WHITE PAPER

Cb Defense
HEALTHCARE ANTI-VIRUS WHITE PAPER

Carbon Black.

Terilyn Floyd-Carney | Senior Consultant
Nick Trenc | Practice Director
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act</td>
<td>3</td>
</tr>
<tr>
<td>HIPAA Security Rule</td>
<td>3</td>
</tr>
<tr>
<td>HITRUST CSF</td>
<td>4</td>
</tr>
<tr>
<td>About Cb Defense</td>
<td>4</td>
</tr>
<tr>
<td>Cb Defense Support for the HITRUST CSF, HIPAA, &amp; HHS Checklist Requirements</td>
<td>4</td>
</tr>
<tr>
<td>Summary and Conclusion</td>
<td>6</td>
</tr>
<tr>
<td>Appendix A: About the Technical Assessment</td>
<td>7</td>
</tr>
<tr>
<td>Audience</td>
<td>7</td>
</tr>
<tr>
<td>Assessment Methodology</td>
<td>7</td>
</tr>
<tr>
<td>Cb Defense Components</td>
<td>7</td>
</tr>
<tr>
<td>Assessment Environment</td>
<td>7</td>
</tr>
<tr>
<td>Tools and Techniques</td>
<td>8</td>
</tr>
<tr>
<td>References</td>
<td>8</td>
</tr>
<tr>
<td>Appendix B: Executed Test Plan</td>
<td>9</td>
</tr>
</tbody>
</table>
INTRODUCTION

Carbon Black, Inc. (Carbon Black) engaged Coalfire Systems Inc. (Coalfire), a leading independent industry provider of IT security, governance, and regulatory compliance services, to conduct an independent technical assessment of their Cb Defense next-generation anti-virus platform. Coalfire was also engaged to determine the platform’s suitability and compliance for meeting the Health Insurance Portability and Accountability Act (HIPAA) and HITRUST CSF controls for anti-virus and anti-malware. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire describes how the Cb Defense platform is able to meet the Anti-Virus and Anti-Malware requirements of the HIPAA Security Rule, HITRUST CSF, and the “Anti-Virus Checklist” from the “Top 10 Tips for Cybersecurity in Health Care”, as published by the U.S. Department of Health and Human Services (HHS), based on the sample testing and evidence gathered during this assessment.

The paper also briefly describes the origin of HIPAA, presents the features of the software that can be leveraged for suitability and compliance, and provides a mapping of available features in the platform specific to HIPAA, which also map to HITRUST CSF and Cybersecurity Best Practices.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA is a 1996 United States legislation that provides data privacy and security provisions for safeguarding medical information. The HIPAA Security Rule provides requirements on the safeguarding of electronic protected health information (ePHI), which sets the standards for patient data security.

HIPAA SECURITY RULE

The HIPAA Security Rule specifically focuses on the protection of ePHI through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a Covered Entity, Business Associate, or Subcontractor. Organizations such as these are required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule; and
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards;
- Physical Safeguards; and
- Technical Safeguards.
HITRUST was founded on the principles of establishing a unified assessment framework for evaluating a wide array of industries such as healthcare, business, and technology. In addition, HITRUST normalizes and harmonizes requirements from ISO, NIST, PCI, and HIPAA. The objective of the HITRUST CSF is to safeguard protected data during all phases of activity, such as transmission, storage, and data at rest.

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 effort.

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 non-malware attacks that exploit memory and scripting languages like PowerShell. This early detection technology allows companies to respond quickly to potential ransomware and other attacks before they gain a foothold.

CB DEFENSE SUPPORT FOR THE HITRUST CSF, HIPAA, & HHS CHECKLIST REQUIREMENTS

**HITRUST CSF**

09.j Controls Against Malicious

Anti-virus and anti-spyware are installed, operating and updated on all devices to conduct periodic scans of the system to identify and remove unauthorized software.

Audit logs of the scans are maintained.

The organization has implemented the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers to lower the chance of spoofed email messages.

