

# **ATTACHMENT 1**

## **Agreement for Services with Kroll**

**STATEMENT OF WORK  
FOR  
Kroll CyberDetectER® Endpoint powered by Red Canary**

This Statement of Work (“SOW”), dated July 13, 2021, is entered into pursuant to and incorporates herein by reference the letter of engagement entered into as of February 8, 2019 (together with this SOW, the “Agreement”), by and between County of Santa Barbara (“Client”) and Kroll Associates, Inc. (“Kroll”) for the Kroll Services described herein. Capitalized terms herein shall have the meaning ascribed in the letter of engagement.

Kroll Services and Red Canary Services are described below and subject to the respective terms and conditions referenced herein.

**A. Description of Kroll Incident Response and Remediation Services (“Kroll Services”)**

As part of **Kroll CyberDetectER® Endpoint powered by Red Canary** service, Kroll will provide the following Kroll Services to Client:

<b>Description of Kroll Services</b>
<p><b><u>Kroll Threat Alert Response and Remediation Support:</u></b></p> <p>Kroll will provide response and remediation support associated with specific Threat Alerts and other suspicious Endpoint activity reported by Kroll or Red Canary, as requested by Client, including:</p> <ul style="list-style-type: none"> <li>● Supplemental threat analysis and intelligence</li> <li>● Malware sandboxing and analysis</li> <li>● Configuration and activation of manual and/or automated response and remediation actions supported within the Portal and/or directly through Endpoint Collection Software (e.g. hash banning, file deletion, process termination, and endpoint isolation)</li> <li>● Threat Alert correlation and root cause analysis using the Endpoint Collection Software</li> <li>● Remediation guidance</li> </ul> <p>Client understands and accepts that, while not anticipated, any response and remediation actions taken could cause unforeseen system errors, outages, or data loss.</p> <p><b><u>Kroll Incident Response and Investigation Services</u></b></p> <p>Kroll may provide additional incident response or investigative services, as requested by Client and pursuant to an additional Statement of Work, including:</p> <ul style="list-style-type: none"> <li>● Emergency and after-hours incident response support</li> <li>● Remote evidence collection and analysis</li> <li>● In-lab forensic imaging and analysis</li> <li>● Malware reverse engineering</li> <li>● Event log collection, analysis and correlation</li> <li>● Custom threat hunting or forensic investigation using the Endpoint Collection Software</li> <li>● Custom analysis and reporting</li> </ul> <p>Kroll Incident Response and Investigation Services and are billed hourly and invoiced separately in accordance with the terms of this Agreement.</p> <hr/> <p>Unless otherwise noted, Kroll Threat Alert Response and Remediation support is available 09:00 to 18:00 EST/EDT, Monday through Friday– excluding US Federal holidays. After-hours Incident Response and Investigation Services are available on an emergency basis.</p>

**B. Fee Structure and Invoicing**

The initial term of this Statement of Work shall be for twelve (12) months (“Initial Term” or “Term”) from the date above (“Effective Date”), ending July 12, 2022.

Invoicing for Managed Threat Detection Services. On behalf of its strategic partner, Red Canary, Kroll shall invoice Client for **Kroll CyberDetectER® Endpoint powered by Red Canary**, Red Canary Services, on a fixed fee basis for **5,950** Endpoints (“End User’s Endpoints”). For the Initial Term, the cost per Endpoint for twelve (12) months is **\$72.00**. “Endpoint” means any kind of computing device that the Endpoint Collection software supports and from which it can

collect data, and may include by is not limited to computer workstations, laptops, file and print servers, e-mail servers, Internet gateway devices, storage area network servers (SANS), and terminal servers.

Kroll shall invoice the Client in full for the cost of this service in advance of the Effective Date of the Initial Term. **The Term is not cancellable, and all payments are non-refundable.** Payment is due upon receipt of the invoice.

**Endpoint True-ups.** In the event that during the Term, the number of Endpoints increases beyond the number listed above, Client will be invoiced for the additional Endpoints on installation of each added Endpoint, at the price listed above per Endpoint. Incremental Endpoints will be billed during the calendar quarter immediately subsequent to the increase in Endpoints and be pro-rated retroactively from date of implementation. The Term will be measured from the date of implementation for each added Endpoint.

**Invoicing for Additional Services.** In addition to the **Kroll CyberDetectER® Endpoint powered by Red Canary** services described above, Client may, at its option, request that Kroll provide additional services, including Kroll Incident Response and Investigation services, each pursuant to an additional Statement of Work, for an additional cost ("**Additional Services**"). To the extent the Client requests Kroll to perform such Additional Services, the Professional Fees for such Additional Services will be charged at Kroll's then-current rates, less a discount of 15%. Kroll's current rates are as follows:

Consulting Services	\$500/hour
Travel Time	50% of Consultant hourly rate
Media Preservation/Replication	\$400/media
Media / Data Storage	\$25/media/month

For Incident Response and Remediation Support hours, or any other Additional Services, Kroll shall invoice Client for the services performed on a monthly basis with the fee due and payable within thirty (30) days of the date of the invoice. In addition to the Professional Fees identified above, additional charges may include reasonable out-of-pocket expenses incurred in connection with these services.

To the extent any expedited and/or emergency services are requested by Client, including work that must be performed over a weekend or holiday, or on an overtime basis, Kroll reserves the right to charge for such expedited services at 1.5 times its normal hourly rates for the applicable services.

To the extent Kroll is requested to provide any written testimony or reports, such additional services will be provided at Kroll's standard applicable hourly rates. However, oral testimony at deposition, a hearing or trial will be provided at 1.5 times such rates.

**C. Red Canary Managed Threat Detection Services (“Red Canary Services”)**

As Kroll’s strategic partner in providing the **Kroll CyberDetectER® Endpoint powered by Red Canary** service, Red Canary will be responsible for providing the following Red Canary Services to Client, subject to Client’s acceptance of, and provided pursuant to, the Red Canary End User Security Platform Agreement and Statement of Work (“EUSPA”), which terms and conditions are included in **Exhibit A**.

Additionally, Client further accepts and agrees to the terms of the Software End User License Agreement(s) (“Software EULA”) for the Endpoint Collection Software, which is incorporated as **Exhibit B**.

**In connection with the Kroll CyberDetectER® Endpoint powered by Red Canary services, Client acknowledges and agrees that Client’s acceptance of and agreement to the EUSPA and the Software EULA as evidenced by Client’s signature below, is required for the provision of the Red Canary Services by Red Canary.**

<b>Description of Red Canary Services</b>
<p><b>Party Services:</b> Red Canary Managed Threat Detection Services, provided by Red Canary for use by Client and Kroll pursuant to the terms and conditions of the mutually executed Red Canary End User Security Platform Agreement and Statement of Work (“EUSPA”).</p> <ul style="list-style-type: none"> <li>● Includes 24x7x365 Red Canary Threat Alert escalation and Portal access.</li> <li>● Includes Automate features</li> </ul>
<p><b>Threat Alerts:</b> Red Canary will provide, as appropriate, Threat Alerts. “Threat Alerts” means analyst-vetted alerts on malicious activity detected by Red Canary on Client Endpoints.</p> <p>Threat Alerts will be sent to Kroll and Client’s technical contacts as configured in the Red Canary Portal. Where applicable, each Threat Alert includes information describing the background of the threat related to the particular Alert.</p> <p>Threat Alerts will contain information that is known to Red Canary about the threat at the time, which typically includes but is not limited to:</p> <ul style="list-style-type: none"> <li>● Summary of the detected threat</li> <li>● Name of affected endpoint and user</li> <li>● Artifacts such as file names, Internet Protocol (IP) addresses, domain names and registry keys that help support both Client remediation efforts and identification of similar threats.</li> </ul>
<p><b>Client Portal:</b> Client and Kroll will be provided with access to the Red Canary portal (“<u>Portal</u>”) through which Client and Kroll can view data and Threat Alerts.</p>
<b>Client’s Software License (“Software EULA”)</b>
<p><b>Third Party Software:</b> The Red Canary Services include the provision of endpoint monitoring using VMware Carbon Black Enterprise Response software (“<u>Endpoint Collection Software</u>”), which is provided to Client in connection with the Red Canary Services and licensed hereunder for use by Kroll and Red Canary on behalf of Client per the terms and conditions of the mutually executed VMware EULA incorporated as Exhibit B.</p>

**D. Client Responsibilities**

In connection with the Kroll Services and Red Canary Services, Client agrees to be responsible for performing the following tasks:

1. Installing and maintaining active Endpoint Collection Software on all Client systems to be monitored.
2. Provide Kroll and Red Canary with continuous access to Client’s instance of the Endpoint Collection Software to facilitate ongoing monitoring and response activities for the monitored Endpoints.



3. Obtaining all required authorizations to perform the Managed Threat Detection Services and any data or information required thereby. Client shall obtain consents and authorizes for Kroll and Red Canary and their employees and agents to gain access to and retrieve Technical Data and analyze Threat Alerts and to perform the Red Canary Services and the Kroll Services.
4. In the course of accessing, obtaining and otherwise using the Managed Threat Detection Services and Threat Alerts, Client shall have sole responsibility for the accuracy, quality, integrity, and authorization for use, and intellectual property ownership or right to use necessary for the transferability to Red Canary and Kroll of Technical Data.
5. Client will permit Kroll to include anonymized data that Kroll obtains from the monitoring of Client's endpoints in Kroll's proprietary threat intelligence database or feeds, as well as sharing any such data with its intelligence partners. This data includes binary hashes, binary metadata, and Carbon Black Response event data such as process hashes, IP addresses, domain names, user context (System vs. Local, Root, Network Service, etc.) and operating system version identifiers.

**Client's signature below hereby also accepts and agrees to the Descriptions of Services and Client Responsibilities above, and to the following terms and conditions with Red Canary attached hereto:**

1. the EUSPA in **Exhibit A**; and
2. the VMware EULA in **Exhibit B**.

**IN WITNESS WHEREOF**, the parties have accepted, agreed, and executed this Statement of Work to be effective on the date executed by COUNTY.

**ATTEST:**  
MONA MIYASATO,  
COUNTY EXECUTIVE OFFICER  
CLERK OF THE BOARD

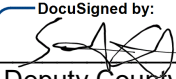
By: \_\_\_\_\_  
Deputy Clerk

**COUNTY**  
**COUNTY OF SANTA BARBARA**

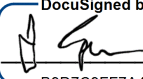
\_\_\_\_\_  
BOB NELSON, CHAIR  
BOARD OF SUPERVISORS

Dated: \_\_\_\_\_

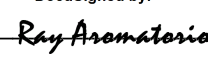
**APPROVED AS TO FORM:**  
MICHAEL C. GHIZZONI  
COUNTY COUNSEL

DocuSigned by:  
By:  \_\_\_\_\_  
Deputy County Counsel


**APPROVED AS TO ACCOUNTING FORM:**  
BETSY SCHAFFER, CPA, CPFO AUDITOR-  
CONTROLLER

DocuSigned by:  
By:  \_\_\_\_\_  
B9D7C9FF7A414AE...


**APPROVED AS TO FORM:**  
RAY AROMATORIO, ARM, AIC  
RISK MANAGER

DocuSigned by:  
By:  \_\_\_\_\_  
D3DB8526E16F47F...

**RECOMMENDED FOR APPROVAL:**  
JANETTE D. PELL, DIRECTOR  
GENERAL SERVICES DEPARTMENT

DocuSigned by:  
By:  \_\_\_\_\_  
1FBA9BD673A445F...

**KROLL ASSOCIATES, INC.**

DocuSigned by:  
  
6ECA2A57DC4849E  
Name: Marc Brawner

Title: Managing Director

Date: 6/4/2021 | 1:54 PM PDT

**[CONTINUE TO NEXT PAGE]**

## **Exhibit A: END USER SECURITY PLATFORM AGREEMENT**

This End User **Security Platform Agreement** (this "Agreement") is entered into this date of July, 13, 2021 (hereinafter referred to as the Effective Date of the agreement), by and between Red Canary, Inc., a Delaware corporation with offices at 1750 15th Street #400, Denver, CO, 80202 (hereinafter referred to as "Red Canary") and client as identified in the Statement of Work (SOW) that incorporates this Agreement, (hereinafter referred to as "Client") (hereinafter individually referred to as "Party" and collectively referred to as "Parties").

**1. Term.** The term ("Term") of this Agreement will begin on the Effective Date and continue until the later of termination as provided in Section 6 herein.

**2. Statements of Work.** During the Term, Red Canary and Client may agree upon statements of work hereunder (each, a "SOW") defining the Managed Threat Detection Services ("Managed Threat Detection Services" or "Services") through which, Red Canary will provide as appropriate, threat alerts as defined in the SOW ("Threat Alerts"), Red Canary's compensation, the period of performance during which the Services will be provided (if applicable), and any additional terms and conditions. Each SOW shall be incorporated into and governed by this Agreement. Any changes to a SOW shall be agreed upon in writing by the parties. The parties agree that this Agreement and the applicable SOW(s) for Services shall govern and supersede any terms and conditions stated on any purchase order submitted by Client for such Services. In the event of any conflict between this Agreement and an SOW, the Agreement will control.

