MDR, POWERED BY ARCTIC WOLF - SERVICE GUIDE

Last Modification Date: 09/22/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 OVERVIEW

1.1 ARCTIC WOLF MANAGED DETECTION AND RESPONSE (MDR) SOLUTION PROVIDES 24×7 MONITORING OF YOUR NETWORKS, ENDPOINTS, AND CLOUD ENVIRONMENTS TO HELP YOU DETECT, RESPOND, AND RECOVER FROM MODERN CYBER ATTACKS. THIS SERVICE IS SUPPLIED BY ARCTIC WOLF'S MSP+ AND IS INTENDED TO BE PAIRED WITH OTHER MANAGED SERVICES TO DELIVER A MORE COMPLETE MANAGED SECURITY EXPERIENCE.

2 SERVICE DESCRIPTION AND DETAILS

Managed Detection and Response (MDR) eliminates alert fatigue and false positives to promote a faster response with detection and response capabilities that are tailored to the specific needs of your organization. Your Arctic Wolf Concierge Security® Team (CST) works directly with you to perform threat hunting, incident response, and guided remediation, while also providing strategic guidance tailored to the unique needs of your environment.

Specific features and functionality provided as part of the Solution include:

- collection of Solutions Data, including Customer's system logs, from Customer's systems using Equipment,
- analysis by Arctic Wolf Security Services of both Equipment and log data through the correlation of Solutions Data with threat and vulnerability information,
- scanning of Customer's internal and external systems,
- escalation of Security Incidents (as defined below) in need of attention by Customer as set forth herein,
- advisory recommendations to intended to improve Customer's security robustness,
- calculation of Customer's Security Score, as more fully described below,
- Log Search capabilities, if purchased by Customer, as evidenced on an Order Form,
- Host Containment functionality (as more fully described below), and
- regular summary Executive Dashboard reports, as described herein and the Documentation.

NOTE: The performance of the Solution, including specifically, notification of Emergencies or Security Incidents, as defined below, will not commence until after onboarding is complete (Service Activation).

The performance of remediation services for Security Incidents (as defined below), the re-imaging of Customer's systems, or change of policy settings is outside the scope of this Solution, but may be provided through other Managed Services.

3 ROLES AND RESPONSIBILITIES

	Client	InterVision Managed Services	Extended InterVision Services**	Arctic Wolf Security Operations
Installation and Configuration				

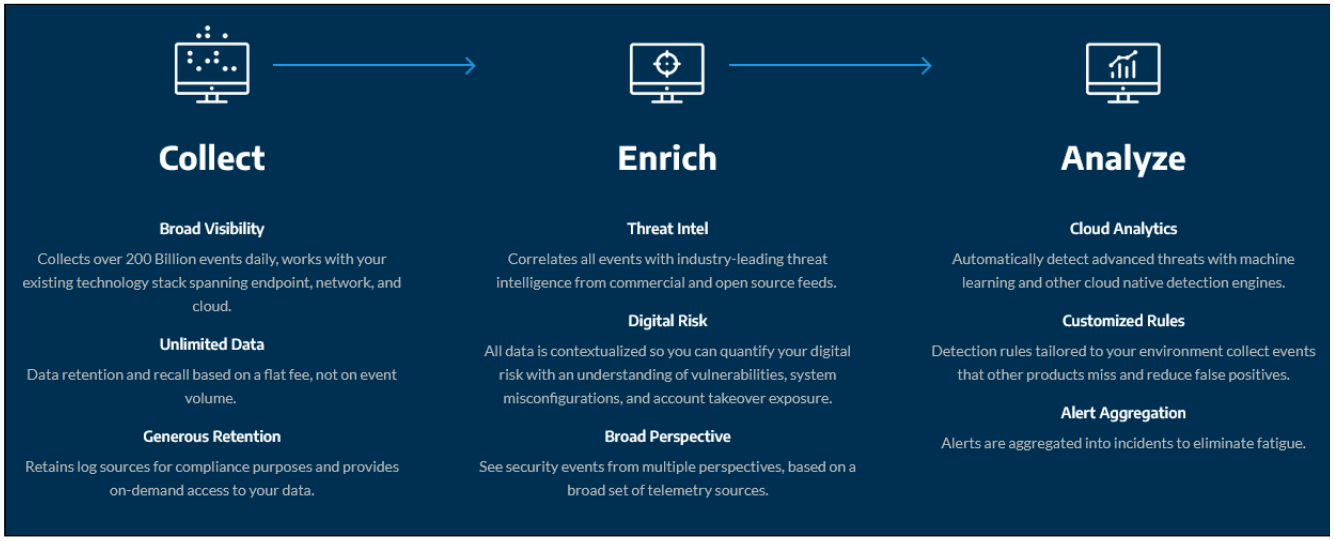
Agent Deployment	X		X	
Sensor Deployment	X		X	
Logging Configuration	X		X	
Monitoring Environment Configuration				X
Monitoring				
Log Search	X*		X*	X
Monitoring, Incident Generation, Investigation, Threat Hunting, and Escalation				X
Rule Implementation and Tuning				X
Incident and Problem Management				
Incident Notification + Escalation				X
Remediation Recommendations				X
RCA for incident				X
Vendor Escalation	X		X*	
Remediation				
Isolate Endpoint via Agent				X
Block Traffic via In-Line Sensor				X
Identify Gaps			X	X
Changes / Updates to Managed Devices		X		
Other Remediation Actions	X		X	
Environmental Architectural Changes	X		X	

