REPORT ON CARBON BLACK, INC.’S DESCRIPTION OF ITS CLOUD SERVICES AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD JULY 1, 2017 TO DECEMBER 31, 2017
# TABLE OF CONTENTS

**SECTION 1**  
Independent Service Auditor’s Report ................................................................. 3

**SECTION 2**  
Carbon Black, Inc.’s Assertion .............................................................................. 9

**SECTION 3**  
Description of Carbon Black, Inc.’s Cloud Services for the Period July 1, 2017 to December 31, 2017 .................................................................................. 13

**SECTION 4**  
Trust Services Security, Availability and Confidentiality Principles, Criteria, Related Controls and Tests of Controls ........................................................................... 25

**SECTION 5**  
Other Information Provided by Carbon Black, Inc. That is Not Covered by the Service Auditor’s Report .............................................................................................. 54
SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT
INDEPENDENT SERVICE AUDITOR’S REPORT

To: Carbon Black, Inc. ("Carbon Black")

SCOPE

We have examined the description in Section 3 titled “Description of Carbon Black, Inc.’s Cloud Services for the Period July 1, 2017 to December 31, 2017” (description) based on the criteria set forth in paragraph 1.26 of the 2015 AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (applicable trust services criteria), throughout the period July 1, 2017 to December 31, 2017. The controls included in the description are those that management of Carbon Black believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of Carbon Black’s Cloud Services that are not likely to be relevant to meeting the applicable trust services criteria. The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Carbon Black’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information in Section 5, "Other Information Provided by Carbon Black, Inc. That is Not Covered by the Service Auditor’s Report," that describes management’s responses to testing exceptions, is presented by management of Carbon Black to provide additional information and is not a part of Carbon Black’s description of Carbon Black, Inc.’s Cloud Services made available to user entities during the period July 1, 2017 to December 31, 2017. Information about Carbon Black’s responses to testing exceptions has not been subjected to the procedures applied in the examination of the description of Carbon Black, Inc.’s Cloud Services and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of Carbon Black, Inc.’s Cloud Services and, accordingly, we express no opinion on it.

As indicated in the description, Carbon Black uses a service organization (subservice organization) for data center colocation services. The description indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of Carbon Black’s controls are suitably designed and operating effectively, along with the related controls at Carbon Black. The description presents Carbon Black’s system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organization. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

SERVICE ORGANIZATION’S RESPONSIBILITIES

In Section 2, Carbon Black has provided its assertion titled “Assertion of the Management of Carbon Black, Inc.” (assertion) about the fairness of the presentation of the description based on the description criteria and
suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Carbon Black is responsible for selecting the applicable trust services principles addressed by the engagement; preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; identifying any applicable trust services criteria relevant to the principles addressed by the engagement that have been omitted from the description and explaining the reason for omission; designing, implementing, and documenting the controls that are suitably designed and operating effectively to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

SERVICE AUDITOR’S RESPONSIBILITIES

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2017 to December 31, 2017. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves:

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2017 to December 31, 2017.
- assessing the risks that the description is not fairly presented based on the description criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description, the suitability of the applicable trust services criteria stated therein, and the suitability of the criteria specified by the service organization in its assertion.

INHERENT LIMITATIONS

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important in its own particular environment. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design
or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

**BASIS FOR QUALIFIED OPINION**

Carbon Black states in the description of its system that a risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. However, as noted in Section 4 of this report, Carbon Black did not perform a risk assessment for the in-scope applications in the last year. This control deficiency resulted in the system’s failure to meet criterion CC3.1, *The entity (1) identifies potential threats that could impair system commitments, and system requirements related to the in-scope TSPs (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.*

Carbon Black states in the description of its system that internal and external network vulnerability scans are performed quarterly. A remediation plan is developed to remediate all critical and high vulnerabilities at a minimum. However, as noted in Section 4 of this report, for 2 out of a sample of 2 quarters, internal and external network scans were not performed for Carbon Black Response and Carbon Black Defense. This control deficiency resulted in the system’s failure to meet criterion CC7.3, *Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity’s commitments and system requirements as they relate to the in-scope TSPs.*

Carbon Black states in the description of its system that the Company software and infrastructure change management process requires that change requests are authorized, formally documented, tested prior to migration to production, peer reviewed by a second developer and reviewed and approved by management. However, as noted in Section 4 of this report, for 25 out of a sample of 25 infrastructure and software changes that occurred during the examination period, software and infrastructure change requests did not evidence that testing occurred prior to migration to production or that peer review occurred by a second developer. This control deficiency resulted in the system’s failure to meet criterion CC7.4, *Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity’s commitments and system requirements related to the in-scope TSPs.*

Carbon Black states in the description of its system that a documented disaster recovery (DR) plan is in place and a DR test is performed at least annually. However, as noted in Section 4 of this report, DR plans are not documented for application service offerings and DR tests are not performed at least annually. In addition, Carbon Black states in the description of its system that it tests restoration of data at least annually or as part of normal business operations. However, as noted in Section 4 of this report, Carbon Black Response did not document restoration of data during the review period. These control deficiencies resulted in the system’s failure to meet criterion A1.3, *Recovery plan procedures supporting system recovery are tested to help meet the entity’s availability commitments and system requirements.*
Carbon Black states in the description of its system that a list of subservice organizations is maintained and those parties are required to maintain their own security practices and procedures. Conformance is assessed annually by reviewing third-party attestation reports or performing a vendor risk assessment. However, as noted in Section 4 of this report, a documented review of third-party attestation reports or vendor risk assessment was not performed within the past year. This control deficiency resulted in the system’s failure to meet criterion C1.5, Compliance with the entity’s confidentiality commitments and system requirements by vendors and other third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.

