

# CimTrak

For Network Devices

## Integrity for Your Network Infrastructure

Even the smallest alteration to a firewall, router, or switch can have tremendous impact to your business. *CimTrak for Network Devices* protects against unauthorized and destructive changes to your network infrastructure. Not only does CimTrak detect and alert you to unwanted change—whether malicious or accidental, initiated externally or internally—it takes instant corrective action returning your network back to normal state.

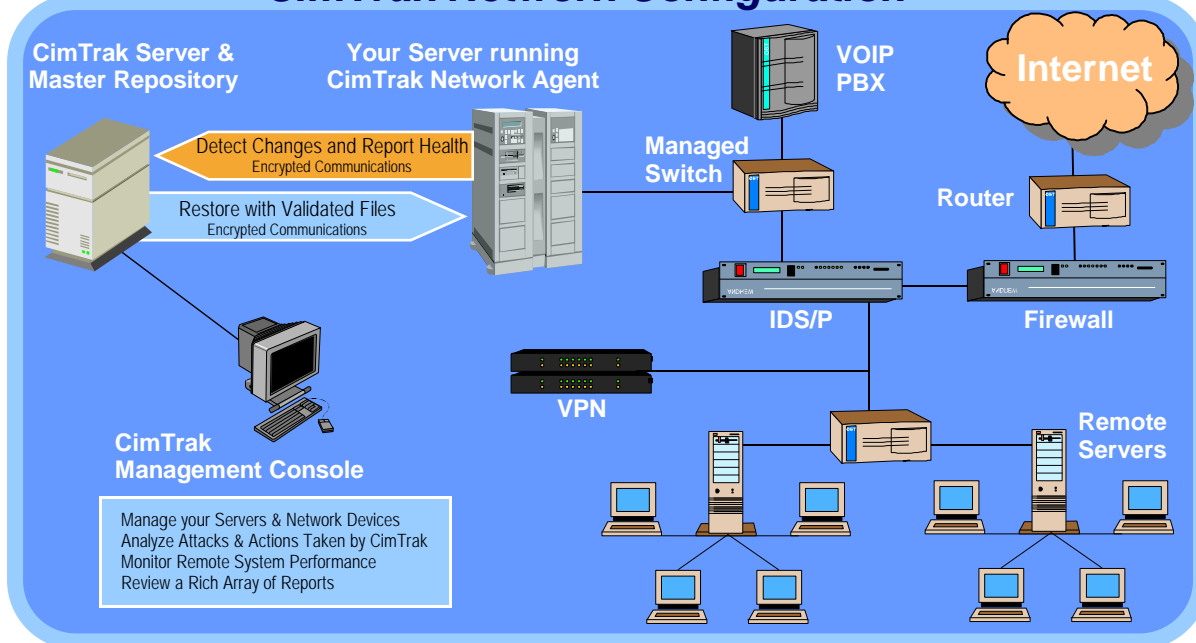
You depend upon your network to access critical business automation tools and data. CimTrak ensures maximum uptime of your network devices guaranteeing that your employees aren't blocked from essential applications, files, and data they need to do their jobs effectively. CimTrak is proactive integrity for your network infrastructure and a vital component to your companies best security practices.

While maintaining network integrity, CimTrak provides detailed reports supporting audit and compliance requirements. You decide when and who can make authorized changes and CimTrak stands guard recording activity and maintaining a revision history. If newly deployed code causes errors and disruption, CimTrak solves the trouble by allowing instant roll back to a previous good version.

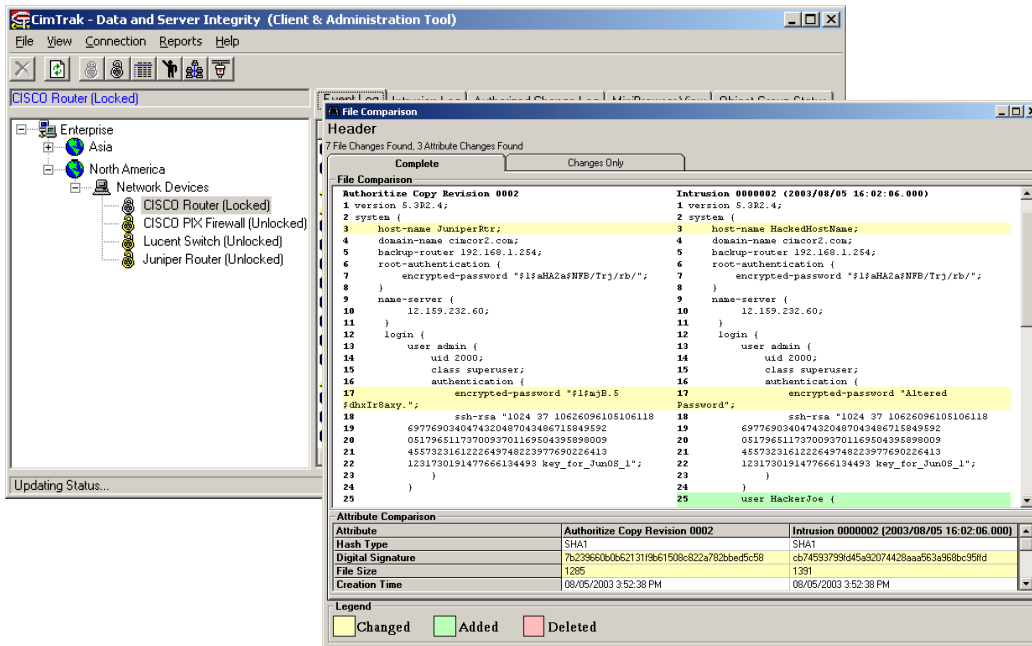
## Features

- Detects changes to configurations
- Removes unauthorized configurations
- Encrypted SSH communication to devices
- Monitors network device performance
- Supports multiple network devices
- Automatically restores modified configurations
- Automated alerts via email and text
- MD5, SHA1, and other Digital Signatures
- Configuration management and revision history
- SNMP traps for network integration

## CimTrak Network Configuration



# Know Exactly What Has Changed On Your Network Devices...and Have Instant and Automatic Correction



## System Requirements

### CimTrak Server:

- Windows NT, 2000, 2003
- Pentium II
- 128M RAM
- 60M hard drive space

### CimTrak Management Console:

- Windows 9x, NT, 2000, XP
- Pentium 133 MHz
- 64M RAM
- 35M hard drive space

### CimTrak Network Device Agent:

- Windows NT, 2000, 2003
- Linux
- Solaris

## Supported Network Devices

- CISCO Firewalls, Switches, Routers
- AVAYA Switches
- Juniper Routers
- Foundry Systems Switches, Routers
- Lucent Switches
- Others

With possibly hundreds or thousands of network devices in your enterprise, how do you know...

- when device configuration has been changed by a hacker or unauthorized person
- where the latest device configuration is located
- when a device has somehow lost its configuration
- exactly what changes have been made to your network devices over time

How long does it take to find out about these events and, more importantly, how much time does it take to recover? In many cases configuration backups are out of date or worse, don't even exist.

Organizations have come to rely on firewalls, routers, and IDS's, but what is checking the integrity of these devices? When investigating an attack, can you easily reference the state of those network devices at the time of the attack?

CimTrak provides a self-healing capability to critical network devices, which dramatically increases survivability from an attack. When configurations are unexpectedly altered, CimTrak detects the change and automatically restores them. CimTrak takes the guess work out of the equation and performs the corrective action before you even receive the alert.

With CimTrak you can finally *Stop Wondering* and have some peace of mind knowing your enterprise is armed with the best protection available.

