TRAPS ADVANCED ENDPOINT PROTECTION SECURITY SOLUTION FOR PCI DSS COMPLIANCE WHITEPAPER

September, 2016

Prepared For:

Palo Alto Networks

Prepared by:

Coalfire Systems

North America I Latin America I Europe

877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

Executive Summary **3**
Audience 4
Methodology 4
PCI DSS Compliance Overview 4
Compensating Controls 5
Summary Findings 5
Application Architecture and Security **6**
Exploit & Malware Prevention **6**
Technical Assessment **9**
Validation Findings for TRAPS Application 10

EXECUTIVE SUMMARY

Palo Alto Networks, Inc. (Palo Alto) engaged Coalfire Systems Inc. (Coalfire), as a respected Payment Card Industry (PCI) Payment Application – Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of their Traps Advanced Endpoint Protection application as it pertains to security and Payment Card Industry Data Security Standard (PCI DSS) scope.

The purpose of this white paper is to provide an overview of Coalfire's assessment of the Traps architecture and to confirm to what extent Traps helps satisfy PCI DSS 3.2 requirements. The scope of the PCI DSS controls selected for validation was derived through collaboration with Palo Alto Networks development team and Coalfire assessors. The review and testing was performed based on the use cases generated for validation of PCI DSS requirements that are addressed when Traps solution is utilized.

The assessment performed included the following components:

- Review overall design and architecture of Traps solution.
- Technical Testing and related evidence collection for the use cases provided:
  - Re-performance testing of the solution
  - Observation of the solution including installation, configuration and functional capabilities
- Interviews with Subject Matter Experts (SMEs).
- Review and feedback of supporting documentation.

It's Coalfire's determination that an organization who was using a traditional AV to remain PCI DSS compliant can confidently replace that solution with Traps and remain compliant. There are no known inhibitors identified with the Traps solution which would prevent an organization from implementing it in a PCI environment. Additionally, there are features within the Traps which facilitate meeting certain PCI DSS requirements. Every organization has unique business, technical and security governance requirements, as a result this paper does not provide detailed recommendations for how to configure Traps application to meet the applicable portions of the PCI DSS and merchants should consult with their QSA to ensure proper implementation.

Traps application provides the flexibility to enable, manage, and meet PCI DSS requirements in multiple areas of the standard. Traps solution also helps organizations with various PCI requirements such as ensuring anti-virus mechanisms are enabled and maintained, not only meeting the requirement in many study cases, but often exceeding it when compared to industry standard solutions available. Proper implementation can also support the development of compensating controls for requirements such as anti-virus and patching (protection of unpatched systems).

Traps architecture and implementation requirements can be deployed in a PCI environment allowing a customer to meet PCI requirements.

Traps is a security solution that also helps satisfy PCI DSS requirements in areas such as logging requirements and ability to track suspicious activities and audit trail retention.

AUDIENCE

This assessment white paper has three target audiences:

- QSA and Internal Audit Community: This audience may be evaluating Traps solution to assess merchant or service provider environment for PCI DSS.
- Administrators and Other Compliance Professionals: This audience may be evaluating Traps for use within their organization for compliance requirements other than PCI DSS.
- Merchant and Service Provider Organizations: This audience is evaluating Traps for deployment in their cardholder data environment and what benefits could be achieved from using this solution.

METHODOLOGY

Coalfire has implemented industry best practices in our assessment and testing methodologies. Coalfire completed a multi-faceted technical assessment process during the course of this project using common PCI environmental scenarios and best practices. Coalfire conducted technical lab testing remotely on 8/1/2016.

The outcome of this testing provides verification that customers implementing Traps will be able to meet specific PCI DSS control requirements in their real world cardholder data environments as well as support developing of compensating controls. A broad spectrum of network, system and application scenarios was used in our validation testing. Test results and lab configurations are summarized in the technical section of the white paper.

