VULNERABILITY MANAGEMENT SERVICE

Service Description

1. Description of Service: This document ("Service Description") describes the vulnerability management service ("VMS" or "Service") offered by BlueVoyant to its customers ("Customer", "Client", or "you") pursuant to a service order explicitly authorizing the purchase and sale of the Service. For the avoidance of doubt, the terms of BlueVoyant Master Services Agreement ("MSA") available at https://www.bluevoyant.com/bvmssterms shall govern in the absence of a master services agreement signed by BlueVoyant superseding those terms.

2. Service Overview: The Service helps Clients collect data needed to identify, investigate, and prioritize the remediation of vulnerabilities and misconfigurations in their IT environment. Results are reported via the BlueVoyant platform, our cloud-based ingestion, processing, analysis, and reporting system (the "Platform"). The Service is supported by a team of analysts in the BlueVoyant Security Operations Centers (SOCs), and includes Service implementation, configuration changes necessary for successful provisioning, as well as vendor software updates in line with the BlueVoyant software update policy described below.

3. Service Tiers: BlueVoyant offers three tiers of VMS service:

3.1

Tier 1: Vulnerability Import: Within this tier, the Client will work with BlueVoyant to enable the automatic import of identified vulnerabilities into the Platform from a vulnerability assessment solution owned and operated by the Client. The identified vulnerabilities will be visible to the Security Operations Center to inform and improve the quality of other BlueVoyant services and the Client can use Wavelength™ to track vulnerabilities and generate reports.

3.2

Tier 2: Vulnerability Scanning: Expanding on the previous service tier, within this service tier BlueVoyant will work with the Client to deploy virtual appliances and conduct asset discovery and vulnerability assessments internally in the Client's environment. BlueVoyant will also use our third party vulnerability management supplier (currently Qualys) to perform external scanning, it being understood that the vendor owns the services it provides and the Client will not receive any

direct right or license to use the supplier's services. Clients within this tier of service will have access to Wavelength™| to track vulnerabilities, assets discovered as part of the vulnerability scan ingestion, as well as related reports. BlueVoyant will schedule Qualys reports ranging from PCI reporting, Executive and Technical reports, Qualys Top 20 report, and Qualys Patch reporting. Reports will be delivered via email in an exportable format: CSV, XML, HTML, DOCX, PDF, and MHT.

3.3

Tier 3: Co-Managed Scanning: Expanding on the previous service tier, Clients within this service tier will also have access to the Client experience offered by our third party vulnerability management supplier's product. Client provisioned access to the vendor product will experience more advanced vulnerability management capabilities. With the CoManaged tier, Client will receive a third party license as part of the service or will bring their own license. BlueVoyant will work with Clients to ensure they have what they need to provision accounts for the Platform, and/or personnel to assist with policy management, vulnerability scanning scheduling, and other configuration items.

A summary of the Service on a tier-by-tier basis is below:

Service Feature	Tier 1 Vulnerability Import	Tier 2 Vulnerability Scanning	Tier 3 CoManaged Scanning
Internal Scanning		✓	✓
External Scanning		✓	✓
Asset Discovery	✓	✓	✓
Software Upgrades		✓	✓
Vulnerability Tracking	✓	✓	✓
BlueVoyant Vulnerability Reports	✓	✓	✓
Integration with BlueVoyant MSS	✓	✓	✓
Detailed Reports			✓

4. Service Features:

4.1 Vulnerability Assessment: Tiers 2 and 3 of the Service utilize both external and internal scanning to perform vulnerability assessments of agreed IT environments, and discover known weaknesses in software. If vulnerabilities

are discovered, remediation recommendations are provided through the BlueVoyant Portal, as well as supporting reports. Additional details are below.

4.1.1 External Scanning: Through external scanning, BlueVoyant seeks to detect vulnerabilities that are exposed beyond the Client's network perimeter and are therefore visible and possibly exploitable by attackers. External scanning is conducted against Internet facing assets -- assets not accessible with a routable IP address will not be scanned. Scans are conducted from BlueVoyant systems and/or systems hosted by the vulnerability management supplier and directed at the Client infrastructure.

4.1.2 Internal Scanning: Through internal scanning, BlueVoyant looks to detect vulnerabilities within the Client's organization that may not be externally facing to an attacker, but could be exploitable by attackers within the environment. The internal vulnerability assessments can perform authenticated scans to obtain the highest level of detail on what software is running on the device, it's patch levels, and possible vulnerabilities. Internal scanning requires the deployment of appropriate infrastructure as described in Service Activation.

