PCI DSS: IS YOUR SYSTEM SECURE AND COMPLIANT?

PCI DSS STANDARDS

The Payment Card Industry Digital Security Standards (PCI DSS) were first introduced in late 2004. Since then, there have been several revisions culminating in the latest standard 3.2. The standards focus on specific requirements in twelve areas of a payment card system. The requirements are applicable to any entity that holds, processes, or transfers payment card information. Each of the twelve covered areas focuses on a specific section of the PCI environment.

With the advent of the latest version of PCI DSS, all organizations that process payment cards are required to prove compliance. Many organizations aren't sure how to comply, and even if they are compliant, still fear that something bad can happen. Recent high profile breaches such as Anthem and Target often bring unnecessary fear to those responsible for PCI compliance. When breaches at companies such as these occur, companies that were supposedly PCI compliant, they often fear that their efforts may end up not being enough.

cimtrak
detecting change throughout the enterprise

COMPLETE INTEGRITY MONITORING

CimTrak gives you instant notification and in-depth insight into all changes within your PCI environment and complete coverage for requirement 11.5.

AUTOMATED CONFIGURATION MONITORING

CimTrak allows you to monitor critical configurations to ensure that they are in a PCI compliant state.

COMPLETE PERIMETER PROTECTION

CimTrak monitors devices such as routers and firewalls to ensure that changes don't allow unauthorized access to your PCI environment.

CONTINUITY OF OPERATIONS

CimTrak offers the option to instantly restore changes, keeping your critical systems running.

COMPLETE LOGGING/REPORTING

CimTrak provides a wide variety of reports on watched systems and seamlessly integrates with all major SIEM solutions.

GETTING COMPLIANT WITH PCI DSS

Certainly, there are a large variety of products available that promise to assist with your PCI compliance efforts. The sheer volume of products can be overwhelming. Of course, given the complexity of PCI DSS, no one product can ensure compliance. Many products however claim to keep you PCI compliant, but can they? Given that breaches have occurred at firms that at one point in time had been certified as PCI compliant, the answer is certainly no. So how do you ensure the security of your PCI environment given this reality?

Compliance with PCI DSS should be viewed as a temporary condition, a “snapshot” of your systems at a given moment. PCI Compliance is subject to change at any moment. Much to their chagrin, many organizations have learned this lesson the hard way. PCI solutions often fall short because while they can show that the environment is compliant at one point in time, they have no ability to assure that the compliance in continual. The key is once you have employed various tools to get your PCI environment into a known good state, you do everything possible to prevent changes that will alter that state.

MAINTAIN CONTINUOUS COMPLIANCE WITH CIMTRAK

CimTrak is a unique solution for your PCI environment. An advanced integrity and compliance tool, CimTrak not only detects and notifies you of changes, but also has the ability to instantaneously revert changes that may occur. This ensures that compliance in continual. Once you have established your known good state, you can ensure that your system stays that way. When a change is detected, CimTrak not only instantly alerts you to the change, but also can instantly take action to remediate the change, up to and including restoring a file or configuration back to its original state.

PCI DSS 3.2 REQUIREMENT	HOW CIMTRAK HELPS
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	CimTrak monitors a wide range of network devices for changes and provides an immediate alert should a change occur. By detecting changes that deviate from a known good state, accidental or malicious changes can be detected before they allow your PCI environment to be compromised.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	CimTrak checks anti-virus and system configurations to ensure that they comply with established security benchmarks and alerts you should a system deviate from the baseline.
Requirement 3: Protect stored cardholder data	CimTrak can detect and alert you to changes to cryptographic files and keys, data files, as well as database tables and schemas.
Requirement 5: Use and regularly update anti-virus software or programs	CimTrak complements anti-virus or other malware preventing technologies by acting as a last line of defense. With the proliferation of malware, threats are constantly changing. CimTrak can detect changes caused by malware that may not yet be signatured and thus bypass your other network defenses.

