tripwire CONFIDENCE: SECURED

WHITE PAPER

PCI DSS 3.2 COMPLIANCE WITH TRIPWIRE SOLUTIONS

TRIPWIRE ENTERPRISE
TRIPWIRE LOG CENTER
TRIPWIRE IP360
TRIPWIRE PURECLOUD

A UL TRANSACTION SECURITY (QSA) AND TRIPWIRE WHITE PAPER

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

CONTENTS

TRADEMARK ACKNOWLEDGEMENTS

The following are trademarks or registered trademarks of Tripwire, Inc.:

- Tripwire
- Log Center
- IP360

PCI Security Standards Council, LLC (the Council) is the owner of the copyright of the material known as PCI Data Security Standards (PCI DSS). PCI DSS is the exclusive property of the Council.

COPYRIGHT

PCI DSS VERSION

This whitepaper has been based on *PCI DSS Requirements and Security Assessment Procedures, Version 3.2*, and *Template for Report on Compliance for use with PCI DSS v3.2*. These documents can be obtained from the PCI SSC website at

https://www.pcisecuritystandards.org/security_standards/documents.php

The PCI SSC website contains a number of other documents that may be helpful in interpreting the PCI DSS specification. These supporting documents can be downloaded from the same location.

INTENDED AUDIENCE

This whitepaper would be a useful guide for security personnel who wants find out how Tripwire® Enterprise, Tripwire Log Center®, Tripwire IP360™ and Tripwire PureCloud could assist in meeting PCI DSS requirements. Qualified Security Assessors (QSAs) might find this document useful as it highlights the areas the PCI DSS requirements that can be verified and met by the Tripwire products reviewed in this paper. Prior knowledge of Tripwire Enterprise, Tripwire Log Center, Tripwire IP360, Tripwire PureCloud and PCI DSS is recommended.

AUTHORS

This whitepaper has been prepared by UL's Transaction Security Division in conjunction with Tripwire.

UL's Transaction Security division guides companies within the mobile, payments and transit domains through the complex world of electronic transactions. UL is the global leader in ensuring security, compliance and global interoperability. Offering advice, test and certification services, security evaluations and test tools, during the full life cycle of your product development process or the implementation of new technologies. UL's people pro-actively collaborate with industry players to define robust standards and policies. Serving you locally whilst acting globally. UL is recognized by leading industry bodies including Visa, MasterCard, Discover, JCB, American Express, EMVCo, PCI, GCF, ETSI, GSMA, GlobalPlatform, NFC Forum and many others.

For more information, go to UL-TS.com

ABOUT TRIPWIRE

Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at www.tripwire.com. Get security news, trends and insights at tripwire.com/blog.

DISCLAIMER

This document should be treated as a guide only. It does not guarantee that an organization will necessarily be compliant by following the recommendations herein. Professional advice should be sought to determine the organization's specific situation and exactly what needs to be done for the organization to achieve PCI DSS compliance. The status in regards to PCI DSS compliance will ultimately be determined by the organization's QSA.

INTRODUCTION

Any entity that processes, transmits or stores account data[1], or can impact the security of cardholder data environment (CDE)[2], is required to be compliant to the Payment Card Industry Data Security Standard (PCI DSS). In PCI DSS all system components[3], processes and people that are included in or connected to the CDE, or can impact the security of the CDE, are considered in-scope. PCI DSS comprises of 12 high level requirements. Each high level requirement includes a number of low-level requirements and each low-level requirement consists of one or more testing procedures. PCI DSS version 3.2 includes 270+ low-level requirements and 460+ testing procedures. The low-level requirements will be referred to as the "requirements" from this point onward.

During a PCI DSS assessment, testing procedures are followed by qualified security assessors (QSAs) to validate if in-scope system components, processes and people meet the intents of the requirements. This whitepaper examines the functionalities provided by Tripwire Enterprise, Tripwire Log Center, Tripwire IP360 and Tripwire PureCloud that can be used to assist entities meeting a number of PCI DSS requirements.

Tripwire Enterprise	Tripwire Log Center	Tripwire IP360	Tripwire PureCloud
32	**18**	**9**	**4**

Table 1: Summary of total number of PCI DSS requirements covered by Tripwire products

This report has been organized as follows: A brief description of the PCI DSS assessment process has been provided in the next section. The following four sections cover the overviews of Tripwire Enterprise, Tripwire Log Center, Tripwire IP360 and Tripwire PureCloud, and how these products can be used to meet PCI DSS requirements.

While Tripwire products can assist entities to comply with certain PCI DSS requirements, these products might be considered to have security impacts on the CDE and therefore would be required to comply with applicable PCI DSS requirements. The last section includes technical information about these products which would be useful to understand how they meet some key PCI DSS requirements, e.g. default user names and password.

[1] Account data consists of the following components:

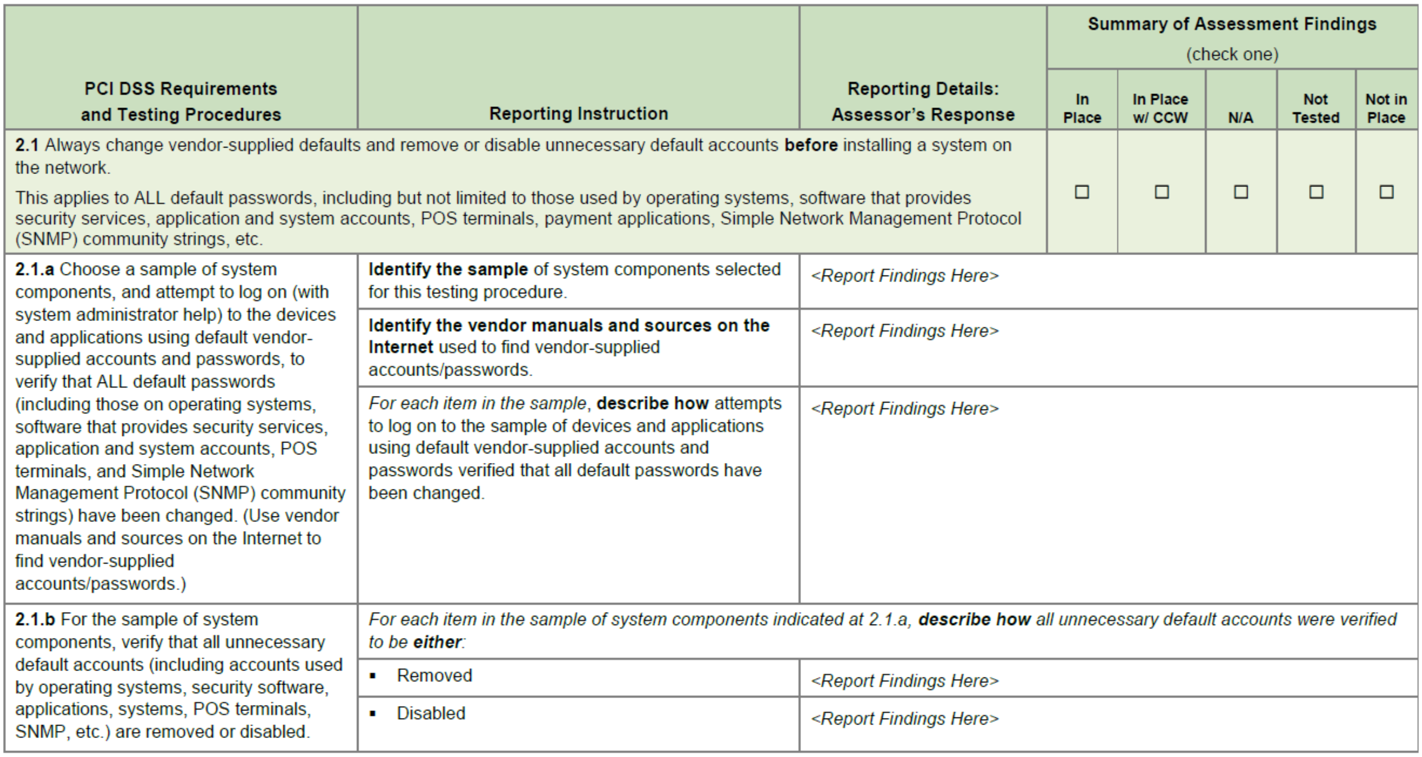
- Cardholder data (CHD) consisting of primary account number (PAN), cardholder name, expiration date and service code
- Sensitive authentication data (SAD) which includes consisting of full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PINs/PIN blocks

[2] Cardholder data environment or CDE refers to the system components (e.g. servers, applications, firewalls etc.), people and processes that store, process or transmit cardholder data or sensitive authentication data. A system component that has not been segmented from the system components within the CDE is considered part of the CDE.

