



ATTACHMENT 1

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

This Statement of Work (“SOW”), dated January 13, 2020, 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 Cyber Security, LLC (“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:

Description of Kroll Services
<p><u>Kroll Threat Alert Response and Remediation Support:</u></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"> • Supplemental threat analysis and intelligence • Malware sandboxing and analysis • 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) • Threat Alert correlation and root cause analysis using the Endpoint Collection Software • Remediation guidance <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><u>Kroll Incident Response and Investigation Services</u></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"> • Emergency and after-hours incident response support • Remote evidence collection and analysis • In-lab forensic imaging and analysis • Malware reverse engineering • Event log collection, analysis and correlation • Custom threat hunting or forensic investigation using the Endpoint Collection Software • Custom analysis and reporting <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 six (6) months ("Initial Term" or "Term") from the date above ("Effective Date"), ending July 31, 2020.

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 **5,500** Endpoints ("End User's Endpoints"). For the Initial Term, the cost per Endpoint for six (6) months is **\$36.00**. "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	\$385/hour - \$675/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.

IN WITNESS WHEREOF, the parties have executed this Agreement to be effective on the date executed by COUNTY.

ATTEST:

MONA MIYASATO,
COUNTY EXECUTIVE OFFICER
CLERK OF THE BOARD

By: Shirley daGuena
Deputy Clerk

COUNTY

COUNTY OF SANTA BARBARA

Gregg Hart
GREGG HART, CHAIR
BOARD OF SUPERVISORS

Dated: 1-28-20

APPROVED AS TO FORM:

MICHAEL C. GHIZZONI
COUNTY COUNSEL

By: SGH
Deputy County Counsel

APPROVED AS TO ACCOUNTING FORM:

BETSY SCHAFFER, CPA, CPFO, AUDITOR-
CONTROLLER

By: C.S.S.

APPROVED AS TO FORM:

RAY AROMATORIO, ARM, AIC
RISK MANAGER

By: RA

RECOMMENDED FOR APPROVAL:

JANETTE D. PELL, DIRECTOR
GENERAL SERVICES DEPARTMENT

By: J. Pell for J. Pell

Accepted and agreed:

COUNTY OF SANTA BARBARA

Name:
Title:
Date:

KROLL CYBER SECURITY, LLC



Name: *Marc Brawner*
Title: *Managing Director*
Date: *1/15/2020*

[CONTINUE TO NEXT PAGE]

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 defined and accessible via the link(s) listed in the table below.

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.

Description of Red Canary Services
<p>Party Services: 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">• Includes 24x7x365 Red Canary Threat Alert escalation and Portal access.• Includes Automate features
<p>Threat Alerts: 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">• 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 help support both Client remediation efforts and identification of similar threats.
<p>Client Portal: 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>

Client's Software License ("Software EULA")

Third Party Software: The Red Canary Services include the provision of endpoint monitoring using Carbon Black Enterprise Response software ("Endpoint Collection Software"), 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 Carbon Black Response EULA incorporated as Exhibit B

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 accepts and agrees to the description of Services and Client Responsibilities above and to the terms and conditions attached hereto:

1. the EUSPA in Exhibit A and
2. the Carbon Black Response EULA in Exhibit B

COUNTY OF SANTA BARBARA

Name:
Title:
Date:

CONFIDENTIAL

Exhibit A: END USER SECURITY PLATFORM AGREEMENT

This End User **Security Platform Agreement** (this "Agreement") is entered into this date of MM, DD, 2019 (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.

CONFIDENTIAL

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.

CONFIDENTIAL

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): 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 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

CONFIDENTIAL

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

Exhibit B: Carbon Black Response EULA

This is a legal agreement between the end user (“You” or “Your”) and Carbon Black, Inc., a Delaware corporation (“Licensor” or “Carbon Black”). This Agreement is part of a package (the “Package”) that also includes, as applicable, executable files that You may download or a CD-ROM or other tangible media, in either case containing CB Response software application in object code only (both referred to herein as the “Software”) and certain written materials (the “Documentation”). Any patch, update, upgrade, modification or other enhancement provided by Licensor with respect to the Software or the Documentation shall be included within the meanings of those terms, for the purposes of this Agreement, except to the extent expressly provided below. If the Software has been provided to You for evaluation purposes (“Evaluation Software”), the terms and conditions set forth below shall apply unless specific alternative terms are expressly set forth for the Evaluation Software.

