# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Overview</td>
<td>3</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard Overview (PCI DSS)</td>
<td>4</td>
</tr>
<tr>
<td>Malwarebytes Endpoint Security</td>
<td>5</td>
</tr>
<tr>
<td>Malwarebytes Management Console</td>
<td>5</td>
</tr>
<tr>
<td>Supported Platforms</td>
<td>6</td>
</tr>
<tr>
<td>Secondary Console</td>
<td>6</td>
</tr>
<tr>
<td>Malwarebytes Anti-Malware Agent</td>
<td>6</td>
</tr>
<tr>
<td>Malwarebytes Anti-Exploit Agent</td>
<td>7</td>
</tr>
<tr>
<td>Malwarebytes Endpoint Security Detection Capabilities</td>
<td>7</td>
</tr>
<tr>
<td>Malwarebytes Data Retention on Endpoints and on the Management Server</td>
<td>8</td>
</tr>
<tr>
<td>Malwarebytes Signature Update</td>
<td>8</td>
</tr>
<tr>
<td>Upstream Connections to the Management Console</td>
<td>9</td>
</tr>
<tr>
<td>Malwarebytes Integrated User Alerts and Messaging</td>
<td>9</td>
</tr>
<tr>
<td>Detection Events on the Endpoint</td>
<td>9</td>
</tr>
<tr>
<td>Malwarebytes Endpoint Security Support for PCI DSS 3.2 Requirements</td>
<td>11</td>
</tr>
<tr>
<td>Requirement 2: Do Not Use Vendor-supplied Defaults for System Passwords</td>
<td>11</td>
</tr>
<tr>
<td>Requirement 5: Protect All Systems Against Exploits and Malware And</td>
<td>11</td>
</tr>
<tr>
<td>Regularly Update Anti-Virus Software or Programs</td>
<td></td>
</tr>
<tr>
<td>Requirement 6: Develop and Maintain Secure Systems and Applications</td>
<td>14</td>
</tr>
<tr>
<td>Requirement 10: Track and Monitor All Access to Network Resources and</td>
<td>16</td>
</tr>
<tr>
<td>Cardholder Data</td>
<td></td>
</tr>
<tr>
<td>Requirement 11: Regularly Test Security Systems and Processes</td>
<td>23</td>
</tr>
<tr>
<td>Coalfire Opinion</td>
<td>24</td>
</tr>
<tr>
<td>A Comment Regarding Regulatory Compliance</td>
<td>24</td>
</tr>
<tr>
<td>References</td>
<td>24</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>25</td>
</tr>
<tr>
<td>About Malwarebytes</td>
<td>25</td>
</tr>
</tbody>
</table>
EXECUTIVE OVERVIEW

A common requirement in virtually all regulatory compliance objectives and defense in depth strategies is to provide endpoint protection against virus, malware, rogue security software, adware, and other breeds of spyware that focus on the user and their personal computer.

Malwarebytes released their initial batch-mode scanner in January of 2006 and rapidly made a name for themselves with one of the first effective tools (capable of detecting and correcting a variety of post-infection impacts) used in conjunction with the mainstream anti-virus tools of that time. In the years that followed, Malwarebytes took their simple, single user product and created the Malwarebytes Endpoint Security (MBES) software suite, which combines a centralized administration and monitoring platform with endpoint and anti-exploit protection for Windows PCs and Apple Macs.

In this Product Applicability Guide for Malwarebytes Endpoint Security, Coalfire reviewed feature alignment with the Payment Card Industry Data Security Standard (PCI DSS) version 3.2, released in April 2016. The review followed our standard methodology where we evaluate the specific PCI DSS requirements (controls) that are addressed by MBES and make a determination of the product’s capacity to support those requirements. Our methodology is specifically directed by the guidance provided in the PCI DSS Requirements and Security Assessment Procedures, Version 3.2, April 2016 document.

Based upon the findings obtained during our review, we concluded that Malwarebytes Endpoint Security, version 1.80 can be effective in meeting many of PCI DSS controls under requirements 2, 5, 6, 10 and 11.

