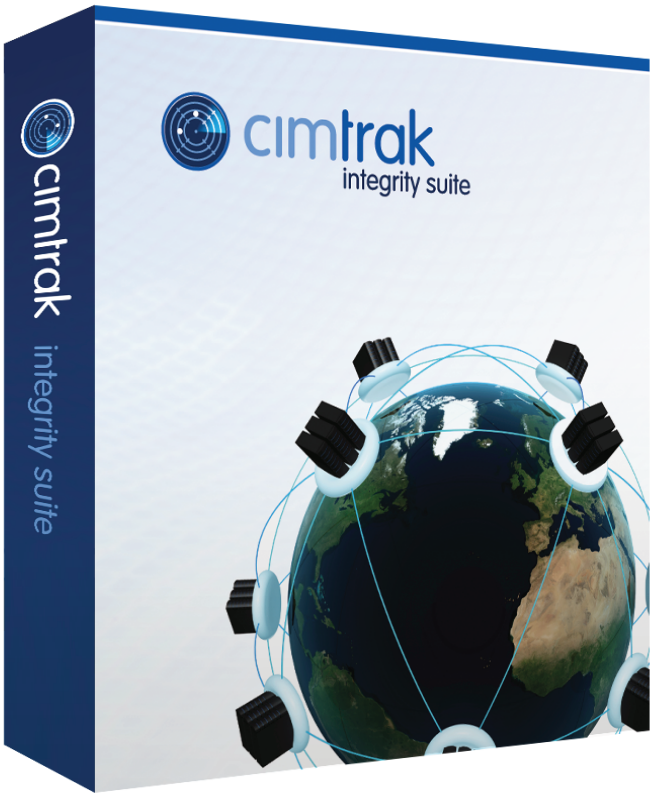


CimTrak Integrity Suite

When your enterprise or agency needs to ensure the integrity and compliance of your IT infrastructure, turn to CimTrak. CimTrak is a leader in helping organizations and government agencies worldwide maintain the security, integrity, compliance and availability of their critical IT assets. With a proven record of industry leading innovations, CimTrak consistently brings new innovations to market.

CimTrak:

- Provides deep insight of a system's state
- Increases situational awareness
- Decreases incident response time
- Improves security posture
- Reduces remediation costs
- Supports continuous monitoring initiatives
- Aids compliance efforts

DETECT All changes across your IT environment

With coverage for your servers, network devices, critical workstations, point of sale systems, and more, CimTrak has your infrastructure covered. CimTrak provides one easy to configure and manage solution which functions as a single point of collection and reporting on changes that can affect operations, security and compliance.

NOTIFY Receive instant notification that a change has occurred

CimTrak gives you deep situational awareness into exactly what is happening in your IT environment. By being instantly aware of changes, you stay on top of, and are constantly aware of the state of your critical IT infrastructure.

REMEDIATE Take corrective action as necessary or let CimTrak do it automatically

Being able to react quickly to changes that can cripple your systems and bring your business to a halt is of utmost importance. The deep visibility and instant notification that CimTrak provides allows you to do just that. Plus, CimTrak gives you're the ability to take instant, automatic remediation that allows you to self-heal systems to their pre-change state.

REPORT Provide documentation on changes across your agency or enterprise

CimTrak gives you a full array of reports both on changes in your IT environment and actions taken within CimTrak. This complete reporting allows change tracking and verification, audit and compliance reports, as well as executive level reports. CimTrak also easily exports collected change information to various reporting and alerting tools present in many enterprises and government agencies including security information and event managers (SIEM).

cimtrak
detecting the unknown

CIMCOR
Phone 219 736 4400 | Toll Free 877 424 6267
www.cimcor.com | info@cimcor.com