If the Package is provided in the form of a CD-ROM or other tangible media, such media may contain software applications other than the Software. This Agreement shall not govern the licensing of such separate software applications if such separate software applications are provided under separate license agreements.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, YOU ACKNOWLEDGE:

1) YOU (EITHER YOU AS AN INDIVIDUAL OR, IF THE SOFTWARE WILL BE USED BY AN ENTITY, ON BEHALF OF THAT ENTITY) REPRESENT AND AGREE THAT YOU HAVE THE CAPACITY AND AUTHORITY TO BIND YOURSELF OR, IF APPLICABLE, THE APPLICABLE ENTITY, TO THE TERMS OF THIS AGREEMENT, THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE BOUND BY THEM; AND
2) YOU UNDERSTAND THAT, IF YOU PURCHASED THE PACKAGE FROM AN AUTHORIZED RESELLER OF CARBON BLACK, THAT RESELLER IS NOT CARBON BLACK’S AGENT AND IS NOT AUTHORIZED TO MAKE ANY REPRESENTATIONS, CONDITIONS OR WARRANTIES, STATUTORY OR OTHERWISE, ON LICENSOR’S BEHALF OR TO VARY ANY OF THE TERMS OR CONDITIONS OF THIS AGREEMENT.

LIMITED LICENSE: Carbon Black hereby grants to You, subject to the terms and conditions of this Agreement, a non-exclusive, non-transferable right and license to use the Software only for Your own internal business purposes. You may not sell or transfer reproductions of the Software or Documentation to third parties in any way. You may only use the functionality in the Software available in the type of license and for operating system and number of operating systems and/or endpoints specified in an order, quote or invoice from Licensor that has been accepted by You (the “Order”); Evaluation Software may be used solely for Your internal evaluation of the suitability of the Software and in no event for production use. You may not use the Software for any purposes not specifically permitted hereunder or on operating systems not specified in the Order or make the Software available to more operating systems than the number specified in the Order, or, if Evaluation Software, on no more than two hundred (200) operating systems or endpoints.

CERTIFICATION AS TO USE: At Licensor’s request not more than once annually, You agree to certify to Licensor Your compliance with the license terms set forth in this Agreement and to allow Licensor or its designee to inspect Your data processing systems and records to verify such compliance, provided that any such inspections will be made on not less than ten (10) days written notice and during regular business hours and that all information obtained during such inspection shall be kept strictly confidential and used by Licensor solely to enforce Carbon Black’s rights under this Agreement. If the inspection reveals an underpayment to Licensor of license fees, You shall promptly pay to Licensor the deficit. Licensor shall bear the expense of such inspection unless the inspection reveals an underpayment of license fees in excess of five percent (5%), in which case You shall bear all reasonable costs associated with the inspection.

OWNERSHIP; COPYRIGHT: Title to the Software and the Documentation, and patents, copyrights and all other property rights applicable thereto, shall at all times remain solely and exclusively with Carbon

CONFIDENTIAL

Black and Carbon Black's licensors, and You shall not take any action inconsistent with such title. The Software and the Documentation are protected by United States and other applicable laws and by international treaty provisions. Any rights not expressly granted herein are reserved to Carbon Black and Carbon Black's licensors.

OTHER RESTRICTIONS: You may not cause or permit the disclosure, copying, renting, licensing, sublicensing, leasing, dissemination or other distribution of the Software or the Documentation by any means or in any form, without the prior written consent of Licensor. You may not use the Software to conduct a service bureau or similar business for the benefit of third parties. You may not modify, enhance, supplement, create derivative work from, adapt, translate, reverse engineer, decompile, disassemble or otherwise reduce the Software to human readable form.

ULTRAHAZARDOUS ACTIVITIES: The Software is not designed, manufactured or intended for use in any environment in which the failure of the Software could lead to death, personal injury or severe physical or environmental damage, which uses and environments may include, but are not limited to, 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 hazardous environment requiring fail-safe performance ("Ultrahazardous Activities"). You represent and warrant to Licensor that You will not install or use the Software for such purposes.

LIMITED WARRANTY: Carbon Black warrants that for a period of ninety (90) days after the delivery of the Software ("Software Warranty Period"), the Software will conform in all material respects to the applicable Documentation. This limited warranty: (i) applies to the initial licensee only and may be acted upon only by the initial licensee; (ii) does not apply in the event of any alteration of the Software or any use of the Software other than as permitted hereby or in accordance with its published specifications; and (iii) does not apply to (x) any patch, update, upgrade, modification, or other enhancement provided by Licensor with respect to the Software or the Documentation, or (y) any information or data, including but not limited to, threat intelligence data originating from third parties and enabled through the Software or by links provided by Carbon Black, which are provided on an AS IS BASIS ONLY and Carbon Black hereby disclaims any liability with respect to accuracy, completeness and/or use.

NOTWITHSTANDING THE FOREGOING, EVALUATION SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND.

