SERVICE ORDER ATTACHMENT:
ENDPOINT DETECTION AND RESPONSE

Capitalized terms not defined in this Attachment will have the meanings set forth in the MSA.

GENERAL TERMS AND CONDITIONS.

1. **"Services"** provided under this Attachment means

- Services Software we make available to you to utilize the Services
- Security event detection and prioritization on Customer devices with deployed Services Software agents ("Covered Devices")
- 24x7 x365 SOC monitoring of Covered Devices
- Monthly reporting on security events on Covered Devices
- Services Software agent installation and configuration
- Updating security policies based on new and emerging threats

We will make the Services Software and/or SDK available to You via download from Our website or other means determined by Us. for deployment on devices you identify on or before the date we first make Services available to you ("**Launch Date**"). Additional devices may become Covered Devices thereafter as you identify devices to Us and We make available Services Software for installation.

2. **ADMINISTRATORS.** Prior to the Launch Date, you will appoint up to 3 administrators, each of whom will have the power to act as your agent, with the authority to make decisions, representations, and give notices on your behalf ("**Administrators**"). Administrators' authority includes, but is not limited to (i) controlling the creation and deletion of Covered Devices; (ii) serving as our authorized technical contact for the Services. At least one (1) Administrator must attend a training session on the Services, which we will provide at no charge. You may replace Administrators at any time upon notice to us.

3. **TECHNICAL SUPPORT.** We will provide technical support in accordance with the Service Level Agreement attached as Appendix 1.

4. **TERM AND TERMINATION.** This Attachment will be in effect during the Initial Term set forth in your order, and will thereafter automatically renew for additional one (1) year renewal terms (collectively the "Term") unless either of us provides the other with written notice of the intention not to renew at least sixty (60) days prior to the beginning of any renewal term. Sections 1 (Services), 4(Term and Termination), 5 (Fees), 6 (Cancellation Fees), 7 (Compliance with Applicable Law), and 8 (Service Specific Terms) and Conditions of this Attachment will survive the expiration or termination of this Attachment for any reason. The provisions of the MSA that are identified in the MSA as surviving the expiration or termination of the MSA will, as they apply to this Attachment, also survive the expiration or termination of the Attachment for any reason. Within ten (10) days after the expiration or termination of this Attachment for any reason, you must pay all fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.

5. **FEES.** You will pay us the fees set forth in *Appendix 1* for Services you purchase. We will invoice you monthly. If You choose to increase the number of Covered Devices You subscribe to under an applicable Order or Quote during Your then-effective Term (a "**Subscription Increase**") or upgrade your subscription to a different subscription plan ("**Plan Upgrade")**, We shall invoice You for the incremental Fees associated with such Subscription Increase and/or Plan Upgrade on a *pro rata* basis at the price per Covered Device specified in the corresponding Quote or valid Order over the remaining period of such Term (which Fees shall be due and payable upon implementation of such Subscription Increase and/or Plan Upgrade) and thereafter in any Renewal Term unless otherwise agreed among the Parties in an Order. No Fees refund or credit shall be granted where You elect to not use the Services on previously subscribed Covered Devices. We reserve the right to increase fees on an annual basis if due to increases for the underlying technology or other general inflationary pressures.

6. **CANCELLATION FEE.** If this Attachment is terminated prior to the end of the Initial Term or any renewal term, for any reason other than our material breach of this Attachment or the MSA, you will pay us a cancellation fee. The cancellation fee will be equal to your average monthly invoices for the six (6) months prior to the date of termination multiplied by the lesser of (a) the number of months remaining in the then current term of this Attachment or (b) twelve (12) months. Your obligation to pay the cancellation fee is in addition to, and not exclusive of, your obligation to pay all fees accrued and unpaid at the time of termination for any reason.

7. **COMPLIANCE WITH APPLICABLE LAW.** Your use of the Services, and the installation of any hardware or software for use in conjunction with the Services (including but not limited to monitoring, intercepting or transmitting to us or any third party, any data or communication) must be in compliance with applicable law. You represent to us that (i) you have received all permissions and authorizations to use the Services as required under applicable law, or (ii) your use of the Services does not require any such permission or authorization. For purposes of this paragraph, your use of the Services includes all monitoring, intercepting, transmitting and other Services conducted by us on your behalf.

SERVICES-SPECIFIC TERMS AND CONDITIONS

8. **SERVICE SPECIFIC TERMS AND CONDITIONS.** These Service Specific Terms and Conditions govern Customer's subscription to the Services, and constitute a binding contract in connection with any paid or Evaluation use of the Services. To the extent of any conflict between the MSA or other Agreement between us and these Service Specific Terms and Conditions, the Service Specific Rems and conditions will control and take precedence.