Platform Management				
SaaS Platform, Sensor, Agent updates				X
Management				
Administer accounts	X		X	X
Identify Stakeholders + Define Escalation Procedures	X		X	
Reporting				
Standard Reports				X
Custom Reports	X		X	X
Data and Trend Analysis				X

* Requires additional feature purchase from Arctic Wolf.

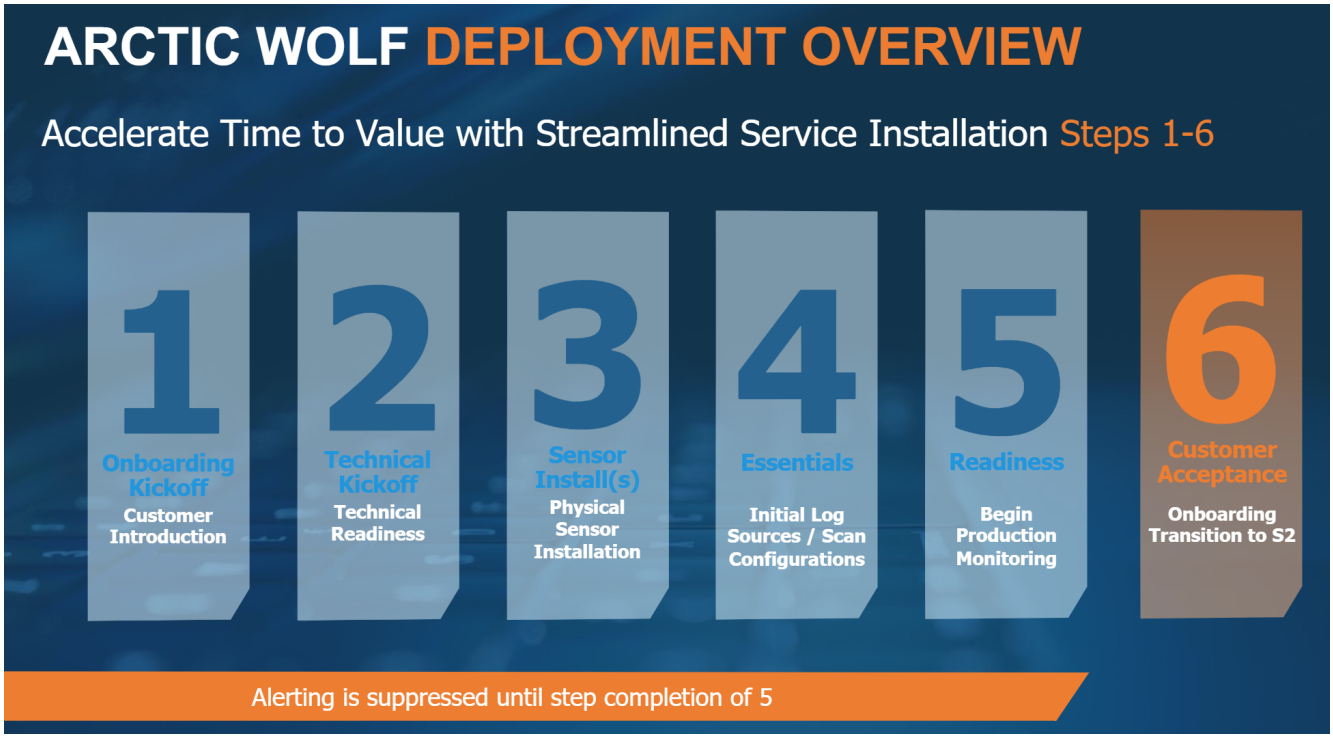
**Extended Services can include but is not limited to additional Managed Services, or Professional Services as documented in the respective service guides or SOWs.