PCI DSS COMPLIANCE OVERVIEW

PCI DSS applies to all organizations that store, process or transmit cardholder data. This includes entities such as merchants, service providers, payment gateways, data centers and outsourced service providers. PCI Standard is mandated by the card brands and administered by the PCI SSC Council. The PCI DSS standard specifies 12 requirements for compliance organized into six major control objectives.

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

COMPENSATING CONTROLS

Compensating controls can be utilized by merchant or service provider organizations to achieve compliance for PCI DSS requirements when an entity cannot currently meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls. [1]

Compensating controls are however required to satisfy the following listed criteria:

1. The intent and rigor of the original PCI DSS requirement has to be met.
2. A similar level of defense as the original PCI DSS requirement has to be provided, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

This whitepaper assumes that the reader is familiar with PCI DSS and relevant guidance publications, card brand requirements and any other supplemental documents from PCI SSC council.

SUMMARY FINDINGS

- Traps architecture and implementation requirements can be deployed in a PCI environment allowing a customer to meet PCI requirements.
- When implemented properly, Traps can provide protection against current malware that targets Point of Sale Systems or any other system within cardholder data environment.
- Traps can provide ability to detect and prevent malware, minimizing the impact of data breach when implemented appropriately.
- When properly configured, Traps can provide audit trail of all detected malware and keep records for required timeframe. Application does also provide functionality to integrate with centralized logging system as required by PCI DSS.
- Compared to other industry standard AV solutions Traps provides additional protection in multiple areas of PCI DSS standard where development of compensating controls is possible.
- When properly deployed and configured, Traps solution can satisfy specific PCI DSS requirements or support the development of compensating controls to meet PCI DSS requirements:

PCI Requirement	Traps Advanced Endpoint Protection	
	Directly Meets Requirements	Supports the Development of Compensating Controls
1.4		✶
2.2.3		✶
5.1	✶	
5.2		✶
5.3	✶	

[1] https://www.pcisecuritystandards.org/security_standards/documents.php

6.2		✶
10.3	✶	
10.5.1, 10.5.2, 10.5.3, 10.5.4	✶	
10.7	✶	
11.2		✶

Note: Traps has to be configured according to the instructions provided in the administrator's guide in order to meet PCI DSS requirements.

APPLICATION ARCHITECTURE AND SECURITY

The Traps solution, which comprises a central Endpoint Security Manager (an ESM Server, ESM Console, and database) and the Traps agent protection software installed on each endpoint, takes an effective approach in preventing malicious attacks. Rather than try to keep up with the ever-growing list of known threats, Traps sets up a series of roadblocks that prevent the attacks at their initial entry points—that point where legitimate executable files are about to unknowingly allow malicious access to the system.

Traps targets software vulnerabilities in processes that open non-executable files using exploit prevention techniques. Traps also uses malware prevention techniques to prevent malicious executable files from running. Using this two-fold approach, the Traps solution can prevent all types of attacks, whether they are known or unknown threats.

Traps enterprise solution consist of multiple components:

- Component one – Traps agent
- Component two – Endpoint Security Manager (an ESM Server, ESM Console, and database)
- Component three – The WildFire service is a natively integrated cloud-based malware analysis service.

EXPLOIT & MALWARE PREVENTION

When a user opens a non-executable file, such as a PDF or Word document, and the process that opened the file is protected, the Traps agent seamlessly injects code into the software. This occurs at the earliest possible stage before any files belonging to the process are loaded into memory. The Traps agent then activates one or more Exploit Protection Modules (EPMs) inside the protected process. The EPM targets a specific exploitation technique and is designed to prevent attacks on program vulnerabilities based on memory corruption or logic flaws.

Examples of attacks that the EPMs can prevent include dynamic-link library (DLL) hijacking (replacing a legitimate DLL with a malicious one of the same name), hijacking program control flow, and inserting malicious code as an exception handler.

In addition to automatically protecting processes from such attacks, Traps reports any prevention events to the Endpoint Security Manager, and performs additional actions according to the settings of the security policy rules. Common actions that Traps performs include collecting forensic data and notifying the user about the event.

The default endpoint security policy protects the most vulnerable and most commonly used applications, but users can also add other third-party and proprietary applications to the list of protected processes.

