

DATASHEET

Key Features

- Embedded rules and policies for PCI-DSS standards
- Expert support for customizing templates into individually defined PCI rules and policies
- Automatic network discovery for multi-vendor network devices with multi-perspective topology views
- Continuous monitoring of configuration standards with auto-generated issues for PCI 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
- Change monitoring and tracking shows who changed what, where, when and the impact of the change on PCI compliance
- Collects and automatically archives current and historical network device configuration files with easy side-by-side comparison for audits
- Dashboard views provide executive-level overview of current state and security issues
- Delivers pre-built single-click PCI compliance reports (standard and customized) for audit, analysis and troubleshooting requirements

Fast Startup with Embedded Expertise

Too often, IT organizations do the bare minimum to receive a passing grade at the PCI compliance audit 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.

Instead of just collecting basic log files, Trinzic PCI Insight focuses on providing a higher level of PCI compliance visibility. A team of network experts scoured the complete PCI requirement and embedded the network-specific rules and policies within the console, so organizations can simply choose specific aspects instead of building them from scratch. The Infoblox expertise assists with building unique and customized rules and policies for each individual customer environment.

Since most IT personnel are not PCI experts, Trinzic PCI Insight provides the intelligence and automation to meet the stringent requirements, and frees up the networking team to focus on other core requirements. An Infoblox expert will work with you for several days to customize specific rules and policies based on your individual network device requirements for PCI—even for complex multi-vendor networks.

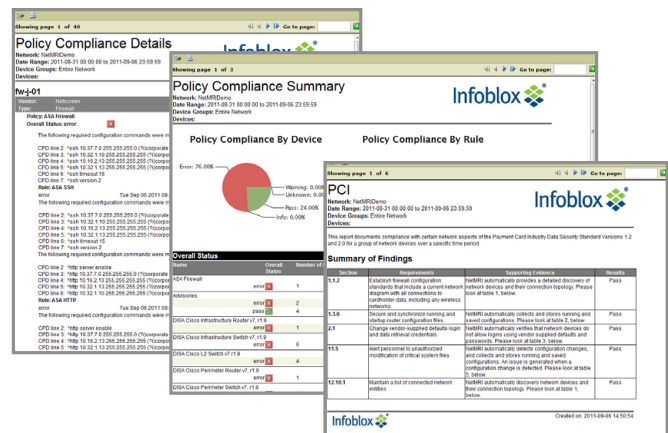
Prove Security Requirements with Change Tracking

For the PCI mandate, knowing there was a device change is not enough to satisfy auditors. You must show documentation that proves control processes have been followed. Trinzic PCI Insight automatically detects device changes, shows who made the changes and when, maintains a history of configurations and allows for fast searching on individual configuration aspects.

The actual changes detected by Trinzic PCI Insight can be compared and audited against the change management process to ensure each planned change was approved and to identify why unplanned changes occurred on the network. Within seconds, the system can drill down on individual devices or changes to see exactly what was modified and by whom.

Security and Documentation for Enhanced 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.



The screenshots display the Trinzic PCI Insight interface, including:

- Policy Compliance Details:** A detailed view of a specific policy violation, showing the device name (fw-01), version, and the specific configuration commands that were non-compliant.
- Policy Compliance Summary:** A high-level overview of the network's compliance status, including the date range of the scan and the overall score.
- Policy Compliance By Device:** A pie chart showing the distribution of compliance scores across different network devices.
- Policy Compliance By Rule:** A table showing the status of various compliance rules across the network.
- Summary of Findings:** A table listing specific findings, such as missing device configurations or unapproved changes, with their severity and remediation steps.

Pre-built reports can prove PCI compliance quickly and easily—either on demand with a single click or via scheduled results

