WHITE PAPER

Cb Defense

PCI DSS ANTI-VIRUS WHITE PAPER

Carbon Black.

Nick Trenc | Practice Director

COALFIRE℠

North America | Latin America | Europe

877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Carbon Black, Inc. (Carbon Black) 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 Cb Defense next-generation anti-virus platform. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire will describe that the Cb Defense platform met the PCI Data Security Standard (PCI DSS) v3.2 anti-malware requirement based on the sample testing and evidence gathered during this assessment.

ABOUT CB DEFENSE

Cb Defense is a next-generation anti-virus solution for desktops, laptops, and servers that protects computers from the full spectrum of modern cyber-attacks, delivering the best endpoint protection with the least amount of work.

Using a combination of endpoint and cloud-based technologies, Cb Defense stops attacks before they can even start. Its 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.

AUDIENCE

This assessment white paper has three target audiences:

1. **QSA and Internal Audit Community:** This audience may be evaluating Cb Defense to assess merchant or service provider environment for PCI DSS.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating Cb Defense for use within their organization for compliance requirements other than PCI DSS.
3. **Merchant and Service Provider Organizations:** This audience is evaluating Cb Defense for deployment in their cardholder data environment and what benefits 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..

At a high level, testing consisted of the following tasks:

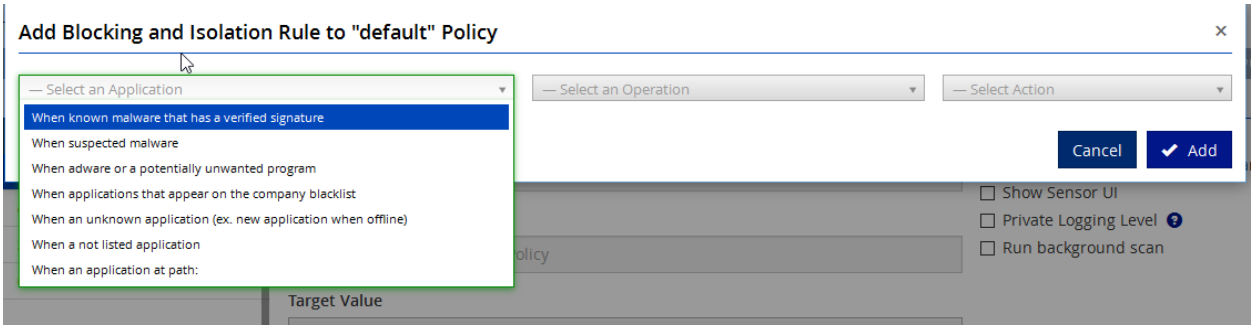
1. Technical review of the architecture of the full solution and its components.
2. Implementation of the Cb Defense agent software in the Coalfire lab environment.
3. Introduction of malware binaries on local systems with anti-virus agent software installed.
4. Confirmation of Cb Defense platform's ability to block and remove known malware samples.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- When properly implemented following vendor guidance, the Cb Defense platform provides coverage for PCI DSS Requirement 5 based on the sample testing and evidence gathered during this assessment.
- The Cb Defense platform was able to detect and effectively block the execution of the provided known malware samples.
- The Cb Defense platform was able to effectively remove all provided known malware samples.
- The Cb Defense platform adequately generated logs of events such that malicious activity could be traced in accordance with PCI DSS requirements.
- Cb Defense can be prevented from being disabled by unauthorized users.
- Cb Defense can also provide additional policy protections to include application whitelisting/blacklisting, preventing processes from accessing 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 - Example of policy protection settings



ASSESSOR COMMENTS

Our assessment scope put a significant focus on validating the use of Cb Defense in a PCI DSS environment, specifically to include its impact on PCI DSS Requirement 5. Cb Defense, when properly implemented following guidance from 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 Carbon Black for policy and configuration questions and best practices.

It should also not be construed that the use of CB Defense 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 Defense agent software to test machines along with enablement of strict policies to enforce the detection and prevention of known malware. Examination of 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. Also evaluate backend component for verification that agents are deployed, communicating, up-to-date, performing periodic scans, and protecting against real-time threats.

CB DEFENSE COMPONENTS

Cb Defense is a next-gen antivirus platform comprised of:

1. Cb Defense Agent – Client-side process for monitoring local systems in accordance with policies set within the Cloud Server. 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. Cb Defense Cloud Server – Web-accessible platform for deploying agents, managing threats, and gaining an overall picture of an environment's threat landscape.