How CimTrak Works

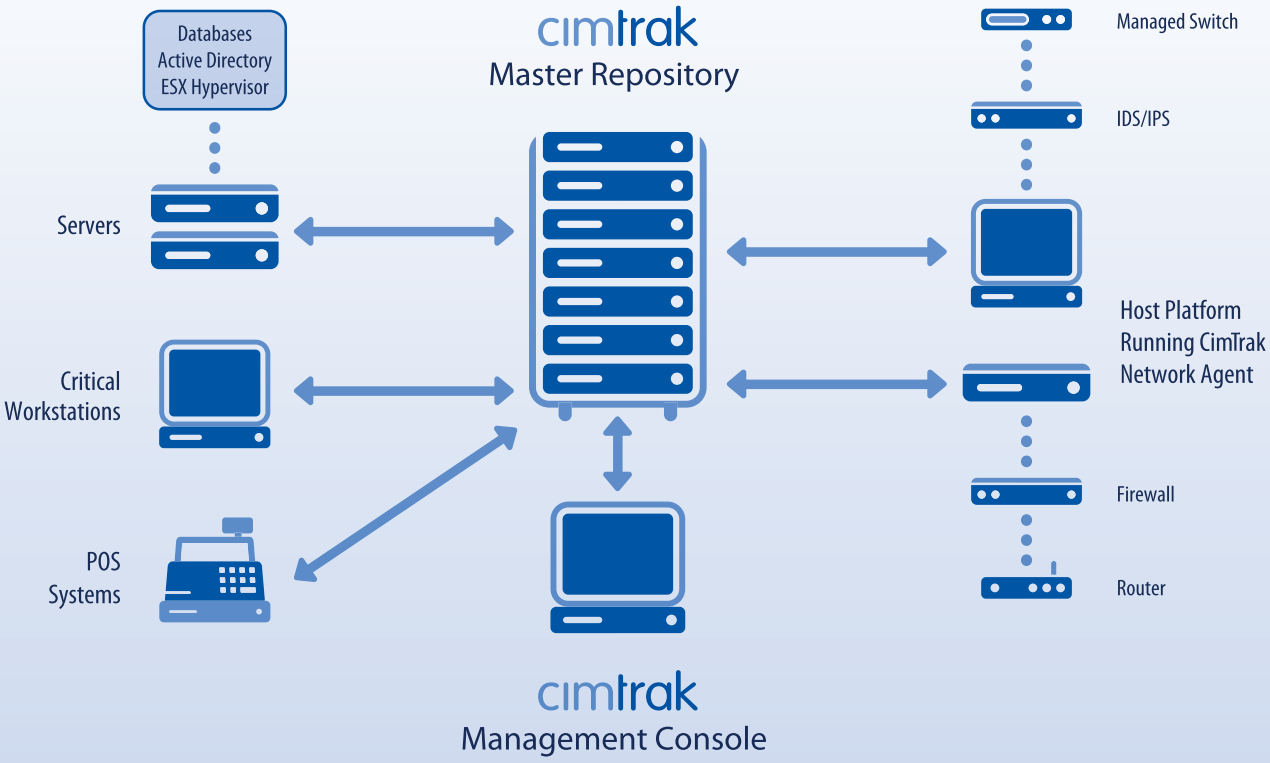
CimTrak works by detecting additions, deletions, and modifications of files and configurations. Upon initial configuration, CimTrak takes a "snapshot" of the files and configurations that you need to monitor. It creates a cryptographic hash of the files and configurations and stores them securely in the CimTrak Master Repository. This establishes a known, good baseline. From there, CimTrak receives data from the various CimTrak agents and modules. When the data received does not match the cryptographic hash of a particular file or configuration, a change has occurred and CimTrak takes action. Depending on how CimTrak is configured, alerts via SNMP, STMP and syslog are sent out and instant or manual change remediation can take place.

CimTrak Master Repository: Securely stores files and configurations and performs comparisons to detect changes.

CimTrak Agents/Modules: Available for a variety of components and applications within the IT environment and sends files or configurations back to the CimTrak master repository for comparison

CimTrak Management Console: Centralized platform to manage and configure the CimTrak solution.

cimtrak
Integrity Suite Architecture



CimTrak Modes of Operation

Log CimTrak logs all changes to watched systems and applications, which can be analyzed and reported on.

Update Baseline CimTrak stores an incremental "snapshot" of a file or configuration as changes occur. This feature allows for changes between snapshots to be analyzed and previous baselines to be redeployed at any time.

Restore CimTrak has the ability to instantaneously take action to reverse a change upon detection. This effectively allows a system to "self-heal." CimTrak is the only integrity tool with this powerful feature.

It is important to note that CimTrak allows a great deal of flexibility when using various modes. You are not locked into using only one mode for each file or configuration. Instead, you can choose what mode CimTrak should run in depending on the type of change. For instance, you may want to simply log modifications to a particular file, but may want the file to restore if it is deleted.

CimTrak is Security

Built with the stringent needs of government customers in mind, CimTrak has been certified to Common Criteria EAL Level 4 +, the highest government certification for a commercially available software product. In addition, the CimTrak cryptographic module has been certified to meet the U.S. Federal Information Processing Standard (FIPS) 140-2 Level 2. CimTrak is also certified and listed on the U.S. Department of Defense Unified Capabilities Approved Products List, an elite list of IT security products.

Further, your critical data is secure. All communications between CimTrak components are fully encrypted and the CimTrak Master Repository stores your files and configurations in both a compressed and encrypted form. No other integrity and compliance tool can match these stringent safeguards to protect your information. Whether you're a government agency or a commercial enterprise, you can rest assured that CimTrak is secure!

cimtrak
Integrity Suite

File System, Registry, Services, Drivers, Local Security Policies Local Users & Groups, Installed Software, Unauthorized File Access

Database Schema and Structure

Critical configurations of ESX server application and host platform

- CimTrak For Servers
- CimTrak For Critical Workstations
- CimTrak For Point of Sale (POS)
- CimTrak For Network Devices
- CimTrak For Databases
- CimTrak For Active Directory/LDAP
- CimTrak PCI Compliance Module
- CimTrak VMware ESX Module
- CimTrak Flex Module

Device Startup and Runtime Configurations

Domain User and Group Privileges and Policies

Assess compliance to configuration baselines based on PCI-DSS 2.0

Custom script or command line execution with output capture

CimTrak for Servers

CimTrak for Servers monitors your files and applications running on both physical and virtual servers. With the ability to detect changes in real-time on most operating systems, CimTrak gives your instant detection and alerting capabilities. Additionally, CimTrak monitors security policies, system configurations, drivers, installed software, services, users, and groups. Further, CimTrak monitors the health of your IT infrastructure including CPU utilization, memory, disk space and network utilization and alerts you to any issues immediately. CimTrak can even detect when a file is opened. CimTrak offers you the most complete integrity for your IT environment without minimal impact to your CPU cycles or network bandwith.

