CIMCOR

SOLUTION BRIEF

Learn How To Harden Systems Using CIS Benchmarks

FEATURES

EASE OF USE

CIS Benchmarks™ are fully incorporated in CimTrak with a library of benchmarks to immediately utilize and choose from.

INCREASE SECURITY POSTURE

Utilizing CIS Benchmarks™ and hardening efforts help mitigate many common threats resulting from misconfigured systems.

REDUCES AND ELIMINATES ACCESS POINTS

Removing unnecessary files, software and applications can reduce the number of access points a bad actor can leverage.

IMPROVES PERFORMANCE

Systems work more efficiently if not burdened with unnecessary services or struggling to operate with limited memory and space.

Secure Configurations

CIS Benchmarks™ are a best practice guide to secure configurations. They are a consensus-based best practices and standards recognized globally by governments, business, industry and academia as the recommended configuration for numerous devices and platforms.

When organizations install a new operating system or application, by default nothing is secure and everything is on. This includes ports being open, application services running, etc. CIS Benchmarks™ help configure that new operating system or application in a hardened manner. CIS Benchmarks™ are integrated into CimTrak's Compliance Module, where CimTrak provides detailed alerts, reports and controls to:

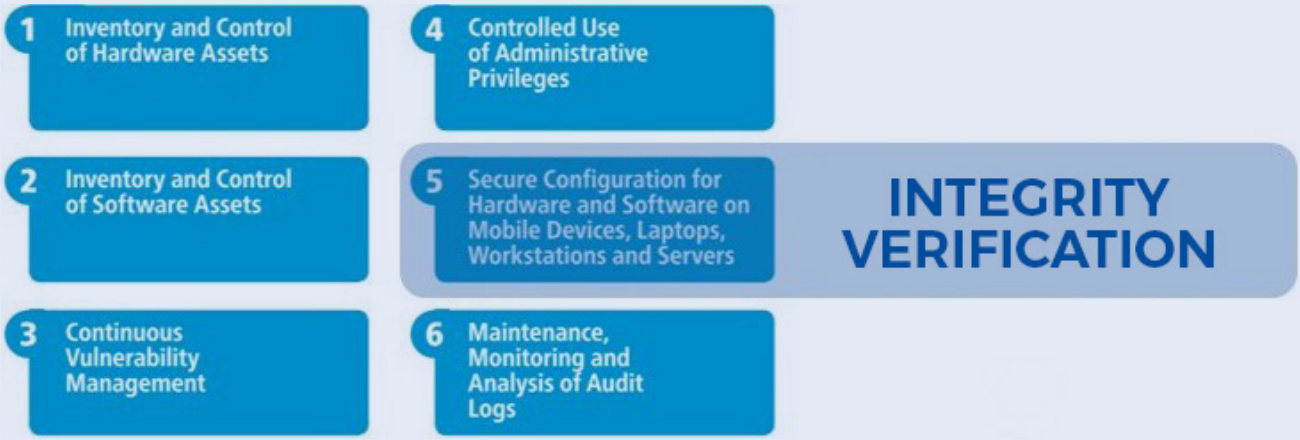
» Assess the current state of configurations
» Provide steps necessary and correct any misconfiguration(s) or security vulnerabilities based on the recommended CIS Benchmarks™
» Alert if/when there are unexpected, unwanted or unauthorized changes to the desired/"correct state"
» Prevent change(s) to designated files and/or configurations
» Allow exception-based rules to align with unique environment and security conditions
» Remediate and roll-back to a previous known and trusted state if a benchmark has been compromised

All this is represented in a customizable, easy to read and graphical interface to simplify efforts of achieving and maintaining CIS Benchmark™ compliance regardless if you're operating on-premise or in the cloud.

If following the prescribed best practices of the CIS Top 20 Controls, CimTrak specifically delivers the necessary controls to manage the configuration and change management processes to prevent attackers from exploiting vulnerability services and settings.

This is what Cimcor calls integrity verification and assurance and is essential to the formation and construct of the CIS "basic controls" and specifically defined within CIS Control #5.

Basic CIS Controls™



"Based on our extensive testing across the DoD, Intelligence community, and rest of government, it was clear to me–secure configuration management is a foundational, must-do element of any successful security management program."

TONY SAGER, CIS
Sr VP & Chief Evangelist

CIS SecureSuite® Membership CIS CyberMarket®

Furthermore, CimTrak utilizes a SCAP 1.2 (Security Automation Protocol) compliant scanning engine in order to monitor configuration elements, approved exceptions and alerts and reports on unauthorized changes. This also helps and enables organizations in efforts of becoming FedRAMP compliant.