In the following sections, this paper discusses in more specific detail the particular features of Malwarebytes Anti-Malware for Business that can be used to address the PCI DSS requirements for an implementing organization. To assist the security planner or inform a potential internal or Qualified Security Assessor (PCI DSS QSA), we provide detailed mapping of available features in MBES to specific requirements in the PCI DSS framework.

For introductory purposes, a brief overview of the PCI DSS requirements is included below.
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD OVERVIEW (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a framework that defines baseline physical, technical, and operational security controls, defined as requirements and sub-requirements, necessary for protecting payment card account data. PCI DSS defines two categories of payment card account data: cardholder data (CHD), which includes primary account number (PAN), cardholder name, expiration date, and service code; and sensitive authentication data (SAD), which includes full track data (magnetic-stripe data or equivalent on a chip), card security code (CAV2/CVC2/CVV2/CID), and personal identification numbers (PINs/PIN blocks) entered during the transaction.

As stated on page 5 of the PCI DSS Requirements and Security Assessment Procedures, Version 3.2, April 2016, PCI DSS applies to any organization that stores, processes, or transmits CHD. These organizations include (but are not limited to): merchants, payment processors, issuers, acquirers, and service providers. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE). The CDE is comprised of people, processes, and technologies that store, process, or transmit CHD or SAD. PCI DSS defines 12 requirements designed to address six objectives, as shown in this high-level overview:

<table>
<thead>
<tr>
<th>OBJECTIVES</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network and Systems</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Protect all systems against malware and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>

Table 1 - PCI DSS – High-Level Overview
MALWAREBYTES ENDPOINT SECURITY

Malwarebytes Endpoint Security (MBES) version 1.7.7 is a suite of three specific agents that are used in concert with each other to provide centralized detection, remediation, orchestration, and monitoring of personal computers in the business environment and to manage spy-ware threats for the organization’s machines. In this section, we briefly provide an overview of these three agents.

MALWAREBYTES MANAGEMENT CONSOLE

For corporate and business users who have special requirements based on corporate security policies, have a fleet of computers, need to provide non-disruptive security, or wish to use Malwarebytes in a fully integrated and holistic fashion incorporating the anti-malware capabilities with existing IT, Malwarebytes provides the Management Console as the orchestration application for MBES. It has the following relationship to the managed clients:

![Figure 1 - Malwarebytes Management Console Overview](image)

![Figure 2 - Management Console Home Screen](image)
Supported Platforms
The Management Console is available for the following platforms:

- Windows
  - Windows Small Business Server 2011
  - Windows Server 2008/2008R2 (excludes Serve Core installation)
  - Windows Server 2012/2012R2 (no Server Core installation)
  - Windows Server 2016 (no Server Core installation variant)
- Hardware and SQL Servers (physical hardware and/or virtual hypervisors)
  - 1 GHz minimum CPU, dual core 1.6GHz recommended
  - 1GB RAM required, 2GB recommended
  - Disk space: 2GB minimal, 10GB recommended
  - Either Embedded SQL or Dedicated SQL Server 2008, 2012, 2014, 2016 Express (10GB max size)

Secondary Console
The Management Server is operated through a primary and/or a secondary console, which have equal utility when operating the Management Server. The primary console resides on the installed server running the Management software. Although not required for operation and intended for operational flexibility, the secondary console supports additional remote administrators running on typical Windows workstations (version XP Pro/SP3 through Windows Server 2016, excluding Server Core installation variants).

MALWAREBYTES ANTI-MALWARE AGENT
As mentioned in the provided support documentation, “this is the flagship Malwarebytes client.” Favored protection for technical computer users, the Anti-Malware client, reviewed in version 1.80, is driven by a signature database that is updated 8-15 times per day, supplemented by heuristic analysis to detect “zero-
“day” patterns not included in any signature database, and protects against known, current, and emerging attacks.

