File Integrity Monitoring - The Last Line of Defense in the PCI Data Security Standard

A New Net Technologies Whitepaper

MARK KEDGLEY

CTO, New Net Technologies

www.nntws.com

NNT
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

Which Tier or Level Merchant are You?

The PCI DSS is applied to all payment card merchants, but the Validation Requirements vary according to transaction volumes:

***Tier 1**: The highest volume merchants, which submit 6 million or more transactions per year.*

***Tier 2**: Merchants that submit 1-6 million transactions per year.*

***Tier 3**: Merchants that submit between 20,000 to 1 million e-commerce transactions per year.*

***Level 4**: Merchants submitting fewer than 20,000 e-commerce transactions per year, and all other merchants processing up to 1 million transactions per year.*

File Integrity Monitoring and the PCI Data Security Standard

Has there ever been a more confusion-generating initiative than the PCI DSS? Even now, nearly fifteen years on from its initial introduction, a clear and definitive understanding of what your organization needs to do may still be a challenge.

Tier 1 Payment Card Merchants will now be entering their second cycle of building a PCI DSS solution and reviewing any investment in monitoring tools they made when they first became subject to the standard.

Tier 2 Payment Card Merchants will be self-certified PCI DSS Compliant, but many will be contemplating their first external QSA audit as they mature in their PCI DSS compliance journey.

This whitepaper focuses on one dimension of the security standard that is often the last one to consider and tackle - File Integrity Monitoring.

"Get Rich, or Die Tryin'"

The importance and understanding of why File Integrity Monitoring (FIM) is a vital component for securing payment card and card holder details has come sharply into focus following the well-publicized Heartland Payment Systems and TJX security breaches masterminded by the notorious Albert Gonzalez and his "Get Rich, or Die Tryin'" plan to steal payment card details. If ever there was a movie waiting to be made about a computer hacker, this is it – see the Miami Herald 'From Snitch to Cyberthief of the Century'.

> *"Highlights are the throwing of a $75,000 birthday party for himself, counting $340,000 by hand because his counting machine broke down, and the theft of millions of credit card numbers used to steal millions of dollars."*

How Does File Integrity Monitoring Help?

FIM verifies that program and operating system files have not been compromised.

Why is this important? The principal benefit of using FIM technology is to ensure that malicious code has not been embedded within critical application and operating system files. The insertion of a 'backdoor' or Trojan into core program files is one of the more audacious and elegant forms of hacking, and also one of the most dangerous.

Likewise, configuration files that govern the security and function of systems will also need to be tracked for any changes. This includes firewall rule files, router running configurations, and of course, significant Linux/Unix/Solaris files such as /etc/hosts.allow and hosts.deny, for example.

Executed properly, card details can be siphoned off with ease. The Albert Gonzalez case is the most high-profile, but by no means unique.

"All the firewalls, Intrusion Protection Systems, Anti-virus, and Process Whitelisting technology in the world won't save you from a well-orchestrated internal hack where the perpetrator has admin rights to key servers or legitimate access to application code - File Integrity Monitoring used in conjunction with tight change control is the only way to properly govern sensitive payment card systems"

File Integrity Monitoring and the PCI Data Security Standard

The PCI DSS (Payment Card Industry Data Security Standard) specifies the following

Requirement 11.5 "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)"

However, Requirement 1 specifies *"maintain a firewall configuration to protect cardholder data"*, Requirement 2 *"Do not use vendor-supplied defaults for system passwords and other security parameters"*, Requirement 6 *"Develop and maintain secure systems and applications"* and in fact, the need to track and assess the impact on IT system security is at the heart of any Security Standard or Policy like the PCI DSS.

Host integrity monitoring software serves as an essential early-warning system and can provide the first indication of a break-in or compromised host.

When properly configured and deployed, this type of software is a powerful addition to the layers that defend your infrastructure in depth.

As a minimum, for any Windows devices 'touching' cardholder data, including EPoS equipment, the System32 and/or SysWOW64 folder should be governed as well as key application program folders.

It is important to verify all adds, changes, and deletions of files as any change may be significant in compromising the security of a host. Changes to monitor for should be any attribute changes and the size of the file. Remember, trojans are designed to impersonate existing system files and will always 'look' and usually behave like the genuine exe, dll or driver file, albeit with some nasty extra functions too!

