

## PCI DSS Overview

The Payment Card Industry Data Security Standards (PCI DSS) version 1.1, are a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

### **Build and Maintain a Secure Network**

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data

*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

### **Protect Cardholder Data**

*Requirement 3:* Protect stored cardholder data

*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

### **Maintain a Vulnerability Management Program**

*Requirement 5:* Use and regularly update anti-virus software

*Requirement 6:* Develop and maintain secure systems and applications

### **Implement Strong Access Control Measures**

*Requirement 7:* Restrict access to cardholder data by business need-to-know

*Requirement 8:* Assign a unique ID to each person with computer access

*Requirement 9:* Restrict physical access to cardholder data

### **Regularly Monitor and Test Networks**

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

*Requirement 11:* Regularly test security systems and processes

### **Maintain an Information Security Policy**

*Requirement 12:* Maintain a policy that addresses information security

How Refense VMS directly assists in PCI DSS Compliance:

Refense VMS provides a scalable, automated method of managing vulnerabilities and miss configurations within network devices. Refense VMS assist organizations with PCI/DSS compliance in 9 of the 12 specific requirement areas. The matrix below provides a mapping of the PCI/DSS compliance requirement and how Refense VMS directly assists in compliance.

PCI / DSS v1.1 Compliance - Matrix

PCI/DSS - Compliance Item	How Refense VMS Directly Assists in Compliance
Requirement 1 – Sub item 1.1.8 <i>Quarterly review of firewall and router rule sets</i>	Refense VMS provides an easy, scalable solution to perform periodic review of firewall and router rule sets by analyzing the stored and running configuration of those devices from a security perspective
Requirement 1 – Sub item 1.1.9 <i>Configuration standards for routers</i>	Our intuitive security solution provides a strong framework towards enabling enterprise organizations in creating and verifying secure configuration standards for all network devices within their organization.
Requirement 1 – Sub item 1.3 <i>Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.</i>	Our proprietary ComparaSec™ algorithm is designed to allow dynamic indexing and searching of firewall configurations to ensure that all enabled rules meet compliance as dictated by the organization.
Requirement 1 – Sub item 1.3.6 <i>Securing and synchronizing router configuration files.</i>	Refense VMS is the only dedicated security product which provides the capability to ensure network devices are securely configured and with the capability to ensure vulnerable services are mitigated and or eliminated
Requirement 2 – Sub item 2.1 <i>Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).</i>	Refense VMS provides the out-of-the box capability identify and assist in eliminating vendor supplied defaults of network devices within items such as SNMP strings, passwords and default user accounts
Requirement 2 – Sub item 2.1.1 <i>For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.</i>	Our security appliance enables organizations to easily audit their wireless networks to identify insecure and vulnerable wireless configurations such as default SSID's and insecure WEP/WPA configurations.

