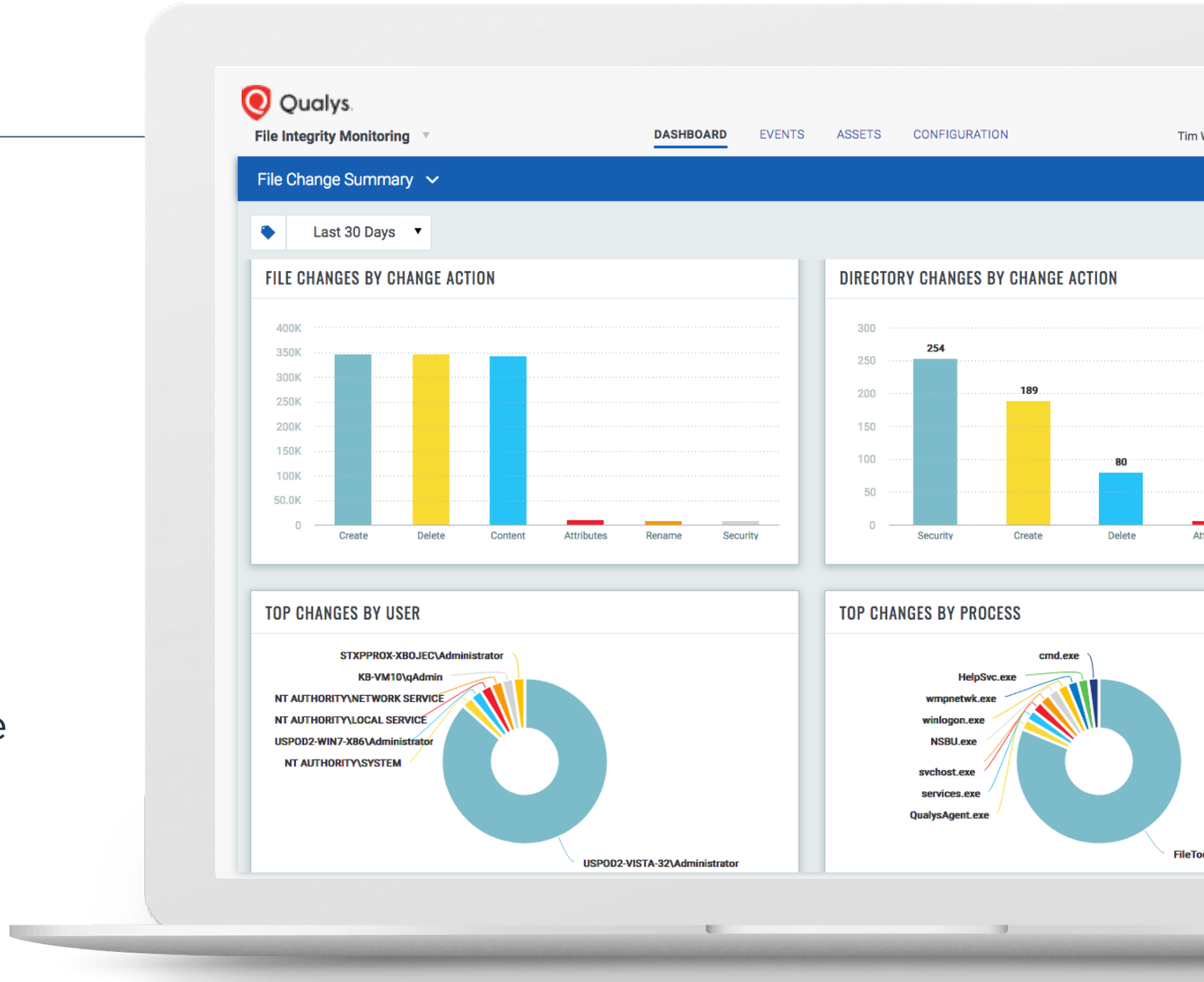
File Integrity Monitoring

Log and track file changes across global IT systems.



Qualys File Integrity Monitoring (FIM) is a highly scalable and centralized cloud app that logs and centrally tracks file change events on common enterprise operating systems in organizations of all sizes. Qualys FIM provides customers a simple way to achieve centralized cloud-based visibility of activity resulting from normal patching and administrative tasks, change control exceptions or violations, or malicious activity — then report on that system activity as part of compliance mandates.

Qualys FIM collects the critical details needed to quickly identify changes and root out activity that violates policy or is potentially malicious. As a cloud-based service, Qualys FIM allows teams to eliminate the expense and complexity of deploying and maintaining point solutions in order to globally comply with change control policy enforcement and change monitoring requirements.

Key Features

Preconfigured content

Deciding what to monitor is a challenge for most security teams, so FIM comes with out-of-the-box profiles based on industry best practices and vendor-recommended guidelines for common compliance and audit requirements, including PCI mandates.

Robust real-time change detection engine

The Qualys Cloud Agent continuously monitors the files and directories specified in the monitoring profile and captures critical data to identify what changed along with environment details such as which user and process was involved. It sends data to the Qualys Cloud Platform for analysis and reporting, whether the systems are on premises, in the cloud, or remote.

Scalable architecture that’s easy to manage

FIM can be instantly activated on existing agents, monitoring for changes locally with minimal impact to the endpoint. The Qualys Cloud Platform allows you to scale to the largest environments, without having to purchase expensive server software, hardware and storage. Performance impact on the endpoint is minimized by efficiently monitoring for file changes locally using a real-time detection driver and sending the data to the Qualys Cloud Platform where all the heavy work of analysis and correlation occur. The Qualys Cloud Agent is self-updating and self-healing, keeping itself up to date with no need to reboot.

Unified security posture

The Qualys Cloud Agent provides unified security capabilities for Qualys FIM, Qualys IoC (Indication of Compromise), Qualys Vulnerability Management, Qualys Policy Compliance and Qualys Asset Inventory within a single agent and console, regardless of the size of the environment. Security analysts can make use of dynamic dashboards, interactive and saved searches, and visual widgets in Qualys’ unified dashboard to monitor changes. The powerful search engine allows you to find related changes quickly, which can be invaluable when responding to a breach or enforcing change control policies.

Qualys FIM is a cloud solution for detecting and identifying critical changes, incidents, and risks resulting from normal and malicious events.

Benefits

Affordable and easy to use

Works across global IT environments in a cost-effective way, while reducing the complexity and the effort involved in deploying and managing multiple on-premises products that are difficult to scale and maintain.

Unimpeded file change visibility

Provides centralized cloud-based visibility of activity resulting from normal patching and administrative tasks, change control exceptions or violations, and malicious activities.

Minimal performance impact

Impacts monitored systems and networks minimally by collecting data with the lightweight Qualys Cloud Agent, and by leveraging Qualys’ cloud for data storage, correlation, and analysis.

Unparalleled precision

Pinpoints potentially problematic file changes amid hundreds of thousands, or even millions of records, so customers can address the most pressing change events.

IDC

“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

Efficiently track changes to files in environments of all sizes

From Qualys FIM's single console, you monitor critical assets for changes across diverse cloud and on-premises environments of all sizes, including the largest ones. This is made possible by a unique combination of Qualys Cloud Agent technology, broad platform support, unparallelled scalability, and a powerful but easy to configure real-time monitoring engine.

- FIM detects changes efficiently in real time, leveraging similar approaches used in anti-virus technologies. Change notifications can be created for entire directory structures, or granularly at the file level. FIM also uses existing OS kernel signals to identify accessed files, instead of the compute-intensive approaches of other products. Events can be triggered for:
  - Creation or removal of files or directories
  - Renaming of files or directories
  - Changes to file attributes
  - Changes to file or directory security settings such as permissions, ownership, inheritance, and auditing
  - Changes to file data stored on the disk

- FIM collects critical change data from the system at the time the change occurs, to make it easier to investigate and correlate changes. It also logs watchlist matches and collects detailed data indicating things like:
  - The exact date and time of the change
  - What user was logged in interactively at the time the change was made
  - What process was involved, and which user owned that process

- Built on the Qualys Cloud Platform, FIM gives you robust scalability, performance and centralized management, while removing the need to purchase expensive servers and software to manage an on-premises solution. This allows you to focus on event review and response, rather than on managing an expensive on-premises solution.

- The Qualys Cloud Agent is very lightweight and versatile, saving you from having to deploy and manage multiple point agents for different security tasks. Qualys Cloud Agent benefits include:
  - Can be activated instantly and installed anywhere
  - Is shared by other Qualys apps for collecting other security and compliance data, as well as file data for indication of compromise, vulnerabilities, configuration details and inventory information.
  - Consumes negligible CPU asset and network resources
  - Is easy to deploy, and once deployed, keeps itself up to date automatically

- Extensive platform coverage:
  - Windows 7/Windows Server 2003 SP2 and later (x86, x64)
  - Red Hat Enterprise Linux/CentOS/Oracle Enterprise Linux 5, 6, 7 (x64)
  - Ubuntu 12, 14, 16 (x64)
  - Additional platform support coming soon for other Linux platforms.

Get started quickly with intuitive deployment and 'out-of-the-box' content

Whether you need file integrity monitoring for PCI, change control enforcement, or another regulatory requirement such as the EU's General Data Protection Regulation (GDPR), Qualys FIM is designed to be easy to configure, offering you maximum flexibility to tailor its capabilities to your organization's specific needs.

You can get started quickly with out-of-the-box monitoring profiles, pre-configured and tuned to monitor critical operating system binaries, configuration files, and other files critical to the security of the operating system. The rules are tested and calibrated by Qualys for accuracy and to reduce alert "noise".

- Ready-to-use profiles:
  - Cover recommended monitoring for PCI for Windows and Linux
  - Are periodically updated and tuned
  - Can be synced to the library for automatic updating
  - Will be expanded to cover other operating systems and applications such as databases, web servers, and more

- You can configure as many custom monitoring profiles as needed for different situations and apply these dynamically to your devices. The FIM application will automatically consolidate rules from multiple profiles, freeing you from the complexity of configuring monitoring on individual agents. You can easily configure monitoring for each of the following and apply the configurations to the appropriate systems based on tags:
  - Application and OS critical binaries
  - Configuration files
  - Application files such as web source
  - Archived logs, reports, and customer data
  - Rights and permissions for databases or log files

Track changes and discover incidents with centralized event search and powerful dashboards

Find related events quickly and track statistics across your entire environment to classify internal changes, identify malicious activity, and provide crucial information during response. Powerful dashboards provide flexible customizable views to fit a variety of change management and compliance needs.

- Qualys FIM logs and centrally tracks file change events across your global IT systems, making it easier than ever to investigate changes to assets, and uncover if they are due to normal events or malicious activity.
  - Mine all event data via a powerful search engine that lets you submit complex queries with multiple criteria and find similar events quickly across a single device or your entire IT infrastructure. This allows you to detect and identify critical changes, incidents and audit risks.
  - Visualize data via interactive, customizable widgets, charts and graphs in the dynamic dashboard, providing complete and instant visibility of file integrity statistics.
  - Drill down to details on events, assets, users and trends, and zero in on potentially damaging changes.
  - Access asset, vulnerability, compliance and inventory data shared across other Qualys apps and use these to refine searches and dashboard widgets.
  - Share findings by exporting events and generating custom reports tailored for different teams, such as security incident response and IT operations.

- With Qualys FIM, you can address all key security and compliance use cases that demand quick identification and tracking of changes to your IT assets including:
  - Change control policy enforcement
  - Audit requirements and compliance with regulations, such as Sarbanes-Oxley and the EU's General Data Protection Regulation (GDPR)
  - Adoption of security best practices, such as the CIS Critical Security Controls
  - Compromise detection & malicious activity

Powered by the Qualys Cloud Platform – the revolutionary architecture that powers Qualys' IT security and compliance cloud apps

Sensors that provide continous visibility

On-premises, at endpoints or in the cloud, the Qualys Cloud Platform sensors are always on, giving you continuous 2-second visibility of all your IT assets. Remotely deployable, centrally managed and self-updating, the sensors come as physical or virtual appliances, or lightweight agents.

All data analyzed in real time

Qualys Cloud Platform provides an end-to-end solution, allowing you to avoid the cost and complexities that come with managing multiple security vendors. The Qualys Cloud Platform automatically gathers and analyzes security and compliance data in a scalable, state-of-the-art backend, and provisioning additional cloud apps is as easy as checking a box.

Respond to threats immediately

With Qualys' Cloud Agent technology, there's no need to schedule scan windows or manage credentials for scanning. And Qualys Continuous Monitoring service lets you proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify you immediately.

See the results in one place, anytime, anywhere

Qualys Cloud Platform is accessible directly in the browser, no plugins necessary. With an intuitive, single-pane-of-glass user interface for all its apps, it lets you customize dashboards, drill down into details, and generate reports for teammates and auditors.

Cloud Platform Apps

Qualys apps are fully integrated and natively share the data they collect for real-time analysis and correlation. Provisioning another app is as easy as checking a box.

ASSET MANAGEMENT

- AI Asset Inventory
- SYN CMDB Sync

IT SECURITY

- VM Vulnerability Management
- TP Threat Protection
- CM Continuous Monitoring
- IOC Indication of Compromise
- CS Container Security

WEB APP SECURITY

- WAS Web App Scanning
- WAF Web App Firewall

COMPLIANCE MONITORING

- PC Policy Compliance
- PCI PCI Compliance
- FIM File Integrity Monitoring
- SCA Security Configuration Assessment
- CSA Cloud Security Assessment
- SAQ Security Assessment Questionnaire

Request a full trial (unlimited-scope) at qualys.com/trial

Qualys is easy to implement, easy to use, fully scalable – and require NO infrastructure or software to maintain.