# VMware Carbon Black Cloud

## Privacy Datasheet

### ABOUT VMWARE CARBON BLACK

VMware Carbon Black Cloud delivers to your organization the key security transformation with cloud native endpoint protection that adapts to meet your needs. Find more details at *https://www.carbonblack.com*

### ABOUT VMWARE'S PRIVACY PROGRAM

- Trust Center – At VMware, we want to bring transparency that underlies trust. *The VMware Trust Center* is the primary vehicle to bring you that information.
- Data Privacy Officer - Please contact the VMware Privacy Team via the *Privacy Contact Form* or by mail at Office of the General Counsel of VMware, Inc., 3401 Hillview Ave, Palo Alto, California, 94304, USA.

## How VMware Carbon Black Cloud brings value to you!

VMware Carbon Black Cloud ("Carbon Black Cloud" or "the Service Offering") is a cloud native security solution designed to modernize your endpoint protection, bring more security related visibility, and simplify your already complex security stack. Using VMware Carbon Black Cloud, you can consolidate multiple endpoint security capabilities using one endpoint agent and console, cutting the management headaches and the console thrashing required when responding to potential incidents. All of this to enable you to minimize downtime responding to incidents and return critical CPU cycles back to the business.

The *VMware Carbon Black Cloud Platform* offers multiple interconnected security services. *VMware Carbon Black Cloud Endpoint Standard* offers next-generation antivirus and behavioural EDR collecting data on process creations, file and registry modifications, cross process events, network connections and binary meta data. Alongside this is *VMware Carbon Black Cloud Managed Detection* providing managed Endpoint Standard's alert monitoring and triage. Completing the response cycle, *VMware Carbon Black Cloud Audit and Remediation* provides real-time device assessment and remediation capabilities by processing the queries you run on the endpoint(s) and the query results (such as hardware or software inventory and files calling for action). *VMware Carbon Black Cloud Enterprise EDR* brings proactive threat hunting and incident response, and collects data on process creations, file and registry modifications, cross process events, network connections, binary files and binary meta data. *VMware Carbon Black Extended Detection and Response (XDR)* strengthens lateral security and unifies security tools so customers can see more and stop more by combining telemetry from endpoint detection and response (EDR) with network telemetry, intrusion detection system (IDS) observations, and identity intelligence.

For more information, see the description of the Carbon Black Cloud Service Offering in the Cloud Services Guide available here.

## VMware and Privacy

In a complex world of data and the digital era our goal is simple: At VMware, you, our customers, and your data are our primary concern. VMware takes privacy and data protection very seriously and is committed to providing clear information about how we collect, use and process your personal data. We have established policies and practices designed to protect the personal data we process on behalf of our customers (as a processor), and as a controller. We are also committed to privacy-by-design when developing products and services. VMware's Privacy Team actively works with the development teams to identify and embed privacy controls for customers.

The personal data collected and processed by VMware are largely dependent on the type of offering you purchase. This Privacy Datasheet provides you with information about how VMware processes and protects your personal data in connection with VMware Carbon Black Cloud Service Offering and associated components.

## Types of Data Collected by VMware Carbon Black Cloud

In connection with the customer's use and VMware's provision of the Cloud Service, VMware collects and processes data as classified in the table below. In some instances, personal data may be included in such data.  Generally, Carbon Black Cloud only processes the personal data of customer end users and customer IT administrators who manage the Carbon Black software for the organization.

| VMware Data Classification | Description and Purpose of processing | Categories of Personal Data |
|---|---|---|
| Customer Content | Content uploaded by customer or its users to the Cloud Service (as set forth in *VMware's General Terms*). To the extent the Cloud Service processes Customer Content, VMware processes such Content to provide the Service. | Generally, customer controls and determines which type of personal data it submits to the Cloud Service. The specific personal data processed will depend on the customer's specific configurations and deployment. |
| Support Request Content | Content uploaded or otherwise provided by customer to VMware to address a technical support issue (a "Support Service" under *VMware's General Terms*). | Any personal data customer shares with VMware in connection with a support request (as controlled and determined by Customer). |
| Account Data | Data collected and used by VMware to manage the customer account and maintain the relationship with customer, such as to bill the customer or deliver notifications and alerts. | Contact Information, such as customer name, email address, address and phone number.<br>Online Identifiers such as customer's IP address or login credentials. |

| | | |
|---|---|---|
| Service Operations Data | Data used by VMware to facilitate the delivery of the Cloud Service. This may include (i) tracking entitlements, (ii) providing support, (iii) monitoring the performance, integrity, and stability of the Service's infrastructure, and (iv) preventing or addressing Service or technical issues. For example:<br>• Configuration, usage and performance data<br>• Authentication Data<br>• Service logs, security logs, and diagnostic data | Contact Information, such as administrators' name and email address.<br>Online Identifiers such as administrators', developers' or users' IP address, login credentials or login time stamps.<br>See the below tables for detailed breakdown of data elements processed by each Carbon Black service offering. |
| Service Usage Data | Information used by VMware for analytics, product improvement purposes, and proactive support. See *VMware Trust & Assurance Center* for additional details regarding VMware's Service Usage Data Program (SUDP). For example:<br>• Configuration, usage and performance data<br>• Survey and feedback data | Contact Information, such as administrators' email address (e.g. to provide proactive support).<br>Online Identifiers such as administrators' or users' IP address. |

