CIMCOR

THE DEFINITIVE GUIDE TO

File Integrity Monitoring

File Integrity Monitoring (FIM) is a solution to a complicated problem, but the solution itself doesn't have to be complicated. With the right methodology and solution, you can easily install, configure and manage the integrity of your systems.

CONTENTS

FILE INTEGRITY MONITORING

COMPLIANCE DRIVERS FOR FIM

KEY QUESTIONS FOR EVALUATION

FILE INTEGRITY MONITORING

WHAT IS FILE INTEGRITY MONITORING (FIM)?

File Integrity Monitoring is an IT security technology used to detect changes in an organization's IT environment by comparing them against a known state.

DO I NEED FIM?

Beyond the fact that you're required to have FIM in place for various compliance drivers such as PCI-DSS, your system security is significantly weaker if you can't readily identify and deal with IT security threats. Without FIM you're vulnerable to external threats such as malware as well as unknown, internally made changes, which can compromise your security posture. Most companies find that file integrity monitoring is extremely useful for ensuring the security of their data and systems. By detecting unknown changes quickly, you can respond swiftly to threats that may cause data breaches or bring down critical IT systems. With the sharp rise in zero-day malware and advanced persistent threats, many traditional IT security tools are not able to offer any sort of protection. Because FIM tools can "see" all changes that are happening, file integrity monitoring is a very valuable asset to have as part of your IT security defenses. File integrity monitoring is required to achieve compliance with numerous regulations as part of a comprehensive IT security strategy

HOW FIM WORKS

All file integrity monitoring products are essentially comparison tools that keep track of cryptographic hashes of files at different points in time. Hashes are a string of characters that uniquely identifies a file (also called a "fingerprint") which is used to compare against itself to determine if a change has been made.
When a file is altered in some way, the hash for that given file changes to a new unique value. A hash provides absolute certainty, or non-repudiation, that a file has indeed changed. Integrity-checking products use various hash algorithms, along with other file parameters, as a basis for proof that a file has, or has not been altered. However, file integrity monitoring products differ drastically in speed, performance, impact, and capabilities in how they accomplish these steps.

THE CIMTRAK SOLUTION

As an advanced integrity solution, CimTrak utilizes innovative technology, maximizing file integrity monitoring performance and providing a robust feature set, all while being simple and easy to use. This provides organizations that utilize CimTrak with a superior ROI and lower total cost of ownership versus other solutions.

WHAT CAN BE MONITORED WITH A FILE INTEGRITY MONITORING SOLUTION?

FIM solutions vary in exactly what all they can monitor, but most advanced solutions can detect changes across a wide variety of items typically found in your IT environment including:

» Files
» Applications
» Windows Registry
» Drivers
» Installed Software
» Services
» Local Users and Groups

WHAT TYPES OF CHANGES ARE DETECTED?

Advanced FIM tools will monitor for any type of change including additions, deletions, and modifications.

THE CIMTRAK SOLUTION

CimTrak goes beyond basic change detection (add/modify/delete) to monitor file reads (opens) to identify if files have been viewed or accessed. This capability is critical for files that may contain sensitive or classified information. CimTrak not only monitors file contents, but file attributes as well. Other solutions don't, which leaves a gaping hole in your change detection abilities.

WHAT ABOUT ROUTINE OR EXPECTED CHANGES? ARE THOSE DETECTED AND ALERTED ON TOO?

This is a common question about file integrity monitoring. The vast majority of all FIM solutions detect and alert on all changes, causing unwanted "noise" that users need to sift through to find truly unexpected changes, and therefore should be investigated.

THE CIMTRAK SOLUTION

CimTrak is the only file integrity monitoring solution that offers an integrated change ticketing system to allow users to plan for and reconcile changes. While CimTrak will still detect all changes, to have a complete audit trail, alerting will be suppressed for planned changes. Unexpected changes are then highlighted within the CimTrak Management Console, making it simple to focus attention on changes that are truly critical to examine. These unexpected changes will identify malicious activity as well as circumvented processes.

WILL FILE INTEGRITY MONITORING AFFECT MY SYSTEM PERFORMANCE?

The short answer: The right FIM solution will provide the resources needed to detect changes in your systems that are extremely minimal. File integrity monitoring should not be intrusive and should run transparently in the background. To better understand this concept, it is important to understand the different types of monitoring that various file integrity monitoring solutions utilize.

