NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/reviews/2004/0419rev.html

Review: TrueControl from Rendition leads strong pack of configuration tools

Clear Choice Tests By Greg Goddard and Curtis Franklin, Network World, 04/19/04

CLEAR CHOICE TEST

Dilbert comic strip creator Scott Adams once said, "Managing engineers is like herding cats." The same can be said for managing the configurations of your network equipment. The network's size, performance and security have made knowing and managing the configuration of individual components more important than ever.

Buyer's Guide: Network configuration management
How we did it
Archive of Network World reviews
Subscribe to the Product Review newsletter

Network configuration management systems should:

- Correctly establish the existing configuration of the network.
- Support a multi-vendor network infrastructure.
- Let administrators make one-time changes or automated changes based on established policies.
- Cooperate with existing network management and security components.
- Provide informative data through a reasonable management console.

We tested five products: AlterPoint's DeviceAuthority Suite, Dorado Software's RedCell, Rendition Networks' TrueControl 3.0, Tripwire's Tripwire for Network Devices (TND) and Voyence's VoyenceControl. Cisco , Gold Wire Technology and Intelliden declined our invitations.

Rendition's TrueControl wins our Clear Choice Award for the best network configuration management tool. While its user interface is not the most intuitive, it provides access to a wealth of detailed information. Its search capabilities and security model are certainly the most robust of any of the products. Its mix of compliance-detection and reporting are top-notch and overcome the lack of auto-discovery, which is easily provided using an external network management system. While TrueControl came out ahead of its competition, the other products fared well.

TrueControl

TrueControl consists of a secure management engine along with syslog and Trivial FTP (TFTP) servers. The TrueControl product stores its information in a SQL database, and does not force a network administrator to choose a specific database engine; TrueControl supports mySQL, Oracle and SQL Server 2000 installations.

The system does not provide device auto-discovery because Rendition says most customers will use an existing network management system (devices can be imported using comma-separated value [CSV], formatted files). Device password rules are used to associate credentials with a device (SNMP passwords may be entered in addition to telnet and enabled passwords) and can be assigned to a specific device or multiple devices. TrueControl also can automatically configure a device to log messages to the system's syslog server.

TrueControl supports most vendor equipment, with Juniper being the one exception. (Rendition says Juniper is not on the list because its customers don't use Juniper devices in its networks. This shows that multi-vendor support in each of these products is heavily customer-driven.) The system integrates with a number of network management systems, including HP OpenView Network Node Manager, Nortel Optivity and Remedy ARS.

Rendition's system provided excellent search, audit and report capabilities - devices, modules, configurations, tasks, sessions and events all can be checked against specified criteria. TrueControl can make changes to the start-up and running configurations of network devices. Groups of equipment can be created to monitor and change configurations on a more easily managed basis. Read/write command scripts (as opposed to diagnostic scripts, which are read-only) can be created and issued to perform different tasks on devices or groups - commands sent to a particular device also can be recorded and "played back" at a later time. TrueControl can be used to deploy user and SNMP passwords, which makes a once-arduous task easy to complete.

In our testing, devices had to be manually added because of the lack of auto-discovery. TrueControl correctly identified the more mainstream Cisco devices but did not correctly identify our MSFC3 or the Supervisor Engine 720 (see "How we did it"
). The Cisco 10720s also came up unidentified. We received a new driver that added support for the MSFC3 and the Supervisor Engine 720, but were told that the Cisco 10720 is an unsupported device.

Once devices had been added to the inventory, configuration snapshots were taken. Configurations on our network devices were then changed, and TrueControl let us view differences in three ways: contextually (showing us only the portions of the configuration that had changed), using a Unix-style diff view, or viewing the full text of the current and previous configurations side by side.

TrueControl detects real-time changes via its proxy interface (which lets telnet and Secure Shell [SSH] access each device in the inventory), SNMP traps and information directed at TrueControl's syslog server. Notifications and reports can be configured (Simple Mail Transfer Protocol [SMTP] alerts are one example) and sent to administrators when changes occur.

