additional Concierge work hours to cover the expected work effort.

- Limitations: All Concierge requests are subject to the technical and contractual limitations of the Microsoft Sentinel software as provided by Microsoft (the "Vendor"). All Concierge requests are subject to review and approval by BlueVoyant. Due to the highly customized and dynamic nature of the Concierge service, there is no SLA for the CCE completion of Concierge requests.
- Billing: Concierge Work Hours for Consulting Concierge Services time can be purchased from BlueVoyant at a $320/hour rate unless stated differently on a separate SOW. Customers can also purchase additional quantities of Concierge Work Hours at a discounted rate.
- Exclusions. Concierge engineers do not fulfill requests for security consulting, posturing, incident response/remediation, legal, or audit support. Please contact your Client Experience Team advisor to direct these types of requests to the appropriate channels. For incident response, please email incident@bluevoyant.com (24/7). On weekends and overnight, please call us at: +1 855-397-5190 (Americas), +020 4571-3795 (Europe, Middle East, and Africa).
- Tracking. CCEs will record and report on hours on a weekly basis to Client as incurred, along with an email summary of work performed.

Concierge Support Activities

- Below is a list of example support activities. Concierge support activities are not limited to the items below, but it can be a helpful list.

Activity type	Activity Name	Concierge Service Type
Standard Inquiries and tuning	Billing questions	Standard
	Request for service details	Standard
	Request for technical advice about any Microsoft tools and technologies	Standard

	Report Service function incident	Standard
	Modify authorized contact/user	Standard
	Update or create a Sentinel constant	Standard
	Request a Sentinel alert investigation (customer-initiated)	Standard
Disable/removal of connectors, alerts, or log sources	Disable/Remove log source type (on-premises/cloud)	Standard
	Disable/remove the alert rule	Standard
	Disable/remove Sentinel playbook	Standard
New custom requests or investigations	Update or create a Sentinel constant	Standard
	Adjustments to an alert rule (related to tuning activities)	Standard
	Request a Sentinel alert investigation (customer-initiated)	Standard
	Request for technical assistance with onboarding an on-premises Syslog collector	Standard
	Investigation of an increase in Microsoft Sentinel consumption (over 10%)	Standard
	Request a Sentinel tuning report (outside of monthly deliverable)	Consulting
	Request a log source analysis report (volume, data field, value, etc.)	Consulting
	Request ad-hoc data report/extraction (post-incident)	Consulting

	Create a new custom alert rule (as per customer requirements)	Consulting
	Add a new custom Sentinel playbook (advanced SOAR automation)	Consulting
	Creation of custom Sentinel workbooks	Consulting
	Onboard and integrate new data connector for Microsoft Sentinel (data connector already exists in Microsoft or Managed Sentinel Catalog)	Consulting
	Develop a new custom data connector + detection rules	Consulting

Service Requests

A type of case generated by you via an email to soc@bluevoyant.com or opened within the portal case section. Shortly after we receive your email you will receive an automated response from our case management system. The response will have the case number in the subject. It's important to keep this number in the email subject line for all future correspondence so that the case history can be appropriately tracked. When you email the SOC and include others on the email, they too will receive the aforementioned response.

Severity Levels

What do the different incident severity levels mean?

- **Critical** - Events that represent an imminent threat to client assets. Some examples are data destruction, encryption, exfiltration, or compromise by malware or malicious attacker. Escalated via phone call and email.
- **High** - Events that represent a significant threat to client assets. Some examples are malware types that include rootkits, keyloggers, or trojans, confirmed suspicious privilege escalation, and confirmed social engineering-based attack. Escalated via phone call and email.
- **Medium** - Events that represent a potential threat to client assets but do not require immediate attention. Some examples are malware types that include bots or spyware, but not defined as "critical" or "high"

- **Low** - Events that represent no threat to client assets and/or are determined to be a false positive. Some examples are adware or other potentially unwanted programs (PUDS).
- **Informational -** Events that do not represent a threat or impact to client assets but are viewable for situational awareness.

Service Level Agreements (SLAs)

- Security Event Monitoring: The Client shall receive a communication (according to the escalation procedures defined or in the manner pre-selected in writing by customer, either through the Portal, email, or telephone) to security incidents according to the matrix below. Incident classification is the process that a BlueVoyant security analyst performs an investigation to confirm the validity of an alert, impact and assign a severity. Notification times for CLient notification are measured by the time differences between when incidents classification has completed and when the Client is notified. Client notifications occur after event classification in order to prevent notification for benign or false positive alerts.

