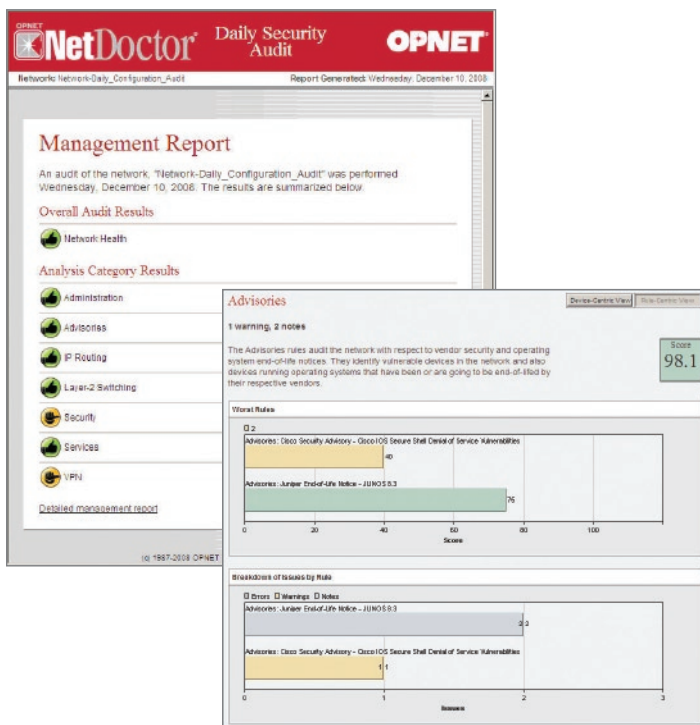


# OPNET Sentinel®

Network Audit, Security, and Policy Compliance

## Avoid Network Outages and Ensure Network Integrity

IT Sentinel® and SP Sentinel® ensure network integrity, compliance, and security for enterprises and service providers. Sentinel performs automated, systematic, network-wide configuration audits of the production network, identifying errors and misconfigurations that can impact network availability, performance, and security. Sentinel detects unexposed problems, and proactively notifies staff of critical errors. Sentinel's approach to auditing relies on a true semantic analysis of the network, providing a vastly more comprehensive detection of important network problems.

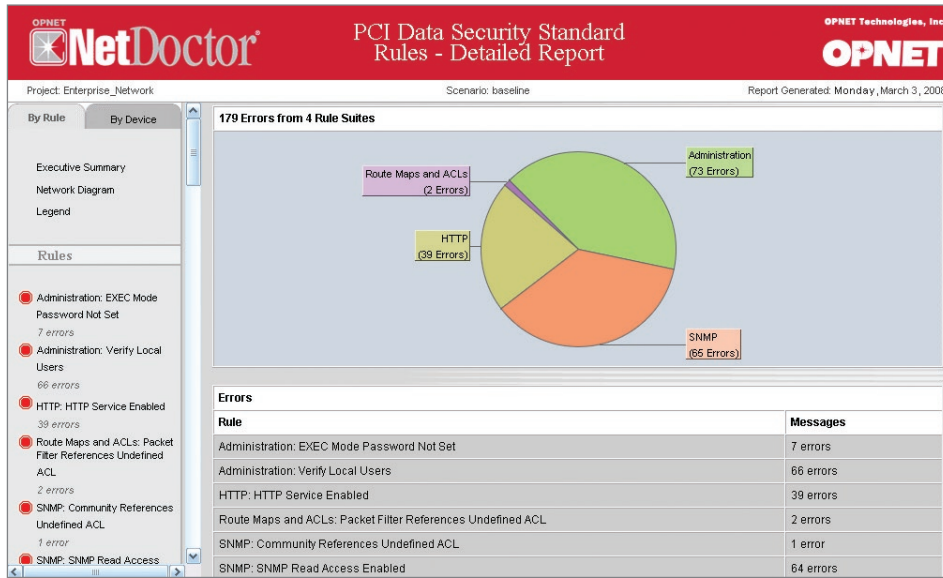


### Benefits

- Comply with regulatory, organizational, and security policies
- Avoid network outages from network misconfigurations
- Reduce operational costs with automated auditing and reporting

### Key Features

- Perform scheduled audits of routers, switches, and firewalls to pinpoint configuration errors before they affect network operations
- Verify that network security policies have been implemented effectively, and ensure compliance with regulatory and industry requirements
- Analyze devices, topology, and routing information against industry best practices
- Diagnose issues not detectable through regular expression-based analysis (the approach used by most auditing tools) using an intelligent semantic check of the entire network configuration
- Identify topology, device, and configuration changes using a comprehensive network differences report
- Customize organization-specific standards and requirements using an open authoring environment
- Publish comprehensive reports and automatically notify key staff about critical issues
- Publish up-to-date physical and logical network diagrams automatically through Sentinel's NetMapper module



“Sentinel takes the manual labor out of running a network audit. It automates the whole process of configuration collection, analysis, and reporting. The reports are created like clockwork every night and they identify a wide array of potential configuration issues that would be virtually impossible to identify manually.”

Senior Network Analyst  
Salt River Project

### Comply with Regulatory, Organizational, and Security Policies

Sentinel verifies that network security policies have been implemented effectively by pinpointing breaches in defenses such as open ports and misconfigured Access Control Lists (ACLs). Sentinel's rules-based analysis demonstrates compliance with security, regulatory, and organizational policies, leveraging out-of-the-box compliance checks for PCI, FISMA, Sarbanes-Oxley, HIPAA, NIST 800-53, NSA and others. In addition, Sentinel's NetMapper module addresses security standards and best practices requiring access to up-to-date network diagrams.

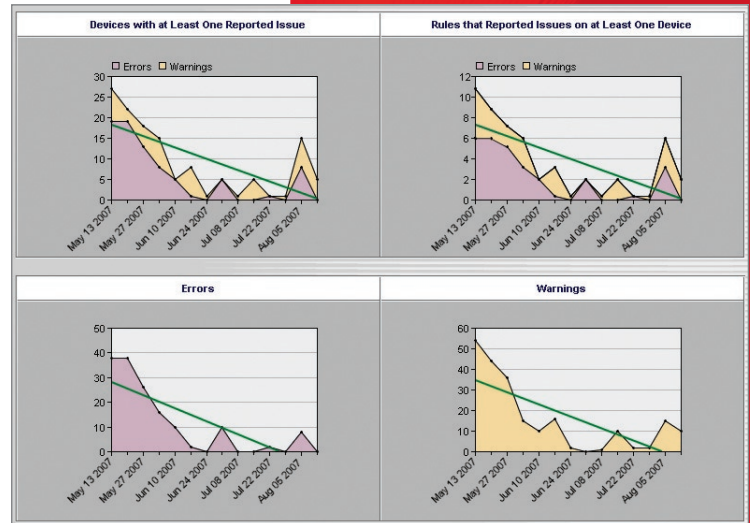
### Avoid Network Outages

Sentinel uncovers latent configuration issues that could cause network outages, leveraging an extensive rules-based analysis engine that checks topology, routing information, individual devices, groups of devices, and the logical relationships between them. Sentinel's best-in-class analytics understand networks and protocols and identify configuration issues not detectable through traditional string matching techniques used by most auditing tools.

### Reduce Operational Costs

Sentinel reduces the overhead of manual auditing and report generation. Sentinel publishes valuable network documentation and compliance reports, including executive summaries, detailed analysis, network differences, trending, and network diagrams.

In addition, Sentinel alerts key staff via email, pager, or trouble ticket, to quickly respond and fix network problems before they become critical.



www.opnet.com

**OPNET**  
Making Networks and Applications Perform®