**3. Services.** Client hereby agrees that Red Canary may collect and use but not distribute, technical information about Client's devices, files, binaries, user activity, networks, systems, and software, and any other data contained therein ("Technical Data") for the purpose of providing Managed Threat Detection Services to Red Canary's customer base. Aggregated and anonymized Technical Data may be used for other purposes or distributed to third parties. Red Canary reserves the right to establish or modify its general practices and limits relating to storage of such data, and/or to delete or destroy any or all such data periodically.

**4. Intentionally Omitted.**

**5. Confidentiality/Ownership.**

(a). To the extent that confidential and proprietary information of each party including without limitation Technical Data ("Confidential Information") is exchanged and received in connection with the Services, each party agrees not to use the other party's Confidential Information except in the performance of, or as authorized by, this Agreement, and not to disclose, sell, license, distribute or otherwise make available such information to third parties. "Confidential Information" does not include: (i) information that was publicly available at the time of disclosure or that subsequently becomes publicly available other than by a breach of this provision, (ii) information previously known by or developed by the receiving party independent of the Confidential Information or independent of Red Canary Information obtained from any client or (iii) information that the receiving party rightfully obtains without restrictions on use and disclosure except where such is obtained from the client. Any Technical Data shall remain the confidential information and exclusive property of Client.

(b) Any Managed Threat Detection Services, Threat Alerts and information used to perform the Services, or included in any Threat Alert or Services, and any derivative works thereof, including but not limited to monitoring and analysis methodologies and tools, software, appliances, methodologies, code, customer, sender and recipient commercial and personal information, templates, service bureaus, tools, policies, records, working papers, knowledge, data or other intellectual property, written or otherwise and data, testing, analysis, evaluations and conclusions resulting from the disclosures herein shall remain the exclusive property of Red Canary.

**6. Termination.** The term of this Agreement expires on the expiration of the SOW incorporating this Agreement.

**7. Limited Warranty.**

OTHER THAN THE SERVICE DESCRIPTION PROVIDED FOR IN ANY APPLICABLE SOW, RED CANARY MAKES NO WARRANTY TO CLIENT, OR ANY OTHER PARTY, AND HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE THIRD PARTY SOFTWARE, THREAT ALERTS, MANAGED THREAT DETECTION SERVICES OR ANY OTHER SERVICES, OR RESULTS OF USE OR ANALYSIS OF THREAT ALERTS AND TECHNICAL DATA INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, OF QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ABSENCE OF HIDDEN DEFECTS, AND ANY WARRANTY THAT MAY ARISE FROM COURSE OF PERFORMANCE, BY REASON OF USAGE OR TRADE OR COURSE OF DEALING. The Managed Threat Detection Services and Threat Alerts are not fault-tolerant and are not designed, manufactured or intended for hazardous environments requiring fail-safe performance, where any failure of the Threat Alerts could lead directly to significant property or data loss or disclosure, interruption of business, breach of security, death, personal injury, or property damage ("High Risk Activities"). IN NO EVENT DOES RED CANARY WARRANT THAT MANAGED THREAT DETECTION SERVICES, THREAT ALERTS OR THIRD PARTY SOFTWARE WILL OPERATE OR BE USEFUL

WITHOUT INTERRUPTION, OR WILL BE FREE OF DEFECTS, OR NOT CAUSE OR RESULT IN A VULNERABILITY TO INTRUSION OR ATTACK OR ANY INTERRUPTION OF BUSINESS OR THAT THE MANAGED THREAT DETECTION SERVICE OR THREAT ALERTS WILL DETECT OR PREVENT ALL BUGS, VIRUSES, INTERRUPTIONS, INTRUSIONS, UNAUTHORIZED ACTIVITY, ERRORS, DATA THEFT OR DESTRUCTION AND DISCLAIM ALL WARRANTIES RELATING THERETO. Client acknowledges and agrees that Managed Threat Detection Services and Threat Alerts does not provide guarantee or warrant of protection, detection or accurate analysis of the Threat Alerts, and that Red Canary shall not be held liable in the event of security breach, attack, unintended release of sensitive information or other such event and that Client has responsibilities referenced in the SOW. Any service level agreements are goals and there is no guarantee or warranty they can be accomplished as no threat detection service is fail safe. As Client's sole remedy and Red Canary's sole obligation hereunder where there is material non-conformity in any Services or Threat Alert, Red Canary shall use good faith efforts to attempt to remedy any such non-conformity.

#### **8. Indemnification.**

(a) Red Canary hereby agrees to indemnify Client from any loss, damage, cost or expense (including reasonable attorneys' fees) ("Loss") arising from any claim, demand, assessment, action, suit, or proceeding ("Claim") as a result of Red Canary's or its personnel's (a) illegal or fraudulent conduct resulting in the disclosure of any Technical Data not permitted to be disclosed by Red Canary under this Agreement, or (b) violation of the intellectual property rights of a third party; except where such Loss or Claim arises in whole or in part from the Client not being in compliance with the terms of this Agreement or Client's or its personnel's illegal or fraudulent conduct.

(b) Client shall indemnify, defend and hold Red Canary and its employees, directors, shareholders, agents, and consultants harmless against any Loss arising from any Claim resulting from (i) access by Red Canary to Technical Data whether made by any of Client's customers, invitees, employees, agents or end users, (ii) Client's use or benefit of the Third Party Software, or use or reliance on the Managed Threat Detection Services or Threat Alerts, or (iii) any third party action resulting from any intrusions or security breaches except in the event of breach of this Agreement with respect to data that is in Red Canary's possession. In the event that Red Canary or any of its employees, directors, shareholders, agents, or consultants are required to testify in any judicial, administrative or legislative proceeding with respect to its Services hereunder, Client shall reimburse Red Canary from any and all costs, expenses, and time incurred in that regard.

**9. Limitation of Liability.** In no event shall Red Canary be liable for any incidental, consequential, special, exemplary or indirect damages, loss or interruption of business operations, lost profits, or data loss arising out of this Agreement or the provision by Red Canary or use by Client of the Services or Threat Alerts. Red Canary's total liability under this Agreement shall be limited to the fees paid by Client to Red Canary for the six (6) month period immediately preceding the claim, for the particular SOW upon which the claim is based. Red Canary, licensors and its suppliers will not be responsible for any damages, losses, expenses or costs that Client or any third party incurs or suffers as a result of any loss or theft of Technical Data.

#### **10. Miscellaneous.**

(a) This Agreement shall be the entire agreement between the parties to the exclusion of all antecedent or present representations, undertakings, agreements or warranties, expressed or implied and annuls, supersedes and replaces any and every other representation, warranty and agreement which may have existed between the parties. This Agreement may be amended only by a written instrument that has been similarly executed by both parties.

(b) The headings of this Agreement are for convenience only. In case of any difficulty in the interpretation of one or more of the headings, the headings shall have no meaning and no effect.

(c) All notices required under the Agreement to be given to a party must be in writing and delivered by hand or sent by registered post or email transmission addressed to the party at its address indicated below or at such other address as may be subsequently notified:

To Red Canary to:       1515 Wynkoop Street #390  
                                  Denver, CO, 80202  
                                  c/o Chris Zook, CFO

Written notices required under the Agreement will be deemed valid if delivered by hand or sent by registered post or email transmission and shall be effective on date of receipt.

(d) It is acknowledged that it is the intent of the parties that the provisions contained in this Agreement should be enforced. Therefore, if any part of this Agreement shall be held unenforceable or invalid, it is the intent of the parties that such provision shall not be wholly invalid but shall be deemed to be the maximum restriction for time, territory, and restriction in activities, which a court of competent jurisdiction deems reasonable and enforceable in any jurisdiction in which such court is convened. If any part, provision or paragraph of this Agreement shall be held unenforceable or invalid, the remaining part, provision or paragraph shall continue to be valid and enforceable as though the invalid portions were not a part thereof.

(e) Red Canary is an independent contractor and shall not be deemed an employee or agent of Client. This Agreement, including all exhibits and any SOWs, contains the complete agreement between the parties relating to the Services. Sections 5 through 10 shall survive termination of this Agreement and any SOW.

(f) The Agreement shall be governed and construed in accordance with the laws of the State of California without regard to the application of conflict of laws or principles. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

(g) Red Canary shall not be responsible for any failure to perform due to unforeseen circumstances or to causes beyond such party's reasonable control, including but not limited to acts of God, changes in governmental laws, rules, taxes, regulations or orders, war, terrorist acts, insurrection, riot, embargoes, supplier stoppages or delays, acts of civil or military authorities, fire, floods, accidents, strikes, or shortages of transportation, facilities, fuel, energy, labor or materials.

(h) This Agreement may be executed in several counterparts, all of which taken together shall constitute one single Agreement between the parties. This Agreement may be executed by digital or scanned signature(s).

## STATEMENT OF WORK (SOW)

All Services performed by Red Canary in accordance with this Statement of Work shall be performed in accordance with the End User Security Platform Agreement ("Agreement"), the terms of which are incorporated herein by reference.

### **A. Managed Threat Detection Services and Threat Alerts Description:**

1. Red Canary will provide, as appropriate, Threat Alerts. "Threat Alerts" means analyst-vetted alerts on malicious activity detected by Red Canary on Client endpoints. Each Threat Alert will include information for Client or Client's partners describing the background of the threat related to the alert. Threat Alerts will be sent to Client technical staff as configured in the Red Canary Portal. These Threat Alerts will contain information that is known to Red Canary about the threat at the time, which usually includes but is not limited to:

- Summary of the detected threat.
- Name of affected endpoint and user.
- Artifacts such as file names, Internet Protocol (IP) addresses, domain names and registry keys that support both Client remediation efforts as well as identification of similar threats.

2. Access to Red Canary portal ("Portal") through which the Client can view data and alerts. Service Level: 24x7x365

3. Investigation of data to with respect to Threat Alerts. Service Level of Security Analyst review: 24x7x365 with analyst review hours of 08:00 to 18:00 Eastern US, Monday through Sunday and 18:00 to 02:00 Eastern US, Monday through Thursday, and escalation to on-call analyst support if Red Canary identifies potentially threatening activity outside of analyst review hours that Red Canary's modeling predicts is malicious.

Third Party Software (license included in this SOW): VMware Carbon Black Enterprise Response ("Endpoint Collection Software", licensed hereunder for use by Red Canary per the terms and conditions of the EULA at <https://redcanary.com/license-agreements/>)

### **B. Client Responsibilities:**

The client will be responsible for the following tasks during the course of using the Red Canary service:

- Installing Endpoint Collection Software on client systems
- Performing remediation and incident response actions in response to Threat Alerts.
- Obtaining all required authorizations to perform the Managed Threat Detection Services and any data or information required thereby. Client shall obtain consents and authorizes for Red Canary and its employees and agents to gain access to and retrieve Technical Data and analyze Threat Alerts and perform Managed Threat Detection Services. In the course of accessing, obtaining and otherwise using the Managed Threat Detection Services and Threat Alerts, Client shall have sole responsibility for the accuracy, quality, integrity,

authorization for use hereunder, and intellectual property ownership or right to use and transferability to Red Canary of Technical Data.

**C. Pricing:**

Term: The term of this SOW is effective during the Term of the SOW that incorporates this Agreement and Statement of Work.

Number of monitored Endpoints (minimum): Specified in the SOW that incorporates this Agreement and Statement of Work

True-ups: Specified in the SOW that incorporates this Agreement and Statement of Work

Payment Terms: Specified in the SOW that incorporates this Agreement and Statement of Work

**Exhibit B:****VMWARE END USER LICENSE AGREEMENT**

**PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.**

**IMPORTANT-READ CAREFULLY:** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT (“EULA”). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

**EVALUATION LICENSE.** If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided “AS-IS” without indemnification, support or warranty of any kind, expressed or implied.