ASSESSMENT ENVIRONMENT

Cb Defense agents were installed on the following machines:

- Mid-2011 MacBook Air Model A1370 running a freshly installed copy of Mac OS 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.

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 both Mac OS X and Windows. • Sample Mac malware obtained from Objective-See at https://objective-see.com/malware.html • Sample Windows malware obtained from theZoo aka Malware DB at http://thezoo.morirt.com/ *Note – Visiting and downloading from the above sites may lead to malware infection. It is highly recommended against.

REFERENCES

Carbon Black Cb Defense website - https://www.carbonblack.com/products/cb-defense/

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 Defense 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 Defense allows users to directly deploy agents to Windows and macOS. 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 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 Defense does signature checking against well-known virus repositories. This allows Cb Defense to get a reputation for all processes to detect those that are known malware, block them from running, and remove them when requested by an administrator. Testing showed that Cb Defense 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	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 they are not considered commonly affected. Cb Defense can support

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
not require anti-virus software.			this by using agentless installs to monitor any system to include those that would be 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. Cb Defense meets this by doing 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 installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.	✓	Cb Defense's online portal shows 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 the Cb Defense portal, 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	✓	Cb Defense's online portal includes logging and alerts for all malware related alerts

PCI REQUIREMENT	PCI TESTING REQUIREMENTS	COMPLIANCE SUPPORTED	COMMENTS
	• Logs are retained in accordance with PCI DSS Requirement 10.7.		(as well as other policy violations).
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. 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. 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.	✓ ✓ ✓	Cb Defense's online portal shows the monitoring status of all enrolled devices. Cb Defense's online portal shows the monitoring status of all enrolled devices. It also can be configured to prevent users from disabling agents from running locally. Requirement 5.3.c involves interviews of responsible personnel who can show/verify with Cb Defense's portal that antivirus is active, running, and cannot be turned off except when needed for limited time period.
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 Defense can help to meet the requirements for protecting against malware, it is up to administrators to create the specific policies as required.

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 DEFENSE 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 the Cb Defense 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 Cb Defense deleted files that were detected as malware and/or triggered a batch that deleted or moved files that were detected as malware.
		3. Protect against all "KNOWN" types of malware: Demonstrated how the solution detects and then banned or blocked known malware that was part of the known malware list either from malware feeds or from the Cb Defense 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 how easily the Cb Defense agent was deployed on any given system (OS coverage and implementation features). Also illustrated how any given system was assessed even though it was not part of the in-scope PCI systems.

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 DEFENSE PCI AV STATUS
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.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. 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.	5.2.a Demonstrated or illustrated where Cb Defense data retrieved malware information (i.e threat and virus informational feeds). 5.2.a Demonstrated or illustrated that Cb Defense policies and threat intelligence data updated, set to dynamically source current information, or can be updated. 5.2.b Demonstrated or illustrated that Cb Defense periodically scans in-scope systems for malware. 5.2.c Demonstrated or illustrated that Cb Defense virus definition policies are sourced from current repositories. 5.2.c Demonstrated or illustrated that Cb Defense periodically scans in-scope systems that are members of the PCI policy.
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**	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. 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.	5.3.a. Demonstrated or illustrated via log reports or live console view that the Cb Defense 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. Demonstrated or illustrated that the Cb Defense agent had tamper protection and that it had the proper administrative parameters.

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 DEFENSE PCI AV STATUS
to be implemented for the period of time during which anti-virus protection is not active.	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. Demonstrated or illustrated that Cb Defense can be configured by a user with proper administrative access and that a policy was in place that dictated when authorized changes were 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 or illustrated that Cb Defense logs were queried and that health statistics regarding the agent were collected to provide proof of agent uptime as well as policy compliance.

ABOUT THE AUTHORS

Nick Trenc | Senior Consultant

Nick Trenc (ntrenc@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire Systems. 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.

QA:
Richard Fleeman | Director

Richard Fleeman (rfleeman@coalfire.com) is the Director of the Application Security team with Coalfire Systems. Richard has several years of experience working in Information Security and has an in-depth understanding of application, network, and system security architectures. He holds a both the CISSP and CISA certifications.

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com

Cb Defense – PCI Requirement 5 10/2016