

Meeting the PCI DSS Compliance Challenge

How Luminet Enterprise Fraud Management Software Can Help

One of the toughest challenges facing organizations trying to comply with the Payment Card Industry Data Security Standard (PCI DSS) comes from section 10.2.1. This section requires them to “implement automated audit trails for all system components to reconstruct all individual user accesses to cardholder data.” In addition, section 10.2.2 requires that “all actions taken by any individual with root or administrative privileges” must be included in the audit trail.

Why Audit Trails Are Hard to Build

Complying with the PCI DSS audit trail requirements is difficult for four reasons:

1. Most applications, both legacy and modern, do not include a logging mechanism that provides a complete history of user access to cardholder data. In many cases, logs include only update actions and not user queries and other read-only actions. An audit of all individual user access must include read-only activity in order to be complete.
2. Simple log aggregation may meet some of the PCI DSS requirements, but falls short of providing the complete audit trail required by section 10.2. If your logs do not contain sufficient data or capture only specific types of activity, then log aggregation will not help you comply with section 10.2.
3. Developing your own in-house solution involves a lengthy and expensive development effort. Thousands of your organization’s application programs may need to be changed, re-tested and re-deployed. Then, after all that work, you’d still be left without a centralized and easily managed view of exactly who did what and when across all applications and systems.
4. Capturing only database activity may also leave you noncompliant since most applications use generic user IDs for database access. As a result, you have no way to meet the requirement for auditing “all individual access.”

Fortunately, technology does exist that can help you overcome these challenges.

See It. Record It. Analyze It.

Attachmate Luminet™ software was specifically designed to capture a complete picture of all user access to payment card information—so you can finally stop combing through cryptic log files in order to create a credible story for auditing purposes. Here’s how Luminet works:

- **Sees user activity**

Luminet gives you the tools to define adaptable business rules that pinpoint suspicious behavior based on your risk management strategy. Then Luminet generates real-time alerts related to questionable activity patterns, allowing you to immediately zero in on anomalies.

- **Records user activity**

Luminet records user activity in real time—screen by screen, keystroke by keystroke—creating an audit trail directly from the network. This audit trail includes both update and read-only actions for both regular and privileged users. Luminet stores this information in a secure repository, from which you can conduct powerful full-text searches through current or recorded activity. These searches allow you to visually play back every screen and keystroke relevant to your audit. Customizable dashboards, graphs, and reports enable your internal auditors to see the big picture at a glance and zero in on activity that puts PCI DSS compliance at risk.

About PCI DSS

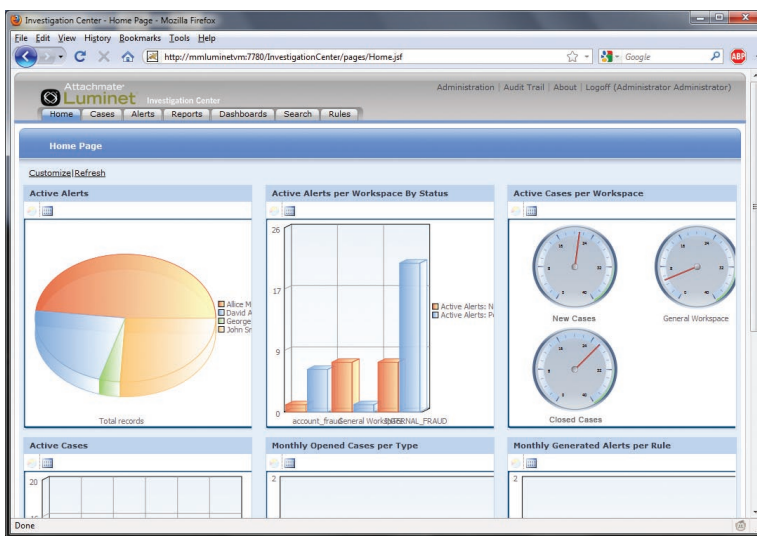
The Payment Card Industry Data Security Standard (PCI DSS) was developed and is maintained by the PCI Security Standards Council (pcisecuritystandards.org)—an open global forum founded by the major credit card companies to define requirements for organizations processing credit card information. The goal of the standard is to prevent payment card fraud and create consistent security measures across all uses of payment card information. The standard defines 12 specific requirements that must be implemented by organizations that store, process, or transmit cardholder data.

PCI DSS Copyright © 2006 - 2010 PCI Security Standards Council, LLC. All rights reserved. www.pcisecuritystandards.org

Analyzes user activity

Luminet helps you clearly distinguish between dubious activity and legitimate work. An interactive tool detects cross-channel patterns across multiple employees and departments, as well as across diverse applications. As a result, you can take immediate and decisive action on suspicious behavior.

In other words, Luminet sees, records, and analyzes user activity across enterprise applications, providing a complete audit trail of individual access to sensitive information such as payment card data. Without adding new controls or changing a line of code in your existing applications, Luminet gives you a complete audit trail that helps you comply with PCI DSS requirements 10.2.1 and 10.2.2.



Monitor key activity metrics with customizable dashboards.

**Luminet:
See It. Record It. Analyze It.**

Luminet fraud management software sees, records, and analyzes user activity across enterprise applications. It removes the guesswork from application monitoring, giving you the intelligence you need to take informed action.

Key features include:

- Agentless architecture
- Cross-channel monitoring
- Real-time alerts
- Visual application screen replay
- Google-like search
- Graphical link analysis
- Legacy application support
- Case management suite
- Custom dashboards and reports

About Attachmate

Attachmate delivers advanced software for terminal emulation, legacy modernization, managed file transfer, and enterprise fraud management. With our technologies, more than 65,000 businesses worldwide are putting their IT assets to work in new and meaningful ways. www.attachmate.com



Corporate Headquarters
 1500 Dexter Avenue North
 Seattle, Washington 98109
 TEL 206 217 7500
 800 872 2829
 FAX 206 217 7515

EMEA Headquarters
 The Netherlands
 TEL +31 172 50 55 55
 FAX +31 172 50 55 51

Asia Pacific Headquarters
 Australia
 TEL +61 3 9825 2300
 FAX +61 3 9825 2399

Latin America Headquarters
 Mexico
 TEL +52 55 9178 4970
 FAX +52 55 5540 4886

WEB attachmate.com
 E-MAIL info@attachmate.com

For regional office information, visit www.attachmate.com.