



**PCI DSS COMPLIANCE Version 1.2 - October 2008**  
**NetFort Technologies helping organisations to meet Payment**  
**Card Industry Data Security Standard**



## DSS Version 1.2: October 2008 Revision

### NetFort LANGuardian 6.3 Offers Risk Prevention and Business Assurance by Meeting Your Organisation's PCI Compliance Requirements

The PCI (Payment Card Industry) DSS (Data Security Standard) was originally introduced to the online transaction world in 2005 in light of growing incidents of identity theft and data leakages surrounding credit card account holder and transaction information. The focus of the standard is to enforce corporate compliance with regard to data security and the assurance of identity protection around all credit card transactions carried out over public networks.

Enforcement of the PCI standard in organizations is currently low because IT departments are lacking the tools necessary for successful implementation. However, industry experts anticipate that the majority of companies will be PCI compliant within the coming 12 months. PCI compliance is no longer an option for corporations. If your organization stores or processes credit or debit card data, including merchants and third-party service providers it is imperative that you are PCI compliant.

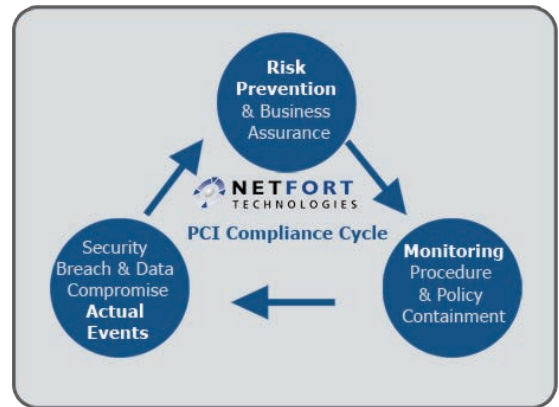
Penalties for non-compliance in the event of a major leakage of confidential transaction or account holder information are severe. Organisations have incurred substantial monetary fines and can, in the worst case scenario, suffer loss of merchant trading license. Ultimately, non-compliance can lead to the ruination of your business.

The implementation of NetFort LANGuardian into an existing IT infrastructure facilitates an easy transition for certain key components of the standard from a non-compliant to compliant status. LANGuardian is tamper-proof and offers assurance that certain measures required for compliancy approval are present in the overall corporate IT system, via LANGuardian's PCI Compliance Cycle of **Risk Prevention, Monitoring Procedures and Actual Event Alerts**.



#### RISK PREVENTION & BUSINESS ASSURANCE

- Assuring that compliancy requirements for firewall and router configuration rules are validated through trend reporting
- Information security policy creation and enforcement, that addresses data security, access issues and rights regarding employees/contractors
- An effective audit trail on data is available to ensure that access to cardholder and sensitive transaction data is restricted to authorized persons only
- The IDS (Intrusion Detection System) feature of LANGuardian does not only rely on signature or pattern matching to detect anomalies and can therefore run in complement to antivirus software to reinforce IT infrastructure protection



#### MONITORING: PROCEDURE & POLICY CONTAINMENT

- Always-on" network and user activity monitoring. Detects systems or network devices that are out of compliance with established standards using signature matching and traffic analysis
- Optimized data forensic tools offer permanent availability of real-time reporting on user access to network resources and cardholder data over preceding three-month period. Historical user information over one year period is always available as back up data



#### SECURITY BREACH & DATA COMPROMISE ALERTS

- Alerting in the event of access to or removal of restricted data by unauthorized users
- Real-time identification of affected systems in buffer overflows, worm infections or Denial Of Service attacks
- Immediate alerts in the event of access to restricted or sensitive information by non-authorized users
- Complementary to antivirus software/does not solely rely on pattern matching or definitions

