5.2WHITE PAPER

VMWARE CARBON BLACK CLOUD

ENDPOINT STANDARD

PCI DSS APPLICABILITY WHITE PAPER

vmware Carbon Black

NICK TRENC | CISA, CISSP, PCI SSLCA, PCI SSA, CISSP, CISA, QSA (P2PE), PA-QSA (P2PE), QPA

LYLE MILLER | CISA, CISSP, QSA, PA-QSA, SSA, SSLC

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

VMware, Inc. (VMWare) engaged Coalfire Systems, Inc. (Coalfire), a respected Qualified Security Assessor (QSA) for the Payment Card Industry (PCI) and Payment Application Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of their VMware Carbon Black Cloud Endpoint Standard endpoint protection and next-generation anti-virus platform. Coalfire conducted assessment activities including technical testing, an architectural assessment, and a compliance validation.

In this paper, Coalfire will describe that the Endpoint Standard solution meets the PCI Data Security Standard (PCI DSS) v3.2 Requirement 5, the anti-malware requirement, based on the sample testing and evidence gathered during this assessment, and the additional ways Endpoint Standard can assist in meeting other PCI DSS requirements.

The original edition of this white paper was published in September 2017 for Carbon Black, Inc. (Carbon Black), which was acquired by VMware in October 2019. A version of this white paper was updated in July 2018 with additional lab testing. This version is an update to those editions and includes testing on an additional operating system. This version was published in April 2020.

ABOUT VMWARE CARBON BLACK CLOUD ENDPOINT STANDARD

VMware Carbon Black Cloud Endpoint Standard is a next-generation application whitelisting and anti-virus solution for desktops, laptops, and servers that protects computers from the full spectrum of modern cyber-attacks using a combination of endpoint agent, server back-end, and cloud-based technologies.

The application whitelisting functionality allows the user or administrator to restrict any process and software from running on the system and therefore increases security of the system by minimizing risk of running any processes other than those intended by the administrator.

Additionally, Endpoint Standard's deep analytic approach inspects files and identifies malicious behavior to block both malware and increasingly common malware-less attacks that exploit memory and scripting languages like PowerShell.

VMware Carbon Black Cloud Endpoint Standard is a next-gen antivirus platform. The components of the solution include:

1. Carbon Black Cloud Agent – Client-side process for monitoring local systems in accordance with policies set within the Carbon Black Cloud Server. Which can either run as a background process with no user interface or with a notification tray-based icon that gives details on current system threats and blocked actions.
2. Carbon Black Cloud Server – Web-accessible platform for deploying agents, managing threats, and gaining an overall picture of an environment's threat landscape.

VMware Carbon Black Cloud Endpoint Standard Agent supports the following operating systems:

- Windows 8, 8.1 and 10
- macOS X: 10.12, 10.13, 10.14, 10.15
- Linux RedHat (RHEL) and CentOS 6/7

Carbon Black Cloud Agent also supports the following servers: Windows 2012, Windows 2012 R2, Windows 2016, and Windows 2019.

AUDIENCE

This assessment white paper has three target audiences:

1. **QSA and Internal Audit Community:** This audience may be evaluating VMware Carbon Black Cloud Endpoint Standard to assess a merchant or service provider environment for PCI DSS.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating VMware Carbon Black Cloud Endpoint Standard for use within their organization for compliance requirements other than PCI DSS.
3. **Merchant and Service Provider Organizations:** This audience may be evaluating Endpoint Standard for deployment in their cardholder data environment and the benefits that could be achieved from using this solution.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using the below industry and audit best practices. Coalfire conducted technical lab testing in our Colorado lab from October 3, 2016, to October 7, 2016. Further testing was completed from July 2, 2018, to July 11, 2018 to review additional features and PCI DSS requirements supported by Endpoint Standard. Additional testing for the current edition of this paper was conducted in Coalfire's lab from April 9, 2020, to April 10, 2020. At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full solution and its components.
2. Implementation of the Carbon Black Cloud Agent software in the Coalfire lab environment.
3. Introduction of malware binaries on local systems with Carbon Black Cloud Agent software installed.
4. Confirmation of the VMware Carbon Black Cloud Endpoint Standard platform's ability to block and remove known malware samples.
5. Review of additionally supported capabilities and functionalities that allow Endpoint Standard to assist organizations in meeting PCI DSS requirements beyond Requirement 5.