FILE INTEGRITY MONITORING METHODOLOGIES

Years ago, poll-based file integrity monitoring solutions were an IT professional's only choice. Even today, many open-source and commercially available solutions still use a poll-based methodology. Polling a file for changes means that a file is checked at certain time intervals. Poll-based file integrity monitoring is the least efficient way to monitor files for changes. This is because it places a sudden load on the monitored system when the polling time is reached. When polling, all of the monitored files must be hashed, and then the hash compared with the existing hash from the last poll interval. In contrast, the new generation of continuous file integrity monitoring technologies such as CimTrak can detect changes on most operating systems in real-time all while running quietly in the background. The newer, more advanced real-time methodology, does exactly what the name suggests. It detects changes the instant that they occur.

Operating at the kernel level, real-time file integrity monitoring intercepts file changes from the operating system itself. This allows for the detection of only the watched files that are changed by the operating system and allows changes to be captured at the moment they occur. This intelligent change detection methodology uses minimal system resources so that CPU cycles and disk I/O remain low. This advanced methodology also provides greater accuracy and other forensic information that is not possible through polling.

Real-time change detection provides a distinct advantage over poll-based solutions. Today, there are numerous threats to IT infrastructures. Organizations store a large amount of data on IT systems and rely on them for almost every aspect of their business. Unexpected or unknown changes can be catastrophic and cause loss of income and reputation. Therefore, every second matters when it comes to change detection. By detecting changes instantly, IT security personnel can be quickly alerted to malicious changes that can cripple critical business functions or lead to a data breach.

THE CIMTRAK SOLUTION

CimTrak was a pioneer in real-time integrity monitoring, becoming the first FIM product commercially available that offered this incredible new technology. It is important to note that all FIM tools that are labeled “real-time” do not necessarily detect changes the millisecond they happen. Some solution vendors deceptively claim they offer real-time monitoring when in reality, files are simply being polled quickly. This approximates real-time but differentiates from CimTrak’s “Truly Real Time™” methodology. CimTrak accomplishes Truly Real Time™ monitoring via proprietary technology that is simply unavailable in other solutions.

**Cimcor owns the patent for “Real-Time Change Detection and Remediation”.*

WHAT SHOULD I MONITOR?

Every environment is unique. There is no one-size-fits-all when it comes to file integrity monitoring. Monitoring everything, (like your entire c: drive) isn’t practical and leads to nothing but tons of noise. For this reason, it is important to be methodical when thinking about what to monitor. One of the first things that you should do before deploying a tool is to sit down and consider which items are critical to your organization, and what items would be beneficial to monitor. Some files and parts of an operating system change constantly, so monitoring those would not yield any valuable data.

Things to consider:
» What files/data is most critical to my organization?
» Where is a likely spot that malware or other malicious items would attach?
» What are the greatest areas of risk in my IT environment?

Robust FIM tools provide base operating system templates, which monitor your underlying critical system files for changes. These templates are usually based on accepted security standards and will specifically exclude files that cause noise or false positives.

THE CIMTRAK SOLUTION

CimTrak makes it simple for users to select exactly what they need to monitor. With built-in OS templates and the ability to easily drill down into the file structure, you can quickly install and operate. What's more, with the built-in regular expression include/exclude function, specific file types can be included or excluded from monitoring, making for quick policy definition and a significant reduction in noise and potentially the number of false positives.

CIMTRAK PROVIDES DEEP SITUATION AWARENESS

Knowing a file change occurred in your IT environment is of little value without more contextual information. In addition to letting you know what contents and attributes of a file have changed, CimTrak provides you with a side-by-side comparison of files and highlights the exact lines that have changed. This prevents the tedious task of searching through a file to determine the exact spot where a change occurred. CimTrak gives you other valuable change data, including who made the change, where the change originated, and what process was used to make the change. This data is immensely helpful in determining whether changes are routine or potentially malicious.

Many file integrity monitoring solutions do not provide this added layer of insight into changes, which greatly limits the value of the solution. Not only will valuable time be wasted trying to pinpoint changes and determine whether the change represents a risk, but an organization's security posture could also be negatively affected.

CAN A FIM SOLUTION TAKE ACTION WHEN A CHANGE IS DETECTED?

Most FIM products can generate an e-mail alert upon detection of a change, while more advanced solutions can send syslog output to a syslog server or security information and event manager (SIEM) which is discussed later in this guide.

THE CIMTRAK SOLUTION

CimTrak offers e-mail alerting as well as being able to output syslog to a syslog server or SIEM solution. What differentiates CimTrak from any other FIM tool is its ability to go beyond those capabilities to truly offer proactive protection from changes that are malicious or can cause critical system downtime.