EXCEPT AS EXPLICITLY STATED ABOVE, CARBON BLACK AND CARBON BLACK'S LICENSORS, RESELLERS AND/OR DISTRIBUTORS MAKE NO OTHER WARRANTY OR CONDITION, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, REGARDING THIS SOFTWARE, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT ERROR FREE OPERATION OR NON-INTRUSION DUE TO HACKING OR OTHER SIMILAR MEANS OF UNAUTHORIZED ACCESS. FURTHER, NO REPRESENTATION OR OTHER AFFIRMATION OF FACT, INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, SUITABILITY FOR USE OR PERFORMANCE OF ANY PRODUCTS OR SERVICES PROVIDED BY CARBON BLACK, OR ANY INFORMATION, CONTENT, OR DATA CONTAINED THEREIN, WHETHER MADE BY CARBON BLACK EMPLOYEES OR OTHERWISE, WHICH IS NOT CONTAINED IN THIS AGREEMENT, WILL BE DEEMED TO BE A WARRANTY BY CARBON BLACK FOR ANY PURPOSE OR GIVE RISE TO ANY LIABILITY OF CARBON BLACK WHATSOEVER.

If You believe You have found any such error or defect in the Software during the Software Warranty Period, call Carbon Black's Customer Service Department at +1 (617) 393-7487 or 877-248-9098 between the hours of 8:00 a.m. and 8:00 p.m. Monday through Friday (Eastern Time), holidays excluded, and provide Your Product number. Carbon Black's and Carbon Black's licensors' entire liability and Your exclusive remedy for breach of this limited warranty shall be the repair or replacement of the Software with a corrected version of the Software, within a reasonable period of time and without charge.

DATA COLLECTION: In the event You affirmatively opt in through the Software, Carbon Black will collect and use information about your binaries, devices, files, systems, software, and endpoints ("Technical Data"), to support your use of the Software. The Technical Data may also be used by Carbon Black and

CONFIDENTIAL

distributed (in aggregated and non-attributable form) to improve the operation and functionality of the Carbon Black's products and service, and for threat detection, threat intelligence, and related analysis. By opting into this data collection, Customer agrees to the collection, use, distribution, transfer, back-up and storage of the Technical Data by Carbon Black and its service providers. Customer also agrees that Carbon Black and its service providers may, distribute, transfer, copy, backup and store your Technical Data in the United States, Europe, or other jurisdictions where data protection standards may be different. Carbon Black shall not be responsible for the deletion, correction, destruction, damage, or loss of any such data collected. Carbon Black 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.

LIMITATION OF LIABILITY:

NOTWITHSTANDING ANY PROVISION OF THIS AGREEMENT TO THE CONTRARY, IN NO EVENT SHALL CARBON BLACK OR ITS SUPPLIERS, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SHAREHOLDERS, RESELLERS, DISTRIBUTORS, OR CONTRACTORS ("RELATED PARTIES") BE LIABLE TO YOU FOR CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING BUT NOT LIMITED TO LOST REVENUES, PROFITS OR DATA OR OTHER ECONOMIC LOSS) REGARDLESS OF THE CAUSE OF ACTION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ADDITION, THE MAXIMUM LIABILITY OF CARBON BLACK AND ITS RELATED PARTIES, TAKEN AS A WHOLE, FOR ANY AND ALL CLAIMS IN CONNECTION WITH THIS AGREEMENT AND PACKAGE, REGARDLESS OF THE FORM OF ACTION, SHALL IN NO CIRCUMSTANCE EXCEED THE PURCHASE PRICE OF THE PACKAGE OR, FOR EVALUATION SOFTWARE, \$100.00.

CONFIDENTIALITY: The Software and all information disclosed by Licensor to You hereunder or otherwise in connection with the Software, together with, for Evaluation Software, all results of Your evaluation (collectively "Confidential Information"), are confidential information of Licensor and shall not be disclosed by You to any third party. You shall only use the Confidential Information as expressly permitted by this Agreement, and in no other manner. You agree to take all necessary precautions to avoid disclosure and misuse of the Confidential Information. You shall promptly notify Licensor if You become aware of any breach of this confidentiality obligation and agrees to remedy any such breach.

TERMINATION: This Agreement is effective until terminated. You may terminate the Agreement at any time if there is an uncured material breach of this Agreement by destroying all copies of the Software, and all media and documentation and by providing Licensor with written notice and confirmation. The Agreement will terminate immediately without notice from Licensor if You fail to comply with any provision of this Agreement. Upon any termination, You must destroy all copies of the Software and all media and Documentation and shall pay to Carbon Black all sums as set forth in the Order then remaining unpaid. The provisions regarding Confidentiality, Limitation of Liability and Evaluation Software Indemnity shall survive termination of this Agreement indefinitely.

EVALUATION SOFTWARE INDEMNITY: You agree 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 claims brought by any third party relating to Your use of the Evaluation Software.

