WHITEPAPER

FIMによるセキュリティおよびポリシー・コンプライアンス違反の防止

リスクとコストを低減するためのファイル整合性監視（FIM）の必須要件

目次

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。FIMソリューションは、重要なシステムファイルやレジストリに対する不正な動きを特定し、変更内容を診断した上で、アラートを送信します。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。

以下では、厳格なサイバーセキュリティ・フレームワークやコンプライアンス要件を満たし、かつ企業の攻撃対象領域、複雑性、コスト、リスクの低減を可能にするFIM（ファイル整合性監視）ソリューションに不可欠な要件について、詳細に解説します。

I. リアルタイム・ファイル・アクセス・モニタリング

File Access Monitoring (FAM) は、機密性の高いファイルへのアクセスを追跡・記録するセキュリティ対策です。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が発生した際にアラートを発報できるよう、FIMソリューションにはFAMの機能が組み込まれている必要があります。サイバーセキュリティのベストプラクティスを実践し、コンプライアンスの最低要件を満たすためにも、FIMソリューションにはFAMを含めるべきです。例えば、PCI DSS 4.0の多くの要件において、現在ではアクセス・モニタリングが規定されています。FAMソリューションは、機密情報へのアクセスに関する包括的な情報を捕捉できるように設計される必要があり、その情報には以下が含まれます。

ユーザー情報

特定のファイルへのアクセスを試みるユーザーに関する情報です。この情報は、説明責任を果たす上でも、また、権限を持つユーザーと持たないユーザーを識別する上でも極めて重要です。

タイムスタンプ

ファイルへのアクセスが発生した正確な時刻。

アクセスされたファイルの詳細

名前や場所など、アクセス対象のファイルに関する情報。
これにより、ファイルに対する操作状況をより詳細に把握することが可能になります。

プロセス

ファイルへのアクセスに使用されるプロセスや手法に関する詳細。

ホストの詳細

ファイルアクセスが行われるホスト。こうした詳細な情報は、ユーザーの特定を強化し、ユーザーに自身の行動に対する責任を負わせるのに役立ちます。

FAM（ファイルアクセス監視）は、脅威の特定やコンプライアンスの達成を目指す組織にとって、大きな「ギャップ」であると同時に「機会」でもあります。ギャップとされる理由は、組織が「すべてのファイルアクセス（成功・失敗を問わず）を記録する機能」の必要性を認識しつつも、システムパフォーマンスへの負荷を懸念し、特定の状況下を除いてはその機能を有効にしない場合があるためです。

以下に、FAMの典型的なユースケースを2つ挙げます。

ユースケース1: サイバーセキュリティの成熟度

- 不正アクセスの検知: 機密ファイルへのアクセスを試みる権限のないユーザーの検知。
- 管理者によるアクセスの検知: 特権ユーザーが管理者権限を悪用し、機密データを含むファイルにアクセスする行為の検知。
- 機密ファイルへのアクセスをリアルタイムで監視しないことによるリスク: データ窃取が見過ごされる恐れがあります。
- 短期間における大量のファイルへのアクセスや変更: ランサムウェア攻撃が進行中であることを示す兆候となる可能性があります。

ユースケース2: コンプライアンスおよび規制要件への対応

コンプライアンス規定により、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組織に義務付けられています。

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

- 情報システムの活動状況のレビュー（必須）。監査ログ、アクセスレポート、セキュリティインシデントの追跡レポートなど、情報システムの活動に関する記録を定期的にレビューする手順を導入してください。

PCI DSS 4.0

- 10.2.1.1 カード会員データへの個々のユーザーによるすべてのアクセスを記録する必要がある。カード会員データへの個々のアクセスを記録することで、どのユーザーアカウントが侵害されたり悪用されたりした可能性があるかを特定できるためである。
- 10.2.1.2 管理者によるすべてのアクセスを記録する必要がある。「administrator」や「root」アカウントのように高いアクセス権限を持つアカウントは、システムのセキュリィや運用機能に重大な影響を及ぼす可能性があるためである。
- 10.2.1.3 N監査ログへのすべてのアクセスを記録する必要がある。悪意のあるユーザーは、自身の行為を隠蔽するために監査ログの改ざんを試みることが多いためである。アセスを記録しておくことで、組織はログの不整合や改ざんの疑いがある箇所を、特定のユザーアカウントにまで遡って追跡できるようになる。
- 10.2.1.4 すべての無効なアクセス試行が確実に記録されるようにする必要がある。

Critical Security Controls Version 8

- 3.14: 機密データへのアクセスをログに記録する

NIST Special Publication 800-53 Revision 4

- AU-2: 監査イベント

Cloud Controls Matrix v4.0

- DSP-17: 機密データの保護
- LOG-04: 監査ログへのアクセスと説明責任

GDPR

- この欧州の規制では、不正なデータアクセスには、送信、保存、またはその他の方法で処理される個人データの偶発的または違法な破壊、紛失、改ざん、あるいは不正な開示が含まれると定められています。機密データに対する承認済みおよび未承認のアクセスを監視することは、データ侵害を早期に検知する上で不可欠です。

IS027001

ISO規格では、ファイルサーバーのアクセスログを解釈・分析できる能力が求められています。FAMは、セキュリティ担当者が直面する以下のような課題を解決します。

- 重要ファイルへのアクセス詳細やアクセス試行状況を即座に可視化する。
- 記録されたイベントに対し、レビュー、フィルタリング、検索を容易に行えるようにする。
- 不審なファイル操作や、特定の極めて機密性の高い情報へのアクセス試行に対し、自動的にインシデントを生成する。
- ファイルアクセスイベントの詳細な監査証跡を示すコンプライアンスレポートを自動生成する。

- アラート疲れ: ファイルアクセスの監視は膨大なデータを生成するため、FAMソリューションには、日常的なイベントと実際のセキュリティインシデントを識別し、ノイズを抑制する機能が求められます。

FAMの機能要件

上記のセキュリティおよびコンプライアンス要件を満たすため、FAMには以下の機能が求められます。

FAM要件	Qualys FAMによるサポート
リアルタイムのFAMアラートを生成する機能	Yes
FAMイベントに対するインシデントを自動生成する機能	Yes
FAMイベントに関するコンプライアンスレポートを自動生成する機能	Yes
アクセスアラート用のカスタムファイルを追加する機能	Yes
信頼できるユーザーやプロセスによる**ノイズを抑制**するための、ユーザーおよびプロセスに基づく包含・除外フィルターを追加する機能	Yes
WindowsおよびLinuxの両OSに対応したリアルタイムFAM機能	Yes