The organization prohibits users from installing unauthorized software, including data and software from external network, and ensures users are made aware and trained on these requirements.

**HIPAA SAFEGARDS**

Protection from Malicious Software – A 164.308(a)(5)(ii)(B) Procedures for guarding against, detecting, and reporting malicious software.

Response and Reporting – R 164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)
ANTI-VIRUS CHECKLIST
☐ Policies are in place requiring use of anti-virus software.
☐ All staff members understand and agree that they shall not hinder the operation of anti-virus software.
☐ All staff members know how to recognize possible symptoms of viruses or malware on their computers.
☐ All staff members know what to do to avoid virus/malware infections.
☐ Anti-virus software is installed and operating effectively on each computer in compliance with manufacturer recommendations.
☐ Anti-virus software is set up to allow automatic updates from the manufacturer.
☐ Anti-virus software is fully up-to-date according to manufacturer’s standards.
☐ Handheld or mobile devices that support anti-virus software have the software installed and operating.

COMPLIANCE

AVAILABLE CAPABILITY
Cb Defense’s centralized management is an online portal that includes logging and alerts for all software violations based on the configuration of the white list or black list policy.

The following findings are relevant highlights from this assessment:

- The Cb Defense platform was able to detect, block, and remove all supplied examples of viruses, Trojans, ransomware, rootkits, and other known malware.
- There is no need for automatic updates as the software checks process signatures in real time against a well-known virus repository.
- The Cb Defense platform adequately generated logs of events such that malicious activity could be traced to the source.
- Cb Defense can be prevented from being disabled by unauthorized users through the policies controlled by the centralized management.
- Cb Defense’s centralized management allows administrators 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 all enrolled devices or agents and allows for the scheduling of scans through the policy or for a scan to be initiated from the management portal.
- Cb Defense can also provide additional policy protections to include application whitelisting/blacklisting, preventing processes from accessing the network, preventing processes from scraping memory of other processes, and preventing processes from injecting code, modifying memory of another process, or trying to execute code from memory, while allowing custom applications to run unaffected if properly whitelisted.
SUMMARY AND CONCLUSION

The assessment scope put a significant focus on validating the use of Cb Defense in a healthcare environment. Cb Defense, when properly implemented following guidance from Carbon Black, can be utilized to meet some of the requirements laid out by the HIPAA Security Rule, HITRUST CSF, and HHS. However, as most computing environments and configurations differ 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 compliance with HIPAA, HITRUST, or HHS. Disregarding these requirements and security best practice controls for systems and networks inside or outside of the scope of the electronic health records environment can introduce many other security or business continuity risks to the healthcare organization. Security and business risk mitigation should be any healthcare organization’s goal and focus for selecting security controls.
APPENDIX A: ABOUT THE TECHNICAL ASSESSMENT

AUDIENCE
This assessment white paper has three target audiences:

1. **Internal Audit Community**: This audience may be evaluating Cb Defense to assess a healthcare organization, business associate, or service provider environment.
2. **Administrators and Other Compliance Professionals**: This audience may be evaluating Cb Defense for use within their organization for compliance requirements.
3. **Healthcare, Business Associate, and Service Provider Organizations**: This audience is evaluating Cb Defense for deployment in their environment and benefits that could be achieved from using this solution.

ASSESSMENT 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.

The assessment used the following methods to assess the potential 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, evaluation of 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:

<table>
<thead>
<tr>
<th>TOOL NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 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](https://objective-see.com/malware.html)  
   - Sample Windows malware obtained from theZoo aka Malware DB at [http://thezoo.morirt.com/](http://thezoo.morirt.com/)  
   *Note – Visiting and downloading from the above sites may lead to malware infection. It is highly recommended against.* |

REFERENCES
Top 10 Tips for Cybersecurity in Health Care - [https://www.healthit.gov/playbook/pdf/top-10-tips-for-cybersecurity.pdf](https://www.healthit.gov/playbook/pdf/top-10-tips-for-cybersecurity.pdf)
# APPENDIX B: EXECUTED TEST PLAN

