Essential FIM Must-Haves for Security and Compliance Practitioners

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. Selecting the right FIM for your organization is critical for achieving streamlined compliance, IT and Security team alignment.

FIM solutions should be assessed for 5 key capabilities:

1 Integration with Asset Management and Inventory Tools

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.

2 Event Management and Alert Prioritization

Many FIM providers boast their ability to generate more alerts with increasingly customized risk ratings. This alert storm buries compliance and security analysts with hundreds of thousands of events that lack 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.

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 also 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.

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.

5 Time-to-Value

The Payment Card Industry Data Security Standard (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 your environment.

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/

v220512