WHITE PAPER

Cb PROTECTION

PCI DSS ANTI-VIRUS WHITE PAPER

Carbon Black.

ANDREY SAZONOV | CISA, GPEN, QSA, PA-QSA
NICK TRENC | CISA, CISSP, QSA, PA-QSA

COALFIRE

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Carbon Black, Inc. (Carbon Black) engaged 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 Cb Protection next-generation endpoint security platform. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire will describe that the Cb Protection platform meets the PCI Data Security Standard (PCI DSS) v3.2 anti-malware and file-integrity monitoring requirements based on the sample testing and evidence gathered during this assessment.

ABOUT Cb PROTECTION

Cb Protection 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. Additionally, the application whitelisting functionality allows administrators 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.

The components included in the solution are as follows:

1. Cb Protection Agent – Client-side process for monitoring and enforcing policies set within the Cb Console Server.
2. Cb Protection Console – Server-side process for managing and enforcing policies for all systems in scope. This component manages whitelisting application functionality, threats, and all files on all systems and gains an overall picture of an environment's threat landscape. The server communicates with the online service, Cb Collective Defense Cloud (CDC), to verify none of the files are a known vulnerability threat to the systems in the environment.
3. Cb CDC – Remote online service used to analyze files for malware, compare hashes of the files to any known malware, and provide a "trust" score for each file on each system.

Besides application whitelisting technology, Cb Protection'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.

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 September 4, 2017 to September 8, 2017. Additional testing was completed July 2, 2018 to July 13, 2018 and updates were made to this paper.

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 Cb Protection Agent and Cb Protection Console in the Coalfire lab environment.
3. Introduction of malware binaries on local systems with anti-virus agent software installed.

4. Confirmation of the Cb Protection platform's ability to block and remove known malware samples.
5. Testing of configurations and implementation of file-integrity monitoring

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- When properly implemented following vendor guidance, the Cb Protection platform provides coverage for PCI DSS Requirement 5, 10.5.5 and 11.5 based on the sample testing and evidence gathered during this assessment.
- The Cb Protection platform was able to detect and effectively block the execution of the provided known malware samples.
- The Cb Protection platform was able to effectively remove all provided known malware samples.
- The Cb Protection platform adequately generated logs of events such that malicious activity could be traced in accordance with all PCI DSS requirements.
- Cb Protection can be prevented from being disabled by unauthorized users.
- Cb Protection provides policy protections to include application whitelisting/blacklisting, preventing unauthorized processes from starting, accessing network, scraping volatile memory, injecting code or modifying memory of another process, or trying to execute code from memory.

ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of Cb Protection in a PCI DSS environment, specifically to include its impact on PCI DSS Requirement 5, 10.5.5 and 11.5. Cb Protection, when properly implemented following guidance from Carbon Black, can be utilized to meet the technical portions of PCI DSS Requirement 5, 10.5.5 and 11.5. 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 Carbon Black for policy and configuration questions and best practices.

It should also not be construed that the use of Cb Protection 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 Cb Protection Agent software and Cb Protection Console server to test machines along with enablement of strict policies to enforce the detection and prevention of unauthorized files and known malware. Examination of component configurations 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. Also 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 configurations for file-integrity monitoring along with verification that configurations generated alerts when specified files were tampered with.

ASSESSMENT ENVIRONMENT

Cb Protection components were installed on the following machines:

- Cb Protection Agent was installed on Windows XP SP3 running as a virtual machine.
- Cb Protection Agent was installed on Dell Latitude E6420 laptop running a freshly installed copy of Windows 10 with all Windows updates installed and Windows Defender enabled and running.
- Cb Protection Console was installed in the virtual environment on Microsoft Windows Server 2012 R2 Standard 64 bits with Microsoft SQL Server Express 2016 database engine and IIS 10 configured as a webserver.

TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this application security review included:

TOOL NAME	DESCRIPTION
Live Malware Samples	Sample binaries of known malware for Windows OS. • Sample Windows malware obtained from theZoo aka Malware DB at https://github.com/ytisf/theZoo/tree/master/malwares/Binaries Note – Visiting and downloading from the above sites may lead to malware infection. It is highly recommended against doing so.

REFERENCES

Carbon Black Cb Protection website - https://www.carbonblack.com/products/cb-protection/

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

APPENDIX A: PCI REQUIREMENTS COVERAGE MATRIX

PCI DSS REQUIREMENTS

Key:

Compliance directly supported via use of Cb Protection platform = ✓

Requires merchant action for full compliance = ✓

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
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.	✓	Cb Protection allows users to directly deploy agents to Windows-based systems. The CB Protection Console provides the status of monitoring for all enrolled devices. The Cb CDC is checks information on new and existing files from the customer to verify no known malware is present in the customer's environment.
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.	✓	Cb Protection does signature checking against well-known virus repositories. This allows Cb Protection to get check the virus repository for any file or process' reputation in order to detect known malware, block them from running, and remove them as configured per policies. Testing showed that Cb Protection 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 process/procedure requirement. Merchants must "periodically" evaluate the systems they use to ensure the systems are not considered commonly affected. However, Cb Protection can support this by using agentless installs to monitor any system to include those that would be

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
			considered not 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.	✓	5.2.a is a policy requirement. Users of CB Protection must have a documented policy that addresses keeping anti-virus software and definitions up to date. Cb Protection assists in meeting this requirment by doing real-time checking of software against well-known virus repositories. There are no definitions that must be stored locally on systems. Merchants must create a policy that identifies how AV software and AV definitions are kept up date.
	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.	✓	Cb Protection Console provides the monitoring status of all enrolled devices and allows for the scheduling of scans. It also allows for configuration of master policies as they apply to system devices. There is no need for automatic updates as the software checks process signatures in real time against well-known virus repositories.
	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. From Cb Protection Console, admins can monitor the enrollment status of all systems.
	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.	✓	Cb Protection Console includes logging and alerts for all malware related alerts (as well as other policy violations). All logs can be configured in a manner that is PCI DSS compliant and can be configured with centralized logging system.
5.3 Ensure that anti-virus mechanisms are actively running and	5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system	✓	Cb Protection Console shows the monitoring status of all enrolled devices.

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
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.***	components, to verify the anti-virus software is actively running.		
	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.	✓	Cb Protection Console shows the monitoring status of all 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.	✓	5.3.c involves interviews of responsible personnel who can show/verify that, with Cb Protection Console, antivirus is active, running, and cannot be turned off except when needed for limited time. CB Protect includes the ability to enforce a setting that prevents the ability for a user to disable the anti-virus agent within the Console thereby adding assurance to administrators that the agent is running on all systems.
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 policies and procedures based requirement. While Cb Protection can help to meet the requirements for protecting against malware, it is up to administrators to create the specific policies as required.
PCI DSS Requirement 10: Track and monitor all access to network resourced and cardholder data			
10.5.5 Use file-integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	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.	✓	Cb Protection can be configured to provide file-integrity monitoring for any files to include log files in order to ensure that log data is not altered without creating any alert.
PCI DSS Requirement 11: Regularly test security systems and processes.			

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel tou unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly	11.5.a Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files • Additional critical files determined by entity (for example, through risk assessment or other means)	✓	Cb Protection file-integrity control prevents unauthorized modification of critical system files and content files while ensuring only authorized processes can write to these files. Files can be monitored by selecting the specific folders and reporting the changes. Advanced Threat Indicators functionality can be used to identify file changes

APPENDIX B: EXECUTED TEST PLAN

PCI DSS REQUIREMENTS V3.2 REQUIREMENT 5 (PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS)	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT Cb PROTECTION PCI AV STATUS
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 Cb Protection 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,	**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 Cb Protection deleted files that were detected as malware and/or triggered a batch that deleted or moved files that were detected as malware.

