NOTICE: This Service Description is no longer being updated. Content has been moved to the Cloud Services Guide, found at https://www.vmware.com/agreements

VMware Carbon Black Cloud™

Service Description

Updated as of 22 September 2022

vmware

As used in this Service Description, "VMware", "we", or "us" means VMware, Inc., a Delaware corporation, if the billing address for your order is in the United States, or VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your order is outside the United States. Terms not defined in this Service Description are defined in the Terms of Service or elsewhere in the Agreement.

The VMware Privacy Notices describe how personal information may be collected, used, shared, or otherwise processed by VMware as a data controller. The VMware Privacy Notices are available at https://www.vmware.com/help/privacy.html.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

1. Introduction

1.1 Service Description

VMware Carbon Black Cloud™ ("VMware Carbon Black Cloud") is a cloud-native Endpoint and workload protection platform that enables customers to protect, prevent, detect, and respond to cybersecurity attacks on their Endpoints and server workloads. VMware Carbon Black Cloud collects and consolidates a customer's system data in a single platform to enable the customer to efficiently protect its environment from breaches. VMware Carbon Black Cloud pulls this information into a centralized data analytics platform, and provides the customer with analysis, alerts, and intelligence on vulnerabilities, suspicious activity, and blocked malware. Customers access the VMware Carbon Black Cloud service offerings through a web browser and by using scripts against a public API.

VMware Carbon Black Cloud ingests a variety of data sources that are processed and stored as cybersecurity events, behaviors, and system state metrics that can be analyzed, visualized, and alerted upon for anomaly detection, incident investigation, and remediation of cybersecurity risks.

This Service Description governs the following cloud service offerings that are available for purchase on the VMware Carbon Black Cloud platform, all of which use the unified VMware Carbon Black Cloud console and, if applicable, the universal Endpoint agent:

- **VMware Carbon Black Cloud Endpoint™ Standard** (formerly known as CB Defense) - Next-generation anti-virus ("NGAV") offering, including behavioral endpoint detection and response ("behavioral EDR").
- **VMware Carbon Black® Cloud Audit and Remediation™** (formerly known as CB LiveOps) – Remote system audit and risk remediation solution for IT, compliance, and security.
- **VMware Carbon Black® Cloud Enterprise EDR™** (formerly known as CB ThreatHunter) – Advanced enterprise endpoint detection and response solution for security operations.
- **VMware Carbon Black Container™ Essentials** – Includes container image scanning, Kubernetes security posture management, and application topology to provide continuous visibility, security, and compliance for the full lifecycle of Kubernetes applications.
- **VMware Carbon Black Container™ Advanced** – Includes all components of VMware Carbon Black Container Essentials, plus runtime traffic management with network workload anomaly detection, egress traffic control, and Kubernetes network map for on-premises and cloud-native environments.
- **VMware Carbon Black Cloud Endpoint™ Advanced** (formerly known as CB Defense and CB LiveOps) – Includes all components of VMware Carbon Black Cloud Endpoint Standard plus VMware Carbon Black Cloud Vulnerability Management™, and VMware Carbon Black Cloud Audit and Remediation capabilities.

- **VMware Carbon Black Cloud Endpoint™ Enterprise** (formerly known as CB Defense, CB LiveOps, and CB ThreatHunter) - Includes all components of VMware Carbon Black Cloud Endpoint Advanced and VMware Carbon Black Cloud Enterprise EDR.
- **VMware Carbon Black Cloud Workload™ Essentials** - Advanced protection for securing modern workloads. Combines VMware Carbon Black Cloud Vulnerability Management™ and foundational workload hardening with advanced prevention, detection, and response capabilities to protect workloads running in virtualized, private and hybrid cloud environments, plus remote audit and risk remediation**.**
- **VMware Carbon Black Cloud Workload™ Advanced** – Includes all components of VMware Carbon Black Cloud Workload Essentials, plus next-generation antivirus protection and behavioral EDR.
- **VMware Carbon Black Cloud Workload™ Enterprise** – Includes all components of VMware Carbon Black Cloud Workload Advanced, plus enterprise threat hunting for workloads.