[3] System components refer to servers, applications and network devices that are included in or connected to the CDE, or can impact the security of the CDE.

PCI DSS ASSESSMENT PROCESS

At the beginning of the assessment process a QSA typically defines the scope of the assessment. During this stage the QSA is required to identify all system components, processes and people that are included in or connected to the CDE, or can impact the security of the CDE. Once the scope is determined, the QSA would typically select a representative sample of the identified system components, processes and people. Then the sampled system components, processes and people would be assessed against applicable PCI DSS requirements and testing procedures. The findings of the assessment would be documented in a template called *Template for Report on Compliance (ROC) for use with PCI DSS*. PCI has published this template that outlines the type of evidence, information and level of detail a QSA is expected to provide for responding to each testing procedure in the ROC.



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.			□	□	□	□	□
2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	**Identify the sample** of system components selected for this testing procedure.	*<Report Findings Here>*					
	Identify the vendor manuals and sources on the Internet used to find vendor-supplied accounts/passwords.	*<Report Findings Here>*					
	For each item in the sample, **describe how** attempts to log on to the sample of devices and applications using default vendor-supplied accounts and passwords verified that all default passwords have been changed.	*<Report Findings Here>*					
2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	*For each item in the sample of system components indicated at 2.1.a,* ***describe how*** *all unnecessary default accounts were verified to be* ***either****:*						
	▪ Removed	*<Report Findings Here>*					
	▪ Disabled	*<Report Findings Here>*					

Figure 1: Extract from *Template for Report on Compliance (ROC) for use with PCI DSS V3.2*

An extract from the template has been provided in Figure 1. The Reporting Instruction column (i.e. 2nd column in Figure 1) contains the instructions for QSAs to follow for writing up the findings for a particular requirement and testing procedure. The template for ROC is available on PCI SSC website and it is recommended that this document is used by entities to understand what type of evidence and information a QSA is likely to look for during an assessment.

PCI DSS COMPLIANCE WITH TRIPWIRE ENTERPRISE

Tripwire Enterprise provides two product components:

- File integrity monitoring (FIM) - known as Tripwire Enterprise File Integrity Manager
- Compliance monitoring - known as Tripwire Enterprise Policy Manager

A FIM or similar technology is required for three requirements. Tripwire Enterprise File Integrity Manager can be used as a FIM to meet these requirements.

Tripwire Enterprise Policy Manager can be used to monitor configuration settings for operating systems and network devices, and alert system/network administrators if any monitored settings change. This feature can be useful to demonstrate to QSAs that monitored system components have been configured as per documented standards.

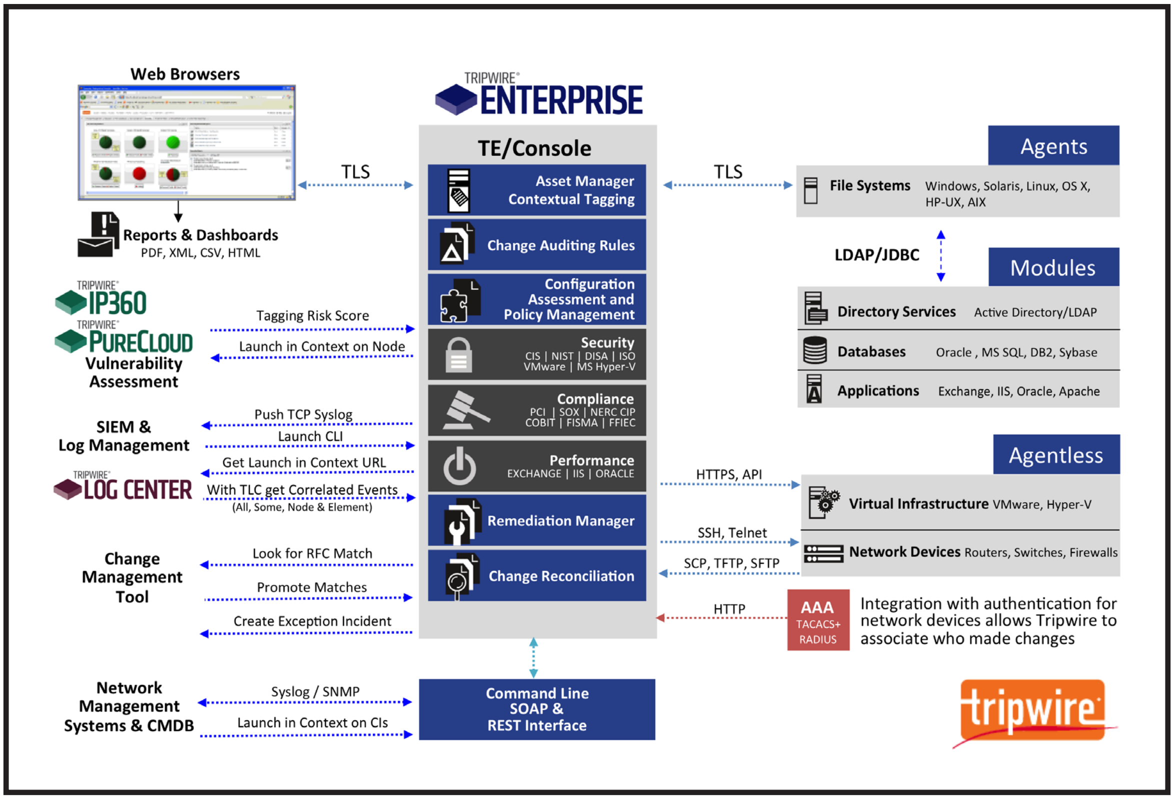


Figure 2: Tripwire Enterprise architecture

Tripwire Enterprise can be installed with either of the following modes:

1. With a single-system installation, where the Tripwire Enterprise Console software and Tripwire Enterprise database[4] are both installed on the same system (the Tripwire Enterprise Server)
2. With a distributed installation, where the Tripwire Enterprise Console software is installed on the Tripwire Enterprise Server, and the Tripwire Enterprise database on another system

In a distributed installation, the Tripwire Enterprise database is also referred to as a remote database. A remote database server is the system on which a remote database is installed.

For some types of systems (e.g. Windows, Solaris, Oracle database) Tripwire Enterprise requires a Tripwire agent to run on the target system to collect information (e.g. system settings, hashes of files) and send the information back to the Tripwire Enterprise Server to analyze. For other systems (e.g. network devices, custom applications, HP NonStop) Tripwire Enterprise needs to be used in agentless mode. In this mode Tripwire Enterprise Server would need to connect to the target system using a user name and password with appropriate privilege that would allow it to run commands/scripts to retrieve information to be analyzed within Tripwire Enterprise server.

[4] A Tripwire Enterprise database stores all data generated by Tripwire Enterprise Console.

TRIPWIRE ENTERPRISE FILE INTEGRITY MANAGER

The capabilities of the Tripwire Enterprise File Integrity Manager were reviewed in relation to the applicable PCI DSS requirements. Findings have been summarized in the next table under the Remarks column. **The areas of the PCI DSS requirements that can be verified using implementing the Tripwire Enterprise File Integrity Manager have been highlighted in bold in the ROC Reporting Instruction column.** To comply with a requirement, the items that have not been bolded also need to be met as per the ROC Reporting Details column, e.g. through interview, review documentations etc.