PCI DSS REQUIREMENTS V3.2 REQUIREMENT 5 (PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS)	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT Cb PROTECTION PCI AV STATUS
	worms, spyware, adware, and rootkits.	**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 Cb Protection 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 Cb Protection agent was deployed on any given system (OS coverage and implementation features). Also illustrated that any given system was assessed even if it was not part of the in-scope PCI systems.
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.	Demonstrated that Cb Protection data retrieved malware information via threat and virus informational feeds. Demonstrated that Cb Protection policies and threat intelligence data updated automatically/constantly, and were set to dynamically 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 Cb Protection periodically scans in-scope systems for malware as well as updating agents automatically and keeping realtime antivirus definitions.
	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 Cb Protection virus definition policies are sourced from current repositories. Demonstrated that Cb Protection periodically scans in-scope systems that are members of the PCI policy.

PCI DSS REQUIREMENTS V3.2 REQUIREMENT 5 (PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS)	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT Cb PROTECTION PCI AV STATUS
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 Cb Protection 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 Cb Protection 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 Cb Protection 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: • Documented, • In use, and • Known to all affected parties.	Demonstrated that Cb Protection logs were queried and that health statistics regarding the CB Protection agent were collected to provide proof of agent uptime as well as policy compliance. The rest of the requirement must be met by generating appropriate policies and procedures for protecting against malware.
PCI DSS Requirement 10: Track and monitor all access to network resourced and cardholder data		
10.5.5 Use file-integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	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.	Configured file-integrity monitoring to report actions when log data and critical files are changed. Notifications were available through the Cb Protection console dashboard. Email notifications were also configured through the Cb Protection console. Assessor tried to make modifications in the core critical system files on the Windows Operating System that were

PCI DSS REQUIREMENTS V3.2 REQUIREMENT 5 (PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS)	TEST DEFINITION PER PCI VALIDATION PLAN	CURRENT Cb PROTECTION PCI AV STATUS
		registered through Cb Protection and was unable to make any changes. Performed forensics using AccessFTK for the operating system with Cb Protection product and a sample payment application on the system. Cb Protection does not capture, store or transmit any cardholder data, only hash of the files are calculated and stored in the Cb Protection database
PCI DSS Requirement 11: Regularly test security systems and processes.		
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel tou unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly	11.5.a Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files Additional critical files determined by entity (for example, through risk assessment or other means)	Configured file-integrity control to report actions when critical system files and content files are changed. Reports were generated for the events occurred and provided details on the changes that occurred on specific files. Results were reviewed through the weekly report generated. Assessor tried to make modifications in the core critical system files on the Windows Operating System that were registered through Cb Protection and was unable to make any changes. Performed forensics using AccessFTK for the operating system with Cb Protection product and a sample payment application on the system. Cb Protection does not capture, store or transmit any cardholder data, only hash of the files are calculated and stored in the Cb Protection database.

ABOUT THE AUTHORS

Andrey Sazonov | Senior Consultant, Solution Validation

Andrey Sazonov (asazonov@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire. Andrey 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 performed multiple security assessments including penetration testing, application security, virtualization, forensics analysis, and PCI DSS and PA-DSS compliance. He holds a CISA, GPEN, QSA, and PA-QSA.

QA / Update Author:
Nick Trenc | Director, Solution Validation

Nick Trenc (ntrenc@coalfire.com) is the Director of the Solution Validation team with Coalfire. Nick has several years of experience working in Information Security and has an in-depth understanding of application, network, and system security architectures. He holds CISA, CISSP, QSA and PA-QSA certifications.

Published September 2017. Updated July 2018.

ABOUT COALFIRE

Coalfire is the 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 more than 16 years and has offices throughout the United States and Europe. Coalfire.com

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

WP_ Cb Protection – PCI Requirement 5_201709