FAMイベントで記録すべき詳細には、以下を含める必要があります。

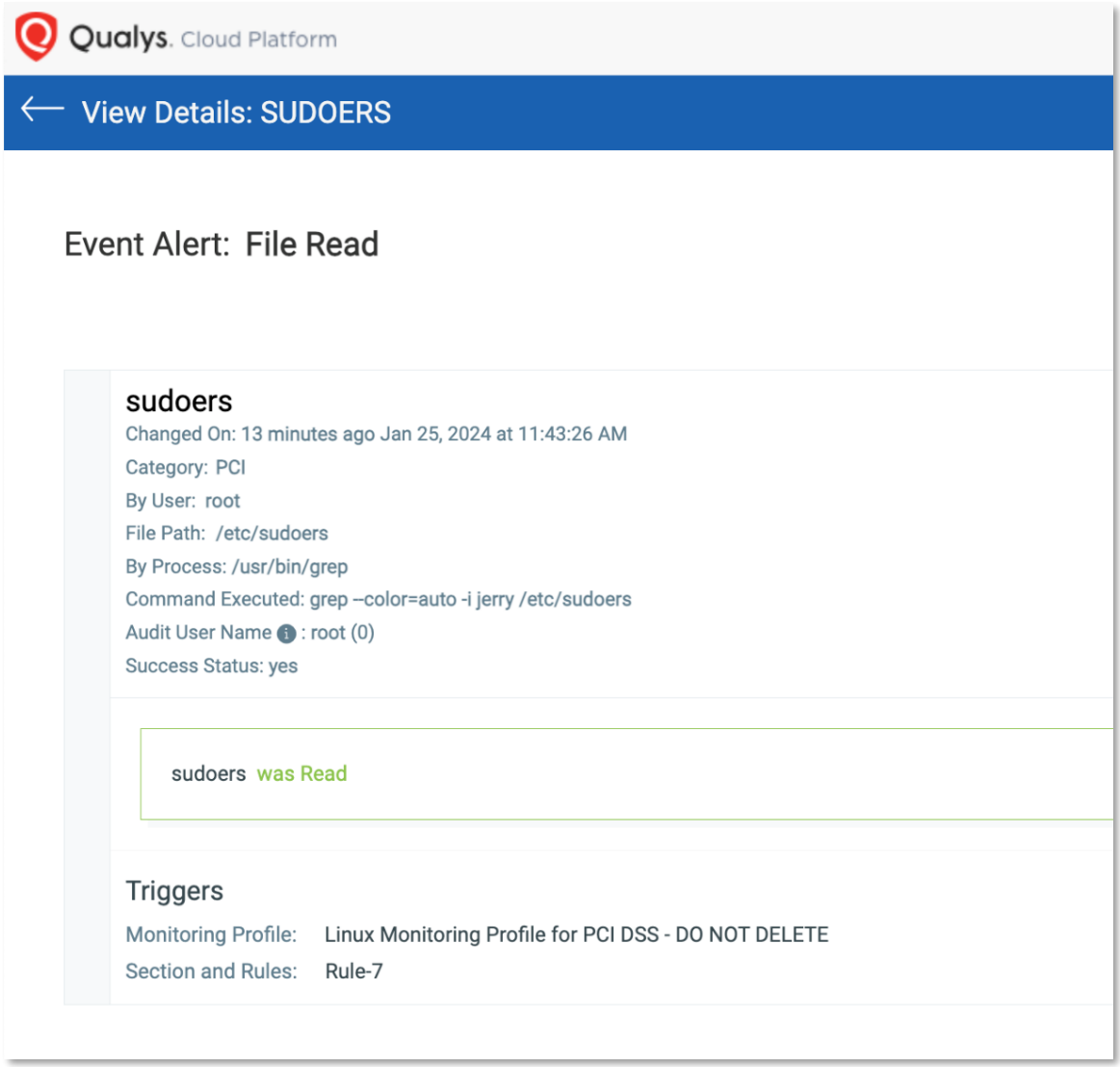
FAMイベントで記録すべき詳細事項	Qualys FAMによるサポート
ユーザー情報 特定ファイルへのアクセスを試みたユーザー情報。この情報は、説明責任を果たす上でも、権限のあるユーザーと権限のないユーザーを識別する上でも極めて重要です。	Yes
タイムスタンプ ファイルへのアクセスが発生した正確な日時。	Yes
アクセスされたファイルの詳細 ファイル名や保存場所など、アクセス対象のファイルに関する情報。これにより、ファイルに対する操作をより詳細に把握できます。	Yes
プロセス ファイルへのアクセスに使用されたプロセスや手法に関する詳細。	Yes
ホスト情報 ファイルへのアクセスが行われたホスト。	Yes

FAMのコンプライアンス要件

優れたFAM（ファイルアクティビティ監視）ソリューションには、ファイルアクセスを追跡する機能が不可欠です。これは、GDPR、HIPAA 2023、PCI DSS 4.0、GLBA、DORA、SOX、FISMA、ISO 27001、その他関連する規制によって義務付けられているコンプライアンス要件だからです。