4.1.3 Scan Frequency: Clients can elect for scans to be conducted on a regular basis at monthly or quarterly intervals for tier 2; and weekly, monthly, or quarterly for tier 3. Scan frequency is established by Client request during service activation, but can be modified at any time. The Client can request execution of ad-hoc re-scans up to four (4) times per month.

4.1.3.1 On-Demand Scanning: BlueVoyant can conduct vulnerability scans on an as-needed basis with a one (1) business day lead time. OnDemand scans are limited to one (1) per month for tier 2, and four (4) per month for tier 3.

4.1.4 Remediation Verification: By comparing new vulnerability scan results against previously identified vulnerabilities, the Service will help 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.

4.1.5 Policy Selection: As part of Service Activation, BlueVoyant staff will work with the Client to understand what their compliance and risk goals are, relative to the impact that vulnerability scanning may make

in their environment and select an appropriate pre-configured scanning policy.

BlueVoyant's VMS Service does not include Web Application Security Scanning.

4.2 Asset Discovery: As part of the Service, assets will be discovered as through normal vulnerability scanning. Asset records will be automatically created as part of processing detected vulnerabilities from the vulnerability assessment software. BlueVoyant will use reasonable efforts to keep the asset repository fresh, accurate and reduce the possibility of duplicate asset records or stale assets.

4.2.1 Asset Prioritization: Through the BlueVoyant Portal, Clients can assign criticality to asset records to indicate which assets are the most important in their environment. When the Service is combined with other BlueVoyant Managed Services, this enables the BlueVoyant Security Operations Center to better understand risk in the environment and take correct action in Client notifications or response actions.

4.2.2 Asset Tagging: Through the BlueVoyant Portal, Clients can apply "tags" to asset records. This enables grouping of assets by Client defined criteria to support dashboards and reports.

4.3 Vulnerability Tracking: Through the BlueVoyant Portal, the Client will be able to see all active vulnerabilities that have been detected in their environment. 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.

4.4 Reports: Through the BlueVoyant Portal, the Client will have access to OnDemand vulnerability reports. Vulnerability reports contain content such as new vulnerabilities, resolved vulnerabilities, critical vulnerabilities on critical assets, and other similar content.

4.5 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 (a software package that runs on Client provided equipment to enable the service) and Platform.

4.6 Integration with BlueVoyant Managed Services: A significant value of the Service is knowledge of the vulnerabilities and exploitation risk which exists within the Client's environment provided to the BlueVoyant Security Operations Center. These insights may support security investigations to understand possible root cause for security incidents or how easily an attacker may traverse across systems within a Client's environment in order to inform the best response action.

4.7 Compatibility with BlueVoyant Managed SIEM: Vulnerability dashboards can be deployed within SIEM to monitor the Vulnerability program. Depending upon the technology selected, clients may have to provision virtual instances to host the scanning solution for internal scans. External scans can be configured and initiated from the vendor's cloud environment. Internal scanning can be done at the against network segments, or if desired, the vendor's scanning agent can be installed on a per-instance basis. Both network scanning and per-device scanning can be combined, as some device types, like network switches, wouldn't be able to typically run a local scanning agent, but could be scanned via a network appliance as part of an internal scan. Note that as with other scanning configurations, Managed SIEM clients will have full visibility into their scanning data via Wavelength™, including a list view of vulnerability scans as well as full details within specific vulnerability entries.

5. Existing Product Purchase ("BYOL"): If a supported vulnerability scanning solution is already deployed and licensed directly with the Client, the Client can purchase CoManaged Scanning (Tier 3) and engage BlueVoyant for vulnerability scanning.

   The Client will be responsible for provisioning a user account with appropriate privileges for the BlueVoyant SOC to enable the service. The Client will remain responsible for the terms & condition of their contract, billing, and invoicing with the vendor.

6. Supporting Features and Teams

   6.1 Security Operations Center (SOC): The Service is supported by the BlueVoyant Security Operations Center which operates 24 hours a day, 7 days a week, across multiple locations.

   6.2 **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 security operations center analysts, view all detected assets, and view vulnerabilities.

6.2.1 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.

6.2.2 Reports: Available through Wavelength™, reports include Client environment content related to alerts, incidents, indicators, assets and vulnerabilities.

6.3 BlueVoyant Client Experience Team: The Client Experience team is the primary support team for the Client. The assigned technical account manager acts as the Client's consultant and enables the best experience for BlueVoyant services. The advisor will meet with the Client on a regular basis (most often monthly) to understand Client's security program goals and will advise how BlueVoyant services can best meet their needs. The advisor is also engaged in any significant security events that occur for the Client. Additionally, the advisor will deliver any requested feedback to the BlueVoyant product and service delivery teams.

