

WHITE PAPER

ACHIEVE COMPLIANCE WITH PARITRA APPLIANCES AND SOFTWARE WHILE SECURING NETWORK DEVICES AND MITIGATING RISK

Network devices play a pivotal role in managing the communication infrastructure of businesses. Traditional security management appliances and software do not provide comprehensive policy implementation architecture to comply with various compliance requirements. Paritra Suite of products, along with offering applications for vulnerability analysis and security audits, offer applications to implement various compliance mandates.

COMPLIANCE IS MANDATORY FOR NETWORKS AND NETWORK DEVICES

Compliance is primarily concerned with the laws that a business must obey. In the absence of compliances, a business faces legal sanctions and the officers of the business may even have to face prison time. Compliances have now become more important than ever because of the recent corporate debacles. A typical organization needs to comply with one or more of the following government and industry regulations: SOX, HIPAA, ISO17799 etc.

In a company's compliance environment, it is natural to see overlap, inconsistency or contradictory rules among different regulations. So, complying with all the regulations applicable to a company is cumbersome. Moreover, traditional software applications focus only on a few specific compliances and do not provide a comprehensive centralized policy and compliance architecture. Compliance with respect to networks and network devices (the primary infrastructure that makes communication possible in a company) is a task in which the IT departments struggle. Trying to create a compliant network often results in wasted resources and an incomplete project where many of the network components are still being non-compliant. The following paragraph discusses why network components need to be compliant.

Computing needs of the businesses are growing rapidly. Businesses rely on networked applications to implement and execute complex business processes. This requires increased collaboration and interaction of various organizational elements. A networked environment makes this orchestration possible. In order to satisfy these requirements, IT operations have evolved into 'network centric' with the networks playing an important role in touching every aspect of the business and its processes.

The Sarbanes-Oxley (SOX) Act of 2002 was passed to ensure that the company executives will be held responsible if they provide wrong financial reports. Also, SOX act focuses on the accuracy of company's financial records and controls. Network security became a fundamental component of SOX because Public Company Accounting Oversight Board (PCAOB) that was created as a result of SOX, defined Standard # 2. This standard states that the company's management is responsible for the way company's information is generated, accessed, collected, stored, processed and transmitted. Networks and its devices play an important role in all of the above mentioned information management processes.

The Health Insurance Portability and Accountability Act (HIPAA) is a set of federal standards that mandates companies to implement security standards to protect patient's data (employees, retirees as well) and to standardize on electronic data interchange of such data. In translating HIPAA requirements to a company's network, Department of Health and Human Services has published recommendations. It can be found at <http://www.cms.hhs.gov/informationsecurity/downloads/ars.pdf> .

ISO 17799 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices.

Businesses have to establish processes and dedicate resources to comply with one or more of these regulations/guidelines. But, compliance is a difficult task worsened by the lack of well-developed compliant management applications. Therefore, there is strong need for policy based security management applications.

PARITRA APPLIANCES AND SOFTWARE MAKE COMPLIANCE POSSIBLE

Paritra suite of products provides a centralized security policy and risk management solution. Paritra's products focus on making network devices that are present in a network, compliant to various regulations. Paritra supports an automated policy framework that makes its applications unique in creating and complying with regulatory compliances SOX, HIPAA, and ISO17799, etc.

With the presence of many regulations, companies should select appropriate controls based on reasonably anticipated risks. This requires prioritization of network assets and its compliance. Paritra's applications include prioritization functions that help companies to achieve compliance of network devices in phases based on business priority.

Paritra's applications are designed to avoid complexity that arises from overlapping, inconsistency or contradictory rules of different regulations. Its easy-to-use wizards enable compliance reporting simple. In summary, Paritra's applications help companies to:

- Make information generation, access, collection, storing, processing, and transmitting processes comply with different government and industry regulations
- Standardize electronic transmission of data
- Institute network administrative and security safeguards
- Protect against known and imminent threats to network and its devices
- Defend against unauthorized access to information
- Make networks and network devices complaint to SOX, HIPAA, and ISO17799

CONCLUSIONS

Networked applications have produced significant gains for businesses through productivity improvements. But, network devices are one of the important agents that make 'networked applications' possible. Paritra suite of products help organizations to make its network devices compliant to various government and industry regulations thereby avoiding financial losses and penalties to companies.



Corporate Headquarters

Pari Networks
1313 North Milpitas Blvd., Suite 165F
Milpitas, CA 95035
USA
Tel: (408) 946 1800

Asia Pacific Office

Pari Networks
203 Srinivasa Somasikhara
Tilak Nagar
Hyderabad - 500044, AP
India
Tel: : + 91 40 27551074

Pari Networks is head quartered in Milpitas, California, with an Asia Pacific Office based in Hyderabad, India.