SUMMARY FINDINGS

The following findings are relevant highlights from the original assessment. Coalfire observed the findings remain valid for testing performed in April 2020:

- When properly implemented following vendor guidance, the VMware Carbon Black Cloud Endpoint Standard platform provided coverage for PCI DSS Requirement 5 based on the sample testing and evidence gathered during this assessment.
- The VMware Carbon Black Cloud Endpoint Standard platform was able to detect and effectively block the execution of the provided known malware samples.
- The VMware Carbon Black Cloud Endpoint Standard platform was able to effectively remove all provided known malware samples.
- The VMware Carbon Black Cloud Endpoint Standard platform adequately generated logs of events such that malicious activity could be traced in accordance with PCI DSS requirements.
- Endpoint Standard can be prevented from being disabled by unauthorized users.

- Endpoint Standard can also provide additional policy protections to include application whitelisting and blacklisting, preventing processes from accessing the network, preventing processes from scraping memory of other processes, preventing processes from injecting code or modifying memory of another process, or trying to execute code from memory.

Figure 1 below shows the different policy protection settings that can be assigned to enrolled systems.

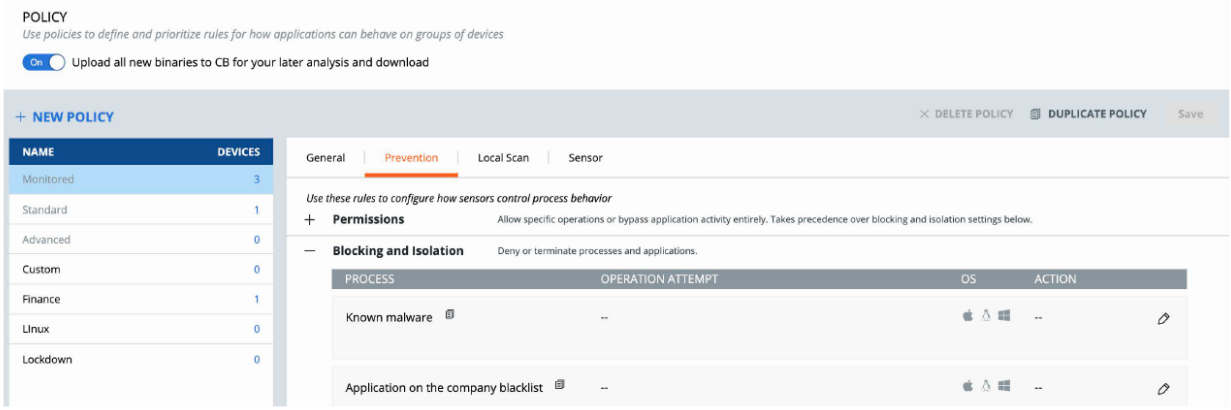

Figure 1 - Example of policy protection settings

ASSESSOR COMMENTS

The scope of this assessment put a significant focus on validating the use of Endpoint Standard in a PCI DSS environment, specifically to include its impact on PCI DSS Requirement 5. Endpoint Standard, when properly implemented following guidance from VMware Carbon Black, can be utilized to meet the technical portions of PCI DSS Requirement 5. However, as most computing environments and configurations vary drastically, it is important to note that use of this product does not guarantee security and even the most robust anti-virus can fail when improperly implemented. A defense-in-depth strategy that provides multiple layers of protection should be followed as a best practice. Please consult with VMWare Carbon Black for policy and configuration questions and best practices.

Also, it should not be construed that the use of Endpoint Standard guarantees full PCI DSS compliance. Disregarding PCI requirements and security best practice controls for systems and networks inside or outside of PCI DSS scope can introduce many other security or business continuity risks to the merchant. Security and business risk mitigation should be any merchant's goal and focus for selecting security controls.

TECHNICAL ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the potential PCI DSS coverage of the solution:

1. Analysis of the architecture and configuration of the solution in accordance with vendor guidelines.
2. Deployment of Carbon Black Cloud Agent software to test machines along with enablement of strict policies to enforce the detection and prevention of known malware. Examination of Carbon Black Agent configuration to confirm protection cannot be turned off by non-administrators.