Severity	Definition	Agreement	Notification Method	SLA Adherence
Critical	Incidents that represent an imminent threat to client assets, including data destruction, encryption, exfiltration, or compromise by malware or malicious attacker.	**30 minutes** Of Incident Classification Completion	• ServiceNow API *(Optional)* • Email • Phone Call • Client Portal	**100%**
High	Incidents that represent a significant threat to client assets, including rootkits, keyloggers, or trojans, but not defined as "critical", confirmed suspicious privilege escalation, confirmed social engineering-based attack.	**1 hour** Of Incident Classification Completion	• ServiceNow API *(Optional)* • Email • Phone Call • Client Portal	**100%**
Medium	Incidents that represent a potential threat to client assets, including malware types that include bots or spyware, but not defined as "critical" or "high".	**4 hours** Of Incident Classification Completion	• Client Portal	**100%**
Low	Incidents that represent a minimal threat to client assets. This includes adware or other potentially unwanted programs (PUPs).	**8 hours** Of Incident Classification Completion	• Client Portal	**100%**

- Service Requests: Standard service requests (applies to all non-change and non-incident tickets) submitted via the Portal, Email, or via telephone will be subject to "acknowledgement" (either through the BlueVoyant ticketing system, email or telephonically) within one (1) hour from the timestamp on the Service Request ticket created by the BlueVoyant platform.

    - Health Outages: Client notification of critical service outages affecting security monitoring of the client's environment. This SLA is notification of the client via email within four (4) hours of creation of a health incident alert. Theis SLA excludes low volume data sources in which detecting outages relative to baselines may not be accurate.

- Maintenance Windows: BlueVoyant may schedule maintenance outages for BlueVoyant software which enables log collection (typically for collecting on-premise data sources) within 24-hours' notice to designate Client contacts. SLAs shall not apply during maintenance outages and therefore are not eligible for any SLA credit during these periods.
    - **Emergency Maintenance**: In the circumstance of immediate necessary changes, BlueVoyant may initiate an emergency maintenance window. When this situation occurs, BlueVoyant will use commercially reasonable efforts to provide notice and minimize the impact to clients.
    - **Client Service Outage:** The SLA shall not apply in the event of any client-caused Service outage that prohibits or otherwise limits BlueVoyant from providing the Service, delivering the SLAs, including, but not limited to Client's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software Devices by Client, its employees, agents, or third parties acting on behalf of Client.
- Third Party Outage: For log collection of third-party sources such as Software-as-a-Service Cloud infrastructure providers, SLAs are not applicable for any outage of the third party in which is related to the delivery of their logs to the BlueVoyant platform.
- SLA Credits: The Client will receive credit for any failure by BlueVoyant to meet the SLAs outlined above within thirty (30) days of notification by Client to BlueVoyant of such SLA failure. In order for the Client to receive an SLA credit, the notification of the SLA failure must be submitted to BlueVoyant within thirty (30) days of such SLA failure occurring. BlueVoyant will research the request and respond to the Client within thirty (30) days from the date of the request. The total amount credited to the Client in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by the Client for such Service. Except as otherwise expressly provided hereunder or in the MSA, the foregoing SLA credit(s) shall be the Client's exclusive remedy for failure to meet or exceed the foregoing SLAs.
- Credit Calculation:
    - If BlueVoyant fails to meet one SLA in a calendar month, then Client will be entitled to a service credit equal to 1/30th of the monthly fee for Service for each calendar day upon which the SLA was not met.
    - If BlueVoyant fails to meet more than one but less than three SLAs in a calendar month, then Client will be entitled to a service credit equal to 1/5th of the monthly fee for Service for each calendar day upon which the SLA was not met.

- If BlueVoyant fails to meet more than three SLAs in a calendar month, then Client will be entitled to a service credit equal to 1/2th of the monthly fee for Service for each calendar day upon which the SLA was not met.

Service credits will be issued up to, but not exceeding, 100% of the monthly fee for Service based upon the annual recurring service fee.

CLIENT COMMUNICATIONS

Below are the standard methods for Clients to obtain information related to the Services or engage BlueVoyant staff.

- Wavelength™ (BlueVoyant Client Portal): Wavelength is the primary method for Clients to stay informed of security activity in their environment and activities of the BlueVoyant SOC. At any time, a Client end-user may go to Wavelength and review any security alerts, dashboards, or reports.
- Email: The Client will receive emails as a regular function of the Services. Email topics can span a wide variety of matters, but most often they relate to security investigations: notification of risk or questions on appropriate environment use or behaviors.
    - Clients can also initiate service change requests via email by sending an email to soc@bluevoyant.com. Upon receipt of any emails, a service request case is created and can be viewed within Wavelength.
- Account Managers (AM): AM's will be the primary point of contact with the Client until the services are implemented into a steady state.
- Client Success Managers (CSM): CSM's will proactively reach out to customers once the solution has been implemented to ensure the Client is satisfied with BV's operations and gather feedback. CSMs are included only in our MDR services unless otherwise purchased
- Security Advisor (SA): SA's will work with the CSM as necessary to support the Client with technical information related to BlueVoyant's Microsoft MSS solutions.
- Calling Security Operations: The BlueVoyant SOC operates 24/7 days a year and can be reached by calling 1-833-BLUEMSS or +1-833-258-3677. Only approved Client users will be allowed to talk with BlueVoyant SOC personnel.