CimTrak offers users the ability to block changes at the system level. Utilizing CimTrak's proprietary technology, changes are completely prevented from occurring. Another mode of operation allows users to instantaneously reverse and roll back changes. It does this without relying on any outside system or application. These advanced capabilities are built right into the CimTrak solution and offer users unprecedented security for critical files and configurations. These features are especially useful for ensuring the protection of unpatchable systems or devices that should not change outside of a change window such as POS systems or ATMs.

FIM AND ITS RELATIONSHIP TO SECURITY INFORMATION AND EVENT MANAGERS (SIEM)

What role FIM plays regarding Security Information and Event Management (SIEM) tools is often a question that many IT and security personnel ask. The answer: FIM is a complementary technology, helping SIEMs do their job better and faster by receiving system, application, and file change data directly from the file integrity monitoring tool itself.

File integrity monitoring tools provide real, actionable data about changes that have occurred. This allows the SIEM to combine critical change information with other data streams, allowing for enhanced event analysis and correlation. This benefits the enterprise by learning about security events more quickly and being able to provide better context surrounding those events. What's more, alerts raised by a SIEM can be traced back to the FIM tool, which can provide all of the forensic data (who, what, when, how) for the event, allowing for quick and simple root-cause analysis.

Not all file integrity monitoring tools can interact with a SIEM or interact with them seamlessly. If you are running a SIEM solution or plan to do so in the future, it is important to inquire whether your FIM tool is capable of interaction, and if so, how complex of a process is it to integrate the two.

THE CIMTRAK SOLUTION

CimTrak simply integrates with any SIEM solution and offers custom syslog output in a wide variety of formats requested by SIEM solutions. Some of the SIEM solutions that CimTrak integrates with include:

» HP ArcSight » IBM QRada » Splunk » LogRhythm
» McAfee Enterprise Security Manager » RSA Security Analytics » Many others

DO FILE INTEGRITY MONITORING SOLUTIONS PROVIDE ME WITH REPORTING?

Most FIM products will offer some type of reporting capability, but solutions vary in the number and depth of these reports. Advanced FIM solutions offer a multitude of reports which give you detail on changes at a high level (entire system) down to very granular levels of detail (change(s) to a single file) as well as the ability to schedule report generation. This allows you to create reports that meet the needs of different report viewers, everyone from high-level managers to auditors.

THE CIMTRAK SOLUTION

CimTrak offers a complete report generation engine, which produces numerous types of reports to meet the needs of the report viewer. CimTrak can generate reports on demand or via a report scheduler.

CAN OTHER IT SYSTEMS/APPLICATIONS BE MONITORED WITH FIM?

File Integrity Monitoring is somewhat of a misnomer. Advanced FIM tools go beyond simply monitoring files and items closely related to them. A better term would be "System Integrity Monitoring." Other items can often be monitored such as:

» Network Device Configurations
» Database Schemas
» Port Settings
» Active Directory/LDAP Object Settings
» Log Files
» Cloud Configurations

Advanced FIM tools can monitor more than files, which provides users with a holistic solution for their enterprise security needs. This includes directories, users, groups, settings, configurations, and more. This greatly simplifies workflow and often results in cost savings as well.

THE CIMTRAK SOLUTION

CimTrak strives to be a single solution for organizations that can "detect change across the entire enterprise." With the ability to detect changes on much more than simply files, CimTrak has your entire IT environment covered.

COMPLIANCE DRIVERS FOR FIM

PAYMENT CARD INDUSTRY DIGITAL SECURITY STANDARD (PCI-DSS)

The Payment Card Industry Digital Security Standards (PCI-DSS) was the first compliance standard to require file integrity monitoring of critical systems that handle payment card data. Section 11.5 specifically requires file integrity monitoring to be implemented to check files in the PCI environment and section 10.5.5 requires FIM to monitor changes to logs. Given the extremely sensitive nature of payment card data, the ability to ensure the integrity and security of systems that handle it is extremely critical.

"10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)."

"11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

THE CIMTRAK SOLUTION

CimTrak allows you to fully meet PCI-DSS requirements 10.5.5 and 11.5 as well as assist with other requirements. CimTrak's built-in templates make installation, setup, and configuration fast and easy. The CimTrak PCI Compliance Module automates the checking of critical operating system configurations to ensure compliance with PCI requirements. Organizations around the globe trust CimTrak to help them meet PCI-DSS requirements.