4 MONITORING



5 SERVICE ACTIVATION

Onboarding Lifecycle consists of 5 stages.



The onboarding timeline will be scoped as part of the solution. Service Activation occurs at the end of the timeline in the agreement. If Onboarding is completed early, the service is available before billing commences.

6 OFFERING SPECIFIC TERMS AND CONDITIONS

Arctic Wolf Terms and conditions are identified in the Arctic Wolf MSP Addendum

7 DEFINITIONS

Data Transfer. Any Equipment provided by Arctic Wolf to Customer is physically or virtually deployed to monitor Customer's system traffic. Such system traffic is augmented with additional sources of log data, as required, to deliver Managed Detection and Response. All such system traffic information is deemed Solutions Data. Essential log sources will be determined by Customer and Arctic Wolf during the onboarding process preceding the Order Form Effective Date.

Any Solutions Data will be securely transmitted to Arctic Wolf. The Solution operates redundantly with Customer's High Availability (HA) specifications in order to minimize potential service interruptions. Hosting providers used by Arctic Wolf to deliver the Solution may experience service interruptions and service outages outside the control of Arctic Wolf. If such a hosting provider issues an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify Customer about the outage and communicate the planned recovery time provided by the hosting provider.

Solutions Data may include personal or confidential information. Customer will provide any such personal or

confidential information in accordance with the terms of the Agreement.

Data Retention. Arctic Wolf will store Solutions Data for the Data Retention period specified in Customer's then-current Order Form. Solutions Data may be returned to Customer in accordance with the terms of the Agreement.

Managed Device. InterVision provides additional management to devices that includes monitoring, specific changes, and critical patching. These services include but are not limited to Managed Firewall, Managed Network, Managed Server, Managed Endpoint Protection, Managed Storage, as well as BaaS and DRaaS. For a comprehensive list of responsibilities, each service has it's own respective Service Guide and can be referenced here: https://intervision.com/service-guides

Updates & Upgrades. Automated maintenance and update cycles to the Equipment will be performed remotely by Arctic Wolf Security Services. Arctic Wolf will provide any services related to the replacement or upgrades of the Equipment. Any costs related to such Equipment replacement or upgrades will be in accordance with the Agreement.

Security Incidents. The CST supporting Customer is available 8:00 am to 5:00 pm (based on the time zone within which the CST is located), Monday through Friday (excluding holidays). The SOC is available 24 hours a day, 7 days a week, including holidays. Customer may schedule specific activities with their CST by contacting the Arctic Wolf SOC at security@arcticwolf.com[1]. Arctic Wolf Security Services will acknowledge any schedule request submitted by Customer to security@arcticwolf.com[2] within one (1) hour of receipt of such request. Arctic Wolf Security Services will provide an estimate of response time determined by scope, size, and urgency.

