CIMCOR

TECHNICAL SUMMARY

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 ideas to market.

FEATURING

- 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

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 many FIM solutions. CimTrak's unique SmartFIM™ 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 rest assured that their systems are always in a state of constant integrity.

DETECT 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. 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. By being instantly aware of changes, you stay on top of, and are constantly aware of the state of your critical IT infrastructure.

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 you the ability to take instant, automatic action to remediate or prevent changes completely.

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 CimTrak's robust integration with industry malware analysis engines.

PROVIDE DOCUMENTATION ON ALL CHANGES

CimTrak gives you 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 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.

www.cimcor.com

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

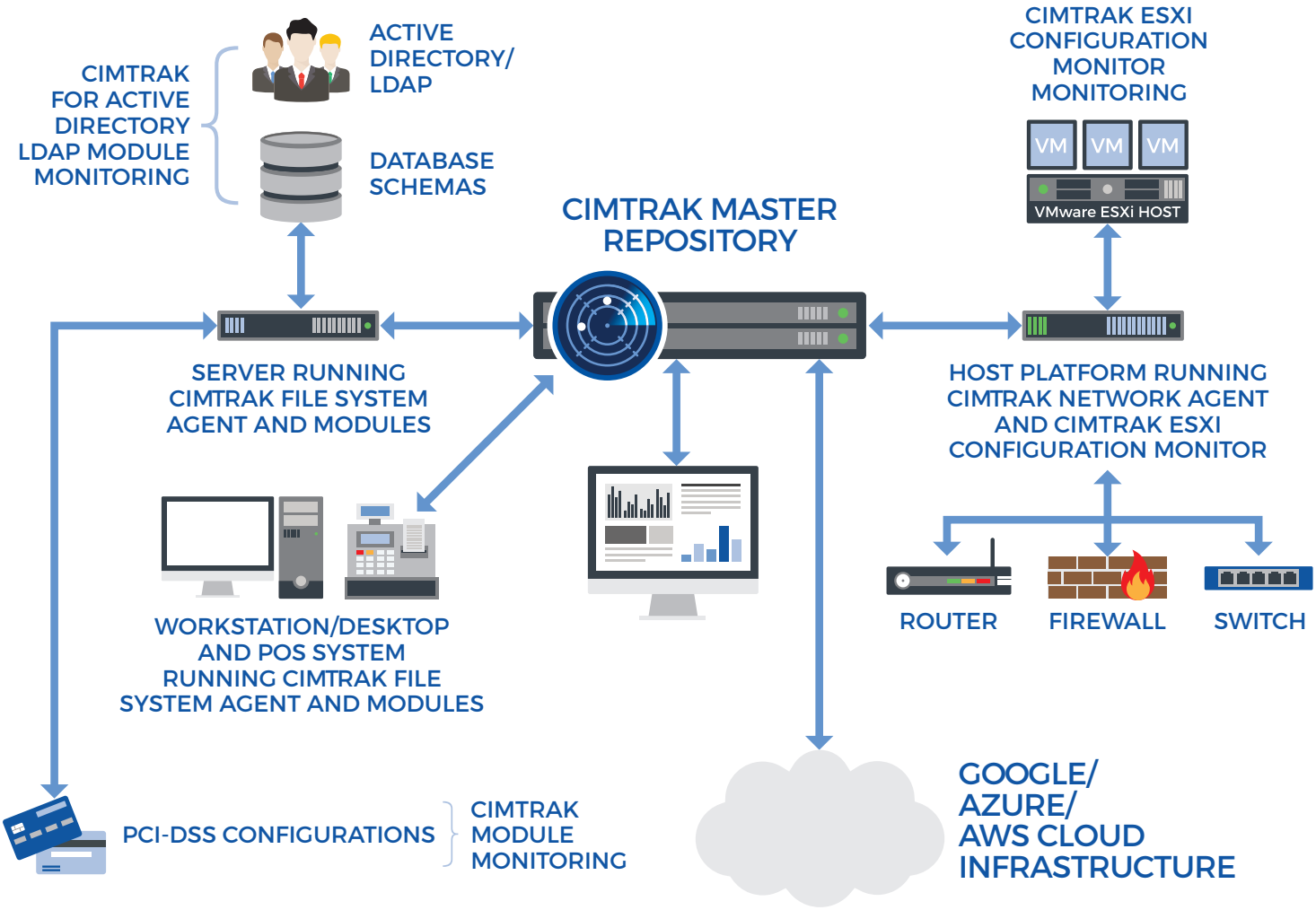
Securely stores files and configurations and performs comparisons to detect changes.

