

## DATASHEET

### Business Benefits

- Easy to get started with built-in templates for best-practice standards, including PCI, NSA, SANS, DISA and others
- Able to prove security requirements by documenting network changes and archiving historical configurations
- Maintain continuous compliance via proactive configuration monitoring and policy violation detection, and prove with one-click reports
- Show access control with user-based tracking and audit logs
- Integrating with existing network management, reporting and ticketing platforms

### Continuous Monitoring for External Compliance and Internal Best Practice Standards

Proving success for both internal and external compliance mandates (including PCI, SOX, HIPAA, NERC, FERC and others) can take up considerable time and valuable IT staff energies. Today's expansive networks are growing even more complex due to initiatives like virtualization and cloud computing, which also heighten the importance of security requirements and network compliance. The onus of meeting the demands of mandates, security requirements and network compliance is magnified when these laborious tasks are taken on by outdated manual methods.

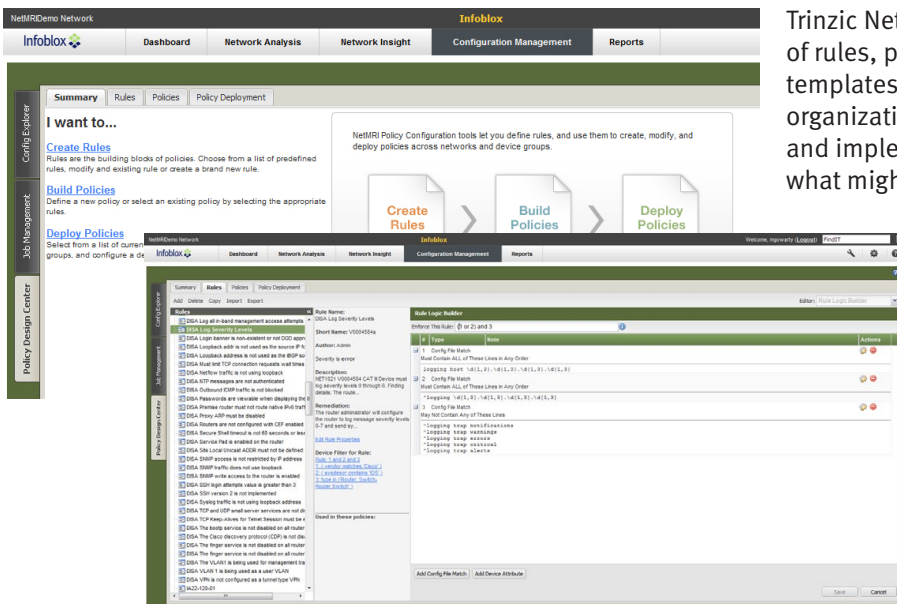
When auditors show up with their thick binders of requirements looking for proof of success, Trinzic Network Compliance makes certain that your network is in compliance at all times by automating the process of maintaining network standardization, meeting security requirements and proving success for external mandates or internal best practices. The automation maintains consistent network compliance for you 24x7x365, and also provides change detection and security requirements tracking, and delivers single click compliance reports.

### Ease of Implementation for Faster Value

Too often, IT organizations think of compliance only when audits are due because, overwhelmed with day-to-day activities, they don't have the time or people to achieve the full security and standardization value of the mandates.

Trinzic Network Compliance embeds hundreds of rules, policies, and industry best practice templates (including PCI, NSA, SANS and DISA) so organizations can simply select specific aspects and implement them faster instead of guessing what might be right for their requirements.

More importantly, the templates allow customization so that specific rules, individual to your organization, can be defined easily. Furthermore, you can create device groups so that specific compliance mandates or security standards can be checked against a designated set of network devices while other devices remain exempt. Instead of IT teams always scurrying to catch up in order to meet audit schedules, Trinzic Network Compliance allows them to get ahead of the curve proactively and automatically, using a proven, expert approach that stops wasting time, effort and money.



Build logical “if/then/else” and “and/or” rules without the need for scripting in most cases (with more than 200 packaged examples)