TrueControl provides a Web and command-line interface (CLI) for users to access command functions. Although the Web-based user interface was fairly straightforward, it wasn't as intuitive as AlterPoint's DeviceAuthority. Like Voyence, Rendition always sends engineers on-site to install the product with the customer. The next release will incorporate advanced scripting support, best practices reporting, graphics capabilities and file system support.

DeviceAuthority

AlterPoint's DeviceAuthority Suite includes DeviceAuthority Server 2.0, DeviceAuthority Audit Module 2.0 and DeviceAuthority Update Module 1.0. The DeviceAuthority Server is the most important piece of the suite and provides services such as user credential management, device version control and backup, scheduling, reporting and notification to the DeviceAuthority Audit and Update Modules. It incorporates multi-vendor support (20 vendors are supported). It also provides a repository of network configuration information that can be integrated with external network management systems and updated in real time based on changes received from TACACS+, RADIUS and the syslog.

The Audit Module is aimed at network managers and provides visibility into network devices and gives an administrator hardware, software and configuration details in real time or on a scheduled basis. Reporting, change notification and comparison, and configuration recovery are the key features of this module. Five predefined reports or custom reports based on one of seven report templates can be scheduled or generated on demand in a variety of output formats (HTML, PDF, text, CSV and XML
). Notifications and reports also can be sent via SMTP on a scheduled or incident-triggered basis.

The Update Module is geared to the needs of network engineers and focuses on managing change in network components. AlterPoint lets each customer build an Integrated Network Environment that incorporates existing network tools and provides an actionable inventory that allows the execution of scripts based on this inventory. Key features of the module include the ability to schedule changes, generate scripts and perform validation of changes and search functions. Similar to TrueControl, the Update Module lets scripts be created by recording commands you issue to a device.

Inventory lists can be populated by importing device information from a file or by manually adding entries. An auto-discovery wizard is also included. In adding a device to the inventory, credentials are specified and applied to each device. Shared credentials can be applied to multiple devices for networks in which devices all share common logon information. A user can specify that DeviceAuthority not poll devices during certain times, such as maintenance windows. The Audit and Update Modules work with the Server module to provide side-by-side device configuration comparisons to assist in tracking configuration changes and errors. DeviceAuthority can act as a proxy interface for telnet and SSH access to devices in the database.

DeviceAuthority auto-discovered each device on our network and had no problem correctly identifying and backing up configurations from the more mainstream Cisco devices. It had trouble with the Cisco 10720s (at first, it incorrectly identified them as C1070s and couldn't back up their configurations), the MSFC3 on-board the Supervisor Engine 720 and the Cisco 12000s. (In both cases, these devices came up unidentified.) AlterPoint delivered new device drivers for each of these devices that fixed the aforementioned problems.

AlterPoint officials say that extended search capabilities and an option for software management will show up in the next release. While compliance reporting is supported indirectly through searching, the next release will support a more robust set of policy and compliance features.

Tripwire for Network Devices

Almost anyone with system administration experience surely will remember running Tripwire to ensure file integrity on Unix systems. TND builds on the foundation of the file integrity assurance product but goes further by incorporating support for network devices. Tripwire has vendor-specific support for products from Check Point, Cisco, Extreme Networks, Foundry Networks , HP, Nortel and others, and says it can manage up to 100,000 devices.

TND can connect to TACACS+ or RADIUS servers to confirm the identity of individuals making changes to the configuration of monitored devices. This is part of TND's configuration security focus, as it reports the who, what, where, when and why (with specifics) of any changes. The security focus continues with a very full set of notification options when configuration changes are detected. E-mail notification and SNMP traps are included, as are device configuration restore and update rollback features.

Configuration information is transmitted via TFTP back to the Tripwire server, or communications can be secured by using SSH/Subscriber Control Platform (SCP). Staying true to its name, TND can capture output from nearly any network device you can log on to - it then can run regular expressions on the corresponding output. In addition to network device configurations, TND stays true to its ancestry by letting Unix files be monitored.