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

The CimTrak Management Console supports multiple users as well as multi-tenant views.



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.

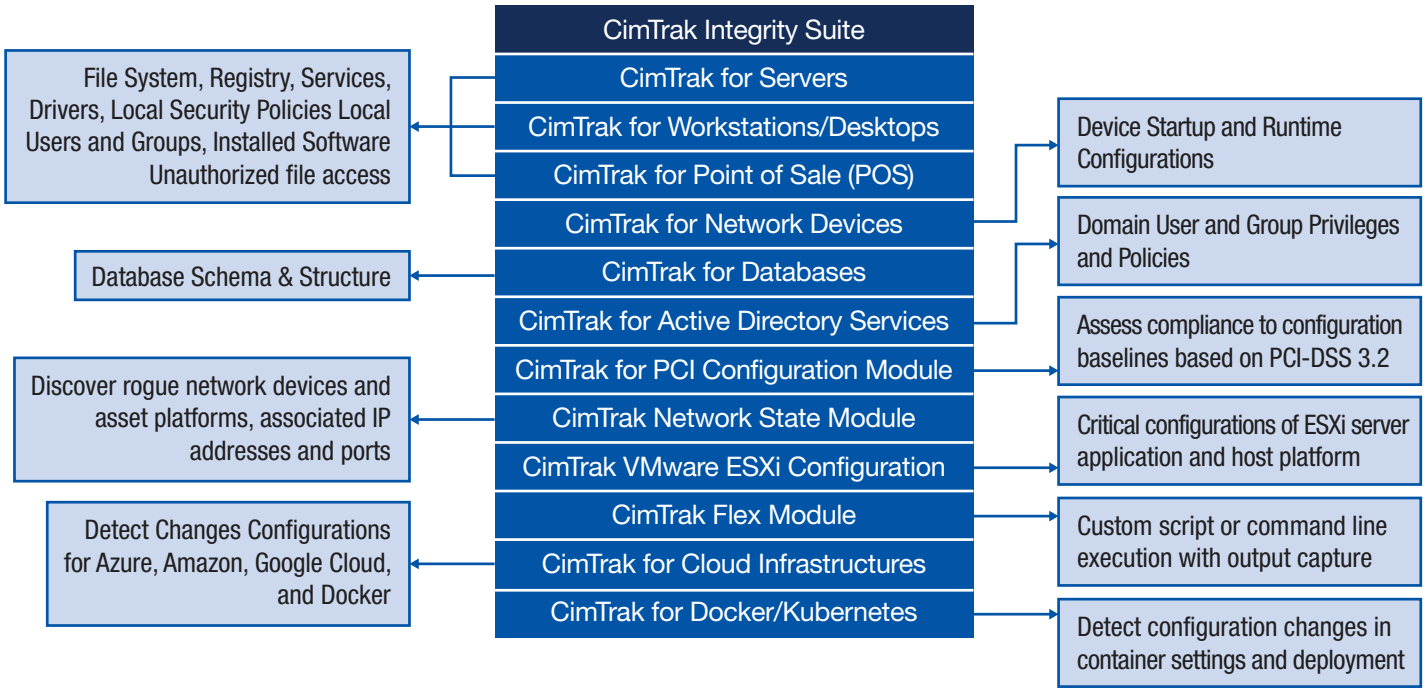
DENY RIGHTS
Denies any access to a file. Since CimTrak runs as the local system account, it does not matter what privilege access a user has, access to a file will not be allowed thus denying reads, changes, deletions or additions. No other integrity tool provides this advanced capability.

It is important to note that CimTrak allows a great deal of flexibility when using 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!

WHAT CIMTRAK MONITORS



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 for your IT environment with minimal impact to your CPU cycles or network bandwith.

