“Based on the customized audit reports in Sentinel, we were able to enforce a global standard across the entire organization. The entire process is now automated, not only leading to significant cost savings, but also detecting policy violations much faster, before they affect service availability. As a result, we have been able to reduce network outages by as much as 30%.”

**Network Architect**
Global IT Services Management Organization

“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**
US Energy Utility

OPNET was selected to add value by allowing us to optimize network performance, including right-sizing links, minimizing mistakes in router configurations and even pointing out inefficient configurations. We have already experienced the benefit of using OPNET software through the reduced number of customer trouble tickets.

**Senior Consultant**
Global IT Services Management Organization

“Misconfigurations were reduced by more than 70% in just a few months through regular network configuration analysis. Our credit card services network is now operating with higher than ever infrastructure availability — over 99.5%.”

**VP, Infrastructure Performance Management**
Major US Bank

NetMapper accelerates network diagramming, auditing, and troubleshooting by automatically generating up-to-date infrastructure diagrams. Diagrams include detailed logical and physical device configuration information and logical views of the network, including Layer 2/3, OSPF, BGP, RSVP, MPLS, VRF, BGP, VLANs, Spanning Tree, VRFs, and device virtualization.

**Network Planner**
Network Planning and Engineering

Network Planner automates analysis and planning of multi-technology, multi-vendor networks. It performs “what if” analyses to manage risk and cost associated with network growth and change — accelerating application deployments and migration to new technologies, such as VoIP, VRFs, IPv6, and more. Network Planner’s predictive design environment trends traffic growth for capacity planning, optimizes network designs to reduce the risk of downtime, and proposes QoS configurations to achieve desired network and application performance.

**nCompass**
Real-Time Network Visualization and Monitoring

nCompass provides unified, real-time visualization and monitoring of large, heterogeneous networks, including devices, their interconnectivity, traffic, status and events. nCompass unifies data from a wide range of network management tools, providing consolidated views for more intuitive and productive navigation and analysis. Third-party tools and scripts can be launched from the nCompass console for deeper drill-down and expedited troubleshooting.

Sentinel is a software appliance for ensuring network integrity, security, and policy compliance. It performs automated network-wide configuration audits, analyzing an up-to-date model of your network to diagnose device mis-configurations, policy violations, configuration inefficiencies, and security violations. Sentinel’s intelligent analysis and reporting engine:

- Employs a unique model-driven auditing approach and rule-based analysis engine to pinpoint configuration mistakes and differences not detectable through traditional string matching techniques.
- Offers over 1,000 out-of-the-box rules based on industry best-practices (e.g., Cisco SAFE, CIS Benchmarks), security standards (e.g., PCI, DISA STIG), and field expertise.
- Provides simple, powerful, and flexible template-based checking of any command line output collected from devices.
- Allows rapid customization of rules and templates to ensure conformance to organizational standards and requirements.

**Benefits**

- Avoid network outages and minimize downtime by rapidly detecting network mis-configurations.
- Ensure compliance with regulatory, organizational, and security policies.
- Reduce operational costs with automated auditing and reporting.
- Plan for timely handling of hardware and software end-of-life announcements.
- Enhance staff productivity.

Perform network audits as frequently as you make changes to ensure policy compliance.
Solution Overview

**OPNET Technologies, Inc.**

**Sentinel**

Network Audit, Security, and Policy Compliance

**Key Features**

- Performs scheduled audits of network devices (e.g., routers, switches, firewalls, and load balancers) to pinpoint configuration errors.
- Analyzes a semantic model of the network to identify network configuration issues and differences not detectable through regular expression-based analysis (the approach used by most other auditing tools).
- Checks topology, routing information, individual device consistency, and logical relationships between devices to accurately pinpoint network configuration inconsistencies and differences.