Policy-driven by the IT administrators operating the Malwarebytes Management Console, scans and updates are controlled by the policies. Aspects of startup, sequencing, real-time protection, and quarantining are also directed through the policies applied on the Management Console. Flexibility for end-user autonomous operation is also policy-controlled. The client is also designed to operate on endpoints protected by Virtual Private Network (VPN) technology. The following are minimum system requirements for endpoints:

- **Hardware**
  - CPU: 1GHz, RAM: 1GB, Disk: 100MB for both program and local logs
- **Operating Systems**
  - Desktop Windows (XP Pro SP3, Vista, 7, 8, 8.1, and Windows 10)

MALWAREBYTES ANTI-EXPLOIT AGENT

Taking a unique and different approach to system security, the Malwarebytes Anti-Exploit Agent version 1.09 does not use the signatures of any known threats. It inspects incoming data streams, analyzes behavior, and determines whether it needs to respond to suspected exploit activity on the system. By bypassing operating system protection mechanisms, malware attempts to find ways to execute in unrestricted fashion, using memory manipulation to operate undetected. By detecting vulnerabilities in commonly-used applications as they are being exploited by malware, Anti-Exploit shields applications and processes from attack, while neutralizing and isolating the attacker.

The Malwarebytes Management Console also policy-orchestrates the operation and response of Malwarebytes Anti-Exploit.

Malwarebytes Endpoint Security Detection Capabilities

MBES is designed to detect, prevent, and remediate the widest variety of malware and advance “crypto virus” exploits by virtue of the combined capabilities of the Anti-Malware and Anti-Exploit agents. Business disruption caused by these attacks has received widespread attention over the past five years due to the combined impacts of data-unavailability and direct economic costs.

Malwarebytes Anti-Exploit agents are enabled on the management console for one or more of the endpoints as depicted in figure 4 below:
Although Coalfire did not rigorously test this feature of MBES, we did confirm basic detection and blocking of a crypto virus variant of CryptoLocker with the Anti-Exploit feature enabled. More specific examples of this process are covered in great detail in a number of Malwarebytes white papers, available on their website, and in technical reviews of the product.

**Malwarebytes Data Retention on Endpoints and on the Management Server**

In the managed business installation, MBES is intended to keep primary data on the Management Console server, with support for syslog integration to external syslog and Security Information and Event Management (SIEM) systems that are typically used by merchants and PCI DSS required entities. Data is retained on the actual endpoints in their local logs and may be retained for a period of time specified by the policy controls set on the Malwarebytes Management Console server.

When used in a SIEM integrated mode, MBES may support integration of the detection activity with HP ArcSight, IBM Q-Radar, Splunk, and other event management platforms via log-integration and log-shipping techniques. Custom APIs were not reviewed in this Product Applicability Guide.

**Malwarebytes Signature Update**

As mentioned previously, Malwarebytes corporate anti-malware signature updates occur (via a port 443 HTTPS connection to endpoints and/or the Malwarebytes Management Server) nearly continuously with an average of 8-15 times per day and are available for download at intervals controlled by policy settings for the enterprise, department, and even the individual endpoint.
Periodic updates are issued to the Anti-Exploit MBES component in the form of patches or updated versions, as it does not rely upon a signature database for its version of endpoint protection.

**Upstream Connections to the Management Console**

The endpoint integration to the Management Server is over port 443 HTTPS using TLS 1.2 with 128-bit AES encryption, as are the signature update mechanism transactions. A trusted-SSL certificate with third-party signing is utilized for Internet-connected signature update transactions, while either self-signed certificates or client requested CSR-generated certificates may be used for the port 443 activity between endpoints and the Management Console server.

**MALWAREBYTES INTEGRATED USER ALERTS AND MESSAGING**

**Detection Events on the Endpoint**

Supported by the centralized control settings of the MBES console, responses to threats in action on endpoints generate real-time messages displayed to the user in two formats. Pop-up status and event indicators, similar to this example in figure 7, are designed to inform the user and take desired actions based on Management Console settings for the user community.
When blocked threats are encountered, a tray icon notification (on Windows) shows the actions taken and provides a link to additional user follow-up activities that may be desired. The following examples in figure 8 shows two “tooltip balloons” depicting an automatic quarantine and a blocked website response:

Figure 7 - Malwarebytes Detection Pop-up on Endpoint

Figure 8 - Tooltip Balloon Responses on Endpoint
MALWAREBYTES ENDPOINT SECURITY SUPPORT FOR PCI DSS 3.2 REQUIREMENTS

Although PCI DSS v3.2 requirements define baseline technical, physical, and operational security controls necessary for protecting payment card account data, the MBES suite implements only technical controls to collect activity data and ultimately provide detection of, and protection from, threats to the implementing organization. Non-technical controls were not reviewed against Malwarebytes Endpoint Security.