8.1. Scope. These Special Terms govern your purchase of the Services which include malware protection, detection and remediation Services, endpoint detection and response Services, device discovery and control Services, and other Services offered by Us over time, together with the software underlying such products and services and any updates, patches, bug fixes and versions thereto ("Enhancements"). You agree to accept all Enhancements necessary for the proper function of the Services as released by Us from time to time, and further agree that We shall not be responsible for the proper performance of the Services or security issues encountered with the Services related to Your failure to accept Enhancements in a timely manner.

8.2. Documentation. All use of the Services shall be in accordance with Our then-current published documentation such as technical user guides, installation instructions, articles or similar documentation specifying the functionalities of the Services and made available by Us to You through the Customer Portal, as updated from time-to-time in the normal course of business ("Documentation").

8.3. License Grant.

8.3.1.

i) Subject to Your compliance with these Special Terms, We hereby grant You a worldwide, non-transferable, non-exclusive license during the Term or any Evaluation Period to install, store, access, use, execute and display the Services (including Enhancements) solely in support of Your (and Your Affiliate(s)) internal business security and operation, in accordance with the Documentation describing the permissible use of the Services ("License"). The License granted herein is limited to the number of physical or virtual Covered Devices licensed to You pursuant to a valid Order.

ii) "Affiliate(s)" means any entity that directly, or indirectly through intermediaries, controls, is controlled by, or is under common control with a Party. The license granted to You herein includes the right to connect Your Affiliates' Covered Devices to the Services so as to provide the Services to such Affiliates' Endpoints, provided that You agree to remain fully responsible and liable under these Special Terms for Your Affiliates use of the Services

a) Other Services. If You decide to enable, access or use third Party products, applications, services, software, networks or other systems, and/or information which may be linked to the Services through Our open APIs (collectively, "Other Services"), including integrating such Other Services directly to Your instance of the Services, be advised that Your access and use of such Other Services is governed solely by the terms and conditions of such Other Services, and We do not endorse, are not responsible or liable for, and make no representations as to any aspect of such Other Services, including, without limitation, their content or the manner in which they handle data or any interaction between You and the provider of such Other Services, or any damage or loss caused or alleged to be caused by or in connection with Your enablement, access or use of any such Other Services. You may be required to register for or log into such Other Services on their respective websites. By enabling any Other Services, You expressly permit Us to disclose Your Login as well as Your Data to such Other Services as necessary to facilitate Your enablement and use of such Other Services.

b) Third Party Service. If You enter into an agreement with a third party to manage the installation, onboarding and/or operation of the Services on Your behalf ("Third Party Service") then You may allow such Third Party Service to use the Services provided that (i) as between the Parties, You remain responsible for all its obligations under the terms of these Special Terms; (ii) such Third Party Service only uses the Services for Your internal purposes and not for the benefit of any third party or the Third Party Service, and agrees to the terms of these Special Terms in providing services to You; and (iii) You remain liable to Us for the Third Party Service's service on Your behalf.

8.3.2 Evaluations; Early Adoption and Beta Use.

a) Evaluation Offering**.** If You receive the Services for evaluation purposes, then You may use the Services for Your own internal evaluation purposes ("Evaluation") for a period of up to thirty (30) days from the start date of the Evaluation (the "Evaluation Period"), unless otherwise agreed to in the valid Order and/or Quote covering the Evaluation.

b) Evaluation License and Restrictions. In addition to the license scope detailed elsewhere in these Special Terms, during Evaluation You: (i) may install and use, solely during the Evaluation Period, the Services Software on up to fifty Covered Devices (unless the Parties mutually agree on a different Evaluation Period, or a different number of copies in an Order executed by both Parties and referencing these Special Terms); (ii) may install an evaluation framework comprising of malware and exploit samples, to the extent applicable, only on a single computer, in a controlled environment, which is not connected to a production network, with access to only the Your management server, all in accordance with documentation and materials furnished by Us; (iii) shall comply with the use restrictions in Section 8.4; and (iv) shall uninstall any portion of the Services Software residing on Your Covered Devices after the Evaluation Period, return all Documentation in its possession to Us, and confirm to Us in writing (email accepted) of such deletion and uninstallation. You understand that We may disable access to the Services automatically at the end of the Evaluation Period, without notice to Your. During and following the Evaluation Period, the Parties shall discuss Evaluation results in good faith.

c) Early Adoption or Beta Use. If You are invited to and agree to participate in an Early Adoption Program or Beta Program, You acknowledge that Early Adoption or Beta versions of the Services are prerelease versions of the Services and as such may contain errors, bugs or other defects. Accordingly, Your use and testing of the Early Adoption and/or Beta versions of the Services is subject to the disclaimers stated in Section (1) below. Additionally, Your use of Early Adoption and/or Beta versions of the Services is subject to Our sole discretion as to length and scope of use, updates and support of such Early Adoption or Beta versions of the Services.