- Provides popular out-of-the-box templates for regulatory and industry standards, e.g., PCI-DSS, FISMA, HIPAA, CIS, SOX, DISA STIG, NIST, NSA, and Cisco SAFE.
- Verifies that network security policies have been implemented effectively by identifying breaches in defenses such as open ports and misconfigured Access Control Lists (ACLs).
- Identifies device configuration, topology, performance, and routing changes in a comprehensive network differences report.
- Validates device configurations against a “golden” configuration.
- Enables proactive problem prevention with automatic download of new security advisories and OS end-of-life announcements.
- Provides a fully customizable rule suite, and an open authoring environment to enable rapid customization of audits based on organizational standards and requirements.
- Automatically alerts on critical issues via email, pager, SNMP trap, syslog, or trouble tickets.

**Compare Sentinel to Other Solutions**

- Unlike most auditing tools that use traditional string matching techniques, Sentinel uses an intelligent semantic analysis of the network to provide a more comprehensive detection of network problems.
- Provides a comprehensive network difference report comparing performance, routing and configuration changes to enable easy correlation of configuration changes to their impact.
- Sentinel offers validation and auditing of proposed changes prior to deployment.

**For Service Providers**

- Out-of-the-box auditing of BGP, IS-IS, OSPF, MPLS, and VPN configurations.
- Service summary reports describing configured L3/L2 VPNs and VPLS instances.
- IPv6 readiness assessments to evaluate a network’s ability to support required features prior to migration or deployment.
- Specialized rules to verify subscription/oversubscription thresholds based on client interfaces and services.

**For Service Providers**

Audit devices against vendor-issued security advisories and end-of-life notices. Plan for timely handling of hardware and software EOE and EOL announcements.

![Image of Sentinel Audit & Compliance](https://example.com/sentinel-audit-and-compliance.png)

**End-of-Life Details for Cisco Systems**

- Operating Systems already past EOL life

**HSRP: Insufficient Number of Routers**

This rule checks if every HSRP standby group in the network includes at least the specified minimum number of routers.

**NOTE**

- This rule operates on Cisco IOS and Cisco IOS XR devices.
- An HSRP standby group needs to have at least two routers in order to work.

**Differences**

- Increased number of active HSRP standby groups.
- Increased number of active HSRP standby group instances.

**For Service Providers**

- Out-of-the-box auditing of BGP, IS-IS, OSPF, MPLS, and VPN configurations.
- Service summary reports describing configured L3/L2 VPNs and VPLS instances.
- IPv6 readiness assessments to evaluate a network’s ability to support required features prior to migration or deployment.
- Specialized rules to verify subscription/oversubscription thresholds based on client interfaces and services.

**Key Features**

- Performs scheduled audits of network devices (e.g., routers, switches, firewalls, and load balancers) to pinpoint configuration errors.
- Analyzes a semantic model of the network to identify network configuration issues and differences not detectable through regular expression-based analysis (the approach used by most other auditing tools).
- Checks topology, routing information, individual device consistency, and logical relationships between devices to accurately pinpoint network configuration inconsistencies and differences.

- Provides popular out-of-the-box templates for regulatory and industry standards, e.g., PCI-DSS, FISMA, HIPAA, CIS, SOX, DISA STIG, NIST, NSA, and Cisco SAFE.
- Verifies that network security policies have been implemented effectively by identifying breaches in defenses such as open ports and misconfigured Access Control Lists (ACLs).
- Identifies device configuration, topology, performance, and routing changes in a comprehensive network differences report.
- Validates device configurations against a “golden” configuration.
- Enables proactive problem prevention with automatic download of new security advisories and OS end-of-life announcements.
- Provides a fully customizable rule suite, and an open authoring environment to enable rapid customization of audits based on organizational standards and requirements.
- Automatically alerts on critical issues via email, pager, SNMP trap, syslog, or trouble tickets.

**Comparison**

- Unlike most auditing tools that use traditional string matching techniques, Sentinel uses an intelligent semantic analysis of the network to provide a more comprehensive detection of network problems.
- Provides a comprehensive network difference report comparing performance, routing and configuration changes to enable easy correlation of configuration changes to their impact.
- Sentinel offers validation and auditing of proposed changes prior to deployment.