Similarly, for Linux and Unix hosts, the /etc/ and /usr/bin/ directories and their constituent files must be tracked for integrity together with all relevant application binary and configuration files.

File Integrity - Guaranteed

However, since we are looking to prevent one of the most sophisticated types of hacks, we need to introduce a truly infallible means of guaranteeing file integrity. This calls for each file to be 'DNA Fingerprinted', typically generated using a Secure Hash Algorithm. A Secure Hash Algorithm, such as SHA1 or MD5, produces a unique, hash value based on the contents of the file.

The concept, therefore, is that a file integrity baseline must be established. Any file-integrity monitoring system works by comparing file attributes, filesizes, and hash signatures from one time to another. The assumption, therefore, is that the initial baseline is for a vulnerability-free, completely uncompromised host and application.

This means that even if a program is modified to expose payment card details, but the file is then 'padded' to make it the same size as the original file and with all other attributes edited to make the file look and feel the same, the modifications will still be exposed.

The schematic on the next page illustrates how such an algorithm generates a unique hash for a file.

File Integrity Monitoring and the PCI Data Security Standard

The diagram in Figure 1 shows how the SHA1 secure hash algorithm generates a distinctly different hash value even for the smallest change to the data within a file. This provides a unique means of verifying that the integrity of a file has been maintained.

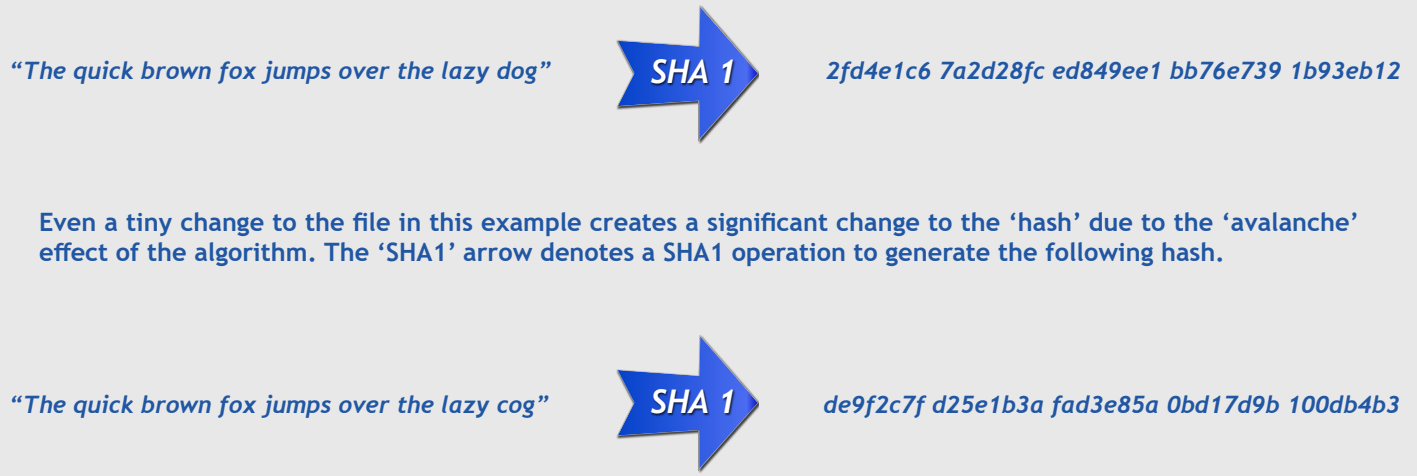


Figure 1 - Illustration of how a secure hash algorithm creates a unique 'hash' based on the contents of a file

The Problem with File Integrity Monitoring?

The main problem with using a secure hash algorithm for FIM is that the processing of files in order to generate the hash is processor intensive. This means that in most implementations of FIM the check can only be performed once a day, outside of business hours.

The other problem with FIM is that you may have several different operating systems and platforms to monitor. The numerous variants of Linux and Unix/Solaris present a number of challenges and the combination of text-based configuration files and binary program files mean that a combination of agent-based and agentless FIM technology will be required. Windows OS components provide the basis for FIM, but identifying 'Who Made The Change?' will require specialized, third-party technology.

