transmosisONE

transmosisONE For

PCI - DSS

FORWARD

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. This document maps and describes transmosisONE security capabilities and various PCI-DSS requirements and is meant to assist security decision makers that need to comply with these requirements in an efficient and economic manner.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

- When properly implemented following vendor guidance, the transmosisONE platform provides coverage for PCI DSS Requirement 5 based on the sample testing and evidence gathered during this assessment.
- The transmosisONE platform is able to detect and effectively block the execution of known malware samples.
- The transmosisONE platform is able to effectively remove all known malware samples.
- The transmosisONE platform adequately generates logs of events so that malicious activity can be traced in accordance with PCI DSS requirements.
- transmosisONE can be prevented from being disabled by unauthorized users.
- transmosisONE can also provide additional policy protections to include application whitelisting/blacklisting, preventing processes from accessing network, preventing processes from scraping memory of other processes, preventing processes from injecting code or modifying memory of another process, or trying to execute code from memory.

Requirement 6: Develop and maintain secure systems and applications

- When properly implemented following vendor guidance, the transmosisONE platform identifies vulnerabilities in installed software, using reputable outside sources for security vulnerability information.

Requirement 10: Track and monitor all access to network resources and cardholder data

- When properly implemented following vendor guidance, the transmosisONE platform generates, collects and parses logs from all critical system components.
- transmosisONE retains its collected logs for the timeframe PCI DSS requires.

Requirement 11: Regularly test security systems and processes

- When properly implemented following vendor guidance, transmosisONE provides the ability to deploy File Integrity Monitoring policies, alerting administrators upon any change from the defined baseline.

transmosisONE FOR PCI-DSS REQUIREMENT TABLE

PCI Requirement	PCI Testing Requirements	Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	transmosisONE allows users to directly deploy agents to Windows, macOS and the vast majority of Linux distributions. The Management UI shows the status of monitoring for all enrolled devices.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; ▶ Detect all known types of malicious software, ▶ Remove all known types of malicious software, and ▶ Protect against all known types of malicious software. Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.	transmosisONE does signature checking against well-known virus repositories. This allows transmosisONE to get a reputation for all processes to detect those that are known malware, block them from running, and remove them when requested by an administrator. transmosisONE was able to detect, block, and remove several examples of viruses, Trojans, ransomware, rootkits, and other known malware.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	**5.1.2** Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	This is a process/procedure requirement. Merchants must “periodically” evaluate the systems they use to ensure they are not considered commonly affected. transmosisONE can support this by using agentless mode to monitor any system to include those that would not commonly be considered affected by malware.

PCI Requirement	PCI Testing Requirements	Comments
5.2 Ensure that all anti-virus mechanisms are maintained as follows: ▶ Are kept current ▶ Perform periodic scans ▶ Generate audit logs which are retained per PCI DSS Requirement 10.7.	**5.2.a** Examine policies and procedures to verify that anti-virus soft-ware and definitions are required to be kept up to date. **5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are: ▶ Configured to perform automatic updates, and ▶ Configured to perform periodic scans. **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: ▶ The anti-virus software and definitions are current. ▶ Periodic scans are performed. **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: ▶ Anti-virus software log generation is enabled, and ▶ Logs are retained in accordance with PCI DSS Requirement 10.7.	5.2.a is a policy requirement. transmosisONE meets this by doing real-time checking of software against wellknown virus repositories. There are no definitions that must be stored locally on systems. transmosisONE's management UI shows the monitoring status of all enrolled devices and allows for the scheduling of scans. It also allows for configuration of master policies as they apply to system devices. There is no need for automatic updates as the software checks process signatures in real time against well-known virus repositories. See previous response. From the transmosisONE portal, admins can monitor the enrollment status of all systems. transmosisONE's management UI includes logging and alerts for all malware related alerts (as well as other policy violations).
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which the anti-virus is disabled.	**5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	transmosisONE's management UI shows the monitoring status of all enrolled devices. transmosisONE's management UI shows the monitoring status of all enrolled devices. It also can be configured to prevent users from disabling agents from running locally. Requirement 5.3.c involves interviews of responsible personnel who can show/verify with transmosisONE's portal that antivirus is active, running, and cannot be turned off except when needed.