1. DISCLAIMER OF WARRANTIES AND LIABILITY. DURING EVALUATION, OR EARLY ADOPTION OR BETA USE OF THE SERVICES, THE SERVICES ARE OFFERED ON AN "AS IS" BASIS, WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NON-INFRINGEMENT, OR THOSE ARISING BY LAW, STATUTE, USAGE OF TRADE, OR COURSE OF DEALING. YOU ASSUME ALL RISK AS TO THE RESULTS AND PERFORMANCE OF THE SERVICES AND ACKNOWLEDGES THAT THE USE OF THE SERVICES, TO THE EXTENT APPLICABLE, MUST BE MADE IN STRICT CONFORMANCE WITH SENTINELONE'S INSTRUCTIONS. WITHOUT DEROGATING FROM THE FOREGOING, IT IS UNDERSTOOD AND AGREED THAT SENTINELONE WILL NOT BE LIABLE FOR ANY NETWORK DOWNTIME, SERVICES DOWNTIME, AND/OR IDENTIFYING AREAS OF WEAKNESS IN THE SERVICES. FOR ALL EVALUATIONS, OR EARLY ADOPTION OR BETA USE OF THE SERVICES, WE SHALL HAVE NO LIABILITY TO YOU OR ANY OTHER PERSON OR ENTITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR PROFIT, LOST OR DAMAGED DATA, LOSS OF PROGRAMS OR INFORMATION OR OTHER INTANGIBLE LOSS ARISING OUT OF THE USE OF OR THE INABILITY TO USE THE SERVICES, OR INFORMATION, OR ANY PERMANENT OR TEMPORARY CESSATION OF THE SERVICES OR ACCESS TO INFORMATION, OR THE DELETION OR CORRUPTION OF ANY CONTENT OR INFORMATION, OR THE FAILURE TO STORE ANY CONTENT OR INFORMATION OR OTHER COMMERCIAL OR ECONOMIC LOSS, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE), EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR THAT THEY ARE FORESEEABLE. WE ALSO ARE NOT RESPONSIBLE FOR CLAIMS BY ANY THIRD PARTY. WHILE THE SERVICES ARE PROVIDED FREE OF CHARGE FOR EVALUATION, EARLY ADOPTION OR BETA PURPOSES ONLY, OUR MAXIMUM AGGREGATE LIABILITY TO YOU SHALL NOT EXCEED US $100. IN JURISDICTIONS WHERE THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES IS NOT ALLOWED OUR LIABILITY OF SHALL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY LAW. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO THE PARTIES OBLIGATIONS UNDER SECTION 7 HEREIN.

8.4 Restrictions. Except as expressly authorized by these Special Terms, You may not do any of the following: (i) modify, disclose, alter, translate or create derivative works of the Services (or any components thereof) or any accompanying Documentation; (ii) license, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Services (or any components thereof) or any Documentation; (iii) use the Services other than as permitted under these Special Terms, as directly related to Your internal business operations and in conformity with the Documentation, and not otherwise use the Services for any other commercial or business use, including without limitation offering any portion of the Services as benefits or services to third parties; (iv) use the Services in violation of any laws or regulations, including, without limitation, to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party privacy rights; (v) use the Services to store, transmit or test for any viruses, software routines or other code designed to permit unauthorized access, disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (vi) probe, scan or test the efficacy or vulnerability of the Services, or take any action in an effort to circumvent or undermine the Services, except for the legitimate testing of the Services in coordination with Us, in connection with considering a subscription to the Services as licensed herein; (vii) attempt or actually disassemble, decompile or reverse engineer, copy, frame or mirror any part or content of the Services, or otherwise derive any of the Services' source code; (viii) access, test, and/or use the Services in any way to build a competitive product or service, or copy any features or functions of the Services; (ix) interfere with or disrupt the integrity or performance of the Services; (x) attempt to gain unauthorized access to the Services or their related systems or networks; (xi) disclose to any third party or publish in any media any performance information or analysis relating to the Services; (xii) fail to maintain all copyright, trademark and proprietary notices on the Services and any permitted copy thereof; or (xiii) cause or permit any Services user or third party to do any of the foregoing.

8.5 Privacy and Security.

8.5.1 Processing Limitations and Security Obligation**.** In providing You the Services We will (i) store, process and access Your Data only to the extent reasonably necessary to provide you the Services and to improve the Services; and (ii) implement and maintain commercially reasonable technical, physical and organizational measures to protect the security, confidentiality and integrity of Your Data hosted by Us or Our authorized third party service providers from unauthorized access, use, alteration or disclosure. **"**Your Data" means all data and information associated with You which is uploaded to, processed by, generated by, and/or stored within the Services by You or through Your use of the Services.