## Refense VMS™ Ensuring a PCI DSS Compliant Network

PCI/DSS - Compliance Item	How Refense VMS Directly Assists in Compliance
<p>Requirement 2 – Sub item 2.2 <i>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 as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).</i></p>	<p>Refense VMS provides enterprises the ability utilize a secure hardened pre-defined security configuration out of the box and or custom tailor that security configuration policy to their own specific needs and requirements. All pre-defined security configuration policies are based on industry standards from organizations such as SANS, NSA and NIST to include vendor recommendations as well.</p>
<p>Requirement 3 <i>Protect stored cardholder data</i></p>	<p>Refense VMS is built upon a modular framework to identify and mitigate vulnerabilities across a wide range of network devices. Most specifically as it relates to Requirement 3, it would provide security compliance and hardening as it relates to storage area networks, a common focal point for sensitive cardholder data.</p>
<p>Requirement 4 – Sub item 4.1.1 <i>For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS.</i></p>	<p>Our security appliance enables organizations to easily audit their wireless networks to identify insecure and vulnerable wireless configurations such as default SSID's and insecure WEP/WPA configurations.</p>
<p>Requirement 6 – Sub item 6.1 <i>Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.</i></p>	<p>Refense VMS is the only dedicated security product which provides the capability to ensure network devices are securely configured and with the capability to ensure vulnerable services are mitigated and or eliminated. This includes the ability to pinpoint current and or non-existent patches to ensure network devices remain up to date as per PCI requirement 6.1</p>
<p>Requirement 6 – Sub item 6.2 <i>Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.</i></p>	<p>Refense' Security Threat Research (STR) Center continuously monitors and researches new and current security vulnerabilities. This undertaking is performing from the perspective of examining all operating system code and updates to the operating as to their effect on security and methods this could be compromised. Therefore, security checks are developed to identify new potential issues before attackers ever zero in. When combined with the security intelligence of current threats, this is a powerful combination enabling Refense customers to be ahead of the threats.</p>
<p>Requirement 7 <i>Restrict access to cardholder data by business need-to-know</i></p>	<p>Network devices are increasing in the level of responsibility and often times are a focal point for an organization from a network, access control perspective and with increasing occurrence from an application perspective as well. Refense provides the capability to ensure security standards as they relate to these devices are securely implemented and followed.</p>
<p>Requirement 8 – Sub item 8.4 <i>Encrypt all passwords during transmission and storage on all system components.</i></p>	<p>Refense VMS provides the ability to establish security policies to comply with the PCI regulation specifically to identify and validate the implementation of password encryption within network devices. By utilizing our scheduled scan module, an organization can ensure they are continuously in compliance with this item of the regulation.</p>

# Refense VMS™

## Ensuring a PCI DSS Compliant Network

PCI/DSS - Compliance Item	How Refense VMS Directly Assists in Compliance
Requirement 8 – Sub item 8.5 <i>Ensure proper user authentication and password management for non-consumer users and administrators on all system components</i>	Our proprietary security appliance provides the capability to comply with section 8.5 of the PCI regulation by ensuring secure and correct username and password management is configured for all users and administrators within network devices.
Requirement 10 – Sub item 10.2 <i>Implement automated audit trails for all system components</i>	Implementing automated audit trails enables organizations to track and better identify security incidents. Refense VMS provides the capability to identify the lack of automated audit trails within all network devices.
Requirement 10 – Sub item 10.3 <i>Record at least the following audit trail entries for all system components for each event</i>	Implementing an audit trail of user actions, network access attempts and administrative changes is crucial towards ensuring a methodology for future forensic analysis. Refense VMS provides the capability to identify the specific implementation and usage of detailed logging within all network devices in your organization.
Requirement 10 – Sub item 10.4 <i>Synchronize all critical system clocks and times.</i>	Maintaining an accurate time within all network devices is critical in tracing and investigation future attacks and compromises within the network. Refense VMS effortlessly provides this capability by identifying correct and secure configuration for NTP services and authentication.
Requirement 10 – Sub item 10.5 <i>Secure audit trails so they cannot be altered.</i>	Refense VMS provides the ability to perform a vulnerability assessment against network devices to determine issues and security threats that would compromise the ability to maintain a secure audit trail.
Requirement 11 – Sub item 11.1 <i>Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.</i>	Refense VMS provides an easy and effortless ability to test security controls and restrictions within network devices, the core of every enterprise infrastructure. Additionally, via our wireless vulnerability module, Refense can identify threats and vulnerabilities within wireless network devices, providing a much more in depth capability than just using a wireless device analyzer.
Requirement 11 – Sub item 11.2 <i>Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).</i>	Refense VMS enables organizations to develop and implement the ability to perform regular and periodic vulnerability scans as per the PCI regulation, Requirement 11 – Sub item 11.2. This enables organizations to be directly in compliance with this policy and also provides them the ability to perform ad-hoc scans as required.
Requirement 11 – Sub item 11.3 <i>Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).</i>	Refense VMS provides the capability to perform security testing against one of the most critical areas within an IT Infrastructure, the network devices. This enables organizations to test security configurations as new devices are modified and or added to the network, to ensure security standards and policies are upheld.