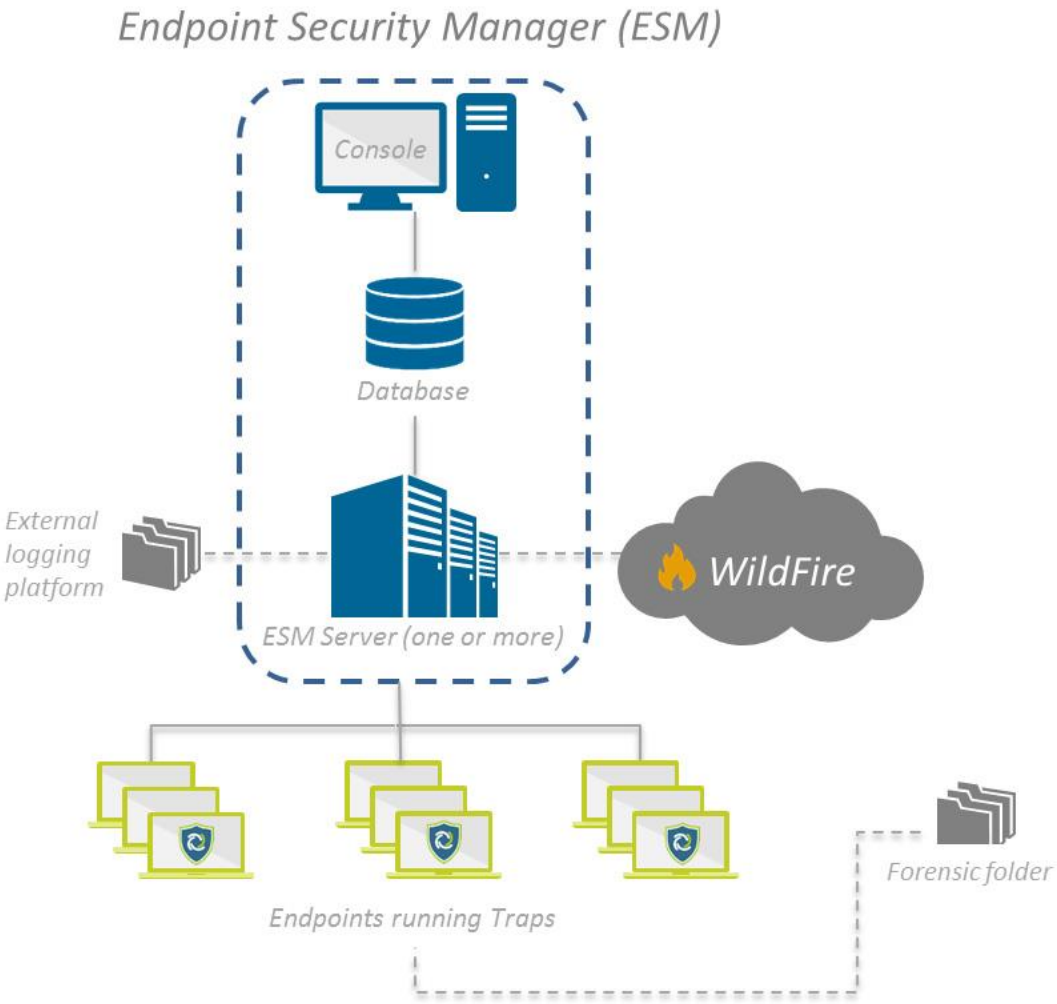
Malicious executable files, known as malware, are often disguised as or embedded in non-malicious files. These files can attempt to gain control, gather sensitive information, or disrupt the normal operations of the system.

