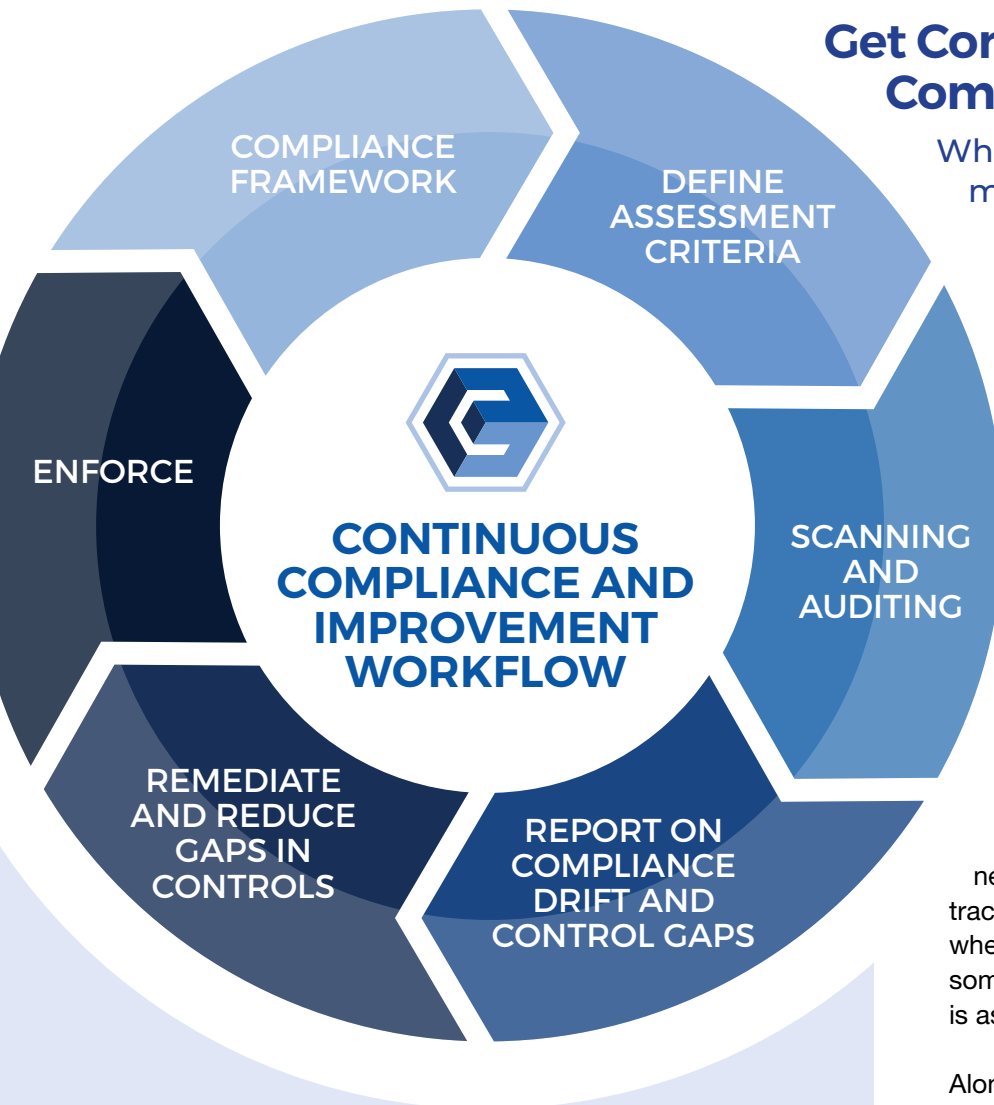


Implementing Compliance and Vulnerability Management with CimTrak



Get Compliant. Stay Compliant. Prove it.

When it comes to compliance management, it is essential to maintain and protect information, remediate problems as they arise, and demonstrate necessary controls are in place to provide required compliance reports. This is applicable for both internal policies and external compliance mandates imposed by governments, industries, and organizations.

CimTrak Next-Gen File Integrity Monitoring adds a vital security layer to critical infrastructure while simultaneously supporting compliance and best practices requirements. Any changes to servers, network devices and applications can be tracked and documented. Determining who, what, when, where, why (ticketing), and how (process) something has changed since the last audit cycle is as simple as generating a report.