Below is a brief description of categories used to identify the coverage status of specific PCI DSS v3.2 requirements by the MBES suite:

- **Available Capability** – The capabilities to satisfy the requirement are available within MBES.
- **Partially Supported Capability** – The features available in MBES can be utilized by the implementing organization to partially satisfy the specifications in the requirement.
- **Not Applicable/Support Not Available** – The requirement is not supported or provided by MBES or is a process requirement that is exclusively the responsibility of the implementing organization.

### REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

MBES does not control all aspects of password use on the endpoints, as that is not an intended feature of the product. Endpoints and servers running MBES endpoint components are inventoried and centrally reported for their anti-malware (requirement 5) operations.

<table>
<thead>
<tr>
<th>PCI DSS REQUIREMENT</th>
<th>TESTING PROCEDURES</th>
<th>COMPLIANCE AND GUIDANCE</th>
<th>SUPPORTED</th>
</tr>
</thead>
</table>
| 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.  
2.4.b Interview personnel to verify the documented inventory is kept current. | Partially Supported Capability. Although maintaining an accurate inventory of the system is a process control that is the responsibility of the entity, the Management Console can help generate an inventory of all active systems if Malwarebytes Endpoint Security has been configured on all systems. | ✔ |

Table 2 - PCI DSS Requirement 2

### REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST EXPLOITS AND MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

Malwarebytes Endpoint Security is an endpoint protection solution that provides detection, prevention, monitoring, and response capabilities to defend against various forms of spy and crypto-ware. The solutions are centrally managed by the common Malwarebytes Management Console server, which coordinates and logs responses from the anti-malware and anti-exploit agents. The events and system heuristics are continuously monitored for suspicious activity. If any suspicious activity is detected, the Management Server will dictate desired response to the activity via pre-set policies. This response
automates what an individual user could do on the stand-alone versions of the product and/or it escalates the event for IT response via either a remote-control or a hands-on intervention.

<table>
<thead>
<tr>
<th>PCI DSS REQUIREMENT</th>
<th>TESTING PROCEDURES</th>
<th>COMPLIANCE AND GUIDANCE</th>
<th>SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</td>
<td>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.</td>
<td>Available Capability. Malwarebytes Endpoint Security can be deployed on every endpoint to gather system events from every host to detect and prevent threats. Malwarebytes Endpoint Security is available for Windows and Mac systems.</td>
<td>✓</td>
</tr>
</tbody>
</table>
| 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. | Available Capability.  
All data collected by MBES is transmitted in real-time to Malwarebytes Management Console and the orchestration engine on that platform. Anti-Exploit response results as well as conventional anti-malware response are both tracked equally.  
Note: some types of malware are flagged as requiring manual removal. | ✓ |
| 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. | Supported Capability.  
Malwarebytes Endpoint Security can be deployed on every endpoint to gather system events from every host to detect and prevent threats.  
The PCI DSS entity is still responsible for ensuring that the sensor is deployed on appropriate systems and proper threat evaluation is performed for non-Windows and non-Mac OS variants. | ✓ |
| 5.2 Ensure that all anti-virus mechanisms are maintained as follows:  
- Are kept current, | 5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. | Available Capability.  
All data collected by MBES metrics are transmitted in real-time to the Malwarebytes | ✓ |
<table>
<thead>
<tr>
<th>5.2.b</th>
<th>Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are:</th>
<th>Management Console server, which is responsible for the coordination of update installation, per defined policies. Both periodic scans and signature updates are granularly controlled for this outcome. Users of the individual endpoints do not need to perform any updates.</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.c</td>
<td>Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:</td>
<td>Available Capability. All metadata associated with user activity, processes, and any suspicious activity is collected centrally and able to abide by (typically 1 year) retention policies mandated by the entity and PCI DSS compliance requirements.</td>
<td>✓</td>
</tr>
<tr>
<td>5.2.d</td>
<td>Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:</td>
<td>Available Capability. Policy-based controls to enforce installation and pervasiveness of the Anti-malware functionality.</td>
<td>✓</td>
</tr>
<tr>
<td>5.3</td>
<td>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.</td>
<td>Available Capability. Malwarebytes Endpoint Security operates in the kernel and does not run in the user space. Only Administrator and root privileges accounts specifically allocated rights to control the Malwarebytes agents may modify the endpoint settings.</td>
<td>✓</td>
</tr>
<tr>
<td>5.3.a</td>
<td>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.</td>
<td>Available Capability.</td>
<td>✓</td>
</tr>
<tr>
<td>5.3.b</td>
<td>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.</td>
<td>Available Capability.</td>
<td>✓</td>
</tr>
<tr>
<td>5.3.c</td>
<td>Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized</td>
<td>Available Capability. Provisions do exist for temporary suspension of the protection by administrative and policy control.</td>
<td>✓</td>
</tr>
</tbody>
</table>
time during which anti-virus protection is not active.