To protect endpoints from malware, Traps uses a unique multi-method malware prevention approach which combines several prevention methods to prevent known and unknown malware from infecting a system:

1. Local Analysis via Machine Learning: This method delivers an instantaneous verdict for any unknown executable before it is allowed to run. Traps examines hundreds of the file's characteristics, without reliance on signatures, scanning or behavioral analysis.
2. WildFire Inspection and Analysis: Leverages the power of Palo Alto Networks WildFire (tm) cloud-based malware analysis environment to detect unknown malware and automatically reprogram Traps to prevent known malware.
3. Trusted Publisher Execution Restrictions: allows organizations to identify executable files that are among the "unknown good" because they are published and digitally signed by trusted publishers-entities that Palo Alto Networks recognizes as reputable software publishers.
4. Policy-Based Execution Restrictions-Organizations can easily define policies to restrict specific execution scenarios, thereby reducing the attack surface of any environment. For example, Traps can prevent the execution of files from the Outlook "temp" directory or prevent the execution of a particular file type directly from a USB drive.
5. Admin Override Policies- Define policies, based on the hash of an executable file, to control what is allowed to run in any environment and what is not. This fine-grained whitelisting (or blacklisting) capability controls the execution of any file, based on user-defined conditions that tie into any object that can be defined with Microsoft Active Directory.

APPLICATION ARCHITECTURE

The Traps solution consists of the Endpoint Security Manager (ESM) and the Traps agent protection software. The Traps agent is installed on each endpoint in the organization.
The following diagram displays the Traps components and their relationships to each other and to other security components.


Endpoint Security Manager (ESM)
Console
Database
External logging platform
WildFire
ESM Server (one or more)
Forensic folder
Endpoints running Traps

TECHNICAL ASSESSMENT

Coalfire assessor performed testing using remote Palo Alto Networks environment running Windows 2012 Server with Endpoint Security Manager (ESM) as well as Windows 7 with the Traps agent.

The scope of the assessment was defined with the following tasks:

- Understand product functionality, architecture, implementation and operation
- Review installation guidance and supporting documentation
- Test Traps product for required controls in the lab environment
- Review and verify Traps administrator's guide for any hardening best practices
- Review Traps configurations and capabilities
- Verification of solution for security and compliance
- Review and validate how Traps provides compliance support for organizations.
    - Review and testing for use of product as compensating control for not having current patches on End of Life (EOL) operating systems for e.g. Windows XP, Windows 2003
    - Review and testing for use of product as antivirus
    - Review and testing for use of product as personal firewall
    - Review and testing of configurations for monitoring and logging requirements as defined by PCI DSS in Requirements 10.1 – 10.8

Note: The assessment was focused on the product's ability to satisfy certain PCI DSS requirements and was not a complete review of the Traps product.

VALIDATION FINDINGS FOR TRAPS APPLICATION

PCI Requirement	How Traps Supports PCI Compliance	Test Procedure
PCI DSS Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	The Traps solution can help in developing compensating control for this requirement. • Traps agent can stop processes that perform malicious activity, including processes that work through the network. • Traps provides signature-less detection and prevention of advanced threats. • Traps provides recorded history of all endpoint and server activity to rapidly respond to alerts and incidents.	Deployed Traps agent and attempted to exploit system through the metasploit console and a known vulnerability in the system. Without Traps agent vulnerable application that was listening on network port would be easily exploited resulting in the system being breached. Traps agent was able to block the malicious process and provided alert notification in the ESM administrator backend.
PCI DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	The Traps solution can help in developing compensating control for this requirement whenever insecure services and protocols are used. Traps solution can provide additional security features for any insecure services. • Traps agent can stop processes that perform malicious activity, including insecure processes that could be exploited. • Traps provides signature-less detection and prevention of advanced threats. • Traps provides recorded history of all endpoint and server activity to rapidly respond to alerts and incidents.	Deployed Traps agent and attempted to exploit system through the metasploit console. For the insecure services and daemons running, the Traps solution was able to prevent any malicious activity and block the process that was misused with alert notification provided in the ESM administrator backend.
PCI DSS Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs		
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**Traps** software is capable of detecting, removing and protecting against all known types of malicious software. • Traps can stop cyber threats that evade antivirus and other traditional defenses using zero-day and targeted attacks. • Traps provides signature-less detection and prevention of advanced threats	Deployed Traps agent and attempted to run various software including malicious software on the system with Traps endpoint agent. Traps was able to block the attempt and provided alert notification in the ESM administrator backend. Traps also has a quarantine feature that is