Arctic Wolf Security Services will notify and escalate to Customer any Security Incidents, the definition of which will be agreed upon by Customer and Arctic Wolf during onboarding or subsequently thereafter during the Subscription Term, discovered by Arctic Wolf within two (2) hours of Arctic Wolf's discovery of such Security Incident. Arctic Wolf standard Security Incident notification process is through a ticket to the Customer; however, during onboarding or subsequently thereafter during the Subscription Term, Arctic Wolf and Customer may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy. Customer is responsible for implementing, in its sole discretion, any remediation strategies identified by Arctic Wolf. Customer may request validation by Arctic Wolf that any such implemented remediation strategies are working as expected.

Emergencies. During onboarding and subsequently thereafter during the Subscription Term, Arctic Wolf and Customer will agree on and document which Security Incidents will be defined as an "Emergency". Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

Any Emergency identified by Customer can be escalated to Arctic Wolf's Security Services by calling: 888-272-8429, option 2. Customer must describe the Emergency in the initial call and Arctic Wolf will respond within 5 minutes. In addition, with respect to any urgent inquiries, Customer may contact Arctic Wolf's Security Services by calling: 888-272-8429, option 2.

Scans. On a monthly basis, Arctic Wolf will use the Solution to conduct external vulnerability assessment scans of Customer's environment. As part of these scans, vulnerability and exploit information will be normalized and correlated with other data sources in order to determine Customer's Security Score and prioritization of any identified remediation strategies. Arctic Wolf will deliver to Customer a summary security report that includes Security Incident and Emergency notification activities on a monthly and quarterly basis.

1 mailto:security@arcticwolf.com
2 mailto:security@arcticwolf.com

Security Score. Customer's Security Score is provided as part of the Solution is for illustrative and informational purposes only and may be used by Customer for internal benchmarking purposes. The Security Score is based on certain information related to the results of the Solution within Customer's environment and is compiled using the Solutions Data made available to Arctic Wolf in conjunction with its delivery of the Solution. Customer's Security Score will be communicated in Customer's summary reports in addition to being available on Customer's online Executive Dashboard. Customers may elect to compare their Security Score against industry averages from organizations in the same industry vertical to assess how Customer is performing against industry norms.

Host Containment. Based upon the agreed upon escalation process and provided that the Arctic Wolf Agent is deployed by Customer, Arctic Wolf's Security Services team will remotely isolate a Customer endpoint device(s) that shows evidence of compromise or other suspicious activity. When the Security Services team identifies certain indicators of attack on an endpoint, the containment action will be initiated systematically, in accordance with the agreed upon escalation process, to rapidly quarantine the suspected compromised system.

The indicators of attack that may drive containment actions include those relating to ransomware (and other types of advanced malware), malicious command-and-control (C2) activity, or active data exfiltration attempts. When an endpoint is in a contained state, only essential control traffic between the Arctic Wolf Agent and the Arctic Wolf server will be allowed in order to enable forensics investigations.

The endpoints under containment will receive a containment notification and the containment action will be detailed in an incident ticket. The customer portal will display the Customer endpoints that are currently in a contained state. Security Services team is available to Customer to answer questions or provide detailed information on the contained endpoints.

*Solutions Data also may be referred to in the Agreement as Customer Data.

8 ADDENDUM FOR ARTIC WOLF SERVICES

ADDENDUM FOR MANAGED DETECTION AND RESPONSE SOLUTION

POWERED BY ARCTIC WOLF

This Addendum for Managed Detection and Response Solution (the "Addendum") is entered into as of the Effective Date by and between InterVision Systems, LLC and _____ (the "Customer"). InterVision and Customer are collectively referred to as the "Parties" and individually as a "Party."

WHERAS, InterVision and Customer are parties to a Master Services Agreement dated _____ (the "MSA") and a Work Order dated _____ (the "Work Order");

WHEREAS, pursuant to the Work Order, InterVision will sell and Customer desires to purchase certain managed detection and response solutions (the "Service") delivered via an InterVision subcontractor as more fully described in the Work Order; and

WHEREAS, as a condition of purchasing the Services, Customer is subject to certain additional terms and conditions as more fully set forth in this Addendum.