3. Execution of known malware samples (to include virus, ransomware, Trojans, rootkits, adware, and worms) deliberately propagated to test machines.
4. Review of backend component for verification of detection, execution prevention, and removal of all test samples. Evaluation of backend component for verification that agents are deployed, communicating, up-to-date, performing periodic scans, and protecting against real-time threats.
5. Review of backend component for verification of ability to assist organizations in meeting a variety of PCI DSS requirements.

ASSESSMENT ENVIRONMENT

Carbon Black Cloud Agents were installed on the following machines:

- Mid-2011 MacBook Air Model A1370 running a freshly installed copy of macOS X Sierra 10.12 including only the default system applications installed and no other antivirus running.
- Dell Latitude E6420 laptop running a freshly installed copy of Windows 10 with all Windows updates installed and Windows Defender fully disabled via system registry.
- Dell Latitude E6420 laptop running a freshly installed copy of Windows 8.1 with all Windows updates installed and Windows Defender fully disabled via system registry.
- CentOS 7.0 virtual machine running a fresh copy of Carbon Black Cloud Agent with no other antivirus software installed or running on the system.

TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this application security review included:

MALWARE SAMPLES	DESCRIPTION
Live Malware Samples	Sample binaries of known malware for both macOS X, Windows, and Linux: • Sample macOS malware obtained from Objective-See at https://objective-see.com/malware.html/ • Sample Windows malware obtained from the Zoo aka Malware DB at http://thezoo.morirt.com/ • Sample Linux malware obtained from Zoo aka Malware DB at https://github.com/greg5678/Malware-Samples

*Note – The above malware sample sites are intentionally not clickable links. Visiting and downloading from the above sites may lead to malware infection. It is highly recommended against doing so.

REFERENCES

VMware Carbon Black Cloud Endpoint Standard website - https://www.carbonblack.com/products/endpoint-standard/

PCI Data Security Standard, v3.2.1 – https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

APPENDIX A: PCI REQUIREMENTS COVERAGE MATRIX

PCI DSS REQUIREMENTS

Key:
Compliance directly supported via use of the VMware Carbon Black Cloud Endpoint Standard platform = ✓

Requires merchant action for full compliance = ✓

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
2.4 Maintain an inventory of system components that are in scope for PCI DSS	2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	✓	For all system components running a Carbon Black Cloud Agent, administrators can utilize the Carbon Black Cloud server to assist in creating and managing a system inventory. Merchants running Endpoint Standard will still be responsible for maintaining the accuracy and enrolling new systems within Endpoint Standard to make sure the inventory is accurate, as well as exporting this list to include a description of functions for said devices. Merchants must also identify all systems that are not covered by Endpoint Standard.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	✓	Endpoint Standard allows users to directly deploy agents to Windows, macOS, and Linux. It also allows direct monitoring of any device via agentless. The cloud monitoring portal shows the status of monitoring for all enrolled devices.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting	5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;	✓	Endpoint Standard performs signature checking against well-known virus repositories. As a result, Endpoint

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
against all known types of malicious software.	• Detect all known types of malicious software, • Remove all known types of malicious software, and • Protect against all known types of malicious software. Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.		Standard is known for the ability to detect known malware, block them from running, and remove them when requested by an administrator. Testing showed that Endpoint Standard was able to detect, block, and remove several examples of viruses, Trojans, ransomware, rootkits, and other known malware.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	5.1.2 Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	✓	This is a policy and procedure based requirement. Merchants must periodically evaluate the systems they use to ensure the systems are not considered commonly affected. Endpoint Standard can support this by using agentless installs to monitor any system to include those that are not be commonly affected by malware.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: **• Are kept current** **• Perform periodic scans** **• Generate audit logs which are retained per PCI DSS Requirement 10.7.**	5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.	✓	This is a policy based requirement. Merchants must periodically examine and confirm the Endpoint Standard solution is using current signatures, is performing periodic scans, and that logs are generated as expected. Endpoint Standard helps meet this by performing real-time checking of software against well-known virus repositories. There are no definitions that must be stored locally on systems.
	5.2.b Examine anti-virus configurations, including the master	✓	Endpoint Standard's online portal shows the monitoring status of all enrolled devices.