NIST 800-53 SYSTEM AND INFORMATION INTEGRITY (SI) GUIDELINES

NIST 800-53 "Recommended Security Controls for Federal Information Systems and Organizations" lays out a framework for U.S. government agencies to safeguard IT systems. While it was developed for government use, it can be applied to any organization as "best practice" guidelines. Consequently, many commercial organizations have also adopted the framework. SI-7 is one control standard that specifically discusses the need for integrity monitoring while SI-3 and SI-4 also benefit from a FIM solution. All of these sections deal with monitoring the IT environment for changes that could affect security and compromise sensitive information. Other evidence of integrity controls is also seen in Configuration Management (CM), Risk Assessment (RA), Audit & Accountability (AU), Incident Response (IR), as well as a few other domain categories. Of the 1,189 total controls outlined in 800-53, 276 are directly related to integrity management functionality.

SI-7

"Software, Firmware, and Information Integrity Control: The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

"Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3."

THE CIMTRAK SOLUTION

CimTrak is utilized by government agencies and other organizations that follow the 800-53 standards for their IT security program. By monitoring for changes to critical systems and applications and reporting on that information in real-time, organizations can prevent human errors or other malicious activity that can cause disastrous system downtime or lead to a data breach.

CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROLS

CIS has taken 18 control domains that entail a total of 153 control safeguards and prioritized them in terms of the importance of implementation into three implementation groups (IG1, IG2, and IG3). Implementation Group 1 (IG1) is considered the most fundamental safeguards required to operate and mitigate security risks. IG1 is made up of 56 safeguards and of those, 21 pertain to integrity management capabilities.

CIS CRITICAL SECURITY CONTROLS, SECTION 4.1

"Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."

THE CIMTRAK SOLUTION

Both public and private organizations utilize CIS Critical Security Controls requirements as prescriptive guidance to implement security best practices. CimTrak provides a controlled, automated scan or enables a process, procedure, or policy to assist with the evidence collection to meet the objective of 43 of the 153 total safeguards within the 18 control families.

Secure Configuration of Enterprise Assets and Software
Application Software Security
Network Monitoring and Defense
Data Protection
Data Recovery
and others…

NERC-CIP

Section 010 of the North American Energy Reliability Council's Critical Infrastructure Protection standard requires that configuration changes to power grid systems be detected. This is commonly done by using a file integrity monitoring tool to develop a baseline from which deviations are noted and alerted upon.

CIP – 010

1.1 The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version) intentionally installed;

1.1.3. Any custom software installed;

1.1.4. Any logical network accessible ports; and

1.1.5. Any security patches applied.

1.2 Authorize and document changes that deviate from the existing baseline configuration.

1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

THE CIMTRAK SOLUTION

You can find CimTrak deployed by energy companies throughout the United States and Canada, monitoring their critical cyber infrastructure including servers, workstations, and network devices for changes that could disrupt power generation or transmission.

MOVING BEYOND FIM TO SYSTEM INTEGRITY ASSURANCE

As more and more firms deploy them, traditional FIM tools and solutions have been unsuccessful in their objective of providing any form of integrity at all. The acronym of FIM is very misleading as there is no "Integrity" in the detection of change. It's all the collective functionality that surrounds the detection of change that enables you to achieve a desired state of trust and confidence through integrity management.

If FIM tools did what they were intended to do, they would help cybersecurity teams identify, protect, and detect most attacks—at least those that target the workload layer—rely on file changes or access. But, as most security professionals already know, FIM tools don't do what they are meant to do. Here's why:

NOISE A typical 'FIM' tool simply monitors files for change and produces alerts—lots of alerts. They produce so many alerts that they often become 'shelfware' for most cybersecurity teams.

LACK OF CONTEXT Typical 'FIM' tools provide a massive list of changes without any context or distinction. This list is too large to triage, so cybersecurity teams typically ignore these change alerts.

TOO RESOURCE INTENSIVE Most FIM tools identify the change by completing daily polling scans of all files in an IT environment. This process is hugely resource-intensive, so it usually happens overnight. While it would be more valuable to scan the environment continuously, this is impossible, as it would interfere with other IT operations.

To better assist in the differentiation between traditional FIM and System Integrity Assurance, the following table highlights the significant differences.