### *VMware Carbon Black Cloud Platform*

| Personal Data Category | Personal Data Attributes | Purpose of Processing |
|---|---|---|
| Identity Details | Console User's Email Address*<br>Console User's Full Name*<br>Console Username and Password*<br>Console User's Telephone Number* | Account creation and authentication for access to the platform, email notifications. This information is collected for all Carbon Black Cloud offerings.<br>** Authorized console users with tenant administrative access can edit/remove.* |

### *VMware Carbon Black Cloud Endpoint Standard*

*Next Generation Antivirus and Behavioral EDR*

| Personal Data Category | Personal Data Attributes | Purpose of Processing |
|---|---|---|
| Online Identifiers | Username associated with process**<br>User Identifiers (SID)**<br>FQDN and FQDN Final Destination**<br>Registry Data**<br>URL**<br>Command Line**<br>IP Addresses and Host Name<br>Last Logged-in User<br>Active Directory Distinguished Name (DN)<br>Device Name, ID and Serial Number | Detection and prevention for both known and unknown security attacks.<br>Threat Intelligence.<br>*** Items that are redacted or disabled via 'Private Logging Level' feature.* |
| *Other* | *File Name and File Path*<br>*Full Binary**** | *Detection and prevention for both known and unknown security attacks.*<br>*Threat Intelligence.*<br>**** Binary file detonation feature provided by a sub-processor (off by default, not enabled in VMware Government Services deployment)* |

### *VMware Carbon Black Cloud Managed Detection*

*Dedicated Managed Alert Monitoring and Triage services*

| Personal Data Category | Personal Data Attributes | Purpose of Processing |
|---|---|---|
| Online Identifiers | Username associated with process**<br>User Identifiers (SID)**<br>FQDN and FQDN Final Destination**<br>Registry Data**<br>URL**<br>Command Line**<br>IP Addresses and Host Name<br>Last Logged-in User<br>Active Directory Distinguished Name (DN)<br>Device Name, ID and Serial Number | Monitoring, triage, and alert management activities.<br>Detection and prevention for both known and unknown security attacks.<br>Managing actionable alert information and false positive reduction.<br>Threat Intelligence.<br>*** Items that are redacted or disabled via 'Private Logging Level' feature within the Carbon Black Endpoint Standard.* |
| Other | File Name and File Path<br>Full Binary | Monitoring, triage, and alert management activities.<br>Detection and prevention for both known and unknown security attacks.<br>Managing actionable alert information and false positive reduction.<br>Threat Intelligence. |

### *VMware Carbon Black Cloud Enterprise EDR and XDR*

*Cloud Based Threat Hunting and Incident Response*

| Personal Data Category | Personal Data Attributes | Purpose of Processing |
|---|---|---|
| Online Identifiers | Username associated with process<br>User Identifiers (SID)<br>FQDN and FQDN Final Destination<br>Registry Data URL<br>Command Line<br>IP Addresses and HostName<br>Last Logged-in User<br>Active Directory Distinguished Name (DN)<br>Device Name, ID and Serial Number<br>Authentication Events<br>Network adapter information *<br>HTTP Request Line Including Query Parameters **<br>HTTP Request Headers **<br>TLS handshake information and TLS JA3 fingerprint *** | Hunting, detection, and tracking of known and unknown attack vectors.<br>Response to security incidents and attacks.<br>Analysis of malware and attacker activities and techniques.<br>Threat Intelligence.<br>* XDR only.<br>** XDR only. Collected only for unencrypted (http://) network connections.<br>*** XDR only. Specific only to encrypted network connections. |
| Other | File Name and File Path<br>Full Binary** | Hunting, detection, and tracking of known and unknown attack vectors.<br>Response to security incidents and attacks.<br>Analysis of malware and attacker |

| | | |
|---|---|---|
| | | activities and techniques.<br>Threat Intelligence.<br>*** Raw file contents for any executable under25 MB not yet observed in the wild by the VMware Carbon Black software reputation catalog or another VMware Carbon Black customer (off by default).* |

### *VMware Carbon Black Cloud Audit and Remediation*

*Real Time Device Assessment and Remediation*

| Personal Data Category | Personal Data Attributes | Purpose of Processing |
|---|---|---|
| Online Identifiers | Username associated with process**<br>User Identifiers (SID)<br>Device IP address and Host Name<br>Device MAC address<br>Device/host name and string number<br>Username<br>Endpoint location (city level) | Endpoint identification<br>Allow visibility into environment by asking questions and examining results:<br>1. Install or uninstall applications or services<br>2. Update or patch installed applications, services, hardware drivers, or firmware<br>3. Manage installed applications or services<br>4. Start or stop services<br>5. Manage Assets<br>6. Access and/or add, remove, or modify files or the contents of files or get a copy of a memory dump or a file. |
| Other | File Name and File PathFull Binary<br>Personal data may appear within the names of the various applications, software or folders created by a user | Endpoint identification<br>Allow visibility into environment by asking questions and examining results:<br>1. Install or uninstall applications or services<br>2. Update or patch installed applications, services, hardware drivers, or firmware<br>3. Manage installed applications or services |