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
	installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.		The software performs automatic updates checking process signatures in real time against any recent updates to virus repositories. All preventions/blocks are also viewable at any time within the console.
	5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: • The anti-virus software and definitions are current. • Periodic scans are performed.	✓	See previous response (5.2.b)
	5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: • Anti-virus software log generation is enabled, and • Logs are retained in accordance with PCI DSS Requirement 10.7.	✓	Endpoint Standard's online portal includes logging and alerts for all malware-related alerts (as well as other policy violations). Log retention can be configured in a PCI DSS compliant manner.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.	✓	Endpoint Standard's online portal shows the monitoring status of all enrolled devices.
	5.3.b Examine anti-virus configurations, including the master installation of the	✓	Endpoint Standard's online portal shows the monitoring status of all

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users.		enrolled devices. It also can be configured to prevent users from disabling agents from running locally.
	5.3.c Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	✓	This is a policy based requirement. However, with Endpoint Standard's portal, merchants can enforce the antivirus agent to be active, running, and to not be turned off except when needed for limited time period. Merchants would have need to enforce a process for when the agents could be turned on/off.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are: • Documented, • In use, and • Known to all affected parties.	✓	This is a policy and procedure based requirement. While Endpoint Standard can help to meet the requirements for protecting against malware, it is up to merchant administrators to create and enforce the specific policies as required.
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. **Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities**	6.1.a Examine policies and procedures to verify that processes are defined for the following: • To identify new security vulnerabilities • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To use reputable outside sources for security vulnerability information.	✓	This is a policy and procedure based requirement. Endpoint Standard can assist in identifying vulnerabilities present on systems within the cardholder data environment where the sensor is installed along with assigning a risk ranking to any vulnerability found. However, it is still up to merchant administrators to ensure that all systems are covered for any additional vulnerabilities along with ensuring coverage for any systems

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.			not running Endpoint Standard. It is also up to merchant administrators to ensure that a policy exists that covers the additional parts of the requirement that Endpoint Standard cannot (i.e., outside sources of vulnerability information, and a policy or procedure document).
	6.1.b Interview responsible personnel and observe processes to verify that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	✓	See previous response (6.1.a).
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	Perform the following: 10.6.1.a Examine security policies and procedures to verify that procedures are defined for reviewing: the following at least daily, either manually or via log tools: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components	✓	This is a policy and procedure based requirement. Merchant must review logs and security events for all system components to identify anomalies or suspicious activity on a regular basis. Endpoint Standard can support the logging of security events relevant to the security of the systems within the cardholder data environment (where a sensor is installed).

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
	that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)		Endpoint Standard also gathers logs that could be considered relevant to servers and system components that perform security functions (antivirus).
	10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	✓	See previous response (10.6.1.a)

APPENDIX B: EXECUTED TEST PLAN

PCI DSS REQUIREMENTS V3.2 2.4, 5 , 6.1, 10.6	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT ENDPOINT STANDARD PCI AV STATUS
2.4 Maintain an inventory of system components that are in scope for PCI DSS	2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	Produced a record of all systems where a Carbon Black Cloud Agent was installed and active.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	Produced a report or log record that indicated that the Carbon Black Cloud Agent was installed, active, and gathered events to detect and prevent threats from endpoints that are in-scope for PCI.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; • Detect all known types of malicious software, • Remove all known types of malicious software, and • Protect against all known types of malicious software. Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.	**1. Detect "KNOWN" types of malware:** Listings from malware feeds provided this type of data assurance and complied.
		2. Remove all KNOWN types of malware: Demonstrated that Endpoint Standard deleted files that were detected as malware or triggered a batch that deleted or moved files that were detected as malware.
		3. Protect against all "KNOWN" types of malware: Demonstrated that the solution detected and then banned or blocked known malware that was part of the known malware list either from malware feeds or from the Endpoint Standard policy.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	5.1.2 Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	Demonstrated that the Endpoint Standard Agent was deployed on any given system (operating system coverage and implementation features). Also illustrated that any given system was assessed even though it was not part of the in-scope PCI systems.
5.2 Ensure that all anti-virus mechanisms are maintained as follows:	5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.	Demonstrated that Endpoint Standard data retrieved malware information via threat and virus informational feeds.