**1. DEFINITIONS.**

- 1.1.** “**Affiliate**” means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls that party, and here “control” means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of that entity.
- 1.2.** “**Documentation**” means that documentation that is generally provided to You by VMware with the Software, as revised by VMware from time to time, and which may include end user manuals, operation instructions, installation guides, release notes, and on-line help files regarding the use of the Software.
- 1.3.** “**Guest Operating Systems**” means instances of third-party operating systems licensed by You, installed in a Virtual Machine and run using the Software.
- 1.4.** “**Intellectual Property Rights**” means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.
- 1.5.** “**License**” means a license granted under Section 2.1 (General License Grant).
- 1.6.** “**License Key**” means a serial number that enables You to activate and use the Software.
- 1.7.** “**License Term**” means the duration of a License as specified in the Order.
- 1.8.** “**License Type**” means the type of License applicable to the Software, as more fully described in the Order.
- 1.9.** “**Open Source Software**” or “**OSS**” means software components embedded in the Software and provided under separate license terms, which can be found either in the open\_source\_licenses.txt file (or similar file) provided within the Software or at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html).
- 1.10.** “**Order**” means a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this EULA and is accepted by VMware as set forth in Section 4 (Order).
- 1.11.** “**Product Guide**” means the current version of the VMware Product Guide at the time of Your Order, copies of which are found at [www.vmware.com/download/eula](http://www.vmware.com/download/eula).
- 1.12.** “**Support Services Terms**” means VMware’s then-current support policies, copies of which are posted at [www.vmware.com/support/policies](http://www.vmware.com/support/policies).
- 1.13.** “**Software**” means the VMware Tools and the VMware computer programs listed on VMware’s commercial price list to which You acquire a license under an Order, together with any software code relating to the foregoing that is provided to You pursuant to a support and subscription service contract and that is not subject to a separate license agreement.
- 1.14.** “**Territory**” means the country or countries in which You have been invoiced; provided, however, that if You have been invoiced within any of the European Economic Area member states, You may deploy the corresponding Software throughout the European Economic Area.
- 1.15.** “**Third Party Agent**” means a third party delivering information technology services to You pursuant to a written contract with You. **1.16.**

“**Virtual Machine**” means a software container that can run its own operating system and execute applications like a physical machine.

**1.17. "VMware"** means VMware, Inc., a Delaware corporation, if You are purchasing Licenses or services for use in the United States and VMware International Unlimited Company, a company organized and existing under the laws of Ireland, for all other purchases.

**1.18. "VMware Tools"** means the suite of utilities and drivers, Licensed by VMware under the "VMware Tools" name, that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine.

## **2. LICENSE GRANT.**

**2.1. General License Grant.** VMware grants to You a non-exclusive, non-transferable (except as set forth in Section 12.1 (Transfers; Assignment)) license to use the Software and the Documentation during the period of the license and within the Territory, solely for Your internal business operations, and subject to the provisions of the Product Guide. Unless otherwise indicated in the Order, licenses granted to You will be perpetual, will be for use of object code only, and will commence on either delivery of the physical media or the date You are notified of availability for electronic download.

**2.2. Third Party Agents.** Under the License granted to You in Section 2.1 (General License Grant) above, You may permit Your Third Party Agents to access, use and/or operate the Software on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this EULA and any breach of this EULA by a Third Party Agent shall be deemed to be a breach by You.

**2.3. Copying Permitted.** You may copy the Software and Documentation as necessary to install and run the quantity of copies licensed, but otherwise for archival purposes only.

**2.4. Benchmarking.** You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or otherwise distribute the results of such studies to third parties as follows: (a) if with respect to VMware's Workstation or Fusion products, only if You provide a copy of Your study to [benchmark@vmware.com](mailto:benchmark@vmware.com) prior to distribution; (b) if with respect to any other Software, only if VMware has reviewed and approved of the methodology, assumptions and other parameters of the study (please contact VMware at [benchmark@vmware.com](mailto:benchmark@vmware.com) to request such review and approval) prior to such publication and distribution.

**2.5. VMware Tools.** You may distribute the VMware Tools to third parties solely when installed in a Guest Operating System within a Virtual Machine. You are liable for compliance by those third parties with the terms and conditions of this EULA.

**2.6. Open Source Software.** Notwithstanding anything herein to the contrary, Open Source Software is licensed to You under such OSS's own applicable license terms, which can be found in the open\_source\_licenses.txt file, the Documentation or as applicable, the corresponding source files for the Software available at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html). These OSS license terms are consistent with the license granted in Section 2 (License Grant), and may contain additional rights benefiting You. The OSS license terms shall take precedence over this EULA to the extent that this EULA imposes greater restrictions on You than the applicable OSS license terms. To the extent the license for any Open Source Software requires VMware to make available to You the corresponding source code and/or modifications (the "Source Files"), You may obtain a copy of the applicable Source Files from VMware's website at [www.vmware.com/download/open\\_source.html](http://www.vmware.com/download/open_source.html) or by sending a written request, with Your name and address to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date You acquired this Software.

## **3. RESTRICTIONS; OWNERSHIP.**

**3.1. License Restrictions.** Without VMware's prior written consent, You must not, and must not allow any third party to: (a) use Software in an application services provider, service bureau, or similar capacity for third parties, except that You may use the Software to deliver hosted services to Your Affiliates; (b) disclose to any third party the results of any benchmarking testing or comparative or competitive analyses of VMware's Software done by or on behalf of You, except as specified in Section 2.4 (Benchmarking); (c) make available Software in any form to anyone other than Your employees or contractors reasonably acceptable to VMware and require access to use Software on behalf of You in a matter permitted by this EULA, except as specified in Section 2.2 (Third Party Agents); (d) transfer or sublicense Software or Documentation to an Affiliate or any third party, except as expressly permitted in Section 12.1 (Transfers; Assignment); (e) use Software in conflict with the terms and restrictions of the Software's licensing model and other requirements specified in Product Guide and/or VMware quote; (f) except to the extent permitted by applicable mandatory law, modify, translate, enhance, or create derivative works from the Software, or reverse engineer, decompile, or otherwise attempt to derive source code from the Software, except as specified in Section 3.2 (Decompilation); (g) remove any copyright or other proprietary notices on or in any copies of Software; or (h) violate or circumvent any technological restrictions within the Software or specified in this EULA, such as via software or services.

**3.2. Decompilation.** Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the Territory give You the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, You must first request such information from VMware, provide all reasonably requested information to allow VMware to assess Your claim, and VMware may, in its discretion, either provide such interoperability information to You, impose reasonable conditions, including a reasonable fee, on such use of the Software, or offer to provide alternatives to ensure that VMware's proprietary rights in the Software are protected and to reduce any adverse impact on VMware's proprietary rights.

**3.3. Ownership.** The Software and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Software and Documentation shall be limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Software or any related Intellectual Property Rights are implied. You are not authorized to use (and shall not permit any third party to use) the Software, Documentation or any portion thereof except as expressly authorized by this



EULA or the applicable Order. VMware reserves all rights not expressly granted to You. VMware does not transfer any ownership rights in any Software.

- 3.4. Guest Operating Systems.** Certain Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that You are responsible for obtaining and complying with any licenses necessary to operate any such third-party software.
- 4. ORDER.** Your Order is subject to this EULA. No Orders are binding on VMware until accepted by VMware. Orders for Software are deemed to be accepted upon VMware's delivery of the Software included in such Order. Orders issued to VMware do not have to be signed to be valid and enforceable.
- 5. RECORDS AND AUDIT.** During the License Term for Software and for two (2) years after its expiration or termination, You will maintain accurate records of Your use of the Software sufficient to show compliance with the terms of this EULA. During this period, VMware will have the right to audit Your use of the Software to confirm compliance with the terms of this EULA. That audit is subject to reasonable notice by VMware and will not unreasonably interfere with Your business activities. VMware may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. You will reasonably cooperate with VMware and any third party auditor and will, without prejudice to other rights of VMware, address any non-compliance identified by the audit by promptly paying additional fees. You will promptly reimburse VMware for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the Software fees payable by You for the period audited, or that You have materially failed to maintain accurate records of Software use.
- 6. SUPPORT AND SUBSCRIPTION SERVICES.** Except as expressly specified in the Product Guide, VMware does not provide any support or subscription services for the Software under this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software developed by VMware unless you separately purchase VMware support or subscription services. These support or subscription services are subject to the Support Services Terms.
- 7. WARRANTIES.**
- 7.1. Software Warranty, Duration and Remedy.** VMware warrants to You that the Software will, for a period of ninety (90) days following notice of availability for electronic download or delivery ("**Warranty Period**"), substantially conform to the applicable Documentation, provided that the Software: (a) has been properly installed and used at all times in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than VMware or its authorized representative. VMware will, at its own expense and as its sole obligation and Your exclusive remedy for any breach of this warranty, either replace that Software or correct any reproducible error in that Software reported to VMware by You in writing during the Warranty Period. If VMware determines that it is unable to correct the error or replace the Software, VMware will refund to You the amount paid by You for that Software, in which case the License for that Software will terminate.
- 7.2. Software Disclaimer of Warranty.** OTHER THAN THE WARRANTY ABOVE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES UNDER THIS EULA, AND DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING OR PERFORMANCE, OR USAGE OF TRADE. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT IT WILL MEET YOUR REQUIREMENTS.
- 8. INTELLECTUAL PROPERTY INDEMNIFICATION.**
- 8.1. Defense and Indemnification.** Subject to the remainder of this Section 8 (Intellectual Property Indemnification), VMware shall defend You against any third party claim that the Software infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to the extent that such countries are part of the Territory for the License ("**Infringement Claim**") and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement. The foregoing obligations are applicable only if You: (i) promptly notify VMware in writing of the Infringement Claim; (ii) allow VMware sole control over the defense for the claim, any settlement negotiations and any related action challenging the validity of the allegedly infringed patent, trademark, or copyright; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.
- 8.2. Remedies.** If the alleged infringing Software become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense, do one of the following: (a) procure the rights necessary for You to make continued use of the affected Software; (b) replace or modify the affected Software to make it non-infringing; or (c) terminate the License to the affected Software and discontinue the related support services, and, upon Your certified deletion of the affected

Software, refund: (i) the fees paid by You for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date such Software was delivered; and (ii) any pre-paid service fee attributable to related support services to be delivered after the date such service is stopped. Nothing in this Section 8.2 (Remedies) shall limit VMware's obligation under Section 8.1 (Defense and Indemnification) to defend and indemnify You, provided that You replace the allegedly infringing Software upon VMware's making alternate Software available to You and/or You discontinue using the allegedly infringing Software upon receiving VMware's notice terminating the affected License.

- 8.3. Exclusions.** Notwithstanding the foregoing, VMware will have no obligation under this Section 8 (Intellectual Property Indemnification) or otherwise with respect to any claim based on: (a) a combination of Software with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer VMware version would have avoided the infringement; (d) any modification to the Software made without VMware's express written approval; (e) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into Software listed on VMware's commercial price list; or (f) any Software provided on a no charge, beta or evaluation basis. THIS SECTION 8 (INTELLECTUAL PROPERTY INDEMNIFICATION) STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

## **9. LIMITATION OF LIABILITY.**

- 9.1. Limitation of Liability.** TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS EULA WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE GREATER OF THE LICENSE FEES YOU PAID FOR THE SOFTWARE GIVING RISE TO THE CLAIM OR \$5000. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

- 9.2. Further Limitations.** VMware's licensors shall have no liability of any kind under this EULA and VMware's liability with respect to any third party software embedded in the Software shall be subject to Section 9.1 (Limitation of Liability). You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises.

## **10. TERMINATION.**

- 10.1. EULA Term.** The term of this EULA begins on the notice of availability for electronic download or delivery of the Software and continues until this EULA is terminated in accordance with this Section 10.

- 10.2. Termination for Breach.** VMware may terminate this EULA effective immediately upon written notice to You if: (a) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; or (b) You breach any other provision of this EULA and fail to cure within thirty (30) days after receipt of VMware's written notice thereof.

- 10.3. Termination for Insolvency.** VMware may terminate this EULA effective immediately upon written notice to You if You: (a) terminate or suspend your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

- 10.4. Effect of Termination.** Upon VMware's termination of this EULA: (a) all Licensed rights to all Software granted to You under this EULA will immediately cease; and (b) You must cease all use of all Software, and return or certify destruction of all Software and License Keys (including copies) to VMware, and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Any provision will survive any termination or expiration if by its nature and context it is intended to survive, including Sections 1 (Definitions), 2.6 (Open Source Software), 3 (Restrictions; Ownership), 5 (Records and Audit), 7.2 (Software Disclaimer of Warranty), 9 (Limitation of Liability), 10 (Termination), 11 (Confidential Information) and 12 (General).

## **11. CONFIDENTIAL INFORMATION.**

- 11.1. Definition. “Confidential Information”** means information or materials provided by one party (“**Discloser**”) to the other party (“**Recipient**”) which are in tangible form and labelled “confidential” or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding VMware’s pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software.
- 11.2. Protection.** Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this EULA; or (b) in connection with the parties’ ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by this EULA, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of this EULA and who are under a duty of confidentiality no less restrictive than Recipient’s duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.
- 11.3. Exceptions.** Recipient’s obligations under Section 11.2 (Protection) with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser’s Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser’s request and expense, in any lawful action to contest or limit the scope of such required disclosure.
- 11.4. Data Privacy.** You agree that VMware may process technical and related information about Your use of the Software which may include internet protocol address, hardware identification, operating system, application software, peripheral hardware, and non-personally identifiable Software usage statistics to facilitate the provisioning of updates, support, invoicing or online services and may transfer such information to other companies in the VMware worldwide group of companies from time to time. To the extent that this information constitutes personal data, VMware shall be the controller of such personal data. To the extent that it acts as a controller, each party shall comply at all times with its obligations under applicable data protection legislation.