## DATASHEET

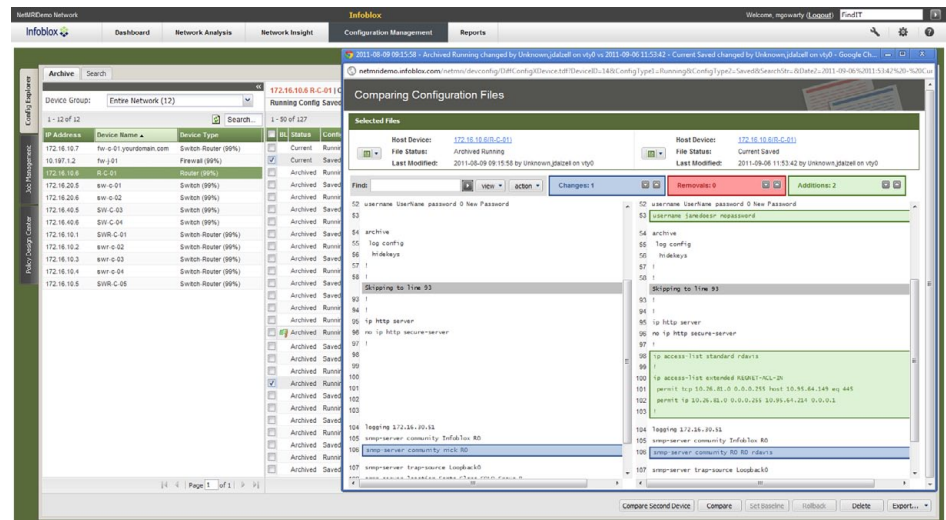
### Key Features

- Hundreds of embedded rules and policies based on industry standards, including PCI-DSS, NSA, SANS and DISA
- Ability to monitor multiple external compliance mandates or internal security standards with a single system
- Continuous monitoring of configuration standards with auto-generated issues for violations
- Detailed device-level or policy-level drill down views show all impacted elements or specific violations
- Device grouping shows which devices must follow the mandate and which ones are exempt
- Provides user-based access rights with multiple responsibility levels and audit logs
- Change monitoring and tracking shows who changed what, where, when and the impact of the change on the health of the network
- Collects and automatically archives current and historical network devices' configuration files with easy side-by-side comparison
- Dashboard views provide high-level overview of current state and security issues
- Delivers pre-built compliance reports (standard and customized) for audit requirements

### Prove Security Requirements with Change Tracking

The goal of any network compliance mandate is to improve security and reduce the risk of unwanted events by providing robust best practices and standards. IT groups want to take advantage of the benefits, but achieving the proof points and delivering the documentation can be overwhelming tasks.

When an auditor requires proof of every network change made during a particular day — who made the change and what was modified — a simple query in Trinzic Network Compliance eliminates the guesswork and shows every change in a matter of seconds.



Automatically collect and save current and historical configuration files with the ability to quickly compare any two files to see side-by-side changes, additions and removals

The comprehensive tracking, auditing and reporting capabilities of Trinzic Network Compliance lessen the time and manual effort needed to prove compliance success. The system automatically documents key criteria on an on-going basis, including tracking every change to any device, maintaining histories of configurations with side-by-side comparisons.

### Proactive Monitoring for Audit Requirements

Assuming that a simple report or merely collecting log files will meet the needs of a compliance audit is a common mistake. The truth is, many proof points must be demonstrated and documented to pass an audit, including tracking changes, showing access control, saving configurations and doing proactive monitoring. Attempting to meet these stringent demands through manual methods is a fruitless, never-ending struggle. Unfortunately, many IT teams procrastinate until an audit forces them to stop or limit operations while the staff puts into place and completes the mandated tasks satisfactorily.

## DATASHEET

Sadly, this disruption is doomed to a repeat performance the very next time an audit occurs. Moreover, the compliance achieved is only good for that single instant in network time. The next change could put the network out of compliance an hour after the audit is successfully passed.

**Policy Violation: PCI DSS 2.0 IOS**  
Showing details for Entire Network group

**Component:** Configurations **Correctness:** -2.0  
**Severity:** Error **Stability:** 0.0  
**Last Seen:** 2011-05-22 23:52:27

Device Name	Device Type	IP Address	Rules	Passed	Error	Warning	Info	Details	Last Seen
DEMO-SVRT-04	Switch-Router (99%)	10.10.10.4	23	12	8	2	1	View	2011-05-22 23:52:27
DEMO-RTR-05	Switch-Router (99%)	10.10.10.16	23	14	7	1	1	View	2011-05-22 23:52:27
DEMO-RTR-01	Switch-Router (99%)	10.10.10.11	23	12	8	2	1	View	2011-05-22 23:52:27
DEMO-SW-06	Switch (99%)	220.20.60.5	23	11	9	2	1	View	2011-05-22 23:52:27
DEMO-RTR-03	Switch-Router (99%)	10.10.10.13	23	12	8	2	1	View	2011-05-22 23:52:27

The continuous compliance monitoring automatically alerts you of policy violations with the ability to drill down into the specific cause

You can now archive all current and modified configurations, and continuously compare the settings against your defined customized standards. When a variation or discrepancy occurs, Trinzic Network Compliance generates an issue to signal the violation so that you can fix the risk quickly rather than wait months until the next audit uncovers the problem.

