CIMCOR

CimTrak Technical Summary

When your enterprise or agency needs to ensure the integrity and compliance of your IT infrastructure, turn to CimTrak.

As the leader in Integrity Verification and Assurance, CimTrak helps 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 ideas and solutions to market.

Why CimTrak?

Relied upon by organizations of all sizes including numerous Fortune 500 companies, CimTrak offers users a full-featured file integrity monitoring solution that is simple to install, configure and manage, all without the budget busting price tag and complexity associated with other File Integrity Management (FIM) solutions. CimTrak's unique next-generation FIM technology means that you get more done in less time, saving your organization both time and money. Backed by a world-class support team, CimTrak users are assured their systems are always in a state of constant integrity.

Detect changes across your IT environment

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

Instant notification when a change occurs

CimTrak gives you deep situational awareness into exactly what is happening in your IT environment. Being instantly aware of changes and understanding if they are known, expected and wanted, allows you to stay on top of and constantly aware of the state of your critical IT infrastructure. This continuous insight helps prevent integrity drift.

Corrective action automatically

Being able to react quickly to changes that can cripple your systems and bring your business to a halt is of utmost importance. CimTrak gives the ability to take immediate, automatic action to remediate to a known, trusted, and operational state or simply prevent changes from happening completely.

FEATURES

- » Deep Insight of a System's State
- » Increased Situational Awareness
- » Decreased Incident Response Time
- » Improved Security Posture
- » Reduced Remediation Costs
- » Support of Continuous Monitoring
- » Aids in Compliance Efforts
- » Easy to Use
- » Simple to Configure
- » Dynamic Threat Feed Response
- » Auto Restore Capability

Identify good changes from bad

When an unexpected change occurs, it's critical to be able to discern if the file that changed is good or bad. This difficult, and often frustrating analysis task, is now quick and simple to perform with the CimTrak Trusted File Registry™, which is a massive white-list database, that features robust integration with ITSM workflow technologies and industry malware analysis engines.

Provide documentation on all changes

CimTrak gives a full array of reports both on changes in your IT environment and actions taken. This complete reporting allows change tracking and verification, audit and compliance reports, as well as providing necessary 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 management tools (SIEMs).

How CimTrak Works

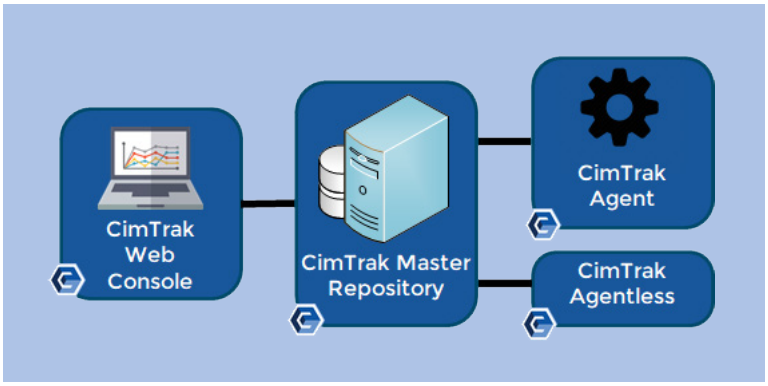
CimTrak works by detecting additions, deletions, modifications, and reads of files and configurations. Upon initial configuration, CimTrak takes a "snapshot" of the files and configurations that you need to monitor. It creates a cryptographic hash of the files and configurations and stores them securely 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 SMTP and syslog are sent out, and instant or manual change remediation can take place if desired.

CimTrak Master Repository

Securely stores files and configurations and performs comparisons to detect changes. If changes are unwanted, a manual or automated roll-back and remediation to a previous known and trusted state can occur.

