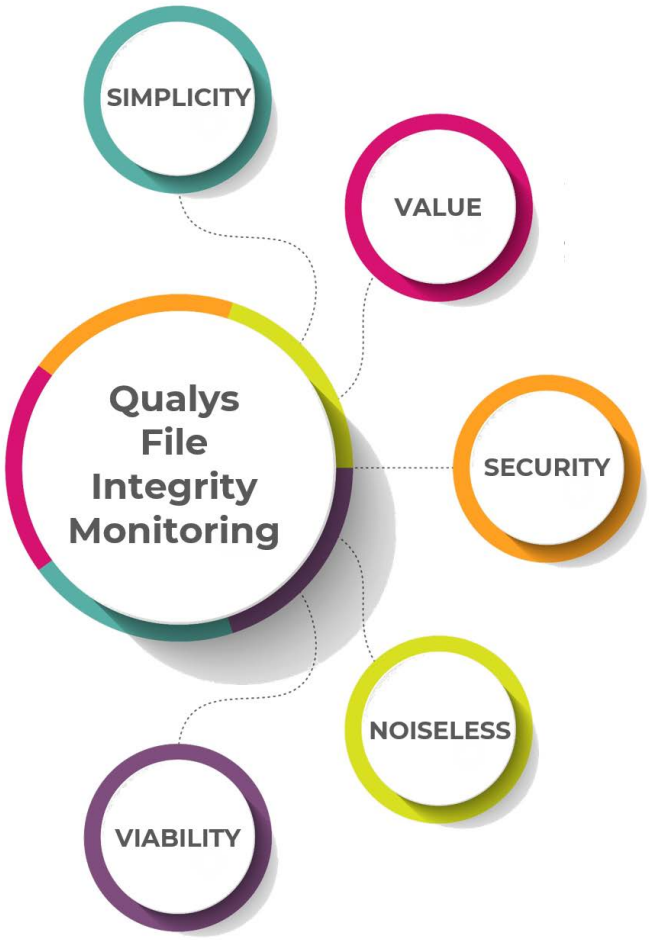
Qualys

Qualys File Integrity Monitoring

単一のプラットフォーム。単一のエージェント。完全なコンプライアンス。

コンプライアンスの確保とサイバーセキュリティの成熟度向上を実現する、ファイル整合性の動的な監視を可能にする単一のプラットフォームおよびエージェントです。

Qualys File Integrity Monitoring (FIM) は、*Vulnerability Management, Detection & Response (VMDR)* を強化し、コンプライアンスの確保とサイバー脅威からの組織の保護を支援します。



ノイズキャンセリング

脅威インテリジェンスデータを活用した独自のノイズキャンセリング技術により、FIM（ファイル整合性監視）の誤検知アラートを90%以上削減します。

検知のコンテキスト

日時、ユーザー、プロセス、プロセス所有者の詳細情報を含む、カーネル/ルートレベルでの変更検知。

ファイルアクセス監視

ホスト上の重要なファイルの中には、通常のユーザーによるアクセスを想定していないものがあります。こうしたファイルへのアクセスが試行されると、アラートが生成されます。

シームレスな統合

CI/CDワークフロー（ゴールデンイメージの作成など）やQualysアプリケーションと統合し、セキュリティポスチャーに関するコンテキストを提供します。

事前設定済みおよびカスタムプロファイル

アプリケーションや環境に合わせてプロファイルをカスタマイズしたり、標準（Out-of-the-box）プロファイルをベースに独自のプロファイルを作成したりすることが可能です。

拡張性の高いプラットフォーム

セットアップの手間を最小限に抑えたホスト型サービスにより、インフラへの負荷を軽減します。

脅威エクスポージャーを低減

アセットタグに基づく動的なポリシー設定により、新規アセットの自動検出と自動設定を実現します。

プラットフォームおよびネットワークの網羅的な対応

エージェントを導入できないネットワークデバイスの設定に関するアラート通知をサポートし、Microsoft WindowsやLinuxにも対応しています。

包括的なレポート機能

イベント、インシデント、アセットに関するレポート機能により、セキュリティの強化とコンプライアンスへの対応を確実にします。

監査に対応可能なコンプライアンスとセキュリティ強化を簡素化・実現する、単一のクラウドネイティブ・ソリューション。

Qualys FIMは、正常なイベントや悪意あるイベントに起因する重要な変更、インシデント、リスクを検知・特定するためのクラウドソリューションです。

Qualys File Integrity Monitoring (FIM) は、重要なファイル、ディレクトリ、レジストリパスの変更をリアルタイムで監視する、拡張性に優れたクラウドアプリケーションです。
本ソリューションは、PCI-DSS、CCPA、HIPAA、GDPRなどのコンプライアンス要件への準拠を支援します。

Qualys FIMの大きな特徴は、ノイズを最小限に抑えるよう厳選された、重要なファイルパスのライブラリです。これらのパスは恣意的に選ばれたものではなく、コンプライアンス要件を満たすために慎重に精査された、極めて重要なパスです。

Qualys FIMは、クラウド、オンプレミス、仮想環境にまたがるWindowsおよびLinuxシステム上のファイル変更をシームレスに監視します。PCI-DSS 4.0などの規制要件に合わせて事前に設定された監視プロファイルが用意されているため、セキュリティチームは監視対象の定義に時間を費やすことなく、変更イベントそのものへの対応に専念できます。直感的なダッシュボードにより、変更状況を継続的に把握できるほか、「何が・誰によって・いつ」変更されたかというコンテキストを含む詳細な情報を確認することが可能です。

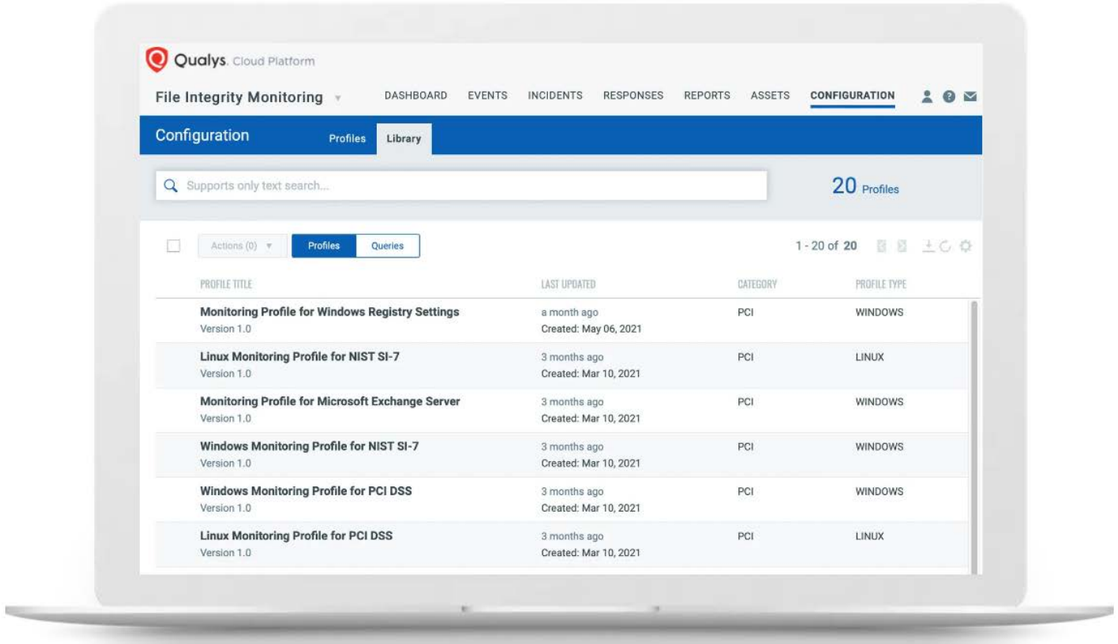
Qualys FIMは、ファイルレピュテーションや信頼性ステータス（Trust Status）に関する画期的な機能を備えており、悪意のある、あるいは不審なファイルの変更や、パッチ適用などの既知の活動に伴う正常な変更が誤って抑制される可能性のあるイベントについて、セキュリティチームに自動的に通知します。

Qualys FIMは、脅威インテリジェンス（特にファイルレピュテーションに関するコンテキスト）を統合することで、従来のイベント監視の枠を超えた機能を提供します。これにより、システム変更が不審なものか、あるいは悪意のあるものかを判断できるようになります。

クラウドベースのサービスであるQualys FIMを活用すれば、監視要件へのグローバルな準拠や変更に関するセキュリティコンテキストの把握のために、複数の個別ソリューションを導入・運用する際にかかるコストや複雑さを解消できます。

Qualys FIMは、エージェントレスのネットワークデバイスにも対応し、ネットワーク設定の逸脱を通知することで、効果的な監視と対応に必要な可視性を高めます。さらに、通常は使用されない重要なホストファイルへのアクセスを検知してアラートを発する「ファイルアクセス監視（FAM）」機能も備えています。

File Integrity Monitoring ダッシュボード



主なメリット

クラウドネイティブな可視性

結果を数秒で一元的に把握。
AssetViewなら、単一のダッシュボードから、すべてのIT資産の全体像を常に最新の状態で確認できます。

一元管理

多種多様な評価に向けたホスト資産の検出を一元化します。ビジネスの構造に合わせてホスト資産グループを構成できます。

容易な導入

Qualysが完全に管理するパブリッククラウドまたはプライベートクラウドから導入できます。サーバーのプロビジョニング、ソフトウェアのインストール、データベースの保守といった作業は一切不要です。

拡張性と柔軟性

オンデマンドでグローバルに規模を拡大できます。拡張性の高いXMLベースのAPIを介して、他のシステムと連携が可能です。Qualysは、GRC、チケット管理システム、SIEM、ERM、IDSなど、幅広いセキュリティおよびコンプライアンスシステムと組み合わせて利用できます。

シンプルさ

Windowsレジストリ設定向けのQualys FIM（ファイル整合性監視）プロファイルを使用すると、Windowsレジストリオブジェクトの変更を追跡し、資産を保護するための予防的な措置を講じることができます。

このプロファイルには、自動実行（Autoruns）、ブートシーケンス、ファイアウォール、その他の重要な機能に対する不正な変更を検知するための主要なレジストリオブジェクトが含まれています。

Qualys FIMには、コンプライアンスイベント、インシデント、および資産に関する自動生成レポート機能が備わっています。

価値

Qualys Cloud Agentは軽量かつ多機能なため、セキュリエィタスクごとに個別のエージェントを導入・管理する手間を省くことができます。

アセットタグに基づいた動的なポリシー設定を活用することで、IT部門の介入なしに新しいエセットを検出
し、FIM（ファイル整合性監視）用に自動設定することが可能です。また、すぐに利用可能なプロファイルがベースアイン設定を支援し、導入にかかる時間をさらに短縮します。

セキュリティ

Qualys FIMは、脅威インテリジェンスと連携してイベントの優先順位付けやノイズの低減を行い、変更イベントに関する高度なインサイトを提供します。これにより、コンプライアンス要件への適合を確実にするとともに、セキュリティ体制を強化し、セキュリティインシデント、コンプライアンス違反による罰金、訴訟などのリスクを未然に防ぐことが可能になります。

また、Qualys FIMは13ヶ月間のデータ保持期間を設けており、インシデントのフォレンジック分析に必要なすべてのイベントに即座にアクセスできます。

ノイズレス

多くのFIMソリューションは、ITチケットの発行やアナリストによるトリアージ（優先順位付け）を必要とする誤ったアラートを生成しがちです。そのため、組織はIT担当者やアナリストの業務時間の25%を、こうしたアラートの選別や確認に費やしていることが少なくありません。

Qualys FIMは独自のノイズキャンセリング技術を搭載しており、誤ったアラートを90%以上削減します。さらに、信頼できるソース（Trusted Source）やファイルのレピュテーション（評価）に関する情報を付加してイベントデータを強化することで、ノイズを抑制し、イベントの優先順位付けを適切に行えるようにします。

実現可能性

Qualys FIMは、データの保存、相関分析、および分析にQualys Cloud Platformを活用するため、オンプレミスのコンピューティングリソースやストレージを必要としません。

Qualys FIMは、手動および自動でのインシデント作成が可能なインシデント管理ワークフローを提供します。この機能は柔軟な設定が可能であり、特定の条件に基づいてインシデントを自動生成するように設定できます。

Before Qualys FIM	After Qualys FIM
Alert fatigue, needed noise reduction	Noise cancellation, automated noise whitelisting
Difficulty deciding 'what to monitor'	Pre-configured FIM profiles for OSes & apps
Lacked asset scope visibility	Automated reporting for non-compliant FIM assets
Siloed agents for VM and compliance	Single agent for real-time, global visibility and response
Complex FIM policies with hundreds or thousands of rules	Better coverage with far fewer number of rules
Legacy interface, difficult to configure and manage	Portal-based FIM solution with automated compliance reporting and incident management

The time between the FIM setup and generation of the first change event was less than five minutes.

Simple Migration

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

Qualys FIM ★★★★½

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.

PCI DSS 4.0に対するQualys FIMのサポートについては、こちらをご覧ください。

Qualys FIMのパブリックAPIについては、こちらをご覧ください。

Qualys File Integrity Monitoring（FIM）の詳細を確認し、30日間の試用をお試しください。

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**