NOW THEREFORE, in consideration of the foregoing and for other valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Review of Information. Customer acknowledges and certifies that Customer has reviewed and hereby agrees to the InterVision Service Guide applicable to the Services.
2. Compliance. Customer agrees that it shall comply at all times with the terms of this Addendum.

3. Customer Interactions. Customer understands that pursuant to InterVision's agreement with the subcontractor, the subcontractor may directly communicate and interact with Customer without InterVision's participation.
4. License. InterVision grants to Customer a limited non-transferable, non-sublicensable, non-exclusive right and/or license during the Subscription Term (as defined below), to the extent a component of the Services being licensed by InterVision to: install, use and access any software that is party of the Services; (ii) use any equipment that ins is included as part of the Services for the purpose of the use of the Services; (iii) load Customer's users and associated information for delivery of content and use of the administrator dashboard; (iv) access the administrator dashboard, subject to the InterVision Privacy Notice which can be found at https://intervision.com/privacy-policy; and (v) access and use the features and functionality of the Services. Customer may access and use the Services, and any documentation associated therewith, solely for its own internal business purposes and in accordance with the terms and conditions of this Addendum.
5. **Reservation of Rights and Ownership.** InterVision has the right to license the Services and any associated documentation. Customer acknowledges and agrees that: (a) the Services are protected by United States and international copyright, trademark, patent, trade secret and other intellectual property or proprietary rights laws; (b) Customer has no right, title and interest (including, without limitation, all patent, copyright, trade secret and other intellectual property rights) in and to the Services, excluding any rights, title, and interest in any third party; (c) there are no implied licenses and any rights not expressly granted to Customer hereunder are reserved InterVision; (d) the Services, excluding any professional services, are licensed on a subscription basis, not sold, and Customer acquires no ownership or other interest (other than the license rights expressly stated herein) in or to the Services; and (e) the Services are offered as an on-line, hosted solution, and Customer has no right to obtain a copy of any software that is a part of the Services.
6. Restrictions. Customer agrees not to, directly or indirectly: (i) modify, translate, copy or create derivative works of the Services; (ii) reverse engineer, decompile, disassemble, or otherwise seek to obtain the intellectual property contained within Services, except to the extent expressly permitted by applicable law (and then only upon advance notice to InterVision); (iii) interfere with or disrupt the integrity or performance of the Services or the data and information contained therein or block or disrupt any use or enjoyment of the Services by any third party; (iv) attempt to gain unauthorized access to the Services or related systems or networks; (v) remove or obscure any proprietary or other notice contained in the Services, including on any reports or data; (vi) use the Services in connection with a service bureau, service provider or like activity whereby Customer operates or uses the Services for the benefit of a third party; (vii) use the Services to monitor or scan any environments for which Customer has not received consent; or (viii) include material or information that is obscene, defamatory, libelous, slanderous, that violates any person's right of publicity, privacy or personality, or otherwise results in any tort, injury, damage or harm to any person. If InterVision, in its reasonable discretion, determines that Customer's use of or access to the Services imposes an actual or imminent threat to the security or stability of InterVision's or its subcontractor's infrastructure or that Customer is abusing its use of the Services in contravention with the terms of this Addendum, InterVision may, in addition to any other right herein, temporarily suspend Customer's access to the Services until such activity is rectified. If commercially practicable, InterVision shall provide Customer with notice prior to any such suspension and shall work with Customer in good faith to reinstate the Services promptly.
7. Personal Data. Customer represents and warrants that it is not disclosing any information that identifies, relates to, describes, is reasonably capable of being associated with or linked to a particular individual including any such information of Customer's customers or employees, whether directly or indirectly ("Personal Information"), to InterVision. Customer further represents and warrants that to the extent it discloses any Personal Information, (i) it has complied with any applicable laws relating to the collection or provision of such Personal Information, (ii) possesses any consents, authorizations, rights and authority, and has given all required notices to individual data subjects as are required to transfer or permit InterVision and its subcontractors to collect, receive, or access any Personal Information in connection with the provision of the Services, and (3) to the extent required by applicable law, informed the individuals of the possibility of InterVision and its subcontractors' processing their Personal Information on Customer's behalf and in accordance with its instructions.

