DATA SHEET

RACK FOUNDRY

Total Security Management PCI DSS Compliance Guide

The Payment Card Industry Data Security Standard (PCI DSS) is a set of regulations to help protect the security of credit card holders. These regulations apply to any organization that accepts, transmits, or stores cardholder data, regardless of the size and number of transactions or the usage of third-party processors. Cardholder data includes, but is not limited to, the full Primary Account Number (PAN), cardholder name, expiration date, and service code. Additionally, sensitive authentication information, including full track data, PINs, PIN blocks, and security codes/values/identity numbers must also be protected. To help ensure the protection of this information, PCI DSS 3.2 includes 12 main requirements that are summarized as follows:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

To meet these requirements, IT teams are left with the daunting task of purchasing multiple security tools and managing each of them individually while maintaining their day to day operations. However, not all organizations have resources available to not only purchase multiple point products but also to hire dedicated security professionals to manage them. Thus, it can be difficult for organizations, especially small to medium size businesses, to achieve compliance. This can result in non-compliance fees of $5,000 to $100,000 per month, increased bank transaction fees, and possible public embarrassment.

RackFoundry Total Security Management (TSM) includes the essential security capabilities to assist organizations with achieving and maintaining compliance. Our solution provides real-time monitoring, threat detection, and expertise to increase network visibility and effectively operationalize network security. RackFoundry TSM includes the following features to help address PCI DSS:

- Security Information Event Management (SIEM)
- Vulnerability Assessment
- Intrusion Prevention/Detection (IPS/IDS)
- Web application Firewall (WAF)
- File Integrity Monitoring (FIM)
- Centralized Logging
- Behavioral Monitoring
- Asset Inventory
- 4 Threat Intelligence Feeds
- 24/7/365 Security Operations Center (SOC)

For a more detailed explanation of how RackFoundry TSM can help organizations meet PCI DSS requirements, please see the table below:

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
Requirement 1: Install and Maintain a firewall configuration to protect cardholder data		
1.1	Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections to cardholder data (including wireless); that use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months.	RackFoundry TSM supports 1.1.1 by detecting Firewall and router configuration changes and generating notifications. RackFoundry's SOC supports 1.1.2, 1.1.3, and 1.1.4 by providing Architecture Reviews to identify connections to cardholder data and implement best practices. RackFoundry TSM supports 1.1.5 and 1.1.6, and 1.1.7 by detecting insecure services, protocols, and ports via alerts and reports.

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	RackFoundry TSM supports 1.2.1, 1.2.2, and 1.2.3 by monitoring firewall and router configuration and inbound/outbound network traffic in the form of events, alerts, and reports.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	RackFoundry TSM supports 1.3.1, 1.3.2, 1.3.3 by monitoring firewall/router configurations and monitoring inbound/outbound network traffic between the DMZ environment and the internal environment. RackFoundry TSM also includes an IPS/IDS, Firewall and WAF to prevent unwanted traffic. Rackfoundry TSM supports 1.3.4 by monitoring authorized/unauthorized outbound traffic from the cardholder data environment to the internet. RackFoundry TSM supports 1.3.5, 1.3.6 by monitoring firewall/router configurations and connections into the internal network. RackFoundry TSM supports 1.3.7 with built-in Firewall and Network Address Translation (NAT) that can be used to obscure IP addressing.
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	RackFoundry TSM supports 1.4.a by monitoring portable computing device activity
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
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, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	RackFoundry TSM supports 2.1.a and 2.1.b by monitoring known vendor default account authentication failures/successes and generating alerts and reports. RackFoundry TSM supports 2.1.1 by monitoring account login attempts and generating alerts for failed logon attempts as well as reports that include user activity.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	RackFoundry TSM supports 2.2.2.a and 2.2.2.b by monitoring host activity and generating alerts and reports detailing allowed/denied network protocols and services.
2.3	Encrypt all non-console administrative access using strong cryptography.	RackFoundry TSM utilizes alerts and reports to provide details of insecure network protocols and services.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	RackFoundry TSM includes an Asset Inventory and Discovery tool to detect network devices and information about the device such as operating system, hostname, and IP address.
Requirement 3: Protect stored cardholder data.		
3.6	Prevention of unauthorized substitution of cryptographic keys.	RackFoundry TSM's File Integrity Monitoring (FIM) monitors file/directory changes, deletions, and changes in real time and sends alert notifications to support 3.6.7.
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	RackFoundry TSM monitors security protocols to notify users of improper usage in the cardholder data environment via alerts and reports.
5. Protect All Systems Against Malware and Regularly Update Anti-virus Software or Programs		

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	RackFoundry TSM integrates with anti-virus software to generate alerts/reports on anti-virus critical conditions and provide information on detected malware.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	RackFoundry TSM utilizes policies to notify users if anti-virus mechanisms are not current, not actively running, or not generating audit logs.
6. Develop and maintain secure systems and applications		
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.	RackFoundry TSM includes a Vulnerability Scanner that detects network vulnerabilities and assigns risk to them.
6.2	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	RackFoundry TSM includes a Vulnerability Scanner to detect patches that need to be installed.
6.3	Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle.	RackFoundry TSM monitors logs written by custom software and utilizes policies to alert users of security threats. RackFoundry TSM includes a Web Application Firewall (WAF) that can be used to monitor and protect custom web applications.
6.4	Following change control processes and procedures for all changes to system components.	RackFoundry TSM supports 6.4.1 and 6.4.2 by monitoring allowed/denied network traffic between the test environment and internal network environments via alerts and reports.
6.5	Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes.	RackFoundry TSM alerts users of any detected vulnerabilities within the software. RackFoundry TSM includes a Web Application Firewall (WAF) that can prevent injection attacks (6.5.1), cross-site scripting (6.5.7), and cross-site request forgery (6.5.9) among other known application level attacks.