PCI DSS 3.2 REQUIREMENT	HOW CIMTRAK HELPS
Requirement 6: Develop and maintain secure systems and applications	CimTrak can check to ensure that systems have current patches installed as required by PCI DSS 6.1. Further, CimTrak is an integral part of change control for systems within the PCI environment. By detecting changes and keeping a secure log, a record of all changes can be kept and reviewed as needed to ensure that all specified changes have in fact occurred and are appropriate. This greatly minimizes internal threats caused by unauthorized or malicious changes.
Requirement 8: Assign a unique ID to each person with computer access	CimTrak ensures that system configurations relating to passwords and user authentication as well as system lock-out are maintained in a known good state based on established security benchmarks.
Requirement 10: Track and monitor all access to network resources and cardholder data	CimTrak collects and retains logs on all system changes as required by requirement 10 of the PCI DSS. Further, it stores these logs securely in the CimTrak database to protect them from unauthorized modification as required by PCI DSS requirement 10.5.2 and limits viewing to only authorized individuals as required by requirement 10.5.1. Additionally, CimTrak provides forensic details associated with each change as indicated in PCI DSS requirement 10.3 and ensures that critical system clocks and time protocols are enabled and synchronized so that accurate audit trails can be established.
Requirement 11: Regularly test security systems and processes	CimTrak is an advanced file integrity monitoring (FIM) solution combining instant detection and notification of changes with the ability to take instant, automatic remediation actions and fully meet PCI requirement 11.5. CimTrak can monitor a wide range of items including configurations, applications, registry settings, drivers, executables, as well as local security policies for changes that can allow a breach of sensitive PCI data. Further, CimTrak can allow you to maintain a strong security posture by acting as a last line of defense in your IT environment. With the ability to instantly restore changes, CimTrak can effectively prevent harmful intrusions that can compromise your PCI environment.
Requirement 12: Maintain a policy that addresses information security for employees and contractors	CimTrak provides instant alerting as well as a secure audit trail with forensic details upon detection of system changes. This is critical to ensuring the security of the PCI environment and is required to be a part of and organization's incident response plan by PCI DSS requirement 12.9.5. Further, CimTrak has the ability to instantly restore changes, effectively preventing critical incidents. Additionally, CimTrak has the ability to quickly roll-back to a previous known good state. This allows for quick recovery of systems should an incident occur.

"As a Level 1, PCI-compliant gateway service provider, we process millions of dollars in credit card and ACH transactions each year. Our file integrity solution must be flexible, expandable, and more importantly, effective at monitoring changes to our critical systems. When our client's money is on the line, we don't have the luxury of waiting several hours to be notified that we have been hacked. CimTrak provides us instant notification and even gives us the ability to automatically restore files that may have been changed or deleted without authorization. It's not just file integrity, it's business integrity."

~Global E-Commerce Provider

CIMTRAK FITS YOUR IT ENVIRONMENT

CimTrak covers many components of a payment card system including servers, network devices, critical workstations, and point of sale (POS) systems. Whether you are a large payment processor or a small merchant, CimTrak has a solution to meet your needs! More importantly, CimTrak is easy to install, configure and use, so you don't need expensive services to quickly get it running nor does your IT staff need to spend large amounts of time with tedious and confusing configurations. By providing key insight into your IT environment, personnel can pinpoint issues and react quickly, maximizing time and saving money.

CimTrak is always on call. Whether it is three a.m. or three p.m., you can be assured that your PCI environment is in a constant state of integrity and compliance. It's why enterprises and government agencies rely on CimTrak to ensure integrity and maintain compliance with regulations such as PCI-DSS.

CIMTRAK IS SECURITY

CimTrak has been built with the stringent needs of government customers in mind. CimTrak has been certified to Common Criteria EAL Level 4 + FLR, the highest government certification for a software product. In addition, the CimTrak cryptographic module has been certified to meet the Federal Information Processing Standard (FIPS) 140-2. 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.