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

- Cloud Trust Center – At VMware, we want to bring transparency that underlies trust. *The VMware Cloud Trust Center* is the primary vehicle to bring you that information.
- Data Privacy Officer - Please contact VMware's Privacy Team at *privacy@vmware.com* 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.

There are currently 4 key offerings within the VMware Carbon Black Cloud Platform. VMware Carbon Black Cloud Endpoint Standard offers next-generation antivirus and behavioral 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). Finally, 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.

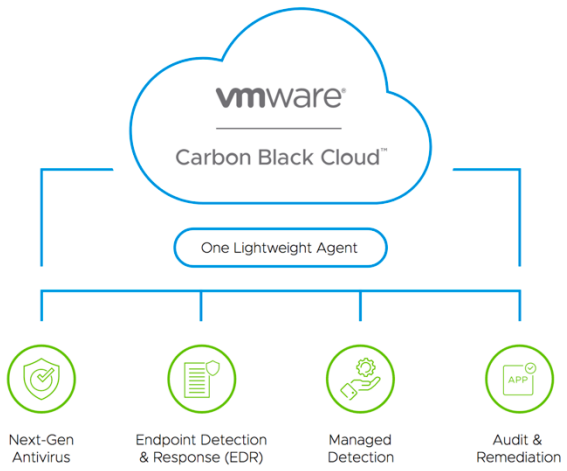

FIGURE 1: VMware Carbon Black Cloud

For more information, see the *Carbon Black Cloud Service Description*.

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 designing our products and services and VMware's Privacy Team 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 the VMware Carbon Black Cloud Service Offering and associated components.

Types of Personal Data Collected by VMware Carbon Black Cloud

VMware collects and further processes the following categories and types of personal data in connection with the provision of the Service Offering to the Customer.

VMware Carbon Black Cloud Endpoint Standard

Next Generation Antivirus and Behavioral EDR

Personal Data Category	Personal Data Attributes	Purpose of Processing
Identity Details	Administrator Email Addresses* Administrator's Full Name* Administrator's Username and Password* Administrator's Telephone Number*	Account creation and authentication for access to the platform, email notifications. ** Authorized administrators can edit/remove. Will be purged after end of business relationship.*

Online Identifiers	Username associated with process** User Identifiers (SID)** FQDN and FQDN Final Destination** Registry Data** URL** Command Line** IP Addresses and Host Name Last Logged-in User Active Directory Distinguished Name (DN) Device Name, ID and Serial Number	Detection and prevention for both known and unknown security attacks. Threat Intelligence. *** Items that are redacted or disabled via 'Private Logging Level' feature.*
Other	File Name and File Path Full Binary***	Detection and prevention for both known and unknown security attacks. Threat Intelligence. **** Binary file detonation feature provided by a sub-processor (off by default)*

VMware Carbon Black Cloud Managed Detection

Dedicated Managed Alert Monitoring and Triage services

Personal Data Category	Personal Data Attributes	Purpose of Processing
Identity Details	Administrator Email Addresses Administrator's Full Name	Sending out the reports generated by the Service Offering, email notifications.

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

VMware Carbon Black Cloud Enterprise EDR

Cloud Based Threat Hunting and Incident Response

Personal Data Category	Personal Data Attributes	Purpose of Processing

Identity Details	Administrator Email Addresses* Administrator's Full Name* Administrator's Username and Password* Administrator's Telephone Number*	Account creation and authentication for access to the platform, email notifications. ** Authorized administrators can edit/remove. Will be purged after end of business relationship.*
Online Identifiers	Username associated with process User Identifiers (SID) FQDN and FQDN Final Destination Registry Data URL Command Line IP Addresses and Host Name Last Logged-in User Active Directory Distinguished Name (DN) Device Name, ID and Serial Number	Hunting, detection, and tracking of known and unknown attack vectors. Response to security incidents and attacks. Analysis of malware and attacker activities and techniques. Threat Intelligence.
Other	File Name and File Path Full Binary***	Hunting, detection, and tracking of known and unknown attack vectors. Response to security incidents and attacks. Analysis of malware and attacker activities and techniques. Threat Intelligence. *** Raw file contents for any executable under 25MB 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
Identity Details	Administrator Email Addresses* Administrator's Full Name* Administrator's Username and Password* Administrator's Telephone Number*	Account creation and authentication for access to the platform, email notifications. ** Authorized administrators can edit/remove. Will be purged after end of business relationship.*
Online Identifiers	Username associated with process** User Identifiers (SID) Device IP address and Host Name Device MAC address Device/host name and string number Username Endpoint location (city level)	Endpoint identification Allow visibility into environment by asking questions and examining results: 1. Install or uninstall applications or services 2. Update or patch installed applications, services, hardware drivers, or firmware 3. Manage installed applications or services 4. Start or stop services 5. Manage Assets 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.