8.5.2 Data Privacy. We will handle Your Personal Information in accordance with these Special Terms, our Privacy Policy, and privacy laws applicable to the Personal Information the Services collect when operating in default mode (expressly excluding specific privacy laws applicable to files the Services may collect if You elect to trigger certain features resulting in the processing of any file by the Services). Such privacy laws include the California Civil Code Sec. 1798.100 et seq. ("CCPA") and the EU General Data Protection Regulation 2016/679 ("GDPR") and We shall act exclusively as a Service Provider (as defined by CCPA), and Data Processor (as defined in GDPR) and shall retain, use, disclose and process Personal Information solely for the purpose of providing and enhancing the Services To the extent You provide to Us Personal Information of individuals residing in the European Economic Area ("EEA"), You and We hereby agree that You shall be deemed the data controller (as defined in GDPR) and any applicable national laws made under it, and where You are established in Switzerland, the Swiss Federal Act of 19 June 1992 on Data Protection, as may be amended or superseded), and in its capacity as Processor of Personal Information, We shall process such Personal Information only for the purpose of providing and enhancing the Services subject to these Special Terms, and as otherwise instructed by the controller of such Personal Information.

8.6 Hosting Location. Unless otherwise specifically agreed among the Parties, Your Data may be processed and/or hosted by Us or Our authorized third-party service providers in the United States.

8.7 Anonymized Data. Notwithstanding anything to the contrary in these Special Terms, We may monitor, collect, use and store anonymous and aggregate statistics and/or data regarding use of the Services solely for Our internal business purposes or the internal business purposes of our third party provider(including, but not limited to, improving the Services and creating new features) and such anonymized and aggregate data shall not be considered Your Data.

8.8 Representations, Warranties and Remedies.

8.8.1 General Representations and Warranties. Each Party represents and warrants it shall deliver (as to Us) and operate (as to You) the Services in material conformity with the Documentation and the terms herein; and (v) it will perform its obligations under these Terms in accordance with applicable federal or state laws or regulations.

8.8.2 Conformity with Documentation. We warrant that at any point in time during the Term, the most recent release of the Services (the "Current Release") will substantially conform in all material respects with the Documentation. Our sole obligation for material non-conformity with this warranty shall be, in Our sole discretion, to use commercially reasonable efforts (i) to provide You with an error-correction or workaround which corrects the reported non-conformity; (ii) to replace the non-conforming portions of the Services with conforming items; or (iii) if We reasonably determines such remedies to be impracticable within a reasonable period of time, to terminate the Services and refund the Fees paid for the Services. The above warranty will not apply: (a) if the Services are not used in compliance with the Documentation; (b) if any unauthorized modifications are made to the Services by You or any third party; (c) to use of early releases of the Services which are not the Current Release or the Services release immediately preceding the Current Release; (d) to defects due to accident, abuse or improper use by You; or (e) to Evaluation or Early Adoption use of the Services.

8.8.3 Disclaimer. EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES SET FORTH IN THIS SECTION 8.8, EACH PARTY ON BEHALF OF ITSELF AND ITS THIRD PARTY LICENSORS DISCLAIMS ANY AND ALL REPRESENTATIONS OR WARRANTIES (EXPRESS OR IMPLIED, ORAL OR WRITTEN) WITH RESPECT TO THESE TERMS AND THE SENTINELONE SERVICES, WHETHER ALLEGED TO ARISE BY OPERATION OF LAW, STATUTE, CUSTOM OR USAGE IN THE TRADE, BY COURSE OF DEALING OR OTHERWISE, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE (WHETHER OR NOT SUCH PARTY KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE AWARE OF ANY SUCH PURPOSE), ACCURACY, NON-INFRINGEMENT, CONDITION OF TITLE. THIS DISCLAIMER AND EXCLUSION WILL APPLY EVEN IF ANY EXPRESS WARRANTY HEREIN FAILS OF ITS ESSENTIAL PURPOSE.