The built-in log viewer is excellent for isolating errors, and TND can share information with several applications through Open Database Connectivity/Java Database Connectivity (ODBC/JDBC) and XML file connectivity. In addition, TND has direct hooks for many major network management frameworks, such as HP OpenView Network Node Manager, IBM Tivoli and Computer Associates Unicenter. A tool can run integrity checks against TND from a source outside the machine hosting TND, which assures administrators that the control system has not been compromised.

The most significant drawback was in establishing a baseline inventory - like TrueControl, TND doesn't support auto-discovery of network devices. Instead, we were forced to manually add or import a list of devices (through XML, CSV or ODBC/JDBC) from an existing inventory management system. Exporting the list of devices and configuration also can be done using those methods. Credentials can be added to a single device, or shared credentials can be established by assigning a credential to a variable and used across multiple devices.

Once devices were added to the inventory, it was easy to import their configurations. Once a configuration had been retrieved, it was marked as a baseline against which to compare subsequent configuration changes. When a change is detected, the device entry is highlighted and a contextual side-by-side comparison of the configuration can be viewed. An MD5 attribute is added to each configuration for security purposes. TND retrieved device configurations from nearly all of the Cisco devices in our network (including the MSFC3) with the exception of the Supervisor Engine 720.

While TND is a system with a lightweight footprint, it still can get the job done - as long as you carefully define the job and let TND work within a system of other network management software. It's worth noting again that TND is the only product in this review that says it supports up to 100,000 devices (find out how many devices the other products support here
). Future releases will focus on enhancing device management, reporting and conformance checking capabilities.

VoyenceControl

Voyence begins a customer installation differently than most network vendors - it typically sends the customer a proof of concept (PoC) document to gather as much information as possible about the network before shipping and installing the product. Information gathered via the PoC document includes IP ranges that will be auto-discovered and network device information that includes vendor name, operating system version, interface type and protocols supported. Customers can have Voyence provide the necessary hardware (loaded with the VoyenceControl software before coming on-site), or Voyence can install it on-site with customer-purchased hardware.

VoyenceControl runs on Red Hat Linux, making it the only Linux-based server in this review. It is part GUI, part database server and part device server. The software has a great deal of flexibility in how it gathers information from network components - SNMP, TFTP, telnet, XML, HTTP and SSH/SCP all are supported. VoyenceControl integrates its alerts and configuration files with most of the major network management platforms, including HP OpenView, Tivoli, Unicenter, Micromuse Netcool, Remedy and other network applications. Information is exchanged with these systems via XML or CSV files. Scheduled events and complex sequences can be scripted, based on a proprietary Voyence scripting language.

VoyenceControl auto-discovered and identified all the devices in our network. It correctly identified some of the more troublesome devices (specifically, Cisco's 10720s and 12000s) that other products (DeviceAuthority, RedCell and TrueControl), couldn't identify properly. Like the other products, it had trouble with the MSFC3 onboard the Supervisor Engine 720 and incorrectly identified the Supervisor portion of the 720. Voyence shipped a new driver that was able to correctly identify the MSFC3 and the Supervisor Engine 720.

Once devices were added to the inventory, configurations were retrieved and marked as baselines. VoyenceControl has superb editing support (there are four types of editing in all) - the config editor lets you edit the entire configuration; the configlet editor lets you edit portions of the config across multiple devices; the interface editor lets you make changes to an interface across multiple devices; and the termlet editor lets you send commands to the router to verify network integrity or for troubleshooting/diagnostic purposes. Wizards let you automate Cisco configuration tasks. Job control is a particularly important feature within VoyenceControl - when a change is made, the job must first be approved before it can be scheduled.

The system stands out because of its superb mix of simplicity and functionality. The GUI is easy to understand and manipulate for discovery and management, and it makes viewing information (model, operating system version and the like) gathered from your network devices easy. A feature that will be useful to those managing widely dispersed networks is VoyenceControl's location integration with MapQuest - maps generated by the software can be logical and geographical. Diagramming capabilities are included, but this is a feature best left to systems such as HP

OpenView. Future versions will incorporate Visio support, a software image library and extend integration with external network management systems.