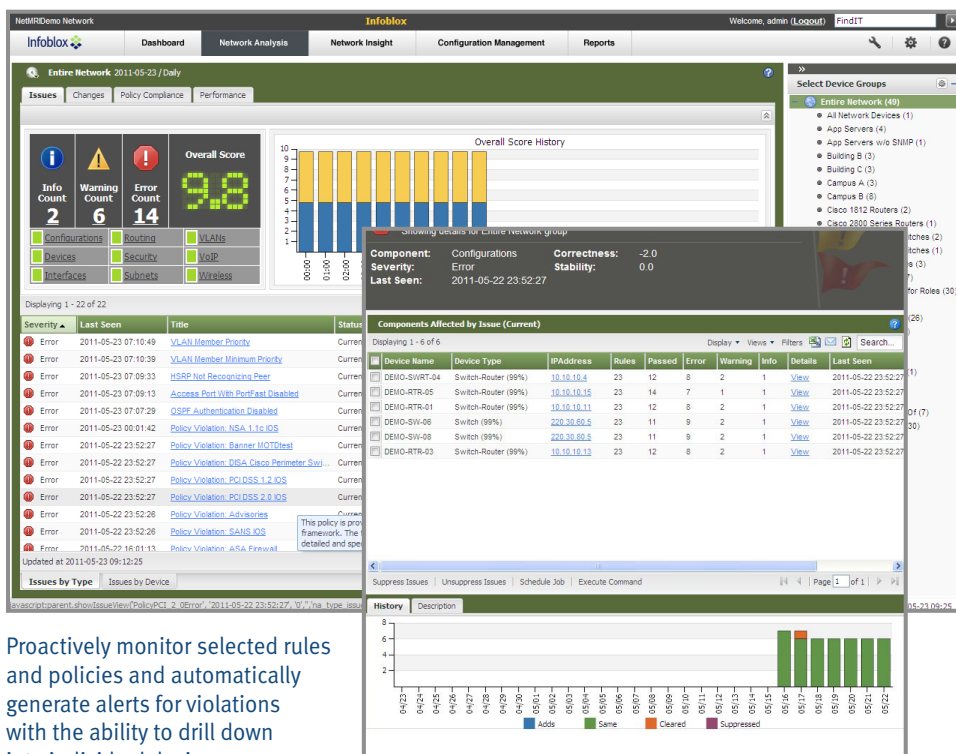
The comprehensive tracking, auditing and reporting capabilities of Trinzic PCI Insight lessen the time and manual effort needed to prove compliance success. The system automatically documents key criteria on an on-going basis, including tracking every change to any device, maintaining histories of configurations with side-by-side comparisons and recording definitions of custom rules and policies built on unique, individual aspects.

Proactive Monitoring for PCI-Specific Requirements

Assuming that a simple report or merely collecting log files will meet the needs of a PCI 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, and 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.

Unfortunately, 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.

While an audit may occur just once a year, Trinzic PCI Insight focuses on compliance monitoring continuously 24x7x365 across the network infrastructure to reduce security risks and identify inconsistencies. Once the specific PCI requirements and impacted devices are defined, the system automatically compares settings against the defined parameters.

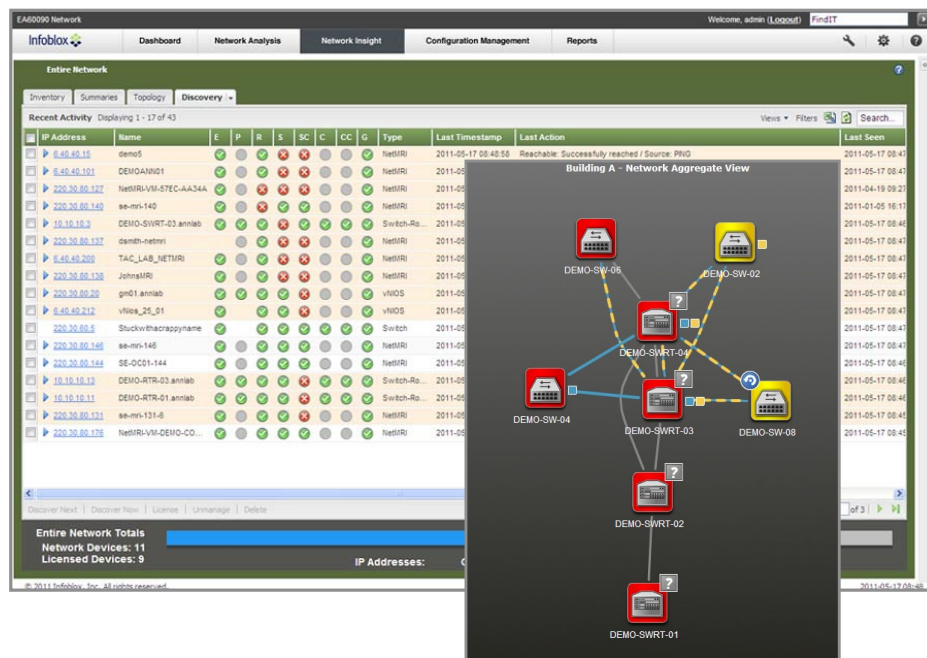


Proactively monitor selected rules and policies and automatically generate alerts for violations with the ability to drill down into individual devices

If any change to the configuration setting causes a discrepancy compared to the rule, the system automatically generates an issue to highlight the violation. The detailed violation notification identifies the impacted devices and reports the exact details of which change caused a violation to a single or multiple PCI-focused rules. Automatic reports provide the current and historical status of compliance.

Automatic Network Discovery and Reporting

Trinzic PCI Insight includes auto-discovery and inventory for multi-vendor, network infrastructure devices. The network discovery and inventory includes detailed Layer 2 physical and Layer 3 logical data, including devices, VLANs, routes, routing tables, HSRP peers, subnets, OS and models.



Auto-discover multi-vendor network devices and receive rich layer 2 physical, layer 3 logical and topology views

Trinzic PCI Insight automatically collects information in real time and continuously keeps it up to date, making it always available for critical tasks such as inventory and troubleshooting. Key views include the network connections, their dependencies and topology views of the entire infrastructure. All of this network discovery information can be automatically synced with the Trinzic IP Address Management platform.

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

In short, Trinzic PCI Insight 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.