Carbon Black states in the description of its system that customer data containing confidential information is purged or removed from the production environment, in accordance with best practices, when customers leave the service. However, as noted in Section 4 of this report, evidence could not be obtained that customer data is being purged or removed from production environments in accordance with best practices when customers leave the service. This control deficiency resulted in the system’s failure to meet criterion C1.8, The entity disposes of confidential information to meet the entity’s confidentiality commitments and system requirements.

OPINION

In our opinion, in all material respects, based on the description criteria identified in Carbon Black’s assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period July 1, 2017 to December 31, 2017.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 1, 2017 to December 31, 2017 and user entities applied the complementary user entity controls assumed in the design of Carbon Black’s controls throughout the period July 1, 2017 to December 31, 2017, and the subservice organization applied the complementary controls assumed in the design of Carbon Black’s controls throughout the period July 1, 2017 to December 31, 2017.

c. except for the matters described under “Basis for Qualified Opinion”, the controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period July 1, 2017 to December 31, 2017 if user entities applied the complementary user entity controls assumed in the design of Carbon Black’s controls, and those controls operated effectively throughout the period July 1, 2017 to December 31, 2017 and if the complementary subservice organization controls assumed in the design of Carbon Black’s controls operated effectively throughout the period July 1, 2017 to December 31, 2017.

DESCRIPTION OF TESTS OF CONTROLS

The specific controls we tested, the tests we performed, and the results of our tests are listed in Section 4, “Trust Services Security, Availability and Confidentiality Principles, Criteria, Related Controls and Tests of Controls” of this report.

RESTRICTED USE

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Carbon Black; user entities of Carbon Black, Inc.’s Cloud Services during some or all
of the period July 1, 2017 to December 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization’s system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than the specified parties.

Coalfire Controls LLC

June 1, 2018
Louisville, Colorado
SECTION 2

CARBON BLACK, INC.’S ASSERTION
Assertion of the Management of Carbon Black, Inc. ("Carbon Black")

We have prepared the description titled "Description of Carbon Black, Inc.'s Cloud Services for the Period July 1, 2017 to December 31, 2017" (description), based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the 2015 AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (description criteria). The description is intended to provide users with information about Carbon Black's Cloud Services, particularly system controls intended to meet the criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (applicable trust services criteria), throughout the period July 1, 2017 to December 31, 2017.

Carbon Black uses a subservice organization, Amazon Web Services (AWS), for data center colocation services. The description includes only the applicable trust services criteria and related controls of Carbon Black and excludes the applicable trust services criteria and related controls of AWS. The description also indicates that certain applicable trust services criteria specified in the description can be met only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that the applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Carbon Black's controls are suitably designed and operating effectively, along with related controls at the service organization and the subservice organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

a. The description fairly presents Carbon Black's Cloud Services throughout the period July 1, 2017 to December 31, 2017 as it relates to controls that are likely to be relevant to meeting the applicable trust services criteria. Our assertion is based on the following description criteria:

i. The description contains the following information:

1) The types of services provided.

2) The components of the system used to provide the services, which are as follows:

- **Infrastructure.** The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

- **Software.** The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

- **People.** The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel and managers).

- **Procedures.** The automated and manual procedures.
Carbon Black.

- *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

3) The boundaries or aspects of the system covered by the description.

4) For information provided to, or received from, subservice organizations and other parties
   a. how the information is provided or received and the role of the subservice organizations and other parties.
   b. the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user entity controls contemplated in the design of the service organization's system.

6) Regarding the subservice organization that is presented using the carve-out method
   a. the nature of the services provided by the subservice organization.
   b. each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

7) Any applicable trust services criteria that are not addressed by a control and the reasons.

8) Relevant details of changes to the service organization's system during the period covered by the description.
   ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the period July 1, 2017 to December 31, 2017 to meet the applicable trust services criteria, if the subservice organization and user entities applied the complementary controls assumed in the design of Carbon Black's controls throughout the period July 1, 2017 to December 31, 2017.

c. Except for the matters described below, the controls stated in the description operated effectively throughout the period July 1, 2017 to December 31, 2017 to meet the applicable trust services
criteria, if the subservice organization and user entities applied the complementary controls assumed in the design of Carbon Black’s controls throughout the period July 1, 2017 to December 31, 2017:

- A risk assessment was not performed for the in-scope applications during the last year, resulting in a failure to address common criteria 3.1.
- Internal and external network vulnerability scans were not performed during the period for Carbon Black Response and Carbon Black Defense, resulting in a failure to address common criteria 7.3.
- Software and infrastructure change requests during the period did not evidence that testing occurred prior to migration to production or that peer review occurred by a second reviewer, resulting in a failure to address common criteria 7.4.
- Disaster recovery plans were not documented or tested during the period and Carbon Black Response did not document restoration of data during the period, resulting in a failure to address availability criteria 1.3.
- A documented review of third party attestation reports or vendor risk assessment was not performed within the past year, resulting in a failure to address confidentiality criteria 1.5.
- Evidence was not retained during the period that customer data is purged or removed from production environments when customers leave the service, resulting in a failure to address confidentiality criteria 1.8.

__________________________
Carbon Black, Inc. Authorized Representative

Ryan Polk
SVP, Chief Product Owner