PCI Objective	Requirements	NetFort Assurance
<b>Build and Maintain a Secure Network</b>	1: Install and maintain a firewall and router configuration to protect cardholder data  2: Do not use vendor-supplied defaults for system passwords and other security parameters	<i>The LANGuardian firewall and router configuration validation service verifies security policy configurations by rapidly identifying non-compliant traffic. User trends and reporting are easily implemented to ensure that the following compliancy standard firewall or router rule breaches are alerted on;</i> <ul style="list-style-type: none"> <li>• Restricted inbound and outbound traffic to cardholder data is not jeopardized</li> <li>• Assurance that traffic from unauthorized sources in the card data environment is specifically identified</li> <li>• All traffic is monitored to prohibit direct routes for inbound and outbound internet traffic</li> </ul> <i>Detection of non-compliant network devices or systems is easily facilitated via the signature matching and traffic analysis channel. In line with the PCI standard requirements to ensure that all servers have only one primary function, LANGuardian has the ability to monitor and alert where this rule is compromised and servers perform two primary functions;</i> <ul style="list-style-type: none"> <li>• Verification that all non-secure and unnecessary services (services and protocols not directly needed to perform the devices' specified function) and protocols are disabled</li> <li>• Detection of all non-encrypted data transmissions</li> </ul>
<b>Protect Cardholder Data</b>	3: Protect stored cardholder data	<i>Validates and reports on the removal of specific data. Alerts if restricted files are accessed. User information is recorded by IP or username</i>

**DSS Version 1.2: October 2008 Revision**

PCI Objective	Requirements	NetFort Assurance
<b>Maintain a Vulnerability Management Program</b>	<b>4:</b> Encrypt transmission of cardholder data across open, public networks	<i>Encrypt transmission of cardholder data across open, public networks is a PCI standard requirement. While LANGuardian does not directly encrypt data, it has the ability to detect and alert unencrypted data in transmission across an environment that requires encryption.</i>
	<b>5:</b> Use and regularly update anti-virus software or programs	<i>Complementary to antivirus software, LANGuardian does not solely rely on pattern matching or signature-based definitions to detect anomalies. The LANGuardian is fully compliant with requirement 5 of the PCI standard, demonstrating the ability to detect and alert to signature and non-signature based anomalies.</i>
	<b>6:</b> Develop and maintain secure systems and applications	<p><i>Software version control: Monitors to ensure most current versions are in use. Detects and alerts where use of earlier versions of software with known vulnerabilities are in use on the network.</i></p> <p><i>Can monitor servers to safeguard different working environments and detect unauthorized traffic into each environment.</i></p> <p><i>Tracks which systems were affected in the event of denial of service attacks or worm infections and whether or not protected systems were affected. In essence LANGuardian will identify DOS and buffer overflows in real time as they occur.</i></p>
<b>Implement Strong Access Control Measures</b>	<b>7:</b> Restrict access to cardholder data by business need-to-know	<p><i>This is undoubtedly one of the LANGuardian's areas of strength in offering real time compliance.</i></p> <p><i>Validates access to cardholder information on an IP, machine name or username basis, providing an audit trail showing which users are accessing sensitive information. Alerts can be set to flag access cardholder data by non-privileged users.</i></p>
	<b>8:</b> Assign a unique ID to each person with computer access	<p><i>The LANGuardian has the ability to monitor lower level of access characteristics of an Active Directory user with MAC and IP addresses.</i></p>
<b>Regularly Monitor and Test Networks</b>	<b>9:</b> Restrict physical access to cardholder data	<p><i>Not Applicable</i></p>
	<b>10:</b> Track and monitor all access to network resources and cardholder data	<p><i>Requirement 10 is one of the LANGuardian's primary areas of strength. Finite visibility of network user activity is the cornerstone of LANGuardian's success, thus meeting the parameters set out in requirement 10 of the PCI standard.</i></p> <p><i>Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis in the event of a compromise. The LANGuardian recognizes that system activity logs are vital in determining the cause of a compromise, therefore, all historical data is kept in storage for a year. Real-time reporting is available on data from the preceding three months.</i></p>
	<b>11:</b> Regularly test security systems and processes	<p><i>The LANGuardian's integrated Intrusion Detection System covers compliancy to PCI with regard to the total monitoring of all network traffic, examining traffic integrity and alerting to vulnerabilities and suspicious traffic.</i></p> <p><i>Vulnerabilities are discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.</i></p>
<b>Maintain an Information Security Policy</b>	<b>12:</b> Maintain a policy that addresses information security for employees and contractors	<p><i>The LANGuardian can accommodate all compliancy requirements in requirement 12 by monitoring and enforcing all facets of the corporate security policy, ensuring that no deviations occur.</i></p>