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	**11.5.a** Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. *Examples of files that should be monitored:* • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log and audit files* • *Additional critical files determined by entity (i.e., through risk assessment or other means)*	**Describe the change-detection mechanism deployed.** **Identify the results from monitored files reviewed to verify the use of a change-detection mechanism.** **Describe how the following verified the use of a change-detection mechanism:** • **System settings** • **Monitored files**	Tripwire Enterprise File Integrity Manager could be used to demonstrate to a QSA that a file-integrity monitoring solution is used to monitor changes to critical system files, configuration files, or content files. Tripwire Enterprise File Integrity Manager can be configured to check changes (e.g. modification, deletion) to files on a scheduled or real-time basis and send alerts if changes are detected.
	11.5.b Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly.	**Describe how system settings verified that the change-detection mechanism is configured to:** • **Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files.** • **Perform critical file comparisons at least weekly.**	
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	Identify the responsible personnel interviewed who confirm 24/7 incident response and monitoring coverage for: • Any evidence of unauthorized activity. • Detection of unauthorized wireless access points. • Critical IDS alerts. • **Reports of unauthorized critical system or content file changes.** Describe how it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for: • Any evidence of unauthorized activity. • Detection of unauthorized wireless access points. • Critical IDS alerts. • **Reports of unauthorized critical system or content file changes.**	This requirement is related to responding to alerts received from various sources, e.g. file integrity monitoring, intrusion detection or prevention. A QSA would want to see that a documented process exists to monitor and respond to alerts The QSA would also check that documented process is being followed. Alerts from Tripwire Enterprise File Integrity Manager can be used as an evidence to detect unauthorized changes to critical system or content files.

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan.	Describe how processes were reviewed to verify that **monitoring alerts from security monitoring systems** are covered in the Incident Response Plan. Describe how processes were reviewed to verify that **responding to alerts from security monitoring systems** are covered in the Incident Response Plan.	Alerts from Tripwire Enterprise File Integrity Manager can be used as one of the inputs for the incident response plan.

TRIPWIRE ENTERPRISE POLICY MANAGER

The Tripwire Enterprise Policy Manager contains a set of policies that can be used to monitor various configuration settings. It starts by performing a scan of configuration settings of the monitored system components (e.g. servers, databases and network devices) to produce a baseline configuration state, the known state. Then it compares the baseline configuration settings against settings specified in a selected Tripwire compliance policy. Tripwire Enterprise Policy Manager then generates a scorecard that shows how configurations measure up against policy. It also allows drill down from the scorecard for specific failures, and provides remediation guidance with step-by-step instructions to get failed configurations into a compliant state.

The features of the Tripwire Enterprise Policy Manager were reviewed in relation to the applicable PCI DSS requirements. Findings have been summarized in the next table under the Remarks column. Findings have been summarized in the next table under the Remarks column. **The areas of the PCI DSS requirements that can be verified using implementing the Tripwire Enterprise Policy Manager have been highlighted in bold in the ROC Reporting Instruction column.** To comply with a requirement, the items that have not been bolded also need to be met as per the ROC Reporting Details column, e.g. through interview, review documentations etc.

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	**2.1.b** For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	**For each item in the sample of system components indicated at 2.1.a, describe how all unnecessary default accounts were verified to be either:** • **Removed** • **Disabled**	Tripwire Enterprise Policy Manager can be configured to check if default accounts have been removed, renamed or disabled. A QSA would also check that if any default password and SNMP string is used. A QSA would typically perform this test by observing over the shoulder of an administrator whether login attempts with default passwords fail.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	**2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.	Identify the sample of system components selected. **For each item in the sample, describe how the enabled system services, daemons, and protocols verified that only necessary services or protocols are enabled.**	Tripwire Enterprise Policy Manager can be used to take a snapshot of all the services and processes running, and ports that are in LISTEN mode. This snapshot can be used to monitor if the list has been changed. As Tripwire Enterprise Policy Manager would be checking against a snapshot, alerts will be generated as soon as the list changes, e.g. if a process ends and starts with a new process ID.
	2.2.2.b Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.	**For each item in the sample of system components from 2.2.2.a, indicate whether any insecure services, daemons, or protocols are enabled. (yes/no)** If "no," mark the remainder of 2.2.2.b and 2.2.3 as "Not Applicable." If "yes," identify the responsible personnel interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol	A list of insecure services, processes and ports can be listed in a rule. If a system component is found to be running a service or process, or listening on a port that has been listed in this rule, this would be detected by the Tripwire Enterprise Policy Manager so that appropriate action can be taken to resolve

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	**2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.	**Describe how configuration settings verified that security features for all insecure services, daemons, or protocols are**: • Documented • **Implemented**	this issue. Documented business justifications must exist for all insecure services, processes and ports. Security features must be implemented to ensure insecure services, processes and ports can be used to compromise cardholder data or system components that store, process or transmit account data.
2.2.4 Configure system security parameters to prevent misuse.	**2.2.4.c** Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how the common security parameters verified that they are set appropriately and in accordance with the configuration standards.**	Common security parameters which are documented can be specified in rules so that Tripwire Enterprise Policy Manager can be used to automatically monitor the compliance status of operating systems, databases and network devices. If a QSA can verify that Tripwire Enterprise Policy Manager has been configured to monitor common security parameters for all in-scope system components, then the QSA could use the compliance status report as an evidence for this testing procedure.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how configurations verified that all unnecessary functionality is removed.**	Rules can be created to check the functionalities enabled (e.g. web server, DNS) in an operating system against a baseline.
	2.2.5.b Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration.	**Describe how the security parameter**s and relevant documentation verified that enabled functions are: • Documented • **Support secure configuration**	The baseline needs to be documented.
	2.2.5.c Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components.	Identify documentation examined for this testing procedure. **Describe how the security parameters verified** that only documented functionality is present on the sampled system components from 2.2.5.a.	
2.3 Encrypt all non-console administrative access using strong cryptography.	**2.3.a** Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.	Describe how the administrator log on to each system verified that a strong encryption method is invoked before the administrator's password is requested. **Describe how system configurations for each system verified that a strong encryption method is invoked before the administrator's password is requested.** **Identify the strong encryption method used for non-console administrative access.**	Tripwire Enterprise Policy Manager can be used to monitor if a secure login protocol (e.g. SSH) is supported by operating systems or network devices. If SSH or Terminal Service is used, it might be possible to create rules to monitor the security settings associated with these protocols. A QSA is might want to observe that passwords are entered only when a secure login protocol is used.
	2.3.b Review services and parameter	**Describe how services and parameter files on**	Tripwire Enterprise Policy

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
	files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	**systems verified that Telnet and other insecure remote-login commands are not available for non-console access.**	Manager can be configured to check if any insecure service (e.g. Telnet) is enabled on an operating system or network device.
	2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	Describe how the administrator log on to each system verified that administrator access to any web-based management interfaces was encrypted with strong cryptography. **Identify the strong encryption method used for any web-based management interfaces.**	Tripwire Enterprise Policy Manager can be configured to check if a web service is running and security settings (e.g. version, enabled cipher suites) associated with the web service.
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	**4.1.an** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.	Identify all locations where cardholder data is transmitted or received over open, public networks. Identify the documented standards examined. Describe how the documented standards and **system configurations both verified the use of:** • **Security protocols for all locations** • **Strong cryptography for all locations**	A QSA needs to identify all possible methods/URLs used for transmitting account data over open, public networks. For each of the methods Tripwire Enterprise Policy Manager can be configured to check if secure configurations are used, and insecure versions (e.g. only the version of TLS is enabled which is not vulnerable to any known vulnerabilities) or configurations (e.g. weak cipher suites) are not enabled.
	4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.	**For all instances where cardholder data Is transmitted or received over open, public networks, describe how system configurations verified that the protocol:** • **Is implemented to use only secure configurations.** • **Does not support insecure versions or configurations.**	Tripwire Enterprise Policy Manager can be configured to check if strong cipher suite, secure version of protocol and appropriate ciphers/key length have been enabled. A QSA would examine vendor recommendations/ best practices for encryption strength to be used for each transmission method.
	4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	For each encryption methodology in use, Identify vendor recommendations/best practices for encryption strength. **Identify the encryption strength observed to be implemented.**	
	4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.	**Indicate whether TLS is implemented to encrypt cardholder data over open, public networks. (yes/no)** If 'no,' mark the remainder of 4.1.g as 'not applicable.' **If "yes," for all instances where TLS is used to encrypt cardholder data over open, public networks, describe how system configurations verified that TLS is enabled whenever cardholder data is transmitted or received.**	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	Identify the sample of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure. **For each item in the sample, describe how anti-virus software was observed to be deployed.**	A QSA would identify all operating systems (e.g. Windows) commonly affected by malicious software. Tripwire Enterprise Policy Manager can be configured to check the list of services/processes running to ensure an anti-virus service/process exists.
7.2.1 Coverage of all system components.	**7.2.1** Confirm that access control systems are in place on all system components.	Identify vendor documentation examined. **Describe how system settings** and the vendor	Tripwire Enterprise Policy Manager can be used to check if