CimTrak for Critical Workstations

CimTrak for Critical Workstations watches workstations that have specific functionalities or run certain critical applications. These exist in many environments including hospitality, restaurant, energy and manufacturing. CimTrak for Critical Workstations allows you to monitor all of the same items as CimTrak for Servers, but is scaled to meet the needs of a workstation, including using minimal system and network resources.

CimTrak for Point of Sale (POS) Systems

CimTrak for Point of Sale Systems adds coverage for point of sale systems in your PCI environment. As an integral part of your payment card infrastructure, protecting these systems helps ensure the security of your customer's payment card data. CimTrak gives you the most complete coverage to protect PCI environments, keeping them secure and in a constant state of integrity.

CimTrak for Network Devices

CimTrak for Network Devices detects and alerts you to configuration changes on your critical network devices including routers, switches and firewalls. Since these devices are often the gateway into your network, changes, whether malicious or accidental can be extremely problematic. CimTrak can even instantly restore changed configurations on newer SNMPv3 network devices.

CimTrak for Databases

CimTrak for Databases adds another layer of security to your IT environment. With support for major platforms including Oracle, IBM, and Microsoft, CimTrak ensures your critical database configurations, user roles and permissions, as well as access settings, don't deviate from their known, trusted state. By utilizing CimTrak for Servers, you can further monitor your database application for changes that can take down your business critical databases.

CimTrak for Active Directory/LDAP

CimTrak for Active Directory/LDAP monitors your directory services for deviations to objects, attributes, and schema. Large environments can suffer from alterations that fly under the radar. Unexpected changes may be limited to a single entity, such as an addition of a new account, or can have broader impact, such as a denial of service, due to the inherent hierarchical design. CimTrak provides the awareness needed to quickly detect and alert when such deviations occur.

CimTrak PCI Module

The CimTrak PCI Module assesses configurations settings on servers, workstations, and point of sale systems within your PCI environment. By checking your configurations against established standards, you can determine if a system is in compliance with PCI-DSS requirements. CimTrak provides a detailed report of non-compliant configurations so you can quickly bring the system into a compliant state. Then, CimTrak ensures that any subsequent configuration changes are detected and alerts you instantly. This ensures that your critical PCI configurations are continually in a compliant and secure state.

CimTrak VMware ESX Module

The CimTrak ESX Module monitors critical core VMware ESX/ESXi configurations such as user/host access permissions, active directory realms, network settings, integrated 3rd. party tools, and advanced user configurations. Because VMware ESX hypervisors generally run many virtual machines, unexpected or malicious changes can quickly cripple an organization's IT infrastructure. The CimTrak ESX module gives you the ability to proactively protect critical ESX applications and ensure the security and continuity of your operations.

Supported Platforms: CimTrak for Servers and Critical Workstations

- Windows: 2000, 2003, XP, 2008, Vista, 7
- Linux: CentOS, Fedora, Gentoo, Red Hat, SUSE, Ubuntu
- HP-UX: Itanium, PA-RISC
- AIX
- Windows Server: 2000, 2003, 2008
- Sun Solaris: x86, SPARC
- Mac: Intel, Power PC

Windows Parameters Monitored

- File additions, deletions, and modifications
- Attributes: compressed, hidden, offline, read only, archive, reparse point
- Creation time
- File opened/read
- Group security information
- Local security policy
- Services
- DACL information
- File Size
- Installed software
- Modify time
- User groups
- Drivers
- File type
- Local groups
- Registry (keys and values)

UNIX Parameters Monitored

- File additions, deletions, and modifications
- Attributes: read only, archive
- File Size
- Modify time
- Access Control List
- Creation time
- File type
- User and Group ID

System Health Monitoring

- CPU
- Disk Space
- Memory
- Network Utilization

Supported Platforms: CimTrak for Network Devices

- Cisco
- HP ProCurve
- Juniper
- Linksys
- Netgear
- NetScreen
- SonicWALL
- 3Com

CimTrak can support almost any device type or manufacturer

Supported Platforms: CimTrak for Databases

- Oracle
- IBM DB2
- Microsoft SQL Server
- MySQL

Parameters Monitored

- Default Rules
- Groups
- Stored Procedures
- User defined data types
- Full text indexes
- Index definitions
- Table definitions
- Users
- Functions
- Roles
- Triggers
- Views

Supported Hypervisors: CimTrak VMware ESX Module

- VMware ESX, ESXi

cimtrak
detecting the unknown

CIMCOR

Phone 219 736 4400 | Toll Free 877 424 6267
www.cimcor.com | info@cimcor.com