## **12. GENERAL.**

- 12.1. Transfers; Assignment.** Except to the extent transfer may not legally be restricted or as permitted by VMware’s transfer and assignment policies, in all cases following the process set forth at [www.vmware.com/support/policies/licensingpolicies.html](http://www.vmware.com/support/policies/licensingpolicies.html), You will not assign this EULA, any Order, or any right or obligation herein or delegate any performance without VMware’s prior written consent, which consent will not be unreasonably withheld. Any other attempted assignment or transfer by You will be void. VMware may use its Affiliates or other sufficiently qualified subcontractors to provide services to You, provided that VMware remains responsible to You for the performance of the services.
- 12.2. Notices.** Any notice delivered by VMware to You under this EULA will be delivered via mail, email or fax.
- 12.3. Waiver.** Failure to enforce a provision of this EULA will not constitute a waiver.
- 12.4. Severability.** If any part of this EULA is held unenforceable, the validity of all remaining parts will not be affected.
- 12.5. Compliance with Laws; Export Control; Government Regulations.** Each party shall comply with all laws applicable to the actions contemplated by this EULA. You acknowledge that the Software is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and accompanying documentation are deemed to be “commercial computer software” and “commercial computer software documentation”, respectively, pursuant to DFARS Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and documentation by or for the U.S. Government shall be governed solely by the terms and conditions of this EULA.
- 12.6. Construction.** The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word ‘including’ means “including but not limited to”.

- 12.7. Governing Law.** This EULA is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), and the federal laws of the United States. To the extent permitted by law, the state and federal courts located in Santa Clara County, California will be the exclusive jurisdiction for disputes arising out of or in connection with this EULA. The U.N. Convention on Contracts for the International Sale of Goods does not apply.
- 12.8. Third Party Rights.** Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.
- 12.9. Order of Precedence.** In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following order of precedence shall apply unless otherwise set forth in an enterprise license agreement: (a) the Product Guide, (b) this EULA and (c) the Order. With respect to any inconsistency between this EULA and an Order, the terms of this EULA shall supersede and control over any conflicting or additional terms and conditions of any purchase order, acknowledgement or confirmation or other document issued by You.
- 12.10. Entire Agreement.** This EULA, including accepted Orders and any amendments hereto, and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This EULA may be amended only in writing signed by authorized representatives of both parties.
- 12.11. Contact Information.** Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.



**CONFIDENTIAL**

Rev. 02/17



**CONFIDENTIAL**

February 8, 2019

John Matis  
County of Santa Barbara  
105 East Anapamu Street  
Santa Barbara 93101

Dear Mr. Matis:

We are pleased to confirm the engagement of Kroll Cyber Security, LLC ("Kroll") by the County of Santa Barbara ("Client", and together with Kroll, the "Parties") pursuant to this letter of engagement and the attached Statement of Work ("SOW") (together, the "Agreement").

1. Kroll Services

On behalf of Client, you have engaged Kroll to perform certain services as set forth in the attached SOW (the "Assignment"). In the event Client requests Kroll to expand the scope of the Assignment or undertake related assignments ("Additional Assignments"), each such Additional Assignment will be set forth in a supplementary writing signed by both Parties that references this Agreement and stipulates the fee for the Additional Assignment. Unless otherwise agreed herein, in the event Kroll is requested to (i) provide testimony, (ii) serve as a witness, (iii) update any report, deliverable or other information provided hereunder (the "Kroll Report(s)") for any events or circumstances occurring subsequent to the initial delivery date of the Kroll Report, or (iv) furnish additional services, such additional services will be agreed in a supplementary writing signed by Kroll and Client.

Kroll shall deliver its services in accordance with Client's instructions. However, if instructed by Client in writing, Kroll will perform the Assignment under the direction of Client's counsel. Kroll understands Client and/or such counsel may provide Kroll with certain information and materials developed in anticipation of litigation that may be protected by the attorney-client privilege and/or the work product doctrine. Kroll agrees to treat such materials as confidential and subject to privilege.

2. Confidentiality

Kroll agrees to take reasonable measures to maintain the confidentiality of non-public, confidential and/or proprietary information received from Client and which is designated by Client as confidential or that a reasonable person would consider, from the nature of the information and circumstances of disclosure, to be confidential to Client ("Confidential Information").

If any person or entity requests or subpoenas any Kroll Reports or other Assignment-related information or materials within Kroll's custody or control, Kroll will, unless legally prohibited, promptly inform Client of such request or subpoena so that Client may seek from a court of competent jurisdiction a protective order or other appropriate remedy to limit the disclosure. If Kroll is required to respond to the request or subpoena or to provide testimony, Client agrees to compensate Kroll for reasonable costs and expenses incurred (e.g., reimbursement of reasonable attorneys' fees and disbursements), including, without limitation, compensating Kroll (at hourly rates, as applicable) for responding to legal requests or demands for information and preparing for and testifying at deposition, proceedings and/or trials.



3. Indemnity

The Assignment undertaken (and associated fees) do not contemplate Kroll being made party to any legal proceedings, or subject to third-party claims. Accordingly, Client agrees to hold harmless and indemnify Kroll against all claims, damages and costs (including reasonable attorneys' fees and disbursements) arising out of the Assignment, except for such claims, damages and costs resulting from any actions by Kroll constituting gross negligence, fraud, willful misconduct or unlawful conduct or a breach of the terms of this Agreement.

Kroll agrees to hold harmless and indemnify Client against all claims, damages and costs (including reasonable attorney's fees and disbursements) arising out of any Assignment resulting from any actions by Kroll constituting gross negligence, fraud, willful misconduct or unlawful conduct or a breach of the terms of the Agreement.

4. Limitation of Liability

Client agrees, on its own behalf and on behalf of its agents, that Kroll will not be liable for any claims, liabilities or expenses relating to this engagement for an aggregate amount in excess of the fees paid by Client to Kroll pursuant to this engagement, except to the extent such liability is finally judicially determined to have resulted from Kroll's gross negligence, fraud or willful misconduct. However, in no event will either Party be liable for consequential, special, indirect, punitive or exemplary losses, damages or expenses relating to this engagement, including without limitation damages for loss of data, loss of business profits, business interruption, or other pecuniary loss, even if such Party has been advised of the possibility of such damages.

5. Data Protection

To the extent applicable, the Parties shall comply with relevant national, international, state and/or regional data protection legislation or regulations, including with respect to information disclosed in connection with an Assignment which is personal data (as defined under the relevant legislation or regulation).

6. Computer Forensics

Client acknowledges that digital/computer equipment, drives, data and media may be damaged, infected or corrupted prior to forensic analysis being performed hereunder, and Kroll does not assume responsibility or liability for such pre-existing damage or further problems resulting therefrom. Any data, especially data restored from unknown sources, may contain viruses or other malware; therefore, Client assumes responsibility to protect itself with respect to the receipt of data and shall advise its agents and third-party recipients to take similar precautions.

Client represents and warrants that (i) it has the right to be in possession of, or is the owner of, all equipment/data/media furnished to Kroll hereunder, (ii) such equipment/data/media is furnished for a lawful purpose, and (iii) where applicable, Client's collection, possession, processing and transfer of such equipment/data/media is in compliance with any and all applicable laws, regulations and Client policies, including without limitation concerning data privacy and employee consents.

If in the course of the examination of computers, telephones or other electronic devices, or the examination of electronic media, software content or materials in hard copy form, Kroll or an affiliate observes or otherwise encounters what may be considered illegal contraband, such as images the mere possession of which Kroll reasonably believes to be unlawful, Kroll reserves the right to disclose such contraband to law enforcement. In such an event, and to the extent Kroll reasonably believes is permitted by applicable laws, Kroll will notify Client of its intention to disclose the existence and/or content of such contraband to the appropriate authorities.

Client acknowledges that penetration testing services are intended to probe and exploit system weaknesses, which can cause damage to vulnerable systems. Client agrees that Kroll shall not be liable for any such resulting damage and Client is advised to fully backup systems, only use the services on non-production or other systems for which Client accepts the risk of damage, and take other measures it deems appropriate given the volatile nature of penetration testing.



To the extent any expedited information security and/or computer forensics services are requested by Client, including work that must be performed over a weekend or holiday, or on an overtime basis, Kroll reserves the right to charge for such expedited services at 1.5 times its normal hourly rates for the applicable services.

To the extent Kroll is requested to provide any written testimony or reports relating to information security and/or computer forensics services, such additional services will be provided at Kroll's standard applicable hourly rates. However, oral testimony at deposition, a hearing or trial will be provided at 1.5 times such rates.

7. Use of Information

Client shall be permitted to use Kroll Reports solely for its internal business purposes. Client shall maintain Kroll Reports as confidential, and shall not disclose, disseminate, redistribute or otherwise make any Kroll Reports available to any third party, whether in whole or in part, without the express written consent of Kroll; provided, however, that Kroll Reports may be disclosed by Client: i) to its employees, counsel, agents, and representatives (the "Representatives") who are aware of and agree to the confidentiality obligations herein, and Client shall be responsible for the use and disclosure of Kroll Reports by the Representatives as if it were Client's own use and disclosure; ii) to third parties subject to the execution by each third party of a form of release reasonably satisfactory to Kroll; and iii) if required by law or in response to a lawful order or demand of any court of competent jurisdiction, regulator, or regulatory authority, provided, however, that before making such a disclosure, Client will provide Kroll with prompt prior notice of any such disclosure so that Kroll and/or Client may seek a protective order or other appropriate remedy. Client further agrees and represents that any Kroll Reports provided hereunder will not be used for employment purposes, credit evaluation or insurance underwriting purposes, and that the services hereunder are being contracted for, and will only be used in connection with a business, investment or other commercial purpose.

8. Fees and Invoicing

The fees shall be as set forth in the attached SOW. Kroll shall invoice Client on a monthly basis, and each invoice will include the contract number Client assigns (see Agreement form), to the Bill-To address on the Agreement form, following completion of the increments identified in the Statement of Work.

Client agrees to pay Kroll within forty-five (45) days from presentation of the invoice. Any unpaid balances shall accrue interest at the rate of 8% per annum, as measured from forty-five (45) days after the date of each invoice. Client acknowledges its obligation to pay undisputed amounts as set forth above. In the event Client disputes any portion of an invoice, Client will notify Kroll in writing of the disputed charges within forty-five (45) days of the invoice date. Kroll reserves the right to terminate its services at any time if Client fails to pay Kroll's invoices in a timely manner. Client agrees to reimburse Kroll for any costs of collection, including reasonable attorneys' fees.

The fees and charges for the Services do not include applicable federal, foreign, state or local sales, withholding, use, value added, gross income, excise, or ad valorem taxes. Client will be solely responsible for all applicable federal, state, local, and withholding taxes levied or assessed in connection with Kroll's performance of Services, other than income taxes assessed with respect to Kroll's income. Client will not be responsible for paying any taxes on Kroll's behalf, and should Client be required to do so by state, federal, or local taxing agencies, Kroll agrees to promptly reimburse Client for the full value of such taxes paid plus interest and penalty assessed, if any. These taxes include, but are not limited to, the following: FICA (Social Security), unemployment insurance contributions, income tax, disability insurance, and workers' compensation insurance. Notwithstanding the foregoing, if Kroll is using a non-California address or a California P.O. Box address for conducting its business with Client, Kroll will be subject to required nonresident withholding for services that Kroll provides in California for Client, unless Kroll is a government entity or unless Kroll provides Client with a California withholding form that shows Kroll is exempt from withholding.

**CONFIDENTIAL**



9. Conflicts

In connection with its case opening process, Kroll follows procedures designed to identify conflicts of interest.

Client understands and agrees that the engagement by Client of Kroll for a discrete Assignment hereunder does not prevent Kroll or its affiliated companies from providing services to other clients adverse to Client on matters not substantially related to the particular Assignment being performed hereunder, provided, however, Confidential Information obtained while performing the Assignment will continue to be treated as confidential and will not be shared or used in connection with the performance of any other services provided by Kroll or its affiliated companies.

In the ordinary course of business, Kroll companies may be asked by two or more different clients to gather and assess information regarding a common subject -- individual or company. The investigation of a common subject shall not, in and of itself, be deemed to constitute or give rise to a conflict of interest. In this regard, information gathered and/or provided by a Kroll company in one assignment may differ from information gathered and/or provided about the same or similar common subject in another assignment, often as a result of differences in client-defined services, scope and budget.

10. Termination

Either Party may terminate this Agreement on thirty (30) days prior written notice to the other Party or earlier upon mutual written agreement.

In the event of any termination, Kroll will be entitled to payment of any invoices outstanding, as well as payment for any disbursements, fees and/or costs incurred through the date of termination. Provisions of this Agreement which by their nature are intended to survive termination or expiration of this Agreement shall survive expiration or termination of this Agreement.