7. Client Communications: Below is the standard methods that the Service enables for the Client to obtain information related to the Service or engage BlueVoyant staff.

7.1 BlueVoyant Customer Portal (Wavelength™): Wavelength™ is the primary method for Clients to stay informed of security activity in their environment and activities of the BlueVoyant Security Operations Center. At any time, a Client end user may go to the BlueVoyant Portal and review any vulnerabilities, dashboards, or reports.

7.2 Email: The Client will receive Emails as a regular function of the Service. 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 the BlueVoyant Portal.

7.3 Calling Security Operations: The BlueVoyant Security Operations Center (SOC) is available 24/7/365 days a year and can be reached by calling 1-833-BLUEMSS or 1-833-258-3677. Only approved Client end-users will be allowed to talk with BlueVoyant Security Operations and will be authenticated when their call is received.

8. Service Level Agreements

8.1 Service Availability: The Client shall receive a communication (according to the escalation procedures defined or in the manner pre-selected in writing by client, either through email) to security availability issues according to the matrix below.

Impact	Definition	Agreement	Notification Method
Priority 1	In the situation of a Priority 1 issue, defined as preventing the service from functioning, or the BlueVoyant Portal outage, BlueVoyant will notify the Client in accordance to the agreement.	**4 business hours** of detection	Email
Priority 2	In the situation of a Priority 2 issue, defined as one or more significant components supporting the Service as unavailable, BlueVoyant will notify the Client. For example, OnDemand reports are unavailable.	**24 business hours** of detection	Email

8.2 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 the next business day from the time stamp on the Service Request ticket created by the Platform.

8.3 Maintenance Windows: BlueVoyant may schedule maintenance outages for BlueVoyant software which enables vulnerability assessments with 24-hours'

notice to designated Client contacts. SLAs shall not apply during maintenance outages and therefore are not eligible for any SLA credit during these periods.

8.3.1 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.

8.4 Client Service Outage: The SLAs 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.

8.5 Third Party Outage: SLAs are not applicable for any outages of the third-party vendor's software related to the delivery of vulnerabilities to the Platform or performance of vulnerability assessments.

9.0 Service Activation: Service activation ("Service Activation") consists of three phases: introduction, provisioning, and tuning. Service Activation begins once the signed Service Order is received and ends with the activation of the Service. Service Activation is dependent on a number of factors, such as the number of physical sites, the complexity of the Client's network, Client requirements, and the ability of Client to provide BlueVoyant with requested information and deployment of supporting software and configuration within a mutually agreed-upon timeframe. BlueVoyant does not provide SLAs for completing Service Activation within a specified period of time.

9.1 Introduction Phase: The introduction phase facilitates information gathering and begins with project kickoff. During the phase there are Introductions between key BlueVoyant and Client staff and Client priorities, expectations, and project timelines are established.

9.1.1 BlueVoyant Project Manager: At the beginning of Client deployment, a BlueVoyant implementation project manager will be assigned and coordinate the onboarding process. The implementation project manager will work with the Client to establish their timeline goals and

what sources and devices will be onboarded in what priority and timeline and when they will move to steady-state monitoring.

9.1.2 Client Experience Team: At the beginning of Client deployment, a BlueVoyant Client Experience Advisor will be assigned to the Client. This person will work directly with the Client and will act as their main point of contact beyond direct calls to the Security Operations Center.

9.1.3 Network Segments: BlueVoyant will work with the Client to understand their network environment and the best deployment locations for BlueVoyant Virtual Appliances to ensure proper vulnerability assessment coverage.

9.1.4 Approved Notification Plan: The Client and BlueVoyant will discuss and agree upon rules of engagement for service operation which includes primary contact points for any service outages or maintenance window notifications.

9.1.5 Scan Policy and Frequency: BlueVoyant will work with the Client to understand their risk and compliance goals and select the best vulnerability scan policies and scan frequency to meet their vulnerability assessment needs. Scan frequency can be conducted on a weekly, monthly, quarterly, semi-annual, or annual basis. Ad hoc scans are also supported with coordination with BlueVoyant.

9.1.6 Cloud Infrastructure: In order to perform vulnerability assessments against cloud infrastructure many cloud providers such as Amazon AWS, Microsoft Azure, and Google Cloud Platform require prior written approval. During the introduction phase, the Client will identify infrastructure that is hosted with a cloud provider and BlueVoyant will work with the Client to obtain prior approval for the scan frequency of that infrastructure.

9.2 Provisioning Phase: The provisioning phase is focused on deployment of the advanced endpoint software to endpoint visibility and response actions.