PCI Requirement	How Traps Supports PCI Compliance	Test Procedure
	• Traps provides recorded history of all endpoint and server activity to rapidly respond to alerts and incidents	capable of moving known malicious files to a local quarantine folder.
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.	**Traps** can be used on systems not affected commonly by malicious software to identify threats on such systems • Traps provides signature-less detection and prevention of advanced threats	Deployed Traps agent and attempted to install various software including malicious software on the system with Traps installed and configured. Traps was able to block the attempt and provided alert notification in the ESM administrator backend.
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.	The Traps solution can help in developing compensating control for this requirement. Application, being an AV replacement, however works in different manner than a typical AV software. It does not require to maintain database with current signatures of malicious files on each local endpoint system. Instead, Traps performs this activity on the enterprise centralized ESM servers, by utilizing its WildFire cloud service with the latest list of known malicious file's signatures. Any file that raised attention on the local system is sent over the network to the centralized server for detailed analysis. Additionally Traps agent has capabilities to detect malicious software by statically analyzing file before it is allowed to execute and immediately prevent malicious activity. Therefore, by having different than the typical AV architecture, there are multiple capabilities that can help develop compensating controls for this requirement. • Automatic updates are not required on the endpoint systems, instead current database with the latest signatures is available on the WildFire cloud service where automatic updates are applied constantly. • Periodic scans are not required since all processes that are executed would be analyzed for any malicious activity instantly. • Traps solution log generation is always enabled and the logs can be retained in the ESM administrator backend (or forwarded to the centralized	Deployed Traps agent and ESM component that worked with WildFire cloud service. Attempted to install various software including malicious software on the system with Traps installed and configured. Compared performance with the industry standard AV solution and confirmed that in many cases, malicious software with modified hash was discovered by Traps and not discovered by other industry standard signature based AV software . Traps was able to block the attempt and provided alert notification in the ESM administrator backend. Performed multiple test scenarios where different type of vulnerabilities were used. Observed logs were generated and retained on the ESM enterprise server.

PCI Requirement	How Traps Supports PCI Compliance	Test Procedure
	logging system) for as long as it is required by the administrator.	
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.	The Traps agent is started during windows OS boot up and is actively running as a service in the background. • Traps can continuously monitor and record all activity on endpoint and servers. • Traps only works as deeply integrated with underlying OS software that end users cannot disable unless authorized administrator grants that access.	Deployed Traps agents on servers and attempted to stop Traps Service and uninstall Traps software, assessor was unable to do so without knowing administrative credentials. Traps tamper protection is enabled by default, starts as a systems service and only Traps administrators can enable/disable the agent from within the ESM administrator backend.
PCI DSS Requirement 6: Develop and maintain secure systems and applications		
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Traps can be used in developing a compensating control for systems with no current patches or for the systems that do not have patches available (e.g. Windows XP, Windows 2003 servers) • Traps can stop cyber threats that evade antivirus and other traditional defenses using zero-day and targeted attacks, even on unpatched systems. • Traps system service running on an endpoint system will block all exploitation of a vulnerable application; even though the application would remain vulnerable, any exploit would fail. • Traps provides recorded history of all endpoint and server activity to rapidly respond to alerts and incidents	Assessor attempted to install unknown/malicious executable files on the system, Traps software was able to block the execution of the software. Unpatched underlying OS system vulnerability was attempted to be exploited and failed with the notification sent to the ESM server.
PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data		
10.3.1 Verify user identification is included in log entries.	Traps can record user identification in audit trails for all types of generated events.	For all records logged, observed user identification (for e.g. administrator and System) information was included for the action or event that occurred.
10.3.2 Verify type of event is included in log entries.	Traps can record type of event in audit trails for all types of generated events.	For all records logged, observed type of event (for e.g. addition, modification to software or files) was included for the action or event that occurred.
10.3.3 Verify date and time stamp is included in log entries.	Traps can record date and time stamp in audit trails for all types of generated events.	For all records logged, observed date and time stamp was included for the action or event that occurred.
10.3.4 Verify success or failure indication is included in log entries.	Traps can record success indication in audit trails for all types of generated events.	For all records logged, observed success indication (for e.g. Login successful) was included for the action or event that occurred.