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 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 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 CONFIGURATION MONITOR

The CimTrak PCI Configuration Monitor 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 ESXI CONFIGURATION MONITOR

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

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 and streamlines IT operations which allows personnel to focus on more pressing issues.

CIMTRAK FOR CLOUD INFRASTRUCTURES

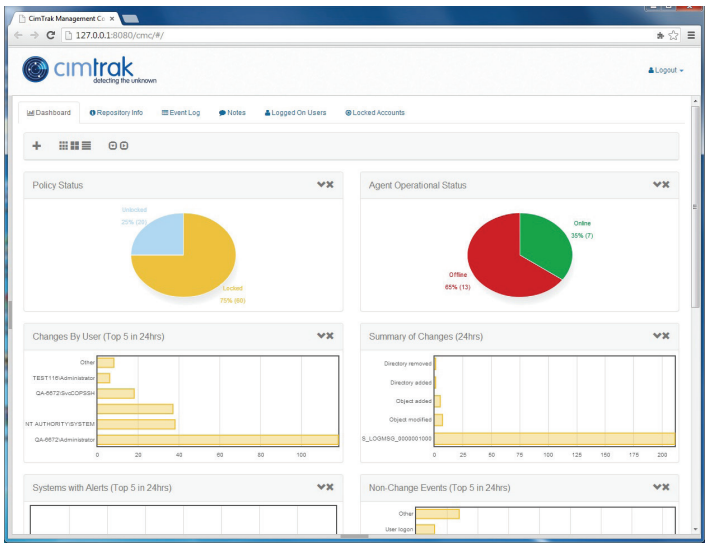
CimTrak for Cloud Infrastructures provides an easy way to know when new cloud servers are provisioned, or changes have occurred to server configuration settings, virtual firewall rules, virtual network settings and much more. CimTrak for Cloud Infrastructures supports Google Compute Engine, Azure, and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

CIMTRAK FOR DOCKER/CONTAINERS

CimTrak for 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 Docker/Kubernetes provides extensive visibility into the settings that drive your container deployments.

LEADING EDGE INTEGRATED SECURITY 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.



EASY INTEGRATION WITH SECURITY INFORMATION AND EVENT MANAGERS (SIEM)

If your organization utilizes SIEM technology, integrating data collected by CimTrak is easy. CimTrak provides vital insight 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 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 powerful data mining engine. The combination of these technologies can help streamline compliance reporting and improve your security posture in the process.

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 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 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 spends responding to change events. CimTrak's SmartFIM™ technology provides users with the only file integrity monitoring system to offer a fully integrated change ticketing system. This provides organizations of all sizes with the ability to plan and document changes at an economical cost.

Further, CimTrak's integrated change ticketing system allows for integration with your existing ticketing solutions such as CA Service Desk, Service Now, Cherwell, and Jira.

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 from managing change from the initial identification of the change, investigation, and triage of the change, 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.

THREAT FEED INTEGRATION

CimTrak integrates with STIX 1.0/2.0 and TAXII Thread Feeds. 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.

REAL-TIME FILE & MALWARE ANALYSIS

When files change, CimTrak can integrate with Virus Total, Palo Alto Wildfire, or Checkpoint's Threat API, to perform real-time 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 on other systems which are monitored by CimTrak.

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.

TRUSTED FILE REGISTRY™

A key component of CimTrak's SmartFIM™ 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 surface, greatly decreasing time spent investigating changes and maximizing the security of the users IT environment.

SUPPORTED PLATFORMS

CIMTRAK FOR SERVERS, CRITICAL WORKSTATIONS & POS SYSTEMS

» Windows: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady
» Windows Server: 2003, 2008, 2012, 2016
» Sun Solaris: x86, SPARC
» Mac: Intel, Power PC
» Linux: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, SUSE, Ubuntu, others
» HP-UX: Itanium, PA-RISC
» AIX

WINDOWS PARAMETERS MONITORED

» File additions, deletions, modifications, and reads
» Attributes: compressed, hidden, offine, 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

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

SUPPORTED HYPERVISORS

CIMTRAK VMWARE ESXI CONFIGURATION MONITOR

» VMware ESXi 3x, 4x, 5x, 6x

CIMCOR

© 2018 Cimcor, All Rights Reserved