



PREVENTING SECURITY & POLICY COMPLIANCE FAILURES WITH FIM

Essential File Integrity Monitoring Requirements to Reduce Risks and Costs

Table of Contents

I. Real-time File Access Monitoring	4
Use Case One: Cybersecurity Maturity	4
Use Case Two: Compliance and Regulatory Requirements	4
FAM Capability Requirements	6
FAM Compliance Requirements	6
Qualys FAM in Action	6
II. Comprehensive File Integrity Monitoring (FIM)	9
Essential Requirements	9
Requirement 1: Noise Cancellation, Efficiently Reducing False Alerts	9
Requirement 2: Single Agent and Platform	11
Requirement 3: Automated Incident Management and Compliance Reporting	12
Requirement 4: Extensive Event Details to Meet Regulatory Requirements	13
Requirement 5: Data retention	14
Requirement 6: Dynamic FIM Dashboard	14
III. Agentless FIM – FIM on Network Devices	15
IV. Time to Value	16
V. Scalability	17
VI. Ready for PCI DSS 4.0	18
Conclusion	18

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 compliance and cybersecurity best practices. The best FIM solutions should include noise cancellation, File Access Monitoring (FAM), and agentless support for network device monitoring.

Most enterprise firms must comply with numerous regulations and mandates, such as PCI DSS 4.0 and other international or U.S. State civil codes, which impose serious penalties for non-compliance. Organizations risk audit failures, fines, lawsuits, and brand damage, with average costs now exceeding \$4 million for breach remediation, \$4 million for litigation, and \$15 million for audit failures. Most organizations have also adopted one or more cybersecurity frameworks such as those offered by the National Institutes of Standards and Technology (NIST) or Center for Internet Security (CIS).

What follows is a detailed discussion of the essential requirements for any FIM solution to meet stringent cybersecurity framework and compliance mandate requirements and allow firms to reduce attack surfaces, complexities, costs, and risks.

I. Real-time File Access Monitoring

File Access Monitoring (FAM) is a security practice that involves tracking and logging access to sensitive files. FAM should be included with any FIM solution to trigger alerts when critical host files, not intended for regular use, are accessed. Any FIM solution should include FAM to also ensure cybersecurity best practices and meet minimum compliance requirements. For example, many PCI DSS 4.0 requirements now specify access monitoring. FAM solutions should be designed to capture comprehensive information about access to sensitive information, which include:



User information

Users that attempt to access specific files. This information is crucial for accountability and to identify authorized or unauthorized users.



Timestamps

Exact timestamp of when a file access occurs.



Accessed File Details

Information about the specific file being accessed, including the name and location. This allows for more granularity about file interaction.



Processes

Details about processes or methods used to access a file.



Host details

Host where the file access takes place. This granular detail helps strengthen user identification and hold users accountable for their actions.

FAM represents both a major gap and an opportunity for organizations looking to identify threats and achieve compliance. It's a gap because organizations may determine that systems need the capability to log every file access as successful or unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Outlined below are two typical use cases for FAM:

Use Case One: Cybersecurity Maturity

- Detecting Unauthorized Access: Unauthorized users attempting to access sensitive files.
- Detecting Administrator Access: Privileged users can misuse their admin rights to access files with sensitive data.
- Failure to monitor access to sensitive files in real-time, as this may lead to undetected data theft.
- Large numbers of files accessed and modified in a short time period, as this can be indicative of a ransomware attack in progress.

Use Case Two: Compliance and Regulatory Requirements

Compliance regulations require organizations to record access events to files containing sensitive data.

HIPPA 2023 45 CFR § 164.308(a)(1)(ii)(D)

- Information system activity review (required). Implement procedures to regularly review records about information system activity, such as audit logs, access reports, and security incident tracking reports.

PCI DSS 4.0

- 10.2.1.1 Need to capture all individual user access to cardholder data as A record of all individual access to cardholder data can identify which accounts may have been compromised or misused.
- 10.2.1.2 Need to capture all access by administrators as Accounts with increased access privileges, such as the “administrator” or “root” account, have the potential to significantly impact the security or operational functionality of a system.
- 10.2.1.3 Need to capture all access to audit logs as Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account.
- 10.2.1.4 Need to ensure that all invalid access attempts are captured.

Critical Security Controls Version 8

- 3.14: Log Sensitive Data Access

NIST Special Publication 800-53 Revision 4

- AU-2: Audit Events

Cloud Controls Matrix v4.0

- DSP-17: Sensitive Data Protection
- LOG-04: Audit Logs Access and Accountability

GDPR

- This European mandate states that unauthorized data access includes accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of personal data transmitted, stored or otherwise processed. Monitoring both authorized and unauthorized access to sensitive data is essential to early data breach detection.

ISO27001

ISO requires the ability to interpret file server access logs. FAM can address a number of challenges for security professionals, including:

- Gaining immediate visibility on access details and attempts related to critical files.
- Logged events, which should be easily accessible, for review, filtering, or searching.
- Automated incident generation for suspicious files, or on any access attempts to specific and highly sensitive information.
- Ability to generate automated compliance reports that show detailed audit trails for file access events.

- Alert fatigue, as monitoring file access generates a significant amount of data and a FAM solution should be able to distinguish between routine events and actual security incidents to suppress noise.