11. Assignability

Except as otherwise provided herein, neither Party shall assign this Agreement or any individual Party's rights or privileges hereunder without the prior written consent of the other Party, which consent shall not be unreasonably delayed, conditioned or withheld; provided, however, that the applicable Kroll company may assign this Agreement to any company which controls, is controlled by, or is under common control with Kroll, or in the event of a merger, acquisition or sale of all or substantially all of the assets thereof.

12. Governing Law and Dispute Resolution

This Agreement is governed by the laws of the State of California without regard to the law of conflicts. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by the applicable California state and federal courts, in the County of Santa Barbara (if in state court), or in the applicable federal district court for Santa Barbara County, if in federal court. Each Party shall bear its own costs in connection with any proceedings hereunder. Nothing herein shall prevent either Party from seeking injunctive relief (or any other provisional remedy) from any court having jurisdiction over the Parties and the subject matter of the dispute as is necessary to protect either Party's proprietary rights. Each Party, to the fullest extent permitted by law, knowingly, voluntarily, and intentionally waives its right to a trial by jury in any action or other legal proceeding arising out of or relating to the Agreement or the services. The foregoing waiver applies to any action or legal proceeding, whether sounding in contract, tort or otherwise.

13. Insurance

Kroll shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property which may arise from or in connection with Kroll's performance of this Agreement and provide evidence of insurance as follows:

- A. Workers' Compensation Insurance (in accordance with applicable law)
- B. Commercial General Liability (CGL): covering CGL on an "occurrence" basis, including personal & advertising injury, with limits no less than \$1,000,000 per occurrence and \$2,000,000 in the aggregate.
- C. Professional Liability (Errors and Omissions) Insurance appropriate to Kroll's profession, with limit of no less than \$1,000,000 per occurrence or claim, \$2,000,000 aggregate.
- D. Cyber Liability Insurance, with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 aggregate.

Kroll will provide, upon written request, proof of insurance in the form of certificates of insurance. .

14. Amendment, Waiver and Entire Agreement

Any of the terms and conditions herein may be amended or waived only with the written consent of the Parties. This Agreement, including any exhibits and appendices thereto, constitutes the entire agreement of the Parties and supersedes all oral negotiations and prior writings with respect to the subject matter hereof.

15. Severability

If any portion of this Agreement is held to be unenforceable under applicable law, the Parties agree that such provision shall be excluded from this Agreement, the balance of this Agreement shall be interpreted as if such provision were so excluded, and the balance of this Agreement shall be enforceable in accordance with its terms.

\* \* \*

This Agreement shall be effective as of the date on which Kroll first provides services to Client. If this letter is satisfactory, kindly execute and return the enclosed copy.

Very truly yours,

KROLL CYBER SECURITY, LLC

DEVON ACKERMAN

Name:	Devon Ackerman
Title:	Managing Director
Date:	02/08/2019

AGREED TO AND ACCEPTED:

COUNTY OF SANTA BARBARA

Ray Aromatorio, Date: 2019.02.08

Risk Manager 13:39:51 -05'00'

Name:

Title:

Date:

00W0000

State licensing information can be found at: [www.kroll.com/licensing](http://www.kroll.com/licensing)

CONFIDENTIAL



**STATEMENT OF WORK  
FOR  
INFORMATION SECURITY AND COMPUTER FORENSICS SERVICES**

This Statement of Work ("SOW"), dated February 8, 2019 is entered into pursuant to and incorporates herein by reference the letter of engagement entered into as of February 8, 2019 (together with this SOW, the "Agreement"), by and between the County of Santa Barbara ("Client") and Kroll Cyber Security, LLC ("Kroll"). Capitalized terms herein shall have the meaning ascribed in the letter of engagement.

**A. Description of Services**

Description of services; scope of Assignment	Estimated delivery date
<p><b>Phase 1 - Malware Infection</b></p> <ul style="list-style-type: none"> <li>• Forensic analysis to determine and document timeline of events, possible malware infection, data exfiltration methods and account compromise.</li> <li>• If possible from available evidence, determine malware infection vector.</li> <li>• Attempt to identify indicators of compromise and if any sensitive data may have been exposed as a result of any identified compromise.</li> <li>• Preservation and analysis of available network logs to include Firewall/NetFlow, VPN, web proxy, and IDS/IPS to identify relevant anomalies.</li> <li>• Work alongside Client to remediate any potential vulnerabilities.</li> <li>• Provide recommendations regarding containment and remediation of data event based on results of investigation.</li> <li>• If available, automated analysis of the ransomware binary and any related ransomware data.</li> <li>• Verbal presentation of findings and drafting of report as requested by Counsel and Client.</li> </ul> <p><b>Kroll CyberDetectER® Powered by Red Canary</b></p> <ul style="list-style-type: none"> <li>• Enterprise-wide end-point threat monitoring by Kroll and its strategic partner, Red Canary, with CarbonBlack for approximately 30 days and up to 20,000 end points.</li> <li>• Leverage CyberDetectER and Kroll's tools for purposes of monitoring endpoints for signs of malware infections, known Indicators of Compromise ("IOC"), and identification of compromised host(s) or account(s).</li> <li>• Kroll may use CyberDetectER and other remote forensic techniques and tools to gather evidence as necessary to facilitate the investigation, including to determine timeframe and scope of any sensitive data exposure.</li> <li>• Provide Client with actionable leads to resolve current security events.</li> <li>• Locate IOCs beyond those discovered in other investigations.</li> </ul>	TBD

**B. Fee Structure**

Professional Fees for Kroll's services under this SOW will be charged on an hourly basis as follows:

Consulting Services..... \$325/hour\*  
 Travel Time.....50% of Consultant/Engineer hourly rate  
 Media Preservation/Replication..... \$400/media

**CONFIDENTIAL**

Media / Data Storage ..... \$25/media/month

\*Indicates Beazley preferred rates.

Based on the information now available and known to Kroll, we estimate completion of this engagement will cost between \$85,000 and \$145,000, plus travel time, travel expenses, media output, freight and any applicable taxes. However, frequently the full scope of work cannot be known without further investigation, and thus this estimate may be subject to change based on newly-discovered information.

Accepted and agreed:

COUNTY OF SANTA BARBARA

KROLL CYBER SECURITY, LLC

Ray Aromatorio, Date: 2019.02.08  
Risk Manager 13:04:21 -05'00'

Devon Ackerman

Name:

Name: Devon Ackerman

Title:

Title: Managing Director

Date:

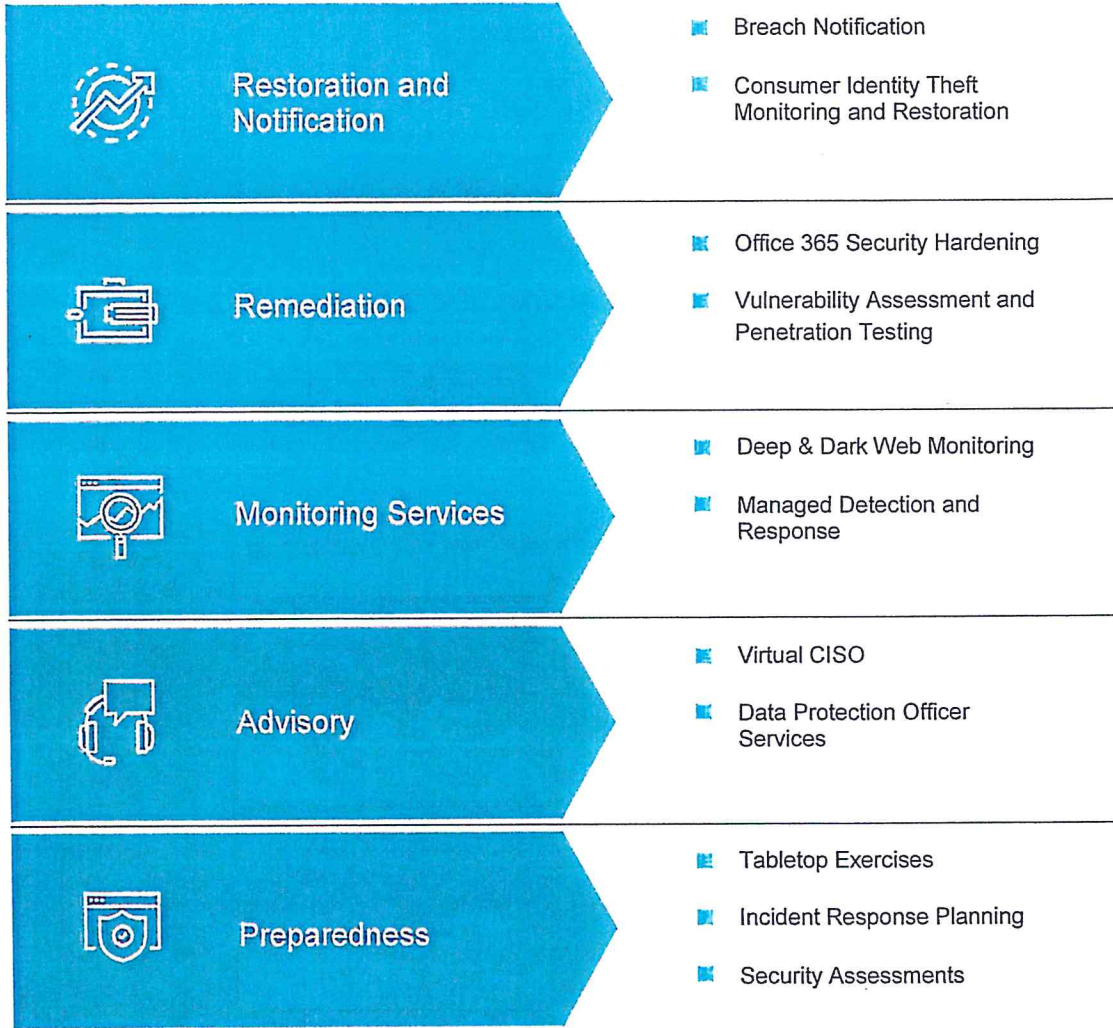
Date: 02/08/2019

State licensing information can be found at [www.kroll.com/licensing](http://www.kroll.com/licensing)



A Division of  
**DUFF & PHELPS**

### Related Cyber Risk Services



### Additional Governance, Risk, Investigation and Diligence Services

- Business Intelligence and Investigations
- Compliance Risk and Diligence
- Disputes
- Compliance Regulatory Consulting
- Legal Management Consulting
- Security Risk Management



## END USER AGREEMENT

This End User Agreement (this "Agreement", also referred to elsewhere as "EULA") is a legal agreement between the entity entering into this Agreement and Carbon Black, Inc., a Delaware corporation ("Carbon Black"). This Agreement governs orders placed by Customer (defined below) to access and use Carbon Black's On-Premise Software, Cloud Services, and/or Cb Services (and any updates and modifications thereto).

BY ISSUING AN ORDER TO CARBON BLACK (OR ITS AUTHORIZED CHANNEL PARTNER) OR OTHERWISE USING OR ACCESSING THE PRODUCTS MADE AVAILABLE BY CARBON BLACK HEREUNDER, CUSTOMER AGREES TO FOLLOW AND BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE AN INDIVIDUAL ("YOU") ACTING ON BEHALF OF CUSTOMER, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO LEGALLY BIND CUSTOMER TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT HAVE AUTHORITY TO BIND CUSTOMER, OR IF YOU OR CUSTOMER DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU AND CUSTOMER MAY NOT USE THE PRODUCTS.

This Agreement consists of, collectively, this base agreement, the terms and conditions detailed in the Product Addendum attached hereto, and the applicable Policies. In the event of any conflict between the terms and conditions set forth in the base Agreement and those set forth in the Product Addendum, the terms and conditions of such Product Addendum shall control.

