



VMware Carbon Black PCI Compliance

The following document identifies how VMware Carbon Black products meet PCI 3.2 requirements. This document is a modified version of our complete mapping matrix, please contact your VMware Carbon Black representative for any further inquiries.

PCI DSS REQUIREMENT 1.4		
Install personal firewall software or equivalent functionality on any portable computing devices that connect to the Internet when outside the network and which are also used to access the CDE.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Today's modern threats look like normal traffic, making personal firewalls less effective. VMware Carbon Black Cloud Endpoint Standard can block or detect malicious activity including, memory scraping, lateral movement, credential theft, persistence, command & control communication and more.	VMware Carbon Black Cloud Enterprise EDR provides real-time visibility into inbound/outbound network connections, and critical system resources within your organization. Contextual analysis allows you to inspect every file on all endpoints and determine if an unknown or malicious file attempted an unauthorized network connection.	VMware Carbon Black App Control's positive security model (application whitelisting), offers complete control and visibility over what processes are allowed to run on an endpoint. Configurable policy settings block or permit execution of unapproved scripts, executables, file names and file hashes. Tamper protection applies rules that prevent disabling a Carbon Black App Control Agent. Through Carbon Black App Control's Console enterprises can perform real-time asset inventory and determine which endpoints configurations are up to date. Endpoints are searchable via IP Address, name, or policy.
PCI DSS REQUIREMENT 2.2		
System configurations and default tracking: Develop configuration standards for all system components and assure that these standards address all known security vulnerabilities consistent with industry accepted system hardening standards.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Carbon Black's streaming analytics engine collects all activity on the endpoint and alerts on behaviors that deviate from normal. Carbon Black Cloud Endpoint Standard allows users to create and assign policies, which gives complete control over the security configuration on each endpoint.	Similar to a security camera, Carbon Black Cloud Enterprise EDR is "always on," surveying the activity on your endpoints. Without processor heavy scanning, Carbon Black EDR can identify the existence of a vulnerable application.	Track changes to system configuration as well as the removal of applications, utilities, and drives with Carbon Black App Control. Ensure your system hardening configurations are maintained with compliance drift reporting.

PCI DSS REQUIREMENT 5.1.1 & 5.1.2 Ensure that all antimalware programs are capable of detecting, removing and protecting against all known types of malicious software. For systems considered to be not commonly affected by malicious software, perform periodic evaluations to confirm they do not require antivirus software.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Carbon Black's NGAV offers breakthrough streaming prevention technology with detection and EDR capabilities on a single lightweight agent to help secure laptops, servers, and virtual workloads.  Direct Control	Carbon Black Cloud Enterprise EDR provides real-time visibility into inbound/outbound network connections, and critical system resources within your organization. Contextual analysis allows you to inspect every file on all endpoints and determine if an unknown or malicious file attempted an unauthorized network connection.	Carbon Black App Control stops cyber threats that evade antivirus and other traditional defenses including zero-day and targeted attacks. Carbon Black App Control provides visibility into everything running on your endpoints and servers; signature-less detection and prevention of advanced threats; and a recorded history of all endpoint and server activity to rapidly respond to alerts and incidents.  Direct Control
PCI DSS REQUIREMENT 5.2 Verify that AV software is kept up to date, examine AV configurations to ensure automatic updates and scans are enabled. Also, confirm AV software log generation is enabled and logs are retained in accordance with PCI DSS requirement 10.7.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Carbon Black Cloud Endpoint Standard collects and transmits unfiltered data in real-time to the VMware Carbon Black Cloud. By applying streaming analytics to that data, consisting of behavioral analytics, machine learning, reputation scoring and real-time signature analysis, Carbon Black Cloud Endpoint Standard goes beyond traditional antivirus and even machine learning AV to predict threats never seen before. The Carbon Black Cloud provides unrivaled visibility into your attack landscape and is always up-to-date with the latest threat intelligence. All Events are stored for 30 days, events associated with an alert for 90.	Similar to a security camera, Carbon Black Cloud Enterprise EDR is "always on," surveying the activity on your endpoints. Without processor heavy scanning, Carbon Black EDR can identify the existence of a vulnerable application.	Carbon Black App Control offers a unique solution to protecting your systems from malware. Instead of relying on traditional AV definitions, Carbon Black App Control only allows trusted processes to execute. Carbon Black App Control was the only solution to stop 100% of attacks in NSS Labs' 2017 Advanced Endpoint Protection (AEP) test.  Direct Control

