DATASHEET

NetMRI

REDUCE RISK AND IMPROVE IT EFFICIENCY BY AUTOMATING NETWORK CONGURATION, CHANGE, AND SECURITY POLICY ENFORCEMENT

Today, up to 80 percent of network problems are caused by change—mistakes made when manually changing devices, the setting of poor configurations that cause problems later, and the undermining of critical security policies and network protection. In addition, more infrastructures are leveraging both layer-2 virtual constructs (VLANs) and layer-3 virtual networks (such as virtual routing and forwarding - VRF), which adds to day-to-day management challenges.

Infoblox NetMRI is the leading automation solution for network change, configuration, security policy, and compliance management—and is the only solution today that manages both traditional and virtualized VRF networking for multivendor environments with a single appliance.

NetMRI is a key solution for managing dynamic and complex environments such as virtualized and cloud networks, and it provides management support for IPv6 deployments. With automation for both physical and virtual devices, NetMRI gives your network the power to keep with pace with rapidly changing network components.

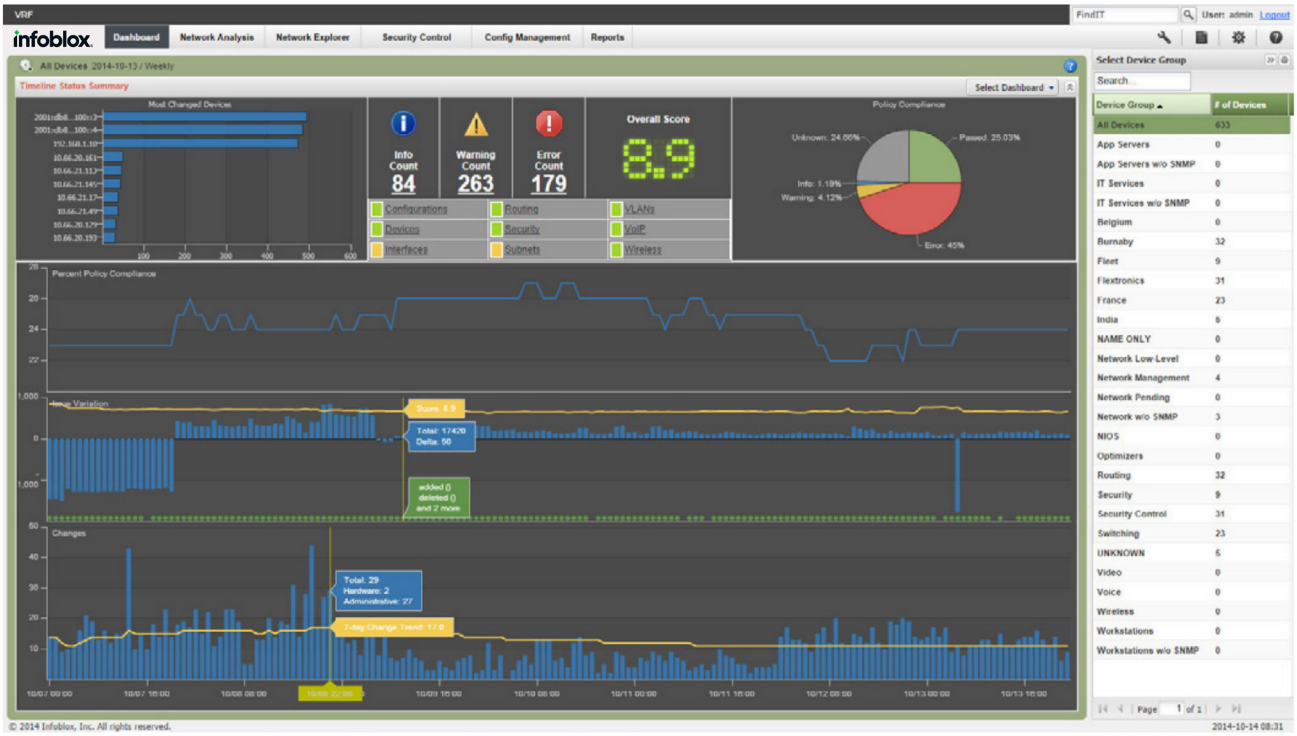
Automated Network Change and Impact Analysis

NetMRI detects and tracks all network changes—including who changed what, where and when—and the impact of changes, and it saves every historical device configuration for easy side-by-side comparisons. NetMRI's change automation engine is the most powerful and flexible solution on the market, including the ability to dynamically leverage device context and topology when analyzing the network or implementing change. This automated network solution also includes numerous embedded example jobs, scripts, and customizable templates to help you move away from manual CLI-based changes.