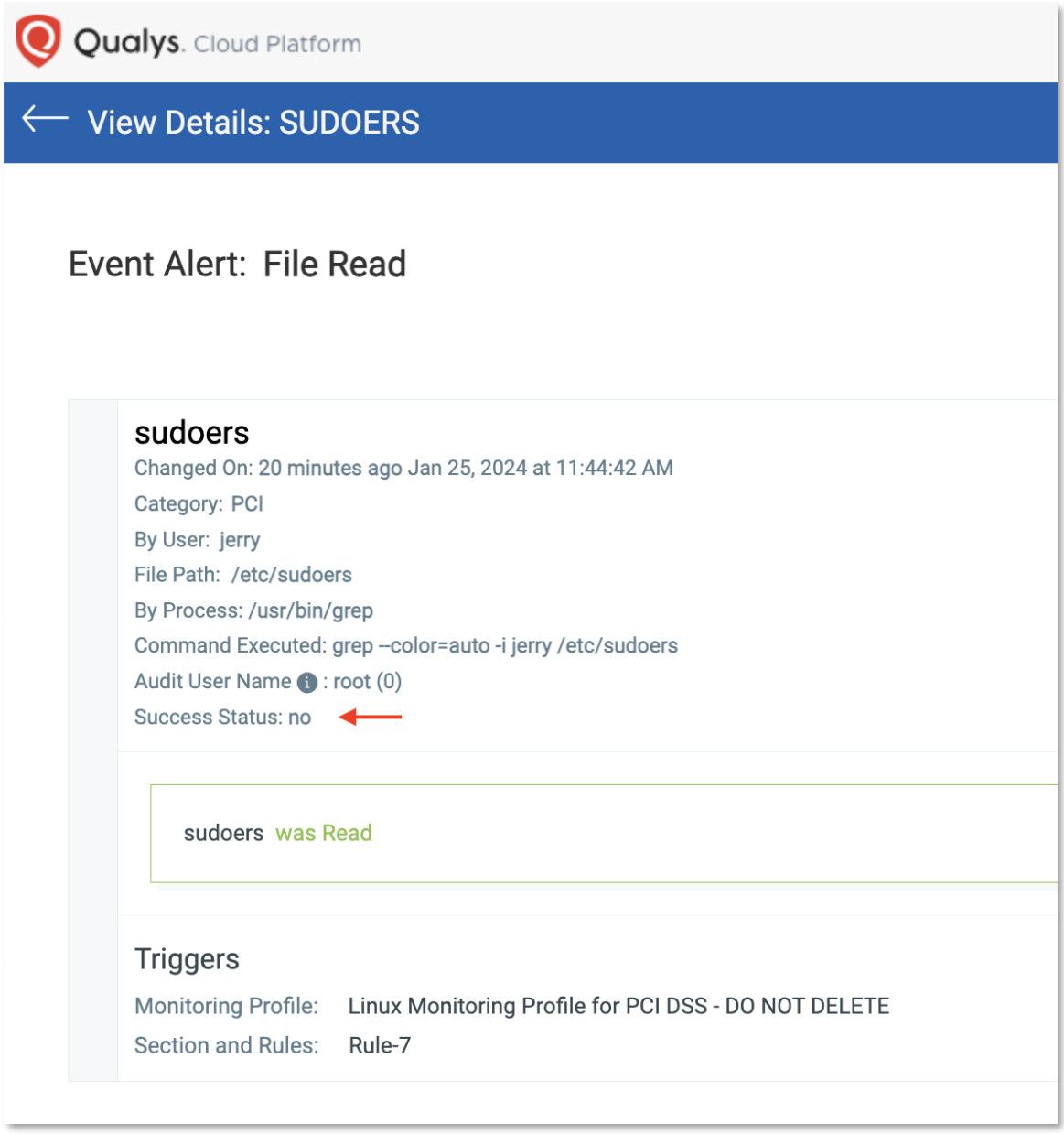
Qualys FAMの活用例

以下は、特権ユーザー「root」が「sudoers」ファイルにアクセスしようとした際に、Qualys FIMによって記録されたFAMイベント詳細の例です。詳細なイベント情報の一部として、「誰が（who）」「いつ（when）」「何を（what）」「どこで（where）」という必要な情報がすべて記録されています。



PCI DSS 4.0の要件では、監査ログにイベントの成否（成功または失敗）を記録することが求められています。

Qualys FAMは、アクセスに失敗した試行についてもイベントを記録することで、プロアクティブなアプローチを実現しています。例えば、一般ユーザーが厳重にアクセス制限されたファイルにアクセスしようとし、権限不足によりオペレーティングシステムからアクセスを拒否された場合、Qualys FAMは直ちにQualys FIMアプリ内でイベントを生成します。このイベントでは、成功ステータスが「No（いいえ）」と記録され、その結果が明確に示されます。



要約すると、ファイルアクセス監視（FAM）は、ファイルに対するユーザーの操作状況をリアルタイムで把握できるようにすることで、包括的なファイル整合性監視（FIM）ソリューションを強化するものです。FIMがデータの整合性を保証するのに対し、FAMは不正アクセスの試みを検知・通知してこれを補完し、ファイルセキュリティに対するより全体的かつ包括的なアプローチを実現します。

II. 包括的なファイル整合性監視（FIM）

Qualys FIMは、市場で最も包括的なFIMソリューションです。Qualysによる完全管理の下、パブリッククラウドまたはプライベートクラウドからQualys FIMを導入できます。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。また、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アセットを検出し、FIM用に自動設定することが可能です。すぐに利用可能なプロファイルがベースとなる設定の構築を支援し、導入にかかる時間をさらに短縮します。

必須要件

要件 1: ノイズキャンセリング、誤検知アラートの効率的な削減

ほとんどのFIMソリューションは、大量の誤検知アラートを生成するため、「ノイズが多い」とみなされています。これらのソリューションは、リスク評価を高度にカスタマイズすることで、より多くのアラートを生成できることを謳っています。しかし、このアラートの嵐は、正確かつ意味のある優先順位付けがされていない何十万ものイベントによって、コンプライアンスおよびセキュリティアナリストに大きな負担をかけています。実際には、ほとんどのアラートは対応を必要とせず、SOCチームやコンプライアンス監査のリソースを著しく圧迫し、効率的なインシデント対応と分析を阻害しています。FIMソリューションを評価する際には、アラートトリガーの実際の有用性をテストする必要があります。

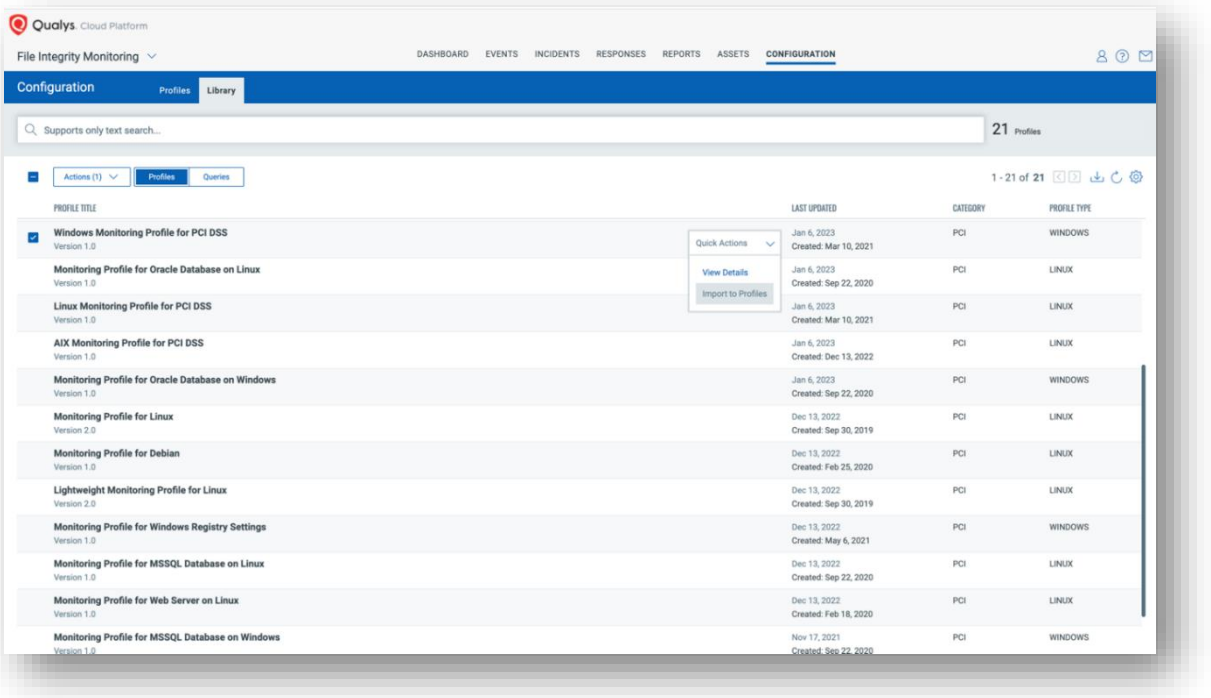
Qualys FIMは、誤検知（ノイズ）を90%以上削減する独自のノイズキャンセリング技術を搭載しています。本機能は、「信頼できるソース」や「ファイルレピュテーション」といったコンテキストをイベントデータに付加することで、ノイズを抑制しつつイベントの優先順位付けを行い、データをより有益なものにします。直感的なダッシュボードにより、変更管理の状況を継続的に把握できるほか、「何が・誰によって・いつ」変更されたかというコンテキストを含む変更イベントのインサイトを確認することも可能です。

FIMのノイズキャンセリング機能がもたらす主なメリットは以下の3点です。

すぐに利用可能なFIMプロファイル

Qualys FIMソリューションの大きな特徴は、ノイズを最小限に抑えるよう綿密に選定された、重要なファイルパスから成る精緻なライブラリにあります。これらのパスは恣意的なものではなく、規制基準への適合を考慮して慎重に厳選された、極めて重要なものです。管理者は、この最適化されたライブラリを活用することで、不正な変更に対して脆弱な要素（重要なシステムファイル、設定ファイル、アプリケーションファイル、ディレクトリ、レジストリオブジェクトなど）を網羅した、事前設定済みの構成を利用できます。