**DEFINITIONS.** Unless otherwise indicated in this Agreement, the following terms, when capitalized, shall have the following meaning: "**Cb Services**" means, as applicable, Professional Services and Maintenance and Support Services. "**Channel Partner**" means, as applicable, the authorized reseller, distributor, or other authorized third party that markets and sells the Products. "**Cloud Services**" means the Web-based application services made generally available by Carbon Black on a subscription basis and identified on the applicable Order. "**Customer**" means the authorized party executing this Agreement and to the extent specified on any Order hereunder its affiliates (including parents, subsidiaries and other entities controlling or under common control with any of such entities) or its authorized third party service providers; provided however, that, in each case, Customer shall be solely responsible for ensuring compliance with the applicable terms and conditions of the Agreement and Customer shall remain liable for any breach of such terms and conditions by its affiliates and third party service providers. "**Customer Data**" means all Customer-specific and Customer-identifiable data submitted to or collected by the Products by or on behalf of Customer. "**Delivery**" means the date Carbon Black provides access to the keys to Customer for On-Premise Software, or the date Carbon Black provides Customer with log-in access to the Cloud Services. "**Documentation**" means, as applicable, the functional specifications, user guides, "help" pages, installation instructions, descriptions or technical requirements created and provided by Carbon Black generally to its customers, either in documentary form or via Product information



websites. **“Endpoint”** means the computer device(s) on which the Sensor Software (defined below) is installed in accordance with the Documentation, including, but not limited to, laptops, desktops, tablets, point of sale devices and servers. **“Feedback”** means suggestions, enhancement requests, recommendations or other input provided to Carbon Black regarding the Products. **“Fees”** means amounts payable for the Products to which the Customer subscribes under this Agreement. **“Maintenance and Support”** means the maintenance and support services detailed in the Carbon Black Maintenance and Support Policy located on the Policies Page (defined below). **“On-Premise Software”** means: (i) Carbon Black’s proprietary software products as specified on Order(s); and/or (ii) Carbon Black’s proprietary sensor software required for use with certain Products, and which is installed on Customer Endpoints (“Sensor Software”). **“Order”** means an order form issued by Customer for the purchase of the applicable Products, or a Customer or Channel Partner purchase order, as applicable. **“Policies”** means the policies and documents applicable to Carbon Black and the Products, that are located at the following URL: <https://www.carbonblack.com/policies> (“Policies Page”). **“Product Addendum”** means the product addendum attached hereto as Exhibit 1 and incorporated herein by reference, which contains product-specific terms and conditions. **“Product(s)”** means, as applicable, the Cloud Services, On-Premise Software, and Cb Services, as applicable, to which Customer subscribes under this Agreement. **“Professional Services”** means, if applicable, training, implementation or Product-related services specified on the Order(s) or detailed in a Statement of Work. **“Subscription Term”** means the period of time Customer is authorized to use Products, as identified on an Order. **“Statement of Work”** means, if applicable, any written, mutually signed work statement that references this Agreement or an Order and which details activities and terms relating to Professional Services.

#### **ORDERS; FEES; TAXES; PAYMENT TERMS.**

**Orders.** Customer shall place Orders directly with Carbon Black or with a Channel Partner. The terms relating to Fees, taxes and payment terms detailed in this Section 2 apply solely to Orders placed directly with Carbon Black. Corresponding terms for Orders placed with a Channel Partner shall be agreed to by and between Customer and such Channel Partner.

**Fees.** The Fees for Products shall be set forth in the Order. All Fees payable hereunder are non-refundable, except as may be otherwise expressly provided in this Agreement.

**Taxes.** The Fees do not include applicable taxes. Customer will reimburse Carbon Black for all sales, use, excise, and property taxes, value-added tax (VAT), goods and services tax (GST), or other taxes, levies, duties or withholdings Carbon Black is required to collect or remit to applicable tax authorities (except for any taxes based on Carbon Black’s net income). In the event that Customer has to withhold any taxes on payments to Carbon Black, Customer shall gross up the amounts payable to Carbon Black so that following such payment and tax withholding, Carbon Black receives the Fees in full.

**Payment Terms.** The Fees for each Order are payable net thirty (30) calendar days from the date of invoice unless otherwise specified in the applicable Order. Unless otherwise agreed to in



writing by Carbon Black or the Channel Partner, all payments hereunder shall be made in U.S. dollars and are free from all setoffs.

## **PRIVACY AND SECURITY.**

**Privacy and Security.** As further described in Carbon Black's Privacy Policy which is located on the Policies Page, Carbon Black will take reasonable and appropriate technical and organizational measures designed to protect Customer Data against unauthorized access, accidental loss or damage, and unauthorized destruction. The security provided by Carbon Black shall be in accordance with Carbon Black's information security policies included on the Policies Page and good industry practices relating to protection of the type of data typically processed by Carbon Black. Carbon Black's European Union General Data Protection Regulation Policy is located on the Policies Page.

**Data Processing.** The parties acknowledge that Customer Data may contain personal data (as defined under applicable data protection laws) and Carbon Black shall process such data in accordance with the documented instructions of Customer regarding the collection, processing and protection of personal data, and in accordance with this Agreement. Customer hereby consents to Carbon Black's processing of Customer Data, including personal data, for the purposes of carrying out its obligations under this Agreement, and for other lawful purposes in accordance with applicable laws and regulations. Customer is responsible for obtaining any required consents from individual data subjects relating to the use of the Products.

**Disclosure of Personal Data.** Carbon Black will not disclose personal data outside of Carbon Black or its controlled subsidiaries except: (i) as Customer directs; (ii) as described in this Agreement; or (iii) as required by law. The Product may include optional functionality provided by third party processors. In the event Customer chooses to utilize such functionality, Customer will be provided advance notification in the Product of the processing details. Following such notification, Customer may choose to: (a) refrain from utilizing the applicable functionality, in which case such processing will not occur; or (b) proceed with the functionality, in which case Carbon Black will be authorized to process in accordance with the details provided. Carbon Black is responsible for its third party processor compliance with Carbon Black's obligations in the Agreement and shall ensure that such third parties are bound by written agreements that require them to provide at least the level of data protection required of Carbon Black by the Agreement.

**Threat Intelligence Data Collection.** Certain Carbon Black Products may collect data relating to malicious or potentially malicious code, attacks, and activities on Customer Endpoints ("Threat Intelligence Data"). Threat Intelligence Data is collected by Carbon Black for analysis and possible inclusion in a threat intelligence feed utilized by certain Products. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in Customer's systems and other Carbon Black customer systems; and/or (ii) be anonymized and made un-attributable to any particular Customer or individual. Carbon Black may distribute Threat Intelligence Data to its customers at its discretion



as part of its threat intelligence data feed. Customer agrees that Threat Intelligence Data is not Customer Data, and Carbon Black may retain, use, copy, modify, distribute and display the Threat Intelligence Data for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed.

## **RIGHTS; CUSTOMER RESTRICTIONS.**

**Rights in Carbon Black Products.** Carbon Black reserves all rights to the Products and all intellectual property relating thereto not specifically granted in this Agreement. All Products under this Agreement are provided under subscription and not sold, and shall remain the sole and exclusive property of Carbon Black.

**Feedback.** If Customer or any users provide Carbon Black with any Feedback, Carbon Black may use and exploit such Feedback at its discretion without attribution of any kind. All Feedback is provided by Customer without warranties. Customer shall have no obligation to provide Feedback.

**Rights in Customer Data.** As between Customer and Carbon Black, except as otherwise set forth in this Agreement, all right, title and interest in and to the Customer Data is owned exclusively by Customer.

**Customer Restrictions.** Except as may otherwise be explicitly provided for in this Agreement, Customer shall not, and shall take reasonable steps to ensure its Administrative Users (defined below) do not: (i) sell, transfer, rent, copy (other than for archival or backup purposes), reverse engineer (except as allowed by and in compliance with applicable law), reverse compile, modify, tamper with, or create derivative works of the Products, (ii) use the Products to operate a service bureau, outsourcing, sublicensing, or similar business for the benefit of third parties; (iii) use the Products other than in connection with Customer's internal business; (iv) remove any copyright and trademark notices incorporated by Carbon Black in the Products; (v) cause or permit others to access or use the Products in order to build or support, and/or assist a third party in building or supporting, software or services competitive to Carbon Black; (vi) perform or disclose any of the following security testing on the Products (including any Cloud Services environment or associated infrastructure): network discovery, port and service identification, vulnerability scanning, password cracking, remote access testing or penetration testing; or (vii) use the Products to: (a) perform any activity that is unlawful, or that interferes with any use of the Products or the network, systems and/or facilities of Carbon Black or its service providers; (b) store, process, publish or transmit any infringing or unlawful material, or material that constitutes a violation of any party's privacy, intellectual property or other rights; or (c) perform any activity intended to circumvent the security measures of Carbon Black or its service providers. Customer is responsible for all administrative access by its personnel and, if applicable, its service providers ("Administrative Users") through its login credentials, for controlling against unauthorized access, and for maintaining the confidentiality of usernames and passwords. If Customer becomes aware of any breach of this Section 4.4, Customer will notify Carbon Black and remedy the situation immediately, including, if necessary, limiting, suspending or terminating an Administrative User's access to the Products.



## REPRESENTATIONS AND WARRANTIES.

**Mutual Representation and Warranties.** Each party represents and warrants to the other that: (i) it has the legal right and authority to enter into this Agreement and perform its obligations hereunder; and (ii) it will not introduce into the Products any virus, worm, Trojan horse, time bomb, or other malicious or harmful code (excluding, however, any legitimate mechanism to disable operation of the Products after the expiration of a Subscription Term).

**Threat Intelligence Feeds.** The information provided via any threat intelligence feed is provided on an "AS-IS" and "AS-AVAILABLE" basis only.

**Sensor Software.** For Products that utilize Sensor Software, Carbon Black warrants that the Sensor Software will conform in all material respects to the specifications detailed in the Documentation at the time of Delivery and, if Customer is entitled to receive Maintenance and Support Services, any Updates provided for the Sensor Software will be compatible with the then-current Cloud Services or version of On-Premise Software, as applicable.

**Cb Services Limited Warranty.** Carbon Black warrants that the Cb Services will be performed in a professional and workmanlike manner consistent with industry standards for similar types of services. For any breach of the foregoing limited warranty, Customer's exclusive remedy shall be to terminate the applicable Cb Services and receive and refund any prepaid but unused Fees applicable to the non-compliant Cb Services.

**Carbon Black Products.** The warranty for specific Carbon Black Products is detailed in the Product Addendum. The limitation on warranties in Section 5.6 below, the exclusion of certain warranties in Section 5.7 below, and the disclaimer of actions set forth in Section 5.8 below, also apply to any warranties set forth in the Product Addendum.

**LIMITATION ON WARRANTIES.** Carbon Black warranties are for the benefit of Customer only and are void if: (i) the Products are integrated by Customer with third party products, unless integrated in accordance with the applicable Documentation; (ii) the Products are altered by anyone other than Carbon Black or an authorized representative of Carbon Black; (iii) the Products are improperly installed, maintained or accessed by anyone other than Carbon Black or an authorized representative of Carbon Black; (iv) Customer is utilizing a version of the On-Premise Software no longer supported by Carbon Black; or (v) the Products are used in violation of the applicable Documentation or Carbon Black's instructions or this Agreement.

**EXCLUSION OF CERTAIN WARRANTIES.** Except for warranties detailed in the Product Addendum, the foregoing warranties are in lieu of and exclude all other express and implied warranties, including but not limited to, warranties of merchantability, title, fitness for a particular purpose, non-infringement, error free operation or non-intrusion due to hacking or other similar means of unauthorized access. No written or oral representation, made by Carbon Black personnel or otherwise, which is not contained in this Agreement, will be deemed to be a warranty by Carbon Black or give rise to any liability of Carbon Black whatsoever. Customer acknowledges that it is impossible under any available technology for any products to identify and eliminate all malware or potential threats.



**DISCLAIMER OF ACTIONS CAUSED BY AND/OR UNDER THE CONTROL OF THIRD**

**PARTIES.** Carbon Black does not and cannot control the flow of data to or from Carbon Black's network and other portions of the internet, and accordingly Carbon Black disclaims any and all warranties and liabilities resulting from or related to a failure in the performance of internet services provided or controlled by a third party other than any contractor or agent of Carbon Black hereunder.

**LIMITATION OF LIABILITY.**

**NO CONSEQUENTIAL DAMAGES.** Except for in relation to: (i) a breach of Section 9 (Confidentiality); (ii) a party's violation of the other party's intellectual property rights; or (iii) a party's indemnification obligation in this Agreement; notwithstanding any provision of this Agreement to the contrary, in no event shall either party or its suppliers, officers, directors, employees, agents, shareholders, or contractors ("Related Parties") be liable to the other party for consequential, incidental, special, punitive or exemplary damages (including but not limited to lost revenues, profits or data, or costs of business interruptions other economic loss) arising from or in connection with any cause including but not limited to breach of warranty, breach of contract, tort, strict liability, failure of essential purpose or any other economic losses, even if the other party is advised of the possibility of such damages.

**LIMIT ON LIABILITY.** Except for liability arising from: (i) a breach of Section 9 (Confidentiality) below; (ii) a party's violation of the other party's intellectual property rights; (iii) a party's indemnification obligation in this Agreement; or (iv) a party's fraud, willful misconduct or violation of Section 10.9; the maximum cumulative liability of a party and its related parties for any and all claims in connection with this Agreement or the subject matter hereof, including but not limited to claims for breach of warranty, breach of contract, tort, strict liability, failure of essential purpose or otherwise, shall in no circumstance exceed the fees paid to Carbon Black for the applicable Product(s) giving rise to the liability in the twelve (12) month period immediately preceding the applicable claim.