In addition, NetMRI adds hundreds of standards and industry best practices to help you understand and correlate the impact of changes on network health, security, and compliance. Instead of assuming a change works, NetMRI detects the change and completes an automated analysis to identify variances from correct configuration and vulnerabilities to the stability of the network. Auto-generated issues, graphical summaries, and the unique Network Scorecard highlight whether changes have a positive or negative impact on the network.

KEY CAPABILITIES

- Improve staff efficiency by leveraging automation to detect changes, enforce security policies, back up configurations, and implement new changes without tedious manual command line interface (CLI) processes
- Reduce risk by enforcing security policies to ensure consistency for internal best practices and requirements through continuous, ongoing monitoring
- Shorten time to prove internal audits or external mandates by using ongoing compliance management and reporting options
- Enable new services by supporting both traditional network environments and virtualized network constructs using technologies like VRF
- Eliminate blind spots and reduce troubleshooting time by automating complete network discovery, network construct views, and topology visualization for multivendor environments

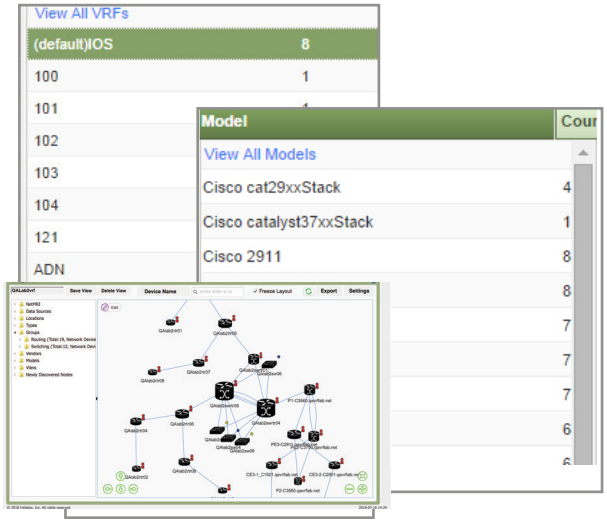


The dashboard view highlights the impact of change over time on both network health and network compliance and stability

Comprehensive View of the Network

Today, many organizations rely on manual spreadsheets and generic ping sweeps for network discovery and inventory, however, the results are often incomplete, inaccurate, missing key topological connection, or simply out of date and can waste valuable staff time in inefficient network management and prolonged troubleshooting efforts. If an unplanned device connects to the network, manual processes are not only inefficient but also add unnecessary risk. The rapid enterprise adoption of virtualized layer-3 networking, including VRFs, is causing outright gaps in network visibility and management.

NetMRI offers complete network discovery and dynamic inventory for multivendor layer-2 and layer-3 physical and virtual network elements. User-friendly analysis and graphical views provide rich information on network elements, including devices, VLANs, VRFs, routes, routing tables, Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) peers, subnets, virtual device contexts, chassis components, operatingsystems, and models.



Auto-discovers multi-vendor network devices including layer 2 physical, layer 3 logical and network topology views

NetMRI automatically collects information and continuously keeps it up to date, making it always available for key tasks such as inventory, troubleshooting, and maintenance reconciliation. It enables you to find planned and rogue devices automatically, report on variances as they happen, and highlight the network connections across the entire infrastructure.