こうした重要なファイルやディレクトリの監視に重点を置くことで、管理者は最も重要なアラートのみを確実に受け取れるようになります。Qualys FIMを活用すれば、セキュリティ運用の効率と透明性を高めることが可能です。



FIMルールにおけるノイズ抑制のための詳細なフィルタリングオプション

QualysのFIMルールは高度な粒度を備えており、以下のような条件を指定することでノイズを効果的に抑制するための多様なオプションをユーザーに提供します。

a) ワイルドカードをサポートするファイルパス（例）

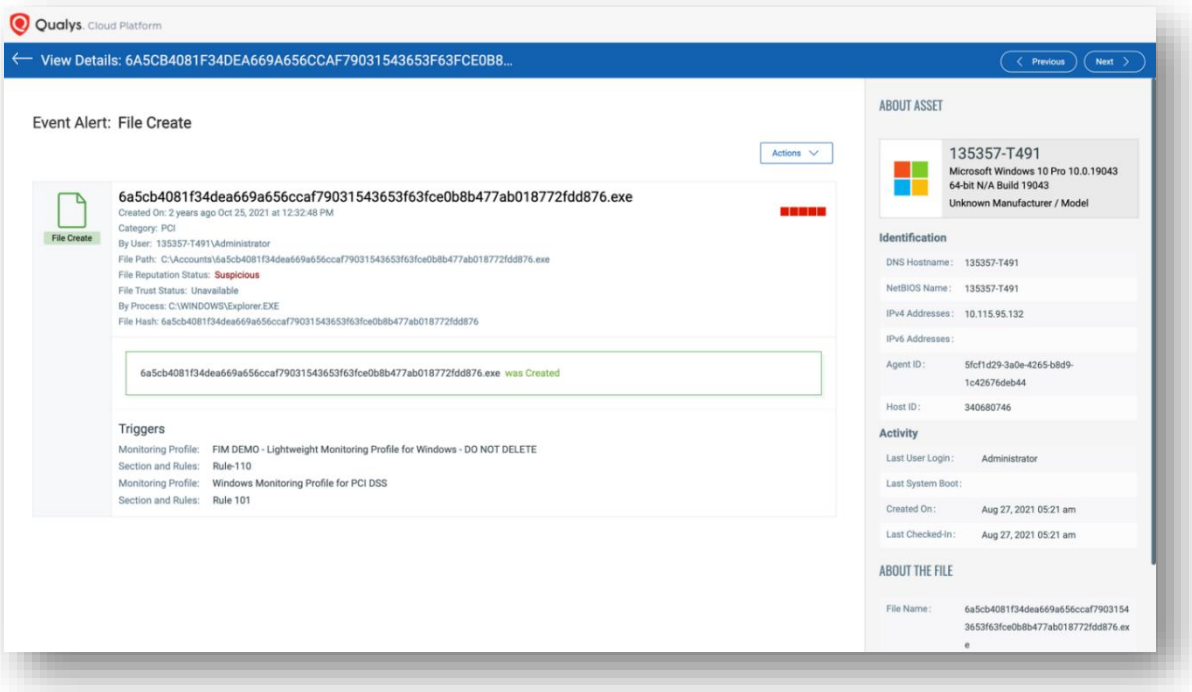
- /var/* or /tmp/*（/tmp and /var/tmp) in Linux
- C:\Users\AppData\Local\Temp or %systemdrive%\Windows\Temp in Windows

b) ユーザーおよびプロセスに基づくフィルタリング

これにより、ホワイトリストに登録されたユーザーやプロセスによって生成されたイベントを除外できるようになります。例えば、システムユーザーが実行するウイルス対策プロセスをFIMプロファイルのグローバル除外フィルターに追加すれば、そのプロセスが不要なイベント（ノイズ）を生成することはなくなります。

脅威インテリジェンスを活用したFIMの高度なノイズキャンセリング機能:
悪意ある、または不審なハッシュの検知

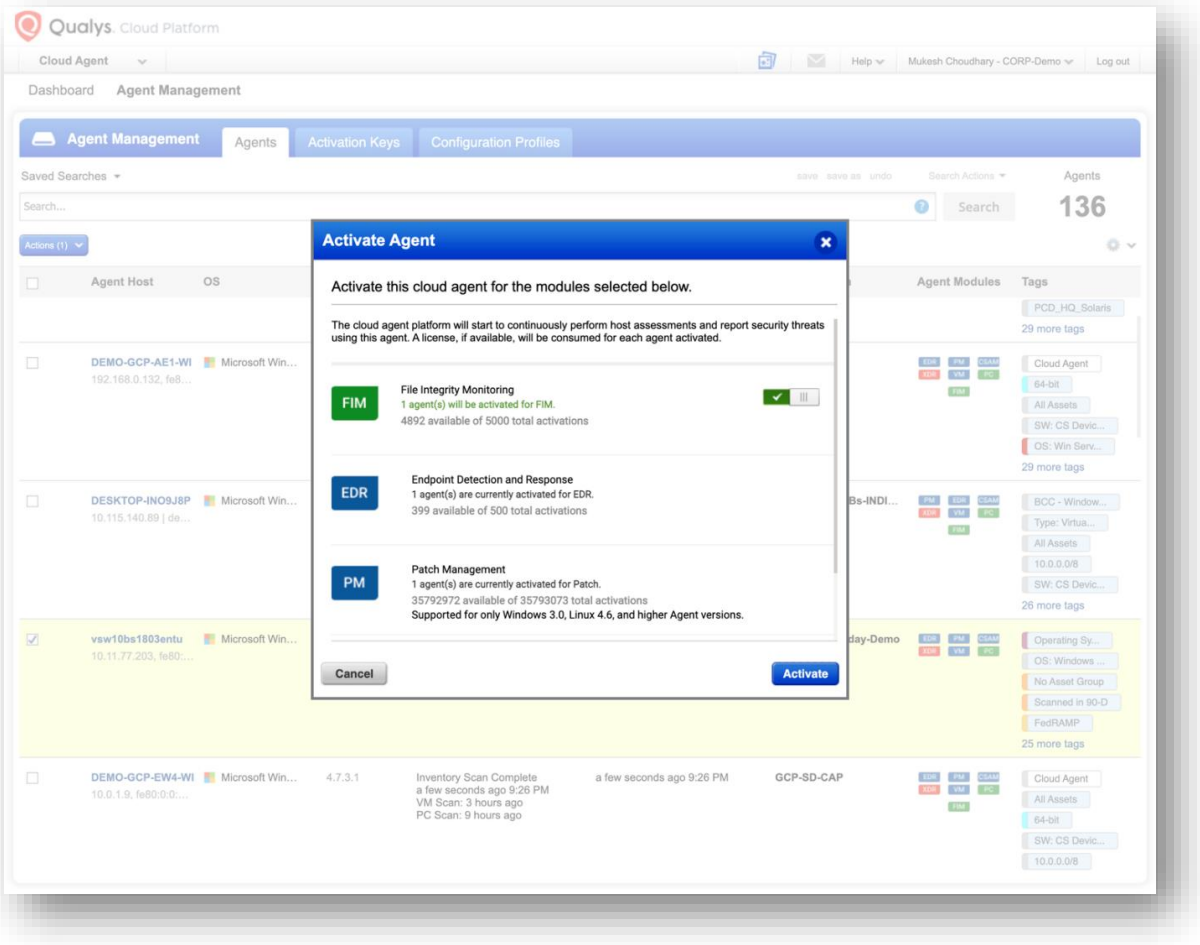
Qualys FIMは、脅威インテリジェンス（特にファイルのレピュテーション情報）を統合することで、従来のイベント監視の枠を超え、システム変更が不審なものか悪意あるものかをユーザーが迅速に判別できるようにします。