PCI DSS REQUIREMENT 5.3 & 5.4 Ensure AV mechanisms are current, running and generating audit logs. Verify that the AV software cannot be disabled or altered by users. Certify that all procedures for protecting systems against malware are documented and affected parties are aware of said policies.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Carbon Black Cloud Endpoint Standard Sensors cannot be disabled or altered without inputting a unique, randomly-generated code. This code is only available to administrators within the Carbon Black Cloud Endpoint Standard Management Console. Carbon Black Cloud Endpoint Standard provides extensive reporting features that can aid in the manual practice of ensuring compliance with your malware policies.  Direct Control		Carbon Black App Control continuously monitors and records all activity on endpoints and servers. Carbon Black App Control cannot be disabled by the user, ensuring your organization continuous coverage. Carbon Black App Control helps enforce compliance policies and puts mechanisms in place to inform and educate end users on established procedures.  Direct Control
PCI DSS REQUIREMENT 6.1 Develop and maintain secure systems and applications. Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities and file assets.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Carbon Black Cloud captures unfiltered endpoint data from millions of devices across our customer footprint and centralizes the data in the cloud. That data is enriched with intelligence from threat feeds and processed to identify threat patterns that are invisible to other solutions. By collecting and analyzing this unfiltered data, the platform can make predictions about, and protect against, future and unknown attacks. Carbon Black Cloud Endpoint Standard scores and prioritizes the relative importance of an alert then correlates the signal to its appropriate stage in the cybersecurity kill-chain.	Carbon Black Cloud Enterprise EDR utilizes the US-CERT threat intelligence feed and the National Vulnerability Database to identify the presence of vulnerable applications within the enterprise.	Carbon Black App Control's Software Reputation Service, combined with internal IT approvals of established policies, enables organizations to apply real-time, proactive threat and trust measurements to their asset inventory, discover potential risky files and enforce policy-based control on all endpoints. Carbon Black App Control's asset reporting applies threat and trust ratings to every file within the infrastructure, providing immediate low-friction analysis and risk ranking of any potential file vulnerability discovered.

PCI DSS REQUIREMENT 10.1 & 10.2.1-10.2.3

Verify through observation and interviewing the system admin, that, audit trails are enabled & active and access to system components is linked to individual users. Verify - Access to card-holder data, root/admin privileges and access to audit trails are logged.

CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Carbon Black Cloud Endpoint Standard collects technical artifacts about potentially suspicious activity on your endpoints, to detect suspicious behavior and investigate compromises. Carbon Black Cloud identifies and alerts you when cardholder data is accessed by searching for events with the Tactics, Techniques, and procedures (TTP) tag, Access_data_Files. The Carbon Black Cloud logs and stores all user access to the Defense counsel. Carbon Black Cloud Endpoint Standard can alert when an administrator logs-in from a suspicious IP address.	Carbon Black Cloud Enterprise EDR lets you define the types of events recorded by each sensor. The sensor can record the username associated with each running process. Carbon Black EDR watchlists can alert you if a privileged account ever runs any process outside of their normal behavior. Carbon Black gives you the ability to look beyond the logs into the real behavior of your most powerful users. Carbon Black EDR keeps an audit trail of user activity on the console. Within the audit trail, you see the full date and time that the user logged in the console, plus the associated IP address.	

PCI DSS REQUIREMENT 10.5.5

Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.

CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
	Carbon Black Cloud Enterprise EDR can alert on file creation, modification, and deletion activity through customizable watchlists.	Carbon Black App Control provides direct coverage for both file-integrity monitoring and control. Carbon Black App Control can block unauthorized writes to log files or any critical files on your endpoints. Carbon Black App Control ensures that only authorized processes can write or update log and critical files.  Direct Control

PCI DSS REQUIREMENT 11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
Through the collection of unfiltered data and streaming analytics the Carbon Black Cloud continually identifies threat patterns that are invisible to other solutions. With this intelligence, the Platform has the ability to identify intrusions which allows Carbon Black Cloud Endpoint Standard to act as a Host Based Intrusion Detection System.		Carbon Black App Control combines application control, file integrity monitoring, device control and memory protection for the strongest system lockdown. This approach stops malware and non-malware attacks by preventing unwanted change. Note that Carbon Black App Control is not on the perimeter, but is safeguarding the endpoint and CDE from being compromised based on the default deny policies.
PCI DSS REQUIREMENT 11.5 Deploy a change-detection mechanism to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.		
CARBON BLACK CLOUD ENDPOINT STANDARD	CARBON BLACK CLOUD ENTERPRISE EDR	CARBON BLACK APP CONTROL
	Only Carbon Black Cloud Enterprise EDR provides unfiltered visibility, fast analysis and a remote remediation toolset that enables fast, end-to-end incident endpoint detection and response. Capture all threat activity with continuous recording and centralized storage means the data you need is always at your fingertips.	With Carbon Black App Control, your organization can enforce the integrity of your deployment configurations, continuously monitor critical-system activity and assess compliance risk. Carbon Black App Control combines application control, file integrity monitoring, device control and memory protection for the strongest system lockdown. ✔ Direct Control