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
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. • Installing a web-application firewall in front of public facing web applications.	RackFoundry TSM generates alerts/reports on detected web application vulnerabilities. RackFoundry TSM includes a Web Application Firewall (WAF) to detect and prevent known security threats at the application level.
Requirement 7: Restrict access to cardholder data by business need to know.		
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	RackFoundry TSM monitors privileged access, host authentication, application access and generates alerts if unusual activity is detected.
Requirement 8: Identify and authenticate access to system components		
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.	RackFoundry TSM supports 8.1.5 by alerting users of vendor authentication failures and access to vendor accounts.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.”	RackFoundry TSM supports 8.2.4 by alerting users of accounts that have not had a password change within 90 days.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods.	RackFoundry TSM generates alerts for detected group, shared, or generic IDs and passwords.
8.5	Restrict access to any database containing cardholder data (including access by applications, administrators, and all other users).	RackFoundry TSM monitors access to databases containing cardholder data and generates alerts when unauthorized access is detected or privileges are changed.
Requirement 9: Restrict physical access to cardholder data		
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	RackFoundry TSM supports 9.1.1 by generating alerts for physical access failures and including information in alerts.
Requirement 10: Track and monitor all access to network resources and cardholder data		

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
10.2	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses 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 identification and authentication mechanisms; initialization of the audit logs; creation and deletion of system-level objects.	RackFoundry TSM maintains a strong audit trail by storing logs and events in a secure repository to keep track of all user activity in support of 10.2.1, 10.2.2, 10.2.3, 10.2.4., 10.2.5, 10.2.6, and 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, and identity or name of affected data, system component or resource.	RackFoundry TSM maintains an audit trail that records user ID (in support of 10.3.1), type of event (in support of 10.3.2), date and time (in support of 10.3.3), success/failure of event (10.4.3), origination of event (in support of 10.3.5), and identity or name of affected data, system component, or resource (in support of 10.3.6).
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	RackFoundry TSM accurately and automatically synchronizes audit log time stamps to the absolute time standard (GTM) to ensure the true time is maintained.
10.5	Secure audit trails so they cannot be altered.	RackFoundry TSM maintains a strong audit trail by storing logs and events in a secure repository that are protected against unauthorized access, change, and deletion.
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	RackFoundry TSM includes a Centralized Logger to serve as a single dashboard to monitor all network logs. RackFoundry TSM correlates logs with related network events to detect security threats and generate alerts.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.	RackFoundry TSM includes up to 30 TB of storage maintain a large audit trail that can be accessed immediately. Logs can be retained for up to 7 years.
11. Regularly test security systems and processes		
11.1	Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	RackFoundry TSM generates alerts upon detection of unauthorized wireless access points.

Compliance Requirement #	Compliance Requirement Description	RackFoundry TSM Solution
11.4	Use intrusion-detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to date.	RackFoundry TSM includes an IPD/IDS tool to monitor network traffic and detect/prevent known security threats. RackFoundry TSM's signatures are automatically updated and pushed to the IPS/IDS tool. RackFoundry integrates with additional IPS/IDS solutions to correlate event data with related events and generate alerts.
11.5	Deploy 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.	RackFoundry TSM includes File Integrity Monitoring (FIM) to alert users of unauthorized changes to system files, configuration files, and content files.
12. Maintain a policy that addresses information security for employees and contractors		
12.3	Develop usage policies for critical technologies (for example, remote- access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.	RackFoundry TSM monitors remote access technologies, wireless devices, removable media, laptops, tablets, PDA's, and email/internet usage and provides information in the form of alerts and reports.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	RackFoundry TSM supports quick response plans by providing real-time continuous monitoring and rapid notifications in the event of a system breach. Alert notifications provide details of threat type, detection method, and appropriate response. RackFoundry's SOC is staffed 24/7/365 to provide continuous monitoring.

RackFoundry TSM leverages essential security capabilities to help organizations monitor important credit card holder data and detect security threats and vulnerabilities. In addition, RackFoundry's SOC ensures that threats are quickly addressed and effectively 24/7/365. Together, TSM helps take the challenge out of achieving and maintaining PCI DSS compliance and provides the tools to build a world-class security program for your organization, within one complete total solution.

About RackFoundry

RackFoundry, the maker of Total Security Management (TSM), is a leader in complete coverage security appliances, secure cloud services and professional services such as SecurityXpert that provides security expertise to organizations of all sizes and industries. The RackFoundry security team, FortressLabs™, help find new vulnerabilities in the wild, mitigate any found vulnerabilities, and head up the RackFoundry Security Operations Center.

For more information visit us at www.rackfoundry.com.