CLIENT RESPONSIBILITIES

- Enable and configure logging on remote systems or devices per BlueVoyant instructions.
- Enable necessary firewall rules and any other network changes to route logs to Azure Sentinel.
- Provide an Azure dedicated management account with “Contributor” permissions required for Microsoft Sentinel management and configuration.
- Cover any expenses related to Azure Sentinel, Log Analytics, Logic Apps, and fees payable to Microsoft.
- Provide timely access to project stakeholders to support the objectives of this Service contemplated herein.
- Provide a Virtual Machine for a Log Collector Virtual Appliance (defined in this document) as needed. The log collector is required for onboarding logs from the network, security devices, other commercial cloud services, and custom log sources.
- Provide remote access for administration of the Log Collector Virtual Appliance, above.
- Provide access to an internal SME responsible for managing the specific log source type.
- Manage log retention & archiving: The Client is responsible for managing their log archiving processes for historical, backup, compliance, regulatory, or other requirements.
- Configure all log sources so that logs are appropriately sent to the agents and log collection devices. This includes, but is not limited to, any intermediary log sources. If changes to The Client’s existing network architecture are required for Service implementation, BlueVoyant will communicate these changes to The Client.
- Notify BlueVoyant of any environmental changes that may affect the execution of the Service.
- Install appropriate collecting agents, such as the Azure Monitoring Agent (AMA), and the Microsoft Monitoring Agent (MMA), software on Windows and Linux endpoints, as per BlueVoyant’s instructions.
- Configuring the network and security devices with the logging details provided by BlueVoyant (i.e., Syslog)
- Provide feedback on fine-tuning alerts and Playbooks when required.

- Provide detailed information on the network environment to facilitate the deployment of the BlueVoyant solution.
- Notify BlueVoyant of any necessary user account changes tied to Client employee termination; this includes employees or contractors that have access to the BlueVoyant Client portal or approval to contact the SOC.
- Perform additional remediation: During an investigation of security alerts, the BlueVoyant Security Operation Center may give guidance to a Client to perform specific actions in their environment to improve their security posture or to fully remediate an incident. The performance of these actions is the Client's responsibility.
- Obfuscate Personally Identifiable Information (PII) data in the Client's environment. BlueVoyant will not extract personally identifiable information from the Partner or Client environment or store it within the BlueVoyant environment except for only the sufficient log data for enrichment, case management, reporting, and automation purposes. No raw or PII data should leave the customer's M365 or Azure environment.
- Configure Lighthouse access for BlueVoyant SOC; as appropriate, the Client will register BlueVoyant as DPOR/CPOR/PAL.

Additional Details

Out of Scope

Any log sources not onboarded within the first 30 days of the "Go Live Date" will require billable hours to be onboarded.

Customer log sources must be onboarded and integrated within 30 days of the Go-Live Date of SOC coverage as they are critical to provide the contracted security service monitoring, and should not be delayed. If a log source is determined to require an extended on-boarding period beyond 30 days, then a separate consulting services agreement will be required.

In the event the the Client requests BlueVoyant to provide additional services that are outside of the scope of what is set forth in this Service Description, to the extent BlueVoyant is able to provide such services, the services will be mutually agreed in separate Statement of Works executed by both parties. More information about this can be found in the "Supporting features and teams Included in all MDR services" section. Available additional services include:

- Post-breach incident response & compromise assessment;
- Forensics;
- Vulnerability patching and resolution; and

- Tabletop exercises;
- Network architecture design;
- Hardware procurement; and
- Security or technology training for end users.

For BEC customers only, the below is also excluded:

- MDR for other M365 tools, such as Defender for Endpoint, Microsoft Defender for Cloud Apps and/or Defender for Identity
- MDR for Microsoft Sentinel, based on other log sources types outside of this service

Additional MDR Services Terms and Conditions

- MDR Services Termination: If an Service Order/Proposals including managed detection and response services is canceled or the MSA is terminated, the Client will have thirty (30) days from the time a cancellation request is initiated, or the MSA has expired (whichever comes first) to request the receipt of archived data. For the purposes of BlueVoyant's services for Client's Microsoft Sentinel, archived data will be any alerts stored in BlueVoyant's case management. Alert data will not contain any raw data from the Client's Azure Tenant, Microsoft Sentinel, or on-premises data. Hourly consulting fees will apply for time spent as well as data transfer costs related to archived data. If a request is not received within the thirty (30) day period, BlueVoyant will permanently destroy all archived data pertaining to security devices no longer under a valid Order Form.
- Customized solutions maintenance (i.e., customized connectors): BlueVoyant will monitor the health status of the customized solution and alert the customer when something breaks. BlueVoyant will not be responsible for repairing the issue; doing so might require a new professional engagement with a new cost (T&M)
- Log Source Continuity: Log sources listed in the initial scope of work cannot be exchanged or modified without a new statement of work.
- Modify Terms: BlueVoyant reserves the right to modify the terms of this Service Description, including the SLAs, 90 (ninety) days in advance of any modification's intended implementation date. Client reserves the right to terminate the Service, at no cost, should the modification(s) not be satisfactory to Client with 30 days prior notice.
- Risk Elimination: This Service Description provides expert security analysis and response to the Client. However, deployment of BlueVoyant managed detection and response services in a Client network does not achieve the impossible goal of risk elimination, and

therefore BlueVoyant makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on a Client network.

