

PCI Compliance

If your company must maintain and verify compliance with the Payment Card Industry (PCI) Data Security Standard (DSS), you are well aware of the mandate's comprehensive nature. And you need to sustain overall good governance of your IT environment not only during periodic audits and assessments, but each and every day.

Make Longitude[®] application performance and network monitoring part of your proactive best practices approach to PCI DSS – one that promotes the availability and performance of your IT environment while helping you automate the daunting process of daily compliance monitoring. Longitude conforms to the PCI DSS principles of vulnerability management, strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

For example, use Longitude to perform the event log monitoring specified by PCI DSS Requirement 10. Longitude automates the daily monitoring required with comprehensive WindowsEventLog and Syslog solutions that collect and centralize event log records for reporting, display, and alerting. Event log records can be consolidated and viewed within the Longitude real-time Event Monitor and used to automatically trigger Longitude actions: including Email, Text Message, SNMP Trap, or Execute a corrective OS command.

To reduce event volume and increase situational awareness, leverage Event Correlation in Longitude to detect patterns in audit events – such as multiple logon failures followed by successful logons, or logon failures from unexpected sources – or combinations of events and data from other sources.

Role-based security also ensures Longitude users see only those specific monitoring tasks and related information they are pre-authorized to view.

Contact Heroix for more information on how Longitude monitoring can support your PCI DSS compliant environment. For complete information about the PCI DSS, visit the PCI Security Standards Council at pcisecuritystandards.org.



165 Bay State Drive
Braintree, MA 02184
Telephone: 800-229-6500 / 781-848-1701
www.heroix.com
info@heroix.com

PCI Compliance at a Glance

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
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