File Integrity Monitoring (FIM) coverage for PCI DSS 4.0

FIM mapping to PCI DSS 4.0 FIM specific requirements

PCI DSS Requirement	Requirement Description	Coverage by Qualys FIM	Qualys Response
10.2.1	Audit logs are enabled and active for all system components and cardholder data.	Yes	All critical system components are marked for real time monitoring under predefined monitoring profiles provided by Qualys FIM Library
10.2.1.1	Audit logs capture all individual user access to cardholder data.	Yes	Complete 'who-data' i.e., user and process details, responsible for the change event, are captured in realtime.
10.2.1.2	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Yes	Alerts are generated for change events by privileged accounts which can be further correlated to create an automated incident.
10.2.1.3	Audit logs capture all access to audit logs.	Yes	Changes to log file security settings or removal of log files triggers real time alerts, with exhaustive event details

10.2.1.7	Audit logs capture all creation and deletion of system-level objects.	Yes	All creation and deletion activities are captured provided that entity is under monitoring radar
10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	Yes	All the event details mentioned in the requirement are captured in real time by Qualys FIM.
10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	Yes	Qualys FIM makes sure that log file integrity modifications are captured in real time. However following is our recommendation for monitoring of log files: Since log files are changing almost in realtime, content change monitoring of log files is not recommended, as it is prone to Noise. Log files should instead be monitored for changes in security settings i.e., permissions or ownership modification. Real time alerts should be generated whenever a log file is deleted.

10.4.1.1 New Requirement	Automated mechanisms are used to perform audit log reviews.	Yes	Qualys FIM supports both, manual and automated. incident generation and review process.
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Yes	Qualys FIM has data retention policy of 13 months
10.7.2 New Requirement	Failures of critical security control systems such as change-detection mechanisms are detected, alerted, and addressed promptly.	Yes	Qualys FIM has a provision to generate automated reports for hosts where change detection mechanism i.e., FIM is not working. We not only check if FIM is deployed and activated; we also check the current state of FIM process on each host and generate on-demand and scheduled reports for non-compliant assets i.e., assets on which FIM was activated but not currently running. Such expanded visibility and documentation keeps your organization Audit Ready.

11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly. Applicability Notes For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	Yes	Qualys' in-house security analysts, with their deep insight and rich subject-matter expertise, provide out-of-the-box FIM profiles (policies) to monitor highly critical files, registry objects, and actions. Qualys FIM Profiles for PCI DSS contains all the critical files as prescribed by PCI DSS.

12.10.5	The security incident response plan includes monitoring and responding to alerts from Change-detection mechanisms for critical files.	Yes	Automated Incident management is supported by Qualys FIM
A3.5.1	A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. • Response to alerts in accordance with documented response procedures	Yes	With Qualys FIM, you can quickly find unauthorized changes and leverage threat intelligence to find malicious or suspicious events from unauthorized change events. For example, use a query like this: not (actor.userName:'NT AUTHORITY' or actor.userName:`root`) and (reputationStatus:MALICIOUS or reputationStatus:SUSPICIOUS).

Key Focus Area - Noise Cancellation

As per Guidance for Requirement 10.3.4, FIM solution should monitor files that do not regularly change, and new log data being added to an audit log should not generate an alert.

The objective is to reduce noise as a FIM solution is applied to files that undergo frequent changes, such as log files, configuration files, or temporary files, and may generate a large number of alerts, leading to noise or excessive notifications. This can make it difficult for

administrators or security teams to distinguish between legitimate and potentially malicious changes.

How can Qualys help?

The Qualys FIM solution provides a finely tuned library of critical file paths to be monitored in order to reduce noise.
By leveraging these library paths, administrators can benefit from preconfigured monitoring settings that are tailored to specific industries, compliance requirements, or best practices. These libraries typically include critical system files, configuration files, application files, and directories and registry objects that are most vulnerable to unauthorized changes or tampering.

Using this finely tuned library of critical file paths helps streamline the setup process and reduce the need for manual configuration. Qualys FIM includes common file paths that are likely to be monitored in most environments. It also help minimize noise by focusing monitoring efforts on the most important files and directories.

Please click here for more information and try Qualys FIM for free.