- MDR vs non-MDR Alerts: BlueVoyant will also track non-MDR-related alerts, with the goal of providing the Client's IT teams insight into IT hygiene and situational awareness of security-related activities. In addition to crafting rules to detect malicious activity, we are also creating value-add queries and detections to help your organization prioritize defensive measures, even in the absence of an incident. This feature and alerting is designed to provide actionable and contextual information within your environment regarding best practices, misconfigurations, and unusual activity. As many of these alerts are informational, they do not require your immediate attention; these rules are designed to provide visibility and assist in the strategic planning of immediate and future security initiatives. These alerts are focused on surfacing configuration issues, external scanning, and visibility of internal processes that may be abused by attackers. This category of informational alerts presents you with data you need to make strategic and impactful configuration changes, which a managed SOC provider cannot perform. Rather than exclude content that is not actionable by a third-party security provider, BlueVoyant has opted to develop this content as an optional value-add service to provide increased visibility and further partner with you on security advisory initiatives. That said, BlueVoyant will continue to observe these alerts to assist in tuning, whitelisting, and notable events we feel you should attend to. Additionally, there may be situations in which a 'hygiene' or 'visibility' alert provides valuable context to a malicious event - all alerts written by BlueVoyant are reviewed by our SOC in the event we detect malicious or suspicious activity on an entity (user, host, cloud resource) and will be presented in our malicious alerting for context and awareness. The context and objective of these alerts may pertain to specific vulnerabilities, out-of-date software, and operating systems, or otherwise benign or unsuccessful security events within your network. Though these events do not indicate a security breach, they provide valuable visibility into your overall exposure to threat actors. We recommend reviewing these alerts to best position your security strategy and roadmap, using data specific to your network, at a cadence that fits your needs. At the client's request, BlueVoyant can turn off all alerting within the scope of this feature. Additionally, BlueVoyant can also turn off specific alerts where you do not wish to receive portions of the content.

- Vulnerability Management System (VMS): The client will work with BlueVoyant to enable the automatic import of identified vulnerabilities into the Platform from a vulnerability assessment solution owned and maintained by the Client. The identified vulnerabilities will be visible to the SOC to inform and improve the quality of other BlueVoyant services and the Client can use Wavelength to track vulnerabilities and generate reports. This service can be provided as an add-on to additional BlueVoyant MSS services.

- Log Collector virtual appliance: Upon service termination, any BlueVoyant Log Collector virtual appliances will be deleted/removed unless other considerations are made. For more details, see the Log Collector appendix.

Data and Privacy

- Microsoft 365 and Microsoft Azure tenants are owned by the Client and as such, data is contained within the Azure and M365 customer subscription.
- BlueVoyant Sentinel team will require only Contributor Role access to the Client's Azure subscription/Resource Group where Sentinel will be deployed. No raw data will be transferred outside of the Client's Microsoft Azure or Microsoft 365 instance.
- Only log data may leave the Client's networks for enrichment, case management, reporting, and automation purposes. No raw or PII data should leave the customer's environment.
- More data on how Microsoft Cloud manages data and privacy can be found at https://azure.microsoft.com/en-us/overview/trusted-cloud/privacy/

Appendix

Appendix: MDR for Microsoft 365 Defender (Additional Details)

Service Overview: BlueVoyant MDR for Microsoft 365 Defender (the "Service") consists of BlueVoyant's monitoring of the contracted Client-owned Microsoft 365 environment and related security devices ("Devices") and application(s) ("Applications") as specified on the Service Order/Proposal. This Service provides the Client with near real-time, security event analysis across the Client's security and critical infrastructure 24 hours a day, 7 days a week per the terms of this Service Description. This Service utilizes the BlueVoyant platform ("The Platform") in conjunction with analysts in BlueVoyant's Security Operations Centers ("SOC") and the Client's Microsoft 365 tenant. The client is responsible for any license and consumption fees for their Azure environment including fees associated with Microsoft 365 and supporting components.

Management activities include Service implementation, configuration changes necessary for the successful provisioning of the Service, tuning the Microsoft 365 tenant for efficiency and cost optimization, as well as configuration updates in line with the BlueVoyant update policy described in this Service Description. Monitoring activities include collection, storage, reporting, and Client notification of security events or device health events in accordance with Service Level Agreements. Tools for self-reporting and analysis are provided through Wavelength™, the BlueVoyant Client Portal ("Wavelength"), as well as through Microsoft 365 and Microsoft Sentinel.

The activities and services provided as part of the Service fall into four segments, in line with Microsoft 365 feature areas, and these are described below.

I. MDR for Defender for Endpoint

MDR for Endpoint provides remote endpoint threat protection, response, and mitigation. It protects data, assets, and business operations by detecting malware to include ransomware variants, zero-days, non-malware, and file-less attacks. The BlueVoyant SOC will investigate and neutralize threats on your behalf 24/7, based on requirements and rules of engagement agreed upon by BlueVoyant and the Client. The client will provide access to, and licensing for, Microsoft Defender for Endpoint.

- Investigation & Notification: Once a suspicious event is detected or a prevention activity occurs, an alert is generated and a BlueVoyant security operations center analyst will perform triage and investigation of the event to confirm true positive, benign, or false positive. The client will be notified according to the nature of the event and service-level agreements.

