“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
Major US Bank

“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 infrastructure has now automated over 99.5% of routing, IP addressing, Hot Standby, ACLs — all of these are too important and too complex to be managed manually.”

Senior Network Analyst
Major US Bank

About OPNET Technologies

OPNET Technologies, Inc. is a leading provider of application and network performance management solutions. OPNET’s solutions deliver broad visibility and monitoring across infrastructure domains as well as deep data collection and analytics to enable powerful root cause diagnosis. These solutions have been operationally proven in thousands of customer environments worldwide.

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 rules-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

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, DOX, 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.

Correlate performance differences with configuration changes.

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 L2/L3 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.

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 L2/L3 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.

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

OPNET Technologies, Inc.

Solution Overview

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 L2/L3 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.

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

OPNET Technologies, Inc.