**INTELLECTUAL PROPERTY INFRINGEMENT INDEMNITY.** Carbon Black shall: (i) defend and indemnify Customer and its officers, directors, employees and agents from and against all claims and causes of action arising out of an allegation that the Products (hereinafter the "Indemnified Product[s]") infringe a third party copyright, trademark, patent, or other intellectual property right; and (ii) pay the resulting cost and damages finally awarded against Customer by a court of competent jurisdiction or the amount stated in a written settlement signed by Carbon Black, as long as Customer gives Carbon Black: (a) prompt written notice of such claim or action; (b) the right to control and direct the investigation, preparation, defense, and settlement of the action; and (c) reasonable assistance and information with respect to the claim or action. If a final injunction is obtained against Customer's right to continue using the Indemnified Product or, if in Carbon Black's opinion an Indemnified Product is likely to become the subject of a claim, then Carbon Black may, at its election, either: (1) obtain the right for Customer to continue to use the Indemnified Product; or (2) replace or modify the Indemnified Product so that it no longer infringes but functions in a materially equivalent manner. If Carbon Black determines that neither of these alternatives is



reasonably available, then Carbon Black may terminate this Agreement and refund any prepaid unused Fees applicable to the infringing Indemnified Product. This section shall not apply to infringement or misappropriation claims arising in whole or in part from: (A) designs, specifications or modifications originated or requested by Customer; (B) the combination of the Indemnified Products or any part thereof with other equipment, software or products not supplied by Carbon Black if such infringement or misappropriation would not have occurred but for such combination; or (C) Customer's failure to install an update or upgrade, where same would have avoided such claim. THE FOREGOING STATES CARBON BLACK'S ENTIRE OBLIGATION AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ACTUAL OR POTENTIAL THIRD PARTY INFRINGEMENT CLAIMS OR CAUSES OF ACTION.

#### **TERMINATION.**

**Termination for Cause.** Either party may terminate this Agreement or an individual Order if the other party: (i) fails to cure a material breach of this Agreement or the applicable Order within thirty (30) calendar days after its receipt of written notice regarding such breach; or (ii) files or acquiesces to a bankruptcy or similar petition. Termination of the entire Agreement shall be deemed to include termination of any and all active Orders.

**Effect of Termination.** Upon the effective date of termination of the Agreement or an Order: (i) Carbon Black will immediately cease providing the applicable Cloud Services and/or Cb Services; (ii) Customer will immediately cease use of any On-Premise Software and remove such On-Premise Software from its systems; and (iii) any and all of Customer's current and, in the case of termination for cause by Carbon Black, future payment obligations under this Agreement immediately become due. In the event of termination for cause by Customer, Carbon Black will refund any prepaid, unused Fees pro rata from the date of termination.

#### **CONFIDENTIALITY.**

**Confidential Information.** As used in this Agreement, "Confidential Information" means all information of either party that is not generally known to the public, whether of a technical, business or other nature, that is disclosed by one party to the other party or that is otherwise learned by the recipient in the course of its activities with the disclosing party, and that has been identified as being proprietary and/or confidential or that the recipient reasonably ought to know should be treated as proprietary and/or confidential under the circumstances of disclosure. Confidential Information of Carbon Black also includes the terms, conditions, and pricing of this Agreement, and the results of any benchmarking, testing, or competitive evaluations Customer performs on the Products. Each party shall use reasonable care to hold the other party's Confidential Information in confidence and not disclose such Confidential Information to anyone other than to its personnel, contractors, attorneys, and accountants with a need to know. A recipient shall not reproduce or use such information for any purpose other than as reasonably required to perform pursuant to this Agreement or as reasonably necessary for use of the Products as contemplated by this Agreement. Either party may disclose the existence and nature of the relationship between the parties established hereby, provided it does not disclose any of the specific terms of such relationship.



**Exceptions.** The obligations of either party pursuant to this Section 9 shall not extend to any information that: (i) recipient can demonstrate through written documentation was already known to the recipient prior to its disclosure to the recipient; (ii) was or becomes known or generally available to the public (other than by act of the recipient); (iii) is disclosed or made available in writing to the recipient by a third party having a bona fide right to do so; (iv) is independently developed by recipient without the use of any Confidential Information; or (v) is required to be disclosed by process of law, provided that the recipient shall notify the disclosing party promptly upon any request or demand for such disclosure.

**Injunctive Relief.** The parties acknowledge that any breach of this Section 9 may cause immediate and irreparable injury to the non-breaching party for which monetary damages may be inadequate, and in the event of such breach, the non-breaching party shall be entitled to seek injunctive relief, in addition to all other remedies available to it at law or in equity.

#### **MISCELLANEOUS.**

**Notices.** Any notice under this Agreement must be in writing and sent by certified letter, receipted commercial courier or e-mail transmission (acknowledged in like manner by the intended recipient) to the respective addresses shown on the Order(s), and shall be deemed given on the date received by the recipient, except that Carbon Black may provide notice of changes to Policies, if required, via written announcement on its customer portal, which shall be deemed given on the date of such announcement. Any party may from time to time change such address or individual by giving the other party notice of such change in accordance with this Section.

**Export Control.** Customer acknowledges that any Products and Confidential Information provided under this Agreement may be subject to U.S. export laws and regulations. Customer agrees that it will not use, distribute, transfer, or transmit the Products or Confidential Information in violation of U.S. export regulations. Without limiting the foregoing: (i) each party warrants and represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports; and (ii) Customer shall not permit individuals to access or use the Products in violation of any U.S. or United Nations export embargo, prohibition or restriction.

**Usage.** Upon request, Customer agrees to certify to its compliance with the quantity and usage restrictions set forth in this Agreement and any Order for On-Premise Software, or to allow Carbon Black or its approved designee to inspect Customer's data processing systems and records to verify such compliance. Carbon Black may review Customer's usage of the Cloud Services to determine Customer's compliance with the quantity and usage restrictions of this Agreement and any Order. Carbon Black will promptly notify Customer if Carbon Black (or a Customer certification) determines that Customer's usage of the Products exceeds purchased quantities, and if so, Customer shall promptly pay to Carbon Black additional Fees applicable to such prior over-usage, and either: (i) immediately discontinue any such overuse; or (ii) purchase such additional quantities to cover Customer's actual usage going forward, at Carbon Black's then current charges.



**Applicable Law.** This Agreement shall be governed by the law of the State of New York, U.S.A., excluding: (i) its conflicts of laws principles; (ii) the United Nations Convention on Contracts for the International Sale of Goods; and (iii) the Uniform Computer Information Transactions Act (UCITA) as adopted by any state.

**Assignment.** Except in the event of a merger, acquisition or sale of all or substantially all of a party's assets, neither party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other party (not to be unreasonably withheld). Any assignment in contravention of this provision shall be null and void. All the terms and provisions of this Agreement will be binding upon and inure to the benefit of the parties and their respective successors and permitted assigns.

**Non-Waiver.** The waiver of any breach or default of this Agreement will not constitute a waiver of any subsequent breach or default, and will not act to amend or negate the rights of the waiving party.

**Relationship of the Parties.** Carbon Black is an independent contractor. The provisions of this Agreement shall not be construed to establish any form of partnership, agency or other joint venture of any kind between Customer and Carbon Black, nor to constitute either party as the agent, employee or legal representative of the other.

**Force Majeure.** Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control.

**Compliance with Laws.** Carbon Black will comply with all laws and regulations applicable to it and its provision of the Products. Carbon Black is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Carbon Black does not determine whether Customer Data includes information subject to any specific law or regulation. Customer must comply with all laws and regulations applicable to it and its use and possession of the Products.

**Severability.** Any provision of this Agreement that is unenforceable shall not cause any other remaining provision to be ineffective or invalid.

**Modification of Agreement.** Except as set forth herein, no addition to or modification of this Agreement shall be binding on either of the parties hereto unless reduced to writing and executed by an authorized representatives of each of the parties.

**Modification of Cloud Services and Policies.** Notwithstanding anything to the contrary in this Agreement, from time to time at its sole reasonable discretion Carbon Black may make upgrades, changes and/or improvements to: (i) the Cloud Services, in order to enhance the Cloud Services generally and/or remedy any issues with the Cloud Services; or (ii) the Policies, in order to address changes to Products or applicable laws or regulations. Notwithstanding the foregoing, except as is required as a result of changes to applicable laws or regulations, Carbon Black will not modify any Cloud Services or Policies in any way designed to: (a) materially degrade the Cloud Services or Policies; or (b) add additional material obligations for Customer.



**Survival.** All provisions of this Agreement that reasonably may be interpreted or construed as surviving termination of this Agreement shall survive the termination of this Agreement.

**Counterparts; Electronic Signature.** This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and all of which taken together shall constitute one and the same instrument. The parties hereby consent to electronic signature as a binding form of execution of this Agreement and related documents.

**Evaluation and Beta Use Terms and Conditions.** Carbon Black may, at its sole discretion and upon mutual written agreement of the parties, grant Customer the right to use the Products for evaluation or beta testing purposes in accordance with the terms of this Agreement.

Notwithstanding anything to the contrary anywhere in this Agreement, the following terms and conditions shall also apply to (and supersede any conflicting terms in the event of a conflict) Customer's evaluation or beta use of the Products: (i) the Products may be used solely for Customer's internal assessment of the capabilities, performance, and suitability of the Products and in no event for production use; (ii) the Products ARE PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, and Carbon Black disclaims all warranties, support obligations, and other liabilities and obligations for Customer's evaluation or beta use of the Products; and (iii) Customer agrees to defend, indemnify and hold harmless Carbon Black from all claims, damages, and losses, howsoever arising and whether direct, indirect, or consequential, including all legal fees and expenses, arising from Customer's evaluation or beta use of the Products.

**Ultrahazardous Activities.** The Products are not designed or intended for use in any hazardous environment requiring fail-safe performance or operation in which the failure of the Products could lead to death, personal injury, or property damage, including without limitation the design or operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems (or the on-line control of equipment in any such environment.) Customer hereby agrees that it will not use the Products in such environments.

**Entire Agreement; English Language Controls.** This Agreement comprises all the terms, conditions and agreements of the parties hereto with respect to the subject matter hereof and supersedes all other negotiations, proposals, or agreements of any nature whatsoever, unless otherwise specifically provided. Any contradictory or pre-printed terms and conditions that Customer may provide in connection with an Order shall be deemed null and void. This Agreement and all Orders, notices, or other documents given or to be given under this Agreement will be written in the English language only.

## **EXHIBIT 1: PRODUCT ADDENDUM**

### **Part 1: Additional Terms and Conditions Specific to Cloud Services**

**Cloud Services.** This Product Addendum Part 1 applies for all Carbon Black Cloud Services.

**Grant of Rights for Cloud Services.** During the applicable Subscription Term, Carbon Black will make the then-current version of the Cloud Services available to Customer, and hereby grants



Customer the right to access and use the Cloud Services for the number of Endpoints identified in an Order. For clarity, the Cloud Services may include and require the use of the Sensor Software. **Cloud Services Warranty.** Carbon Black warrants that the Cloud Services will conform in all material respects to the specifications detailed in the applicable Documentation during the Subscription Term. If the Cloud Services do not comply with this warranty, Carbon Black will (at its option), as Customer's sole and exclusive remedy: (i) within a reasonable period of time repair, replace, or modify the Cloud Services so that they comply with this warranty, or (ii) terminate this Agreement or applicable Order and refund any prepaid but unused Fees applicable to the non-compliant Cloud Services.

**Service Level Warranty.** Carbon Black warrants that the Cloud Services will be available in accordance with the Carbon Black Service Level Agreement ("SLA"), which is available on the Policies Page and incorporated herein by reference. The SLA states Customer's sole and exclusive remedy for any breach of this Service Level Warranty.

**Suspension.** In the event of a breach or suspected breach of any of the restrictions in Section 4.4 of the body of the Agreement, Carbon Black reserves the right to suspend Customer's Cloud Services if reasonably necessary to prevent harm to Carbon Black, Customer, other customers, and/or Carbon Black's partners, vendors and suppliers, with such notice and for such period as may be reasonable in the context of the prospective harm.

**CB Defense for VMware.** In the event Customer purchases a subscription to Cb Defense for VMware, this Product Addendum Part 1 applies in its entirety, and: (i) Customer hereby consents to the transfer of Customer Data, including, if applicable, personal data, by and between Carbon Black and VMware as necessary, for the purposes of processing such data in accordance with this Agreement; and (ii) references to "Endpoints" shall be deemed references to "CPUs" as applicable.

## **Part 2: Additional Terms and Conditions Specific to On-Premise Software**

**On-Premise Software.** This Product Addendum Part 2 applies for all Carbon Black On-Premise Software.

**Grant of Rights for On-Premise Software.** Customer is granted for the Subscription Term specified in the applicable Order(s) a worldwide, non-exclusive, non-assignable (except pursuant to a permitted assignee under the Agreement), non-transferable right to: (i) install and use (in accordance with the Documentation and for internal business purposes only) the applicable On-Premise Software (including Sensor Software) on the number of servers and/or Endpoints specified in the applicable Order(s); and (ii) copy and run the applicable On-Premise Software for testing and disaster recovery purposes.

**On-Premise Software Warranty.** Carbon Black warrants that for a period of ninety (90) days from Delivery, the On-Premise Software will conform in all material respects to the specifications detailed in the Documentation. If the On-Premise Software does not comply with this warranty, Carbon Black will (at its option), as Customer's sole and exclusive remedy: (i) within a reasonable period of time repair, replace, or modify the applicable On-Premise Software so that it complies with this

warranty, or (ii) terminate this Agreement or applicable Order and refund any prepaid but unused Fees applicable to the non-compliant On-Premise Software Product (if any).