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

- All compliance certifications are available in the *VMware Trust Center's Compliance Page.*

| | | |
|---|---|---|
| | | 4. Start or stop services<br>5. Manage Assets<br>6. Access and/or add, remove, or modify files or the contents of files or get a copy of a memory dump or a file. |

Personal data other than listed above may also be included in any content that the customer submits to the Service Offering. VMware may not know what types of personal data are submitted to the Service Offering by the customer and the customer is responsible for understanding the types of personal data processed in connection with the customer's use of the Service Offering.

## How We Process and Protect Data as a Controller

To the extent VMware processes personal data as part of Account Data, Service Operations Data and Service Usage Data, VMware acts as the Controller in respect to such personal data. The following privacy notices explain how VMware collects, uses and protects any personal data in its capacity as a Controller:

> *VMware Privacy Notice:* This notice addresses the personal data we collect when you purchase VMware products and services and provide account-related personal data.
>
> *VMware Products and Services Privacy Notice:* This notice applies only to the limited personal data we collect and use for our own purposes in connection with our provision of VMware products and services, including (i) any cookies and similar tracking technologies we may use when providing the products or services; (ii) any information we use to facilitate the delivery of VMware services; and (iii) any data we collect to improve our products and services and our customer's experience.

## How We Process and Protect Data as a Processor

Where VMware processes personal data contained in Customer Content in connection with the provisioning of the Cloud Service, VMware will process such personal data on behalf of the customer as a "processor" (acts on the instruction of the controller). The customer is the "controller" of any personal data contained in Customer Content and determines the purposes of the processing.

### Data Protection Addendum

VMware's obligations and commitments as a data processor are set forth in VMware's *Data Processing Addendum* ("DPA"). VMware will process personal data contained within Customer Content in accordance with the DPA and VMware General Terms available *here*.

### Data Storage and Cross-Border Data Transfers

VMware Carbon Black Cloud currently stores Customer Content in data centers located in Australia, Germany, Japan, United Kingdom or United States, except for VMware Carbon Black Cloud Managed Detection which is only available in Australia and the United States Hosting location options may be added from time to time so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery location details.

### DATA PRIVACY REQUESTS

If you wish to exercise any of your rights under applicable data privacy laws for personal data processed by your organization while using the Cloud Service, please contact your organization. See *VMware's Privacy Notice* for information about how to exercise your rights where VMware is processing personal data in connection with its business operations.

### FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Contact your VMware account representative or call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller.

### UPDATES

Reading from a PDF? Don't be outdated, be informed! Find the latest information in the current version of this document from the *VMware Trust Center's Privacy Page*.

For cross-border personal data transfers from the EEA, Switzerland, the UK and the US, VMware relies on recognized data transfer mechanisms such as the EU Standard Contractual Clauses, including the Data Privacy Framework when we are acting as a processor and transfer personal information between our customer and VMware Group members and within the VMware Group members.

## Sharing with Sub-Processors

For the Cloud Service, VMware utilizes third-party companies to provide certain services on its behalf. As set forth in the *Data Processing Addendum*, VMware has agreements and data transfer mechanisms in place with each sub-processor. A list of these sub-processors is available *here*.

Additional sub-processors providing technical support functionality for the Service Offering is available in the *Support Services Sub-Processor List.*

VMware also provides customers with an easy mechanism to monitor changes to our list of sub-processors. If you would like to receive notifications, you can subscribe through the *Sub-processor page on VMware ONE Contract Center*.

## Data Retention and Deletion Practices

VMware retains personal data collected in connection with the customer's use of the Cloud Service for as long as it is needed to fulfill the obligations of the VMware General Terms.

The *VMware Data Processing Addendum* and Service Guide (visit *VMware ONE Contract Centre* for the service specific guide) set forth how personal data contained in Customer Content is deleted after contract expiration or termination. Upon termination of your account, Customer Content will be retained by backup systems for up to 90 days. VMware advises you to retrieve any data you wish to retain before the account termination takes place. VMware has no obligation to retain data beyond 30 days of the effective termination date.

During the subscription term Customer Content retention is as follows:

VMware Carbon Black Cloud Endpoint Standard:

- Short term events are retained and available for customer for a minimum of 30 days and a maximum of 32 days for search and investigation.
- Alerts & 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 Managed Detection:

- Customer Content is deleted upon termination of your account.

VMware Carbon Black Cloud Enterprise EDR and XDR

- 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 usage of VMware Carbon Black Cloud diagnostic logs are purged after seven days and audit logs are removed every 12 months.