FAM Capability Requirements

To meet the above security and compliance requirements, FAM capabilities should include the following:

FAM requirements	Supported by Qualys FAM
Ability to generate real time FAM alerts	Yes
Ability to generate automated incidents for FAM events	Yes
Ability to generate automated compliance reports for FAM events	Yes
Ability to add custom files for access alerts	Yes
Ability to add user and process-based inclusion-exclusion filter to suppress noise generated by known-good users and processes	Yes
Real-time FAM for both Windows and Linux operating systems	Yes

Details captured in FAM events should include the following:

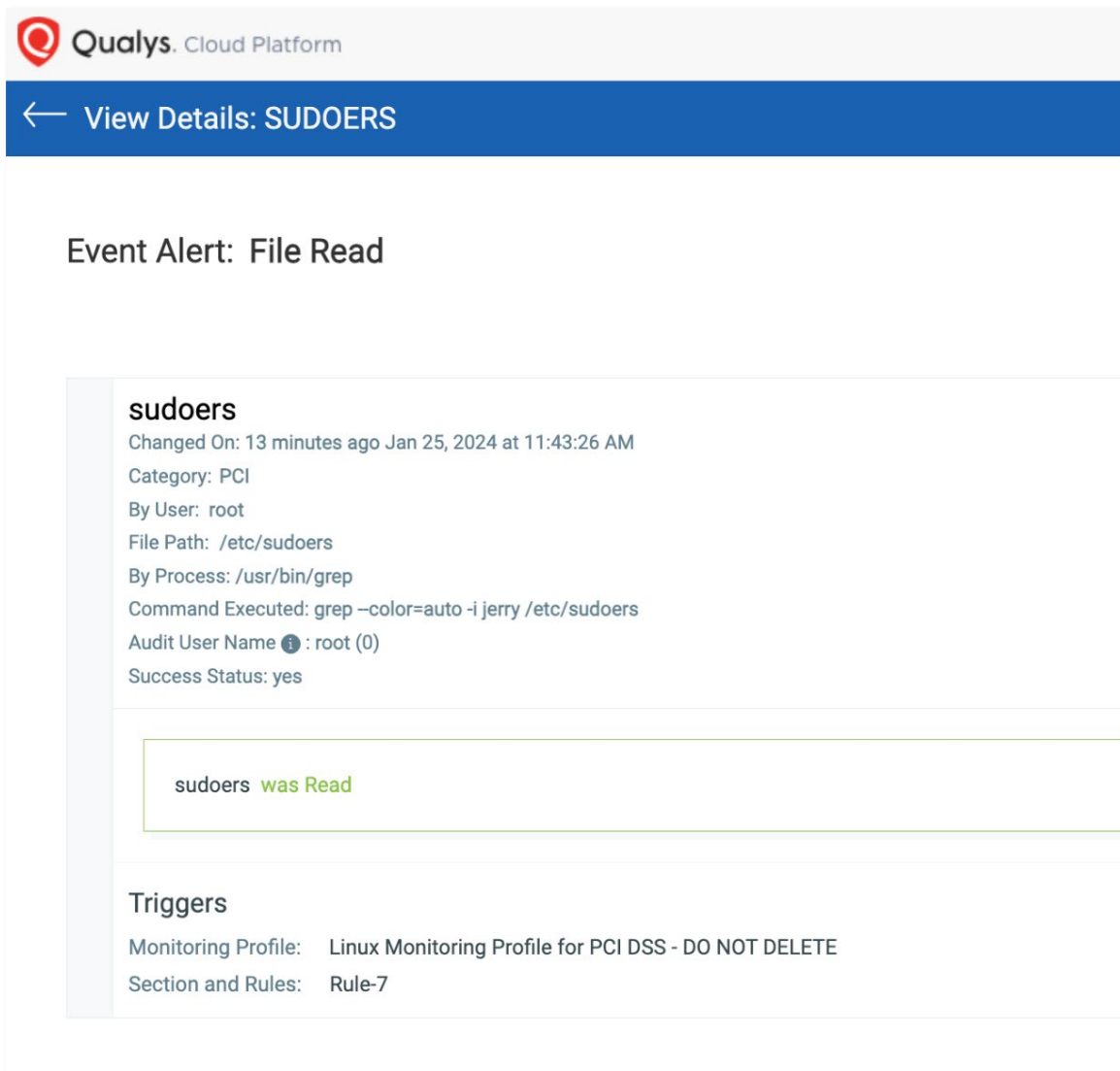
Details to be captured in FAM Events	Supported by Qualys FAM
User information Users that attempt to access specific files. This information is crucial for accountability and to identify authorized or unauthorized users.	Yes
Timestamps Exact timestamp of when a file access occurs.	Yes
Accessed file details Information about the specific file being accessed, including the name and location. This allows for more granular on file interaction.	Yes
Process Details about processes or methods used to access a file.	Yes
Host details Host where the file access takes place.	Yes

FAM Compliance Requirements

Any FAM solution worth its salt should include capabilities to track file access, which is a compliance requirement mandated by various regulations such as GDPR, HIPAA 2023, PCI DSS 4.0, GLBA, DORA, SOX, FISMA, ISO 27001, and other relevant regulations.

Qualys FAM in Action

Below is an example of the FAM event details captured by Qualys FIM when a privileged user 'root' tries to access a 'sudoers' file. All the required who, when, what, and where details have been captured as part of the exhaustive events details.



The screenshot displays the Qualys Cloud Platform interface. At the top, the Qualys logo and 'Cloud Platform' text are visible. Below this is a blue navigation bar with a back arrow and the text 'View Details: SUDOERS'. The main content area is titled 'Event Alert: File Read'. A detailed view of the 'sudoers' file is shown, including the following information:

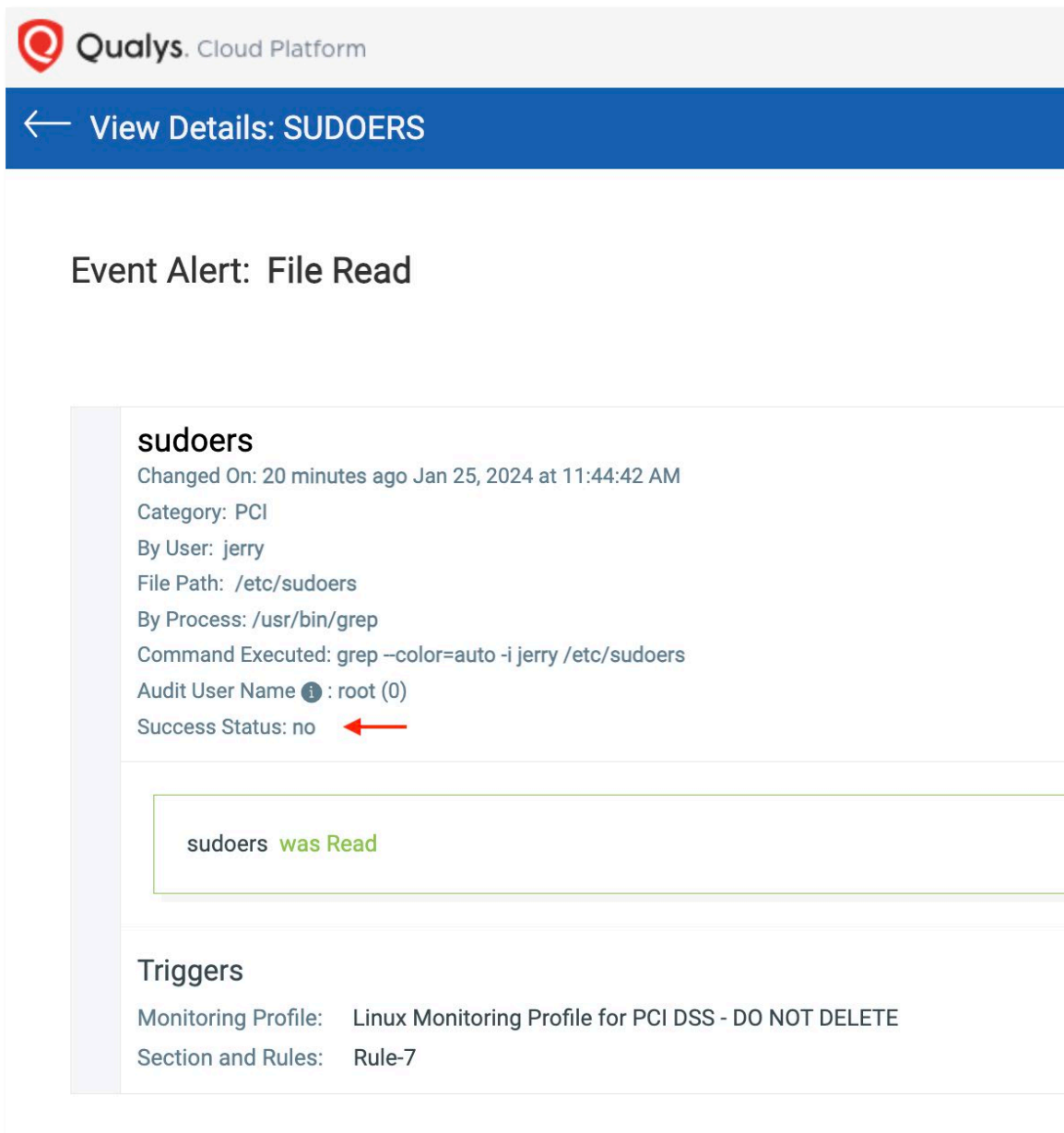
- sudoers**
- Changed On: 13 minutes ago Jan 25, 2024 at 11:43:26 AM
- Category: PCI
- By User: root
- File Path: /etc/sudoers
- By Process: /usr/bin/grep
- Command Executed: grep --color=auto -i jerry /etc/sudoers
- Audit User Name ⓘ : root (0)
- Success Status: yes

A summary box below the details states: **sudoers was Read**. At the bottom, the 'Triggers' section is shown:

- Monitoring Profile: Linux Monitoring Profile for PCI DSS - DO NOT DELETE
- Section and Rules: Rule-7

PCI DSS 4.0 requirements state that audit logs must record the Success and Failure Indication of an event.

Qualys FAM demonstrates a proactive approach by logging events for unsuccessful access attempts. For instance, if a regular user tries to access a highly restricted file and faces denial from the operating system due to insufficient permissions, Qualys FAM promptly generates an event within the Qualys FIM app. This event clearly indicates the outcome with the Success Status marked as "No."



The screenshot displays the Qualys Cloud Platform interface. At the top, the Qualys logo and 'Cloud Platform' text are visible. Below this is a blue navigation bar with a back arrow and the text 'View Details: SUDOERS'. The main content area is titled 'Event Alert: File Read'. A detailed view of the event shows the following information:

- sudoers**
- Changed On: 20 minutes ago Jan 25, 2024 at 11:44:42 AM
- Category: PCI
- By User: jerry
- File Path: /etc/sudoers
- By Process: /usr/bin/grep
- Command Executed: grep -color=auto -i jerry /etc/sudoers
- Audit User Name ⓘ : root (0)
- Success Status: no ←

A summary box below the details states: 'sudoers was Read'. At the bottom, the 'Triggers' section lists:

- Monitoring Profile: Linux Monitoring Profile for PCI DSS - DO NOT DELETE
- Section and Rules: Rule-7

In summary, File Access Monitoring (FAM) enhances a comprehensive File Integrity Monitoring (FIM) solution by providing real-time insights into user interactions with files. While FIM ensures the integrity of data, FAM complements this by detecting and alerting on unauthorized access attempts, offering a more holistic and comprehensive approach to file security.

II. Comprehensive File Integrity Monitoring (FIM)

Qualys FIM is the most comprehensive FIM solution on the market. You can deploy Qualys FIM from a public or private cloud, fully managed by Qualys. There are no servers to provision, software to install, or databases to maintain. You can also leverage dynamic policy configurations based on asset tags to ensure new assets are discovered and automatically configured for FIM without IT involvement. Out-of-the-box profiles help you set base profiles, further reducing onboarding time.

