



Exposing Security Shortcomings of PCI Compliance-in-a-Box; Real-Time Correlation is Critical

TriGeo Helps Meet 11 of 12 PCI Requirements, Surpassing After-the-Fact Forensic Logs to Spot and Stop Sophisticated Attacks as They Occur

POST FALLS, Idaho (July 29, 2008) — [TriGeo Network Security](#), the leading provider of [security information and event management](#) (SIEM) technology for mid-market enterprises, is providing real-time correlation to help meet 11 of the 12 [Payment Card Industry Data Security Standard](#) (PCI DSS) Requirements.

While log aggregators only provide after-the-fact breach forensics, [TriGeo Security Information Manager \(SIM\)](#) analyzes user and network actions as they occur to identify, correlate and block unauthorized insider and hacker activity. This approach helps merchants comply with PCI by providing policies, controls and visibility across the network to safeguard credit card data.

“PCI compliance – and security in general – are ongoing processes, requiring network logs to constantly be analyzed and correlated for unusual and authorized patterns,” said David Taylor, founder of the [PCI Knowledge Base](#)[™]. “Post-breach log analysis offers little comfort to victimized organizations and their customers.”

Grocery store chain Hannaford, for example, recently revealed that malicious software recorded credit card data in transit, exposing thousands of account numbers – even though it was PCI compliant at the time of the breach. The lessons: compliance is not synonymous with security, and hackers will continue to evolve their attack methods to exploit network weaknesses.

“The ultimate goal is to fully secure data and systems, not comply with PCI or any other regulation,” said Michelle Dickman, president and CEO of TriGeo Network Security. “Merchants need intelligence, insight and actionable information about network activities. Logs stuffed into a server and check-box reports give organizations a false sense of protection.”

The Missing Ingredient: Real-Time Actions

TriGeo provides the industry's only real-time SIEM solution, helping streamline PCI compliance with 11 of the 12 standards. Key examples:

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - TriGeo audits firewall policy changes and VPN access, and goes a step beyond the requirement by allowing organizations to block suspicious IP addresses and lock down systems when a potential breach is detected.
- Requirement 7: Restrict access to cardholder data by business need-to-know
 - TriGeo captures access to sensitive files and alerts IT staff of unauthorized changes. Administrators can also create policies to automatically terminate connections when unapproved actions are detected.

(more)

- Requirement 10: Track and monitor all access to network resources and cardholder data
 - TriGeo tracks logon failures and rules for change management and file auditing, notifying IT when users or systems perform anomalous activities.

“Every penny mid-market companies spend on IT has to pay off,” said Dickman. “While promising PCI compliance in a box is a profitable approach, it doesn’t work – because those products lack the real-time correlation, analysis and response required to protect cardholder data from today’s and tomorrow’s threats.”

TriGeo SIM gives merchants more than 600 pre-built rules and 240 reports – dozens dedicated to PCI – for data and network protection, and the ability to easily create new rules and reports on the fly to meet any new requirements or data security needs. TriGeo’s customer base of hundreds of mid-market organizations includes dozens of banks, retailers, non-profit organizations and other merchants that must abide by PCI standards.

“There are dozens of products on the market that promise PCI compliance. TriGeo is the only one we found that provides real-time analysis – at an affordable price,” said Brady Decker, CTO at the National Aquarium in Baltimore. “We had an immediate need to pass our PCI audits, but the more important long-term goal is strong security.”

TriGeo SIM goes far beyond log management, providing the standard documentation of all machine, user and network activity, plus proactive responses such as quarantining, blocking, routing and controlling services, processes, accounts and privileges in real time – at a price starting below \$20,000.

###

About TriGeo Network Security

TriGeo Network Security delivers enterprise security information and event management (SIEM) designed specifically for the needs of the mid-market. TriGeo SIM is the only real-time SIEM appliance that automatically identifies and responds to network attacks, suspicious behavior and policy violations. This award-winning product combines real-time log management, event correlation, USB detection and prevention with powerful active response technology. TriGeo SIM is both a unique network defense technology and an “Audit-Proven” compliance solution that meets the security monitoring and log management requirements imposed by PCI, GLBA, NCUA, FDIC, HIPAA, SOX and more.

TriGeo has hundreds of customers across key vertical markets including financial services, health care, government, utility, retail and media/entertainment. TriGeo SIM has won numerous awards including the 2007 and 2008 *SC Magazine* Reader Trust Award, 2007 Frost & Sullivan North American Technology Innovation of the Year Award, the *Bank Technology News* #1 ranking in the 2008 FutureNow List, and the *SC Magazine Best Buy* of 2006 award for Event Management. The Company is a member of the PCI Security Standards Council and PCI Security Vendor Alliance and is represented by partners nationwide.

For additional information about TriGeo and its products, services and partners, please contact TriGeo at 1 (866) 664-9292 or at www.TriGeo.com.

Media contact:

Dan Brennan
Corporate Ink Public Relations
(617) 969-9192
dbrennan@corporateink.com