NonStop File Integrity: Check It! Protect It!

Callum Barclay, CTO, CSP

File Integrity Monitoring on NonStop

File Integrity Monitoring (FIM) is an important requirement of the PCI data security standard for maintaining confidential (e.g. cardholder) information, and is considered a crucial part of protecting business assets.

NonStop systems are now being used in far more dynamic situations and have more external connections than ever before. The ubiquity of payment cards for personal electronic transactions has changed the security equation in a fundamental way.

Any compromise in security is likely to have far reaching consequences, both for the immediate damage that may be done in terms of financial loss, and for the wider damage done to a merchant's reputation. The security of personal cardholder information has become paramount.

In this context, FIM should be considered an important security necessity, not just for PCI systems, but for all NonStop systems.

FIM and PCI DSS

PCI DSS Requirement 11.5 stipulates that members must " Deploy a change-detection mechanism (for example file-integrity monitoring tools) to alert personnel of unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform the critical file comparisons at least weekly."

In version 2.0 of the security standard, in a clarification to Requirement 11.5.b, it was further specified that it is an audit requirement to "Verify that tools are configured to alert personnel to unauthorized modification of critical files."

PCI DSS Requirement 11.5 version 3.1 further clarifies that unauthorized modifications include changes, additions, and deletions of critical systems files.

It is clear from these excerpts that FIM is a key requirement of PCI DSS, and therefore a FIM solution must be implemented on any system that handles cardholder information.

What is FIM?

FIM includes any technology that monitors files for changes. Assuming that at least some file change is expected on a system, then FIM's primary purpose should be to identify possible "bad" changes so that they can be rolled back or remediated in some way. A "bad change" is any change that is undesirable. This is not the same as an unplanned, unauthorized or suspect change.

An unplanned change is not necessarily a "bad" change. Most system administrators have found it necessary to intervene on occasion to remedy a problem. Their actions might include changing a configuration parameter, or perhaps changing the security of a file due to an oversight.

In both cases, the change is both unplanned and unauthorized. Regardless, the change must be appropriately recorded and reported, then reviewed and either made permanent or modified.

Of course other changes that may be unplanned and unauthorized can be part of an active security threat, in which case FIM may provide the first notice that the system has been compromised. Accidental change represents no less of an issue and is probably the most likely source of unplanned and unauthorized change.

FIM can also be used as part of a change control regime, whereby planned changes are detected and recorded to have occurred as expected.

Components of FIM

Basic FIM functionality should allow the administrator to:

1. Create and store a baseline for specified files and their attributes of interest
2. Update the baseline to take into account planned or allowable change
3. Run periodic checks and report the results
4. Store the results of each check

What to monitor?

A major concern is that FIM generates "noise" about file changes. Too much activity is recorded on too many files. Like excessive audit, excessive FIM can result in a reduction of useful information.

An effective FIM solution must therefore provide flexible integrity check mechanisms able to select files based on name and property. In deciding what files should be monitored, judgment is needed to determine the risk created by a change to a file.

Obvious monitoring choices would include system files. Files which are LICENSE'd or PROGID'd would also be candidates.

Added to these would be key application files, including data, executables and configuration files.

Other files should be added as required. Any files related to cardholder data are especially sensitive. While a file's contents may be dynamic, other file attributes can be monitored to ensure that the correct attributes are in place and remain so.

Types of change

The FIM solution should allow for the specification of different types or categories of change, for example:

- Content, both complete and incremental
- Security settings, including flags for ownership, file permissions and special security bits
- Basic attributes like file type, last modified etc.

Grouping checks by change type simplifies both the scheduling of checks and the review of the results.

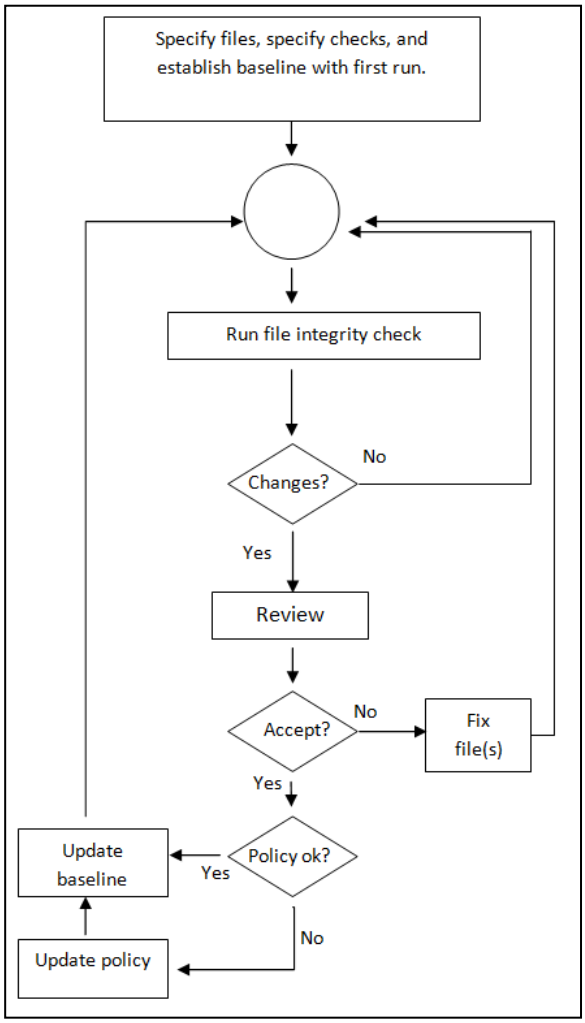
Low and high risk changes

As noted, a significant challenge is presented by the potential quantity of change notices that can accumulate. To counter this problem the FIM solution should be configured so that it supports the appropriate specification of risk for each file.

For example, a file may represent a risk if compromised and may also have relatively dynamic content. Monitoring for content change is therefore not useful. It is better to look at the attributes that directly impact the risk-level and monitor for those. These are most likely to be security settings.

Grouping files into filesets based on their risk profile is therefore recommended.

Typical FIM workflow:



Change notification

When the FIM has completed its check, there should be a way to quickly identify any changes that have occurred, since trawling through lengthy detail reports could lead to oversights.

Ideally, an exception report could be created that feeds into a central event management system, in order to ensure that all high-risk changes are considered collectively, and are acted upon promptly.

Real-time alerts

Some files are too sensitive to wait for changes to be analyzed. In this case, event monitoring solutions can be used to immediately invoke both notifications (alerts) and investigative or remedial actions.

Certain changes will also be recorded in the Safeguard audit trail, e.g. security setting modifications. These can also be detected in real-time by event monitoring solutions and made actionable.

Change analysis

As each monitoring cycle is completed, any changes should be reviewed. The number of changes to be reviewed must be manageable. For some filesets the cycle will occur daily, for others weekly or monthly.

Advanced FIM solutions provide the ability to check multiple filesets, enabling the verification of groups of critical files more often (i.e. daily), and less critical files less often, (i.e. weekly).

Files that have been marked as changed in one of the specified attributes should be reviewed by the individual responsible for the contents or the attributes of the file. If, after review, the change is acceptable, then the baseline for that file is reset immediately. Otherwise, further investigation is required.

Change history

The results of each monitoring cycle should be stored. Information should include the details of the change so that there is a complete record of all changes. Such information can be correlated with audit records to determine who made the change.

Unauthorized, unplanned or suspicious change

If detected changes are not promptly analyzed, the value of FIM rapidly diminishes. The purpose of the analysis should be to establish quickly as possible that the change should either stand or be rolled back.

Unauthorized or unplanned change is not necessarily undesirable change – such as an emergency change made to remedy a production problem. By the same token, change that is authorized may turn out to be bad change. FIM solutions should save all change information for possible future remediation.

Suspicious change is simply change that has not been categorized for acceptance or rejection. Hence, the need to analyze change information as quickly as possible in order to identify it as good or bad.

Once a change is identified as "good", then a new baseline is set for the file in question.

Change Approval

If a change has been identified as "good" and the baseline must be reset, it is important to require that the reset is properly approved. Otherwise the temptation to let "ok" changes roll through will be hard to resist, particularly in busy environments.

Any update to the baseline should therefore be separately authorized using an additional level of authentication requiring the entry of a special PIN.

Multi-Node File Compare

FIM solutions should also have the ability to compare files on different nodes, e.g. between production and disaster recovery systems. This is to ensure that no unwanted or unauthorized changes occur during the synchronization of files between systems. A record count difference threshold should be used to reduce false positives due to latency across nodes.

Integration with other security products

The significant quantities of data that can be generated by FIM solutions can be more easily managed by integration with other security products, in particular with auditing and event monitoring solutions.

Not all file changes represent equivalent risk. By developing mechanisms to extract high risk file changes and make them part of a broader event monitoring effort for similar security events (attempted breaches, logon attacks etc.), users can make FIM significantly more effective.

Correlating such file changes with other suspicious activity will also become easier – allowing security administrators to provide a more complete view of activity that may threaten to compromise the system.

Conclusion

FIM is a critical requirement for security, and key to PCI DSS compliance. However, the detection of any particular change is just the start of the process.

To be effective, FIM solutions must differentiate low-risk from high-risk change; integrate with other security solutions for log and security event management (including real-time alerts) and support a fully-managed history database of changes.

CSP's File Integrity Checker (FIC) is widely used by financial institutions to deliver FIM in NonStop Guardian and OSS environments, and is tightly integrated with CSP's other solutions for audit, compliance and Safeguard, EMS and Base24 OMF real-time event monitoring. FIC's new "Guardian Fileset Compare" feature permits the attributes of any two file sets on any two systems to be compared against each other. Find out more at www.cspsecurity.com.