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 products and services, CimTrak consistently brings new ideas and solutions to the 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 Integrity Management solutions. CimTrak's unique next-generation File Integrity Management (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 that their systems are always in a state of constant integrity.

DETECT CHANGES ACROSS 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 functions as a single point of collection and reporting on enterprise-wide changes that can negatively affect operations, security, and compliance.

INSTANT NOTIFICATION WHEN A CHANGE OCCURS

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 prevention of integrity drift.

CORRECTIVE ACTION AUTOMATICALLY

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

FEATURES

- » Detect Malicious Events in Seconds vs Months
- » 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

IRREFUTABLE FILE INTEGRITY

When an unexpected change occurs, it's critical to be able to discern if the file that changed is a good or bad change. 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/white-list database that provides additional information and integrity assurance that the current or changing files are known and trusted as determined by the software manufacturer.

PROVIDE DOCUMENTATION ON ALL CHANGES

CimTrak gives a full array of reports on changes in your IT environment, the process used to determine if the change is good/bad, and the actions taken. This complete reporting allows change tracking and verification, audit and compliance reports, as well as necessary executive-level reports. 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 them securely in the CimTrak Master Repository.

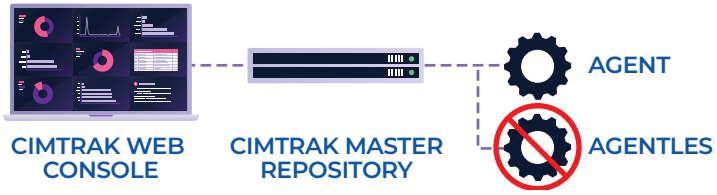
This establishes a known, trusted baseline. From there, CimTrak receives data from the various CimTrak agents and modules. When the data received does not match the cryptographic hash of a particular file, configuration, or setting, a change has occurred, and CimTrak takes action. Depending on how CimTrak 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

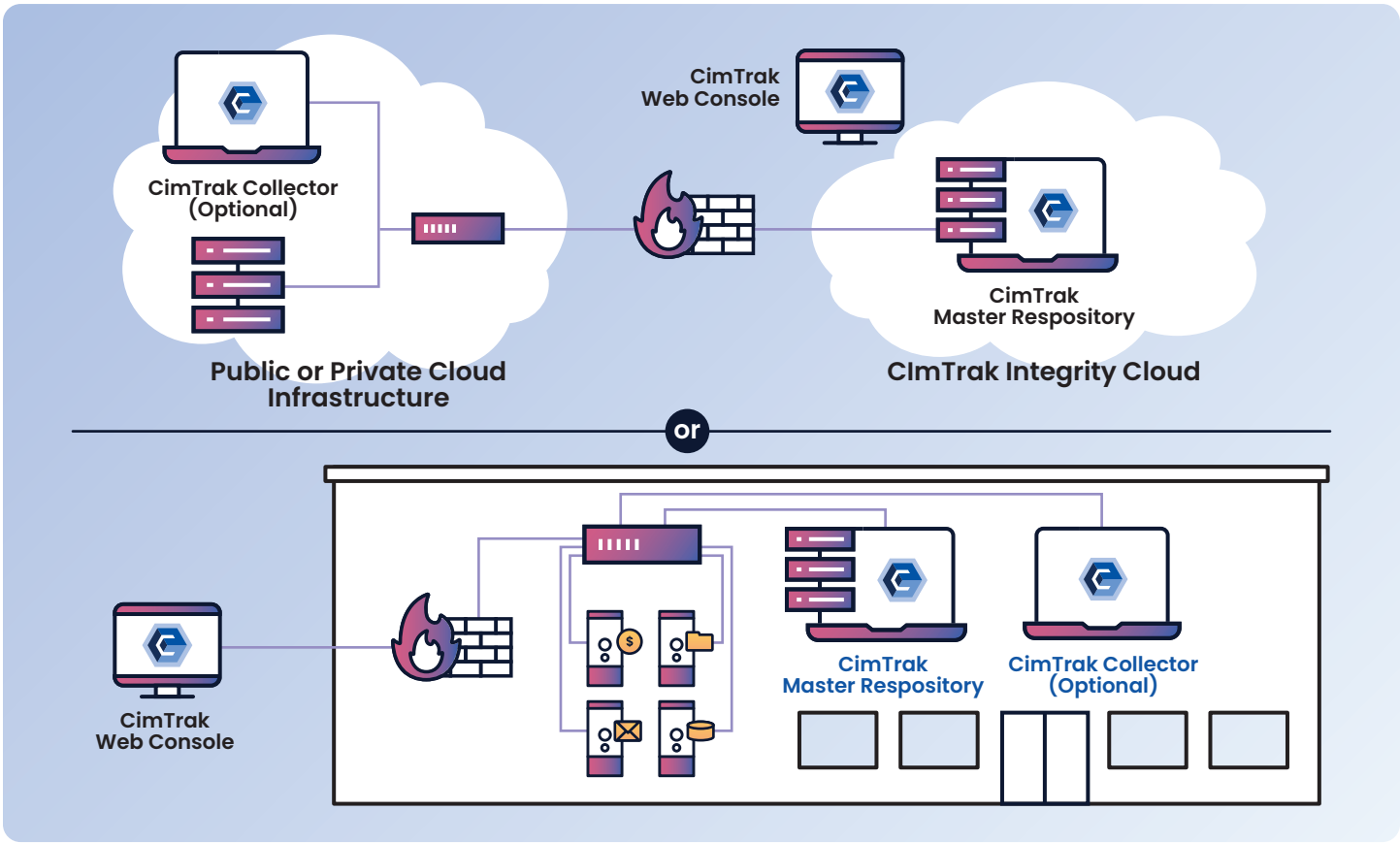
CimTrak supports a variety of systems, devices, and applications within the IT environment. CimTrak offers agent and agentless solutions depending on your specific business and technical requirement(s).