In addition, customers can purchase the following add-on service offerings which operate along with VMware Carbon Black Cloud service offerings:

- **VMware Carbon Black® Cloud Managed Detection™** (formerly known as CB ThreatSight) – Managed service dedicated to triaging and prioritizing alerts from the VMware Carbon Black Cloud Endpoint Standard service offering, and providing the customer with proactive advisories and timely consolidated results in an actionable report format. VMware Carbon Black Cloud Managed Detection requires that a customer has also purchased a subscription to a VMware Carbon Black Cloud service offering that includes a NGAV and/or behavioral EDR component.
- **VMware Carbon Black® Cloud Managed Detection and Response™** – Builds upon VMware Carbon Black Cloud Managed Detection offering that provides analyst-backed continuous monitoring, alert triage, and threat analyst guidance on policy changes, by additionally providing available assistance with responding to an alert in the event of an incident. When configured, VMware analysts can take actions on a customer's behalf in response to an alert. As with VMware Carbon Black Cloud Managed Detection, VMware Carbon Black Cloud Managed Detection and Response ("MDR") requires that a customer has also purchased a subscription to a VMware Carbon Black Cloud service offering that includes a NGAV and/or behavioral EDR component.
- **VMware Data Retention™ for VMware Carbon Black Cloud™** - VMware Data Retention is delivered as a platform add-on to other VMware Carbon Black Cloud service offerings. Data Retention for VMware Carbon Black Cloud allows VMware Carbon Black Cloud customers to purchase extended event data retention periods. Data Retention for VMware Carbon Black Cloud provides 60, 90, and 180 day event data retention options. Once a customer has purchased this add-on, any subsequently retained data will be stored for the period of time purchased.
- **VMware Carbon Black Cloud Vulnerability Management** – Prioritized vulnerability reporting and continuous visibility across a customer's environment.

Vulnerability Management is included with Carbon Black Endpoint Advanced, Carbon Black Endpoint Enterprise, Carbon Black Workload Essentials, Carbon Black Workload Advanced, and Carbon Black Workload Enterprise bundles, or it can be purchased as an add-on to Endpoint Standard.

Customers can also purchase the following service offerings which include VMware Carbon Black Cloud platform functionality in combination with other VMware products:

- **VMware Workspace Security™** - The VMware Workspace Security offerings may include certain VMware Carbon Black Cloud functionality in combination with VMware Workspace ONE® and/or VMware Horizon® Service capabilities.
  For details on the Workspace ONE offerings, see the Service Description at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/workspace-one-service-description.pdf

  For details on the Horizon Service offerings, see the Service Description at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmw-horizon-service-description.pdf
- **VMware Advanced Security™ for VMware Cloud Foundation™** – VMware Carbon Black Workload Advanced, plus VMware NSX® Advanced Load Balancer™ and VMware NSX® Advanced Threat Prevention™ add-on.

The individual VMware Carbon Black Cloud platform cloud service offerings (excluding VMware Carbon Black Cloud Managed Detection) all include:

- A cloud-hosted, high-availability, and high-performance database for aggregation and storage of high-volume data from the customer's Endpoints or server workloads.
- A REST API that allows users to perform a subset of the operations that they can carry out through the VMware Carbon Black Cloud service offering. Users can integrate VMware Carbon Black Cloud service offerings with third-party cybersecurity products, such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.
- Software agents ("Sensor Software") installed on the customer's Endpoints or Server workloads.

1.2 Technical Documentation

A Quick Start guide, conceptual guides on key areas of the platform, workflow guides for navigating through key features, help pages, information about APIs, product resources, community forums, and FAQs are available only to customers logged in to the following URL:
https://community.carbonblack.com/.

1.3 Legal Terms

Terms of Service

Use of the VMware Carbon Black Cloud service offerings is subject to the VMware Cloud Service Offerings Terms of Service ("Terms of Service"), that can be found though a link at the VMware end user terms landing page, at:
https://www.vmware.com/download/eula.html

The Terms of Service supersede any terms that may be presented to a customer upon logging into the particular VMware Carbon Black Cloud service offering.