- Indicator Enrichment: Indicators of compromise associated with detections are automatically extracted, scored, and enriched leveraging open source and BlueVoyant proprietary threat intelligence. Enriched indicators are visible within Wavelength™ and are assigned a reputation (ex: good, suspicious, bad) and classification (ex: botnet, Zeus, crypto-miner, etc.).

- Endpoint Response: BlueVoyant will take a specific set of response actions at the completion of an investigation, subject to the pre-approved action's profile established as part of MDR Services Activation (as that term is defined below).

    - Quarantine: Isolation of an endpoint so that it can no longer communicate with any other devices in the Client environment or to the Internet. BlueVoyant will move an endpoint into the quarantine state typically when there is evidence of lateral movement of an advanced threat within the Client environment or detection of command-and-control (C2) software attempting to beacon to an attacker's infrastructure.

    - Delete File: BlueVoyant will delete specific files on an endpoint if a specific file is known and confirmed to be malicious. File deletion can occur in broader cases per the direction of the Client as part of policy enforcement (ex: pre-approval to delete potentially unwanted programs).

    - Whitelist: Typically performed as a response to an application that is incorrectly being blocked or terminated as malicious by the advanced endpoint software, BlueVoyant will update policies to whitelist the application for proper execution or set the correct privileges and actions it is allowed to perform. Whitelisting applications are also performed as part of MDR Services Activation in order to reduce the likelihood of unintended business disruption.

- Monitor Only: As part of diagnosing misbehaving advanced endpoint software, a BlueVoyant security operations center analyst can move an endpoint into a monitor-only mode, this is done with collaboration with the Client. Monitor Only mode will direct the endpoint software not to interfere with any end-user activities on the endpoint.

- Blacklist: BlueVoyant will blacklist specific files on an endpoint if a specific file is known and confirmed to be malicious. Blacklisting a specific application either by computed hash or process name will inform the advanced endpoint software not to allow the application to run on any endpoint (that has the advanced endpoint software deployed).

- Remote Intrusion Response: As part of an advanced investigation, BlueVoyant will use the live/real-time response capabilities in the advanced endpoint software to perform intrusion response activities such as searching and modifying the registry, analyzing volatile memory, remote file deployment, and remote file retrieval. Remote Intrusion Response activities are subject to pre-approval guidelines set as part of MDR Services Activation.

- Threat Detection: BlueVoyant will leverage the advanced endpoint software to perform detections and provide visibility to activity on the endpoint. BlueVoyant expands the default detections deployed to the advanced endpoint software utilizing proprietary intelligence, indicator enrichment, and enhanced behavioral correlations.

  - Signature Detection: BlueVoyant will use traditional antivirus techniques to identify malicious software by the reputation of their computed hash.

    - BlueVoyant Signatures: BlueVoyant may detect new malware before it has been included into the signature database of advanced endpoint platforms. When this happens, BlueVoyant may deploy proprietary new signatures to the advanced endpoint software.

  - Behavioral Detection: BlueVoyant will classify activity on endpoints as distinct actions and then holistically analyze them as part of known tactics, techniques, and procedures (TTPs) to detect patterns of adversarial behavior. Behavioral Detection enables identification of malware, not by whether it has been seen previously by detection software, but instead by how it behaves. BlueVoyant may expand on the list of known TTPs provided by the advanced endpoint software with the BlueVoyant developed set of TTPs.

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

Service Elements

The following table presents a short summary of the MDR for Defender for Endpoint Service Features:

Description	MDR for Defender for EndPoint Service
• Defender for Endpoint Advanced configuration and setup	• Part of Microsoft 365 Accelerator service
• Defender for Endpoint MSSP Accounts provisioning & ongoing management	• Client's responsibility • BlueVoyant requires Admin access to Defender for Endpoint Portal and full access to REST APIs. Client will continue to have full access (Global Admin) access to Defender for EndPoint Portal
• 24x7 Defender for Endpoint security monitoring and response	• Included
• Defender for Endpoint on-going tuning	• Included
• Integration with customer Microsoft Sentinel instance • SOAR Automation	• Included • BlueVoyant SOC will monitor and respond to all security incidents originating from Defender for Endpoint. SOAR Automation is offered to selected Microsoft built-in Threat Anomalies policies
• Standard Managed Prevention	• Utilizing Microsoft Defender for Endpoint, BV will block malicious indicators of compromise (IOCs) and behaviors of compromise (BOCs) with expert review of detections to ensure there is always human oversight on technology.
• Customized Managed Prevention	• Manually written and managed custom enforcement policies to neutralize sophisticated malware and lateral

	movement utilizing ”living off the land” techniques that can potentially evade standard detections.
• Continuous Policy Adaptation and Enforcement	• In coordination with the Client, BlueVoyant will continuously review enforcement policies to ensure aggressive prevention does not impact sensitive business operations.
• Investigations/Root Cause Analysis:	• Remote root cause analysis of all positively identified malicious activity.
• Security incidents - manual remediation	• Included, subject to Client approval. • (No SLA/SLO is provided to this activity)
• Centralized reporting	• Via BlueVoyant SOC Wavelength Portal

II. MDR for Defender for Office 365

MDR for Defender for Office 365 provides threat detection, investigation, response and reporting against malicious threats posed by email messages, external links (URLs) in files, and collaboration tools.