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
		documentation **verified that access control systems are in place on all system components.**	• A centralized access control system has been deployed on operating systems and network devices. • The centralized access control system has been configured as per the policy specified in Tripwire Enterprise Compliance Policy Manager
7.2.2 Assignment of privileges to individuals based on job classification and function.	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	**Describe how system settings** and the vendor documentation at 7.2.1 **verified that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.**	
7.2.3 Default “deny-all” setting.	**7.2.3** Confirm that the access control systems have a default “deny-all” setting.	**Describe how system settings** and the vendor documentation at 7.2.1 **verified that access control systems have a default “deny-all” setting.**	
8.1.4 Remove/disable inactive user accounts within 90 days.	**8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	**Describe how user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled.**	Tripwire Enterprise Policy Manager can be configured to monitor account expiry/lockout settings on supported system components to ensure user accounts inactive for more than 90 days are disabled/removed/locked.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts.**	Tripwire Enterprise Policy Manager can be configured to check account lockout threshold and duration settings on supported systems.
	8.1.6.b Additional procedure for service provider assessments only: Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	Additional procedure for service provider assessments only, identify the documented internal processes and customer/user documentation reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. **Describe how implemented processes were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.**	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	**8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.**	
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that system/session idle time out features have been set to 15 minutes or less.**	Tripwire Enterprise Policy Manager can be configured to check session idle time-out setting on supported systems. The settings related to screen lockout with password protection can also be checked with Tripwire Enterprise Policy Manager on supported operating systems (e.g. Windows).

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	**8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.	Identify the vendor documentation examined to verify that passwords are protected with strong cryptography during transmission and storage. Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that passwords are protected with strong cryptography during transmission.** **For each item in the sample, describe how system configuration settings verified that passwords are protected with strong cryptography during storage.**	Tripwire Enterprise Policy Manager can be configured to monitor settings for login methods (e.g. SSH, Terminal Service) and password storage (e.g. *Do Not Store Lan Manager Password Hash* for Windows) in operating systems and network devices.
8.2.3.a Passwords / passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	**8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that user password/passphrase parameters are set to require at least the following strength/complexity:** • **Require a minimum length of at least seven characters.** • **Contain both numeric and alphabetic characters.**	Tripwire Enterprise Policy Manager can be configured to check password length and complexity setting on supported systems.
	8.2.3.b Additional procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	Additional procedure for service provider assessments only: Identify the documented internal processes and customer/user documentation reviewed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • A minimum length of at least seven characters. • Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters. **Describe how internal processes were observed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:** • **A minimum length of at least seven characters.** • **Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters.**	
8.2.4 Change user passwords/passphrases at least once every 90 days.	**8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days.**	Tripwire Enterprise Policy Manager can be configured to monitor password expiry setting on supported systems.
	8.2.4.b Additional procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that: • Non-consumer customer user passwords/passphrases are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances,	Additional procedure for service provider assessments only, identify the documented internal processes and customer/user documentation reviewed to verify that: • Non-consumer customer user passwords/passphrases are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
	passwords/passphrases must change.	**Describe how internal processes were observed to verify that:** • **Non-consumer customer user passwords/passphrases are required to change periodically; and** • **Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.**	
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	**8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password/passphrases parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	Identify the sample of system components selected for this testing procedure. **For each item in the sample, describe how system configuration settings verified that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.**	Tripwire Enterprise Policy Manager can be configured to check password history setting on supported systems.
	8.2.5.b Additional Procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.	Additional procedure for service provider assessments only, identify the documented internal processes and customer/user documentation reviewed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. **Describe how internal processes were observed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.**	
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.	**For all items in the sample at 10.2, describe how configuration settings verified all actions taken by any individual with root or administrative privileges are logged.**	Log settings on supported systems can be monitored with Tripwire Enterprise Policy Manager to ensure following events are captured: • Actions taken with privileged access, e.g. changing security settings, adding/modifying user accounts, installing applications, changing log settings etc. • Failed login attempts
10.2.4 Invalid logical access attempts.	**10.2.4** Verify invalid logical access attempts are logged.	**For all items in the sample at 10.2, describe how configuration settings verified that invalid logical access attempts are logged.**	
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 deletions to accounts with root or administrative privileges.	**10.2.5.a** Verify use of identification and authentication mechanisms is logged.	**For all items in the sample at 10.2, describe how configuration settings verified that use of identification and authentication mechanisms is logged.**	
	10.2.5.b Verify all elevation of privileges is logged.	**For all items in the sample at 10.2, describe how configuration settings verified that all elevation of privileges is logged.**	
	10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	**For all items in the sample at 10.2, describe how configuration settings verified that all changes, additions, or deletions to any account with root or administrative privileges are logged.**	
10.2.6 Initialization, stopping, or pausing of the audit logs.	**10.2.6** Verify the following are logged: • Initialization of audit logs. • Stopping or pausing of audit logs.	**For all items in the sample at 10.2, describe how configuration settings verified that initialization of audit logs is logged.** **For all items in the sample at 10.2, describe how configuration settings verified that stopping and pausing of audit logs is logged.**	
10.2.7 Creation and deletion of system-level objects.	**10.2.7** Verify creation and deletion of system level objects are logged.	**For all items in the sample at 10.2, describe how configuration settings verified that creation and deletion of system level objects are logged.**	
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	**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.	**Identify the time synchronization technologies in use.** (If NTP, include version) Identify the documented time-synchronization configuration standards examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Tripwire Enterprise Policy Manager can be used to check the list of services/processes running to check if time synchronization service is running and where possible get the version info as well.

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
time. *Note: One example of time synchronization technology is Network Time Protocol (NTP).*		**Describe how processes were examined to verify that time synchronization technologies are:** • **Implemented.** • Kept current, per the documented process.	A QSA would also ask for • Documents that define processes to keep the time synchronization technology patched as per requirements 6.1 and 6.2, and current. • Evidence that the documented processes are followed
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify: • Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. • Systems receive time only from designated central time server(s).	Identify the sample of system components selected for 10.4.1.b-10.4.2.b **For all items in the sample, describe how the time-related system-parameter settings verified:** • **Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.** • **Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.** • **Systems receive time only from designated central time server(s).**	Time configuration settings can be monitored by Tripwire Enterprise Policy Manager to ensure • Only designated external time sources are used by internal time servers • Each internal system receives time only from designated internal timer servers.
10.4.2 Time data is protected.	**10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	**For all items in the sample from 10.4.1, describe how configuration settings verified that access to time data is restricted to only personnel with a business need to access time data.**	Access rights assigned to groups/users of the host system can be monitored by Tripwire Enterprise Policy Manager to ensure only authorized groups/users can make changes to time settings
	10.4.2.b Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	**For all items in the sample from 10.4.1, describe how configuration settings and time synchronization settings verified that any changes to time settings on critical systems are logged.** For all items in the sample from 10.4.1, describe how the examined logs verified that any changes to time settings on critical systems are logged. **Describe how time synchronization processes were examined to verify changes to time settings on critical systems are:** • **Logged** • Monitored • Reviewed	Log settings of the host system can be monitored by Tripwire Enterprise Policy Manager to ensure modifications to time settings are logged.
10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	Identify the sample of time servers selected for this testing procedure. For all items in the sample, describe how configuration settings verified either of the following: • That the time servers receive time updates from specific, industry-accepted external sources. OR • That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines.	Time configuration settings can be monitored by Tripwire Enterprise Policy Manager to ensure only designated external time sources are used by internal time servers.