9.2.1 BlueVoyant Virtual Appliance: Deployment of the BlueVoyant Virtual Appliance (a software package that runs on Client provided equipment to enable the service) at specific locations in the Client environment to enable vulnerability assessments. BlueVoyant will provide system requirements for the software deployment to the Client.

9.2.2 Wavelength™ User Onboarding: Client will provide a list of identified users and their email addresses for access to Wavelength™ and Security Operations Center. Client users will receive an onboarding email to access the BlueVoyant Portal and will configure multi-factor authentication with their device. BlueVoyant will conduct Wavelength™ training for Client users.

9.3 Tuning Phase: BlueVoyant will use the first 14-30 days post installation to identify a baseline of the Client environment and tune the Service.

9.3.1 Inventory of Assets: 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 the Client and contextualization will be applied. This includes the identifying "Key Terrain" devices and applications as well as asset tagging and assigning asset criticality.

9.4 Onsite Deployment: Should onsite installation and configuration be necessary, BlueVoyant will provide such a resource for an additional fee as well as travel and lodging expenses.

10.0 Client Responsibilities

10.1 Software Deployment: If required, during the service activation process, the Client will deploy the BlueVoyant Virtual Appliance software on provisioned devices.

10.2 Notification of Environment Changes: Client will notify BlueVoyant of any environment changes that may affect the execution of the Service.

10.3 Notification of User Changes: Client will 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 Security Operations Center.

10.4 Internet Access: Client is required to maintain Internet connection for BlueVoyant Virtual Appliances so they can deliver scan results back to the Platform.

11.0 Other Services & Capabilities (Not Included): Below is a list of other notable services and capabilities provided by BlueVoyant that are outside the scope of this Service. These services and capabilities can be purchased alongside this Service.

11.1 Managed Detection and Response (MDR): Advanced detection of threats against the Client's endpoints with supporting response action including process termination, whitelisting, blacklisting, and quarantining.

11.2 Detection-as-a-Service: Monitoring of Client's devices and infrastructure for security and compliance.

11.3 Managed SIEM: Delivered utilizing Splunk as a best-of-breed Security Information and Event Management tool to monitor the Client's devices and applications. Clients have access to Splunk directly to create their own searches and correlations.

12.0 Out of Scope: The parties agree that services, deliverables and equipment not listed in the applicable Service Order (as agreed to by the parties) are out of scope and are not part of this Agreement. In the event the Client requests BlueVoyant to provide serves that are outside of the scope of this Schedule, to the extent BlueVoyant is able to provide such services, the services will be detailed in a statement of work executed by both parties.

12.1 Breach Response & Compromise Assessment

12.2 Forensics

12.3 Vulnerability Patching and Resolution

12.4 Tabletop Exercises

12.5 Network architecture design

12.6 Hardware procurement

12.7 Security or Technology Training for End Users

13.0 Service Prerequisite: The Service requires that the Client purchase alongside or already have purchase either the BlueVoyant Protected Endpoint, Managed Detection and Response ("MDR"), Detection-as-a-Service ("DaaS") or Managed SIEM service. The Vulnerability Management Service is an add-on service to either of those services.

14.0 Service Termination: If the Service Order with BlueVoyant is cancelled or the Agreement is terminated, the Client will have thirty (30) days from the time a cancellation request is initiated, or the Agreement has expired (whichever comes first) to request the receipt of archived data. Hourly consulting fees will apply for all time spent restoring the archived data. If a request is not received within the 30 day period, BlueVoyant will permanently destroy all archived data pertaining to security devices no longer under a valid Service Order or Agreement.

15.0 Additional Service Terms and Conditions:

15.1 Modify Terms: BlueVoyant reserves the right to modify the terms of this Service Description, including SLAs, with 30 days prior notice.

15.2 Impact to Environment: The nature of vulnerability assessments is such that certain vulnerabilities and mis-configurations of Client devices can pose risks when scanned. BlueVoyant cannot guarantee that the VMS vulnerabilities assessment will not adversely affect the performance or availability of the targeted systems.

15.3 **Third Party Product:** Relevant to Tier 2 Vulnerability Scanning; Qualys, Inc. will retain ownership of the cloud services it provides. The Client will not receive any right or license to use the Qualys cloud services.

15.4 Indemnification: Client agrees to indemnify, defend, and hold BlueVoyant harmless from and against any and all claims, losses, liabilities and damages, including reasonable attorney's fees, arising from any and all third party claims brought against BlueVoyant that arise out of the scanning, testing, and/or evaluation of incorrect or unauthorized IP addresses that are provided by Client or any breach of a Client representation or warranty.

15.5 Discovery: BlueVoyant does not guarantee that every vulnerability on every tested device will be discovered. BlueVoyant does not guarantee that every identified vulnerability is a true vulnerability.