<table>
<thead>
<tr>
<th>BEST PRACTICE FOR PROTECTING SYSTEMS AGAINST MALWARE AND REGULARLY UPDATES TO ANTI-VIRUS SOFTWARE OR PROGRAMS</th>
<th>TEST VALIDATION PLAN</th>
<th>CURRENT CB DEFENSE AV STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</td>
<td>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.</td>
<td>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 were in-scope.</td>
</tr>
</tbody>
</table>
| Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | 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 virus repository or any other malware feed 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 detected and then banned or blocked known malware that was part of the known malware list either from virus repository or from the Cb Defense policy. |
<p>| 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. | 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 systems. |</p>
<table>
<thead>
<tr>
<th>BEST PRACTICE FOR PROTECTING SYSTEMS AGAINST MALWARE AND REGULARLY UPDATES TO ANTI-VIRUS SOFTWARE OR PROGRAMS</th>
<th>TEST VALIDATION PLAN</th>
<th>CURRENT CB DEFENSE AV STATUS</th>
</tr>
</thead>
</table>
| Ensure that all anti-virus mechanisms are maintained as follows:  
- Virus definitions are kept current.  
- Critical system file scans are performed during system boot and every 12 or 24 hours.  
- Periodic reviews/scans can be set up to be required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software.  
- Audit logs that are generated and retained. | Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.  
Examine anti-virus configurations, including the master installation of the software, to verify that anti-virus mechanisms are:  
- Configured to perform automatic updates, and  
- Configured to perform periodic scans.  
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 where Cb Defense data retrieved malware information (i.e. threat and virus informational feeds).  
Demonstrated that Cb Defense policies and threat intelligence data updated, were set to dynamically source current information, or could be updated.  
Demonstrated that Cb Defense periodically scanned in-scope systems for malware.  
Demonstrated that Cb Defense virus definition policies were sourced from current repositories.  
Demonstrated that Cb Defense periodically scanned in-scope systems that were members of the policy. |
| Malicious code and spam protection mechanisms shall be centrally managed, and that the 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.* | Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software is actively running.  
Examine anti-virus configurations, including the master installation of the software and a sample of system components, interview responsible personnel, and observe processes to verify that the 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 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 specifications on in-scope assets.  
Demonstrated that the Cb Defense agent had tamper protection and the proper administrative parameters.  
Demonstrated that Cb Defense could be configured by a user with proper administrative access and that a policy was in place that dictated when authorized changes could be made. |
<table>
<thead>
<tr>
<th>BEST PRACTICE FOR PROTECTING SYSTEMS AGAINST MALWARE AND REGULARLY UPDATES TO ANTI-VIRUS SOFTWARE OR PROGRAMS</th>
<th>TEST VALIDATION PLAN</th>
<th>CURRENT CB DEFENSE AV STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal policies shall be required prohibiting the use or installation of unauthorized software, and automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations).</td>
<td>Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against unauthorized software are in place. Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software has the ability and is configured to prevent unauthorized software.</td>
<td>Demonstrated that Cb Defense could be configured by a user with proper administrative access and that a policy was in place that dictated that mobile code execution could be prevented though a white list and black list function.</td>
</tr>
</tbody>
</table>
ABOUT THE AUTHORS

Terilyn Floyd-Carney | Senior Consultant
Terilyn Floyd-Carney (tfloyd-carney@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire Systems. Terilyn has several years of experience working as a PA-QSA and HITRUST Certified CSF Practitioner helping clients develop systems and software for use in healthcare, pharmacy, and retail environments and has authored and spoken on multiple security topics including application security, cybersecurity best practices, and compliance. She holds a CISSP, CISA, HCISPP, HITRUST Certified CSF Practitioner, QSA, and PA-QSA.

Nick Trenc | Practice Director
Nick Trenc (ntrenc@coalfire.com) is an Application Security Specialist and Practice Director 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.

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

Copyright © 2014-2017 Coalfire Systems, Inc. All Rights Reserved. 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.