Along with securing your systems and data, you must also prove that your cybersecurity policies and procedures are aligned with internal audits, internal security policies as well as external standards and regulations. From internal controls and risk management to regulatory affairs, CimTrak helps organizations stay compliant.

FEATURES

- » Benchmarks can be uploaded for real-time testing, auditing and reporting
- » Track any changes or deviations regarding compliance
- » Create specific benchmarks for compliance
- » Discover and collect information on physical assets and assign to appropriate compliance policy
- » Allow for a condition to exist within a policy and take exception

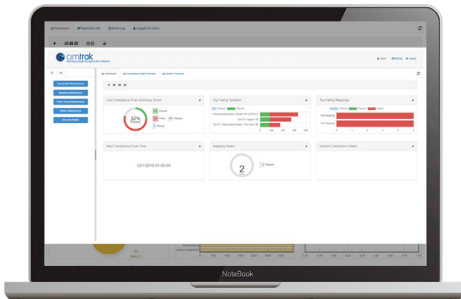


Features

Benchmark Scanning

Many compliance standards and organizations require the use of benchmarks to ensure compliance in applicable systems and services. These benchmarks can be uploaded to the Compliance Module for CimTrak for robust testing, auditing, reporting and instructions to remediate where applicable.

Policy Monitoring and Grouping Regularly scanning the devices in your organization based on a single policy, you can track any changes or deviations regarding compliance. These policies can also be grouped together to provide a common compliance framework where compliance criteria across various regulatory requirements can be represented as a single test.



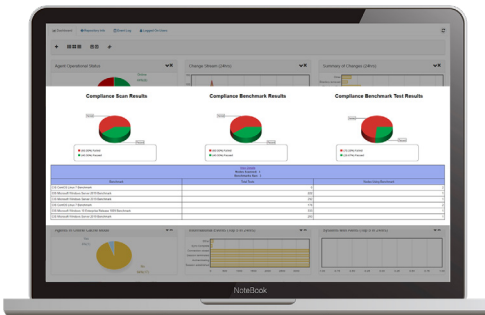
Screenshot of CimTrak's Compliance Dashboard

Compliance Mappings Compliance mappings enables your organization to create a custom set of benchmark tests to comply to specific standards that may not otherwise exist, or that need to be tailored to your organization's own specific requirements.

Network Discovery Network device discovery helps you to discover, inventory and collect information about physical assets such as routers, switches, servers, hosts and firewalls which can then be assigned an appropriate compliance policy with a simple point and click.

Waiver Management Given every infrastructure is different and unique, often times there's a need to allow a condition to exist within a policy(s) and take exception. This exception is highlighted as a waiver for future auditing activities.

Compliance Dashboard Simply put... there is no need for an additional console to gain the necessary visibility into compliance activity! The Compliance Module for CimTrak is fully integrated with our core product to simplify and correlate with security and integrity management activities into a single pane of glass.



Screenshot of CimTrak's Reporting

Agent & Agentless

CimTrak Compliance Module provides an agent-based or agentless solution which can be on-demand or scheduled to perform benchmark or compliance scans, giving you the ability to understand your systems' state at the time of the scan.

