Essential FIM Must-Haves: A Quick Guide for Choosing a File Integrity Monitoring Solution

FIM

File Integrity Monitoring (FIM) is an essential layer of defense for any small, medium, or large enterprise network. FIM solutions identify illicit activities across critical system files and registries, diagnose changes, and send alerts. Their purpose is preventing disruption of IT and IT/OT hybrid environments. Selecting the right FIM for your environment and organization is critical for achieving streamlined compliance and IT/SOC team alignment.

FIM solutions should be assessed for 5 key capabilities:

1 Integration with Asset Management and Inventory Tools

A FIM without a comprehensive asset inventory is almost worthless. Surprisingly, most FIM tools do not come with a built-in asset inventory capability, so security and compliance stakeholders typically must rely on external third-party asset inventory products. Consequently, standalone FIMs often increase the complexity of security and compliance tools that IT must then manage. As you assess FIM alternatives, look for a solution that improves convergence between security, compliance, and IT by including asset inventory capabilities. This function can strengthen the contextual analysis of IT assets as well as the efficiency of file integrity monitoring tasks across a distributed organization.

How we do it

Qualys FIM, as part of Qualys Cloud Platform, brings the asset context present in both Qualys Vulnerability Management, Detection, and Response (**VMDR**) and Qualys Cyber Security Asset Management (**CSAM**). As soon as Qualys FIM logs an event, the potential issue is enriched with Qualys threat intelligence. This information is instantly available in an intuitive dashboard that lets users quickly review the events and take appropriate action. Qualys FIM helps organizations to address their day-to-day security and compliance needs while continuously honing their overall threat intelligence capabilities by leveraging the automated machine learning capabilities of Qualys Cloud Platform.

2 Event Management and Alert Prioritization

When it comes to alerting, many File Integrity Monitoring (FIM) providers believe "more is better." Tool differentiation often boasts of generating more alerts with increasingly customized risk ratings. This alert storm buries compliance and security analysts with hundreds of thousands of events with a lack of accurate or meaningful prioritization. The truth is: most alerts require no action, dramatically taxing SOC teams and compliance audit resources and thwarting efficient incident response and analysis. Your assessment of FIM solutions should test the real-world utility of alerts provided. In addition, ensure that alerting adheres to PCI DSS Standard 10.3.4, which states that "existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)."

How we do it

At Qualys, we understand that more alerts do not equal more security. **Qualys FIM** reduces up to 99% of alert noise with trusted source intelligence and profile tuning to optimize compliance and risk analysis. With the "Trusted Source Status" feature, users can easily identify the good changes resulting from patches and security updates and update them within an allow-list. With the "File Reputation Status" feature, Qualys FIM allows users to identify if any change on the system is malicious or suspicious and take necessary action to kill the attack chain.

3 Scalability

Not all FIM solutions scale to support large organizations with high performance or lower total cost of ownership. Most FIM tools are stand-alone solutions, which makes integrations with SIEMs, EUBAs, asset inventory, and other critical security and compliance tools difficult, labor-intensive, and ultimately expensive. Many FIMs require consulting services as your infrastructure grows in node number and distribution. Test the capabilities of FIM solutions under evaluation for tight interoperability with your organization's security stack.

How we do it

Qualys FIM provides an automated incident generation capability for malicious changes. Qualys designed this feature to automatically send an incident alert for each malicious change. When Qualys FIM identifies the file reputation status as "malicious," an incident is automatically created with the details about associated malware disposition, indicators of compromise, policy violation, and contextual information. Issues discovered by Qualys FIM can automatically integrate with **more than 70** SIEMs, CI/CD tools, governance, risk and compliance tools, and other infrastructure monitoring applications.

4 APIs and Integrations

While FIM is a critical part of a comprehensive security and compliance stack, it must interact with the total cybersecurity ecosystem. The FIM solution you select should include API development to support bi-directional data exchange between your organization's data lake repositories. FIM solutions that can support native integrations

with Splunk, QRader, and ServiceNow will dramatically increase the ROI of your FIM solution and streamline coordination between compliance, security, and IT stakeholders.

How we do it

Qualys FIM APIs are designed to enable easy custom integrations. The Rich FIM API set produces data in well-defined and structured JSON format which can be easily exported to the ELK stack. It supports native integrations with Splunk, IBM QRadar, and ServiceNow. For example, the Qualys Technology Add-on (TA) for Splunk | Splunkbase service provides a dashboard for Qualys FIM event data and pulls indexed data to produce dashboards and reports.

5 Time-to-Value

PCI DSS 11.5 requires that file change detection mechanisms are used for early intervention of compliance and security risks. However, some FIMs do not include reliable change detection rules and parameters that have been pre-configured with critical files for the related operating system. This missing capability makes their deployment complex and time-consuming. With any FIM solution, be sure to test its reconfiguration capabilities and ability to monitor critical files within unique to specific applications.

How we do it

Qualys FIM features rapid one-click deployment, allowing customers to skip time-consuming baselining and move straight into monitoring. Per PCI requirement 11.5, Qualys FIM leverages a rich asset inventory and **Qualys CSAM** to continuously inventory assets, apply business criticality, and add risk context to files in real-time. Best of all, Qualys FIM deploys quickly without any hidden fees.

In summary, **Qualys File Integrity Monitoring (FIM)** is a lightweight and highly scalable cloud service that provides continuous system monitoring of critical files, folders, and registry objects for changes to help organizations adhere to compliance mandates such as PCI-DSS, FedRAMP, HIPAA, GDPR, and more. Leveraging the Qualys Cloud Platform and FIM library, Qualys reduces alert noise by adding greater event context to alerts with event severity, out-of-the-box rules, and integrated threat intelligence. It provides streamlined asset visibility and monitoring capabilities at lower cost and with greater system performance than conventional FIM solutions.

To learn more about Qualys File Integrity Monitoring and how we are helping customers reduce alert noise and optimize compliance and security tasks go to:
www.qualys.com/forms/file-integrity-monitoring/

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**

v220512

©2022 Qualys, Inc. All Rights Reserved.