FUNCTIONALITY	FIM	SYSTEM INTEGRITY ASSURANCE	ACTION
Change Detection	✓	✓	Detect
Attributes Beyond Simply Files		✓	Protect
System Hardening & Benchmarks		✓	Protect
Configuration Management		✓	Protect
Change Management		✓	Protect
Change Reconciliation		✓	Respond
Rollback & Remediation		✓	Recover
Change Prevention		✓	Protect
Side-by-Side File Comparison		✓	Respond
File Allowlisting		✓	Detect
File Reputation Service(s)		✓	Detect
STIX & TAXII Feed(s)		✓	Detect
Workflow & Ticket System		✓	Protect/Detect/Respond/Recover
Compliance Mappings & Enforcement		✓	Protect/Detect/Respond/Recover

THE CIMTRAK SOLUTION

CimTrak assesses an infrastructure's risks and vulnerabilities by utilizing various controls to determine when unknown, unexpected, and unauthorized changes occur and can roll back those changes either manually or automatically. These unknown changes are the result of either a security incident or a circumvented process. Either way, CimTrak can identify in real-time and take corrective action to ensure a resilient infrastructure.

CimTrak's continuous configuration compliance module provides a further assessment of risk and vulnerability by utilizing CIS Benchmarks and DISA STIGs to determine if systems and devices are configured to industry best practices. Furthermore, CimTrak takes the CIS Benchmarks and DISA STIGs and maps them to leading compliance mandates as a reference point and evidence to determine if a particular compliance control passes or fails. If a system fails a compliance scan, CimTrak provides the necessary guidance to fix and remediate failed scans. Minimizing risk and vulnerabilities in real-time drastically reduces the risk of security breaches and improves the ability to pass compliance audits.

BRINGING INTEGRITY TO YOUR ENVIRONMENT (NOT JUST FILES)

Integrity is the accuracy and completeness of data throughout its entire life cycle. That means no matter what service, device, or user accesses, stores, processes, transmits, or receives data, it remains accurate and complete. For this to be possible, four things are needed:

1. An authoritative baseline of what data should look like.
2. A way to identify and protect data from unauthorized change.
3. A way to roll back unauthorized changes not blocked at the source.
4. A way to verify that controls 1 – 3 are in place and working correctly.

Notice we're talking about data, not just files. To have integrity, you need to protect all of the data in your environment—including data held in configuration files, network devices, users, groups, policies, active directories, database schemas, hypervisors, container orchestrations, cloud configurations, and more…

THE CIMTRAK SOLUTION

WORKING FROM A TRUSTED BASELINE

Working from a trusted baseline includes all of the assets, file hashes, configuration settings, etc, allowed to exist in an environment. CimTrak leverages best practices from authoritative sources such as CIS Benchmarks and DISA STIGs to establish a known and trusted baseline.

VERIFYING INTEGRITY

CimTrak monitors changes in real-time and responds instantly to unknown/unwanted/unexpected changes. This proactively detects cyberattacks at the source without restricting operations to reactive threat feeds.