PCI DSS COMPLIANCE WITH TRIPWIRE LOG CENTER

Tripwire Log Center consists of two product components:

1. Tripwire Log Center Manager (TLC Manager) is the core software for Tripwire Log Center environment. TLC Manager collects and processes log messages from a wide variety of systems and devices.

2. Tripwire Log Center Console (TLC Console) is the software for the Tripwire Log Center graphical user interface (GUI). This can be used to configure Tripwire Log Center and to view logs and alerts.

Tripwire Log Center can be used as a central repository for storing logs from various systems components within the network. It can store logs encrypted using AES-256. Logs from supported operating systems are pushed by Tripwire agents into Tripwire Log Center. Logs from agentless devices (e.g. network devices) are collected by Tripwire Log Center. Tripwire Log Center provides a user interface that can be used for management purposes (e.g. configuration, log review). Tripwire Log Center can be configured to generate alerts on events of interest. These alerts can be sent to responsible personnel via various methods such as email, syslog.

Eighteen requirements are related to storing logs in a remote or centralized location, protecting the logs from unauthorized modifications and reviewing logs at least daily to identify malicious activities. Tripwire Log Center can be configured to assist companies meeting these requirements.

The capabilities of the Tripwire Log Center were reviewed in relation to the applicable PCI DSS requirements. Findings have been summarized in the next table under the Remarks column. **The areas of the PCI DSS requirements that can be verified using Tripwire Log Center have been highlighted in bold in the ROC Reporting Instruction column.** To meet a requirement, the entity assessed would be expected to demonstrate to a QSA how other items in the ROC Reporting Details column for the particular requirement comply with PCI DSS.

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
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.	Identify the system administrator(s) interviewed who confirm that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users. **Describe how audit trails were observed to verify the following:** • **Audit trails are enabled and active for system components.** • **Access to system components is linked to individual users.**	If audit logs are sent to Tripwire Log Center, following requirements could be verified by the QSA during a PCI DSS assessment: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users. • All the events listed in requirements 10.2 and 10.4.2 are logged • Each log event includes the information listed in requirements 10.3.1-10.3.6
10.2 Implement automated audit trails for all system components to reconstruct the following events: • All individual access to cardholder data. • All actions taken by any individual with root or administrative privileges. • Access to all audit trails. • Invalid logical access attempts. • Use of and changes to identification and	**10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: • All individual access to cardholder data. • All actions taken by any individual with root or administrative privileges. • Access to all audit trails. • Invalid logical access attempts. • Use of and changes to identification and authentication mechanisms, including: ○ All elevation of privileges. ○ All changes, additions, or	Identify the responsible personnel interviewed who confirm the following from 10.2.1-10.2.7 are logged: • All individual access to cardholder data. • All actions taken by any individual with root or administrative privileges. • Access to all audit trails. • Invalid logical access attempts. • Use of and changes to identification and authentication mechanisms, including: ○ All elevation of privileges. ○ All changes, additions, or deletions to any account with root or administrative privileges. • Initialization of audit logs. • Stopping or pausing of audit logs. • Creation and deletion of system level objects.	

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
authentication mechanisms, including: ○ All elevation of privileges. ○ All changes, additions, or deletions to any account with root or administrative privileges. • Initialization of audit logs. • Stopping or pausing of audit logs. • Creation and deletion of system level objects.	deletions to any account with root or administrative privileges. • Initialization of audit logs. • Stopping or pausing of audit logs. • Creation and deletion of system level objects.	**Identify the sample of audit logs selected for 10.2.1-10.2.7.**	
10.3 Record at least the following audit trail entries for all system components for each event: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource	**10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource	Identify the responsible personnel interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource **Identify the sample of audit logs from 10.2.1-10.2.7 observed to verify the following are included in log entries:** • **User identification** • **Type of event** • **Date and time** • **Success or failure indication** • **Origination of event** • **Identity or name of affected data, system component, or resource**	
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	**For all logs in the sample at 10.3, describe how the audit logs verified that user identification is included in log entries.**	
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	**For all logs in the sample at 10.3, describe how the audit logs verified that type of event is included in log entries.**	
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	**For all logs in the sample at 10.3, describe how the audit logs verified that date and time stamp is included in log entries.**	
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	**For all logs in the sample at 10.3, describe how the audit logs verified success or failure indication is included in log entries.**	
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	**For all logs in the sample at 10.3, describe how the audit logs verified origination of event is included in log entries.**	
10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	**For all logs in the sample at 10.3, describe how the audit logs verified the identity or name of affected data, system component, or resource is included in log entries.**	
10.4.2 Time data is protected.	**10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	For all items in the sample from 10.4.1, describe how configuration settings and time synchronization settings verified that any changes to time settings on critical systems are logged. **For all items in the sample from 10.4.1, describe how the examined logs verified that any changes to time settings on critical systems are logged.**	

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
		Describe how time synchronization processes were examined to verify changes to time settings on critical systems are: • **Logged** • **Monitored** • **Reviewed**	
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Only individuals who have a job-related need can view audit trail files.	**For each item in the sample at 10.5, describe how system configurations and permissions verified that only individuals who have a job-related need can view audit trail files.**	Each Tripwire Log Center user can be assigned different roles and privileges to ensure only individuals who has a documented job-related need have privileged access to the product to perform administrative tasks. Roles and privileges assigned to sampled users in Tripwire Log Center will be examined by a QSA during an assessment.
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.	**For each item in the sample at 10.5, describe how system configurations and permissions verified that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.**	If Tripwire Log Center is used to store audit trails centrally from connected system components (e.g. operating systems, network devices), then the user list in Tripwire Log Center can be used to show that personnel who have access to connected systems do not have access to Tripwire Log Center. This could be used to demonstrate that audit trails are protected from unauthorized modifications via access control mechanisms. As Tripwire Log Center would usually be on a separate physical system, QSA would be able to validate that audit trail files are protected from unauthorized modifications via physical segregation.
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.	**For each item in the sample at 10.5, describe how system configurations and permissions verified that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.**	Tripwire Log Center can be used to promptly backup audit trails from connected system components (e.g. operating systems, network devices). This can be demonstrated by logging into one of the connected system components and simultaneously showing in Tripwire Log Center that this event has been captured by Tripwire Log Center in real time. User access control settings implemented in Tripwire Log Center and permission
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.	**For each item in the sample at 10.5, describe how system configurations and permissions verified that logs for external-facing technologies are written onto a secure, centralized, internal log server or media.**	

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
			of folders (e.g. “Data” folder) where raw audit trails are stored can be used to demonstrate that it is difficult to alter audit trails stored in Tripwire Log Center.
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.	**For each item in the sample at 10.5, describe how the following verified the use of file-integrity monitoring or change-detection software on logs:** • **System settings** • **Monitored files** • **Results from monitoring activities** **Identify the file-integrity monitoring (FIM) or change-detection software verified to be in use.**	When Tripwire Log Center receives a log message from a log collector, it first places the message in an internal cache. When the log messages in the cache exceed specified time and size thresholds, Tripwire Log Center flushes the cache contents in a compressed file and calculates SHA-256 hash of the file. Tripwire Log Center can be configured to alert when a compressed log file checksum is altered.
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.an** 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.).	Identify the documented security policies and procedures examined to verify that procedures define 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. **Describe the manual or log tools used for daily review of logs.**	Tripwire Log Center might be capturing audit logs from tens and hundreds of system components (e.g. operating systems, network devices). Manually going through these logs daily might be inefficient and impractical. Unusual/abnormal activities need to be reviewed on a daily basis. To assist with this process rules can be created in Tripwire Log Center to filter out logs containing abnormal activities, e.g. a privileged user logging into a system component outside normal business hours.
	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.).	Identify the responsible personnel interviewed who confirm 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. **Describe how processes were observed 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.**	