- Security Support Services: The service includes a quarterly assessment of the security configurations enabled for Defender for Office 365, including assessing external email forwarding statuses for new users and domains, review of DKIM, DMARC, and SPF records, and a review of in console Email reports for continuous improvement opportunities. In addition, the team provides a Monday through Friday support service to support configurations, modifications, and change management within the Defender for Office 365 exchange admin console (EAC).

- Business Email Compromise Investigation Services: This is a component of the service which triages **non-user submitted** email alerts from Microsoft Defender for Office 365. The team will investigate the following alert types to identify severity and blast radius of the attack and escalate accordingly:

    - Email messages containing phish URLs removed after delivery
    - Email messages containing malware removed after delivery
    - Admin triggered manual investigation of an email

- A potentially malicious URL click was detected
- Suspicious email sending pattern detected
- User restricted from sending email

- Investigation & Notification: Once a suspicious event is detected or a prevention activity occurs, an alert is generated and a BlueVoyant security operations center analyst will perform triage and investigation of the event to confirm true positive, benign, or false positive. Client will be notified according to the nature of the event and service-level-agreements.
- Indicator Enrichment: Indicators of compromise associated with detections are automatically extracted, scored, and enriched leveraging open source and BlueVoyant proprietary threat intelligence. Enriched indicators are visible within Wavelength™ and are assigned a reputation (ex: good, suspicious, bad) and classification (ex: botnet, Zeus, crypto-miner, etc.). Certain indicators will also be updated within Microsoft Sentinel
- Key Services Delivered:
    - Report on suspicious activity around file content and email and Teams content, for example, if malicious content is detected and file quarantine may be required.
    - Monitor configuration settings for Safe Links and URLs within emails, messages, and Office files.
    - Centralized SIEM Alerting, Automation and Remediation: Through Sentinel integration, BlueVoyant SOC will provide advanced playbooks to automate the response for several built-in Threat Detection policies provided by Microsoft
    - Monitor for suspicious phishing or other alerts, based on standard or custom alert policies, and apply specified playbook
    - Additional details:
        - Standard Managed Prevention: Utilizing Microsoft Defender for Office, automatically block malicious indicators of compromise (IOCs) and behaviors of compromise (BOCs) with an expert review of detections to ensure there is always human oversight on technology.
        - Continuous Security Policy Adaptation and Enforcement: In coordination with the Client, BlueVoyant will assist with continuously reviewing enforcement policies to ensure aggressive prevention does not impact business operations.

- Manual Remediation: In instances where malware has evaded Defender for Office visibility, BlueVoyant will manually quarantine computers and/or terminate and delete malicious activity, as authorized by Client.
- Investigations/Root Cause Analysis: Remote root cause analysis of all positively identified malicious activity using telemetry from Defender for Office, and, if BlueVoyant is providing additional services (i.e. MDR for Microsoft Sentinel), will investigate other available telemetry from other sources to which BlueVoyant has access.
- Integration with Microsoft Automated Investigation and Response. BlueVoyant SOC will provide incident response information via the Wavelength Client portal and appropriate comments and responses will also be communicated via Microsoft Sentinel reports and console.

Service Elements

The following table presents a short summary of the MDR for Defender for Office 365 Service Features:

Description	MDR for Defender for Office Service
• Defender for Office Advanced configuration and setup	• Part of BlueVoyant Microsoft 365 Accelerator service
• Defender for Office MSSP Accounts provisioning & ongoing management	• Client's responsibility • BlueVoyant requires Global Admin access to Defender for Office Portal and full access to REST APIs. Client will continue to have full access (Global Admin) access to Defender for Office Portal
• 24x7 Defender for Office security monitoring and response	• Included
• Defender for Office on-going tuning	• Included
• Integration with customer Microsoft Sentinel instance • (SOAR Automation)	• Included • BlueVoyant SOC will monitor and respond to all security incidents originating from Defender for Office. SOAR Automation is offered to selected Microsoft built-in Threat Anomalies policies

• Data Loss Prevention Advanced configuration and support	• Included in Microsoft 365 Accelerator service. • Client is responsible to manage the ongoing DLP policy in accordance with its organization security policies. All DLP related security incidents originating from Defender from Office 365 will not be responded to by the BlueVoyant SOC, but will flow through Microsoft Sentinel and alerts forwarded to Client.
• Security incidents - manual remediation	• Included, subject to Client approval. • (No SLA/SLO is provided to this activity)
• Centralized reporting	• Via BlueVoyant SOC Wavelength Portal
• End user interaction	• Client is responsible to address all end-user trouble tickets and communication
• Content Search, Message trace, custom reports (outside of identified security incidents)	• Included, subject to additional fees (Microsoft 365 Concierge service)
• Service Assurance Reports	• Not included. Client can schedule their own reports (compliance and audit) via Defender for Office Portal

III. MDR for Defender for Identity

MDR for Defender for Identity monitors the signals and events returned by Microsoft 365 Defender for Identity, and provides the ability to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization via on-premises Active Directory domain controllers, and Active Directory Federation Services, including hybrid scenarios.