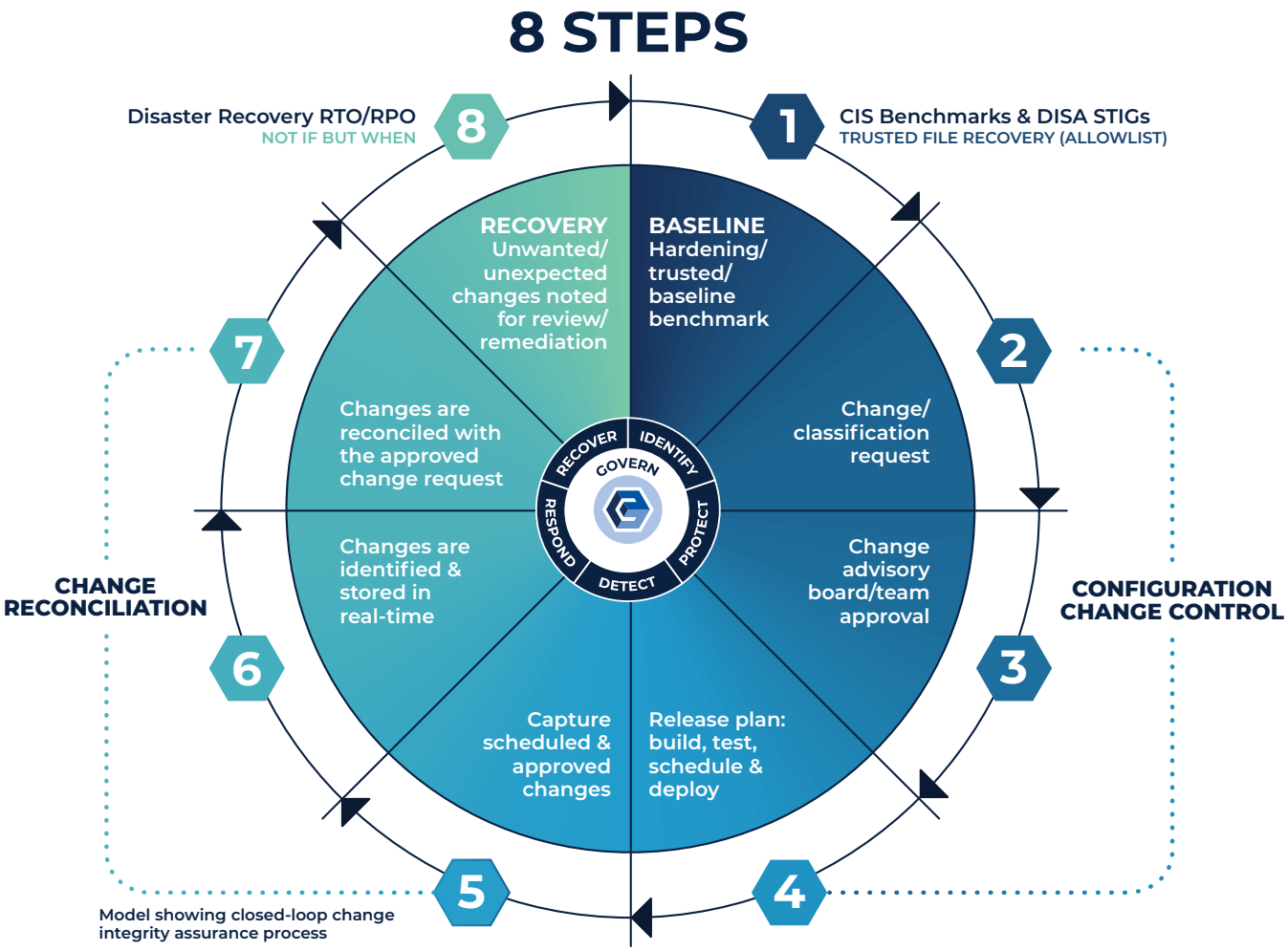
COMPLETE CHANGE DETAIL

CimTrak pinpoints exactly what has changed and provides complete change audit information. Forensic details provided with changes include; WHAT exactly changed, WHEN it was changed, WHO changed the information, HOW it was changed, and the PROCESS in which it was changed.

SYSTEM INTEGRITY ASSURANCE

System integrity assurance works under the same principle as physical security. It establishes a known, trusted, and authoritative baseline of what is allowed and then prevents, limits, or rolls back any unauthorized change (malicious or circumvented). The change is then highlighted for review and action is required.

System Integrity Assurance can be demonstrated as the following workflow:



This is a closed-loop process for managing changes from a trusted baseline. Similar to the change management procedures articulated by best practices of ITIL, NIST, CIS, and other frameworks, this process covers all stages needed to ensure only acceptable changes are allowed to proceed, while others are prevented or rolled back.

KEY QUESTIONS FOR EVALUATION

» Is the solution capable of truly real-time detection?

» Is the solution easy to install, configure and use?

» Does the solution only log file changes or does it have other capabilities?

» Does the solution give you important information regarding changes such as who made the change, what process was used, and the originating IP address of the change?

» Can the solution show you exactly what within a file was changed, giving you a side-by-side comparison with the original file?

» Does the solution integrate with other solutions such as SIEMs and ITSM frameworks?

» Is the solution capable of providing a holistic look at change across your IT environment, or does it only monitor file changes?

» Can the solution differentiate between “good” and “bad” changes, allowing you to focus your attention on those that are most critical?

» Does the solution have centralized policy management and reporting?

» Does the tool have a simple methodology for reconciling changes in your infrastructure?

» Does your FIM tool have the ability to restore to previously trusted baselines?

» Does your FIM utilize Benchmarks and STIGs for system hardening?

» Can your FIM digest allow lists, file reputation services, or STIX/TAXII feeds?

» Can your FIM prevent changes from occurring, even with system admin privileges?

File Integrity Monitoring plays a critical role in maintaining the security, integrity, and compliance of your organization’s IT assets. By providing you with key information on changes, file integrity monitoring allows you to be aware of and react to changes quickly and efficiently. Understanding how various solutions differ is the first step in finding and implementing a solution that meets your needs.

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