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.

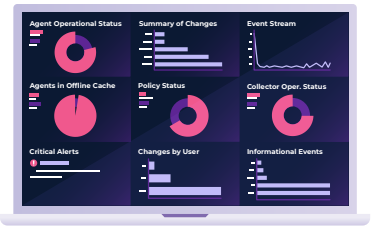


CIMTRAK AVAILABLE ON-PREMISE OR IN THE CLOUD



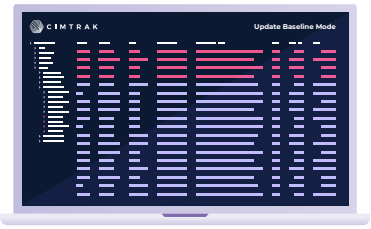
*CimTrak Collector is required when the technical need includes network devices, container orchestration, hypervisors, and compliance.

CIMTRAK MODES OF OPERATION



LOG

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

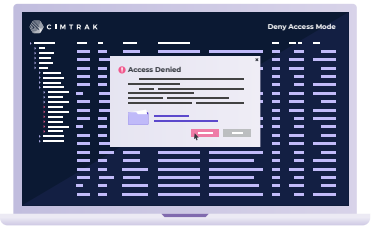


UPDATE BASELINE

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

RESTORE

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

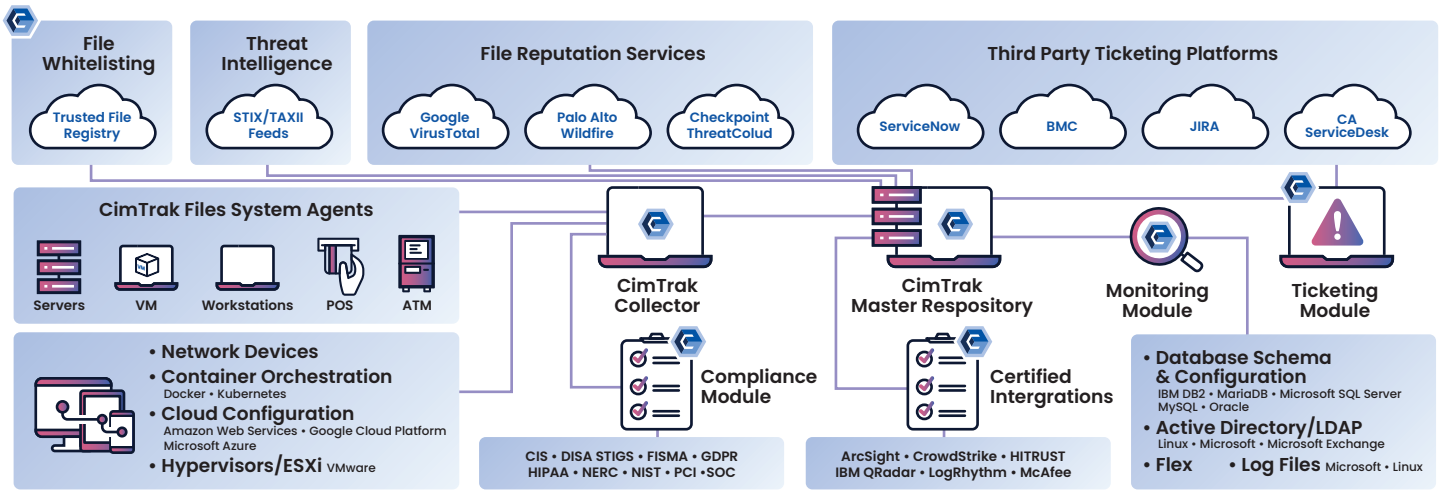
Denies any access to a file. Since CimTrak runs as the local system account, it does not matter what privilege access a user has. Access to a file will not be allowed, thus denying reads, changes, deletions, or additions. No other integrity management tool provides this advanced capability.

It is 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 that file to be restored 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.

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 SECURITY SUITE

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 your 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 you the most complete integrity solution for your IT environment with minimal impact on your 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 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 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 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 the addition of a new account, or can have a 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

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 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 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 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 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 FOR SCADA DEVICES

CimTrak provides the necessary detective controls that help you meet several key NERC-CIP requirements and covers 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 incorporates the use of CIS Benchmarks and DISA STIGs as a trusted source for hardening systems, devices, operating systems, applications, and more. 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 as well as 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 download from any number of 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 on current systems or if they have ever 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 update the master CimTrak denylist/blacklist dynamically and automatically 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 should be investigated 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 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, 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 the analysis, correlation, and situational awareness needed to mitigate attacks, ensure operational integrity, 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 integrity management data broadens SIEM's and ITSM's compliance reporting capability 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, improve your security posture, ensure operational availability, and meet numerous control objectives of best practices of 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 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 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 feature/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.

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.

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. 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 in 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 simpler and 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, assigning the task 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

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.

REQUEST A DEMO

CIMTRAK

CIMCOR.COM | FOLLOW US @CIMTRAK

© CIMCOR 2024 | TECHNICAL SUMMARY v4.2