CimTrak Agents/Modules

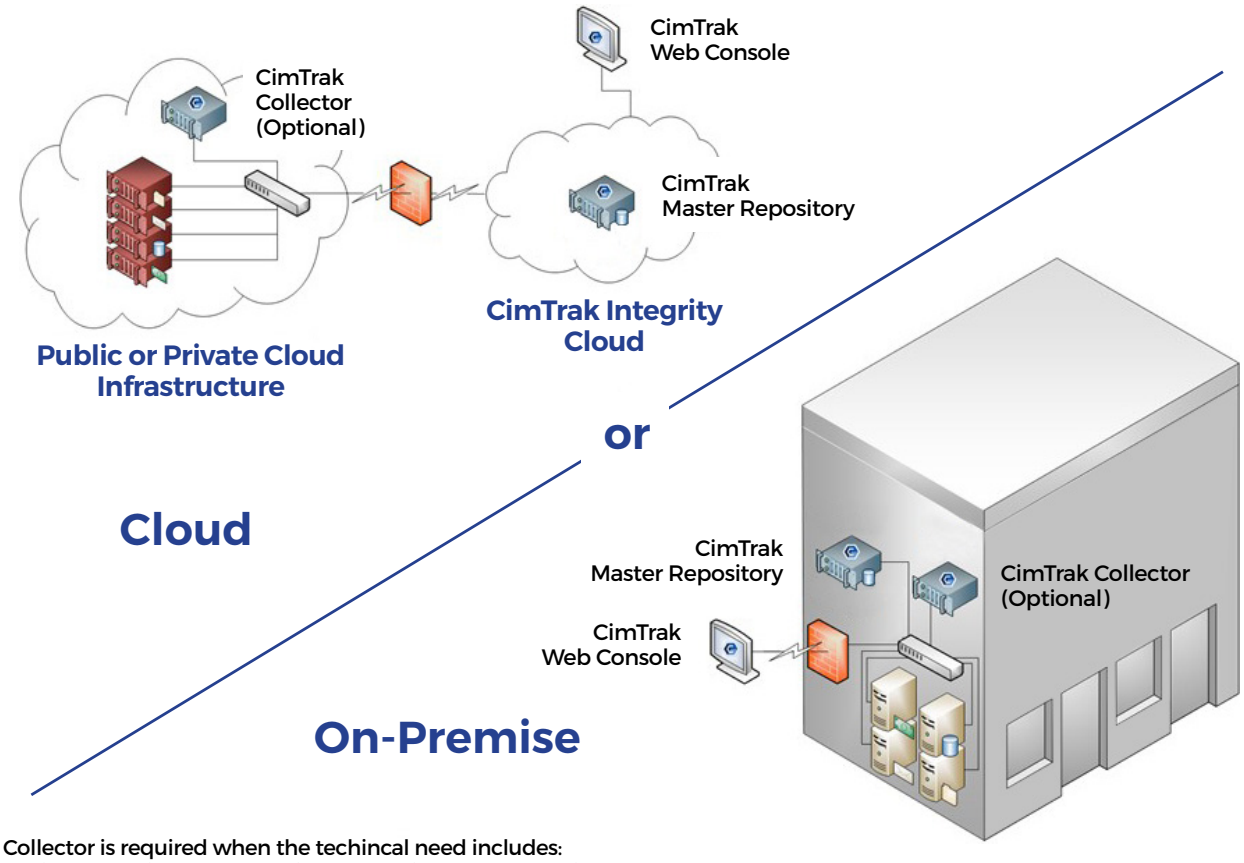
Available for a variety of components and applications within the IT environment where files or configurations are sent back to the CimTrak Master Repository for comparison. CimTrak offers agent and agentless solutions depending upon your specific business and technical requirement(s).



CimTrak Management Console

The CimTrak Management Console supports multiple users as well as multi-tenant views and is the management interface for the creation of all CimTrak policies, procedures and reports.

CimTrak Available On-Premise or in the Cloud



*CimTrak Collector is required when the techincal need includes: network devices, container orchestration, hyper visors and compliance

CimTrak Modes of Operation

Log
CimTrak logs all changes to target 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.

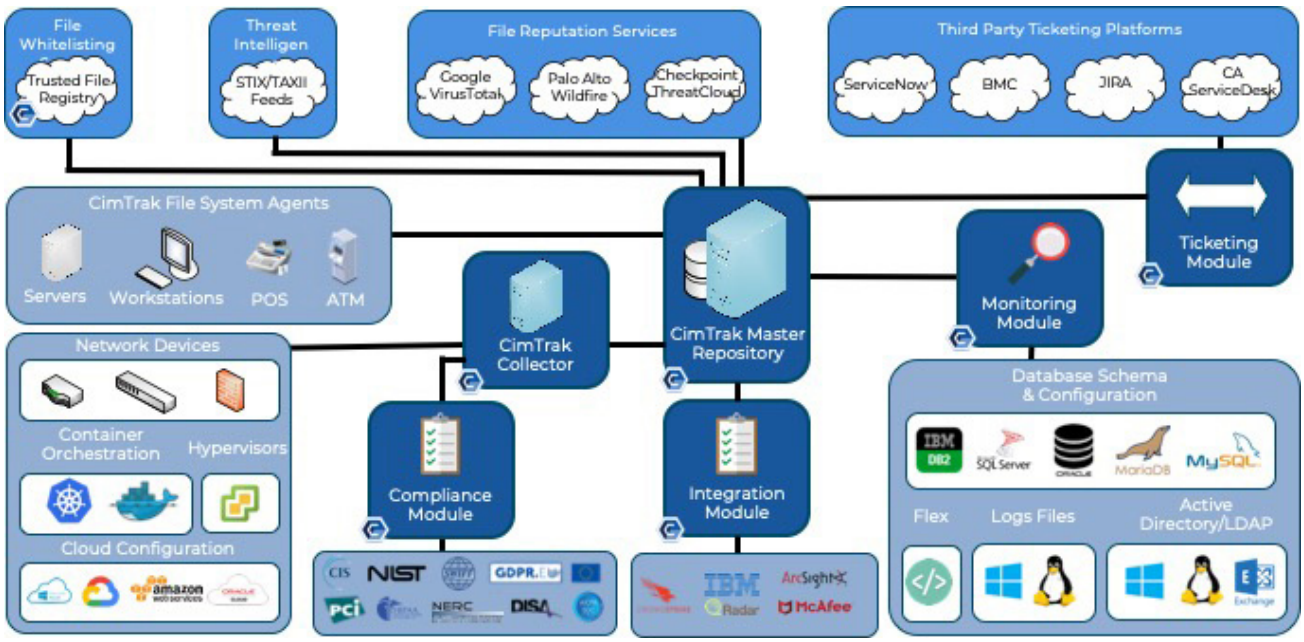
Restore
CimTrak has the ability to instantaneously take action to reverse a change upon detection. This effectively allows a system to "self-heal". CimTrak is the only integrity tool with this powerful feature.

Deny Rights
Denies any access to a file. Since CimTrak runs as the local system account, it does not matter what privilege access a user has, access to a file will not be allowed, thus denying reads, changes, deletions or additions. No other integrity tool provides this advanced capability.

It is important to note that CimTrak allows a great deal of flexibility when using these 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 and requirements 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 Products

CIMTRAK CORE

CimTrak for Servers

CimTrak for Servers monitors your files and applications running on both physical, virtual or cloud-based 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, Windows Registry, system configurations, drivers, installed software, services, users, and groups. CimTrak can even detect when a file is opened. CimTrak offers you the most complete integrity solution for your IT environment with minimal impact to your CPU cycles or network bandwidth.

CimTrak for Workstations/Desktops

CimTrak for Workstations/Desktops watches workstations and desktops that have specific functionalities or run certain critical applications. These exist in many environments including hospitality, restaurant, energy and manufacturing. CimTrak for Workstations/Desktops allows you to monitor all of the same items as CimTrak for Servers but is scaled to meet the needs of a smaller machine, including consideration for 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 payment card 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 payment card environments, keeping them secure and in a constant state of trust and assurance that they have not been compromised.

CimTrak for ATMs

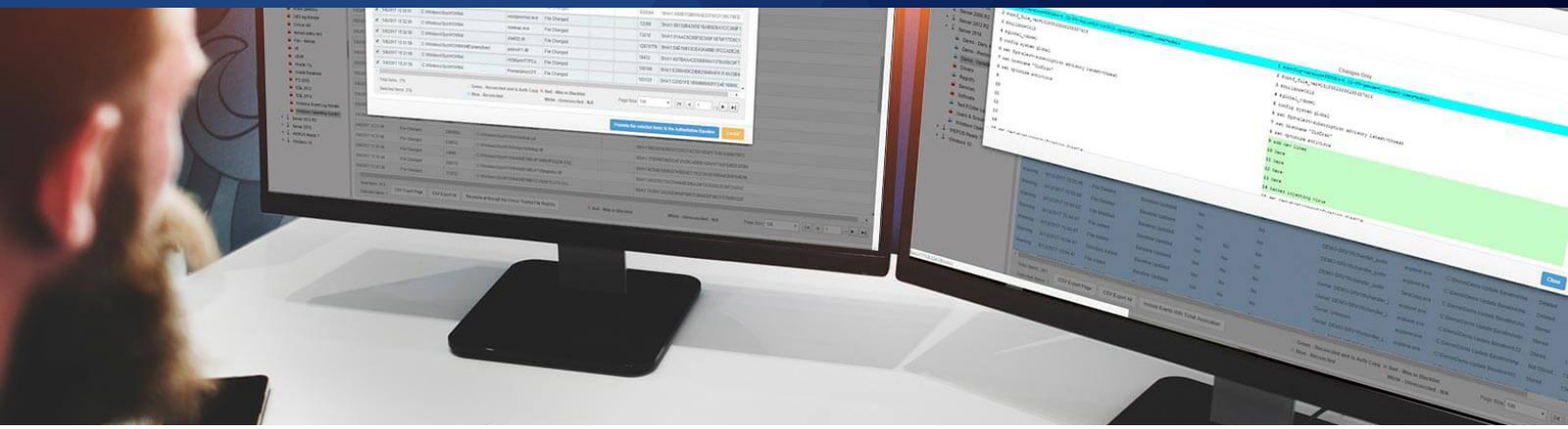
CimTrak for ATMs provides a light agent to help monitor and protect Automatic Teller Machines (ATMs). ATMs can be difficult to update and patch in the same cycle as other IT assets. CimTrak provides an additional level of threat mitigation by helping to ensure the integrity of the ATM machines while providing an audit trail of both authorized and unauthorized changes. CimTrak integrates with all leading SIEM solutions including HP ArcSight, IBM QRadar, McAfee Enterprise Security Manager, RSA Security Analytics, and Splunk, all without any complicated configuration or setup.

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. Coupling this with CimTrak for Servers, you can further monitor your database environment for changes that can take down your business-critical databases.



CIMTRAK FOR DIRECTORY SERVICES

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, alert, and restore when such deviations occur.

CIMTRAK FOR HYPERVISORS

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

CIMTRAK FOR CLOUD & CONTAINERS

CimTrak for Containers

CimTrak for Containers (Docker/Kubernetes) helps administrators understand when container configurations have changed, new containers have been instantiated, virtual network configurations have changed, storage settings have been modified, and more. CimTrak for Containers provides extensive visibility into the settings that drive your container deployments.

CimTrak for Cloud

CimTrak for Cloud provides an easy way to know when new cloud servers are provisioned, or changes have occurred to server configuration settings, virtual firewall rules, virtual network settings, and much more. CimTrak for Cloud supports Google Compute Engine, Azure, and Amazon AWS. CimTrak for Cloud Infrastructures allows you to monitor all of the changes that occur to your cloud infrastructure configuration outside of your guest operating system.

CIMTRAK THREAT INTELLIGENCE

CimTrak integrates with STIX 1.0/2.0 and TAXII Thread Feeds to provide an additional layer of security intelligence. This constant stream of threat data provides CimTrak with additional data to provide even greater insight into your organization. As the hashes of new threats download from the threat feed, CimTrak automatically updates its blacklist with the malware/threat hashes. The result is that anytime there is a change, CimTrak verifies that those changes or new files are not on the blacklist. Furthermore, as new threats are identified, CimTrak will proactively review all monitored systems, to ensure that the newly identified threats are not already on current systems.

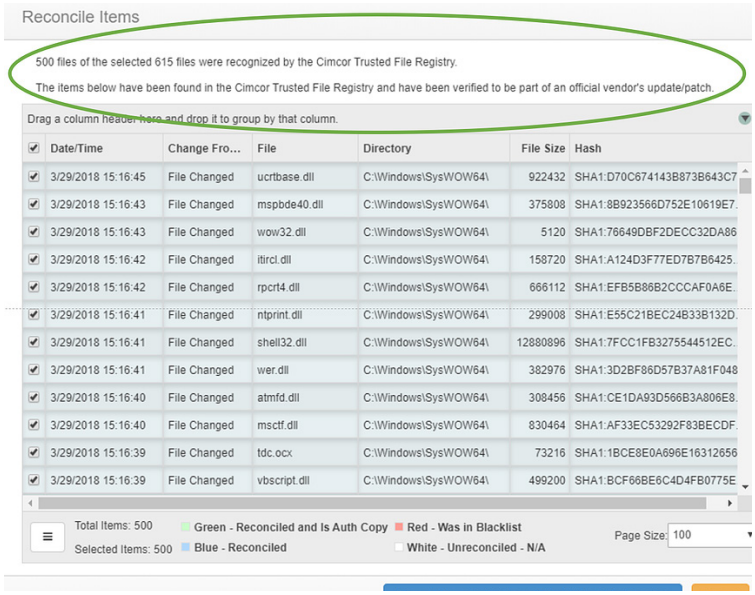
CIMTRAK INTEGRITY CLOUD

Embrace the future with an easy to manage, comprehensive, and cost-effective System Integrity Assurance & Verification solution delivered on-demand. CimTrak is available as-a-service with the same feature/functionality as if deployed on-premise but leveraging the value and efficiencies of cloud computing. Cimcor has partnered with a leading cloud provider to simplify the burden of deployment, operation, and maintenance making this option extremely cost effective with immediate time-to-value.

CIMTRAK ESSENTIALS

CimTrak Trusted File Registry™

A key component of CimTrak's technology is the patent-pending, CimTrak Trusted File Registry™. This highly innovative solution virtually eliminates false positives caused by known, good vendor patches and updates such as those for Windows and Red Hat Linux. By automatically promoting patches and updates to the authoritative baseline, changes that are truly of importance rise to the top, greatly decreasing time spent investigating good changes and maximizing efforts to identify and remediate unknown, unwanted and unauthorized changes.



CimTrak Trusted File Registry™

CimTrak Ticketing Module

Differentiating between known "good" change and unknown changes that should be investigated is a critical part of maximizing the time you and your team spend responding to change events. CimTrak provides users with the only file integrity monitoring system to offer a fully integrated change ticketing system that is bi-directional where information and commands can be executed through automation to ensure only approved changes are allowed. This provides organizations of all sizes with the ability to minimize change noise, reconciliate expected changes with observed changes, and highlight unwanted, unauthorized and unexpected activity resulting from circumvented processes or malicious activity. CimTrak integrates with all leading ITSM solutions including ServiceNow, BMC, Atlassian Jira, and more.

CimTrak Compliance Module

The CimTrak Compliance Module assesses the configurations settings on servers, workstations, network devices, point of sale systems and other IT devices within your environment. By checking your configurations against established regulatory standards, you can determine if systems are compliant with any number of requirements including SOX, PCI, HIPAA, FFIEC, FISMA, NERC-CIP, SWIFT, GDPR, CDM, CJIS, and many others. CimTrak then provides a detailed report of non-compliant systems and provides necessary instructions on how to quickly correct and bring into a compliant state. Then, CimTrak will detect and ensure that any subsequent configuration changes are highlighted and alerts are immediately delivered to the specified personnel. This ensures that your systems are continually compliant and secure.

CimTrak Integration Module

If your organization utilizes other security tools such as SIEM technology, integrating data collected by CimTrak is easy. CimTrak provides vital insight and information from servers and other endpoints. CimTrak's file integrity monitoring (FIM) and configuration monitoring provides timely intelligence that enhances the analysis, correlation, and situational awareness needed to mitigate attacks and detect other anomalies. By detecting binary, configuration or other actual changes in system state, CimTrak complements network traffic analysis solutions, which may miss events that are out of band. CimTrak's logs and audit trails broaden a SIEM's compliance reporting by increasing the coverage of security controls that can be monitored. CimTrak's unprecedented capture of forensic assisting details also add vital information for a SIEM's data mining engine. The combination of these two technologies can help streamline compliance reporting, improve your security posture and fulfill CIS Critical Controls #5 and #6. CimTrak integrates with all leading SIEM solutions including HP ArcSight, IBM QRadar, McAfee Enterprise Security Manager, RSA Security Analytics, and Splunk, all without any complicated configuration or setup.

CimTrak Flex Module

The CimTrak Flex Module allows monitoring the output of applications and scripts that write to a command line such as ipconfig/ifconifg network configurations, firewall settings, Security Enhanced Linux configuration status and more. The CimTrak Flex Module is also useful for monitoring physical hardware status such as SAN health, as well as component and resource availability. Further, it allows for rapid development of monitoring tools for custom applications within the IT environment. By detecting any change to script/application output, deviations can be instantly alerted on and responded to. The ability to automatically monitor and analyze custom script or command line execution streamlines IT operations, which allows personnel to focus on more pressing issues.

CimTrak File Reputation Services

When files change, CimTrak can integrate with Virus Total, Palo Alto Wildfire, or Checkpoint's Threat API, to perform real-time file and malware analysis of file changes. Combined with the CimTrak Trusted File Registry™, it is now easier than ever to identify if a file is malicious or not. This data can be used to update the master CimTrak Blacklist dynamically, and automatically check for the existence of those malicious files on other systems which are monitored by CimTrak.

MANAGE YOUR ENVIRONMENT AT SCALE: CIMTRAK FEATURES

CimTrak Integrated Dashboard

CimTrak's interactive, graphical dashboard allows users to see the status of their environment at a glance. The dashboard is completely customizable with various graphs and charts to choose from. Each CimTrak user can customize their dashboard to offer a unique view of the entire IT environment or just the systems they are responsible for.

Scale Easily With Consolidated Management View

Several CimTrak Master repositories can be bound together, via CimTrak Clustering, to scale CimTrak horizontally. This technique allows CimTrak to meet the needs of even the largest infrastructures. Once clustered, CimTrak automatically enables the consolidated view feature, which presents the user with a robust "Single Pane of Glass" for managing configurations, creating policies, and reviewing security-related events.

CimTrak Reports

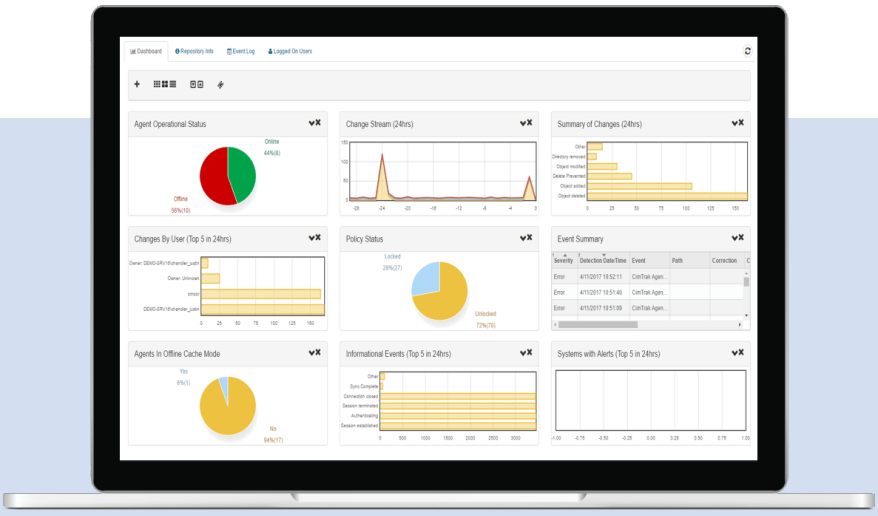
Being able to provide change information reports is essential for proving compliance for IT audits, verifying planned changes occurred, and keeping all IT operations personnel informed. In the enterprise, individuals and functional areas often need different reports with varying levels of detail. With an integrated reporting engine, CimTrak offers a wide variety of reports available in .pdf, .html, and .csv format. Users can even customize reports to display information unique to their organization. From comprehensive change detail reports to high-level overview reports, which are ideal for management presentations, CimTrak gives you the level of granularity your organization needs.

CimTrak Change Reconciliation Workflow

Managing change enterprise-wide is much more efficient with CimTrak. The CimTrak Change Reconciliation workflow provides a seamless, easy to use methodology for managing change from the initial identification of the change, investigation, and triage of the change, for assigning the task to an engineer, final remediation and confirmation. The CimTrak Change Reconciliation Workflow provides a robust toolset for analyzing the nature of changes, performing malware analysis, verifying if the change is a verified component of an OS patch and a simple way to document what was done and by whom.

Test CimTrak in your environment today with a Free Trial

»TRY CIMTRAK NOW



Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.