

Compliance Overview

Establishing the integrity and security of electronic information has become an absolute imperative. A broad range of electronic information now falls under the umbrella of an ever-expanding set of laws and regulations that require companies to protect that information and the systems that contain it. Companies must have the systems in place to capture, collect and protect all of the data needed for the growing number of compliance reports required by federal and state government regulatory organizations.

Network Intelligence simplifies and streamlines corporate compliance by collecting and protecting All the Data[™] that drives your business from every element in your IT infrastructure, including routers and switches, applications, servers and storage. This ensures that you have ready access to All the Data from everywhere in your enterprise, thus facilitating compliance reporting for regulations governing customer, patient and financial information. Network Intelligence assures your ability to accurately correlate, analyze and report the information required. It makes security information and event management (SIEM) a simple, highly accurate process that is capable of managing whatever volume of data your business generates with the ability to retain All the Data you need to address particular compliance reporting and security requirements at any time.

Network Intelligence Compliance Solutions

Compliance regulations supported by Network Intelligence include:

- **Sarbanes-Oxley (SOX)** ensures the accurate disclosure of corporate information.
- **Health Insurance Portability and Accountability Act (HIPAA)** protects the privacy and security of healthcare information.
- **US Patriot Act** helps the government combat the financing of terrorism while safeguarding the confidentiality of citizens.
- **Gramm-Leach Bliley Act (GLBA)** requires financial institutions to protect the security, integrity and confidentiality of consumer information.
- **Basel II** stipulates how banks must manage operational risk.
- **Payment Card Industry (PCI) Data Security Standard** establishes best practices to avoid Internet fraud and protect consumer information.
- **ISO27001/ISO17799** sets an information-systems standard for companies to use to ensure that the security controls for a system are fully commensurate with its risks.
- **Federal Information Security Management Act of 2002 (FISMA)** seeks to protect federal information through better computer and network security.
- **California Senate Bill 1386** requires all state agencies to immediately notify California residents when personal information in state control is compromised.
- **European Union (EU)** regulations are in the process of being streamlined into a cohesive set of laws governing data security, cyber-crime and anti-terrorism efforts. All require the comprehensive log capture, reporting and retention capabilities offered by Network Intelligence solutions.

Virtually all of the global compliance regulations address a broad range of varied regulatory requirements, and all require that companies solve a core set of problems and document resolutions with a core set of information for reporting and retention purposes. These include:

- **Access Control** monitors attempts to access anything on a company's access-protected systems including files, directories, database records or applications.
- **Configuration Control** monitors the configuration, policies and software installed on systems covered by a particular compliance regulation, as well as all other systems with which they interact.
- **Malicious Software** capabilities collect and report malicious activities caused by viruses or other malicious code.
- **Policy Enforcement** verifies that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- **User Monitoring and Management** creates a complete audit of the activities of non-employees with access to private data, and takes steps to minimize the risk from compromised accounts.
- **Environment and Transmission Security** involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measures such as VA scans. Additional monitoring is required to ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

To achieve and maintain compliance in those areas, companies must take the following actions with respect to the data collected by the Network Intelligence Log Management solution:

- Efficiently **Collect, Protect and Store** data in a secure, non-filtered and non-normalized fashion.
- Establish **Baseline** levels of activity for the entire system and network environment to define “normal activity” and detect unusual levels of activity.
- **Report** summary and detailed reports for the mandated periods of time.
- **Alert** companies to deviations from baseline activities, and detect complex patterns of malicious activity across multiple, disparate devices.
- Perform **Forensic Analysis** on systems to correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment.
- Establish **Incident Management** capabilities for close monitoring and correction of violations to make sure they are recorded, escalated and corrected in a timely and thorough manner.

The Network Intelligence Internet Protocol Database

Using its advanced LogSmart® Internet Protocol Database™ (IPDB) architecture that is deployed in hundreds of enterprises worldwide, Network Intelligence is able to capture All the Data from network, security, host, application and storage devices across the enterprise. LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization — from the IT department, to the security department, to the compliance and risk officers and executive management.

The benefits of LogSmart IPDB include:

- Designed to store and work efficiently with unstructured data natively, without any filtering or data normalization
- Maintain a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered — unlike most data schemas used in RDBMS-based solutions
- No agents are required
- Distributed peer-to-peer architecture enables high scalability and performance

Compliance Alerts

Network Intelligence provides the ability to automatically generate alerts based on non-compliance with an observed baseline. This means, should a particular control deviate above certain thresholds, an alert can be triggered and action can be taken to maintain compliance.

About Network Intelligence Corporation

Network Intelligence, part of RSA, The Security Division of EMC, is the market-proven leader in transforming enterprise-wide data into compliance and security information. The LogSmart® Internet Protocol Database (IPDB)™ provides the only architecture proven to efficiently collect and protect all the data that drives customers’ businesses. Network Intelligence takes the cost and complexity out of compliance and security for hundreds of customers worldwide. Network Intelligence was acquired by EMC in September 2006. For more information, please visit www.network-intelligence.com, or phone 781-375-9000.