8.9 Customer Indemnity. Customer, at its sole expense, will indemnify us and its directors, officers, employees and agents or other authorized representatives and its licensors and third party service providers from and against any Claim, and be liable for any related damages, payments, deficiencies, fines, judgments, settlements, liabilities, losses, costs and expenses (including, but not limited to, reasonable attorneys' fees, costs, penalties, interest and disbursements) arising out of: (a) Customer's use of the Services in breach of these Special Terms; (b) Customer's use of any third party IP; (c) breach or alleged breach of Customer's obligations under Sections 8.3.1.a) (Other Services) 8.3.1.b) (Third Party Service) or 8.4 (Restrictions) herein; or (d) the failure of Your administrators of Your account to maintain the confidentiality of their login information to such account. Customer's indemnification obligations under this Section 8.9 are conditioned upon Our: (i) giving prompt written notice of the Claim (provided that failure to provide prompt written notice to the indemnifying Party will not alleviate Customer's obligations under this Section 8.9 to the extent any associated delay does not materially prejudice or impair the defense of the related Claims); (ii) granting You the option to take sole control of the) and settlement of the Claim (except that Our prior written approval will be required for any settlement that reasonably can be expected to require an affirmative obligation of Us); and (iii) providing reasonable cooperation to You and, at the Your request and expense, assistance in the defense or settlement of the Claim.

8.10 Limitation of Liability.

8.10.1 SUBJECT TO ANY SPECIFIC LIMITATIONS ON LIABILITY STATED IN THIS SECTION, IN NO EVENT WILL EITHER PARTY'S TOTAL LIABILITY ARISING OUT OF OR RELATED TO THESE TERMS EXCEED THE FEES PAID OR PAYABLE BY CUSTOMER TO US FOR 6 MONTHS SERVICES FEES AT THE TIME OF THE EVENT OR EVENTS LEADING TO THE ALLEGED DAMAGES.

8.10.2 IN THE EVENT OF A BREACH OF SECTION 8 5 (PRIVACY AND SECURITY) THE TOTAL CUMULATIVE LIABILITY OF US OR ANY OF OUR LICENSORS OR THIRD PARTY SERVICE PROVIDERS SHALL NOT EXCEED THE FEES PAID OR PAYABLE BY CUSTOMER TO US FOR 12 MONTHS SERVICES FEES EFFECTIVE AT THE TIME OF THE EVENT OR EVENTS LEADING TO THE ALLEGED DAMAGES.

8.10.3 THE LIMITATIONS ON LIABILITY IN THE MSA OR IN SECTIONS 8.10.1 AND 8.10.2 SHALL NOT APPLY TO BREACHES OF SECTION 8.3 (LICENSE GRANT) SECTION 8.4 (RESTRICTIONS), OR TO SECTION 9 (CUSTOMER INDEMNITY).

8.10.4 IN NO EVENT WILL EITHER PARTY OR ITS LICENSORS OR THIRD PARTY SERVICE PROVIDERS BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOSS OF PROFITS, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, ANY INTERRUPTION OF BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF, OR IN CONNECTION WITH THESE TERMS, WHETHER IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN ADVISED OR IS OTHERWISE AWARE OF THE POSSIBILITY OF SUCH DAMAGES. MULTIPLE CLAIMS WILL NOT EXPAND THIS LIMITATION. THIS SECTION 10 WILL BE GIVEN FULL EFFECT EVEN IF ANY REMEDY SPECIFIED IN THESE TERMS IS DEEMED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

8.11 Export Compliance. The Services, and Services Software or other components of the Services which We may provide or make available to You for use by Your users are subject to U.S. export control and economic sanctions laws. You agree to comply with all such laws and regulations as they relate to Your access to and use of the Services. You shall not access or use the Services if You are located in any jurisdiction in which the provision of the Services is prohibited under U.S. or other applicable laws or regulations (a **"Prohibited Jurisdiction")** and You agree not to grant access to the Services to any government, entity or individual located in any Prohibited Jurisdiction. You represent, warrant and covenant that (i) You are not named on any U.S. government list of persons or entities prohibited from receiving U.S. exports, or transacting with any U.S. person; (ii) You are not a national of, or a company registered in, any Prohibited Jurisdiction; (iii) You shall not permit users to access or use the Services in violation of any U.S. or other applicable export embargoes, prohibitions or restrictions; and (iv) You shall comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which You and users are located. You represent that neither You nor any of Your subsidiaries is an entity that (a) is directly or indirectly owned or controlled by any person or entity currently included on the Specially Designated Nationals and Blocked Persons List or the Consolidated Sanctions List maintained by the Office of Foreign Assets Control, US Department of the Treasury ("OFAC") or other similar list maintained by any governmental entity, or (b) is directly or indirectly owned or controlled by any person or entity that is located, organized, or resident in a country or territory that is, or whose government is, the target of sanctions imposed by OFAC or any other governmental entity.

