SOCAAS, POWERED BY CYBERSAFE - 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

Cybersafe's Security Operations Center as a Service (SOCaaS) solution is a fully managed service that provides comprehensive real-time detection and containment of cyber threats that jeopardize your networks and endpoints. The Cybersafe SOC can provides 24x7x365 monitoring of provided endpoint software, network and cloud infrastructure, and Office 365 activity to prevent intrusions from becoming breaches. When sold as an InterVision Managed Service, Cybersafe SOCaaS is intended to be paired with other InterVision Managed Services to deliver a more complete managed security experience.

2 SERVICE DESCRIPTION AND DETAILS

Cybersafe provides Network & Cloud Security Monitoring solution for critical network cybersecurity defense today. Their network security engineers monitor your organization's network traffic in real-time, 24 hours a day, 7 days a week, 365 days a year. Cybersafe network security monitoring provides:

- **Enhanced visibility**. Cybersafe sensors provide significantly improved information over log-based monitoring solutions with support for on premise networks as well as Amazon Web Services, Microsoft Azure Cloud, Office 365 and more. All from a single integrated platform.
- **Increased efficiency**. Customers have no additional operational overhead to invest in their own SIM/SIEM (Security Information and Event Management) tools, nor do they need to maintain a team of expert analysts resulting in a lower total cost of ownership (TCO).
- **Constant vigilance**. Cybersafe Solutions team of certified security analysts turn data into action identifying the real attacks from the noise. Cybersafe is there monitoring alerts 24/7/365 so you don't have to be.
- **Purpose-built technology and architecture**. Cybersafe supports customers through geographically dispersed Security Operations Centers (SOCs) to provide scalable solutions for our customers.
- **Focused resources**. Customers' teams can spend their time on core business activities instead of monitoring and analyzing security threats.
- **Agile processes**. Cybersafe Solutions is flexible to meet the individual security needs of each organization.

The Cybersafe Network & Cloud security monitoring platform includes five essential security capabilities managed through a central console. These capabilities, **Asset Discovery, Vulnerability Assessment, Intrusion Detection, Behavioral Monitoring, and SIEM & Log Management** encompass everything needed for complete real-time visibility into your cyber threats**.** These integrated features are supplemented with multiple external threat feeds including those from the Open Threat Exchange - the world's largest crowdsourced collaborative cyber threat repository.

Whether large or small, all organizations need the complete visibility our platform offers to:

- Detect emerging threats across your environment
- Respond and contain incidents quickly
- Conduct thorough investigations and provide detailed information on events
- Measure, manage, and report on compliance (PCI, HIPAA, ISO, GLBA and more)
- Optimize your existing security investments and reduce risk

Asset Discovery

- We find all assets on your network to ensure no rogue devices exist for a hacker to exploit.

Vulnerability Assessment

- Identify systems that are vulnerable to exploits with active network scanning & continuous vulnerability monitoring

Intrusion Detection

- Detect & respond to threats targeting your on-prem and cloud environments faster with our built-in intrusion detection algorithms

Behavioral Monitoring

- Instantly spot suspicious network behavior with deep traffic analysis, service monitoring, & full packet capture

SIEM & Log Management

- Quickly correlate & analyze security event data from across your network and cloud environments with built-in SIEM & log management.

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 SERVICE OPTIONS

Cybersafe services can be ordered in one of four combinations of solutions (SOL):

1. **SOL-EDR =** Fully Managed Endpoint Detection and Response (EDR). Endpoint software is deployed to all workstations and servers and the SOC wrapper is added to monitor events from it.
2. **SOL-EDR + O365** = Fully Managed EDR plus Office365 Tenant Monitoring.
3. **SOL-SIEM** = Fully Managed Security Information and Event Management (SIEM). Network and Cloud Monitoring with no endpoint agent coverage.
4. **SOL-XDR** = Extended Detection and Response (XDR). Combined Network, Cloud, and Endpoint Monitoring. Endpoint software is deployed to all workstations and servers, a sensor and firewall are deployed on the customer network at each major infrastructure node to collect log data and perform internal vulnerability scanning, and the SOC wrapper is added to monitor events from all systems. Office 365 monitoring is included by default.

Service Offerings Detail	SOL-EDR	SOL-EDR + O365	SOL-SIEM	SOL-XDR
24x7x365 SOC Monitoring with Real Time Alert Investigation and Response	✓	✓	✓	✓
Endpoint Detection & Response	✓	✓		✓
Next Gen Anti-Virus Agent	✓	✓		✓
Endpoint Isolation and Containment	✓	✓		✓

Security Information & Event Management (SIEM) Log Ingestion Platform			✓	✓
Intrusion Detection/Deep Packet Inspection			✓	✓
Asset Inventory			✓	✓
Vulnerability Scanning			✓	✓
Office 365 Cloud Monitoring		✓	✓	✓
On Premise Hardware			✓	✓
Full Cloud Service Ingestions (AWS/Azure/etc)			✓	✓
Domain Doppelganger		*		*
Dark Web Monitoring		*		*
Deception Technology				✓
EDR/SIEM Event Cross Correlation				✓
Remote Incident Response with unlimited escalations (Covered Assets)	✓	✓	✓	✓

* = Optional add-on

4 ROLES AND RESPONSIBILITIES

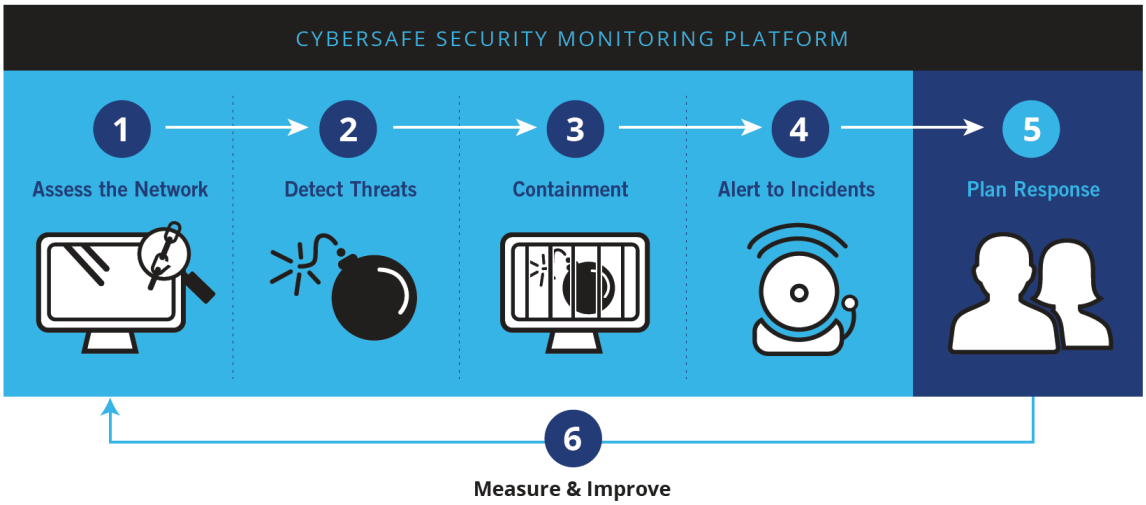
	Client	InterVision Managed Services	Extended InterVision Services*	Cybersafe Security Operations
Installation and Configuration				
Agent Deployment	X		X	

Sensor + Firewall 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
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, Firewall, 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

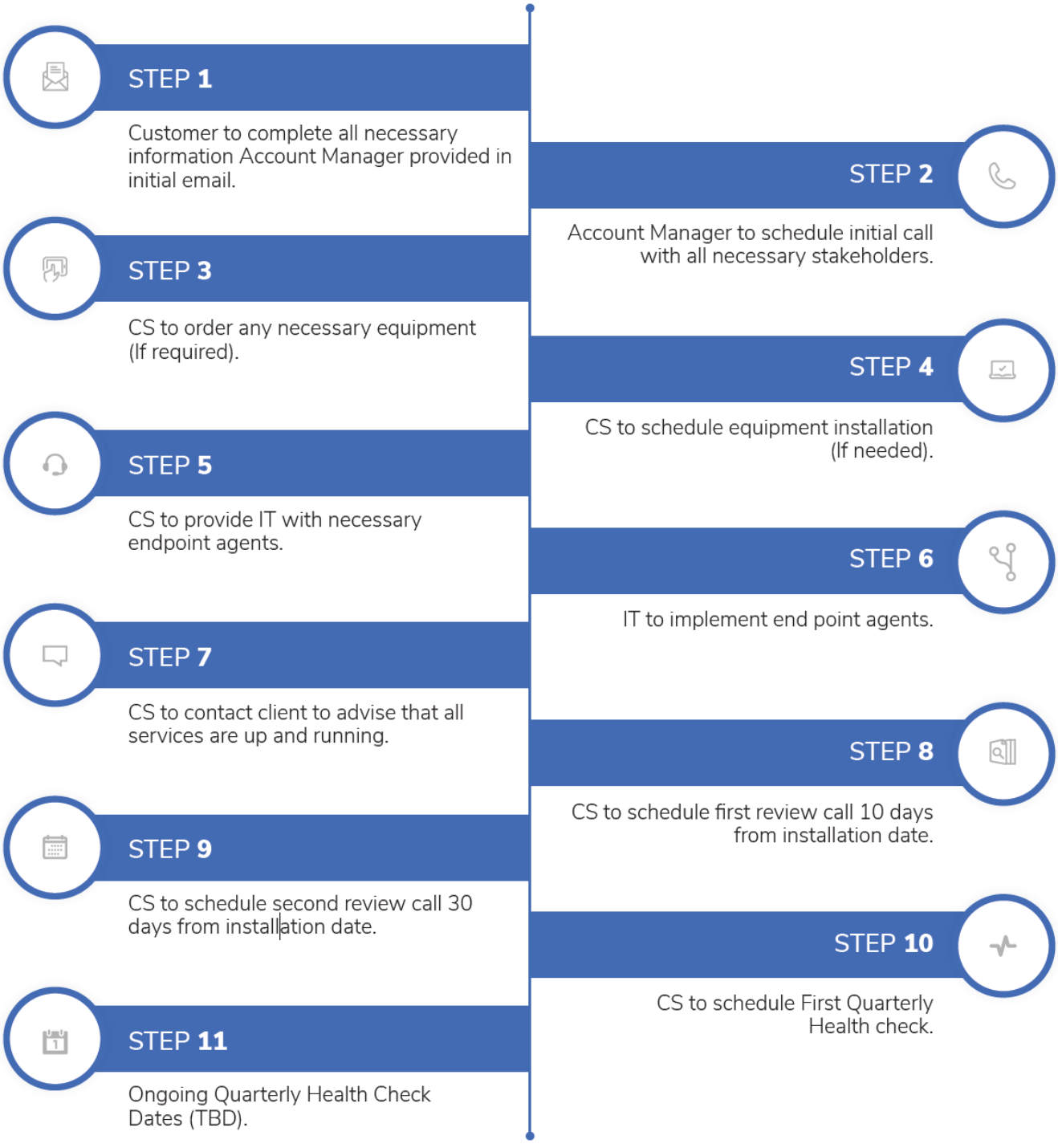
*Extended Services can include but is not limited to additional Managed Services, or Professional Services as documented in the respective service guides or SOWs.

5 MONITORING



6 SERVICE ACTIVATION

Process Timeline



The onboarding timeline will be scoped as part of the solution. Service Activation occurs at the end of Step 7. If Onboarding is completed early, the service is available before billing commences.

7 ADDENDUM FOR CYBERSAFE SERVICES

ADDENDUM FOR MANAGED DETECTION AND RESPONSE SOLUTION

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 Statement of Work dated _____ (the "SOW");

WHEREAS, pursuant to the SOW, InterVision will sell and Customer desires to purchase network and end-point security monitoring, detection, response and mitigation to prevent networks, data, and computer devices from security threats (together with any and all upgrades, enhancements, and updates, the "Services") offered by a third-party provider; 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.

1. No Guarantees. InterVision (which by definition includes its authorized third-party provider, Cybersafe Solutions LLC) will use reasonable, industry-standard care in the performance of the Services. CUSTOMER ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT INTERVISION DOES NOT COVENANT, GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, DISCOVER AND/OR REPAIR ANY OR ALL OF CUSTOMER'S SYSTEMS VULNERABILITIES, OR THAT INTERVISION WILL BE ULTIMATELY SUCCESSFUL IN DETERMINING THE SOURCE OR FULL IMPACT OF ANY AUTHORIZED OR UNAUTHORIZED ACCESS OR SECURITY BREACH (OR ATTEMPTED ACCESS OR SECURITY BREACH), AND WILL NOT HOLD INTERVISION RESPONSIBLE THEREFORE. ALL DETERMINATIONS REGARDING THE CUSTOMER'S APPROACH TO COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS, INCLUDING HOW AND WHETHER THE SERVICES CONTRIBUTE TO SUCH APPROACH, SHALL BE MADE SOLELY BY THE CUSTOMER AND CUSTOMER SPECIFICALLY ACKNOWLEDGES THAT INTERVISION HAS NOT REPRESENTED, WARRANTED, OR OTHERWISE GUARANTEED PERFORMANCE OF THE SERVICES WILL RESULT IN ANY SUCH COMPLIANCE.
2. Possible Damage or Disruption. InterVision hereby disclaims responsibility for any and all claims of loss arising from or in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein arising from or related to the provision of the Services, other than directly arising from willful misconduct by InterVision, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.
3. Consents and Data. Customer is solely responsible for the content of the data contemplated to be accessed by InterVision from Customer's systems under this Addendum. Customer has the right to grant to InterVision and does hereby grant to InterVision (except to the extent otherwise specified in a SOW), the right to access all such data, all such systems, and all facilities associated with such systems and data for the purpose of providing the Services. Customer further acknowledges that it has right to and does hereby authorize InterVision to conduct any forensic or other investigations, to access computers, files or other data reasonably necessary to conduct such investigations, and to view information as necessary to perform the Services. Customer shall, at its own cost and expense, obtain and maintain all necessary third-party consents required for InterVision to so access such systems and data. Customer represents and warrants to InterVision that the Customer has authority to provide InterVision with access to endpoints owned or operated by the Company's employees, and hereby does extend such authority to InterVision. Customer agrees to indemnify InterVision for damages related to a breach of this representation and warranty.

Customer represents and warrants that InterVision' performance of the Services does not and will not conflict with any obligations of Customer to any third party, including without limitation employees of Customer. Customer further represents and warrants that Customer has taken and will take all necessary actions (including without limitation obtaining consents) required for Customer to legally disclose all personally identifiable or equivalent data contained within the data to be accessed by InterVision as the result of InterVision's performance of the Services, and that Customer shall not grant InterVision access to data and shall not disclose data to InterVision to the extent such access and disclosure is not then permitted under all applicable laws. Customer shall not provide InterVision access to any data which require, pursuant to any law or regulation, protection of such data to any legally and/or regulatory specified standard of care, to include without limitation export/import restrictions. Customer shall indemnify, defend, and hold harmless InterVision from any claims related to any breach by Customer of any of the foregoing representations, warranties, and obligations.

4. Excuse. InterVision shall be excused from the performance of any obligation to the extent that such performance conflicts with any applicable law or regulation, including without limitation when InterVision in good faith believes that such performance is likely to so conflict.
5. Customer Data To Be Maintained in Confidence. Data that is within the scope of information contemplated and/or permitted to be accessed by InterVision in connection with the provision of the Services will be deemed to be "Customer Data." Except as otherwise provided in a SOW, Customer Data will be maintained by InterVision in confidence and will be used by InterVision only for purposes of performing and enforcing this Addendum. Keeping Customer Data in confidence means that InterVision will intentionally disclose Customer Data only in support of InterVision's performance and enforcement of the Addendum. InterVision shall not be liable for the inadvertent or accidental disclosure of Customer Data, or its disclosure through theft or fraud, if such disclosure occurs despite the exercise of such standard of care.
6. Cooperation; Customer Tasks; Use of Data. Customer acknowledges that InterVision's ability to perform the Services is dependent on Customer providing InterVision with access to data, systems, facilities, employees and/or information directly related to the security incident(s) giving rise to a SOW, as well as providing InterVision with such other assistance as reasonably requested. Customer acknowledges that the results of the Services may not be suitable for use to determine legal liability for an authorized or unauthorized access to Customer's systems, facilities, and/or data.
7. Limitation of Liability.

(a) NOTWITHSTANDING ANYTHING SET FORTH IN THE MSA OR THE SOW, TO THE EXTENT ARISING UNDER THE MSA OR THIS ADDENDUM, THE LIABILITY OF INTERVISION FOR DAMAGES UNDER AND RELATED TO THE MSA OR THIS ADDENDUM, THE SERVICES AND ITS SUBJECT MATTER FOR ALL EVENTS, ACTS, OR OMISSIONS WILL BE LIMITED TO A TOTAL AGGREGATE AMOUNT OF $25,000, WHETHER BASED ON ONE OR MORE ACTIONS OR CLAIMS IN CONTRACT, EQUITY, WARRANTY, STRICT LIABILITY, NEGLIGENCE OR OTHER TORT, OR OTHERWISE. FOR THE AVOIDANCE OF DOUBT, CLAIMS RELATED TO ANY SOW ARE SUBJECT TO THE LIMITATION IN SECTION 7(b) BELOW *IN LIEU* OF THIS LIMITATION IN SECTION 7(a).

(b) TO THE EXTENT ARISING UNDER THE MSA OR THIS ADDENDUM, AND RELATED TO A SOW, THE LIABILITY OF INTERVISION FOR DAMAGES UNDER AND RELATED TO THE MSA OR THIS ADDENDUM AND ITS SUBJECT MATTER FOR ALL EVENTS, ACTS, OR OMISSIONS RELATED TO SUCH SOW, WILL BE LIMITED TO A TOTAL AGGREGATE AMOUNT OF THE GREATER OF: (i) PAYMENTS MADE BY CUSTOMER TO INTERVISION UNDER SUCH SOW DURING THE FIRST SIX (6) MONTHS OF SUCH SOW, OR (ii) $25,000, WHETHER BASED ON ONE OR MORE ACTIONS OR CLAIMS IN CONTRACT, EQUITY, WARRANTY, STRICT LIABILITY, NEGLIGENCE OR OTHER TORT, OR OTHERWISE. FOR THE AVOIDANCE OF DOUBT: MULTIPLE CLAIMS RELATED TO A SINGLE SOW WILL BE SUBJECT TO THE AGGREGATE LIMITATION OF LIABILITY FOR SUCH SOW; EACH CLAIM RELATED TO A SOW MUST BE ASSOCIATED WITH ONLY ONE SOW; AND CLAIMS RELATED TO ANY SOW ARE SUBJECT TO THE LIMITATION IN THIS SECTION 7(b) *IN LIEU* OF THE LIMITATION IN SECTION 7(a).

(c) IN NO EVENT WILL INTERVISION BE LIABLE FOR, NOR WILL THE MEASURE OF DAMAGES SET FORTH IN SECTIONS 7(a) OR 7(b) INCLUDE, ANY INDIRECT, INCIDENTAL, PUNITIVE, EXEMPLARY, SPECIAL OR CONSEQUENTIAL DAMAGES OR AMOUNTS FOR LOSS OF INCOME, PROFITS, GOOD WILL, OR SAVINGS, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(d) MONETARY DAMAGES AS SET FORTH IN THIS SECTION 7 ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AGAINST INTERVISION.

(e) IN NO EVENT SHALL INTERVISION BE LIABLE OR OTHERWISE RESPONSIBLE FOR ANY DAMAGE, OBLIGATION OR LOSS ARISING FROM, RELATED TO, OR IN CONNECTION WITH: (i) THE FAILURE OF THE CUSTOMER TO FOLLOW INSTRUCTIONS, DIRECTIVES OR ALERTS ISSUED BY INTERVISION; (ii) ENDPOINTS WHICH A CUSTOMER INSTALLS ON PERSONAL DEVICES; (iii) ENDPOINTS WHICH DO NOT HAVE INTERVISION'S SECURITY MONITORING SERVICES IMPLEMENTED; AND (iv) INCIDENT RESPONSE WORK WHICH ORIGINATES FROM ENDPOINTS WHICH LACK INTERVISION'S SECURITY MONITORING SERVICES. CUSTOMER WILL REMAIN LIABLE FOR INCIDENT RESPONSE FEES ADDRESSING AN INTRUSION VIA THE CUSTOMER'S UNPROTECTED ASSETS, EVEN IF THE SAME AFFECTS PROTECTED ASSETS.

(f) NOTWITHSTANDING ANYTHING SET FORTH IN THE MSA OR SOW, THE LIMITATIONS OF LIABILITY SET FORTH IN THIS SECTION 7 SHALL APPLY TO ALL WORK PERFORMED PURSUANT TO THE MSA, SOW OR THIS ADDENDUM AND SHALL APPLY TO ANY INDEMNIFICATION OBLIGATION THAT INTERVISION MAY HAVE WITH RESPECT TO THE SERVICES COVERED BY THIS ADDENDUM.

1. Import and Export Compliance. In connection with this Addendum, each party will comply with all applicable import, re-import, export, and re-export control laws and regulations, including the Export Administration Regulations, the International Traffic in Arms Regulations, and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control. For clarity, Customer is solely responsible for compliance related to the manner in which Customer choose to use the Services, including Customer's transfer and processing of its Content, the provision of its Content to End Users, and the region in which any of the foregoing occur.