Instead of focusing on a one-time snapshot for compliance, Trinzic Network Compliance is a system for continuously monitoring and ensuring standardization. One-click reports highlight the current status of compliance for either external mandates or internal best practices anytime.

**Change Tracking and Audit Logs**

Change ID	IP Address	Device Name	Device Type	Change Type	Change Status
2011-09-01 11:22:11	172.16.30.5	SW-01	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-02	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-03	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-04	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-05	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-06	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-07	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-08	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-09	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-10	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-11	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-12	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-13	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-14	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-15	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-16	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-17	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-18	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-19	Switch (99%)	joined on vif0	Spang Config
2011-09-01 11:22:11	172.16.30.5	SW-20	Switch (99%)	joined on vif0	Spang Config

## Access Tracking and Audit Logs

For most security and audit requirements, IT organizations much show sufficient control of access to devices, as in answering the query, “How do you know the planned changes occurred, or that unplanned modifications didn’t happen?” Trinzic Network Compliance helps provide exactly what happened by tracking the exact changes made to the network devices. The automated tracking and audit feature provides a “checks and balances” view, and is a complementary solution to the traditional change management process and CMDBs.

Automatically track all changes made to the network devices (including physical card changes) & answer what device changed, by who, when and what changed

### Device Management, Issue Resolution, Requirement Customization and Constant Compliance Readiness

The screenshot displays three overlapping windows from the Infoblox interface. The top window shows a 'Policy Compliance Summary' for the network 'InfobloxDemo' with a date range from 2011-08-31 00:00:00 to 2011-09-06 23:59:59. It includes a pie chart for 'Policy Compliance By Device' showing 76.00% Error, 0.00% Warning, 0.00% Unknown, 24.00% Pass, and 0.00% Info. Below the chart is an 'Overall Status' table.

Overall Status	Overall Count	Number of Devices
ASA Firewall	error 2	1
Adapters	error 2	2
DSA Cisco Infrastructure Module v7.1.3	error 2	4
DSA Cisco Infrastructure Switch v7.1.9	error 2	1
DSA Cisco L2 Switch v7.1.9	error 2	4
DSA Cisco Perimeter Router v7.1.9	error 2	1
DSA Cisco Perimeter Switch v7.1.9	error 2	1

The middle window shows 'Policy Compliance Details' for device 'hw-j-01' under 'Policy ASA Firewall'. It lists several configuration commands that are missing, such as 'Rule ASA SSH' and 'Rule ASA HTTP', and provides the specific error messages.

The right window shows 'ISO 27002' compliance details for the network 'InfobloxDemo'. It includes a 'Summary of Findings' table with columns for Scope, Requirements, Supporting Evidence, and Results.

Scope	Requirements	Supporting Evidence	Results
7.1.1	Inventory of Assets An inventory or register is maintained with the important assets associated with each information system.	Infoblox automatically discovers network devices and provides a detailed inventory of network assets and their connection topology. See Table 1.	Pass
8.2.4	Equipment Maintenance Hardware should be kept at all support or failure faults, and all preventive and corrective maintenance.	Infoblox Event Analyzer automatically collects the log data of network devices. See Table 4.	Fail
10.1.2	Change Control Operational systems and application software should be subject to strict change management control.	Infoblox automatically detects configuration changes and collects and stores running and loaded configuration. Configuration is available for management system.	Pass
10.3.1	Capacity Planning The size of resources should be monitored, based, and projections made to ensure capacity requirements to ensure the longest system performance.	Infoblox automatically monitors key performance metrics of network devices and interfaces. See Table 3.	Pass
10.5.1	Information Back up The copy copies of information and software should be taken and backed regularly in accordance with the agreed back policy.	Infoblox automatically collects and stores running and saved configurations for network devices. See Table 2.	Pass
10.10.2	Monitoring system use Procedures for monitoring use of information processing facilities should be established and their results after monitoring activities reviewed regularly.	Infoblox Event Analyzer automatically collects the log data of network devices. See Table 4.	Fail
10.10.4	Administration and Operator Logs System administrator and a custom operator activities should be logged.	Infoblox Event Analyzer automatically collects the log data of network devices. See Table 4.	Fail
10.10.5	Event Logging Events should be logged, analyzed and appropriate actions taken.	Infoblox Event Analyzer automatically collects and continuously analyze the log data of network devices according to user defined rules. See Table 4.	Fail

Pre-built and customizable reports can prove compliance quickly and easily – either on demand or with scheduled results

In short, Trinzic Network Compliance not only keeps you ever-ready for a compliance audit with success reports and documentation of proof just a click away, but also gives you the tools you need to manage network devices, resolve issues as they arise, reduce the risks of fines and security breaches, and customize requirements specific to your network, including those for multi-vendor devices from over 30 manufacturers.

#### Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.