Essential Requirements

Requirement 1: Noise Cancellation, Efficiently Reducing False Alerts

Most FIM solutions are considered “noisy” in that they generate a great deal of false positive alerts. They promote their ability to generate more alerts with increasingly customized risk ratings. This alert storm burdens compliance and security analysts with hundreds of thousands of events that lack accurate or meaningful prioritization. The truth is that most alerts require no action, dramatically taxing SOC teams and compliance audit resources and thwarting efficient incident response and analysis. Your assessment of any FIM solution should include testing the real-world utility of alert triggers.

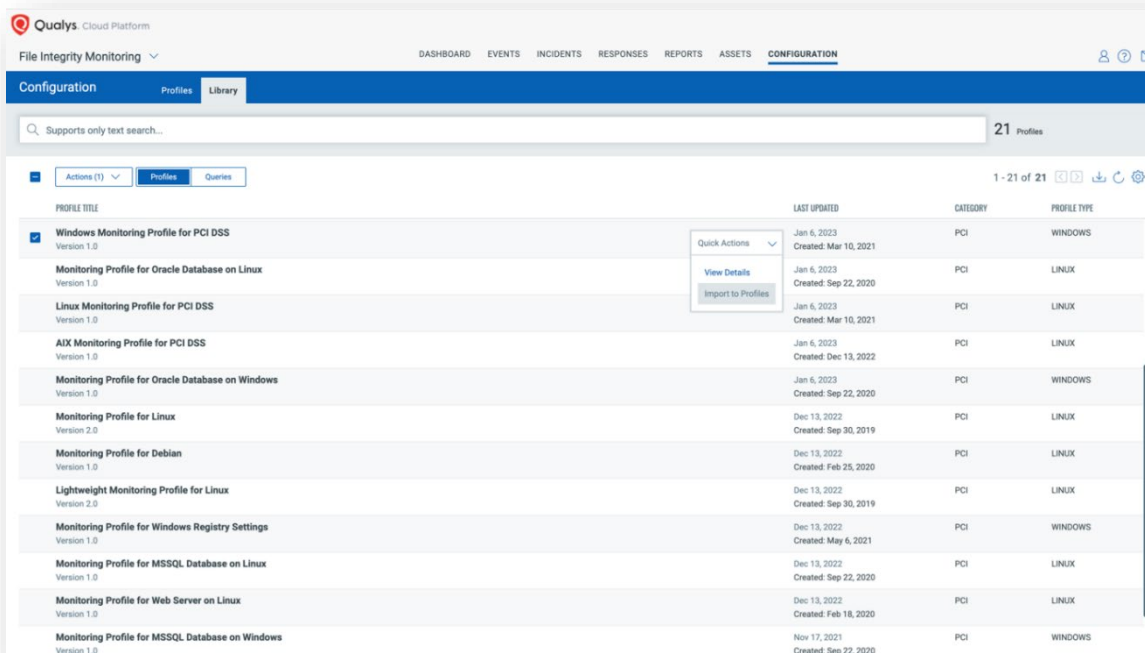
Qualys FIM includes unique noise cancellation technology that reduces false alerts by 90%+. Qualys FIM enriches event data with threat intelligence by adding Trusted Source and File Reputation context to control noise and prioritize events. With intuitive dashboards, you can continuously track your change posture, as well as view insights on change events with ‘what-who-when’ context

Three major contributions offered by FIM noise cancellation are:

Out-of-the-box FIM Profiles

The Qualys FIM solution stands out with its expertly crafted library of essential file paths, meticulously chosen to minimize noise. These paths aren’t arbitrary; they are the most critical ones, carefully curated to meet regulatory standards. By leveraging this finely tuned library, administrators benefit from preconfigured settings that cover everything—from critical system files to configuration files, application files, directories, and registry objects—each selected for their vulnerability to unauthorized changes.

Focusing more on monitoring efforts related to these critical files and directories ensures administrators receive only the most pertinent alerts. With Qualys FIM, you can enhance efficiency and clarity in your security operations.



In-Depth Filtering Options in FIM Rules for Noise Suppression

Qualys FIM rules offer a high level of granularity, providing users with diverse options to effectively suppress noise by specifying conditions such as:

- a) File paths, with wildcard support, for example:
 - `/var/*` or `/tmp/*` (`/tmp` and `/var/tmp`) in Linux
 - `C:\Users\AppData\Local\Temp` or `%systemdrive%\Windows\Temp` in Windows
- b) User and process-based filtering

This allows users to drop events generated by whitelisted users and processes. For example, an antivirus process being run by a system user would not be able to generate any noise if added as a global exclusion filter in a FIM Profile.

Advanced Noise Cancellation in FIM with Threat Intelligence to Detect Malicious or Suspicious Hashes

Qualys FIM goes beyond traditional event monitoring by integrating threat intelligence, specifically file reputation context, to help users quickly distinguish if a system change is suspicious or malicious.

Event Alert: File Create

View Details: 6A5CB4081F34DEA669A656CCAF79031543653F63FCE0B8...

File Create

6a5cb4081f34dea669a656ccaf79031543653f63fce0b8b477ab018772fd876.exe

Created On: 2 years ago Oct 25, 2021 at 12:32:48 PM

Category: PCI

By User: 135357-T491\Administrator

File Path: C:\Accounts\6a5cb4081f34dea669a656ccaf79031543653f63fce0b8b477ab018772fd876.exe

File Reputation Status: **Suspicious**

File Trust Status: Unavailable

By Process: C:\WINDOWS\Explorer.EXE

File Hash: 6a5cb4081f34dea669a656ccaf79031543653f63fce0b8b477ab018772fd876

6a5cb4081f34dea669a656ccaf79031543653f63fce0b8b477ab018772fd876.exe was Created

Triggers

Monitoring Profile: FIM DEMO - Lightweight Monitoring Profile for Windows - DO NOT DELETE

Section and Rules: Rule-110

Monitoring Profile: Windows Monitoring Profile for PCI DSS

Section and Rules: Rule 101

ABOUT ASSET

135357-T491

Microsoft Windows 10 Pro 10.0.19043
64-bit N/A Build 19043
Unknown Manufacturer / Model

Identification

DNS Hostname: 135357-T491

NetBIOS Name: 135357-T491

IPv4 Addresses: 10.115.95.132

IPv6 Addresses:

Agent ID: 5fc1d29-3a0e-4265-bbd9-1c42676deb44

Host ID: 340680746

Activity

Last User Login: Administrator

Last System Boot:

Created On: Aug 27, 2021 05:21 am

Last Checked-in: Aug 27, 2021 05:21 am

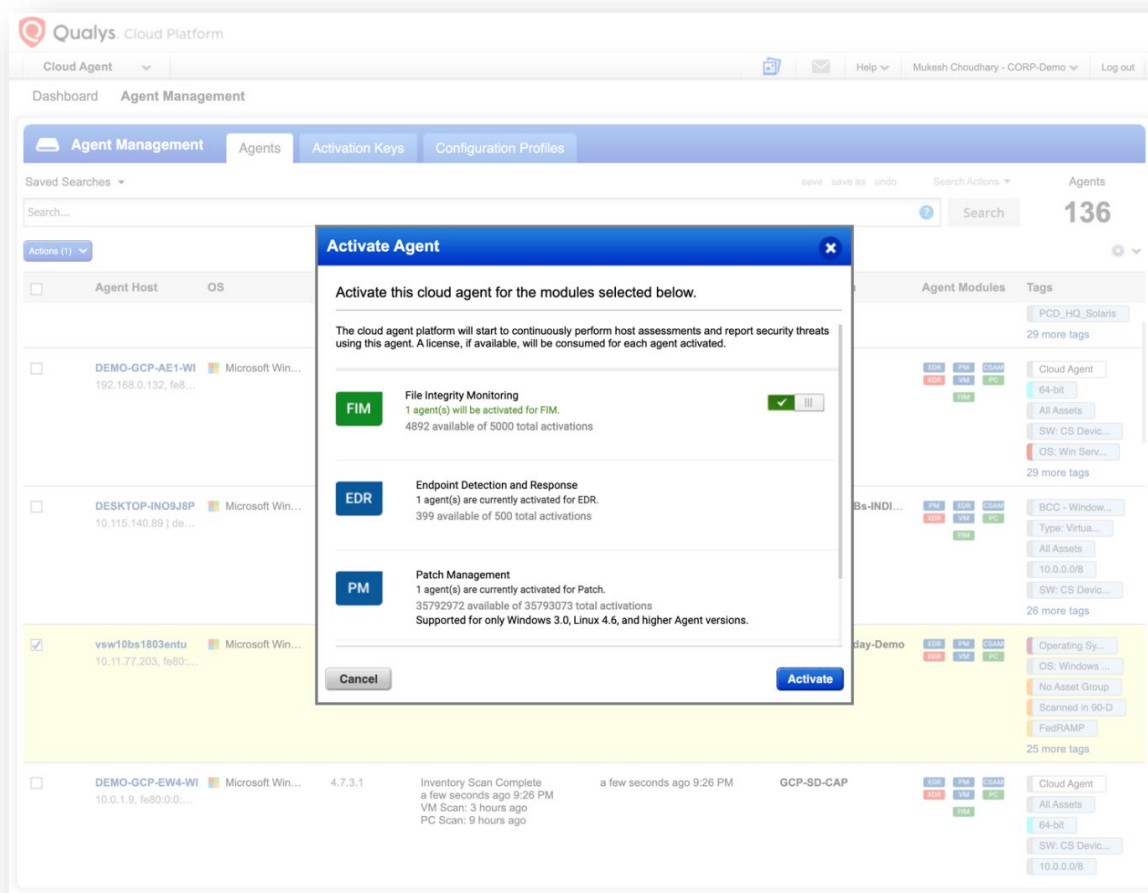
ABOUT THE FILE

File Name: 6a5cb4081f34dea669a656ccaf79031543653f63fce0b8b477ab018772fd876.exe

Requirement 2: Single Agent and Platform

Many solutions require multiple agents, platforms, and dashboards. This can dramatically increase management time and efforts that can impact Total Cost of Ownership (TCO). The Qualys Cloud Agent is lightweight and versatile, saving you from deploying and managing multiple point agents for different security tasks.

The Qualys TruRisk Enterprise Platform offers a single pane of glass to manage FIM alongside other security apps. You can also leverage dynamic policy configurations based on asset tags to ensure new assets are discovered and automatically configured for FIM without IT involvement. Out-of-the-box profiles help to set base profiles, further reducing onboarding time.



Requirement 3: Automated Incident Management and Compliance Reporting

Qualys FIM offers an **Incident Management Workflow** that allows manual and automated incident creation. This feature is highly configurable, enabling automatic incident generation based on specific criteria such as:

- Deletion of activities by non-privileged users
- Detection of changes in ownership or permission by non-privileged users
- Detection of malicious or suspicious files on the host
- Unauthorized modification of initialization files, and much more

This functionality streamlines incident response, helping organizations immediately identify and address security concerns.

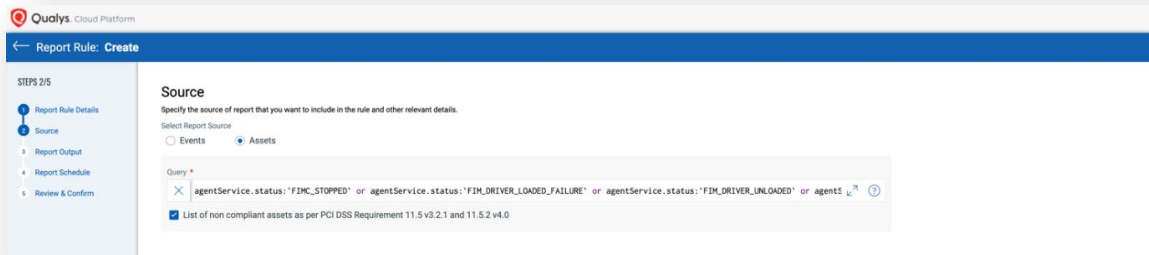
The Qualys FIM solution includes automated compliance reports that are pivotal in supporting compliance audits, making them a cornerstone of the FIM system. These reports can be categorized into three key types:

- Event-Based Reports

- These reports detail specific security events and activities tracked by the FIM system.
- Incident-Based Reports
 - This category documents security incidents and breaches within the monitored environment.
- Asset-Based Reports
 - Asset-based reports offer a comprehensive snapshot of individual assets within the FIM scope.
 - They assess the security posture and compliance of these assets with relevant standards.
 - Using asset-based reports, you can readily identify non-compliant assets vital for maintaining compliance readiness, especially within your PCI DSS 4.0 scope.

Non-compliant assets encompass two critical categories:

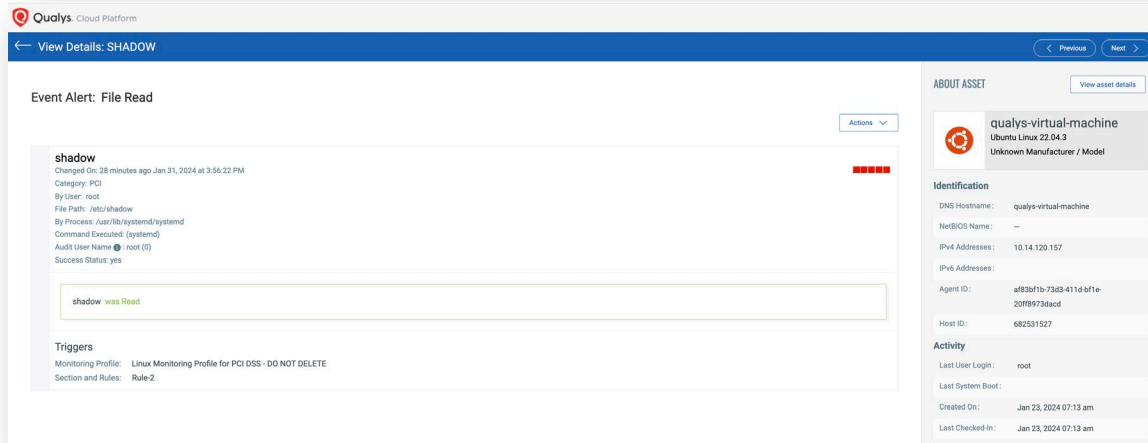
- Assets on which FIM was activated but not currently running – this condition contradicts PCI DSS Requirement 11.5 (v3.2.1) and 11.5.2 (v4.0), emphasizing the necessity of continuous FIM monitoring to maintain compliance and security standards.
- Non-Communicating Assets: These are not communicating with the Qualys platform. Identifying and addressing non-communicating assets is crucial to ensure that all relevant systems are actively monitored and assessed.



Requirement 4: Extensive Event Details to Meet Regulatory Requirements

Qualys FIM covers all aspects of an auditable event such as:

- User Identification
- Type of Event
- Date and Time
- Success and Failure Indication
- Origination of Event
- Identity or name of affected data, system component or resource

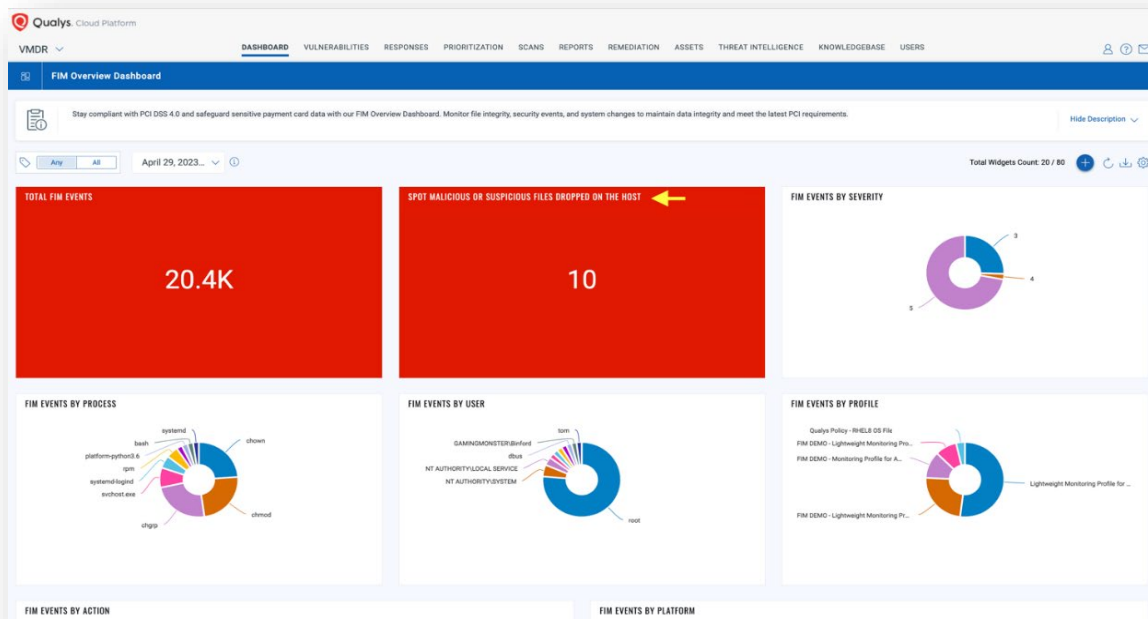


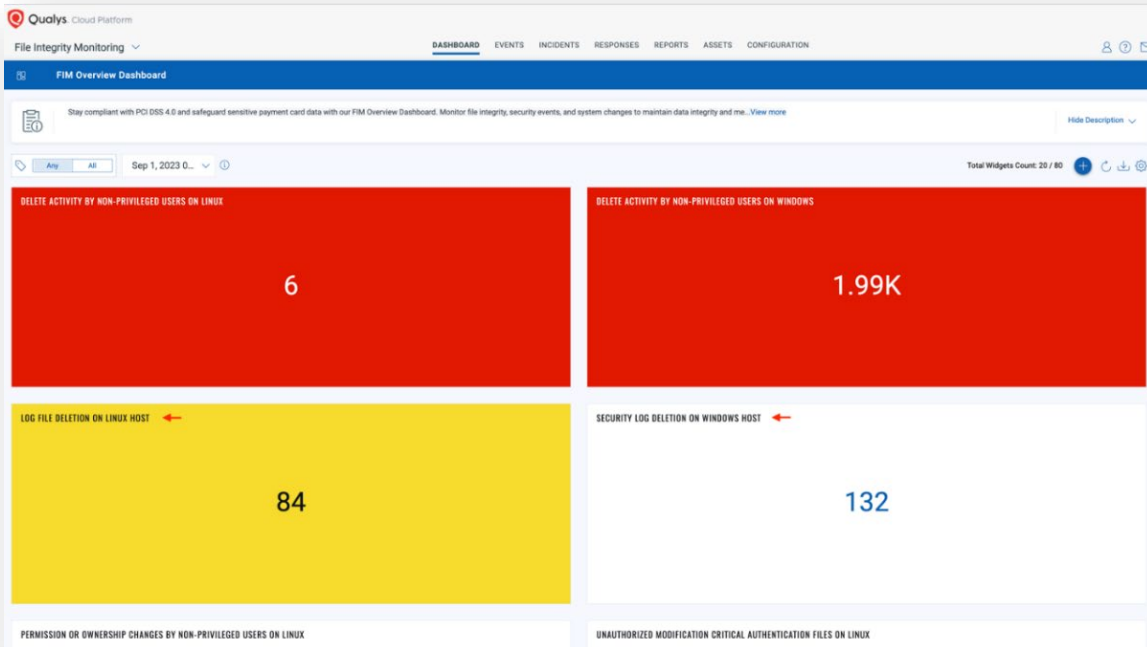
Requirement 5: Data retention

Many solutions have limited data retention, such as only 30 days, which may trigger compliance audit failures. Qualys FIM offers a 13-month data retention policy, guaranteeing immediate accessibility to all events for comprehensive forensic analysis in the event of an incident. This meets most compliance mandates, such as the 12-month data retention requirements stipulated by PCI DSS 4.0.

Requirement 6: Dynamic FIM Dashboard

Qualys FIM features a dynamic default dashboard that offers a comprehensive summary of environmental change events, focusing on highlighting critical issues that demand immediate attention. It also includes predefined widgets that quickly provide an overview of your complete FIM environment.

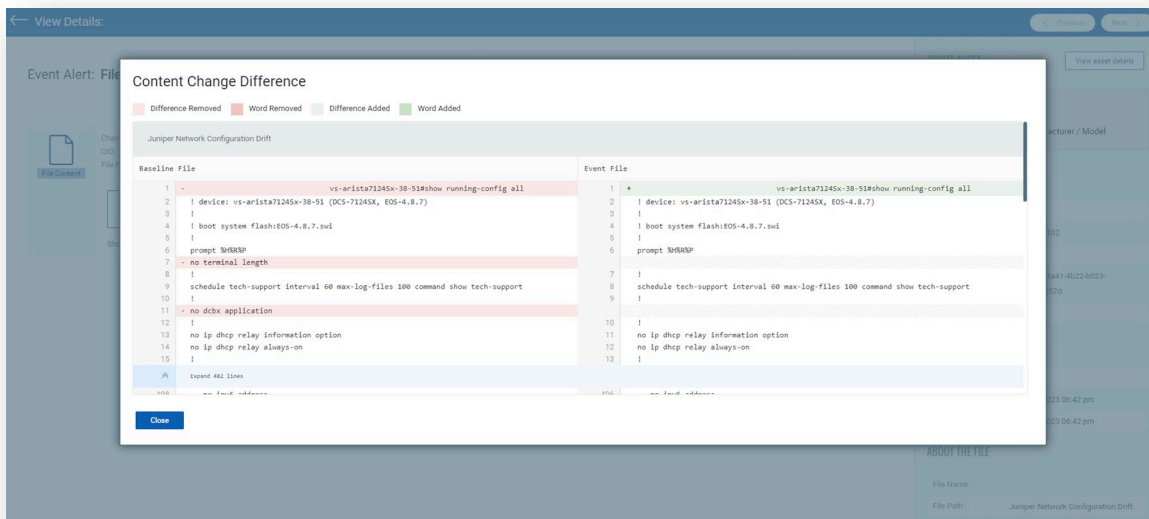
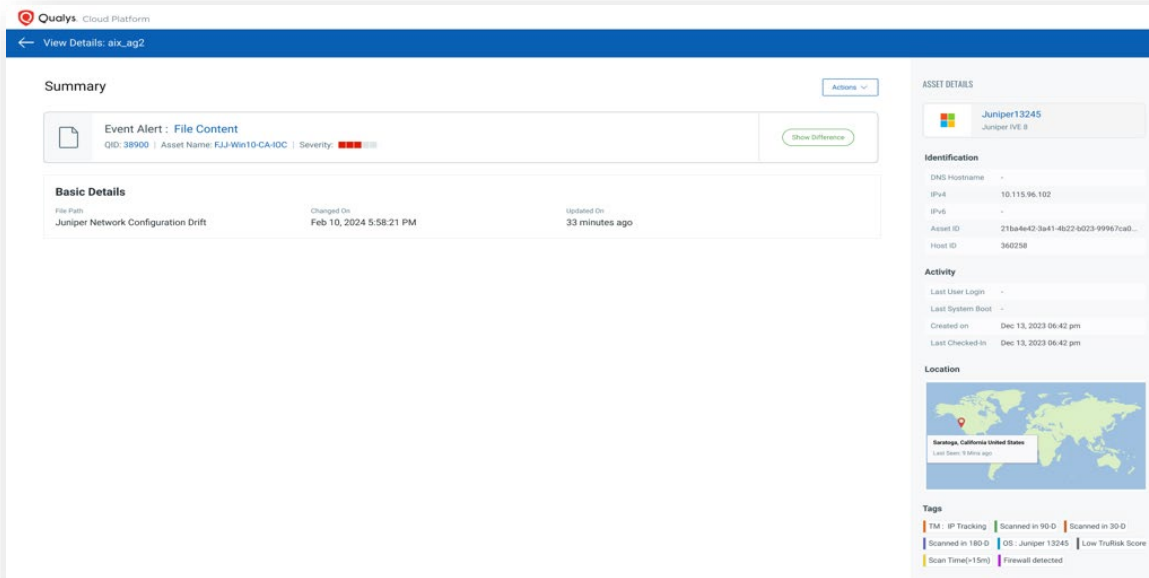




III. Agentless FIM – FIM on Network Devices

Qualys introduces agentless File Integrity Monitoring (FIM), starting with FIM on network devices like JuniperOS, Arista, and PaloAlto. This capability triggers alerts that precisely pinpoint the differences in network configurations during routine scan intervals, offering detailed insights into what changed in the configuration.

Implementing FIM on network devices is a proactive security measure that helps organizations maintain the integrity, security, and compliance of their network infrastructure. It provides a critical layer of defense against unauthorized changes, configuration drift, and potential security threats in the dynamic and evolving landscape of cybersecurity.



IV. Time to Value

PCI DSS 4.0 requirements stipulate that file change detection mechanisms must be used for early intervention of compliance and security risks. However, some FIM solutions do not include reliable change detection rules and parameters that have been pre-configured with critical files for related operating systems. This missing capability makes deployment complex and time-consuming. With any FIM solution, be sure to test reconfiguration capabilities and abilities to monitor critical files unique to your environment.

With Qualys FIM, you can leverage dynamic policy configuration based on asset tags to ensure new assets are discovered and automatically configured without IT or the security team's involvement. Out-of-the-box profiles help in setting the base profile, further reducing onboarding time. 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 Return of Investment (ROI) of your FIM solution and streamline coordination between compliance, security, and IT stakeholders.



"Deploying FIM via a cloud-based security and compliance platform allows enterprises to easily scale these efforts and take advantage of a consolidated security solution to achieve compliance on a global scale, while reducing the high costs of multiple point products." **Robert Ayoub, Research Director, IDC**

V. Scalability

Many FIM customers and industry experts have reported that some FIM solutions may have scalability challenges. They often require multiple servers to support thousands of endpoints, and IT time and effort for management may become a challenge. A single console may not be able to service beyond 10,000 assets, requiring additional consoles at more cost. Some solutions may require thousands of rules to monitor a host, which can be taxing for resource-constrained teams and could require expensive professional services.

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 make integrations with SIEM, EUBA, asset inventory, and other critical security and compliance tools difficult, labor intensive, and expensive. Many FIM solutions also require consulting services as your infrastructure grows in node number and distribution. Be sure to test the capabilities of any FIM solution for tight interoperability with your organization's security stack.

With Qualys FIM, you can scale dynamically. Minimal setup and hosted services for event management significantly reduce demands on existing infrastructure, further optimizing costs. With the Qualys TruRisk Enterprise cloud platform, you can scale up globally and on demand. Also, easily integrate with other systems via extensible XML-based APIs and seamlessly use Qualys FIM with a broad range of security and compliance systems such as GRC, ticketing systems, SIEM, ERM, and IDS.

VI. Ready for PCI DSS 4.0

Qualys FIM is audit-ready to support PCI DSS 4.0 requirements. Below are links to more information:

[PCI DSS 4.0 FIM Requirements Simplified with Qualys File Integrity Monitoring](#)

[Qualys FIM Playbook for PCI 4.0](#)

Conclusion

To avoid costly audit failures, security breaches, and litigation, any File Integrity Monitoring (FIM) solution should have seven essential capabilities, including File Access Monitoring (FAM), noise cancellation, agentless network support, and more. The Qualys FIM solution is a lightweight and highly scalable cloud service that includes these capabilities and provides continuous system monitoring for critical files, folders, and registry objects for changes.

Qualys FIM helps organizations adhere to compliance mandates such as PCI DSS 4.0, HIPAA 2023, CCPA, GDPR, and others. By leveraging the Qualys TruRisk Enterprise Platform and the extensive FIM library, you can reduce alert noise and add greater event context to alerts with event severity, out-of-the-box rules, and integrated threat intelligence. Qualys FIM provides streamlined asset visibility and monitoring capabilities at a lower Total Cost of Ownership (TCO) and with greater system performance than virtually any other FIM solution.

To learn more about Qualys FIM and how we're helping customers reduce alert noise, audit failures, and cybersecurity risks, visit: www.qualys.com/forms/file-integrity-monitoring/



Simple Migration

- ✓ Full migration in less than two days
- ✓ In-product support for smooth transition
- ✓ Free Qualys sales engineering support as needed

Qualys FIM ★★★★★

Best in one tool to monitor critical files, directories, and registry paths or changes in real-time, with great visibility and control, helps adhere to compliance mandates such as PCI-DSS, FedRAMP, HIPAA, GDPR and others.

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