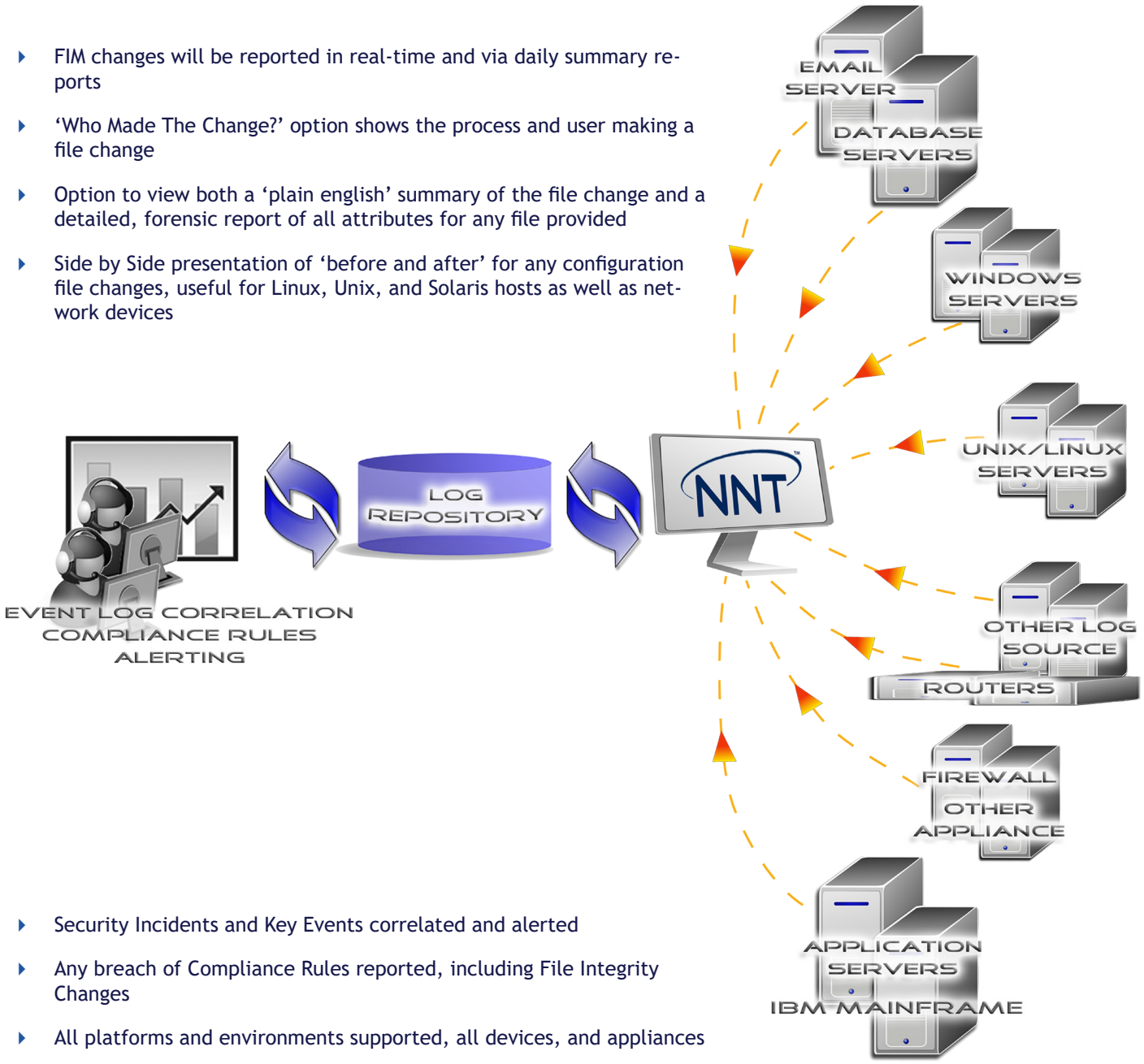
In both instances for Linux/Unix/Solaris and Windows, the need to filter changes based on file types, application type, and/or location is essential to avoid spurious alerts for files that regularly change or are simply not relevant in this context e.g. log files and database files will always be changing, while executables/binaries will only ever change during an update/upgrade, similarly, image files and content on a website will change often, while configuration and program files should be fixed.