THIRD-PARTY INFRINGEMENT INDEMNIFICATION. Carbon Black shall (a) defend, indemnify and hold Customer and its officers, directors, employees and agents harmless from and against all claims and causes of action arising out of an allegation that the Software infringes a third party copyright, trademark or U.S., Canadian or European Union patent, and (b) 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 (1) prompt written notice of such claim or action; (2) the right to control and direct the investigation, preparation, defense, and settlement of the action; and (3) 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 Software or, if in Carbon Black's opinion the Software are likely to become the subject of a claim, then Carbon Black may, at its election, either (a) obtain the right for Customer to continue to use the Licensed Material; or (b) replace or modify the Software 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

CONFIDENTIAL

this Agreement and (a) with respect to any perpetual licenses, refund any monies paid by Customer for the Software less depreciation for use, assuming straight line depreciation over a five-year useful life, or (b) with respect to any subscription licenses, refund any prepaid fees for such subscription on a pro rata basis. This section shall not apply to infringement or misappropriation claims arising in whole or in part from (1) designs, specifications or modifications originated or requested by Customer; (2) the combination of the Software 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 (3) Customer's failure to install a maintenance update, where same would have avoided such claim. THIS SECTION STATES CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND CARBON BLACK'S ENTIRE LIABILITY FOR THIRD PARTY INFRINGEMENT CLAIMS.

EXPORT AND IMPORT COMPLIANCE: In the event You export the Software from the country in which You first received it, You assume the responsibility for compliance with all applicable import, export and re-export regulations, as the case may be, including but not limited to, any regulations of the Office of Export Administration of the U.S. Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, and other U.S. agencies and the export control regulations of the European Union. You acknowledge and agree the Software shall not be used, and none of the underlying information, software, or technology may be transferred or otherwise exported or re-exported to countries as to which the United States and/or the European Union maintains an embargo (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders (collectively, "Designated Nationals"). The lists of Embargoed Countries and Designated Nationals are subject to change without notice. By using the Software, You represent and warrant that You are not located in, or are under the control of, or a national or resident of, an Embargoed Country or Designated National. You agree to comply strictly with all applicable laws and assume sole responsibility for obtaining licenses to import, export or re-export as may be required.

The Software may use encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations, 15 C.F.R. Parts 730-774 and Council Regulation (EC) No. 1334/2000. Carbon Black makes no representation the Software is appropriate or available for use in locations outside the United States. If You use the Software from outside the United States, You are solely responsible for compliance with all applicable laws, including without limitation export and import regulations of other countries. Any diversion or use of the Software contrary to United States law is prohibited.

You represent and warrant to Carbon Black that You will not use the Software or any portion thereof in violation of applicable laws or regulations, and You agree to indemnify and hold Carbon Black harmless from and against claims, losses, costs, or liability, arising in connection with Your breach of this Section.

GOVERNMENT RESTRICTED RIGHTS: The Software and Documentation are "commercial computer software" or "commercial computer software documentation." Absent a written agreement to the contrary, the U.S. Government's rights with respect to such Software or Documentation are limited by the terms of this Agreement, pursuant to FAR § 12.212(a) and/or DFARS § 227.7202-1(a), as applicable.

GOVERNING LAW: This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, U.S.A., excluding (a) its conflicts of laws principles; (b) the United Nations Convention on Contracts for the International Sale of Goods; (c) the 1974 Convention on the Limitation Period in the International Sale of Goods (the "1974 Convention"); (d) the Protocol amending the 1974 Convention, done at Vienna April 11, 1980; and (e) the Uniform Computer Information Transactions Act (UCITA) as adopted by any state. You hereby submit to the exclusive jurisdiction of the federal and state courts located in Suffolk County, Massachusetts in connection with any dispute arising out of or relating to this Agreement and waive any objection to such venue.

EQUITABLE RELIEF: You agree that, because of the proprietary nature of the Software, Carbon Black's remedies at law for a breach by You of Your obligations under this Agreement will be inadequate and that Licensor shall, in the event of a breach or threatened breach, be entitled to equitable relief, including injunctive relief, without the posting of any bond, in addition to all other remedies provided under this Agreement or available at law.

CONFIDENTIAL

GENERAL: This Agreement constitutes the entire understanding between Carbon Black and You with respect to subject matter hereof. Any change to this Agreement must be in writing, signed by Licensor and You. Terms and conditions as set forth in any order which differ from, conflict with, or are not included in this Agreement shall not become part of this Agreement unless specifically accepted by Licensor in writing. You shall be responsible for and shall pay, and shall reimburse Licensor on request if Licensor is required to pay, any sales, use, value added (VAT), consumption or other tax (excluding any tax that is based on Licensor's net income), assessment, duty, tariff, or other fee or charge of any kind or nature that is levied or imposed by any governmental authority on the Package.