- Key Services Delivered:
    - Protect user identities and credentials stored in Active Directory

- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain, including potential compromised credentials and detecting potential lateral movements inside the network.
- Provide clear incident information on a simple timeline for fast triage
- Centralized SIEM Alerting, Automation and Remediation: Through Sentinel integration, BlueVoyant SOC will provide advanced playbooks to automate the response for several built-in Threat Detection policies provided by Microsoft
- Monitor Azure ATP sensors health and status and alert Client on possible outages (health issues)
- The following alert types are supported use cases:
  - Security Principal Reconnaissance
  - NMAP Reconnaissance
  - DC-Sync Attacks (Directory Services Replication)
  - Suspected Pass the Ticket (Identity theft)
  - Kerberos and NTLM brute force attacks
  - SMB User and IP address reconnaissance

Service Elements

The following table presents a short summary of the MDR for Defender for Identity Service Features:

Description	MDR for Defender for Identity Service
• Defender for Identity Advanced configuration and setup	• Part of Microsoft 365 Accelerator service
• Defender for Identity MSSP Accounts provisioning & ongoing management	• Client's responsibility • BlueVoyant Guest account to be added into Client AD AzureATP_(instance name) Administrators group. Additionally for automatic alert extraction, BlueVoyant SOC will require access to Defender for Identity REST APIs
• Azure ATP sensors health and status monitoring	• Included

• Integration with Client Microsoft Sentinel instance • (SOAR Automation)	• Included • BlueVoyant SOC will monitor and respond to all security incidents originating from Defender for Identity via Microsoft Sentinel.. SOAR Automation is offered to selected Microsoft built-in Threat Anomalies policies
• Periodic review of Defender for Identity configuration	• Monthly
• Deployment and management of Defender for Identity sensors in customer environment	• Client responsibility

IV. MDR for Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security)

MDR for Microsoft Defender for Cloud Apps provides protection, detection, response, and mitigation powered by Microsoft's Defender for Cloud Apps solution. Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and the modern features of its reverse proxy.

All of these techniques and monitors provide a rich level of events and incidents to the BlueVoyant SOC that enable rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

While Microsoft Cloud Application security offers DLP and compliance features, these features are out of scope for detection and response services.

Alerts with category: Threat Detection within MCAS offer the highest quality detections for MDR, and are in scope for the service:

- Impossible Travel
- Multiple Failed Login attempts to a service
- Activity from TOR IP address

- Multiple failed login attempts
- Suspicious oauth app file download activities
- Data exfiltration to an unsanctioned app
- Discovered app security breach
- Multiple powerBI sharing report activities
- Malware detection
- Misleading oauth app name
- Mass download by a single user
- Cloud discovery anomaly detection
- File shared with personal email addresses
- Data exfiltration to an app that is not sanctioned
- Activity from an anonymous proxy
- Activity from infrequent country
- Externally shared source code
- Logon from risky IP address
- New high volume app
- External user added to Teams
- Investigation priority score increase
- Ransomware activity
- Suspicious inbox manipulation rule
- New high upload volume app

- Key Services Delivered:
  - 24x7 Cloud App Monitoring and response: Monitors suspicious behavior and provides detailed visibility of alerts and their responses within the Sentinel integration.
  - On-going MCAS policies tune-up: BlueVoyant SOC will adjust all MCAS policies in order to reduce the number of false positives alerts
  - Centralized SIEM Alerting, Automation and Remediation: Through Sentinel integration, BlueVoyant SOC will provide advanced playbooks to automate the response for several built-in Threat Detection policies provided by Microsoft
  - Application labeling and categorization: BV SOC via custom developed MCAS policies will assist the Client with app tagging (sanctioned vs. unsanctioned)
  - Support and remediation of security incidents related to users with high investigation score: BlueVoyant SOC has developed a set of Sentinel alert rules and playbooks to actively remediate incidents related to high investion priority score users (score>100)
  - Conditional Access App Control apps: BlueVoyant team will assist Client with setup and monitoring of new SAML applications (subject to scope of Consulting Concierge Services)

  Via Sentinel integration, our MDR service will monitor, triage and respond to the following alert types:

  - Activity policy violation: This type of alert is the result of a policy you created.
  - File policy violation: This type of alert is the result of a policy you created.
  - Compromised account: This type of alert is triggered when Cloud App Security identifies an account that was compromised. This means there's a very high probability that the account was used in an unauthorized way.
  - New location: An informative alert about access to a connected app from a new location, and it's triggered only once per country/region.
  - New discovered service: This alert is an alert about Shadow IT. A new app was detected by Cloud Discovery.
  - Suspicious activity: This alert lets you know that anomalous activity has been detected that isn't aligned with expected activities or users in your organization.

- Use of personal account: This alert lets you know that a new personal account has access to resources in your connected apps.
- Use of unsanctioned application: When using a list of sanctioned apps in the Cloud app catalog, this alert will inform if an unsanctioned application is being used or attempted access.