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

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

Other	File Name and File Path Full Binary Personal data may appear within the names of the various applications, software or folders created by a user	Endpoint identification Allow visibility into environment by asking questions and examining results: 2. Install or uninstall applications or services 3. Update or patch installed applications, services, hardware drivers, or firmware 4. Manage installed applications or services 7. Start or stop services 8. Manage Assets 9. 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 Protect Data Processed in Connection with the Operation of Our Business (as a Controller)

In connection with VMware's provision of the Service Offering to the Customer, VMware processes the types of data shown in the below table related to the platform, which may include personal data. In this instance, VMware is acting as a "controller" and determines the purposes of the processing.

Type of Data	Purposes for which it is used
Relationship Data – Authentication and customer account information	Used to provision the Service Offering, such as managing the account and maintaining relationship data
Service Operations Data – Configuration Data, Feature Usage Data, Authentication Data, Performance Data, Service Logs, Security Logs, Diagnostic Data, Support and Survey Data.	Information used to facilitate the delivery of the Service Offering, including managing and monitoring the infrastructure, and providing support. See *VMware Products and Services Privacy Notice* for details.
Service Usage Data – Configuration Data, Feature Usage Data, Performance Data.	Information used for VMware's own analytics and product improvement purposes See *VMware Service Usage Data Program disclosure* for details.

The following privacy notices explain the different ways in which VMware collects, uses and protects any personal data included in the above categories of data:

VMware Privacy Notice: This notice addresses the personal information we collect when you purchase VMware products and services and provide account-related personal information.

VMware Products and Services Privacy Notice: This notice applies only to the limited personal information 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 Protect Data as a Service Provider (as a Processor)

In connection with the provisioning of the Service Offering, VMware will process personal data contained in Customer Content (as such term is defined in the relevant VMware agreement, e.g. *VMware Terms of Service*) on behalf of the Customer. In this instance, VMware is acting as a "processor" (acts on the instruction of the controller), while the Customer has the role of the "controller" (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 applicable agreement and the DPA. The applicable agreements for each product and service, including the VMware Terms of Service, the Service Descriptions for each specific service, and other relevant legal document can be found *here*.

Data Storage and Cross-Border Data Transfers

VMware Carbon Black Cloud currently enables you to choose the data storage location for Customer Content from the following geographic regions: United States, Germany or Japan, except for VMware Carbon Black Cloud Managed Detection which is only available in the United States. Hosting location options are constantly evolving so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery location details.

For cross-border personal data transfers, VMware has achieved Binding Corporate Rules ("BCR") as a processor, thus acknowledging we have met the standards of the EU General Data Protection Regulation for international transfers of personal data it processes on behalf of our customers. View the VMware BCR or the EU Commission BCR Listing in the *VMware Cloud Trust Center*.

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 Service Offering, 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 Cloud Trust Center's Privacy Page*.

Sharing with Sub-Processors

For the Service Offering, VMware utilizes 3rd-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 full list of these sub-processors is available *here*.

Additional sub-processors providing supporting functionality for the Service Offering is available in the *Support Services Sub-Processer List*.

Data Retention and Deletion Practices

VMware retains personal data that we may collect in connection with the customer's use of the Service Offering for as long as it is needed to fulfill the obligations of the VMware Terms of Service. The *VMware Data Processing Addendum*, the *Terms of Service,* and the *Service Description* set forth how personal data contained in Customer Content is deleted after contract expiration or termination.

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

- 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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.