8. Term and Termination. This Addendum will commence on the Effective Date and will terminate (i) when this Addendum terminates for any reason or (ii) when Customer breaches any term or condition of this Addendum, whichever comes first. Customer acknowledges and agrees that this Addendum may not be terminated for convenience. The Services are provided for a subscription term of one year (the "Subscription Term") unless otherwise stated in the Service Order (but not in excess of one (1) year) and shall automatically be renewed for additional one (1) year terms unless Customer provides no less than sixty (60) days' notice prior to end of the existing Subscription Term to InterVision of the termination of the Services. In addition to the termination rights set forth in the MSA and Work Order, Customer understands that either party may terminate this Addendum, including the rights to use the Services, for cause if the other party commits a material breach of this Addendum, provided that such terminating party has given the other party ten (10) days advance notice to try and remediate the breach. If InterVision terminates this Addendum and Services for cause, the Work Order shall terminate for cause and Customer shall be responsible to pay InterVision fees and costs for the remainder of the existing Subscription Term in addition to fees, costs and value added taxes ("VATs") attributable to the Services up to the date of termination. If Customer terminates this Addendum without cause, Customer shall be responsible for all fees and costs for the remainder of the existing Subscription Term in addition to fees, costs and VATs attributable to the Services up to the date of termination.
9. Modifications. Customer understands InterVision may update this Addendum and the Services in its sole discretion provided that any such modifications shall not materially decrease the features and functionalities that Customer has subscribed to during the then-current Subscription Term. Should InterVision make any modifications to this Addendum and/or any associated documentation, InterVision will post the amended terms on the applicable URL links, will update the *"**Last Updated Date**"* within such documents and notify Customer via the Customer Portal, from time-to-time, of any such changes. Customer shall notify InterVision in writing within thirty (30) days after the effective date of the modification of its rejection of such modification. If Customer notifies InterVision of its rejection during such thirty (30) day period, then Customer will remain governed by the terms in effect immediately prior to the change until the end of Customer's then-current Subscription Term. However, any subsequent renewal of the Subscription Term will be renewed under the then-current terms, unless otherwise agreed in writing by the Parties.
10. Warranties. INTERVISION WARRANTS THAT DURING THE SUBSCRIPTION TERM AND PROVIDED THAT CUSTOMER IS NOT IN BREACH OF THIS AGREEMENT THAT: (I) THE SERVICE PROVIDED UNDER THIS ADDENDUM DO NOT INFRINGE OR MISAPPROPRIATE ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY; (II) THE SERVICES WILL COMPLY WITH ALL FOREIGN, PROVINCIAL, FEDERAL, STATE AND LOCAL STATUTES, LAWS, ORDERS, RULES, REGULATIONS AND REQUIREMENTS, INCLUDING THOSE OF ANY GOVERNMENTAL AGENCY APPLICABLE TO INTERVISION AS IT PERTAINS TO ITS OBLIGATIONS AND THE DATA REQUIRED FOR THE PERFORMANCE OF THE SERVICES DESCRIBED HEREIN. IN THE EVENT OF ANY BREACH OF THIS SECTION 8, INTERVISION SHALL, AS ITS SOLE LIABILITY AND CUSTOMER'S SOLE REMEDY, REPAIR OR REPLACE THE SERVICES THAT ARE SUBJECT TO THE WARRANTY CLAIM AT NO COST TO CUSTOMER OR IF INTERVISION IS UNABLE TO REPAIR OR REPLACE, THEN INTERVISION WILL REFUND ANY PRE-PAID FEES FOR THE SERVICESS, OR PARTS THEREOF, SUBJECT TO THE WARRANTY CLAIM. EXCEPT FOR THE WARRANTIES DESCRIBED IN THIS SECTION, THE SERVICES ARE PROVIDED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES OF TITLE. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE PROVIDED "AS IS" AND FURTHER ACKNOWLEDGES THAT INTERVISION DOES NOT WARRANT: (A) THE OPERATION OF THE SERVICES WILL BE UNINTERRUPTED, OR ERROR FREE; (B) THE SERVICES ARE NOT VULNERABLE TO FRAUD OR UNAUTHORIZED USE; AND (C) THE SERVICES WILL IDENTIFY OR DETECT EVERY VULNERABILITY OR SECURITY ISSUE. CUSTOMER IS RESPONSIBLE AND INTERVISION SHALL HAVE NO RESPONSIBILITY FOR DETERMINING THAT THE USE OF THE SERVICESS COMPLIES WITH APPLICABLE LAWS IN THE JURISDICTION(S) IN WHICH CUSTOMER MAY DEPLOY AND USE THE SERVICES. To the extent any open-source software is included as part of the Services, the open-source software is governed solely by the applicable open-source licensing terms, if any, and is provided "AS IS", and