Today there are over 150 CIS Benchmarks™. Currently, there are 70+ relevant benchmarks included within CimTrak and our list continues to be modified, updates and new benchmarks added regularly. Most CIS Benchmarks™ include multiple configuration profiles. Those profiles describe and define configurations which are assigned to the various benchmark recommendations.

» Level 1 profile is considered the most basic requirement with minimal operating and performance impact. The objective is to essentially minimize the attach surface while considering the impact to overall business demands and functionality.
» Level 2 profile is what CIS calls "defense and depth" where the intent is to maximize the security posture when and where security is vital to the organizations overall business livelihood and sustainability.

Mapping & Compliance

Cimcor has eliminated the headaches and confusion of mapping the various compliance mandates with the CIS Benchmarks™ in order to simplify efforts of assessing, maintaining, reporting and correcting misconfigured devices.

Show: All / None

Mapping Name	Pass/Fail	Total Tests	Pass Tests	Fail Tests	Waived Tests	Percentage
CIS Controls	Fail	0	665	460	0	59.11%

CIS Controls						
1 - Inventory and Control of Hardware Assets						
1.1 - Utilize an Active Discovery Tool						
1.2 - Use a Passive Asset Discovery Tool						
1.3 - Use DHCP Logging to Update Asset Inventory						
1.4 - Maintain Detailed Asset Inventory						
1.5 - Maintain Asset Inventory Information						
▶ 1.6 - Address Unauthorized Assets	Pass: 0	Fail: 1	Skip: 0	Waived: 0	Total: 1	Pass: 0.00%
1.7 - Deploy Port Level Access Control						
1.8 - Utilize Client Certificates to Authenticate Hardware Assets						
2 - Inventory and Control of Software Assets						
2.1 - Maintain Inventory of Authorized Software						
2.2 - Ensure Software is Supported by Vendor						
2.3 - Utilize Software Inventory Tools						
2.4 - Track Software Inventory Information						
2.5 - Integrate Software and Hardware Asset Inventories						
2.6 - Address unapproved software						
2.7 - Utilize Application Whitelisting						
2.8 - Implement Application Whitelisting of Libraries						
2.9 - Implomont Application Whitelisting of Scripts						
2.10 - Physically or Logically Segregate High Risk Applications						
▶ 3 - Continuous Vulnerability Management	Pass: 1	Fail: 0	Skip: 0	Waived: 0	Total: 1	Pass: 100.00%
3.1 - Run Automated Vulnerability Scanning Tools						
3.2 - Perform Authenticated Vulnerability Scanning						
3.3 - Protect Dedicated Assessment Accounts						
▶ 3.4 - Deploy Automated Operating System Patch Management Tools	Pass: 11	Fail: 0	Skip: 0	Waived: 0	Total: 11	Pass: 100.00%
3.5 - Deploy Automated Software Patch Management Tools						
3.6 - Compare Back-to-back Vulnerability Scans						
3.7 - Utilize a Risk-rating Process						
4 - Controlled Use of Administrative Privileges						
4.1 - Maintain Inventory of Administrative Accounts						
4.2 - Change Default Passwords						
▶ 4.3 - Ensure the Use of Dedicated Administrative Accounts	Pass: 2	Fail: 0	Skip: 0	Waived: 0	Total: 2	Pass: 100.00%

Compliance efforts include:

PCI DSS
NIST 800-53
NIST 800-171
GDPR
DISA STIGS
SOX SARBANES OXLEY 404
HIPAA
ISO 27K
AND MANY MORE

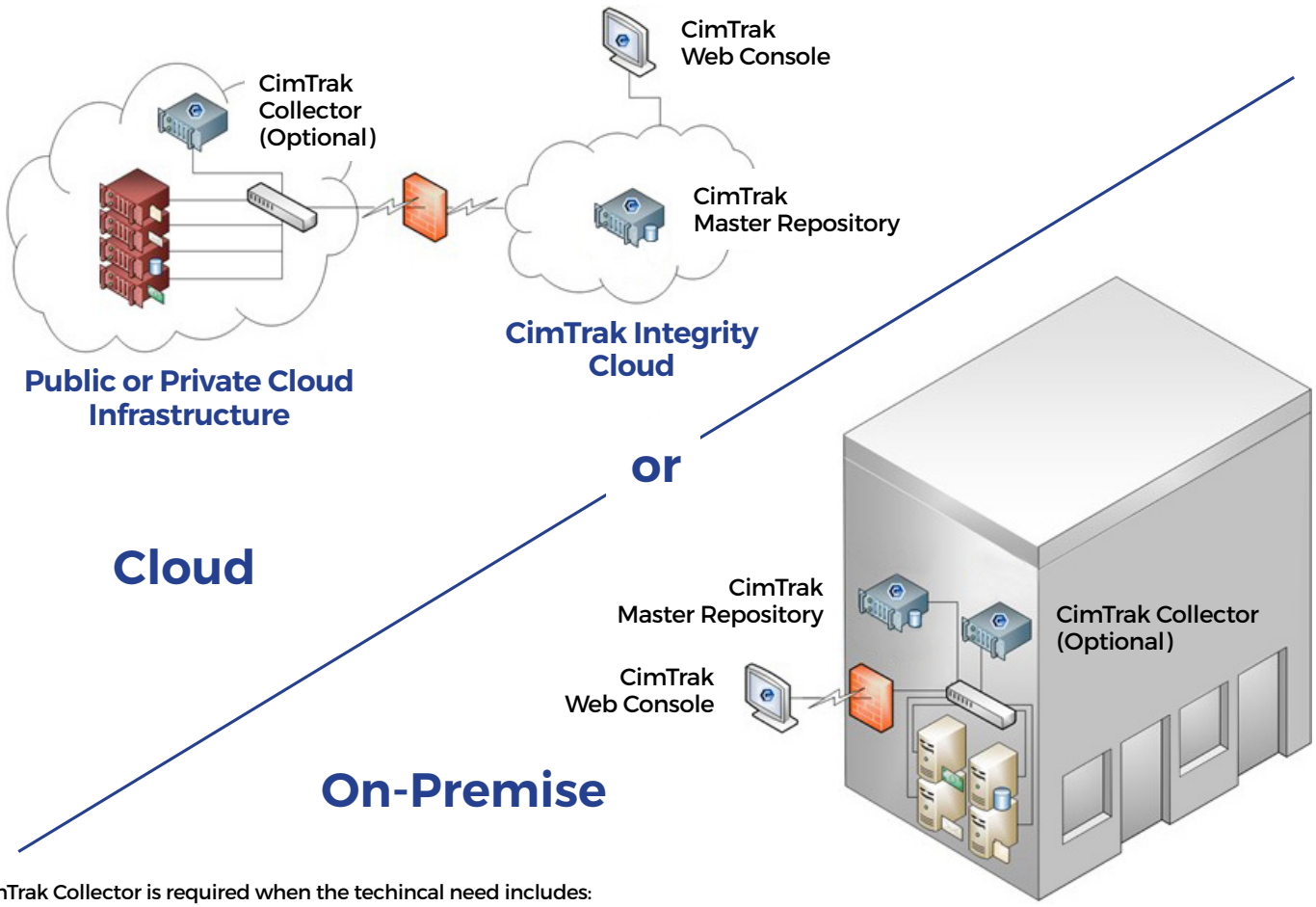
Benchmarks integrated within CimTrak include:

AMAZON LINUX
APPLE OS
CENTOS LINUX
CISCO
DEBIAN LINUX
FEDORA FAMILY LINUX
GOOGLE CHROME
IBM AIX
MIT KERBEROS
MICROSOFT IIS
MICROSOFT OFFICE
MICROSOFT SQL SERVER
MICROSOFT WEB BROWSER
MICROSOFT WINDOWS DESKTOP
MICROSOFT WINDOWS SERVER
MONGODB
MOZILLA FIREFOX
NGINX
ORACLE DATABASE
ORACLE LINUX
ORACLE MYSQL
ORACLE SOLARIS
POSTGRESQL
RED HAT ENTERPRISE LINUX
SUSE LINUX
UBUNTU LINUX
VMWARE
AND MANY MORE

Management & Architecture

The CIS Benchmark™ Compliance Module for CimTrak, an add-on feature to the CimTrak Integrity Suite, is designed to simplify your CIS Benchmark needs. It's dashboard and reporting capabilities are intuitive, allowing for single views of test results and compliance scoring. This view provides for common CIS compliance requirements to be illustrated as a single test with remediation instructions, aiding to bring your organization into full CIS compliance, and ensuring that it stays that way. The Compliance Module can be operated on-premise or in the cloud.

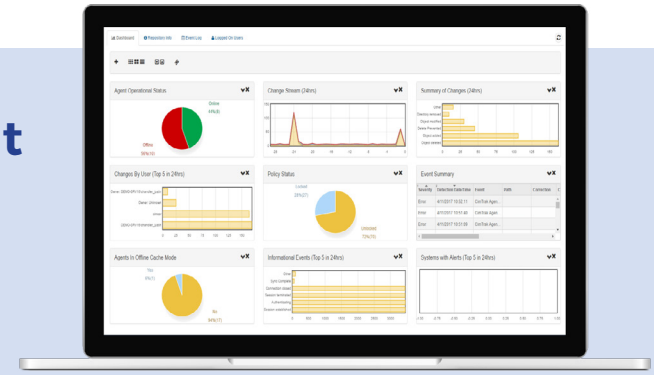
CimTrak Available On-Premise or in the Cloud



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

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 SEIM 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.