SERVICE LEVEL AGREEMENT:
FOR MANAGED ENDPOINT DETECTION AND RESPONSE SERVICES ("MANAGED EDR SLA")

The following terms and conditions apply to the service levels of Services provided pursuant to this Attachment. In the event we fail to meet the levels defined in Service Level Agreement for a minimum of two (2) consecutive months, you must notify us in writing of any violations and allow us thirty (30) days from notification to cure the breach. If still unresolved, you may immediately terminate the Service giving rise to such breach without additional notification or incurring early termination fees within thirty (30) days of our failure to cure.

1. SERVICE HOURS OF OPERATION. We maintain Security Operations, Network Operations, and Technical Support departments on a 24 x 7 x 365 basis. You may reach an individual in each of these departments by calling the appropriate support service.

2. RESPONSE TIME. We commit to certain incident response times. These commitments are subject to your providing us accurate and current contact information for your designated points of contact. Our failure to respond in accordance with the parameters defined herein will entitle you to receive, as your sole remedy and our sole obligation, credits described below, *provided however*, that you may obtain no more than one credit per day, regardless of how often in that day we failed to meet these parameters.

2.1. Security and Network Operations Events. We classify all events as high, medium, or low level. We will identify or begin analysis of high level events within fifteen (15) minutes, medium level events within one (1) hour, and low level events within twenty-four (24) hours of occurrence. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 1 credit for high level events or one-day Tier 2 credit for medium and low level events.

2.2. Change Requests. We will make commercially reasonable efforts to begin implementation of changes you request to your service or equipment within twenty-four (24) hours of receipt of the appropriate change control form, requested changes will normally be implemented during Customer's non-business hours. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 2 credit.

3. SERVICE AVAILABILITY GUARANTEE. Our commitment is to have the Services available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Service(s) were not available to you in a calendar month (**"Service Unavailability")**. Service Unavailability will not include unavailability continuing for an hour or less or any unavailability that you fail to report to us within five (5) days. Failure to meet the service level described in this Section will entitle you to receive a Tier 1 credit.

4. MAINTENANCE. We reserve the following weekly maintenance windows during which you may experience periodic service outages:

(i) Tuesday and Thursday (12 AM – 2 AM ET)

(ii) Saturday (12 AM – 5 AM ET)

In the event we must perform maintenance during a time other than the service windows provided above, we will provide notification prior to performing the maintenance.

5. CREDIT REQUEST AND PAYMENT PROCEDURES. For failures to meet service levels herein in a calendar month, you will be entitled to receive a credit as specified below:

(i) **Tier 1.** Equal to twice the prorated portion of the monthly fee for the affected service; or

(ii) **Tier 2.** Equal to the prorated portion of the monthly fee for the affected service;

provided however that a breach of this SLA due to Exceptions described below will not qualify for such credits.

To receive a credit under this SLA, you must be current with your payments at the time Service Unavailability occurred. In addition, all credit requests must be submitted in writing, either through our ticketing system, via email or fax, or by certified U.S. mail, postage prepaid. You must submit each request for credit within seven (7) days of the occurrence giving rise to the credit claim. The total credit amount we will pay to you in any calendar month will not exceed, in the aggregate, half of the total fees invoiced to you for the Services for which a claim is made in the applicable month. (Credits are exclusive of any applicable taxes charged to you or collected by us.)

6. EXCEPTIONS. You will not receive any credits under this SLA in connection with any failure or deficiency of the Services or a failure to meet service level caused by or associated with any of the following:

(i) Maintenance, as defined above;

(ii) Fiber cuts or other such issues related to telephone company circuits or local ISP outside of our control;

(iii) Your applications, equipment, or facilities;

(iv) You or any of your end-user' acts or omissions;

(v) Reasons of Force Majeure as defined in the MSA;

(vi) Any act or omission on the part of any third party, not reasonably within our control;

(vii) First month of service for the specific Services for which a credit is claimed;

(viii) DNS issues outside our direct control;

(ix) Broadband connectivity.

7. Fair Usage Cap for Log Collection on Monitoring Service

(i) SilverSky maintains a fair usage policy to ensure the availability and sustainability of the Monitoring Service. Failure to adhere to the fair usage policy will result first in a notification to you and then, if you fail to take remedial action, suspension of this SLA until such time as the usage level on the affected device falls below the notification threshold set forth below. Usage information is made available to you within our portal

1. SilverSky will notify you that you are exceeding the Fair Usage Threshold or "FUT" when you exceed any of the following FUTs:

   1. The average events per second across the set of monitored devices exceeds 25 events per second per device, over a 7 day period. An individual device exceeds an average of 100 events per second, over a 1 hour period

   2. The average events per second across the set of monitored devices exceeds 20 events per second per device, over a 30 day period.

(ii) Partial Service Suspension Threshold

Following the notice as set forth in (i) A.1 above, if the average events per second across the set of monitored devices exceeds 25 events per second per device, over a 7 day period, SilverSky reserves the right cease ingestion of security events from an affected device, starting from the device producing the most events per second, until the average events per second across the set of monitored devices falls beneath the FUT.