**Updates and Upgrades.** Carbon Black may release patches, bug fixes, updates, upgrades, maintenance and/or service packs (“Updates”) for the On-Premise Software from time to time, which may be necessary to ensure the proper function and security of the Products. Carbon Black is not responsible for performance, security, warranty breaches, support or issues encountered in connection with the Products that result from Customer’s failure to accept and apply Updates within a reasonable timeframe.



## END USER SECURITY PLATFORM AGREEMENT

This End User **Security Platform Agreement** (this "Agreement") is entered into this date of 2018 (hereinafter referred to as the Effective Date of the agreement), by and between Red Canary, Inc., a Delaware corporation with offices at 1750 15th Street #400, Denver, CO, 80202 (hereinafter referred to as "Red Canary") and client as identified in the Statement of Work (SOW) that incorporates this Agreement, (hereinafter referred to as "Client") (hereinafter individually referred to as "Party" and collectively referred to as "Parties").

**1. Term.** The term ("Term") of this Agreement will begin on the Effective Date and continue until the later of termination as provided in Section 6 herein.

**2. Statements of Work.** During the Term, Red Canary and Client may agree upon statements of work hereunder (each, a "SOW") defining the Managed Threat Detection Services ("Managed Threat Detection Services" or "Services") through which, Red Canary will provide as appropriate, threat alerts as defined in the SOW ("Threat Alerts"), Red Canary's compensation, the period of performance during which the Services will be provided (if applicable), and any additional terms and conditions. Each SOW shall be incorporated into and governed by this Agreement. Any changes to a SOW shall be agreed upon in writing by the parties. The parties agree that this Agreement and the applicable SOW(s) for Services shall govern and supersede any terms and conditions stated on any purchase order submitted by Client for such Services. In the event of any conflict between this Agreement and an SOW, the Agreement will control.

**3. Services.** Client hereby agrees that Red Canary may collect and use but not distribute, technical information about Client's devices, files, binaries, user activity, networks, systems, and software, and any other data contained therein ("Technical Data") for the purpose of providing Managed Threat Detection Services to Red Canary's customer base. Aggregated and anonymized Technical Data may be used for other purposes or distributed to third parties. Red Canary reserves the right to establish or modify its general practices and limits relating to storage of such data, and/or to delete or destroy any or all such data periodically.

**4. Intentionally Omitted.**

**5. Confidentiality/Ownership.**

(a). To the extent that confidential and proprietary information of each party including without limitation Technical Data ("Confidential Information") is exchanged and received in connection with the Services, each party agrees not to use the other party's Confidential Information except in the performance of, or as authorized by, this Agreement, and not to disclose, sell, license, distribute or otherwise make available such information to third parties. "Confidential Information" does not include: (i) information that was publicly available at the time of disclosure or that subsequently becomes publicly available other than by a breach of this provision, (ii) information previously known by or developed by the receiving party independent of the Confidential Information or independent of Red Canary Information obtained from any client or (iii) information that the receiving party rightfully obtains without restrictions on use and disclosure except where such is obtained from the client. Any Technical Data shall remain the confidential information and exclusive property of Client.

(b) Any Managed Threat Detection Services, Threat Alerts and information used to perform the Services, or included in any Threat Alert or Services, and any derivative works thereof, including but not limited to monitoring and analysis methodologies and tools, software, appliances, methodologies, code, customer, sender and recipient commercial and personal information, templates, service bureaus, tools, policies, records, working papers,



knowledge, data or other intellectual property, written or otherwise and data, testing, analysis, evaluations and conclusions resulting from the disclosures herein shall remain the exclusive property of Red Canary.

**6. Termination.** The term of this Agreement expires on the expiration of the SOW incorporating this Agreement.

**7. Limited Warranty.**

OTHER THAN THE SERVICE DESCRIPTION PROVIDED FOR IN ANY APPLICABLE SOW, RED CANARY MAKES NO WARRANTY TO CLIENT, OR ANY OTHER PARTY, AND HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE THIRD PARTY SOFTWARE, THREAT ALERTS, MANAGED THREAT DETECTION SERVICES OR ANY OTHER SERVICES, OR RESULTS OF USE OR ANALYSIS OF THREAT ALERTS AND TECHNICAL DATA INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, OF QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ABSENCE OF HIDDEN DEFECTS, AND ANY WARRANTY THAT MAY ARISE FROM COURSE OF PERFORMANCE, BY REASON OF USAGE OR TRADE OR COURSE OF DEALING. The Managed Threat Detection Services and Threat Alerts are not fault-tolerant and are not designed, manufactured or intended for hazardous environments requiring fail-safe performance, where any failure of the Threat Alerts could lead directly to significant property or data loss or disclosure, interruption of business, breach of security, death, personal injury, or property damage ("High Risk Activities"). IN NO EVENT DOES RED CANARY WARRANT THAT MANAGED THREAT DETECTION SERVICES, THREAT ALERTS OR THIRD PARTY SOFTWARE WILL OPERATE OR BE USEFUL WITHOUT INTERRUPTION, OR WILL BE FREE OF DEFECTS, OR NOT CAUSE OR RESULT IN A VULNERABILITY TO INTRUSION OR ATTACK OR ANY INTERRUPTION OF BUSINESS OR THAT THE MANAGED THREAT DETECTION SERVICE OR THREAT ALERTS WILL DETECT OR PREVENT ALL BUGS, VIRUSES, INTERRUPTIONS, INTRUSIONS, UNAUTHORIZED ACTIVITY, ERRORS, DATA THEFT OR DESTRUCTION AND DISCLAIM ALL WARRANTIES RELATING THERETO. Client acknowledges and agrees that Managed Threat Detection Services and Threat Alerts does not provide guarantee or warrant of protection, detection or accurate analysis of the Threat Alerts, and that Red Canary shall not be held liable in the event of security breach, attack, unintended release of sensitive information or other such event and that Client has responsibilities referenced in the SOW. Any service level agreements are goals and there is no guarantee or warranty they can be accomplished as no threat detection service is fail safe. As Client's sole remedy and Red Canary's sole obligation hereunder where there is material non-conformity in any Services or Threat Alert, Red Canary shall use good faith efforts to attempt to remedy any such non-conformity.

**8. Indemnification.**

(a) Red Canary hereby agrees to indemnify Client from any loss, damage, cost or expense (including reasonable attorneys' fees) ("Loss") arising from any claim, demand, assessment, action, suit, or proceeding ("Claim") as a result of Red Canary's or its personnel's (a) illegal or fraudulent conduct resulting in the disclosure of any Technical Data not permitted to be disclosed by Red Canary under this Agreement, or (b) violation of the intellectual property rights of a third party; except where such Loss or Claim arises in whole or in part from the Client not being in compliance with the terms of this Agreement or Client's or its personnel's illegal or fraudulent conduct.

(b) Client shall indemnify, defend and hold Red Canary and its employees, directors, shareholders, agents, and consultants harmless against any Loss arising from any Claim resulting from (i) access by Red Canary to Technical Data whether made by any of Client's customers, invitees, employees, agents or end users, (ii) Client's use or benefit of the Third Party Software, or use or reliance on the Managed Threat Detection Services or Threat Alerts, or (iii) any third party action resulting from any intrusions or security breaches except in the event of breach of this Agreement with respect to data that is in Red Canary's possession. In the event that Red Canary or any of its employees, directors, shareholders, agents, or consultants are required to testify in any judicial,



administrative or legislative proceeding with respect to its Services hereunder, Client shall reimburse Red Canary from any and all costs, expenses, and time incurred in that regard.

**9. Limitation of Liability.** In no event shall Red Canary be liable for any incidental, consequential, special, exemplary or indirect damages, loss or interruption of business operations, lost profits, or data loss arising out of this Agreement or the provision by Red Canary or use by Client of the Services or Threat Alerts. Red Canary's total liability under this Agreement shall be limited to the fees paid by Client to Red Canary for the six (6) month period immediately preceding the claim, for the particular SOW upon which the claim is based. Red Canary, licensors and its suppliers will not be responsible for any damages, losses, expenses or costs that Client or any third party incurs or suffers as a result of any loss or theft of Technical Data.

**10. Miscellaneous.**

(a) This Agreement shall be the entire agreement between the parties to the exclusion of all antecedent or present representations, undertakings, agreements or warranties, expressed or implied and annuls, supersedes and replaces any and every other representation, warranty and agreement which may have existed between the parties. This Agreement may be amended only by a written instrument that has been similarly executed by both parties.

(b) The headings of this Agreement are for convenience only. In case of any difficulty in the interpretation of one or more of the headings, the headings shall have no meaning and no effect.

(c) All notices required under the Agreement to be given to a party must be in writing and delivered by hand or sent by registered post or email transmission addressed to the party at its address indicated below or at such other address as may be subsequently notified:

To Red Canary to: 1515 Wynkoop Street #390  
Denver, CO, 80202  
c/o Chris Zook, CFO

Written notices required under the Agreement will be deemed valid if delivered by hand or sent by registered post or email transmission and shall be effective on date of receipt.

(d) It is acknowledged that it is the intent of the parties that the provisions contained in this Agreement should be enforced. Therefore, if any part of this Agreement shall be held unenforceable or invalid, it is the intent of the parties that such provision shall not be wholly invalid but shall be deemed to be the maximum restriction for time, territory, and restriction in activities, which a court of competent jurisdiction deems reasonable and enforceable in any jurisdiction in which such court is convened. If any part, provision or paragraph of this Agreement shall be held unenforceable or invalid, the remaining part, provision or paragraph shall continue to be valid and enforceable as though the invalid portions were not a part thereof.

(e) Red Canary is an independent contractor and shall not be deemed an employee or agent of Client. This Agreement, including all exhibits and any SOWs, contains the complete agreement between the parties relating to the Services. Sections 5 through 10 shall survive termination of this Agreement and any SOW.

(f) The Agreement shall be governed and construed in accordance with the laws of the State of Colorado without regard to the application of conflict of laws or principles. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.



(g) Red Canary shall not be responsible for any failure to perform due to unforeseen circumstances or to causes beyond such party's reasonable control, including but not limited to acts of God, changes in governmental laws, rules, taxes, regulations or orders, war, terrorist acts, insurrection, riot, embargoes, supplier stoppages or delays, acts of civil or military authorities, fire, floods, accidents, strikes, or shortages of transportation, facilities, fuel, energy, labor or materials.

(h) This Agreement may be executed in several counterparts, all of which taken together shall constitute one single Agreement between the parties. This Agreement may be executed by digital or scanned signature(s).

## **STATEMENT OF WORK (SOW)**

All Services performed by Red Canary in accordance with this Statement of Work shall be performed in accordance with the End User Security Platform Agreement (“Agreement”), the terms of which are incorporated herein by reference.

### **A. Managed Threat Detection Services and Threat Alerts Description:**

1. Red Canary will provide, as appropriate, Threat Alerts. “Threat Alerts” means analyst-vetted alerts on malicious activity detected by Red Canary on Client endpoints. Each Threat Alert will include information for Client or Client’s partners describing the background of the threat related to the alert. Threat Alerts will be sent to Client technical staff as configured in the Red Canary Portal. These Threat Alerts will contain information that is known to Red Canary about the threat at the time, which usually includes but is not limited to:

- Summary of the detected threat.
- Name of affected endpoint and user.
- Artifacts such as file names, Internet Protocol (IP) addresses, domain names and registry keys that support both Client remediation efforts as well as identification of similar threats.

2. Access to Red Canary portal (“Portal”) through which the Client can view data and alerts. Service Level: 24x7x365

3. Investigation of data to with respect to Threat Alerts. Service Level of Security Analyst review: 24x7x365 with analyst review hours of 08:00 to 18:00 Eastern US, Monday through Sunday and 18:00 to 02:00 Eastern US, Monday through Thursday, and escalation to on-call analyst support if Red Canary identifies potentially threatening activity outside of analyst review hours that Red Canary's modeling predicts is malicious.

Third Party Software (license included in this SOW): Carbon Black Enterprise Response (“Endpoint Collection Software”, licensed hereunder for use by Red Canary per the terms and conditions of the EULA at <https://www.carbonblack.com/license-agreements/enterprise-response-license-agreement/>)

### **B. Client Responsibilities:**

The client will be responsible for the following tasks during the course of using the Red Canary service:

- Installing Endpoint Collection Software on client systems
- Performing remediation and incident response actions in response to Threat Alerts.
- Obtaining all required authorizations to perform the Managed Threat Detection Services and any data or information required thereby. Client shall obtain consents and authorizes for Red Canary and its employees and agents to gain access to and retrieve Technical Data and analyze Threat Alerts and perform Managed Threat Detection Services. In the course of accessing, obtaining and otherwise using