PCI DSS Requirements	Testing Procedures	ROC Reporting Instruction	Remarks
10.6.2 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.	**10.6.2.a** 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.	Identify the documented security policies and procedures examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. **Describe the manual or log tools defined for periodic review of logs of all other system components.**	This requirement applies to lower risk system components that are in-scope, but do not require daily log reviews as per requirement 10.6.1, e.g. workstations which do not handle CHD, but can impact the security of the CDE. Logs from these types of system components can also be sent to Tripwire Log Center and reviewed and monitored through Tripwire Log Center as per the organization’s policies and risk management strategy.
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).	**10.7.b** Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.	Identify the responsible personnel interviewed who confirm that audit logs are retained for at least one year. **Describe how the audit logs verified that audit logs are retained for at least one year.**	Tripwire Log Center stores raw logs in flat files. The usual name of the folder is “Data.” Date and time stamps of the flat files can be used to demonstrate how long the audit trails logs are stored. The Tripwire Log Center GUI can be used to show logs from flat files in a readable format. This feature can be used to query and show logs from last three months.
	10.7.c Interview personnel and observe processes to verify that at least the last three months’ logs are immediately available for analysis.	Identify the responsible personnel interviewed who confirm that at least the last three months’ logs are immediately available for analysis. **Describe how processes were observed to verify that at least the last three months’ logs are immediately available for analysis.**	

PCI DSS COMPLIANCE WITH TRIPWIRE IP360

Tripwire IP360 is a vulnerability management system which can be used by organizations to scan various operating systems, network devices and web applications and assign risk ranking of identified vulnerabilities.

The solution consists of the following two key product components:

1. VnE Manager: VnE Manager is a hardened appliance that serves as the central data repository and management platform, and can be physical hardware or virtualized.
2. Device Profiler (DP). DP is a hardened, diskless appliance that scans operating systems, network devices and web applications and reports its findings to the VnE Manager.

The Tripwire Vulnerability and Exposure Research Team (Tripwire VERT) is dedicated to researching this area and responsible for providing timely and up-to-date vulnerability discovery signatures to the Tripwire IP360 solution. VnE Manager can be configured to connect to Tripwire over the Internet to receive latest signatures automatically. If VnE Manager is not connected to the Internet, then latest signatures need to be downloaded from the Tripwire website using a customer account as a file referred to as the ASPL (Advanced Security Profiling Language) update.

Tripwire IP360 was reviewed in relation to the applicable PCI DSS requirements. Findings have been summarized in the next table under the Remarks column. **The areas of the PCI DSS requirements that can be verified using Tripwire IP360 have been highlighted in bold in the ROC Reporting Instruction column.** To meet a requirement the entity assessed would be expected to demonstrate to a QSA how other items in the ROC Reporting Details column for the particular requirement comply with PCI DSS.

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	**2.1.b** For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	**For each item in the sample of system components indicated at 2.1.a, describe how all unnecessary default accounts were verified to be either:** • **Removed** • **Disabled**	Tripwire IP360 can be used to scan supported platforms to identify if vendor supplied default user names and passwords are still used.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	**2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.	Identify the sample of system components selected. **For each item in the sample, describe how the enabled system services, daemons, and protocols verified that only necessary services or protocols are enabled.**	As part of the normal scanning Tripwire IP360 identifies all the services listening on ports. This information can be used to for the following purposes: • Compare with the list of documented services/protocols to ensure only necessary services/protocols are enabled • Identify insecure services/protocols (e.g. FTP, Telnet) • Identify if SSL and early TLS are used
	2.2.2.b Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.	**For each item in the sample of system components from 2.2.2.a, indicate whether any insecure services, daemons, or protocols are enabled. (yes/no)** If "no," mark the remainder of 2.2.2.b and 2.2.3 as "Not Applicable." If "yes," identify the responsible personnel interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure	**2.2.3.b** If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	**Indicate whether SSL/early TLS is used. (yes/no)** If 'no,' mark the remainder of 2.2.3.b as 'not applicable.' If 'yes,' provide the name of the assessor who attests that the testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS were performed.	
2.3 Encrypt all non-console administrative access using strong cryptography.	**2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	**Describe how services and parameter files on systems verified that Telnet and other insecure remote-login commands are not available for non-console access.**	
	2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	Describe how the administrator log on to each system verified that administrator access to any web-based management interfaces was encrypted with strong cryptography. **Identify the strong encryption method used for any web-based management interfaces.**	
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the	**4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.	Identify all locations where cardholder data is transmitted or received over open, public networks. Identify the documented standards examined. Describe how the documented standards and **system configurations both verified the use of:** • **Security protocols for all locations** • Strong cryptography for all locations	
	4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.	**For all instances where cardholder data Is transmitted or received over open, public networks, describe how system configurations verified that the protocol:** • Is implemented to use only secure configurations. • **Does not support insecure versions or**	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
encryption methodology in use.		**configurations.**	
	4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.	**Indicate whether TLS is implemented to encrypt cardholder data over open, public networks. (yes/no)** If 'no,' mark the remainder of 4.1.g as 'not applicable.' If "yes," for all instances where TLS is used to encrypt cardholder data over open, public networks, describe how system configurations verified that TLS is enabled whenever cardholder data is transmitted or received.	
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.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 "high" risk and "critical" vulnerabilities. • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	Identify the responsible personnel interviewed who confirm that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. **Describe the processes observed to verify that: New security vulnerabilities are identified.** • **A risk ranking is assigned to vulnerabilities to include identification of all "high" risk and "critical" vulnerabilities.** • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. Identify the outside sources used.	Tripwire IP360 can be used to identify vulnerabilities within the internal network. Information on how Tripwire IP360 scores vulnerabilities can be found in the following URL http://www.tripwire.com/register/tripwire-vulnerability-scoring-system/ The entity undergoing PCI DSS assessment can use the score provided by Tripwire IP360 as one of the inputs for evaluating and assigning risk rating (e.g. "critical", "High", "Medium", "Low") to a new vulnerability as it comes out. Note: To fully meet the intent of this requirement, entities need to subscribe to reputable outside sources (e.g. US-CERT) to identify security vulnerabilities in timely manner for all types of in-scope systems.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an	**6.6** For public-facing web applications, ensure that either one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed - using either manual or automated vulnerability security assessment tools or methods - as follows: ○ At least annually. ○ After any changes. ○ By an organization that specializes in application security. ○ That, at a minimum, all vulnerabilities in	**For each public-facing web application, identify which of the two methods are implemented:** • **Web application vulnerability security assessments, AND/OR** • Automated technical solution that detects and prevents web-based attacks, such as web application firewalls. *If application vulnerability security assessments are indicated above:* **Describe the tools and/or methods used (manual or automated, or a combination of both).** Identify the documented processes that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows: • At least annually. • After any changes. • By an organization that specializes in application security. • That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment.	Tripwire IP360 includes options to scan web applications. This feature can be used to demonstrate that an automated web application vulnerability security assessment tool is used to identify vulnerabilities for public-facing web applications. Tripwire PureCloud, based on Tripwire IP360, provides coverage for nine of the OWASP top 10 categories at the time of this paper.