RedCell

RedCell is an integrated suite of products that allows extensive discovery and management of network configurations. RedCell Management Center is the core of the product and provides a multi-vendor management interface to each of the other products in the suite. The RedCell NetConfig module is vendor-specific and provides comprehensive configuration management capabilities, including the ability to back up, compare, restore and synchronize device configurations. Dorado builds RedCell on Oware, its framework for developing carrier-class applications.

RedCell supports a variety of vendor equipment. It's the only product in this test with device drivers that take specific advantage of the Juniper CLI, which lets two configurations be merged or a configuration change to be scheduled (via the Juniper device, not the configuration management system). Dorado also makes versions of RedCell that work specifically with Cisco, Dell, Extreme, Foundry and Riverstone Networks equipment.

Dorado's system was easy to stop and restart, either via the command line or an icon in the system tray. The tray icon changes color to indicate system status, showing red when services are stopped, yellow when initializing and green when the system is ready to use. The software runs on Solaris and Windows server platforms and will use all the memory you can throw at it.

In our test, RedCell accurately pinged and discovered all the devices in our network. All our Cisco components were accurately picked up as Cisco devices, although some were displayed as type CiscoRouter or CiscoSwitch instead of the actual model type. (To be specific, Cisco Multilayer Switching Feature Cards [MSFC] were identified as type CiscoSwitch, whereas Cisco 10720s were identified as CiscoRouters.) The Supervisor Engine 720 was discovered and correctly identified, but the MSFC3 portion of the device was not correctly identified as a Cisco device. Dorado shipped new drivers that were able to correctly identify the Cisco 10720s, but said that the Supervisor Engine and MSFC3 were currently unsupported.

When the device type is identified correctly, RedCell builds a hierarchical view of the device, complete with line cards, interfaces and ports - you can drill down to get detailed information (this is what Dorado terms "deep discovery"), add notes to specific interfaces, and change and edit device parameters. Configurations are easily backed up, restored or synchronized. Configurations on the same device or different devices can be compared side by side, but there is no contextual way to see what changes have been made. RedCell also includes a firmware and operating system image library and diagramming capabilities. The image libraries are a nice touch, but diagramming capabilities are probably best left to systems such as HP OpenView.

While the user interface is sometimes too complex for easy understanding and management - common actions such as perusing the equipment manager required significantly more hunting through screen items and clicking options than in the other systems we tested. Make no mistake, this is a very powerful system that is chock full of features.

Conclusion

It's important to understand that these products are designed to be integrated into a larger network management and security infrastructure. They make extensive use of ports beyond those used by "normal" enterprise applications, so it is necessary to check access control lists and firewall settings to make sure the system can communicate with the devices being managed (and vice versa). Administrators who integrate these products into their infrastructures will gain substantial benefits in inventory and security control.

Click to see:

OVERALL RATING

TrueControl 3.0

4.83

Company: Rendition Networks **Cost:** $19,900 for 50 nodes. **Pros:** Very detailed permissions model; excellent search capabilities; software image management. **Cons:** No auto-discovery; user interface not as intuitive as it could be. Requirements: Solaris or Windows.

OVERALL RATING

DeviceAuthority Suite

4.68

Company: AlterPoint **Cost:** $19,950 for 100 devices. **Pros:** Great user interface; Audit and Update Modules separate functionality between engineers and management. **Cons:** No software image library; lack of compliancy reporting. Requirements: Windows (next release will incorporate support for Linux servers).

OVERALL RATING

VoyenceControl

4.65

Company: Voyence **Cost:** Minimum system price starts at $55,000; pricing derived from number of devices under management. **Pro:** Strong editing capabilities. **Con:** Currently unable to kill running jobs from the GUI. Requirements: Linux.

OVERALL RATING

Tripwire for Network Devices

4.65

Company: Tripwire **Cost:** $19,995 for 100 devices. **Pros:** Lightweight but powerful; excellent regular expression capabilities. **Con:** No auto-discovery. Requirements: Solaris or Windows.