InterVision hereby disclaims all copyright interest in such open-source software. InterVision provides no warranty specifically related to any open-source software or any applicable open-source software licensing terms.

11. California Consumer Privacy Act**.** The Parties acknowledge and agree that InterVision is a service provider for the purposes of the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA") and may receive personal information (as defined by the CCPA) from Customer pursuant to this Addendum for a business purpose. The Parties agree to comply at all times with the applicable provisions of the CCPA in respect to the collection, transmission, and processing of all personal information (as defined by the CCPA) exchanged or shared pursuant to the Agreement. InterVision shall not sell any such personal information. InterVision shall not retain, use or disclose any personal information provided by Customer pursuant to this Addendum except as necessary for the specific purpose of performing the Services for Customer pursuant to this Addendum or as permitted by the CCPA. The terms "personal information," "service provider," "sale," and "sell" are as defined in Section 1798.140 of the CCPA. InterVision certifies that it understands the restrictions of this Section 9. It is Customer's sole responsibility to notify InterVision of any requests from consumers (as defined in the CCPA) seeking to exercise rights afforded in the CCPA with regard to personal information received or processed in connection with the Services. InterVision agrees to provide reasonable cooperation to Customer in connection with such requests.
12. Supplementation of Work Order. This Addendum supplements and is incorporated into the Work Order between InterVision and Customer. In the event of any conflict between this Addendum and the MSA, this Addendum shall take precedence. In the event of any conflict between this Addendum and the Work Order, the Addendum shall take precedence.
13. Compliance with Applicable Laws. Customer shall comply with all applicable laws pertaining to the use of the Services including but not limited to all import, re-import, sanctions, anti-boycott, export and re-export control laws that apply to a United States Company. Customer represents and warrants that Customer is not a Prohibited Person nor owned or controlled by a Prohibited Person. "*Prohibited Persons*" shall mean a person or entity appearing on the lists published by the U.S. Department of Commerce, the U.S. Department of State, the U.S. Department of Treasury or any other list that may be published by the U.S. Government, as amended from time to time, that is prohibited from acquiring ownership or control of items under this Agreement, or with which InterVision is prohibited from doing business.
14. Effective Date. The Effective Date of this Addendum shall be effective date of the Work Order.
15. Full Force and Effect. Except as specifically amended by the Addendum, all terms and provisions of the MSA and Work Order shall remain in full force and effect.
16. Counterparts and Delivery. This Addendum may be executed by facsimile or by electronic signature, and in counterparts, each of which will deemed an original, and all of which together shall constitute one and the same instrument. Electron delivery of a counterpart shall be accepted as if the original had been delivered.
17. Notice Addresses. Any notice requirements in this Addendum shall be in the case of InterVision and Customer governed by the MSA.

IN WITNESS WHEREOF, InterVision and Customer have executed this Addendum as of the Effective Date.