by management on a case-by-case basis for a 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.

5.4 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.

Not Applicable.

This is a process requirement that is the responsibility of the implementing organization.

### Table 3 - PCI DSS Requirement 5

#### REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

The Malwarebytes Endpoint Security suite provides the latest intelligence on threats and responses, as coordinated by the centralized support delivered by Malwarebytes corporate Internet resources. Significant details provided on malware and spyware threats may be used by CHD entities to evaluate the risk of specific vulnerabilities to their organizations. Outside of the control of MBES are: system patching, development practices, change management, and implementation of secure coding practices, which are exclusively the responsibility of the entity.

<table>
<thead>
<tr>
<th>PCI DSS REQUIREMENT</th>
<th>TESTING PROCEDURES</th>
<th>COMPLIANCE AND GUIDANCE</th>
<th>SUPPORTED</th>
</tr>
</thead>
</table>
| 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. | 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. | Partially Supported Capability.  
MBES centralized web updates provide the latest intelligence on threats, attackers, and other significant information.  
Although Malwarebytes continuously provides an evaluation and threat ranking service, evaluation of the threat against the vulnerabilities and assigning a risk ranking is exclusively the responsibility of the implementing organization. | ✔ |
|  | 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 | | ✔ |
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.

“high risk” and “critical” vulnerabilities.

- Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.

| Table 4 - PCI DSS Requirement 6 |
**REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA**

MBES Management Console and the companion Anti-Malware and Anti-Exploit components collect detection and Event Activity Monitoring (EAM) data. All data is centrally recorded into the activity database on the Management Console server and optionally streamed to external syslog servers or SIEM systems.