PCI Requirement	How Traps Supports PCI Compliance	Test Procedure
10.3.5 Verify origination of event is included in log entries.	Traps can record origination of event in audit trails for all types of generated events.	For all records logged, observed origination of event (for e.g Name of system component, IP address) was included for the action or event that occurred.
10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	Traps can record identity or name of affected data, system component, or resources in audit trails for all types of generated events.	For all records logged, observed identity or name of affected data, system component, or resources (for e.g. Name of system component) was included for the action or event that occurred.
10.5.1 Only individuals who have a job-related need can view audit trail files.	Audit trails can be viewed by administrators via the ESM application and audit trail files/DB access can be restricted by organization on job need basis.	Observed that only authorized users can login and access audit files within the ESM software. Local copy of Traps logs are not available for local users, but stored in secured folder.
10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	ESM collects data from all endpoint systems, however that data cannot be accessed unless user has access to the ESM. It is organization's responsibility to ensure access to server is restricted to authorized individuals and that system is segmented appropriately in network.	Assessor observed the Traps server and the system components in a test network zone and verified that ESM administrative component is available only for administrator in the enterprise backend, as instructed in the administrator's guide document. Audit trail files could not be accessed from endpoint systems where the Traps agent is installed.
10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	ESM collects data from all endpoint systems, organization can choose to review and maintain the ESM logs configure logs to be forwarded to centralized logging server.	Collected data from various system components on the Traps server and had access control in place to restrict access to log information. Audit trail file data is difficult to alter as users have to create watchlists and process criteria in order to view the information as required for PCI DSS requirements.
10.7 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).	Using ESM application, all audit trail history can be retained within the server indefinitely. The data can be immediately available for analysis.	Traps settings were observed to confirm that the event log is configured to store logs indefinitely by the default. Traps can hold event log files and data can be backed-up by customer to centralized server. Retention policy can be configured by organization to meet current PCI policies. **Exception:** Depends on the capacity of server and how much data organizations are willing to keep available. It is organizations responsibility to have log data backed up to centralized log server if the server runs out of space.
PCI DSS Requirement 11: Regularly test security systems and processes		

PCI Requirement	How Traps Supports PCI Compliance	Test Procedure
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Traps application can help develop compensating controls for this requirement. It provides proactive approach to organizations to analyze data in real-time so that no vulnerability can be exploited. Process for responding to alerts received remains the responsibility of the merchant/ service provider organization.	Deployed Traps agent and attempted to run various software including malicious software on the system with Traps endpoint agent. Traps was able to block the attempt and provided alert notification in the ESM administrator backend.

CONCLUSION:

After reviewing the requirements of PCI DSS, Coalfire has determined through review of business impact and technical assessment that Traps solution as outlined in this document meets several PCI DSS requirements. The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of the Traps products in the context in which it is implemented.

Traps application demonstrated high levels of performance compared to industry standard solutions available. Innovative malware and exploit prevention mechanisms provided by Traps application allow for excellent performance in the real world scenarios.

It's Coalfire's determination that an organization that was using a traditional AV to remain PCI DSS compliant can confidently replace that solution with Traps and remain compliant.

Traps can be used as a direct or compensating control for several PCI DSS requirements (as detailed on page 5-6), helping organizations meet the evolving compliance and security needs of their environments. Traps aligns with compliance requirements related to:

- Audit trail retention
- Antivirus requirements
- Patch requirements (protection of unpatched/end-of-life systems)

ABOUT COALFIRE

Coalfire is the global technology leader in cyber risk management and compliance services for private enterprises and government organizations. Our professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple cyber risk management and compliance objectives, tied to a long-term strategy to prevent security breaches and data theft.