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	Requirement 6.5 are included in the assessment. ○ That all vulnerabilities are corrected. ○ That the application is re-evaluated after the corrections. • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: ○ Is situated in front of public-facing web applications to detect and prevent web-based attacks. ○ Is actively running and up-to-date as applicable. ○ Is generating audit logs. ○ Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	• That all vulnerabilities are corrected • That the application is re-evaluated after the corrections. Identify the responsible personnel interviewed who confirm that public-facing web applications are reviewed, as follows: • At least annually. • After any changes. • By an organization that specializes in application security. • That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. • That all vulnerabilities are corrected. • That the application is re-evaluated after the corrections. **Identify the records of application vulnerability security assessments examined for this testing procedure.** **Describe how the records of application vulnerability security assessments verified that public-facing web applications are reviewed as follows:** • At least annually. • After any changes. • By an organization that specializes in application security. • **That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment.** • That all vulnerabilities are corrected • That the application is re-evaluated after the corrections.	
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high-risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.	**Identify the internal vulnerability scan reports** and supporting documentation **reviewed.** Provide the name of the assessor who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period.	Tripwire IP360 can be used to identify vulnerabilities of supported operating systems, network devices and web applications in the internal network. It provides CVSS scores, and prioritizes and ranks vulnerabilities. This result can be used to identify "High" vulnerabilities and perform rescanning until passing results are obtained.
	11.2.1.b Review the scan reports and verify that all "high-risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	Identify the documented process for quarterly internal scanning to verify the process defines performing rescans as part of the quarterly internal scan process. For each of the four internal quarterly scans indicated at 11.2.1.a, indicate whether a rescan was required. (yes/no) **If "yes," describe how rescans were verified to be performed until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.**	
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**11.2.3.b** Review scan reports and verify that the scan process includes rescans until: • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. • For internal scans, all "high-risk" vulnerabilities as defined in PCI DSS	For all scans reviewed in 11.2.3.a, indicate whether a rescan was required. (yes/no) If "yes" – for external scans, describe how rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist. **If "yes" – for internal scans, describe how rescans were performed until either passing results were obtained or all "high-risk"**	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
	Requirement 6.1 are resolved.	**vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved.**	

PCI DSS COMPLIANCE WITH TRIPWIRE PURECLOUD

Tripwire PureCloud is Tripwire's hosted vulnerability management solution, based on Tripwire's IP360 vulnerability management product.

Tripwire PureCloud for PCI (ASV – Approved Scanning Vendor) uses the same software as Tripwire IP360 in their hosted environment to implement this solution. Each customer is given unique credentials to log into the Tripwire PureCloud web portal from which they can perform the following types of vulnerability scans:

1. Perimeter: An agentless vulnerability scan of Internet-facing systems, including web-based applications
2. Internal: Customers would need to download Tripwire PureCloud Enterprise software for use as their internal scanning tool and run it from an internal host to scan internal systems. This would typically run on a physical or virtualized Windows server.
3. Tripwire PureCloud for PCI: This service is similar to the perimeter scan. As part of this service customers are able to download scan reports as per PCI DSS and PCI ASV formats and take advantage of automatic submissions on a quarterly basis per the PCI DSS standard to their verifying institution. Tripwire PureCloud and PureCloud for PCI uses Tripwire IP360 as the underlying software which is listed on the PCI SSC website as an ASV.

The perimeter scan and PCI ASV services of Tripwire PureCloud were reviewed in relation to the applicable PCI DSS requirements. **The areas of the PCI DSS requirements that can be verified using these services have been highlighted in bold in the ROC Reporting Instruction column.** To meet a requirement the entity assessed would be expected to demonstrate to a QSA how other items in the ROC Reporting Details column for the particular requirement comply with PCI DSS.

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	**4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.	Identify all locations where cardholder data is transmitted or received over open, public networks. Identify the documented standards examined. Describe how the documented standards and **system configurations both verified the use of:** • **Security protocols for all locations** • Strong cryptography for all locations	Tripwire PureCloud uses the Tripwire IP360 scanning and assessment solution to check external IP addresses for PCI DSS compliance purpose. The scan can be used to identify if any insecure service or protocol is used (e.g. Telnet, SSL V3.0) on the externally facing interfaces.
	4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.	**For all instances where cardholder data Is transmitted or received over open, public networks, describe how system configurations verified that the protocol:** • Is implemented to use only secure configurations. • **Does not support insecure versions or configurations.**	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
	4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.	**Indicate whether TLS is implemented to encrypt cardholder data over open, public networks. (yes/no)** If 'no,' mark the remainder of 4.1.g as 'not applicable.' If "yes," for all instances where TLS is used to encrypt cardholder data over open, public networks, describe how system configurations verified that TLS is enabled whenever cardholder data is transmitted or received.	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**6.6** For public-facing web applications, ensure that either one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed - using either manual or automated vulnerability security assessment tools or methods - as follows: o At least annually. o After any changes. o By an organization that specializes in application security. o That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. o That all vulnerabilities are corrected. o That the application is re-evaluated after the corrections. • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution	**For each public-facing web application, identify which of the two methods are implemented:** • **Web application vulnerability security assessments, AND/OR** • Automated technical solution that detects and prevents web-based attacks, such as web application firewalls. *If application vulnerability security assessments are indicated above:* **Describe the tools and/or methods used (manual or automated, or a combination of both).** Identify the documented processes that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows: • At least annually. • After any changes. • By an organization that specializes in application security. • That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. • That all vulnerabilities are corrected • That the application is re-evaluated after the corrections. Identify the responsible personnel interviewed who confirm that public-facing web applications are reviewed, as follows: • At least annually. • After any changes. • By an organization that specializes in application security. • That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. • That all vulnerabilities are corrected. • That the application is re-evaluated after the corrections. **Identify the records of application vulnerability security assessments examined for this testing procedure.** **Describe how the records of application vulnerability security assessments verified that public-facing web applications are reviewed as follows:** • At least annually. • After any changes. • By an organization that specializes in application security. • **That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment.** • That all vulnerabilities are corrected • That the application is re-evaluated after the corrections.	"Web Application Scan" under "Scan Settings" of the Tripwire PureCloud perimeter scan service includes options to scan web applications. This feature can be used to demonstrate that an automated web application vulnerability security assessment tool is used to identify vulnerabilities for public-facing web applications. Tripwire PureCloud, based on Tripwire IP360, provides coverage for nine of the OWASP top 10 categories at the time of this paper.

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
	that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: ○ Is situated in front of public-facing web applications to detect and prevent web-based attacks. ○ Is actively running and up-to-date as applicable. ○ Is generating audit logs. ○ Is configured to either block web-based attacks, or generate an alert that is immediately investigated.		
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period.	**Identify the external network vulnerability scan reports and supporting documentation reviewed.** Provide the name of the assessor who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period.	Tripwire PureCloud uses Tripwire IP360 scan solution to scan external IP addresses for PCI DSS compliance purpose. It generates following reports as per the PCI SSC ASV Program Guide: • ASV Scan Report Attestation of Scan Compliance • ASV Scan Report Executive Summary • ASV Scan Report Vulnerability Details These reports can be used during the PCI DSS assessment to demonstrate compliance to this requirement.
	11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures).	**Provide the name of the assessor who attests that the results of each quarterly scan were reviewed and verified that the ASV Program Guide requirements for a passing scan have been met.** For each of the four external quarterly scans indicated at 11.2.2.a, indicate whether a rescan was necessary. (yes/no) **If "yes," describe how the results of the rescan verified that the ASV Program Guide requirements for a passing scan have been met.**	
	11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	Provide the name of the assessor who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV).	
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**11.2.3.b** Review scan reports and verify that the scan process includes rescans until: • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. • For internal scans, all "high-risk" vulnerabilities as	For all scans reviewed in 11.2.3.a, indicate whether a rescan was required. (yes/no) **If "yes" – for external scans, describe how rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist.** If "yes" – for internal scans, describe how rescans were performed until either passing results were obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved.	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details	Remarks
	defined in PCI DSS Requirement 6.1 are resolved.		

TECHNICAL INFORMATION ABOUT TRIPWIRE PRODUCTS TO COMPLY WITH PCI DSS

While a Tripwire product can assist an entity to meet certain PCI DSS requirements (which have been discussed in the previous sections), it might be subject to a number of PCI DSS requirements. This can happen if it is found that the Tripwire product can impact the security of the systems in CDE. For example a malicious individual might be able to compromise the Tripwire Enterprise Policy Manager and run privileged commands through the Tripwire Enterprise Policy Manager in the target systems in the CDE to gain unauthorized access.