<table>
<thead>
<tr>
<th>PCI DSS REQUIREMENT</th>
<th>TESTING PROCEDURES</th>
<th>COMPLIANCE AND GUIDANCE</th>
<th>SUPPORTED</th>
</tr>
</thead>
</table>
| 10.1 Implement audit trails to link all access to system components to each individual user. | 10.1 Verify, through observation and interviewing the system administrator, that:  
- Audit trails are enabled and active for system components.  
- Access to system components is linked to individual users. | Partially Supported Capability.  
Malwarebytes Anti-Malware and Anti-Exploit suites record running processes and meta data associated with the processes. Any specific activity performed within applications is not visible to MBES. | ✓ |
| 10.2 Implement automated audit trails for all system components to reconstruct the following events: | 10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: | | |
| 10.2.1 All individual user accesses to cardholder data | 10.2.1 Verify all individual access to cardholder data is logged. | Support Not Available. Out of the scope of Anti-Malware. | |
| 10.2.2 All actions taken by any individual with root or administrative privileges | 10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged. | Partially Supported Capability.  
Malwarebytes Endpoint Security elements record running processes and meta data associated with root or administrative privilege. | ✓ |
| 10.2.3 Access to all audit trails | 10.2.3 Verify access to all audit trails is logged. | Supported Capability.  
All activity recorded by Malwarebytes Endpoint Security is stored in the Management Server database. The database is extensible to users with credentials approving access. | ✓ |
| 10.2.4 Invalid logical access attempts | 10.2.4 Verify invalid logical access attempts are logged. | Support Not Available. | |
| 10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or | 10.2.5.a Verify use of identification and authentication mechanisms is logged. | Partially Supported Capability.  
MBES records if its identification and authentication mechanism is running and all access to it is maintained in the system event logs. | ✓ |
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10.2.5</strong></td>
<td>Deletions to accounts with root or administrative privileges</td>
<td>Support Not Available.</td>
</tr>
<tr>
<td><strong>10.2.5.b</strong></td>
<td>Verify all elevation of privileges is logged.</td>
<td>Support Not Available. Beyond scope of Malwarebytes Endpoint Security.</td>
</tr>
<tr>
<td><strong>10.2.5.c</strong></td>
<td>Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.</td>
<td>Support Not Available.</td>
</tr>
<tr>
<td><strong>10.2.6</strong></td>
<td>Initialization, stopping, or pausing of the audit logs</td>
<td>Available Capability.</td>
</tr>
<tr>
<td><strong>10.2.6</strong></td>
<td>Verify the following are logged: - Initialization of audit logs - Stopping or pausing of audit logs</td>
<td></td>
</tr>
<tr>
<td><strong>10.2.7</strong></td>
<td>Creation and deletion of system-level objects</td>
<td>Support Not Available.</td>
</tr>
<tr>
<td><strong>10.2.7</strong></td>
<td>Verify creation and deletion of system level objects are logged.</td>
<td>Supported Capability.</td>
</tr>
<tr>
<td><strong>10.3</strong></td>
<td>Record at least the following audit trail entries for all system components for each event:</td>
<td>Available Capability.</td>
</tr>
<tr>
<td><strong>10.3.1</strong></td>
<td>User identification</td>
<td>Available Capability. MBES records the user identification for all collected activities.</td>
</tr>
<tr>
<td><strong>10.3.2</strong></td>
<td>Type of event</td>
<td>Available Capability. MBES keeps a record of the type of process/activity for all anti-malware activities.</td>
</tr>
<tr>
<td><strong>10.3.3</strong></td>
<td>Date and time</td>
<td>Available Capability. MBES suite records the date and time stamp for all collected activities.</td>
</tr>
<tr>
<td><strong>10.3.4</strong></td>
<td>Success or failure indication</td>
<td>Support Not Available. Out of scope for Anti-Malware.</td>
</tr>
<tr>
<td><strong>10.3.5</strong></td>
<td>Origination of event</td>
<td>Partially Supported Capability. The Anti-Exploit Agent records the origination of the exploit event (parent process, exploited process, etc.).</td>
</tr>
<tr>
<td><strong>10.3.6</strong></td>
<td>Identity or name of affected data, system component, or resource.</td>
<td>Support Not Available. Out of scope for MBES.</td>
</tr>
</tbody>
</table>
| 10.4 | Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.  
Note: One example of time synchronization technology is Network Time Protocol (NTP). | 10.4 | Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS requirements 6.1 and 6.2. | Supported Capability.  
All systems in MBES receive time signals from reputed external sources.  
Implementation of time synchronization on the monitored systems is exclusively the responsibility of the entity. | ✓ |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5</td>
<td>Secure audit trails so they cannot be altered.</td>
<td>10.5</td>
<td>Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:</td>
<td></td>
</tr>
<tr>
<td>10.5.1</td>
<td>Limit viewing of audit trails to those with a job-related need.</td>
<td>10.5.1</td>
<td>Only individuals who have a job-related need can view audit trail files.</td>
<td>Supported Capability.</td>
</tr>
</tbody>
</table>
| 10.5.2 | Protect audit trail files from unauthorized modifications. | 10.5.2 | Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. | Partially Supported Capability.  
Via either Active Directory role-based access controls and Mac IOS ugo (User/Group/Other) permissions and group rights enforcement.  
Physical and network segregation do not apply to MBES. | ✓ |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | 10.5.3 | Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. | Supported Capability.  
With or without the use of a syslog server or SIEM system. | ✓ |
| 10.5.4 | Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | 10.5.4 | Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media device. | Supported Capability.  
All recorded activity is transported to the Management Console server database and off-system to syslog and SIEM services. | ✓ |
| 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. | Partially Supported Capability.  
MBES generates all logs directly to a SQL database, which is protected by MS SQL integrity checking and runs standard SQL/ADC authentication. | ✓ |
| 10.6 | Review logs and security events for all systems | 10.6 | Perform the following: | | |
components to identify anomalies or suspicious activity.