Service Elements

The following table presents a short summary of the MDR for MCAS Service Features:

Description	MDR for MCAS Service
• MCAS Advanced configuration and setup	• Part of Microsoft 365 Accelerator service
• Account MSSP MCAS provisioning & ongoing management	• Client's responsibility • BlueVoyant requires Global Admin access to MCAS Portal and full access to MCAS REST APIs
• 24x7 Cloud App security monitoring and response	• Included
• MCAS Security Policies on-going tuning	• Included
• Development of new MCAS policies (as per Client's request)	• Included • (Standard Concierge Service)
• Integration with customer Microsoft Sentinel instance (SOAR Automation)	• Included • BlueVoyant SOC will monitor and respond to all security incidents originating from MCAS. SOAR Automation is offered to selected Microsoft built-in Threat Anomalies policies
• Periodic review of MCAS policies with Client	• Monthly
• App tagging (sanctioned vs. unsanctioned)	• Included • Client is required to provide regular feedback

• High Investigation Score Users	• Included in service and offered via Microsoft Sentinel alert rules and playbooks
• Conditional Access App Control	• Included • Onboarding of new SAML apps in MCAS is subject to additional fees (Consulting Concierge Service)
• Service Health Security Monitoring	• Included • BlueVoyant SOC will monitor the status of log collector(s) and app connector(s) events flows and report if any disruptions
• Management of Docker image (Log Collector)	• Client responsibility
• MCAS Data Enrichment	• Included in Microsoft 365 Accelerator service. • Additional changes requested by Client are subject to additional fees (Consulting Concierge Services)
• Deployment and management of MCAS agents, sensors, collectors on customer environment	• Client responsibility

A. Appendix: Advanced Threat Hunting (Service Details)

Advanced Threat Detection: BlueVoyant's Tier 2 Managed Detection and Response (generally referred to as "Threat Hunting", but also includes additional capabilities as described below) may be added as an additional extended service to BlueVoyant MDR Services and includes all detection and service delivery components of Tier 1 (Standard MDR), with additional detection capabilities and techniques, as listed here.

- Anomaly Detection: BlueVoyant will perform statistical analysis of several types of endpoint metadata to identify anomalous user, process, and endpoint activity that could indicate malicious use. BlueVoyant uses anomaly models to detect malicious activities that cannot be identified from distinct events, such as uncommon network flows, unusual authentication events and lateral movement.

- Threat Hunting: Some advanced adversaries can evade the standard detection mechanisms of cyber security detection tools. BlueVoyant will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions. BlueVoyant will also conduct remote hunt missions that will perform manual and semi-automated activities for targeted data analysis to search for signs of advanced adversaries. Additional action may be required by the Client depending on the severity of findings.

- Forensic Artifact Analysis: BlueVoyant Threat Hunters perform advanced forensic artifact collection and analysis to triage anomalous events and determine adversary activity beyond actions captured by real-time telemetry.

- Attacker Abuse Insights: BlueVoyant Threat Hunters continuously analyze endpoint data to identify tools, configurations, and security hygiene concerns that would benefit an adversary. BlueVoyant shares these insights via our weekly threat intelligence reporting with our Clients, along with mitigation recommendations, to better prepare endpoint defenses for any findings that can be actioned via the Endpoint Agent.

- Ad-hoc IOC Discovery: As BlueVoyant researchers and Clients identify new indicators of compromise or new attacker methodologies, BlueVoyant Threat Hunters proactively search Client environments for specific network connectivity events associated with these IOCs and provide response actions and recommendations based on any findings.

Microsoft Partner Associations

Microsoft encourages partners to associate themselves with the Microsoft customers supported through the delivery of their solutions and services. These associations provide visibility for Microsoft to identify and recognize partners who are helping customers achieve business objectives and realize value in the cloud. As a result, high performing partners receive targeted investment that helps us innovate our solutions, upskill our talent, and expand our coverage to better protect your business or organization.

Partner Admin Link (PAL)

All Azure services included in the delivery scope will be registered for PAL.

Partner Admin Link (PAL) enables Microsoft to identify and recognize where BlueVoyant is helping customers achieve business objectives and realize value in the cloud. Customers must

provide access to their Azure resources. Once access is granted, the partner's Microsoft Partner Network ID (MPN ID) is associated. This association helps

Microsoft understands the ecosystem of service providers and to refine the tools and programs needed to best support customers.

Frequently asked questions,

- What data does PAL collect?

  The PAL association to existing credentials provides no new customer data to Microsoft. It simply provides the telemetry to Microsoft where a partner is actively involved in a customer's Azure environment. Microsoft can attribute influence and Azure consumed revenue from customer environment to partner organization based on the account's permissions (Azure role) and scope (Management Group, Subscription, Resource Group, Resource) provided to the partner by the customer.

- Does this impact the security of a customer's Azure Environment?

  PAL association only adds partner's MPN ID to the credential already provisioned and it does not alter any permissions (Azure role) or provide additional Azure service data to partner or Microsoft

Claiming Partner of Record (CPOR)

All Microsoft 365 workloads included in the delivery scope will be registered for CPOR.

CPOR enables Microsoft to identify and recognize partners who are helping customers achieve business objectives and realize value in the cloud. Once BlueVoyant associates itself to a workload or subscription they will obtain access to usage and/or sold seats data. This association allows BlueVoyant to monitor active usage and utilization while providing recommendations of how to maximize usage/utilization. BlueVoyant will not have access to any other customer data.