For VMware Carbon Black Cloud Managed Detection and MDR, any warranties in the Terms of Service are expressly excluded. The sole and exclusive warranty for VMware Carbon Black Cloud Managed Detection and MDR, express or implied, is as follows: VMware Carbon Black warrants that VMware Carbon Black Cloud Managed Detection and MDR will be performed in a professional and workmanlike manner consistent with industry standards for similar types of services.

Additional Terms

In addition to the terms and conditions in the Terms of Service and elsewhere in the Agreement, VMware Carbon Black Cloud service offerings are also subject to the following additional terms:

Threat Intelligence Data Collection

Certain VMware Carbon Black Cloud service offerings may collect data relating to malicious or potentially malicious code, binaries, attacks, activities, and vulnerabilities on the customer's Endpoints or workloads ("Threat Intelligence Data"). Threat Intelligence Data is collected by VMware for analysis and possible inclusion in a threat intelligence feed utilized by certain VMware Carbon Black service offerings. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in the customer's systems and other customers' systems and/or (ii) be anonymized and made un-attributable to any particular customer or individual (collectively "Un-attributable Threat Intelligence Data"). VMware may distribute Un-attributable Threat Intelligence Data to its customers at its discretion as part of its threat intelligence data feed or in published reports or research. By using a VMware Carbon Black Cloud service offering, the customer is deemed to have agreed that Un-attributable Threat Intelligence Data is not customer content, and VMware may retain, use, copy, and modify the Threat Intelligence Data for its internal business purposes, and additionally distribute and display the Un-attributable Threat Intelligence Data, for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed or in published reports and research. The information provided via any threat intelligence feed is provided on an "AS IS" and "AS AVAILABLE" basis only.

Updates and Upgrades to Sensor Software

VMware may release patches, bug fixes, updates, upgrades, maintenance and/or service packs ("Updates") for the Sensor Software from time to time, which may be necessary to ensure the proper function and security of the VMware Carbon Black Cloud service offerings. VMware is not responsible for performance, security, warranty breaches, support or issues encountered in connection with the VMware Carbon Black Cloud service offerings that result from a customer's failure to accept and apply Updates within a reasonable time frame.

2. Service Operations

The following outlines VMware's roles and responsibilities in providing the VMware Carbon Black Cloud service offerings. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not the duty of VMware or are assumed to be your responsibility.

2.1 Service Provisioning

VMware will provide the following provisioning services (for first-time customer purchases; not all items may apply for purchases by existing customers or for purchases of VMware Carbon Black Cloud Managed Detection):

- VMware will create an instance of the applicable cloud service offering for you.
- VMware will create a corresponding service account and send an email or other notification to the contact that you identified in your Order inviting that contact to the newly created instance via a URL to access the cloud service.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.

Your responsibilities include:

- Deploying and configuring the Sensor Software in the authorized endpoints, in the quantity purchased, to collect and route data into the Service Offering as needed.
- Configuring the Service Offering as needed.
- Maintaining accurate records of your use of the Sensor Software during the Subscription Term, and for 12 months after the effective termination date of your subscription, sufficient to show compliance with the Agreement. VMware has the right to audit those records. Any audit will be subject to reasonable prior notice and will not unreasonably interfere with your business activities. VMware may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. You must reasonably cooperate with VMware and any third-party auditor and you must, without prejudice to our other rights, address any non-compliance identified by the audit by paying any additional fees required as a result of that non-compliance. You must reimburse VMware for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the fees payable by you for the period audited, or that you have materially failed to maintain accurate records of Sensor Software use.

2.2 Disaster Avoidance and Disaster Recovery

The VMware Carbon Black Cloud service offerings are subject to a disaster recovery/business continuity policy. Notwithstanding the foregoing, any VMware Carbon Black Cloud service offering should not be considered the database of record for your data, and you should not rely on or consider that cloud service offering as the sole source of your data, nor a complete copy of your data.