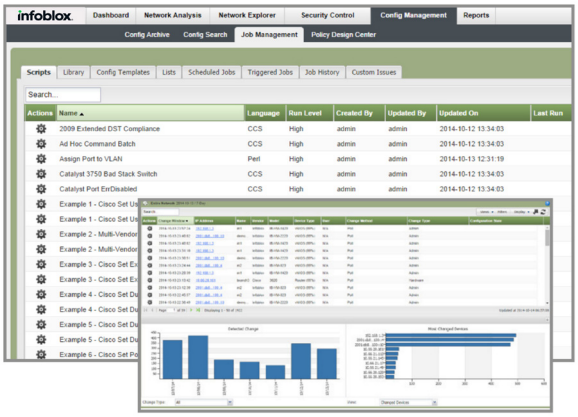
KEY FEATURES

- Automatic network discovery for multivendor network devices with multi-perspective topology views
- End-host views connected to switch ports include capacity planning visibility
- Robust and dynamic network change automation capabilities with dynamic device analysis context with topology reference and auto-lookup variables
- Built-in expert analysis of configuration and health assessments
- Support for layer-2 virtual constructs (VLANs) and layer-3 virtual networks (VRFs)
- Standard and custom rule and reporting for faster compliance analysis
- Change monitoring and tracking for who changed what, where, when and the impact of the change on the health of the network
- Collection and archiving of current and historical of network devices' configuration files with easy side-by-side comparison
- Built-in packaged scripts, such as OS upgrades, password changes and many others
- Job scheduling, approval and peer-review enforcement
- Executive-level dashboards that show correlation of change with network health and compliance, overall network score and other high-level views
- In-bound and out-bound API support for third-party solutions
- Customizable device grouping for improved ease of management

NETWORK CHANGE AUTOMATION

Even though networks are becoming ever more dynamic through technologies such as virtualization and cloud computing, many IT teams still use manual processes such as CLIs or write custom scripts to make changes. These processes require extensive internal expertise, require large time commitments, and increase the risk of human error. Moreover, manual processes simply cannot keep pace with the changes that virtual devices bring to the network.

NetMRI can automate configuration changes faster and with fewer errors by enabling you to leverage embedded tasks, customize existing templates, or create your own specific jobs using RegEx, Perl, or Python scripting. Changes can range from password updates to access control list (ACL)modifications to upgrading operating systems.

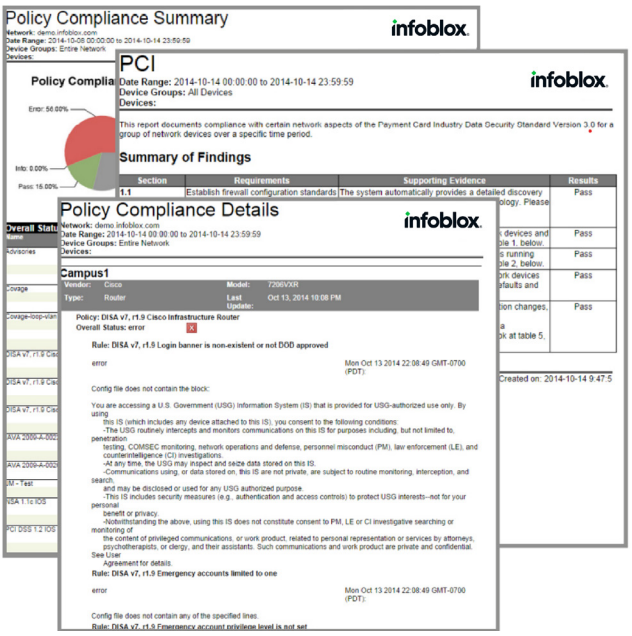


Leverage embedded jobs, modify templates for new tasks or import existing scripts to reduce the time and effort needed to make changes.

The NetMRI automation task engine can include powerful logic with or without scripting as well as dynamic device analysis context with topology reference and auto-lookup variables that allow a single job to be completed across different network locations, usage, device types, and vendors. Building a job one time and flexibly using it forever frees skilled staff from redundant tasks and eliminates common errors.

SECURITY POLICY ENFORCEMENT AND COMPLIANCE

Most IT organizations have one or both of two key standardization requirements—internal security policy enforcement and external compliance mandates. While each is critical, many organizations simply file the specifications documents in a large binder when they arrive and don't think about them again until there is a problem or an audit is scheduled. Then members of the IT staff go through the network from one device to the next, rule by rule, and attempt to find the issues, ascertain the state of the requirements, institute the newly mandated regulations, and scramble to prove that the processes have been followed. The result is chaos and—worse still—undetected security vulnerabilities in the production network.



For both internal best practices and external compliance mandates, NetMRI's continuous monitoring and single-click reporting ensures ongoing standardization

NetMRI solves the problem of security policy enforcement and network compliance by automating the process with built-in example rules and templates for common standards, including PCI, NSA, SANS, DISA, and others and also allowing you to create your own custom policies and reports. NetMRI passes each rule across every single network device 24/7, and highlights all violations immediately as detected.

Using the same dynamic and powerful automation engine, wrapped with a purposed policy design center to make custom policy creation and maintenance extremely simple, NetMRI automatically alerts you to any rule violation the moment a change is made in the network, shows you who caused the problem, and offers remediation options in real time. Instead of spending weeks chaotically compiling the information for audits, you are able to generate reports for both internal standards and external mandates (such as SOX, HIPAA, FERC, and NERC) automatically with a single click.