Furthermore, the scheduling, alerting, and reporting of file integrity changes must in itself be a manageable and automated process.

Footnote: SHA1 and MD5 are both, theoretically at least, not infallible as encryption algorithms and have been shown to be breakable, hence a SHA2 algorithm is being developed by the NSA. However, in this application (i.e. as a means of determining file content integrity), both are ideal tools for the job.

What Do NNT Provide?

- FIM changes will be reported in real-time and via daily summary reports
- 'Who Made The Change?' option shows the process and user making a file change
- Option to view both a 'plain english' summary of the file change and a detailed, forensic report of all attributes for any file provided
- Side by Side presentation of 'before and after' for any configuration file changes, useful for Linux, Unix, and Solaris hosts as well as network devices



- Security Incidents and Key Events correlated and alerted
- Any breach of Compliance Rules reported, including File Integrity Changes
- All platforms and environments supported, all devices, and appliances
- Planned Changes and all Unplanned Changes are detected
- Device Hardening Templates can be applied for all Security and Governance Policies, providing a fast Compliance Audit of all Devices

About NNT

NNT Change Tracker Gen provides continuous protection against known and emerging cyber security threats in an easy to use solution, offering true enterprise coverage through agent-based and agentless monitoring options.

- NNT analyzes every configurable component within your IT Estate and allows you to define a 'Known, Good, Secure and Compliant State' for all of your in scope systems.
- NNT-Change Tracker scans your devices and compares them to a standard policy, either user defined or based on an industry standard such as the Center for Internet Security (CIS).
- Policies can be automatically assigned based on the device type or priority via a centrally managed console.
- Gen7 is able to fully automate change approval for you, using the NNT FAST (File Approved-Safe technology) that combines unique intelligent change control knowledge base and whitelists.
- With NNT's real-time capabilities, unlike traditional scanning or exclusively agentless technologies, potential breaches to systems or policies are spotted immediately.

NNT Change Tracker Gen 7 helps you to prevent security breaches of your systems by providing you with a powerful feature-rich, easy to use and affordable solution for validating, achieving and maintaining compliance with corporate governance or security standards.

www.nntws.com

UK Office - Spectrum House,
Dunstable Road, Redbourn,
AL3 7PR
Tel: +44 8456 585 005

US Office - 9128 Strada Place,
Suite 10115, Naples, Florida
34108
Tel: +1-888-898-0674

Conclusion - The NNT View

As the familiarity and understanding of the PCI DSS matures, so will the expectation levels increase for all payment card merchants of all levels/tiers to implement every technological security measure available.

Delivering a pragmatic response to the need for file integrity monitoring across all platforms that is effective, easy to deploy and manage and, above all, affordable, will continue to pose a challenge.

NNT can help – using our Change Tracker Gen7 and Log Tracker Enterprise solution set will provide everything that a Payment Card merchant needs to become, and remain, PCI DSS compliant.

NNT PCI DSS Compliance solutions cover the following

- Configuration Hardening
- Change Management
- Event Log Correlation
- File Integrity Monitoring

NNT Change Tracker and Log Tracker Enterprise - Compliance Clarified

- Compare Audited Settings against Policy - Configuration settings are assessed for compliance with any policy or standard relevant to your organization and deviations highlighted.
- Continuously Monitor Configuration Settings - Configuration attributes are then monitored continuously for all changes, both from a compliance standpoint and from a general change management/control standpoint.
- Change Management Process Underpinned - Authorized changes which have been approved via the formal change management process are reconciled with the original RFC to ensure the correct changes were implemented accurately.
- The Change Management 'Safety Net' - Unplanned changes are flagged up for review immediately to mitigate security integrity or service delivery performance.
- Real-Time FIM with 'Who Made the Change?' for Windows, Linux, Unix and Solaris hosts tracked for both binary program, and text-based, configuration files.
- SIEM Event Log Correlation - Centralize and correlate event logs messages from all Windows, Unix/Linux, firewall and IPS systems.

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com