

NETWORK FORENSICS AND COMPLIANCE



»

“Currently none of the existing regulatory or industry requirements and standards take into account the entire spectrum of controls to ensure the overall security of the enterprise.”

— Jason Stradley, CSO, BT

Regarding advanced persistent threats...

“There are people smarter than you, they have more resources than you, and they are coming for you. Good luck with that.”

Matt Olney, VRT Researcher,
Sourcefire™

Compliance to information security regulations is a crucial issue for almost every organization within every industry. The vast scale of penalties for non-compliance has increased the need for making it an ongoing process (rather than quarterly or yearly), which has in turn put immense stress on manpower and time critical to the stability of each company. It also does nothing to address that simply adhering to compliance regulations does not guarantee security.

COMPLIANCE AND SECURITY

Solera Networks is the one answer for both problems: The need to be compliant to regulations and also ensure good overall security. The truth is, you can't stop what you can't find. That's why you need network forensics to better enable you to adhere to compliance requirements and to ensure swift, intelligent incident response. Active network forensics makes all network data flows instantly visible and replayable, enabling organizations to identify the full source and extent of any network security event and protect the network against further attack. Combining high speed data capture, indexed storage, and comprehensive analysis tools, active network forensics is comparable to putting a security camera on your network.

A network forensics platform from Solera Networks addresses the following compliance-related categories: Monitoring, testing, surveillance, logging, auditing, data retention, and overall network security. However, compliance alone is not enough to protect against determined intruders. Information security regulations are “best practices” and only go so far. They cannot protect against the unknown unknown - the next threat and method of intrusion that has yet to be executed.

Banks install surveillance cameras to capture events of a robbery, identify the intruder, and provide evidence to locate and prosecute. Each and every industry needs to protect their customers and themselves beyond the practices of simply complying with their respective information security regulations. Complete network surveillance and forensics is the key to effective information assurance.

While the complexity of compliance regulations continues to grow, the opportunity to dramatically reduce costs and manpower for both maintaining compliance and improving incident response is now a reality. With Solera Networks, a simple search of recorded network traffic eliminates the need for endless hours of searching through terabytes of data. Our network forensics