PCI DSS REQUIREMENTS V3.2 2.4, 5 , 6.1, 10.6	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT ENDPOINT STANDARD PCI AV STATUS
• **Are kept current** • **Perform periodic scans** • **Generate audit logs which are retained per PCI DSS Requirement 10.7.**		Demonstrated that Endpoint Standard policies and threat intelligence data were updated, and were set to automatically source current information.
	5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.	Demonstrated that Endpoint Standard periodically scans in-scope systems for malware and updates Carbon Black Cloud Agents automatically. (Note: this function is supported for Windows and macOS only, however, not for Linux)
	5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: • The anti-virus software and definitions are current. • Periodic scans are performed.	Demonstrated that Endpoint Standard virus definition policies are sourced from current repositories. Demonstrated that Endpoint Standard periodically scans in-scope systems that are added to the applicable PCI policy with the Carbon Black Cloud server backend.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. **Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.**	5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.	Demonstrated via log reports or live console view that the Carbon Black Cloud Agent was running and that the policy was enforcing the proper configuration as per the PCI specifications on in-scope PCI assets.
	5.3.b Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users.	Demonstrated that the Carbon Black Cloud Agent had tamper protection and that it had the proper administrative parameters.
	5.3.c Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Demonstrated that Endpoint Standard can be configured by a user with proper administrative access and that a policy was in place that dictated when authorized changes were to be made.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are:	Demonstrated that Endpoint Standard logs were queried and that health statistics regarding the Carbon Black Cloud Agent were collected to

PCI DSS REQUIREMENTS V3.2 2.4, 5 , 6.1, 10.6	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT ENDPOINT STANDARD PCI AV STATUS
	• Documented, • In use, and • Known to all affected parties.	provide proof of agent uptime as well as policy compliance.
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. **Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.**	6.1.a Examine policies and procedures to verify that processes are defined for the following: • To identify new security vulnerabilities • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To use reputable outside sources for security vulnerability information.	Demonstrated Endpoint Standard's ability to categorize adverse events based on a criticality rating that could be incorporated into a vendor's risk ranking and security vulnerability processes.
	6.1.b Interview responsible personnel and observe processes to verify that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	See previous response (6.1.a).
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	Perform the following: 10.6.1.a Examine security policies and procedures to verify that procedures are defined for reviewing: the following at least daily, either manually or via log tools: • All security events	Demonstrated Endpoint Standard's ability to categorize security-related events in a dashboard that could be reviewed by security personnel daily for determining threats and suspicious activity for any device where a Carbon Black Cloud Agent is installed.

PCI DSS REQUIREMENTS V3.2 2.4, 5 , 6.1, 10.6	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT ENDPOINT STANDARD PCI AV STATUS
	• Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	
	10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	See previous response (10.6.1.a).

ABOUT THE AUTHORS

Nick Trenc | Director, Solution Validation (2017 edition)

Nick Trenc (ntrenc@coalfire.com) is the Director of the Solution Validation team and an Application Security Specialist with Coalfire. Nick has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including mobile security, application security, virtualization, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, CISA, QSA, and PA-QSA

Lyle Miller | Principal**,** Solution Validation (2020 edition)

Lyle Miller (lmiller@coalfire.com) is an application security specialist for the Solution Validation team at Coalfire. Lyle has over 9 years of experience working as a QSA and PA-QSA helping clients secure their systems and software for use in PCI DSS environments. Lyle currently holds CISA, CISSP, QSA, PA-QSA, SSA, and SSLC-A certifications. As a PA-QSA, Lyle supports assessments for some of the largest payment software providers in the world, helping teams recognize the importance of secure code development and information security within their operational practices.

ABOUT THE REVIEWER

Bhavna Sondhi | Senior Security Consultant

Bhavna Sondhi (bsondhi@coalfire.com) is a Senior Security Consultant for the Solution Validation team at Coalfire. Bhavna is responsible for conducting PCI DSS, PA-DSS, and P2PE assessments as well as authoring technical whitepapers. Bhavna joined Coalfire in 2013 and brings over 11 years of software engineering and information security experience to the team, leading extensive consulting and assessment engagements within USA, Europe, and Asia. As a lead PA-QSA and P2PE-QSA, Bhavna supports assessments for some of the largest payment software providers in the world, and her software engineering experience plays a vital part in ensuring the teams recognize the importance of secure code development and information security within their operational practices.

Published September 2017. Updated July 2018. Updated April 2020.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.