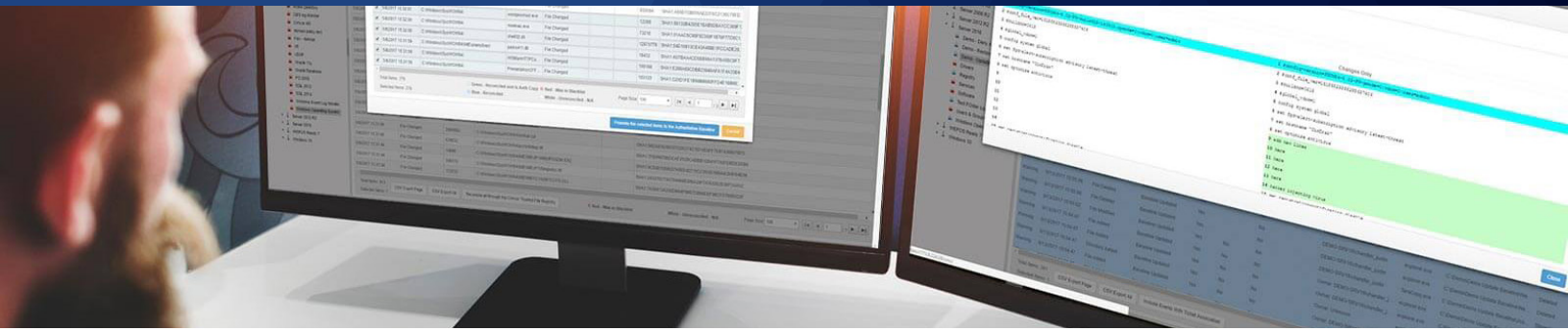
Reporting

When your organization is being audited, the CimTrak Compliance module provides an easy solution to show current and historical compliance to your industry standards and compliance requirements.

Vulnerability Management

CimTrak has a unique ability to identify, classify, and prioritize vulnerabilities allowing for corrective actions to be performed, remediating problems such as open ports, software configuration issues, and malware.

Regulations such as SOX, PCI, HIPAA, FFIEC, FISMA, NERC-CIP, SWIFT, GDPR, CDM, CJIS, and many others have evolved to ensure accountability and privacy. CimTrak's integrated compliance module provides the necessary auditing, alerting, and reporting capabilities to track changes and maintain compliance. This compliance assurance is simple to use, cost-effective, and will eliminate the ongoing headaches of continuous and manual audits.



Regulatory Requirements



CIS
 CimTrak detects unauthorized changes, cybersecurity threats and compliance risks



PCI DSS
 CimTrak ensures cardholder data security and file integrity



GDPR
 CimTrak helps monitor the security of personal data for GPDR compliance



SWIFT
 CimTrak helps the financial community comply with many mandatory and advisory controls



HIPAA
 CimTrak ensures healthcare systems are authentic and tamper-free for healthcare compliance



GLBA
 CimTrak provides intrusion detection and real-time remediation for financial institutions



SARBANES OXLEY
 CimTrak rigorously tracks and reports changes made to IT systems



NIST
 CimTrak helps with compliance and security of NIST



CDM
 CimTrak helps agencies with Phase 1 and Phase 3 of CDM



CJIS
 CimTrak helps security teams and organizations with policy and implementation, and information integrity



NERC-CIP
 CimTrak detects and eliminates unauthorized changes, cybersecurity threats and compliance risks



FEDRAMP
 CimTrak helps with FedRAMP compliance by ensuring security and integrity across the infrastructure

Library of Mappings

- AICPA GAPP
- AICPA SOC2 and SOC3 TSC 2017
- AICPA SOC2 and SOC3 TSPC
- ANSSI - 40 Measures
- Australian Essential 8
- Australian Top 35
- Canadian CSE Top 10
- CIS Controls v7.1
- CMMC
- COBIT 5
- CoM 201 CMR 17.00
- CSA CCM v3
- DHS CDM Program
- DHS Chem Anti-Terrorism
- FFIEC Booklet 2016

- FFIEC CAT
- FFIEC Examination Handbook
- FY15 FISMA Metrics
- GCGQ 10 Steps
- HIPAA
- IEC 62443-3-3-2013
- IRS Pub1075
- ISO 27002-2005
- ISO 27002-2013
- ITIL 2011 KPIs
- NERC CIP v6
- NERC CIP v7
- NIST 800-171
- NIST 800-53 rev4
- NIST 800-82 rev2

- NIST CSF 1.1
- NIST SMB Guide
- NSA MNT
- NSA Top 10
- NV Gaming MICS
- NYCRR 500
- PCI DSS 3.2
- Saudi AMA
- SEC OCIE Audit Guide for AWS
- SG MAS TRM
- SWIFT
- UK Cyber Essentials
- UK IICO Protecting Data
- Victorian PDSF v1.0
- And dozens more**

How the Compliance Module for CimTrak Helps

The Compliance Module for CimTrak, an add-on feature to the CimTrak Integrity Suite, is designed to simplify your compliance needs. Regardless of the standards or number of regulatory requirements imposed within your organization, dashboard and reporting capabilities are intuitive, allowing for single views of test results, compliance scoring, and policy groupings. This view provides for common compliance requirements to be illustrated as a single test with remediation instructions, aiding to bring your organization into full compliance, and ensuring that it stays that way.

How the Compliance Module for CimTrak Works

