REPORT ON CARBON BLACK, INC.’S DESCRIPTION OF ITS CLOUD SERVICES SOLUTION AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD APRIL 1, 2018 TO MARCH 31, 2019
TABLE OF CONTENTS

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

SECTION 2
Assertion of Carbon Black, Inc. Management......................................................... 8

SECTION 3
Description of Carbon Black, Inc.’s Cloud Services Solution Throughout the Period
April 1, 2018 to March 31, 2019 ............................................................................. 11

SECTION 4
Trust Services Categories, Criteria, Related Controls and Tests of Controls Relevant
to Security, Availability and Confidentiality ......................................................... 25

SECTION 5
Other Information Provided by Carbon Black, Inc. That Is Not Covered by the
Service Auditor’s Report......................................................................................... 67
SECTION 1

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

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

SCOPE

We have examined Carbon Black’s accompanying description of its Cloud Services Solution found in Section 3 titled “Description of Carbon Black’s Cloud Services Solution Throughout the Period April 1, 2018 to March 31, 2019” (description) based on the criteria for a description of a service organization’s system set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2018 to March 31, 2019, to provide reasonable assurance that Carbon Black’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Carbon Black, to achieve Carbon Black’s service commitments and system requirements based on the applicable trust services criteria. The description presents Carbon Black’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Carbon Black’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5, "Other Information Provided by Carbon Black, Inc. That Is Not Covered by the Service Auditor’s Report," is presented by Carbon Black’s management to provide additional information and is not a part of Carbon Black’s description of its Cloud Services Solution made available to user entities during the period April 1, 2018 to March 31, 2019. Information about Carbon Black’s responses to testing exceptions have not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Carbon Black uses subservice organizations to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Carbon Black, to achieve Carbon Black’s service commitments and system requirements based on the applicable trust services criteria. The description presents Carbon Black’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Carbon Black’s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

SERVICE ORGANIZATION’S RESPONSIBILITIES

Carbon Black is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Carbon Black’s service commitments and system requirements were achieved. In Section 2, Carbon Black has provided the accompanying assertion titled “Assertion of Carbon Black, Inc. Management” (assertion) about the
description and the suitability of design and operating effectiveness of controls stated therein. Carbon Black is also responsible for 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; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

SERVICE AUDITOR’S RESPONSIBILITIES

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

INHERENT LIMITATIONS

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 individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that
controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

**DESCRIPTION OF TESTS OF CONTROLS**

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, “Trust Services Categories, Criteria, Related Controls and Tests of Controls Relevant to Security, Availability and Confidentiality” of this report.

**CONTROLS THAT DID NOT OPERATE DURING THE PERIOD**

Carbon Black’s description of its Cloud Services Solution discusses its incident response and recovery plan, which includes the controls implemented and operated to respond to and recover from security incidents. Carbon Black’s incident response and recovery plan includes procedures to help understand, contain, monitor, or eradicate a security incident; restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. However, during the period April 1, 2018 through March 31, 2019, Carbon Black did not experience a security incident that would warrant the operation of the response and recovery processes and controls. The description also discusses the disposition of confidential information, which includes the controls implemented and operated to purge or destroy electronic media containing confidential information. However, during the period April 1, 2018 to March 31, 2019, no electronic media containing confidential information was required to be purged or destroyed.

Because the controls described above did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using the following trust services criteria:

- **CC7.4** - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
- **CC7.5** - The entity identifies, develops, and implements activities to recover from identified security incidents.
- **C1.2** - The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.

**BASIS FOR QUALIFIED OPINION**

Carbon Black states in the description of its system that customer data containing confidential information is purged or removed from the application environment when customers leave the service. However, as noted in Section 4 of this report, the job configurations to purge or remove customer data did not align with the Company’s policies. This control deficiency resulted in the system’s failure to meet criterion C1.2, *The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.*

**OPINION**

In our opinion, in all material respects—

a. the description presents Carbon Black’s Cloud Services Solution that was designed and implemented throughout the period April 1, 2018 to March 31, 2019 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that Carbon Black’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated...
effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Carbon Black’s controls throughout that period.

c. except for the matter described under “Basis for Qualified Opinion”, the controls stated in the description operated effectively throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that Carbon Black’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Carbon Black’s controls operated effectively throughout that period.

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’s Cloud Services Solution during some or all of the period April 1, 2018 to March 31, 2019, business partners of Carbon Black subject to risks arising from interactions with Carbon Black’s Cloud Services Solution, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements 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
Westminster, Colorado
June 10, 2019
SECTION 2

ASSERTION OF CARBON BLACK, INC.
MANAGEMENT
Assertion of Carbon Black, Inc. (“Carbon Black”) Management

We have prepared the accompanying description of Carbon Black’s Cloud Services Solution titled “Description of Carbon Black’s Cloud Services Solution Throughout the Period April 1, 2018 to March 31, 2019” (description), based on the criteria for a description of a service organization’s system set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the Cloud Services Solution that may be useful when assessing the risks arising from interactions with Carbon Black’s system, particularly information about system controls that Carbon Black has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Carbon Black uses subservice organizations for data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Carbon Black, to achieve Carbon Black’s service commitments and system requirements based on the applicable trust services criteria. The description presents Carbon Black’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Carbon Black’s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Carbon Black, to achieve Carbon Black’s service commitments and system requirements based on the applicable trust services criteria. The description presents Carbon Black’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Carbon Black’s controls.

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

a. the description presents Carbon Black’s Cloud Services Solution that was designed and implemented throughout the period April 1, 2018 to March 31, 2019, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that Carbon Black’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Carbon Black’s controls throughout that period.

c. except for the matter described in paragraph d, the controls stated in the description operated effectively throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that Carbon Black’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Carbon Black’s controls operated effectively throughout that period.

d. Carbon Black states in the description of its system that customer data containing confidential information is purged or removed from the application environment when customers leave the service. However, as noted in Section 4 of this report, the job configurations to purge or remove
customer data did not align with the Company's policies. This control deficiency resulted in the system’s failure to meet criterion C1.2.

Controls That Did Not Operate During the Period
Our description of the Carbon Black Cloud Services Solution discusses Carbon Black’s incident response and recovery plan, which includes the controls implemented and operated to respond to and recover from security incidents. Carbon Black’s incident response and recovery plan includes procedures to help understand, contain, monitor, or eradicate a security incident; restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. However, during the period April 1, 2018 through March 31, 2019, Carbon Black did not experience a security incident that would warrant the operation of the response and recovery processes and controls, which address trust services criteria CC7.4, The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate, and CC7.5, The entity identifies, develops, and implements activities to recover from identified security incidents. Our description also discusses the disposition of confidential information, which includes the controls implemented and operated to purge or destroy electronic media containing confidential information. However, during the period April 1, 2018 to March 31, 2019, Carbon Black did not experience the circumstances that would warrant the operation of the electronic media purging and destruction control, which addresses trust services criteria C1.2, The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.

Carbon Black, Inc.