Following the notice posted to the portal as set forth in A.2 above, if an individual device exceeds an average of 250 events per second, over a 1 hour period, SilverSky may upon notification to the Customer cease ingestion of security events from the affected device.

Managed Endpoint Detection and Response (MEDR)

SCOPE OF WORK

SilverSky will provide the customer with the following services:

- An agent that can be deployed on each endpoint that Customer identifies as needing the service
- Reducing false positives
- Security event detection and prioritization as per the SLA
- Monthly reporting

SERVICE IMPLEMENTATION

SilverSky Responsibilities

a. Conduct a knowledge-sharing survey to collect information about the Customer's environment, including devices to be monitored and processes needed to support the implementation of services.
b. Establish a method of installing the agent on Customer devices.
c. Provide assistance to the Customer to configure devices chosen for installation.
d. Notify the Customer that the devices are operational to ensure alerting.
e. Provide initial training and training materials for the portal.

Customer Responsibilities

a. The Customer shall designate a qualified and trained Technical Lead to oversee the Customer engagement for this project. The Technical Lead will oversee the project, track status, facilitate the delivery of services and progress of the project, and communicate to the Customer's stakeholders.

Service Deliverables

a. Capture information from the Customer's devices.
b. Perform analysis of the data. This includes, but is not limited to, aggregation, parsing, correlation and alerting.
c. In cases of significant risk, our security engineers will analyze incidents following an alert based on the-risk notification system.
d. Security Engineers will notify the Customer of incidents requiring a response.
e. Security alerts will be sent to the Customer within 10-minutes of its creation.

ASSUMPTIONS

SilverSky

a. Shall provide resources who have been trained on products, technologies, and services applicable to this Scope of Work.
b. All communications, notifications, and alerts will be provided to Customer.

Customer

a. The Customer shall furnish, in a timely manner, all resources including personnel, systems, information, and software necessary to commence service implementation.
b. The Customer shall designate an appropriately qualified and trained technical lead who will be a permanent stakeholder throughout engagement.
c. The Customer retains authority and responsibility for decisions made regarding this service implementation.
d. The Customer will be responsible for project management and coordination of Customer resources necessary to complete the service implementation.
e. The Customer is responsible for coordinating, following, and communicating in a timely manner all internal processes for change management, SDLC, etc.
f. The Customer is responsible for the quality of data and any remediation efforts that may be necessary to complete this service implementation.
g. The Customer is accountable for all non-oral output, including documentation, plans, recommendations, diagrams, etc.
h. The Customer is responsible for any direct or physical remediation.

Specific Ransomware Warranty for MEDR

1. **Ransomware Warranty.** During the Ransomware Warranty Agreement, so long as the Customer also subscribes to the Services in compliance with the Agreements, the Customer's Endpoints will be protected by the Services which will screen for any Ransomware. The Ransomware Warranty granted herein shall apply to all such Endpoints provided that:

(a) The Services are deployed in the Endpoints in accordance with the Documentation and such Endpoints are currently active and properly configured;

(b) Only Files that are on Endpoints are covered under this Ransomware Warranty;

(c) All Endpoints of the Customer have the following required configurations:

(i) Services:

- Policy mode options are set to Threats: Protect and Suspicious: Protect.
- All Engines are set to ON.
- Cloud Connectivity is not disabled.
- Anti-Tamper is turned ON
- Snapshots are turned ON
- Scan New Agents is turned ON
- The latest General Availability (GA) version (or GA with a critical security Service Pack (SP), if issued) or the GA (or GA with a critical SP, if issued) version immediately preceding such latest GA version, of the SentinelOne Windows Endpoint Agent (as specified in the SentinelOne Knowledge Base "Latest Information" article) is deployed prior to the time of Ransomware infection.
- There are no Pending Actions (such as Reboot) listed on any covered Endpoint.
- A supported version of the Management Console is deployed.
- Exclusions specified in the SentinelOne Knowledge Base "Not Recommended Exclusions" article, are not deployed in the Management Console or Agent.

(ii) Operating system:

- The Ransomware Warranty applies to Standard (not Legacy) Windows Agents, and on supported versions of Microsoft Windows (as specified in the SentinelOne Knowledge Base "System Requirements" article).
- Each endpoint is malware-free prior to SentinelOne Windows Agent installation.
- OS is fully updated and patched on each covered Endpoint, and all compromised applications are updated to latest releases.
- VSS (Volume Shadow Copy Service) is enabled and functioning on all Windows endpoints. VSS Disk Space Usage allocation must be configured with at least 10% on all disks.