-

1. Governing Law; Jurisdiction; Jury Trial Waiver; Venue; Prevailing Party Counsel Fees. This Addendum: (a) shall be governed and construed in accordance with the laws of the State of Missouri, without regard to principles related to conflict of laws; (b) incorporates the entire understanding of the parties with respect to the subject matter hereof and supersedes any previous understanding, commitment or agreement, oral or written, with respect to such; and (c) may not be amended or modified except in writing executed by both parties hereto. All actions between the parties will be heard and tried by the court sitting without a jury and the parties irrevocably waive any rights to a jury trial. InterVision and Customer hereby irrevocably submit to the jurisdiction of the state courts located in St. Louis County, Missouri or the United States District Court for the Eastern District of Missouri and none other. The prevailing party in any such litigation shall be entitled to an award of its reasonable attorneys' fees and other expenses and costs.
2. Authorization Under Laws. To the extent that Customer can or must provide InterVision with authorization under any applicable law or regulation to perform any task associated with Services, Customer hereby does so, will continue to do so while InterVision is performing the Services, and will provide further written confirmation of such to InterVision or to others as InterVision directs upon request. Such authorizations include, without limitation, those under: the Computer Fraud and Abuse Act, 18 U.S.C. §1030, et seq., and the Electronic Communications Privacy Act, 18 U.S.C. §2701, et seq. Customer also authorizes InterVision or its agents to have access to such personal data or special category personal data, collectively referred to as "Personal Data," related to an identified or identifiable non-US person ("data subjects") protected by national privacy directives or laws as necessary to perform the tasks under the relevant SOW(s). Customer represents and warrants that, where it provides Personal Data to InterVision or requests InterVision to process Personal Data it (i) has complied with any applicable laws or regulations relating to the collection or provision of such information, (ii) possesses any consents or authorizations, rights and authority required to transfer to or permit InterVision to process Personal Data and (iii) has informed, to the extent required by

applicable laws or regulations, the data subjects of the possibility of InterVision processing their Personal Data on Customer's behalf and in accordance with its instructions. The terms "process" or "processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Additionally, Customer hereby appoints InterVision as the agent of Customer for purposes of 18 U.S.C. §2511(2) (a) (i) and Customer represents that InterVision is retained to provide the Services for the protection of Customer's rights and property.

1. European Union General Data Protection Regulation and United Kingdom Data Protection Ac
2. Customer is a Data Controller of certain Personal Data and appoints InterVision as a Data Processor to process this Personal Data on its behalf.
3. If and to the extent that Customer submits to InterVision Personal Data (as that term is defined under the General Data Protection Regulation ("GDPR") and the United Kingdom Data Protection Act ("UK DPA")) of individuals located in the European Economic Area or United Kingdom, the Customer agrees to complete and execute the Standard Contractual Clauses appended to this Addendum as may be necessary under the GDPR and UK DPA to transfer personal data from the EEA or UK to the United States, as may be necessary in delivery of the Services.
4. It is the Customer's sole responsibility to notify InterVision of requests from data subjects related to the modification, deletion, restriction and/or objection to processing of Personal Data. Customer represents and warrants that any processing of Personal Data in accordance with its instructions is lawful.
5. Customer acknowledges and agrees that InterVision may engage Sub-Processors to access and process Personal Data in connection with the Services. Customer provides authorization for InterVision to engage Sub-Processors as necessary to perform the Services. InterVision will enter into a written agreement with Sub-Processors imposing obligations comparable to those imposed on InterVision under this Addendum with respect to the protection of Personal Data. In case a Sub-Processor fails to fulfil its obligations under such written agreement InterVision, InterVision will remain liable to Customer for the performance of the Sub-Processor's obligations under such agreement.

1. Supplementation of MSA and SOW. This Addendum supplements, amends and is incorporated into the MSA and SOW between InterVision and Customer. In the event of any conflict between this Addendum and the MSA or SOW, this Addendum shall take precedence. In the event of any conflict between this Addendum and the SOW, the Addendum shall take precedence.
2. Effective Date. The Effective Date of this Addendum shall be effective date of the SOW.
3. 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.
4. 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. Electronic delivery of a counterpart shall be accepted as if the original had been delivered.
5. 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.