CIMCOR

File Integrity Monitoring for PCI DSS in 3 Easy Steps

CimTrak is an advanced file and system integrity monitoring platform offering real-time change detection capabilities that map and align with nearly half of the PCI DSS technical requirements. Many PCI environments lack integrity management because it is often perceived as being too expensive, too hard to install and manage, and produces too much "noise."

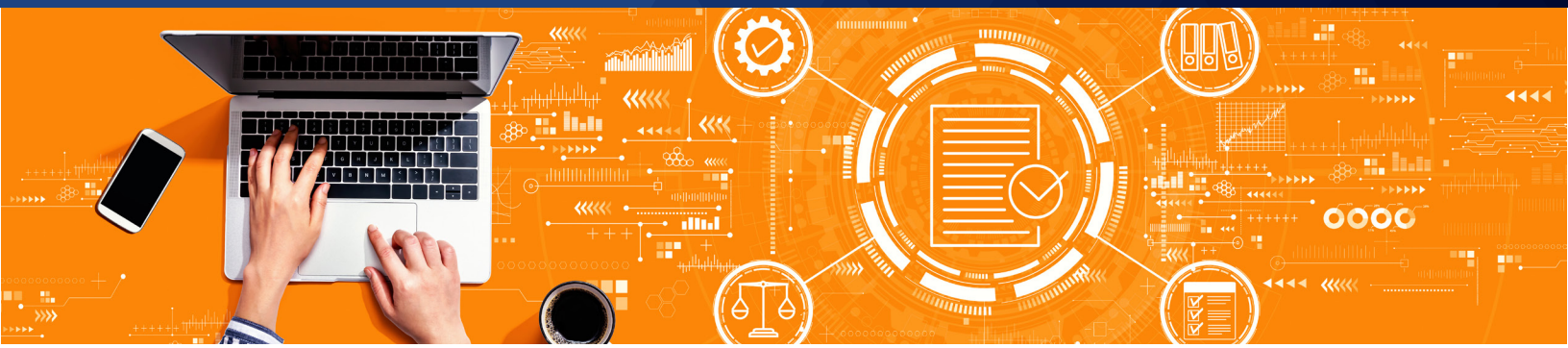
PCI DSS and file integrity monitoring fit together like a hand and glove. Sections 10.5.5 and 11.5 are perfect examples where change detection controls are identified and required:

PCI DSS 11.5

"Deploy file integrity monitoring software to alert personnel to unauthorized changes of critical system files, configurations files, or content files; and configure the software to perform critical file comparisons at least weekly."

PCI DSS 10.5.5

"Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be altered without generating alerts ..."



Security professionals know unexpected changes can mean that something bad is happening to your systems. With new forms of malware continuously being unleashed daily, much of it is classified at zero-day, and requires a robust integrity solution to detect such threats.

As these threats are unsignatured, many will find their way through perimeter defenses and attempt to take up residence in your infrastructure. Each day seems to bring news of the latest breach and compromise of payment card data. Proactively being alerted to unexpected and unauthorized changes can mean the difference between eliminating a threat quickly or losing your customer's personal information.

Many people have been fallen victim to the notion that there is only one FIM product on the market. Because of this, organizations suffer through the extremely high costs of ownership and operation, scalability limitations and general complexity believing they have no other available options.

CimTrak Makes File Integrity Monitoring Easy

1. INSTALL

First, install CimTrak on the endpoints you wish to monitor. CimTrak quickly and easily installs on servers, workstations and POS systems and supports a wide variety of operating systems including Windows, Linux, Mac OSX and UNIX

2. SET UP

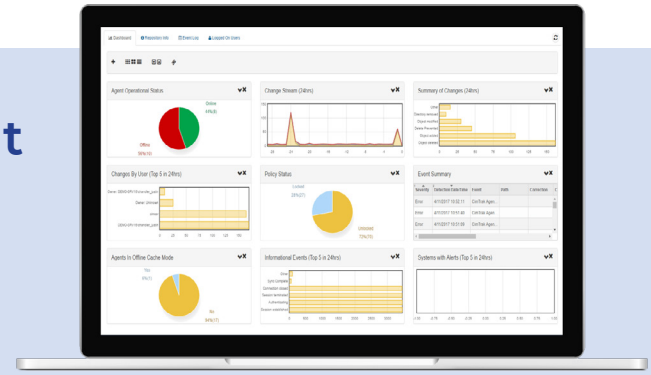
Next, set up policies for what you want to monitor. Don't worry though, it's quite simple. CimTrak includes library of base operating system templates, which you can apply to instantly monitor the underlying critical system files. This means with a few clicks, you are on your way to meeting 50% of the PCI requirements. From there, pick the other files on your systems that are critical to monitor. These are generally files associated with your payment card application and log files within your PCI environment.

3. CONFIGURE/CONNECT

Finally, configure any alerts you would like to receive when unexpected and unauthorized changes occur, and optionally, connect CimTrak to any log management or SIEM solution that you may utilize. With granular user control, you can also set up user permissions to restrict certain operations and/or viewing certain systems or files. And if by chance a change got through by way of accident or malicious activity, CimTrak can manually or automatically roll-back those files/directories/devices back to any number of previous approved and compliance states. That's it, all finished. You are now detecting changes to critical files and logs as required by PCI-DSS!

Try CimTrak In Your Environment With A Free Trial Today

»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 SIEM 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.