

## PCI DSS and other IT Security Compliance

### Are you snowed under by event logs and alerts?

### Are you responding to threats and vulnerabilities quickly enough?

You may have anti-virus, firewalls and IDS installed, but you are not compliant unless you are monitoring, analysing and responding to the hundreds and thousands of alerts and event log entries made by those devices. Very few organisations have the staff to do this and many rely on periodic checking of logs. Syslog correlation software may help but you are still not compliant unless you have the mechanisms and resources to analyse and respond immediately to a threat.

**TriGeo** - specifically designed for mid-sized organisations without limitless budgets or resources - is an award-winning security information and event management system that helps you solve this problem. TriGeo automatically monitors alerts and syslog entries from devices such as anti-virus, firewalls, IDS/IPS/routers and servers (regardless of manufacturer), provides automatic correlation of alerts and event logs, AND it can be configured for active response with appropriate blocking commands to the alerting device - all in real-time.

### Is wireless LAN a threat to you?

The PCI standards consider wireless LAN a particularly strong threat and require regular scans for wireless activity. If you are using wireless LAN in your network, how do you check that it is still configured for maximum security and how do you guard against wireless intruders? If you have decided not to use wireless technology, how do you know it hasn't been introduced accidentally or maliciously (e.g. through a wireless-enabled laptop)?

**AirMagnet** provides a range of wireless security tools - from portable analysers for regular scans to permanently installed probes for 24x7 surveillance of wireless activity.

### Is your network safe against insider attack? Is your network safe against innocent insider mistakes?

People inside your firewalls can cause more loss than external attacks, through either malicious or accidental actions or even innocent unknown activity after hacking. Are you doing enough about internal security?

**Sourcefire** Enterprise Threat Management systems provide protection by combining Snort-based Intrusion Prevention, Network and User Behavior Analysis - spotting anomalous traffic for instance - Network Access Control - enforcing policies - and Vulnerability Assessment.

### Are your security devices connected in the best possible way?

Relying on span or mirror ports to connect in security devices is not good enough. Modern network access taps provide greater security, reliability and accuracy, particularly on heavily loaded networks or networks under attack. Better still, the latest generation of intelligent taps provide much greater flexibility and economy, connecting single network segments to multiple monitors, for instance, or aggregating multiple network segments onto one or multiple monitors and analysers.

**VSS Monitoring** provides a complete range of taps from simple 1:1 taps to intelligent, totally configurable n:n multiple taps featuring both data aggregation and data filtering.

**These are just a few of the ways in which we can help you meet PCI DSS and other IT security compliance standards. Other security products include IDS/IPS and full network data capture and forensics solutions.**