Note: Log harvesting, parsing, and alerting tools may be used to meet this requirement.

10.6.1 Review the following 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.).

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 that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)

Partially Supported Capability.

For all activity, collected by and transported to the Management Server.

CHD/SAD logging is out of scope for non-system components that either don’t have MBES installed or are not protected from malware.

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.)

✅
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Support Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.6.2</td>
<td>Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment.</td>
<td>Partially Supported Capability. For all activity, collected by MBES and transported to the Management Console server, detection and alerting capabilities are built in. Out of scope for MBES.</td>
</tr>
<tr>
<td>10.6.2.a</td>
<td>Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy.</td>
<td></td>
</tr>
<tr>
<td>10.6.2.b</td>
<td>Examine the organization’s risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization’s policies and risk management strategy.</td>
<td></td>
</tr>
<tr>
<td>10.6.3</td>
<td>Follow up exceptions and anomalies identified during the review process.</td>
<td>Support Not Available. Out of scope for MBES. This is a process requirement that is the responsibility of the implementing organization.</td>
</tr>
<tr>
<td>10.6.3.a</td>
<td>Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.</td>
<td></td>
</tr>
<tr>
<td>10.6.3.b</td>
<td>Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.</td>
<td></td>
</tr>
<tr>
<td>10.7</td>
<td>Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).</td>
<td>Supported Capability. All recorded activity is transported to the Management Server logging mechanism and the database, plus any duplication to syslog entities. Retention may be customized to support all activity being retained for at least a period of 1 year by default. A programmable interval of activity is available immediately via the console. MBES has processes in place to modify the retention period of activity, for immediate availability in console to a period of 90 days.</td>
</tr>
<tr>
<td>10.7.a</td>
<td>Examine security policies and procedures to verify that they define the following: - Audit log retention policies - Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online</td>
<td></td>
</tr>
<tr>
<td>10.7.b</td>
<td>Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.</td>
<td></td>
</tr>
<tr>
<td>10.7.c</td>
<td>Interview personnel and observe processes to verify that at least the last three months’ logs are immediately available for analysis.</td>
<td></td>
</tr>
<tr>
<td>10.8</td>
<td>Additional requirement for service providers only: Implement a process for the timely detection and reporting</td>
<td>Partially Supported Capability. MBES records creation and deletion of executables and</td>
</tr>
</tbody>
</table>
of failures of critical security control systems, including but not limited to failure of:
- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

**10.8.b** Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.

**10.8.1 Additional requirement for service providers only:**
Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:
- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- Implementing controls to prevent cause of failure from reoccurring

**10.8.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure and include:
- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- Implementing controls to prevent cause of failure from reoccurring


This is a process requirement that is the responsibility of the entity.

Both Anti-Malware and Anti-Exploit technologies perform integrity checks via digital signatures and hash validation of certain update components.
Resuming monitoring of security controls

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 10.8.1.b | Examine records to verify that security control failures are documented to include:  
- Identification of cause(s) of the failure, including root cause  
- Duration (date and time start and end) of the security failure  
- Details of the remediation required to address the root cause |  

10.9 | Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.  
| Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are:  
- Documented,  
- In use, and  
- Known to all affected parties. | Support Not Available. Out of scope for MBES.  
This is a process requirement that is the responsibility of the entity. |

Table 5 - PCI DSS Requirement 10
**REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES**

Execution of vulnerability scans and penetrations tests are the responsibility of the implementing organization. MBES provides intrinsic host-based intrusion detection capabilities via capturing suspicious activity like “phone home”, NMAP scanning, and Bot-net behavior.