2.3 Incident and Problem Management

VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which VMware has direct, administrative access and control, including servers and services used to provide the VMware Carbon Black Cloud service offerings.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Your account settings and configurations in the VMware Carbon Black Cloud service offering administrative management console.
- User-deployed and user-configured assets such as proxy agents.
- Third-party services to which you connect the VMware Carbon Black Cloud service offerings.
- Anything else not under VMware's direct control and administration.

2.5 Change Management

VMware will provide the following change management elements:

- Online documentation for all new material updates and upgrades to the VMware Carbon Black Cloud services.
- Processes and procedures relating to installation, upgrade and management of Sensor Software.

You are responsible for:

- Management of changes to your tagging process, alert settings, dashboards, and other content.
- Administration of self-service features provided through the VMware Carbon Black Cloud service offering's system console and user portal, up to the highest permission levels granted to you.
- Changes in the data collection agents used.
- Cooperating with VMware when planned or emergency maintenance is required.

2.6 Data Privacy

Service Operations Data

In connection with providing the Service Offering, VMware collects and processes information (such as configuration, performance, and log data) from VMware's software or systems hosting the Service Offering, and from the customer's systems, applications, and devices that are used with the Service Offering. This information is processed to facilitate delivery of the Service Offering, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, integrity, and stability of the Service Offering's infrastructure, and (iv) preventing or addressing service or technical issues. To the extent any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with VMware's Privacy Notice, including the VMware Products and Services Notice available at: https://www.vmware.com/help/privacy.html.

Usage Data

VMware Carbon Black Cloud offerings collect data (such as configuration, performance, and usage data) directly from VMware's software or systems hosting the Service Offering, and from the customer's systems, applications, and devices involved in the use of the Service Offering to improve VMware products and services, and your and your users' experiences as more specifically described at the VMware Trust & Assurance center, at: https://www.vmware.com/solutions/trustvmware.html.

See https://www.vmware.com/solutions/trustvmware/usage-data-programs.html.

With respect to user-entered values within configuration object names such as the machine names, host names or dashboard names, customer should not name such systems using confidential or personal data. To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with the VMware Privacy Notice, including the VMware Products and Services Notice available at:
https://www.vmware.com/help/privacy.html.

In connection with the collection of usage data, VMware and its service providers use cookies. Detailed descriptions of the types of cookies we can be found in the VMware Privacy Notices available at https://www.vmware.com/help/privacy.html. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link.

Additional controls may also be provided to users in the user interface.

You agree to provide the above information regarding the collection and use of usage data, including any available controls in relation to the cookies or tracking technology, including those provided by third parties, set forth in this section, to all users of the VMware Carbon Black service offerings.

Use of Google Analytics

VMware Carbon Black Cloud utilizes Google Analytics to collect data directly from any browsers used to access and use the Service Offering. The data collected and inferred is used by VMware to diagnose and improve its products and services, and to address issues. Further information on how Google collects and uses this data when you use the VMware Carbon Black Cloud offerings can be found at: www.google.com/policies/privacy/partners.

For users who wish to opt out of Google Analytics, Google makes the following browser add-on available: https://tools.google.com/dlpage/gaoptout.

You agree to provide the information in this section to all end users of any VMware Carbon Black Cloud service offering.

Data Retention and Deletion

During the subscription term, content will be deleted as detailed below.

VMware Carbon Black Cloud Endpoint Standard:

- Short term events are retained and available to the customer for a minimum of 30 days and a maximum of 32 days for search and investigation.
- Alerts and their associated event data ("long term events") are retained for a minimum of 180 days and a maximum of 210 days.

VMware Carbon Black Cloud Enterprise EDR:

- Endpoint data is stored for 30 days in the following two formats: (1) proprietary format for endpoint data optimized for fast retrieval, and (2) Solr indices.
- Raw protobufs (for troubleshooting purposes) are stored for 7 days.

VMware Carbon Black Cloud Audit and Remediation:

- The past query list is retained for 30 days.
- The results of a query are retained for 30 days (VMware stores up to 7,500 results per endpoint per day). The user can choose to export the results on their own device.