OVERALL RATING

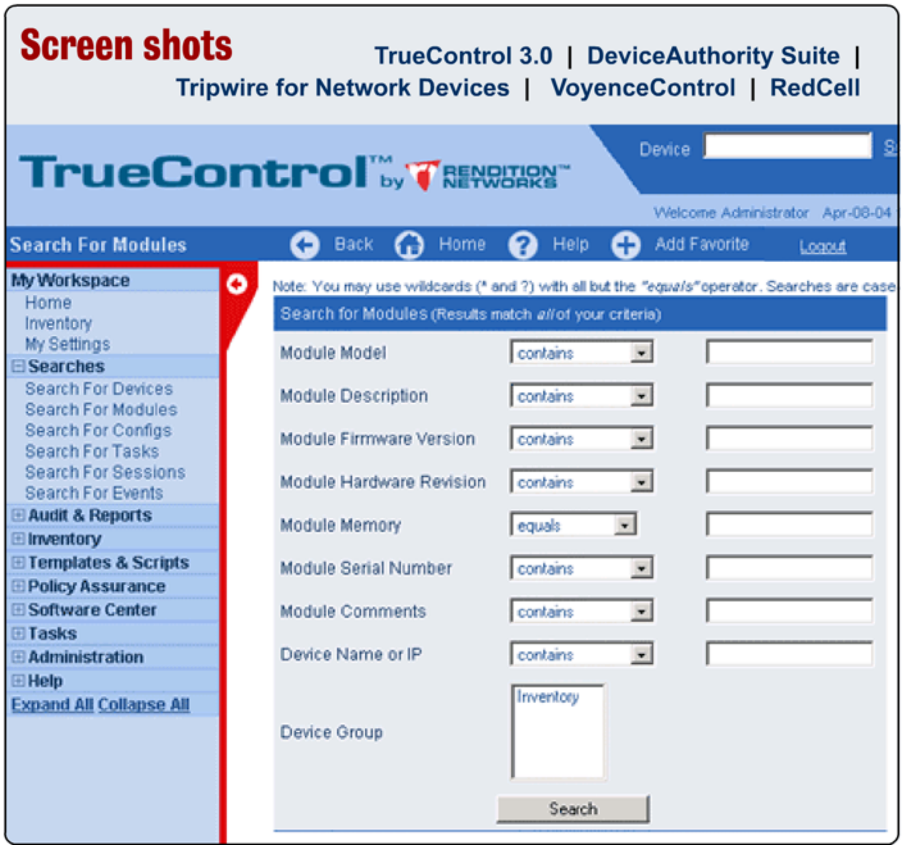
RedCell

4.4

Company: Dorado Software **Cost:** $12,000 list pricing. **Pros:** Detailed device information at the line-card, port and interface level. **Con:** User interface needs work. Requirements: Solaris or Windows.

The breakdown	Rendition	AlterPoint	Voyence	Tripwire	Dorado
Configuration control 25%	4.5	5	4.5	4.5	4
Monitoring and reporting 25%	5	4.5	4.5	4.5	4
Multi-vendor support 10%	4.5	5	5	5	5
Security features 10%	5	5	5	5	4
Installation 10%	5	5	5	5	5
Documentation 10%	5	5	5	5	5
Special features 10%	5	3	4	4	5
TOTAL SCORE	4.83	4.68	4.65	4.65	4.4

Scoring Key: 5: Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Consistently subpar



Screen shots

TrueControl 3.0 | DeviceAuthority Suite | Tripwire for Network Devices | VoyenceControl | RedCell

Note: You may use wildcards (* and ?) with all but the "*equals*" operator. Searches are case

Search for Modules (Results match *all* of your criteria)

Module Model	contains	
Module Description	contains	
Module Firmware Version	contains	
Module Hardware Revision	contains	
Module Memory	equals	
Module Serial Number	contains	
Module Comments	contains	
Device Name or IP	contains	
Device Group	Inventory	