

CimTrak

For Servers

Instant Detection – Proactive Correction

As a critical component to your company's multi-layered security approach, CimTrak detects in real-time any unauthorized change to vital computer server elements: operating system settings, operating system files, directories, data files and file attributes. CimTrak ensures the integrity of your business-critical servers by instantly restoring them to normal or desired state – no matter what caused the unwanted change. CimTrak protects against external attacks that slip by your firewall or intrusion detection system as well as internal attacks that originate from inside your network or the occasional accident by IT personnel.

CimTrak is a unique IT Security and Integrity solution maximizing the availability of your mission critical applications and data. While firewalls and IDS/P systems are essential and sophisticated, they are dependent on known attack-signatures to be effective and they are often useless against zero-day attacks, disgruntled employees, or programmer mistakes. CimTrak is not dependent on outside intelligence of new hacker or virus methods to be 100% effective. CimTrak knows exactly what the directories, files, and data on your critical servers are suppose to look like and if there is ANY unauthorized change CimTrak detects it instantly and, just as quickly, takes corrective action.

Control and Manage Change

Change is inevitable in any dynamic IT environment; from implementing new technologies to upgrading existing systems. CimTrak has a simple but extremely effective methodology for making authorized changes. The outcome is a richly featured version manager that controls who can modify your files while reporting *who, what and when* for every change. Keep as long a revision history as necessary and instantly roll back to any previous version you require. CimTrak also maintains a complete audit trail of all changes. This powerful accountability tool will help you meet both existing and upcoming regulatory requirements.

CimTrak Configuration

Features

- Detects changes in real-time
- Automatically restores modified files
- Instantly removes unauthorized files
- Provides detailed change analysis
- Automated alerts via email and text
- Monitors remote server performance
- Live disaster recovery capability
- Version control & management
- Revision history with roll back capability
- SNMP traps for network integration
- Selectable encryption (RC4, 3DES, AES)
- MD5, SHA1 and other Digital Signatures
- Windows and Unix platforms

CimTrak Server & Master Repository

Your Critical Servers running CimTrak Agent



CimTrak Management Console

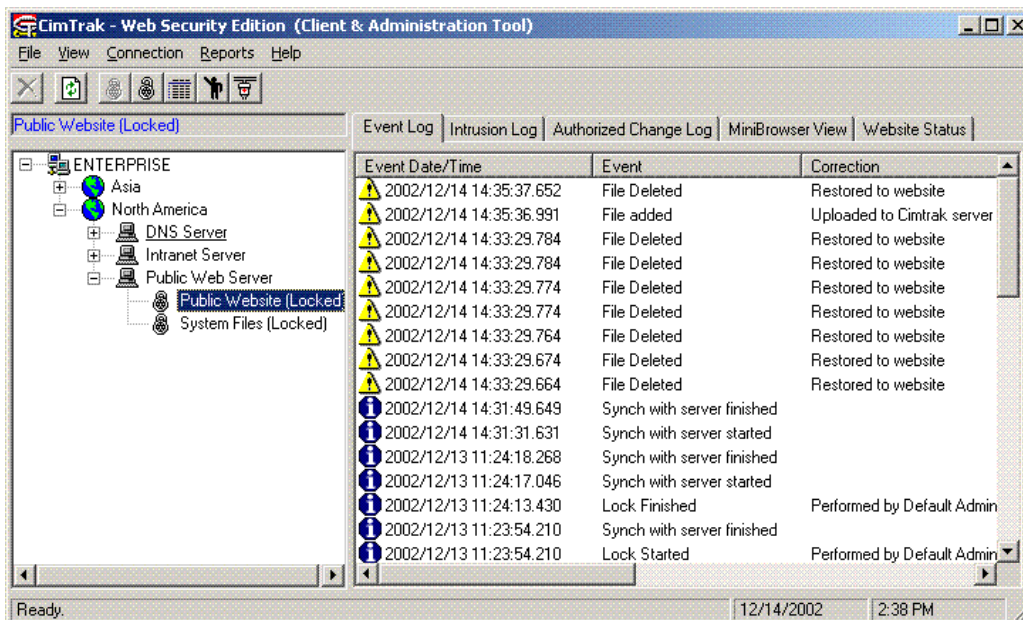
Detect Changes and Report Health
Encrypted Communications

Restore with Validated Files
Encrypted Communications



Manage your Servers & Network Devices
Analyze Attacks & Actions Taken by CimTrak
Monitor Remote System Performance
Review a Rich Array of Reports

Know Exactly What Has Changed On Your Critical Servers...In Real Time



System Requirements

CimTrak Server:

- Windows NT, 2000, XP, 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 Agent:

- Windows NT, 2000, XP, 2003
- Linux
- Solaris
- NetBSD
- Other Unix Variants Available

Potential Applications

- DNS Servers
- Database Servers
- Critical Business Logic
- Web Servers
- Application Servers
- File Servers
- Custom Software

With thousands of critical files on your corporate servers, how do you know...

- when a file has been changed by a hacker or other unauthorized person
- when a new virus or worm is causing havoc
- when a Trojan horse and other malicious code is introduced to your system

With CimTrak you can finally *Stop Wondering* and have some peace of mind knowing your servers are armed with the best real time protection available.

| Feature | Standard | Pro |
|---|----------|-----|
| Real Time Detection | ✓ | ✓ |
| Automated alerts via email and text messaging | ✓ | ✓ |
| RC4 Encryption and MD5 Digital Signatures | ✓ | ✓ |
| Configurable Encryption and Digital Signatures (Including FIPS 140-2) | | ✓ |
| Real Time Correction of Unauthorized Changes | | ✓ |
| Advanced Change Management for Roll Back and Disaster Recovery | | ✓ |
| Complete Revision History and Audit Trail for Compliance Requirements | | ✓ |

