コンプライアンス対策の自動化
Qualys FIM(ファイル整合性監視)のご案内

Qualys Japan K.K
更新日2026年６月

Qualys FIMが必要な理由

File Integrity Monitoring (FIM) は、中小企業から大企業まで、あらゆる規模の企業ネットワークにおいて不可欠な防御層です。コンプライアンスの確保やサイバーセキュリティのベストプラクティスの実践には、自社の組織に最適なFIMを選定することが極めて重要です。優れたFIMソリューションには、ノイズ（不要な通知）の抑制機能、ファイルアクセス監視（FAM）機能、そしてネットワーク機器監視のためのエージェントレス対応機能が備わっている必要があります。

多くの企業は、PCI DSS 4.0やその他の国際的・米国の州法といった数多くの規制や要件を遵守しなければなりません。

これらに違反した場合、厳しい制裁が科される可能性があります。企業は監査不合格、罰金、訴訟、ブランド毀損といったリスクに直面しており、その対応にかかる平均コストは、侵害への対処に400万ドル超、訴訟に400万ドル、監査不合格への対応に1,500万ドルに達しています。

また、多くの組織が、米国国立標準技術研究所（NIST）やCenter for Internet Security（CIS）が提供するものなど、1つ以上のサイバーセキュリティ・フレームワークを導入しています。

FIM未導入によるリスク

- ランサムウェアによる重要ファイル改ざん
- 管理者権限の不正利用
- Webサイト改ざん
- 設定変更によるシステム障害
- PCI DSS監査不適合
- 監査証跡不足による対応工数増大

- 侵害対応コスト：400万ドル超
- 訴訟コスト：400万ドル
- 監査不合格対応：1500万ドル

Qualys FIM

File Integrity Monitoring

オペレーティングシステム、アプリケーションソフトウェア、ファイルのリアルタイムの整合性を継続的に監視および検証し、不正な変更に対して迅速にアラートを発生させ、システムのセキュリティと信頼性を確保する内部統制またはプロセスを実現！

PCI DSS 4.0、HIPAA、NERC CIP、GDPR、CCPA、NISTなどの規制コンプライアンスフレームワークに準拠するための機能の1部を提供します。

アラート疲れを軽減！リアルタイムのアラート、「すべて」を監視するために必要な多くの誤警報を削減します。

監査用のすべてのデータを保存し、監査用のレポートを作成し、無関係なデータを無視する費用対効果の高い実装を提供します。

PCI Security Standards Council

U.S. Department of Health and Human Services
Enhancing the health and well-being of all Americans

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

GDPR.EU

California Consumer Privacy Act (CCPA)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Qualys.

リアルタイムモニタリング

イベントの詳細を網羅的にキャプチャ

ユーザー識別

プロセス情報

イベントの種類

日付と時刻

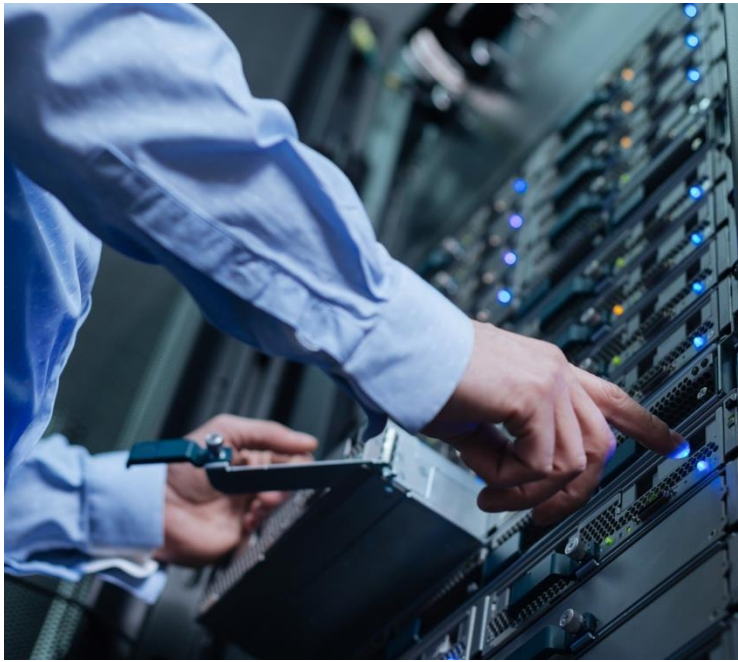
成功と失敗の表示

イベントの起源

影響を受けるデータまたはシステムコンポーネントの ID または名前

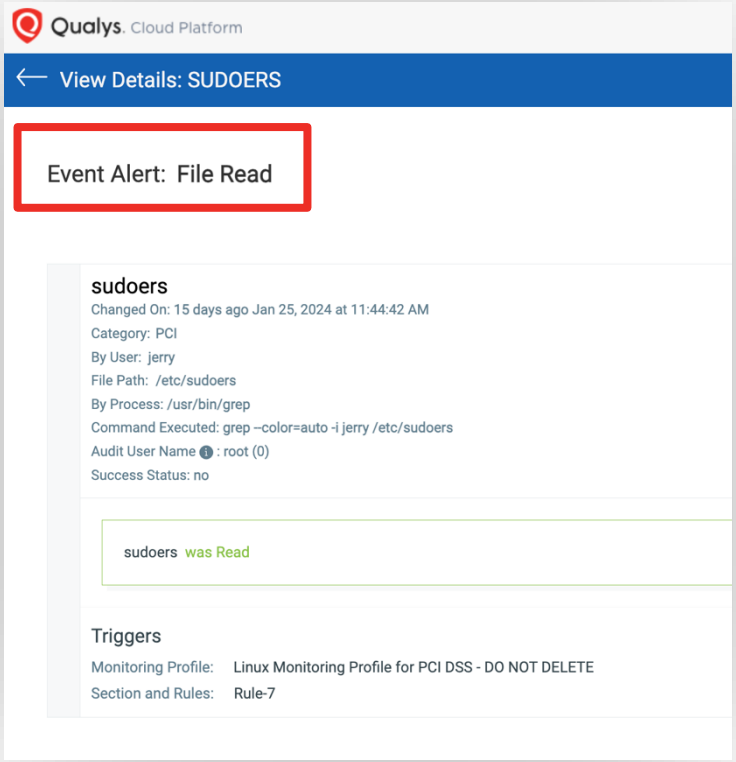
ファイル、フォルダ、レジストリ、オブジェクト

変更のリアルタイムモニタリング



ファイルアクセス監視(FAM)

- 機密ファイルへのリアルタイムトラッキングアクセス
- 包括的なアクセスイベントの詳細、ユーザーとプロセス情報を収集
- 管理者アクセスの検出、権限アクセス権の不正使用の追跡
- コンプライアンスおよび規制要件を満たす コンプライアンスコントロールにより、組織は機密データを含むファイルへのアクセスイベントを記録することが義務付けられています



Qualys.

FIMだけでは不十分　～FIMとFAMの用途の違い

FIMは「何が変更されたか」を監視し、FAMは「誰がアクセスしたか」を監視します。両者を組み合わせることで、改ざんだけでなく不正アクセスや情報漏えいの兆候まで包括的に可視化できます。

FIM	FAM
変更を検知	アクセスを検知
改ざん後に把握	試行段階で把握
Whatが分かる	Whoが分かる
ファイル変更	ファイルアクセス

サイバーセキュリティの成熟度向上におけるFAM活用例

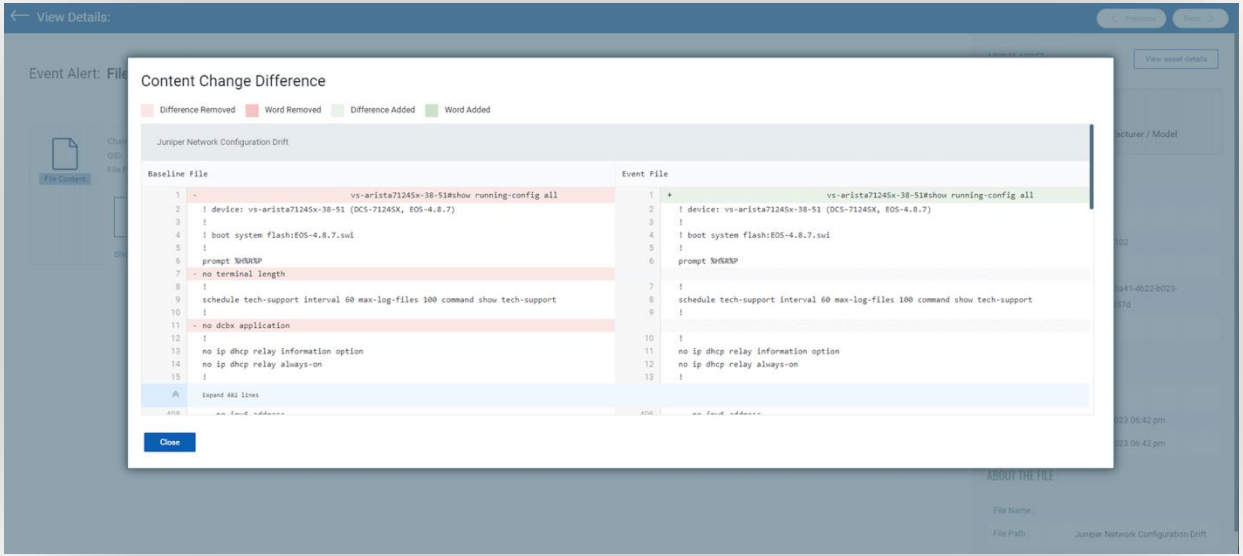
不正アクセスの検知
権限のないユーザーが機密ファイルへのアクセスを試みた場合、その操作を即座に検知し、内部不正やアカウント侵害の早期発見につなげます。
特権アカウントの監視
管理者や特権ユーザーによる機密情報へのアクセス状況を可視化し、権限の悪用や不適切な操作を検知します。
データ窃取リスクの低減
機密ファイルへのアクセスをリアルタイムで監視することで、不正なデータ持ち出しや情報漏えいの兆候を早期に把握できます。
ランサムウェア攻撃の早期発見
短時間に大量のファイルへのアクセスや変更が発生した場合、ランサムウェアによる暗号化活動の可能性を検知し、迅速な対応を支援します。

エージェントレス FIM ～ネットワーク デバイスにおけるFIM

Qualysは、JuniperOS、Arista、Palo Altoなどのネットワークデバイスを対象とした、エージェントレスのファイル整合性監視（FIM）機能を提供します。この機能は、定期的なスキャン時にネットワーク設定の差異を正確に特定してアラートを生成し、設定のどのような変更が行われたかについて詳細な情報を提供します。

- ネットワーク設定の変更に関するアラートを発信
- エージェントのないデバイスでベースラインからの変更を追跡する

- 包括的なイベントの詳細:変更点に関する詳細なインサイト



Qualys.

アラートによる疲労を最小限に抑える

調整およびキュレーションされたプロファイル:進行中のイベントを「最適化されたプロファイル」により最小限に抑え、「ノイズ」なしで特定のコンプライアンスフレームワークに関連するイベントを送信します。

脅威インテリジェンス: 悪意のあるハッシュや疑わしいハッシュを検出するための脅威インテリジェンスが組み込まれています

単一ペイン:Qualysのアセットおよびデータと完全に統合されたネイティブダッシュボード

必要なものだけをエクスポート:SIEMツールと統合し、重要なイベントのみを送信します。

ユーザーとプロセスベースのイベント抑制:イベントの90%を排除し、既知の良好なユーザーとプロセスによって生成されたFIMイベントを除外します。

Qualys.

セットアップが簡単！
15分で最初のイベントを収集

同じ Qualys エージェント：新しいエージェントをインストールする必要はありません

同じQualysクラウドプラットフォーム:インストールする必要はなく、ストレージとスケールについて心配する必要はありません

すぐに使用できる調整されたプロファイル:必要なデータのみを収集するように自動構成します-　例）PCIプロファイル

インシデント管理とコンプライアンスレポートが組み込まれています。

使いやすく、あらゆる監査目的に対応しています。他の製品をセットアップして購入する必要はありません。

FIMソリューションはリソースを大量に消費する可能性がありますか？

軽量エージェント: Qualys エージェントは軽量で、11 MB 未満で、CPU を 2% 以上消費しないように構成できます。Qualysエージェントは、インストールが簡単でメンテナンスフリーになるように設計されています。さらに、Qualys は 1 つのエージェントを使用するため、エンドポイントの合計消費量は少なくなります。

最も包括的なFIMカバレッジを提供するプラットフォーム

Scanner Appliance

エージェントレス FIM

ネットワークデバイス上のスキャンベースのFIM

ルーター、スイッチ、ファイアウォールなどのネットワーク機器の設定変更を検出します。

Cloud Agent

エージェントベースのFIM

サーバーとエンドポイントのリアルタイム監視

リアルタイムファイルアクセス監視(FAM)

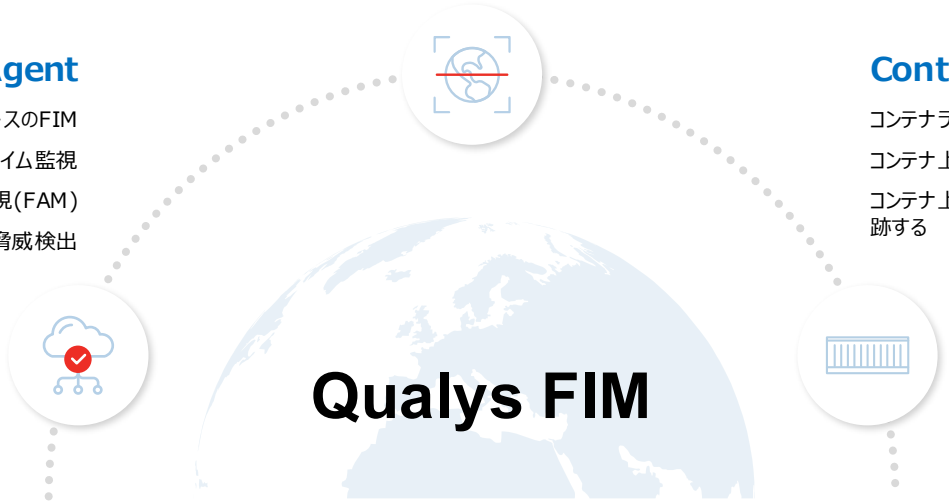
脅威検出

Container Sensor

コンテナランタイムセキュリティ

コンテナ上のリアルタイムFIM

コンテナ上の重要なファイルへの不正アクセスを追跡する

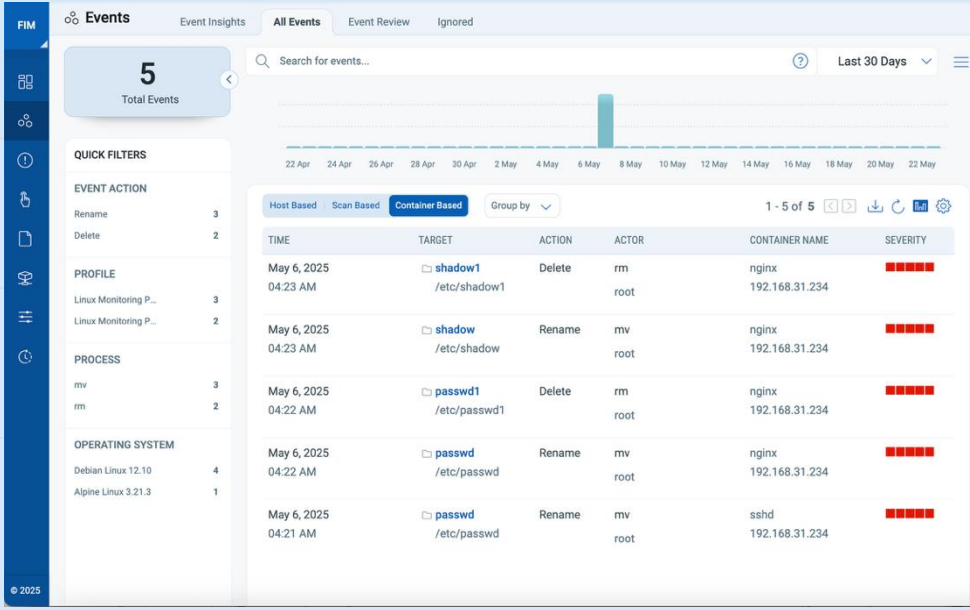


Qualys

統合ファイル整合性監視

ホストやコンテナを横断してPCI DSS 4.0のニーズを満たす

- すべてのFIMに一つのモジュールを
- Kubernetesコンテキストで優先順位付け
- 大規模モニタリングのカスタマイズ
- ファイルアクセスロックなどのレスポンシブな対応を取る



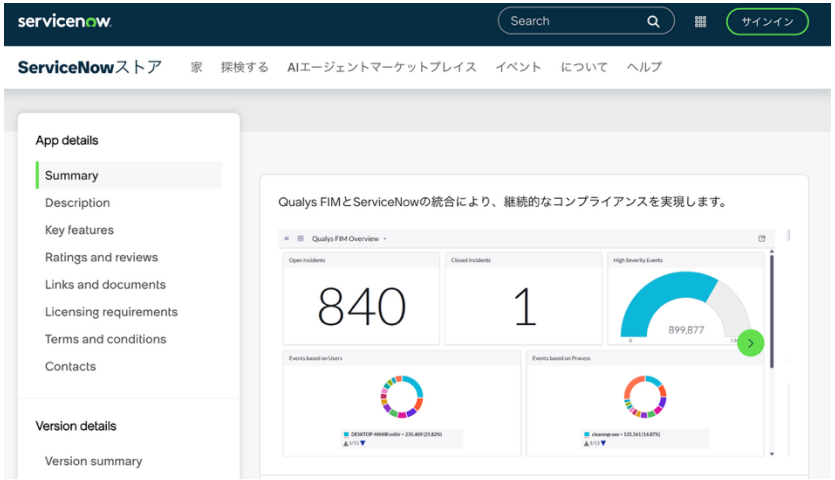
Unify All Your File Integrity Monitoring Across Hosts and Containers

Qualys.

SNOW との統合

主なメリット

- ファイル変更検知を**自動的にインシデント化**
- ServiceNowの既存ワークフローで**即時対応・トラッキング**
- セキュリティイベントから対応までの**完全な自動化を実現**
- 構成変更・権限変更・不審変更を**一元管理**
- 変更履歴をインシデントとして蓄積し、**監査証跡を自動生成**
- 手動対応の削減により、**SOC運用負荷を大幅軽減**
- 優先度に応じた**インシデント対応の標準化**
- SLAに基づく**対応時間の可視化・改善**
- スケジュール・オンデマンド両方の同期に対応
- コンフィグレーションデータ（CMDB）と連携し、**影響範囲を即把握**
- リアルタイム監視により、**変更リスクの早期検知**
- 複数環境（クラウド／オンプレ）を跨いで**統合可視化**
- 変更イベントとITSMを連携し、**DevSecOpsを促進**
- PCI DSS / HIPAA / SOX / NISTなどの**コンプライアンス対応を効率化**
- セキュリティとIT運用のサイロを解消し、**チーム連携を強化**



Qualys.

クォリスのFIMを選択すべき理由

01 **同一エージェント,**サイロ化されたツールの必要性を排除する

02 PCI 4.0に向けすぐに使えるセットアップで、**最も簡単なオンボーディング**

03 **最大データ保持:**追加費用なしで**15ヶ月のホットストレージ(競合他社は30～60日、追加費用あり)**

04 「FIMプロファイルの調整」と「高度なユーザー/プロセスレベルのフィルタリング」による**最小ノイズ**

05 サーバー、エンドポイント、ネットワークデバイス、コンテナに対する**最も包括的なFIMカバレッジ**

成果

FIM管理の運用コストを大幅に削減

PCI DSS 4.0 FIM要件の達成

Qualys.

Qualys | De-risk Your Business

製品紹介およびDemoリクエストなどは
sales-jp@qualys.comまでお問い合せください。

解決したい課題

- 「いつ・誰が・どのファイルを変更したか追えない」
- 設定変更ミスによるシステム停止や障害の発生
- マルウェアやランサムウェアの侵入に気づけない
- 内部不正（情報持ち出し・改ざん）の検知ができない
- 監査対応の証跡収集に工数がかかる
- PCI DSS / ISO27001などのコンプライアンス対応が大変

FIM 導入事例（金融機関の場合）

課題
- PCI DSS（要件11.5）でFIMが必要
- 本番サーバの変更履歴が不透明
- 内部監査で「証跡不足」を指摘

導入内容
- 重要サーバ（決済系・顧客DB）へのFIM導入
- /etc, /varアプリ設定ファイルを監視
- 変更ログの一元管理

導入効果
- 監査対応時間を約70%削減
- 誰がいつ変更したかを即時可視化
- PCI DSS監査をスムーズに通過

FIM 導入事例（EC企業の場合）

課題
- Web改ざんリスク（不正スクリプト埋め込み）
- -攻撃を受けても検知が遅れる-
- DevOpsで変更が頻繁に発生

導入内容
- Webサーバのコンテンツ監視
- `/var/www/html`配下をリアルタイム監視
- 異常変更時にSOCへ通知

効果
- 改ざん検知までの時間が「数日 → 数分」に短縮
- 不正JavaScript埋め込みを即時検知
- ブランド毀損リスク低減

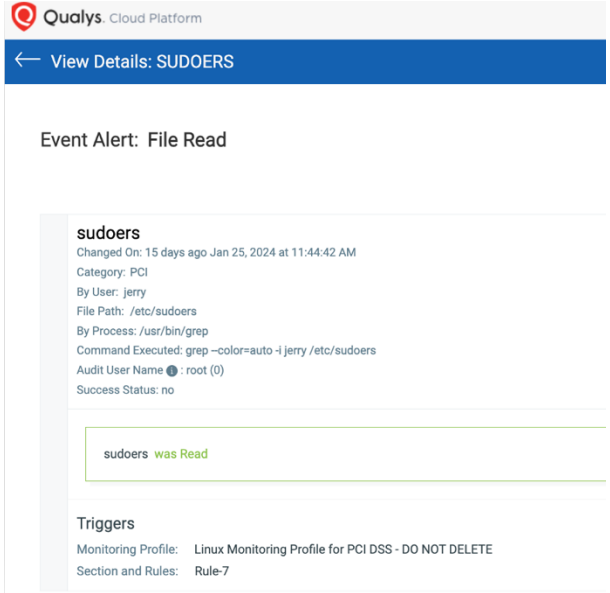
Qualys.

FIM

File Integrity Monitoring

不正なファイル、フォルダ、レジストリ、オブジェクトアクセスをリアルタイムに監視、記録し、アラート通知するコンプライアンスに不可欠な機能

カテゴリ	機能	説明
リアルタイム監視	ファイル、フォルダ、レジストリの変更を即時検出	システムファイルや設定の変更をリアルタイムで検知し、詳細を記録。
ユーザー操作の追跡	操作記録「誰が・いつ・どのように」	操作ユーザーや変更内容を詳細に記録。
アラート・レポート	自動通知と監査レポート	不正な変更の通知とコンプライアンス対応レポートを生成。
ファイルアクセス監視（FAM）	アクセス試行の記録	機密ファイル等へのユーザーアクセス履歴を詳細に記録。
エージェントレス監視	ネットワーク機器の監視	ルーターやファイアウォールなども対象。
コンプライアンス対応	規制準拠	PCI DSS、HIPAA、GDPR、NISTをなどに対応。
誤検知の削減	アラート精度向上	信頼された変更をホワイトリスト化し不要なアラートを最大90%削減。
一元管理とダッシュボード	ワンプラットフォームによる統合監視	複数環境（オンプレミス、AWS、Azureなど）を統合



PCI Security Standards Council
California Consumer Privacy Act (CCPA)
GDPR.EU
U.S. Department of Health and Human Services
NERC
NIST

Qualys FIM 導入効果（数値実績）

指標	導入前	導入後	改善率
不正変更の検知時間	数日から数週間	数分からリアルタイム	最大99%短縮
証跡収集・ログ確認	数日～数週間	数分～数時間	60～80%削減
原因特定時間	数時間～数日	数分～数時間	50～70%短縮
重大インシデント	基準値100	60～80	20～40%削減
構成ミスによる障害	100%基準	50～60%	40～50%削減
アラート調査時間	基準値100	50～70	30～50%削減

「Qualys FIMの導入により、検知速度がリアルタイムとなり、ファイル変更の監視・ログ化によりSOC効率が上昇します。迅速なインシデント対応によりMTTが目に見えて短縮します。」

Qualys.