Live Response Feature

- Using the Live Response feature, your administrator may remote into a device to take an action. If the action involves getting a copy of a file, the file is temporarily captured in the session cache for the duration of the Live Response session and in any event is automatically deleted after 15 minutes of inactivity. This time frame is configurable.

Log Data

- During your Subscription Term, diagnostic logs are purged after seven days and audit logs are removed every 12 months.

Following expiration or termination of your subscription, all of your content, and all personal data contained in your content, will be deleted from VMware's primary database and (if applicable) back-up database in accordance with the applicable VMware retention schedule(s), unless: (i) VMware is required by applicable law to retain any of the personal data (in which case VMware will implement reasonable measures to isolate the personal data from any further processing), or (ii) VMware is otherwise permitted to retain the data in accordance with the Agreement.

3. Business Operations

Billing and Usage Metering

The VMware Carbon Black Cloud service offerings are sold on a per-Endpoint basis except as follows: (i) VMware Carbon Black Cloud Workload offerings may be priced on a per Endpoint, per-Processor, or per-Core basis (Core purchases are required and only available for use on VMware Cloud environments), (ii) when included in various multi-product bundles including VMware Workspace Security™ bundles and Advanced Security Bundle for VMware Cloud Foundation, components of those bundles may have additional or different metrics that apply as described in their respective Service Descriptions, and (iii) Carbon Black Cloud Container Essentials offerings may be priced on a per-Processor or per-Core basis.

For purposes of this Service Description:

- "Core" means a unit of measure that is defined based on the environment in which the product operates: (1) in a physical computing environment, a Core is a Physical Core; (2) in a virtualized or hypervisor (VM) computing environment, a Core is a single physical computational unit of the Processor which may be presented as one or more vCPUs; and (3) in a public cloud computing environment, a Core is defined as a single physical computational unit of the Processor, which may be presented as one or more vCPUs, but which may be named differently by the public cloud vendors (e.g., Amazon Web Services defines Core as "vCPU", Microsoft Azure defines Core as "Core" or "vCPU", Google Cloud Platform defines Core as "Virtual CPU", and Heroku defines Core as "Compute"). In cases where these proxies are *not* identified as Hyperthreads, one (1) proxy is recognized as one Core. In cases where these proxies *are* identified as Hyperthreads, two (2) proxies are recognized as one Core.
- **"**Endpoint**"** means the computer device(s) on which the Sensor Software is installed, including but not limited to laptops, desktops, tablets, point of sale devices, and servers.
- "Hyperthread" means a technology by which a single physical core is shared between two logical cores.
- "Node" means a single host/OS that runs containers. A Node can be a virtual or a physical machine.
- "Physical Core" means a single physical computational unit of the Processor.
- "Processor" means a single, physical chip that houses at least one, but not more than 32, Physical Cores that can execute computer programs. A physical chip

containing more than 32 Physical Cores requires the purchase of one additional subscription for every additional 32 (or portion thereof) Physical Cores in the Processor.

- "Virtual CPU" or "vCPU" means a single unit of virtual processing power configured to a Virtual Machine.
- "Virtual Machine" means a software container that can run its own operating system and execute applications like a physical machine.

All Cores existing in an environment must be covered by appropriate entitlements. You will be billed for committed fees and charges, in advance, and if applicable for overage charges in arrears.

VMware Carbon Black Cloud service offerings can be purchased for a committed term subscription of one, three, or five years. The subscription term begins on the date that we send a welcome email to the contact identified in your Order, which tells you how to download any on-premise components and log in to the service offering, and provides the needed credentials.

If you wish to purchase additional subscriptions, the Subscription Terms for those additional subscriptions may not always be coterminous with subscriptions already purchased.

Termination

Termination of your subscription will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the environments and configurations.

If you wish to extract your content from the VMware Carbon Black Cloud service offering (to the extent you have not already done so prior to termination of your Subscription Term), you must notify us within five (5) days after the effective termination date, and we will assist you in extracting your content from the VMware Carbon Black Cloud service offering. You will be responsible for all fees associated with content extraction. If you do not notify us within that five-day period, Your Content may be permanently deleted and may not be recoverable.