<table>
<thead>
<tr>
<th>PCI DSS REQUIREMENT</th>
<th>TESTING PROCEDURES</th>
<th>COMPLIANCE AND GUIDANCE</th>
<th>SUPPORTED</th>
</tr>
</thead>
</table>
| 11.4 Use intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment, as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up to date. | 11.4.a Examine system configurations and network diagrams to verify that techniques (such as intrusion detection systems and/or intrusion prevention systems) are in place to monitor all traffic:  
- At the perimeter of the cardholder data environment  
- At critical points in the cardholder data environment. | Partially Supported Capability. Malwarebytes Endpoint Security can detect certain patterns of intrusion on the endpoints it protects and can implement prevention and repair methods. Many systems are out of scope for protection by MBES where endpoint software is not available: for example, routers, switches, and other appliances not based on Windows or Mac operating systems. | ✓ |
| | 11.4.b Examine system configurations and interview responsible personnel to confirm intrusion detection and/or intrusion prevention techniques alert personnel of suspected compromises. | | ✓ |
| | 11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion detection and/or intrusion prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | | ✓ |

*Table 6 - PCI DSS Requirement 11*
COALFIRE OPINION
The Payment Card Industry Data Security Standard version 3.2 (PCI DSS v3.2) was developed to protect cardholder data (CHD) and sensitive authentication data (SAD) from loss, theft, and exploitation and has been mandated by the Card Brands since introduction in 2005. Technical products are used in conjunction with other measures to address information system security controls enumerated within the specific requirements of the standard. Malwarebytes is a technical product candidate for this purpose.

In our opinion, the Malwarebytes Endpoint Security version 1.7.7 solution is effective in providing significant and substantial support for the key requirements and controls of PCI DSS and can assist in a comprehensive program of cybersecurity for merchants, issuing banks, processors, services providers, and other entities required to comply with PCI DSS v3.2.

Our opinion is dependent on a number of underlying presumptions, which are listed here:

- Installation of server and workstation operating systems follow vendor best practices and recommended hardening after deployment
- Hardening of the Microsoft Active Directory for SQL has been performed and logging is enabled
- Other aspects of the cardholder data environment (CDE) are PCI DSS compliant
- The recommended best practice of network segmentation is used to reduce PCI DSS scope
- All type 1 (direct CHD storage, processing and transmission) and type 2 (connected to type 1) have anti-malware software installed and centrally managed
- Required logging support systems and ideally SIEM functionality are deployed and pervasive
- Alignment of technical controls with actual PCI entity missions, roles, responsibilities, policies, procedures, baselines, mandates, etc.
- Physical and organizational controls are established and in force
- Presence and/or availability of IT staff at the payment card entity and any service providers

A COMMENT REGARDING REGULATORY COMPLIANCE
Coalfire disclaims generic suitability of any product to cause a customer using that product to achieve regulatory compliance. Customers attain compliance through a Governance, Risk Management, and Compliance (GRC) program, not via the use of a specific product. This is true for PCI DSS compliance required entities as well as for customers targeting compliance with other regulations.

REFERENCES
ACKNOWLEDGEMENTS

The author would like to acknowledge the following individuals from Malwarebytes for their input on this PCI DSS Product Applicability Guide: Ken Liao as the executive sponsor of this project and Pedro Bustamante for his technical contributions and timely support. The author is also thankful to Brittany Miller at Coalfire for managing the project efficiently.

ABOUT MALWAREBYTES

“Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company’s flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.”

They may be contacted on the web at http://malwarebytes.com/business, via email corporate-sales@malwarebytes.com, or by telephone 1.800.520.2796.
ABOUT THE AUTHORS AND CONTRIBUTORS

Chris Krueger | Author | Managing Principal, Cyber Engineering, Coalfire
Chris contributes as an author and thought leader on information security and regulatory compliance topics for Coalfire’s clientele in the “new and emerging” technical areas.

Jason Macallister | Reviewer | Senior Consultant, Cyber Engineering, Coalfire
Jason consults on information security and regulatory compliance topics as they relate to advanced infrastructure, emerging technology, and cloud products.

Pedro Bustamante | Technical SME | Vice President Technology, Malwarebytes
Pedro envisions the future of advancements and threats that will impact the industry while leading his innovative team of engineers and developers to find proactive solutions. Pedro joined Malwarebytes in 2013 and was co-founder of the company’s anti-exploit technology.

Published June 2017.

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