(d) The Customer adheres to the following manual actions post infection (i.e. discovery of Ransomware):

- immediately adds the specific Ransomware threat to blacklist;
- in case the Ransomware was not blocked but only detected – takes a remediation and rollback action within 1 hour of infection/discovery of the Ransomware; and
- notifies SentinelOne of the Ransomware discovery within 24 hours at Ransomware Warranty@sentinelone.com.

this Section 1(d) shall not apply if the Customer is subscribed to the Vigilance Response service during the Ransomware Warranty Agreement.

2. **Scope of the Ransomware Warranty**. Subject to the terms of this Ransomware Warranty Addendum, including the specific requirements of Section 1 above, in case of a successful ransomware attack on Customer Endpoints covered by the Ransomware Warranty, as shown in SentinelOne's logs and other records, SentinelOne will pay as sole and exclusive remedy to the Customer actual damages caused by such attack, capped at $1,000 USD per Endpoint affected by a Breach, and further capped at $1,000,000 USD for every consecutive 12 months in which Customer subscribes to the Services with respect to the affected Endpoint. For the avoidance of doubt, the recovery amount set forth herein is limited to 1,000 Endpoints for each applicable 12 month period.

3. **Condition Precedent to Ransomware Warranty Payment**. SentinelOne shall only provide the remedy for the Breach of the Ransomware Warranty as described above if (i) the Ransomware attack has occurred, is discovered by the Customer and reported to SentinelOne during the Ransomware Warranty Agreement and Customer's subscription to the Services under the Agreements; (ii) Customer's Endpoints and the Services are configured in accordance with the Documentation and Section 1 above; (iii) the Customer demands in writing to recover for damages caused by the Breach; and (iv) sufficient evidence is provided by Customer supporting the Ransom demand amount for each Ransomware infection covered by this Ransomware Warranty.

4. **Exclusions**: The Ransomware Warranty shall not apply to a breach caused primarily by (i) any deployment, configuration and/or use of the Services (or a portion thereof), for any or no reason, in a manner inconsistent with the Documentation or the requirements of Section 1 herein; (ii) Customer's negligence or misconduct; or (iii) other products and/or services which directly or indirectly cause the malfunction or non-performance of the Services with respect to the subject Ransomware.

5. **Sole and Exclusive Remedy**. The aforementioned remedy for the Breach shall be the Customer's sole and exclusive remedy and the entire liability of SentinelOne for any Breach of the Ransomware Warranty.

6. **Definitions.** The capitalized terms below shall have the following meaning:

(a) **"Breach"** means the unauthorized access to at least one Customer Endpoint in the form of Ransomware which has caused material harm to the Customer, whereby "material harm" must include at least one of the following: (i) the unauthorized acquisition of unencrypted digital data that compromises the security, confidentiality, or integrity of personal information or confidential information maintained by the

Customer; (ii) public disclosure of personal information or confidential information maintained by the Customer; or (iii) the compromise of at least one Customer Endpoint resulting the blocking of access to such Endpoint.

(b) **"Ransomware**" means a malware software program that infects Customer's systems from external sources (i.e. in the wild), which installs, persists and encrypts a large portion of files at the operating system level, and continuing to demand payment (the "**Ransom**") in order to decrypt the encrypted files. For clarification, Ransomware does not include any malware introduced by the Customer or any third party to Customer's internal systems, whether intentionally (i.e., malware testing) or through a breach in the system's security.

(c) "**Endpoints**" shall mean any computing device with a Microsoft Windows operating system, that has the Services installed per the Documentation under valid Agreements among SilverSky and the Customer.

7. **Other Agreements and Conditions.** Any other terms and conditions of the Agreements shall be unaffected by this Ransomware Warranty, except as expressly stated in the Agreement. In case of any conflict between the terms of this Ransomware Warranty and the terms and conditions within the Agreement relating to the Ransomware Warranty, the terms and conditions within this Ransomware Warranty shall prevail.

8. **Miscellaneous.** This Ransomware Warranty represents the complete agreement between the parties concerning the Ransomware Warranty granted hereunder and supersedes any and all prior agreements or representations between the parties. SentinelOne may revise the terms of this Ransomware Warranty from time to time in its reasonable discretion, provided that such revisions shall not reduce or eliminate the monetary remedy described in Section 2 herein. To the extent that SentinelOne pays to the Customer under the Ransomware Warranty, Customer agrees that SentinelOne shall acquire a subrogation right to assert a claim against the hacker who delivered the Ransomware to Customer and caused damages for which SentinelOne incurred Ransomware Warranty costs, and Customer further agrees to assist SentinelOne should it decide to assert a claim against such hacker. If any provision of this Ransomware Warranty is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable.