



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

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。



**California Consumer
Privacy Act (CCPA)**



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

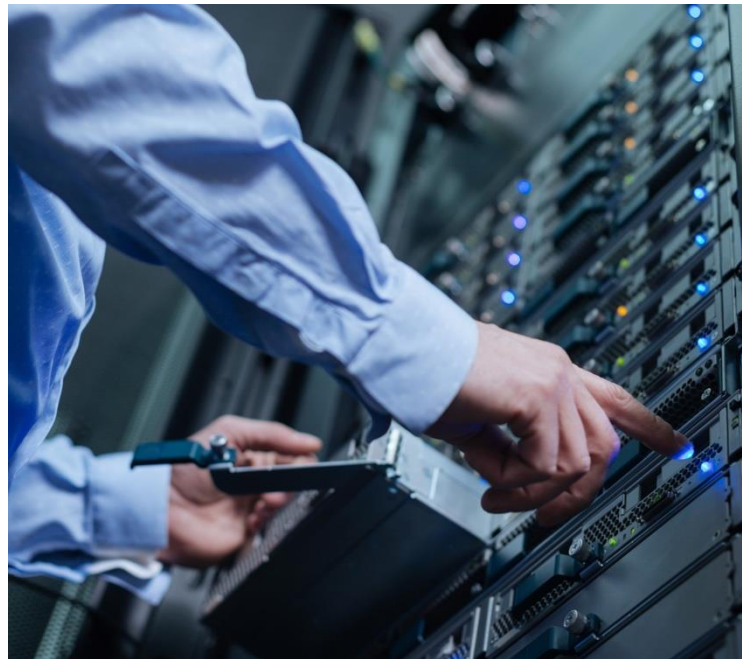
成功と失敗の表示

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. Cloud Platform

← View Details: SUDOERS

Event Alert: File Read

sudoers

Changed On: 15 days 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

sudoers was Read

Triggers

Monitoring Profile: Linux Monitoring Profile for PCI DSS - DO NOT DELETE

Section and Rules: Rule-7

エージェントレス FIM: ネットワーク デバイス上の FIM



- 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

← View Details: Event Alert: File

Content Change Difference

■ Difference Removed ■ Word Removed ■ Difference Added ■ Word Added

Juniper Network Configuration Drift

Baseline File	Event File
1 - vs-arista71245x-38-51show running-config all	1 + vs-arista71245x-38-51show running-config all
2 ! device: vs-arista71245x-38-51 (DCS-71245X, EOS-4.8.7)	2 ! device: vs-arista71245x-38-51 (DCS-71245X, EOS-4.8.7)
3 !	3 !
4 ! boot system flash:EOS-4.8.7.swi	4 ! boot system flash:EOS-4.8.7.swi
5 !	5 !
6 prompt %\$K&P	6 prompt %\$K&P
7 - no terminal length	
8 !	7 !
9 schedule tech-support interval 60 max-log-files 100 command show tech-support	8 schedule tech-support interval 60 max-log-files 100 command show tech-support
10 !	9 !
11 - no dbx application	
12 !	10 !
13 no ip dhcp relay information option	11 no ip dhcp relay information option
14 no ip dhcp relay always-on	12 no ip dhcp relay always-on
15 !	13 !

Expand 482 lines

Close

ABOUT THE FILE

File Name: Juniper Network Configuration Drift

File Path: Juniper Network Configuration Drift

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。



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

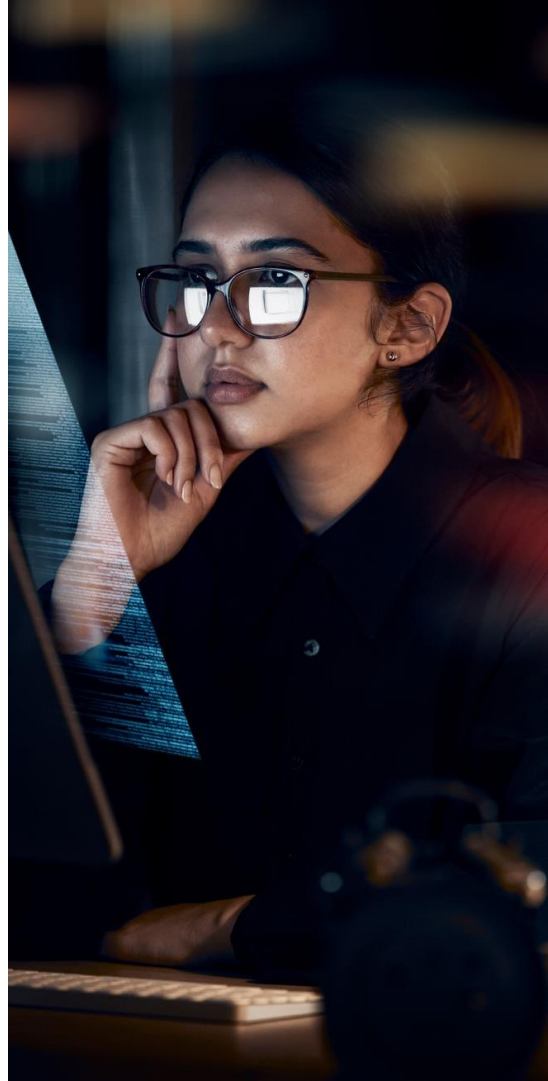


インシデント管理とコンプライアンスレポートが組み込まれています。

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



Qualys FIM

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

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



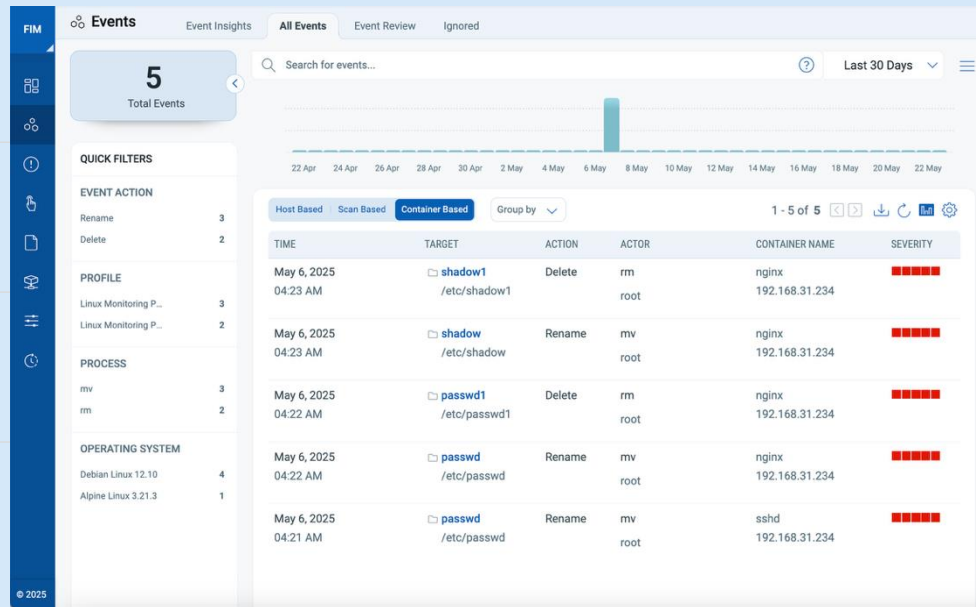
Kubernetesコンテキストで優先順位付け



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スな
対応を取る

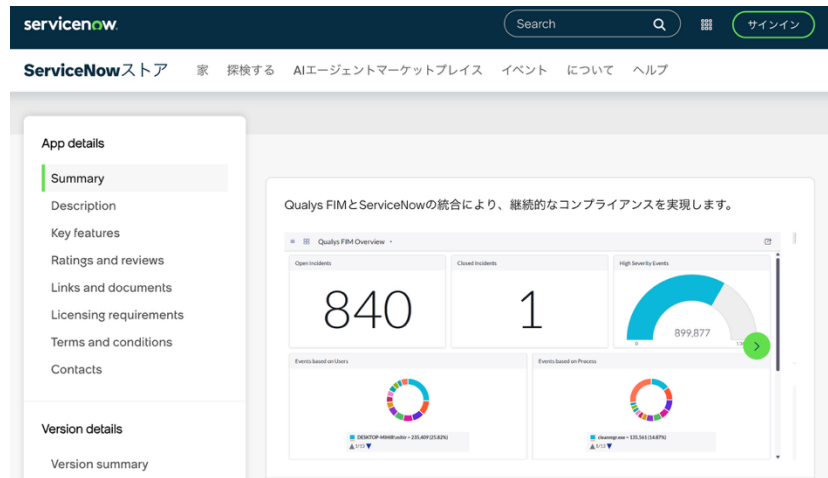


Unify All Your File Integrity Monitoring Across Hosts and Containers

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**



クオリスの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®

De-risk Your Business

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

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



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

Qualys Cloud Platform

← View Details: SUDOERS

Event Alert: File Read

sudoers
Changed On: 15 days 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

sudoers was Read

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

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。」