PROACTIVE NETWORK CONFIGURATION MANAGEMENT

NetMRI identifies and exposes lurking and intermittent problems often caused by poor configurations, which are typically very difficult and sometimes impossible to troubleshoot. Using built-in expertise and analytic techniques to identify network issues and poor configurations, NetMRI detects symptoms before they evolve into faults.

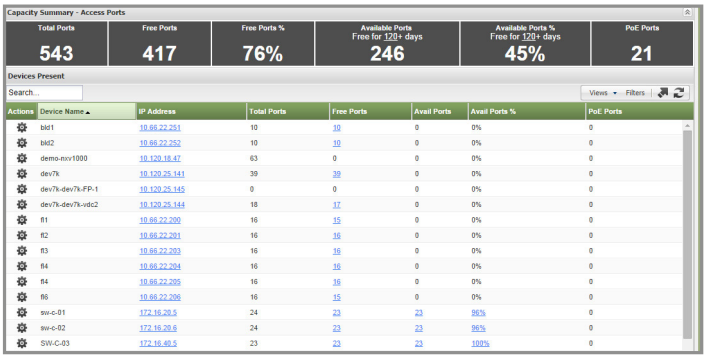
Focusing on a holistic network view and analysis instead of just individual devices, NetMRI helps you discover hidden problems and remediate them faster than any manual processes can. By uncovering potential issues early, NetMRI empowers you to take preventive action well before end users experience poor performance or application degradation.

Proactively monitor against industry best practices and compliance rules receive automated alerts when issues are detected with the ability to drill down into individual devices

SWITCH PORT MANAGEMENT VISIBILITY

As new servers or applications come on line, new switch ports are needed. Instead of reclaiming unused ports, IT teams typically go to the next available port or add another blade for more capacity. This approach increases security risks because of limited visibility and compounds expenses. With NetMRI, you can automatically track connected end devices and monitor what was connected, by whom, when, and where.

NetMRI lets you easily identify and locate rogue devices or use device forensics for troubleshooting. Since NetMRI monitors all end devices, determining used, free, and available ports is easy and simple andallows IT teams to plan capacity throughout the organization with more assurance and insight.

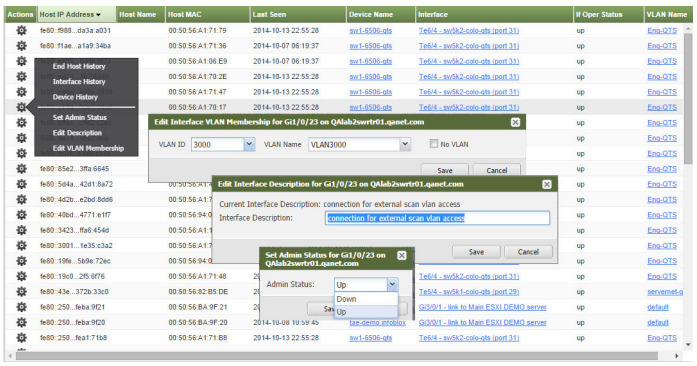


View total, free and available ports (as defined by end user tied to time being free), and filter by custom and dynamic device groupings

AUTOMATING AND SIMPLIFYING COMMON NETWORK TASKS

Common networking tasks that appear to be simple and fast still require manual effort from experienced staff and multiple handoffs that all too often lead to human error and excessive delays. Turning a port up or down, reconfiguring a VLAN, or creating a new subnet is not extremely complex, but still takes hours or days for most organizations as it goes from request to help desk to network administrator.

NetMRI leverages an intelligent GUI interface to complete common tasks quickly, effectively, and securely. Initiating tasks through a single interface, authorized staff can make common changes immediately, thereby eliminating the need for elaborate custom scripts and manual processes. The intelligence and control processes are built into the platform, which allows cross-organizational cooperation and lets more experienced staff focus on critical business initiatives instead of dealing with manual, repetitive tasks.



Simplify common network changes with the intuitive interface and powerful user-based controls

NETWORK AUTOMATION FOR EFFICIENCY, SECURITY, ANALYSIS, AND COMPLIANCE

In short, NetMRI empowers your network with automation that shortens time to deploy changes, ensures up-to-date security policy enforcement, offers full visibility in real time at all times, controls change and configuration management, gives you the insight you need for fast troubleshooting, and provides the tools for managing today's dynamic and complex environments, including the challenges of virtualization and cloud computing.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com