PCI Requirement	PCI Testing Requirements	Comments
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are: ▶ Documented, ▶ In use, and ▶ Known to all affected parties.	This is a policies and procedures based requirement. While transmosisONE can help to meet the requirements for protecting against malware, it is up to administrators to create the specific policies as required.
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. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.	**6.1.a** Examine policies and procedures to verify that processes are defined for the following: ▶ To identify new security vulnerabilities ▶ To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. ▶ To use reputable outside sources for security vulnerability information. **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.	transmosisONE Vulnerability Assessment capabilities automate the discovery and ranking of unpatched vulnerabilities across all applications that run on the endpoints. Requirement 6.1.b involves interviews of responsible personnel who can show/verify with transmosisONE Vulnerability Assessment that vulnerabilities are identified and ranked.
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.	transmosisONE provides administrators with all the required audit trails.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	transmosisONE provides administrators with all the required audit logs.
10.2.1 All individual user accesses to cardholder data.	**10.2.1** Verify all individual access to cardholder data is logged.	transmosisONE logs all user access within the monitored environment.
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.	transmosisONE logs all user access within the monitored environment.

PCI Requirement	PCI Testing Requirements	Comments
10.2.3 Access to all audit trails.	**10.2.3** Verify access to all audit trails is logged.	
10.2.4 Invalid logical access attempts.	**10.2.4** Verify invalid logical access attemptsare 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. **10.2.5.b** Verify 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.	
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.	transmosisONE log collection and retention satisfies all the requirements listed in 10.2.6 to 10.3.6.
10.2.7 Creation and deletion of system-level objects.	**10.2.7** Verify creation and deletion of system level objects are logged.	
10.3 Record at least the following audit trail entries for all system components for each event.	**10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following	
10.3.1 User identification.	**10.3.1** Verify 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.	
10.3.3 Date and time.	**10.3.3** Verify 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.	
10.3.5 Origination of event.	**10.3.5** Verify 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.	

PCI Requirement	PCI Testing Requirements	Comments
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	**10.6** Perform the following:	transmosisONEmeets this requirement with both logs generated by its security modules, as well as logs it collects and parses from other system components.
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, or that could impact the security of CHD and/or SAD. ▶ Logs of all critical system components. ▶ Logs of all servers and system components that perform security functions (for example, firewalls, intrusion detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**10.6.1.a** Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: ▶ All security events. ▶ Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of 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.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, or that could impact the security of 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.).	transmosisONE meets this requirement by aggregating and retaining various types of logs: **Activity logs which transmosisONE engine collects itself:** ▶ User logon. ▶ Network access. ▶ File execution. ▶ Software updates. ▶ File creation/deletion/access/ ▶ execution/renaming. **External activity logs:** ▶ Windows events. ▶ VPN logs. ▶ Proxy logs. ▶ Logs from. **Security logs:** ▶ Logs that transmosisONE generates: alerts from transmosisONE's AV, NGAV, EDR, Network Analytics, UBA and deception. ▶ Logs that transmosisONE parses: firewall logs.

PCI Requirement	PCI Testing Requirements	Comments
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.	**0.6.2.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. **10.6.2.b** Examine the organization's risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	transmosisONE enables user to meet this requirement via its log collection and parsing capabilities.
10.6.3 Follow up exceptions and anomalies identified during the review process.	**10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. **10.6.3.b** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	transmosisONE anomalies monitoring supports all requirements to achieve compliance with 10.6.3a, 10.6.3.b.
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.a** Examine security policies and procedures to verify that they define the following: ▶ Audit log retention policies. ▶ Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. **10.7.b** Interview personnel and examine audit logs to verify that audit logs are available for at least one year. **10.7.c** Interview personnel and observe processes.	transmosisONE retains all the logs it collects (either natively or through parsing) for an unlimited length of time.

PCI Requirement	PCI Testing Requirements	Comments
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	**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 (for example, through risk assessment or other means). **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.	transmosisONE meets this by applying a policy that alerts upon any change in the user-defined status and configuration of selected files. transmosisONE's visibility UI shows all components of the internal environment – executables, installed apps, user activity and host properties, enabling users to capture a desired state of chosen entities and save it the 'known good' state. File Integrity Monitoring alerts must be configured by the user per the environments' specific requirements and are not part of the default configuration.