In the following table technical information about Tripwire Enterprise, Tripwire Log Center and Tripwire IP360 have been provided against some PCI DSS requirements as a guide to show how these products can comply with these requirements. During a PCI DSS assessment the requirements that would apply to a Tripwire product would be determined by the assessor (e.g. QSA) depending on how the product has been implemented and what extent it can impact the security of the systems in the CDE.

PCI DSS Requirements	Tripwire Enterprise (TE)	Tripwire Log Center (TLC)	Tripwire IP360
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. ***This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.***	GUI • A default password is provided with the system, and is required to be changed upon first login • The default user name cannot be removed or locked, but can be changed CLI • User name and password are as same as GUI • CLI access is available once the user has logged into the operating system where Tripwire Enterprise has been installed. • CLI access cannot be used to make configuration changes in Tripwire Enterprise like the GUI	GUI • Default user name is provided with the system, and is recommended to be changed upon installation. • Default password: Needs to be specified at the time of install • A password needs to be specified at the time of install. The default user name can be changed or disabled CLI • No CLI access is available	GUI for VnE Manager • A default password is provided with the system, and is recommended to be changed upon installation • The default user name can be changed or disabled CLI for VnE Manager • User name and password are different from GUI • A default password is provided with the system, and is recommended to be changed upon installation • The default user name cannot be changed or disabled GUI for DP (Device Profiler) • No GUI access is available CLI for DP (Device Profiler) • Same as CLI for VnE Manager
2.3 Encrypt all non-console administrative access using strong cryptography.	GUI • Tripwire Enterprise uses a customized Tomcat Apache server • The "server.properties" file under "<te_root>/server/data/config/" needs to be modified to support only strong ciphers CLI • As interactive access to the CLI is obtained by logging into the host operating system, the host operating system would need to comply to this requirement	GUI • TLSv1.2 is used between TLC Manager and TLC Console communications. Tripwire Log Center does not specify any cipher to be used in these communications as it relies on the .NET framework for this. The framework works based on the Windows policies. CLI • No CLI access is available	GUI for VnE Manager • Can be configured to FIPS 140-2 mode to support only TLS at the server side CLI for VnE Manager • SSH access is enabled, but disabled by Tripwire personnel as part of the installation. Once this is done the user needs to be physically present at the device to login via the device console. GUI for DP (Device Profiler) • No GUI access is available CLI for DP (Device Profiler) • CLI access is required for the initial install and deploy authentication key (shared key between VnE manager and DP) to communicate with VnE. • SSH access – Same as CLI for VnE Manager

PCI DSS Requirements	Tripwire Enterprise (TE)	Tripwire Log Center (TLC)	Tripwire IP360
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: **7.2.1** Coverage of all system components. **7.2.2** Assignment of privileges to individuals based on job classification and function. **7.2.3** Default "deny-all" setting.	GUI • Users (except the local administrator account) can be authenticated against a centralized authentication server, e.g. Microsoft Active Directory. • Users need to be assigned groups which are maintained within Tripwire Enterprise CLI • Same as GUI	GUI • Users (except the local administrator account) can be authenticated against a centralized authentication server, e.g. Microsoft Active Directory. • Users need to be assigned groups which are maintained within Tripwire Log Center CLI • No CLI access is available	GUI for VnE Manager • Users (except the local administer account) can be authenticated against a centralized authentication server, e.g. Microsoft Active Directory. • Users need to be assigned groups which are maintained within Tripwire IP360 CLI for VnE Manager • SSH access is enabled, but disabled by Tripwire personnel as part of the installation. Once this is done the user needs to be physically present at the device to login via the device console. • CLI access cannot be used to run scan or change scan profile settings • CLI access cannot be integrated with a centralized authentication server, e.g. Microsoft Active Directory. GUI for DP (Device Profiler) • No GUI access is available CLI for DP (Device Profiler) • Same as CLI for VnE Manager
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	GUI • Tripwire Enterprise requires assigning unique user IDs if multiple user accounts are used to access the product CLI • Same as GUI	GUI • Tripwire Log Center requires assigning unique user IDs if multiple user accounts are used to access the product CLI • No CLI access is available	GUI for VnE Manager • Tripwire IP360 requires assigning unique user IDs if multiple user accounts are used to access the VnE Manager CLI for VnE Manager • Additional user accounts cannot be created GUI for DP (Device Profiler) • No GUI access is available CLI for DP (Device Profiler) • Same as CLI for VnE Manager
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	GUI • Storage - Passwords for TE Console local accounts are hashed using PBKDF2 with HMAC SHA256. A random salt is generated each time a password is hashed and stored. • Transmission - refer to the comments under requirement 2.3 CLI • Same as GUI Credentials to access monitored systems • A valid user name and password with privileged access may be needed to access system components where Tripwire agents cannot be installed. • The password is stored encrypted within	GUI • Storage - 256 bit AES key is used to store passwords for TLC Console local accounts. • Transmission - Refer to the comments under requirement 2.3 CLI • No CLI access is available Credentials to access systems by TLC File Collector • A valid user name and password with privileged access may be needed by TLC File Collector to access system components which cannot forward logs or where Tripwire Log Center agents cannot be installed. • The password is stored within Tripwire Log Center using a 256 bit AES key. • The File Collector can collect log files via SMB (file copy), FTP or SFTP from the remote system components. • To comply with PCI DSS following methods must not be used	GUI for VnE Manager • A 128 bit AES key is used to store passwords for the local accounts to access the VnE Manager. CLI for VnE Manager • No command is available to view the password file GUI for DP (Device Profiler) • No GUI access is available CLI for DP (Device Profiler) • Same as CLI for VnE Manager Credentials to access systems by DP to perform authenticated scans • Tripwire IP360 requires a user name and password to perform authenticated scans on system components. This user name and password are stored through the "Credential Management" section of VnE Manager GUI. The password is stored within the VnE Manager local database using a 128 bit AES key

PCI DSS Requirements	Tripwire Enterprise (TE)	Tripwire Log Center (TLC)	Tripwire IP360
	Tripwire Enterprise using 256 bit AES	○ FTP ○ SMB if password is sent in clear	
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	GUI • If the password for the local administrator account is known to more than one person, then compensating controls need to be documented and implemented as per PCI DSS appendix C to ensure activities performed using this account can be traced to an individual. CLI • Same as GUI Credentials to access monitored systems • A valid user name and password with privileged access may be needed by Tripwire Enterprise to access system components where Tripwire agents cannot be installed. • Compensating controls may need to be documented and implemented as per PCI DSS Appendix C for this user account to ensure activities performed using this account by an individual can be traced to that individual.	GUI • If the password for the local administrator account is known to more than one person, then compensating controls need to be documented and implemented as per PCI DSS appendix C to ensure activities performed using this account can be traced to an individual. CLI • No CLI access is available Credentials to access systems by TLC File Collector • A valid user name and password with privileged access may be needed by TLC File Collector to access system components which cannot forward logs or where Tripwire agents cannot be installed. • Compensating controls may need to be as per PCI DSS Appendix C for this user account to ensure activities performed using this account by an individual can be traced to that individual.	GUI for VnE Manager • If local administrator account is enabled and the password for the account is known to more than one person, then compensating controls need to be documented and implemented as per PCI DSS appendix C to ensure activities performed using this account can be traced to an individual. CLI for VnE Manager • If the password for the local admin account is known to more than one person, then compensating controls need to be documented and implemented as per PCI DSS Appendix C to ensure activities performed using this account can be traced to an individual. GUI for DP (Device Profiler) • No GUI access is available CLI for DP (Device Profiler) • Same as CLI for VnE Manager Credentials to access systems by DP to perform authenticated scans • Tripwire IP360 requires a user name and password to perform authenticated scans on system components. This user name and password are stored through the "Credential Management" section of VnE Manager GUI. • Compensating controls may need to be documented and implemented per PCI DSS Appendix C for this user account to ensure activities performed using this account by an individual can be traced to that individual.

◆ Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER