CIMCOR

Technical Summary

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

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 Integrity Management solutions. CimTrak's unique next-generation File Integrity Management (FIM) technology enables you to accomplish more in less time, saving your organization both time and money. Backed by a world-class support team, CimTrak users are assured that their systems are always in a state of constant integrity.

Cimcor's CimTrak platform is the trusted solution for real-time integrity verification and assurance. Organizations rely on CimTrak to protect critical infrastructure, maintain compliance, and ensure the security and availability of their most important IT assets.

CORE BENEFITS

- » Detect malicious or unauthorized changes instantly
- » Full visibility to understand exactly what changed and why
- » Faster, more accurate incident response
- » Strengthen security posture and reduce risk
- » Lower operational and remediation costs
- » Maintain continuous compliance
- » Simple deployment, easy to use, and straightforward to maintain
- » Real-time, dynamic threat intelligence
- » Auto-restore capability to return systems to a trusted baseline

FULL VISIBILITY OF YOUR IT ENVIRONMENT

With coverage for servers, workstations, VMs, network devices, hypervisors/ESXi, containers, cloud configurations, databases, directory services, and more, CimTrak has your infrastructure covered. CimTrak serves as a single point of collection and reporting for enterprise-wide changes that can negatively impact operations, security, and compliance.

INSTANT IDENTIFICATION OF UNAUTHORIZED CHANGE

CimTrak gives you deep situational awareness of exactly what is happening in your IT environment. Continuously managing and understanding if the change(s) are known, expected, and authorized allows you to immediately pinpoint malicious or circumvented changes. This enables organizations to detect zero-day breaches and problems related to human error, ensuring a trusted operating environment and preventing integrity drift.

AUTOMATIC CORRECTIVE ACTION

It is imperative to be able to react quickly to changes that can cripple your systems and bring your business to a halt. CimTrak enables organizations to take immediate and corrective action to remediate unwanted and unexpected activity, returning to a last known and trusted state of operation. Furthermore, CimTrak can also prevent changes from happening completely, regardless of your administrative privilege.

IRREFUTABLE FILE INTEGRITY

When an unexpected change occurs, it's critical to be able to discern if the file that changed is intentional or unintentional. This difficult and often frustrating task is now quick and simple to perform with CimTrak's Trusted File Registry™ (TFR). TFR is the world's largest allowlist database, providing additional information and integrity assurance that the current or changing files are known and trusted, as determined by the software manufacturer.

COMPREHENSIVE REPORTING

CimTrak gives a full array of reports on changes in your IT environment, the process used to determine whether the change is expected or unexpected, as well as the actions taken. This comprehensive reporting enables change tracking and verification, as well as audit and compliance reports, all necessary for executive-level decision-making. CimTrak easily exports collected change information to various reporting and alerting tools present in many enterprises and government agencies, including Security Information and Event Management (SIEMs), Security Orchestration, Automation, and Response (SOARs), and IT Service Management (ITSM) platforms.

HOW CIMTRAK WORKS

CimTrak works by detecting additions, deletions, and modifications to files, configurations, and/or settings. Upon initial configuration, CimTrak takes a "snapshot" of what needs to be monitored and stores it securely in the CimTrak Master Repository.

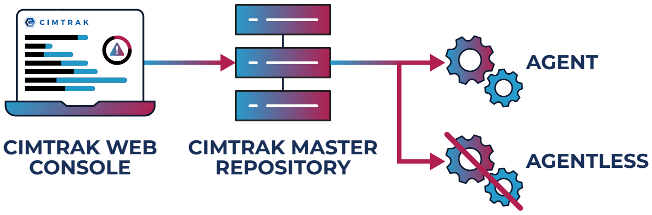
This establishes a known, trusted baseline. From there, CimTrak receives data from the various CimTrak agents and modules. When the data received does not match the cryptographic hash of a particular file, configuration, or setting, a change has occurred, and CimTrak takes action. Depending on how CimTrak is configured, alerts via SMTP and Syslog are sent out, and instant or manual change remediation efforts 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 previously known and trusted state can occur.

CIMTRAK AGENTS/MODULES

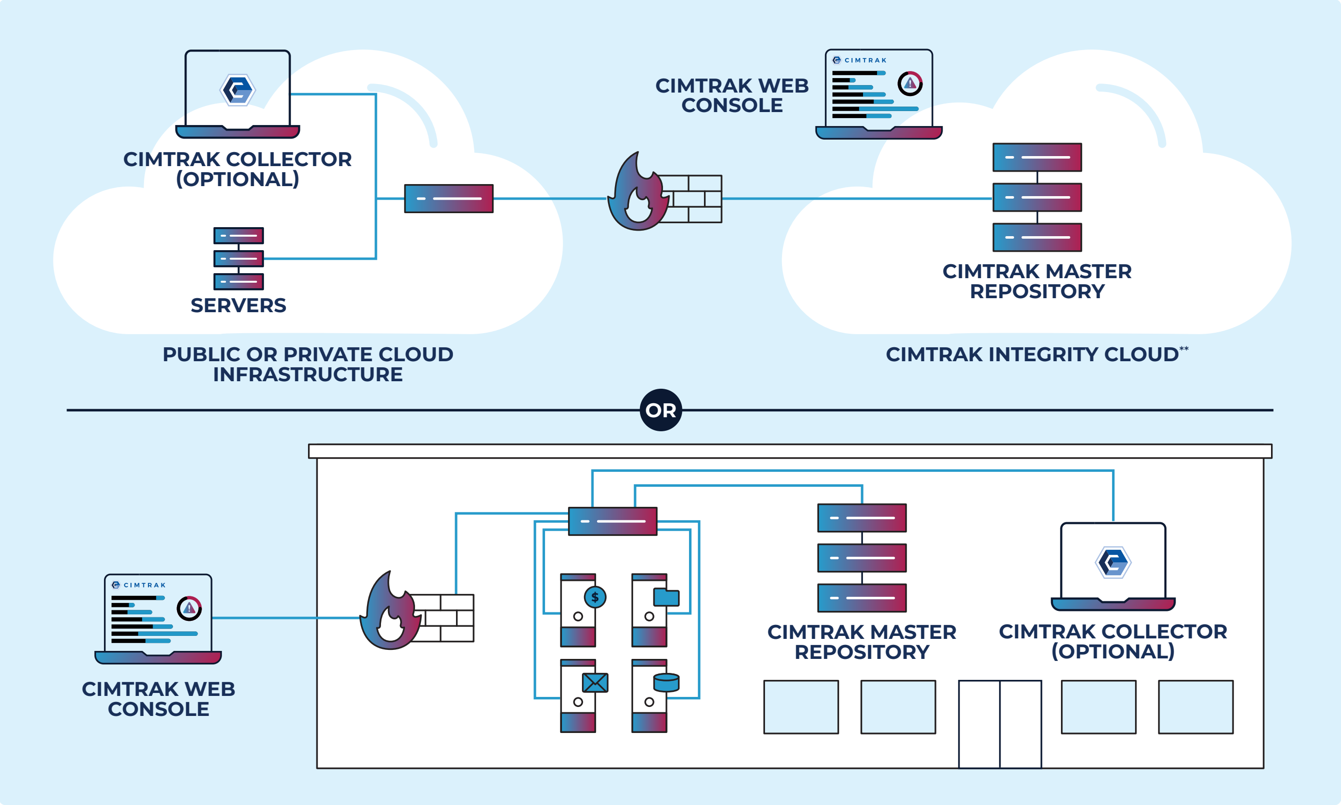
CimTrak supports a variety of systems, devices, and applications within the IT environment. CimTrak offers agent-based and agentless solutions, depending on your specific business and technical requirements.

CIMTRAK MANAGEMENT CONSOLE

The CimTrak Management Console supports multiple users and offers multi-tenant views, serving as the management interface for creating all CimTrak policies, procedures, and reports.

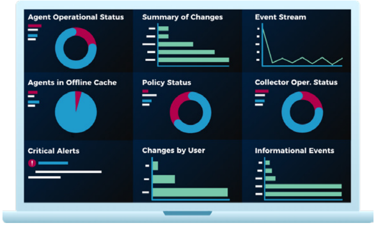


CIMTRAK AVAILABLE ON-PREMISE OR IN THE CLOUD


CIMTRAK COLLECTOR (OPTIONAL)
SERVERS
PUBLIC OR PRIVATE CLOUD INFRASTRUCTURE
CIMTRAK WEB CONSOLE
CIMTRAK MASTER REPOSITORY
CIMTRAK INTEGRITY CLOUD**
OR
CIMTRAK WEB CONSOLE
CIMTRAK MASTER REPOSITORY
CIMTRAK COLLECTOR (OPTIONAL)

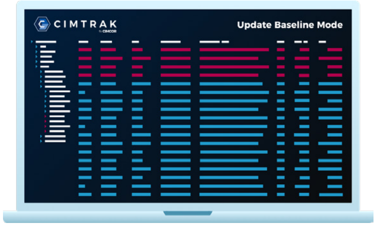
*CimTrak Collector is required when the technical need includes network devices, container orchestration, hypervisors, and compliance.
**Check for availability

CIMTRAK MODES OF OPERATION



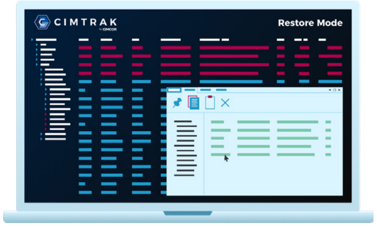
LOG MODE

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



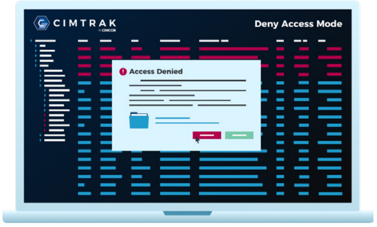
UPDATE BASELINE MODE

CimTrak stores an incremental “snapshot” of files, configurations, and settings. As changes occur, they can be immediately viewed for comparison with pre- and post-activities. This feature enables the analysis of changes between snapshots and the redeployment of previous baselines at any time.



RESTORE MODE

CimTrak can automate restoration by instantaneously taking action to reverse a change, whether it was something added, modified, or deleted. This effectively allows a system to “self-heal” and enable a resilient infrastructure. CimTrak is the only integrity management tool with this powerful feature.



DENY RIGHTS MODE

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 management tool provides this advanced capability.

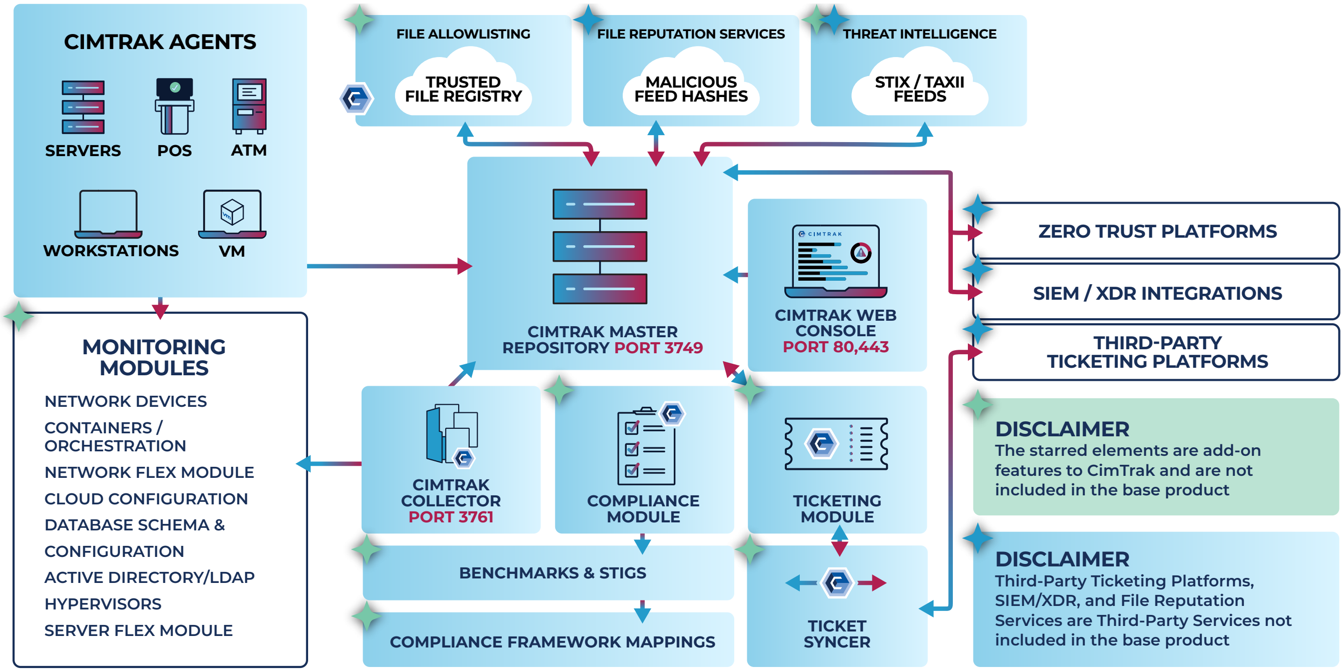
It is essential to note that CimTrak offers considerable flexibility when utilizing these various modes. You are not locked into using only one mode for each file or configuration. Instead, you can choose what mode CimTrak should run in depending on the type of change. For instance, you may want to simply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

SECURITY YOU CAN TRUST

CimTrak has been built with the stringent needs and requirements of government customers in mind. Having previously achieved Common Criteria EAL 4+ certification, CimTrak successfully met rigorous independent testing to verify compliance with internationally recognized security standards. While CimTrak no longer maintains active certification due to the significant cost of renewal, the same trusted design and security principles continue to guide our development—ensuring suitability for deployment in federal, defense, and critical infrastructure environments.

Additionally, 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.

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!



DISCLAIMER
The starred elements are add-on features to CimTrak and are not included in the base product

DISCLAIMER
Third-Party Ticketing Platforms, SIEM/XDR, and File Reputation Services are Third-Party Services not included in the base product

CIMTRAK INTEGRITY PLATFORM

CIMTRAK FOR SERVERS

CimTrak for Servers monitors your files and applications running on physical, virtual, or cloud-based servers. With the ability to detect changes in real-time on most operating systems, CimTrak gives you instant detection and alerting capabilities. Additionally, CimTrak monitors security policies, Windows Registry, system configurations, drivers, installed software, ports, services, users, and groups. CimTrak can even detect when a file is opened. CimTrak offers the most comprehensive integrity solution for your IT environment, with minimal impact on CPU cycles or network bandwidth. 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 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 systems in your payment card environment. As an integral part of your payment card infrastructure, protecting these systems helps ensure the security of your customers' payment card data. CimTrak provides the most comprehensive coverage to protect payment card environments, ensuring they remain secure and in a state of trust and assurance that they have not been compromised

CIMTRAK FOR ATMS

CimTrak for ATMs provides a light agent to 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 ATMs while providing an audit trail of both authorized and unauthorized changes.

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 Cisco IOS.

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 that your critical database configurations, user roles, and permissions, as well as access settings, remain in 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 go unnoticed. Unexpected changes may be limited to a single entity, such as the addition of a new account, or can have a broader impact, such as a denial-of-service attack, 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, including user/host access permissions, Active Directory realms, network settings, integrated third-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 provides the ability to proactively protect critical ESXi and Hyper-V applications, ensuring the security and continuity of your operations.

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 enables you to monitor all changes to your cloud infrastructure configuration outside of your guest operating system.

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 been modified, storage settings have been updated, and more. CimTrak for Containers provides extensive visibility into the settings that drive your container deployments.

CIMTRAK FLEX MODULE

The CimTrak Flex Module enables monitoring of the output from applications and scripts that write to a command line, such as ipconfig/ifconfig network configurations, firewall settings, Security-Enhanced Linux configuration status, and more. The CimTrak Flex Module is also useful for monitoring hardware status, including SAN health, as well as component and resource availability. Furthermore, it enables the 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 to and responded to. The ability to automatically monitor and analyze custom script or command-line execution streamlines IT operations, allowing personnel to focus on more pressing issues.

CIMTRAK FOR SCADA DEVICES

CimTrak provides the necessary detective controls that help you meet several key NERC-CIP requirements, covering a broad range of critical servers, SCADA devices, workstations, and network devices typically found in manufacturing, energy facilities, and other industrial environments. The same processes and change detection capabilities are used for baselining, comparing, and restoring unwanted change(s) to SCADA devices to ensure operational integrity.

THREAT INTELLIGENCE

CIS BENCHMARKS AND DISA STIGS

CimTrak utilizes CIS Benchmarks and DISA STIGs as trusted sources for hardening systems, devices, operating systems, applications, and other components. These benchmarks are used to establish a referenceable root of trust. As CimTrak identifies changes to these configuration settings (benchmarks), it can immediately alert to the changes and take corrective action to remediate them.

STIX/TAXII

CimTrak integrates and digests STIX and TAXII Threat 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 are downloaded from various threat feeds, CimTrak automatically updates its denylist/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 denylist/blacklist. Furthermore, as new threats are identified, CimTrak will proactively review all monitored systems to ensure that the newly identified threats are not already present in current systems or have existed previously.

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 the most critical and important rise to the top, greatly decreasing time spent investigating authorized changes and maximizing efforts to identify and remediate unknown, unwanted, and unauthorized changes.

CIMTRAK FILE REPUTATION SERVICES

When files change, CimTrak's integration with Virus Total, Palo Alto Wildfire, or Checkpoint's Threat API performs 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 dynamically and automatically update the master CimTrak denylist/blacklist, and to check for the existence of those malicious files on or previously on systems that CimTrak monitors.

CIMTRAK WORKFLOW & REPORTING

CIMTRAK TICKETING MODULE

Differentiating between known "good" changes and unknown changes that require investigation is a critical part of maximizing the time you and your team spend responding to change events and alerts. CimTrak provides users with the only integrity monitoring solution that offers a fully integrated change ticketing system, which is bi-directional, allowing information and commands to be executed through automation to ensure only approved changes are permitted. This provides organizations of all sizes with the ability to minimize change noise, reconcile 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 INTEGRATION–SIEM, SOAR, AND ITSM

If your organization utilizes other security and operational management tools such as SIEM, SOAR, or ITSM technologies, integrating data collected by CimTrak is easy. CimTrak provides vital insight and information from servers and other endpoints. CimTrak's integrity monitoring and configuration monitoring software provides timely intelligence that enhances analysis, correlation, and situational awareness, enabling the mitigation of attacks, ensuring operational integrity, and detecting 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 integrity management data enhances the compliance reporting capabilities of SIEMs and ITSMs by increasing the coverage of security controls that can be monitored. CimTrak's comprehensive forensic details also add vital information for a SIEM's data mining engine, as well as a SOAR's ability to restore through automation.

The combination of CimTrak and these various technologies can help streamline compliance reporting, enhance your security posture, ensure operational availability, and meet numerous control objectives of best practices, including CIS Controls, HITRUST, NIST 800-53, and many others.

CimTrak integrates with all leading SIEM/SOAR solutions, including HP ArcSight, IBM QRadar, McAfee Enterprise Security Manager, RSA Security Analytics, and Splunk, all without any complicated configuration or setup. CimTrak also integrates with leading ITSM frameworks such as ServiceNow, BMC, Atlassian, and CA to create a closed-loop process for change management.

COMPLIANCE

CIMTRAK COMPLIANCE

CimTrak Compliance assesses the configuration 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 various 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 them 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 AS A SERVICE

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 features and functionality as if deployed on-premise, but leveraging the value and efficiency 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.

*Check for availability

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 fully customizable, offering a range of graphs and charts to choose from. Each CimTrak user can customize their dashboard to provide a unique view of the entire IT environment or just the systems for which they are responsible.

EASILY SCALE WITH CONSOLIDATED MANAGEMENT VIEW

Several CimTrak Master repositories can be bound together via CimTrak Clustering to scale CimTrak horizontally and vertically. This technique allows CimTrak to meet the needs of the largest infrastructures in both commercial and government sectors. 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 demonstrating compliance during IT audits, verifying that planned changes have been implemented, 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 formats. 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 simpler and more efficient with CimTrak. The CimTrak Change Reconciliation workflow provides a seamless and easy-to-use methodology for managing change, from initial identification and investigation through triage, task assignment to an engineer, and final remediation and confirmation. The CimTrak Change Reconciliation Workflow provides a robust process 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.

SUPPORTED PLATFORMS

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS XP, Vista, 7, 8, 10, 11, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise, Windows 11 IoT Enterprise

WINDOWS SERVER 2003, 2008, 2012, 2016, 2019, 2022

LINUX Alma, Amazon, ARM, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, Rocky, SUSE, Ubuntu, others

FREEBSD 12, 13

SUN SOLARIS x86/SPARC

MACOS 5, 6, 7, 8, 9, 10, 11

HP-UX Itanium, PA-RISC

AIX 6.1, 7.1, 7.2, 7.3

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

Arista, Aruba, Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Palo Alto, Sophos, others

Supported Platforms CimTrak For Databases

IBM DB2, Microsoft SQL Server, MySQL, Oracle

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

Amazon AWS, Google Cloud, Microsoft Azure

Supported Container & Orchestration Integrations

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

Supported Ticketing Integrations

Atlassian Jira, BMC Remedy, CA ServiceDesk, ServiceNow

Supported SIEM Integrations

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

Supported Under CimTrak's Trusted File Registry™

CentOS 7, Microsoft Windows 7, 8, 8.1, 10, 11, XP, 2003, 2008, 2012, 2016, 2019, 2022, Oracle Linux 7, Redhat Enterprise Linux 7

SUPPORTED BENCHMARKS

ALIBABA
ALMA
AMAZON ELASTIC KUBERNETES
AMAZON LINUX
APACHE
APPLE MAC OS
AZURE
CENTOS
CISCO Firewall, IOS
DEBIAN
DISTRIBUTION INDEPENDENT
FEDORA
GOOGLE Chrome, Container, Kubernetes
IBM
KUBERNETES
MICROSOFT Access, Edge, Excel, IIS, Intune, Office, PowerPoint, SharePoint, SQL, Windows, Windows Server, Word
MONGODB
NGINX
ORACLE Cloud, Database, Linux, MySQL
PALO ALTO
POSTGRESQL
RED HAT
RHEL8
ROCKY
ROS
SUSE
UBUNTU LXD, Linux
VMWARE

REQUEST A DEMO

CIMTRAK

CIMCOR

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.

CIMCOR.COM | FOLLOW US @CIMTRAK