要件 2: 単一のエージェントとプラットフォーム

多くのソリューションでは、複数のエージェント、プラットフォーム、ダッシュボードが必要とされます。これらは管理にかかる時間や労力を大幅に増大させ、TCO（総所有コスト）に影響を及ぼす可能性があります。Qualys Cloud Agentは軽量かつ多機能であるため、セキュリテ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。

Qualys TruRisk Enterprise Platformは、FIM（ファイル整合性監視）と他のセキュリティアプリケーションを一元管理できる単一のインターフェースを提供します。また、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アセットを検出し、FIM用に自動設定することが可能です。すぐに利用可能なプロファイルがベースとなる設定を支援するため、導入にかかる時間をさらに短縮できます。



要件 3: インシデント管理とコンプライアンス報告の自動化

Qualys FIMは、インシデントの手動および自動作成が可能な**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、以下のような特定の条件に基づいてインシデントを自動生成できます。

- 権限を持たないユーザーによる削除操作
- 権限を持たないユーザーによる所有者やアクセス権限の変更の検知
- ホスト上での悪意あるファイルや不審なファイルの検知
- 初期化ファイルの不正な変更など

この機能はインシデント対応を効率化し、組織がセキュリティ上の懸念事項を即座に特定して対処できるよう支援します。

Qualys FIMソリューションには、コンプライアンス監査を支援する上で極めて重要な役割を果たす自動コンプライアンスレポートが含まれており、これらはFIMシステムの中核を成すものです。これらのレポートは、主に以下の3つのタイプに分類できます。

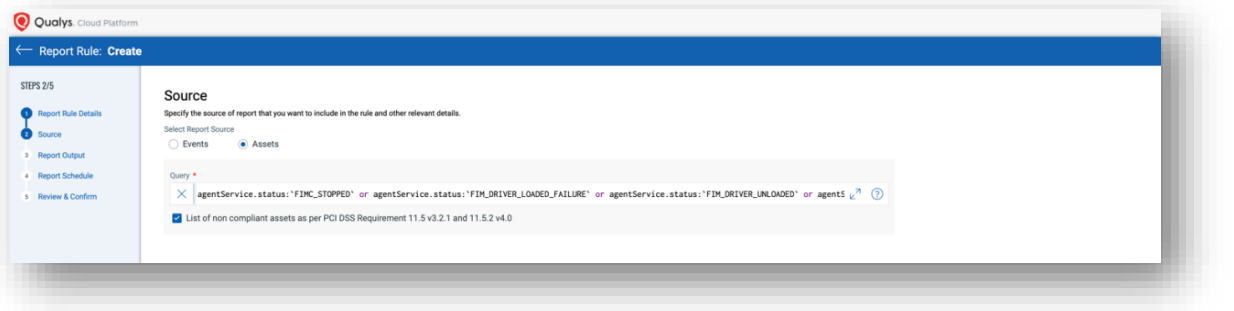
- イベントベースのレポート

    - これらのレポートは、FIMシステムによって追跡された特定のセキュリティイベントやアクティビティを詳細に示します。
- インシデントベースのレポート
    - このカテゴリでは、監視対象環境におけるセキュリティインシデントや侵害を記録します。
- 資産ベースのレポート
    - 資産ベースのレポートは、FIMの監視範囲内にある個々の資産に関する包括的なスナップショットを提供します。
    - これらのレポートは、各資産のセキュリティポスチャーおよび関連する基準への準拠状況を評価します。
    - 資産ベースのレポートを活用することで、特にPCI DSS 4.0の適用範囲内において、コンプライアンス体制の維持に不可欠な「基準に準拠していない資産」を容易に特定できます。

コンプライアンスに適合していない資産には、主に以下の2つの重要なカテゴリが含まれます。

- FIM（ファイル整合性監視）が有効化されているものの、現在は稼働していない資産:
  この状態は、コンプライアンスおよびセキュリティ基準を維持するために継続的なFIM監視を求めているPCI DSS要件11.5（v3.2.1）および11.5.2（v4.0）に違反しています。

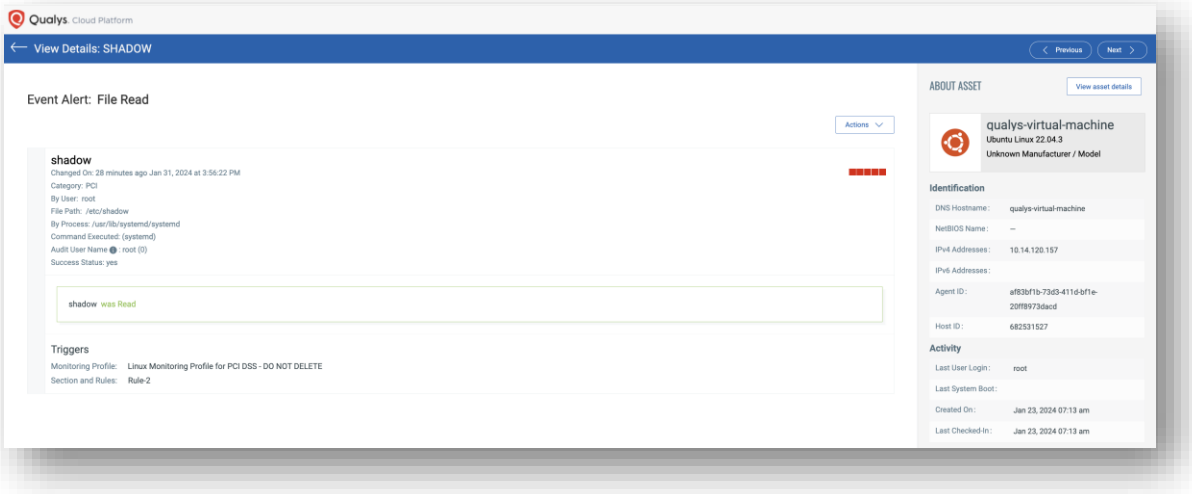
- 通信が行われていない資産:
  Qualysプラットフォームと通信していない資産を指します。関連するすべてのシステムが確実に監視および評価の対象となるようにするには、こうした通信のない資産を特定し、適切に対処することが不可欠です。



要件 4: 規制要件を満たすための詳細なイベント情報

Qualys FIMは、監査対象となるイベントのあらゆる側面を網羅しています。
具体的には以下の通りです。

- ユーザーの識別情報
- イベントの種類
- 日時
- 成功または失敗の成否
- イベントの発生源
- 影響を受けたデータ、システムコンポーネント、またはリソースの識別情報や名称

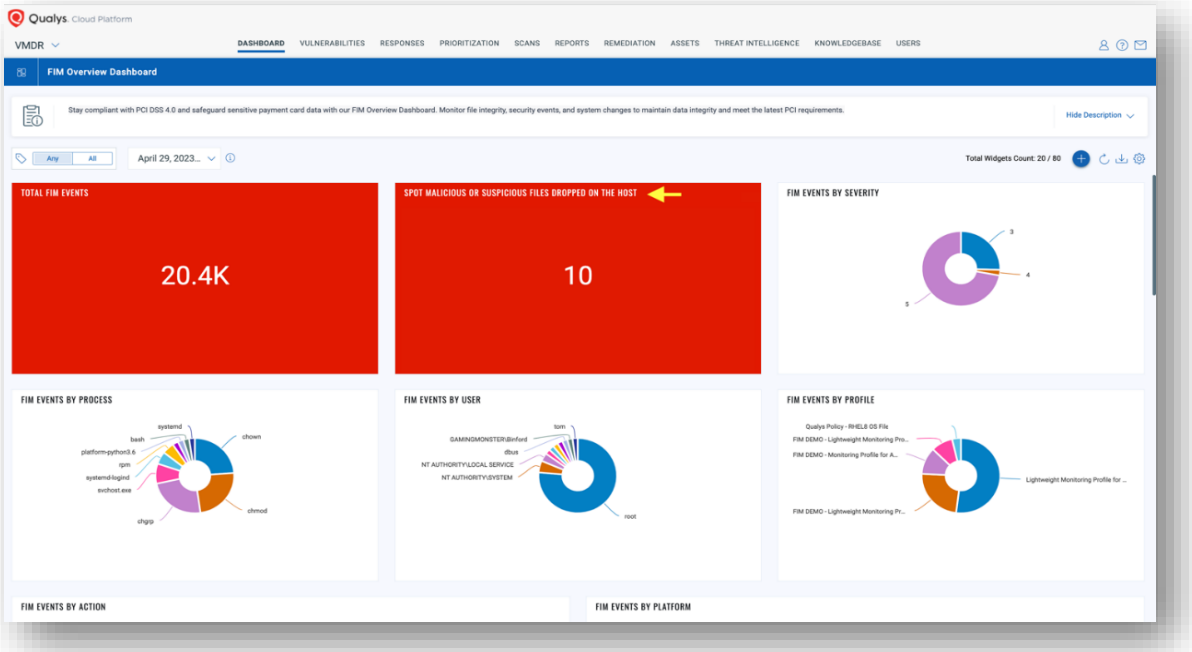


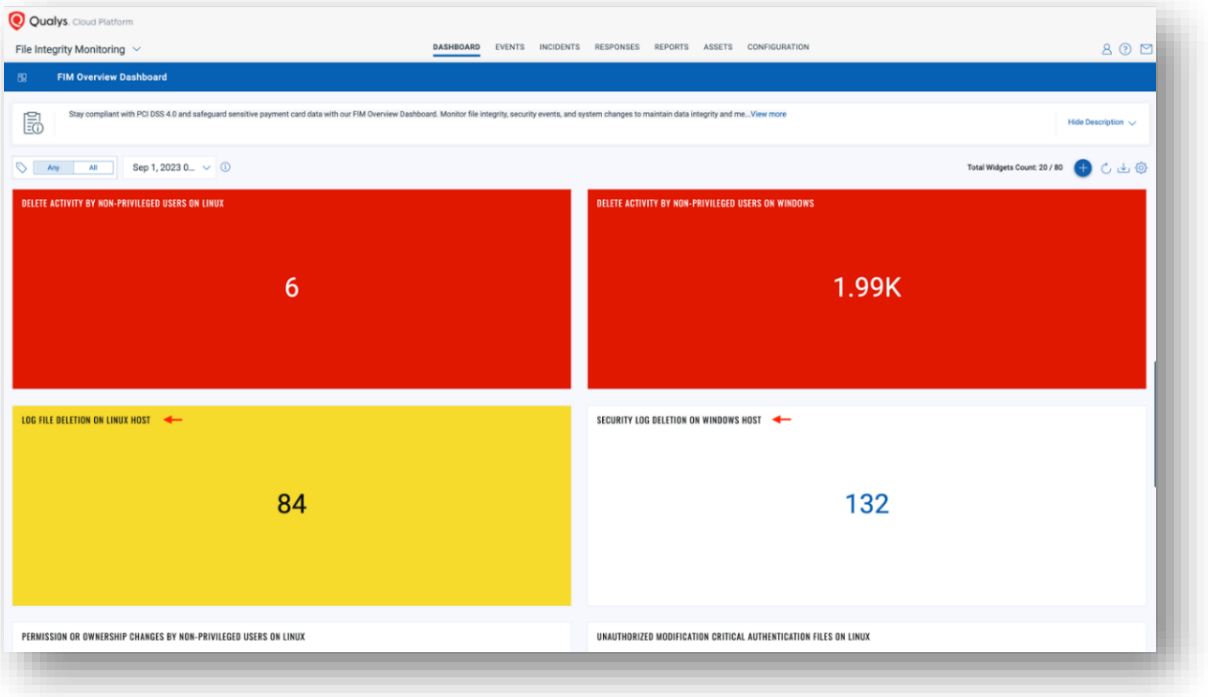
要件 5: データの保持

多くのソリューションではデータの保持期間が30日間などと限られており、コンプライアンス監査で不適合とみなされる可能性があります。Qualys FIMは13ヶ月間のデータ保持ポリシーを採用しており、インシデント発生時にはすべてのイベントに即座にアクセスし、包括的なフォレンジック分析を行うことが可能です。これにより、PCI DSS 4.0で規定されている12ヶ月間のデータ保持要件をはじめ、多くのコンプライアンス要件を満たすことができます。

要件 6: 動的なFIMダッシュボード

Qualys FIMは、環境内の変更イベントに関する包括的な概要を提供する動的なデフォルトダッシュボードを備えており、特に即時の対応を要する重大な問題の強調に重点を置いています。また、FIM環境全体の状況を迅速に把握できる、あらかじめ定義されたウィジェットも含まれています。

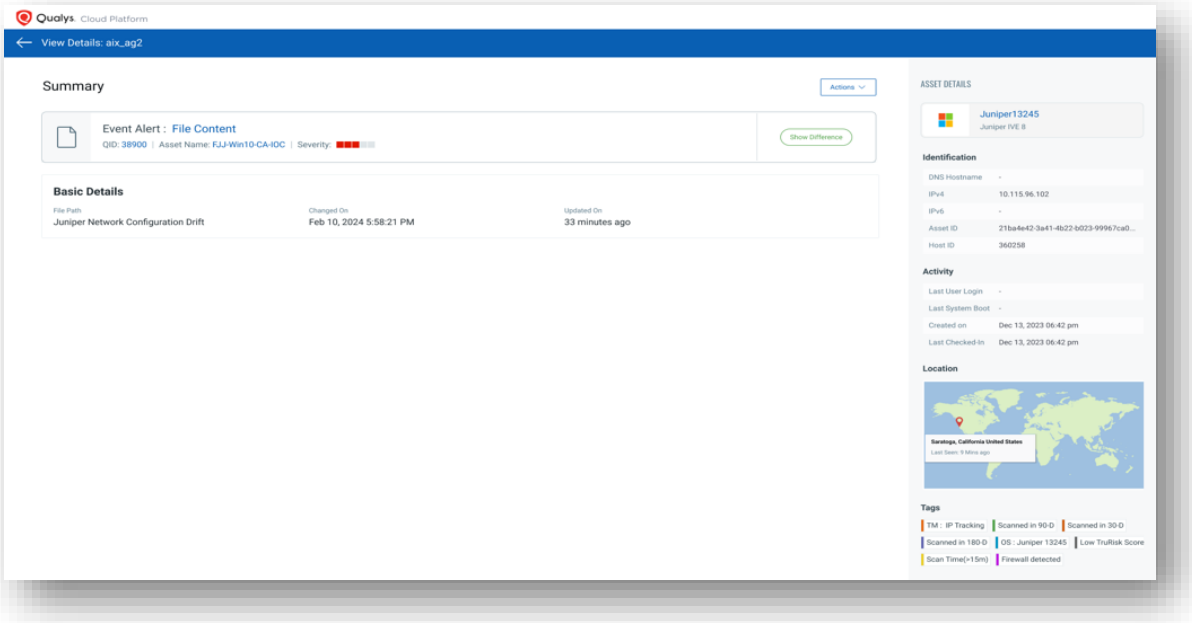


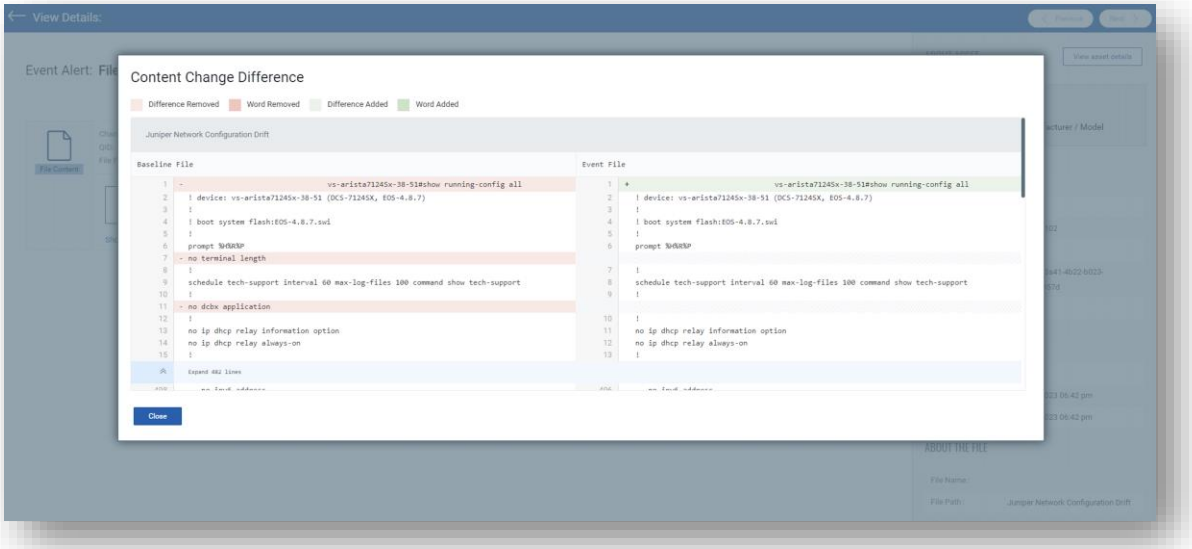


III. エージェントレスFIM – ネットワークデバイスにおけるFIM

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。

ネットワークデバイスへのFIM導入は、組織がネットワークインフラストラクチャの整合性、セキュリティ、およびコンプライアンスを維持するのに役立つ、予防的なセキュリティ対策です。絶えず変化・進化するサイバーセキュリティ環境において、不正な変更、設定の乖離、および潜在的なセキュリティ脅威に対する重要な防御層となります。





IV. 価値創出までの時間

PCI DSS 4.0の要件では、コンプライアンスやセキュリティ上のリスクに早期に対処するため、ファイル変更検知メカニズムの導入が求められています。しかし、一部のFIM（ファイル整合性監視）ソリューションには、各OSの重要ファイルに対応した信頼性の高い変更検知ルールやパラメータが事前に設定されていません。こうした機能の欠如は、導入作業を複雑化させ、多大な時間を要する原因となります。どのようなFIMソリューションであっても、再設定機能や、自社環境特有の重要ファイルを監視する能力について、必ず事前にテストを行うようにしてください。

Qualys FIMでは、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部門やセキュリティチームの介入なしに、新規アセットの検出と自動設定を行うことが可能です。すぐに利用可能なプロファイルがベースライン設定を支援し、導入にかかる時間をさらに短縮します。FIMは包括的なセキュリティおよびコンプライアンス体制の重要な構成要素ですが、それ単独ではなく、サイバーセキュリティのエコシステム全体と連携して機能する必要があります。選定するFIMソリューションには、組織内のデータレイク・リポジトリ間での双方向データ交換を可能にするAPI機能が備わっているべきです。Splunk、QRadar、ServiceNowとのネイティブな連携に対応したFIMソリューションであれば、投資対効果（ROI）が飛躍的に向上し、コンプライアンス、セキュリティ、ITの各担当部門間の連携も円滑になります。

"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."

クラウドベースのセキュリティおよびコンプライアンス・プラットフォームを通じてFIM（ファイル整合性監視）を導入することで、企業はこうした取り組みを容易に拡張し、統合型セキュリティ・ソリューションを活用してグローバル規模でのコンプライアンスを達成できると同時に、複数の個別製品に伴う高額なコストを削減することが可能になります。 **Robert Ayoub, Research Director, IDC**

V. スケーラビリティ

多くのFIM（ファイル整合性監視）製品の顧客や業界の専門家から、一部のFIMソリューションにはスケーラビリティに関する課題があるとの指摘がなされています。数千ものエンドポイントをサポートするには複数のサーバーが必要となることが多く、管理にかかるIT部門の工数や労力が課題となる場合があります。単一のコンソールでは1万台を超える資産を管理しきれないことがあり、その場合は追加のコンソール導入に伴うコストが発生します。また、ホストを監視するために数千ものルール設定が必要となるソリューションもあり、リソースが限られたチームにとっては大きな負担となり得るほか、高額なプロフェッショナル・サービスの利用が必要になる可能性もあります。

すべてのFIMソリューションが、高いパフォーマンスや低いTCO（総所有コスト）を維持しつつ、大規模組織の規模拡大に対応できるわけではありません。FIMツールの多くはスタンドアロン型のソリューションであるため、SIEM、UEBA、資産インベントリ管理、その他重要なセキュリティ・コンプライアンス・ツールとの連携が困難になりがちで、多大な労力やコストを要します。また、インフラのノード数が増加し、分散化が進むにつれて、コンサルティングサービスが必要となるFIMソリューションも少なくありません。導入を検討する際は、そのFIMソリューションが自社のセキュリティスタックと緊密に連携できるかどうか、その能力を必ず検証するようにしてください。

Qualys FIMなら、動的なスケーリングが可能です。最小限のセットアップとイベント管理用のホスト型サービスにより、既存インフラへの負荷を大幅に軽減し、さらなるコストの最適化を実現します。Qualys TruRisk Enterpriseクラウドプラットフォームを活用すれば、グローバルかつオンデマンドでのスケールアップが可能です。また、拡張性の高いXMLベースのAPIを介して他のシステムと容易に連携でき、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Qualys FIMをシームレスに統合・運用できます。

VI. Qualys FIMのサポート対象プラットフォーム

Qualys FIMのサポート対象プラットフォームは以下の通りです。Qualysは、新しいオペレーティングシステムおよびそのアップデートに対し、最新の2つのエージェントリリースを認定しています。明示的な認定は行われていませんが、サービス終了（End-of-Service）を迎えていないすべてのエージェントバージョンも、これらのオペレーティングシステムをサポートするはずです。

Microsoft Windows 7, Windows 8/8.1, Windows 10** (1507 から 22H2), Windows 11 (22H2): **FIM 5.3, 5.4**

Microsoft Windows 10 IOT LTSC 2019 および 2021: **FIM 5.4**

Microsoft Server 2003 SP2+ から Server 21H2*, Server 2022: **FIM 5.3, 5.4** (excluding Server 2003)

Linux Red Hat Enterprise Linux 6, Enterprise Linux 7 から 7.9, Enterprise Linux 8 から 8.8, Enterprise Linux 9, Enterprise Linux 9.1, 9.2, 9.3, CentOS 6 から 6.7, CentOS 7 から 7.9, CentOS 8 から 8.5: **FIM 6.1, 6.2**

SUSE Linux Enterprise Server (SLES) 15, 15 SP1, SP2, SP3, Linux Enterprise Server (SLES) 15 SP4, Linux Enterprise Server (SLES) 12: **FIM 6.1, 6.2**

Amazon Linux 2 2017.03 から 2.0.2021, Linux 2 2022 のカーネルバージョン 4.14 および 5.10 , Linux 2023: **FIM 6.1, 6.2**

Oracle Enterprise Linux 8 から 8.5, Enterprise Linux (OEL) 8.6, Enterprise Linux (OEL) 8.7, Enterprise Linux (OEL) 8.8, Enterprise Linux (OEL) 6, Enterprise Linux (OEL) 7 から 7.9, Enterprise Linux (OEL) 9.0 のカーネルバージョン 5.15.0-3.60.5.1.el9uek.x86_64, Enterprise Linux (OEL) 9.1, 9.2, 9.3: **FIM 6.1, 6.2**

Debian 11.x, Debian 10.x, Debian 9.x, Debian 8.x, Debian 7.x, Debian 12.x, **FIM 6.1, 6.2**

Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS, 22.10 LTS, 23.04 LTS: **FIM 6.1, 6.2**

AlmaLinux 8.6, 8.8, 9.0, 9.2: **FIM 6.1, 6.2**

Rocky Linux 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 9, 9.1, 9.2: **FIM 6.1, 6.2**

Alibaba Cloud Linux 2, 3, 6, 7, 8: **FIM 6.1, 6.2**

VMware Photon 3, 4: **FIM 6.1, 6.2**

Linux (ARM CPU) Current Release 5.0

Red Hat Enterprise Linux 8.7, 8.8, 9, 9.1, および 9.2: **FIM 4.18, 5.0**

Amazon Linux 2 2022 のカーネルバージョン 4.14 および 5.10, Linux 2023: **FIM 4.18, 5.0** Ubuntu 14.04 LTS, 15.x, 16.04 LTS, 18.04 LTS, 19.10, 20.04 LTS, 22.04, 23.04: **FIM 4.18, 5.0**

Debian 9.x, 10.x: **FIM 4.18, 5.0**

Red Hat CentOS 7.x, CentOS 8 Stream, CentOS 9 Stream: **FIM 4.18, 5.0**

Oracle Enterprise Linux (OEL) 7.9, Enterprise Linux (OEL) 8.8, 9.2: **FIM 4.18, 5.0**

AlmaLinux 8.7, 8.8, 9, 9.2: **FIM 4.18, 5.0**

IBM AIX Current Release 4.17 (scan-based)
IBM AIX 7.1 TL1, TL2, TL3, TL4, TL5, TL5 SP4, AIX 7.2 TL1, TL2, TL3, TL4, TL5 (Standard および Enterprise Editions), AIX 7.3 TL0 (Standard および Enterprise Editions), AIX 6.1 TL0-9 (Standard および Enterprise Editions): **FIM 4.17, 4.20**

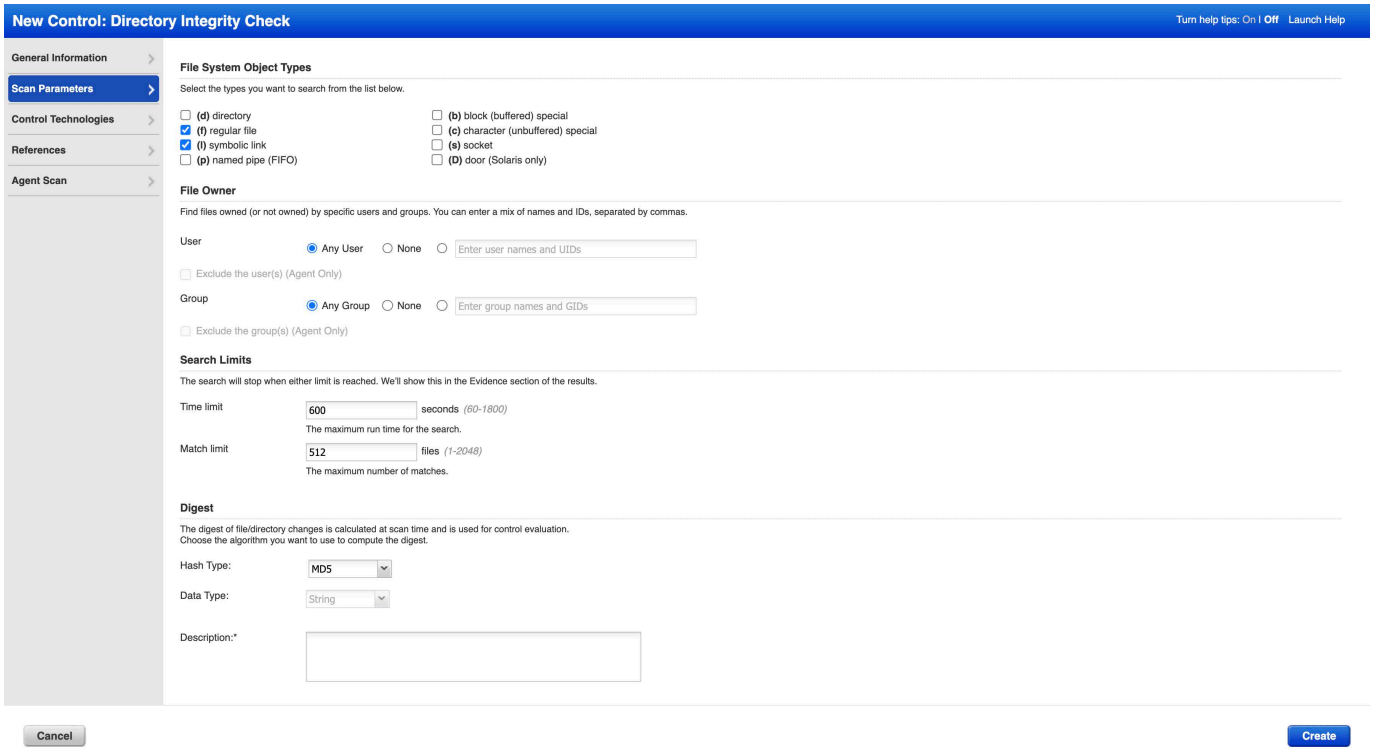
VII. Solarisにおけるハッシュベースの FIM

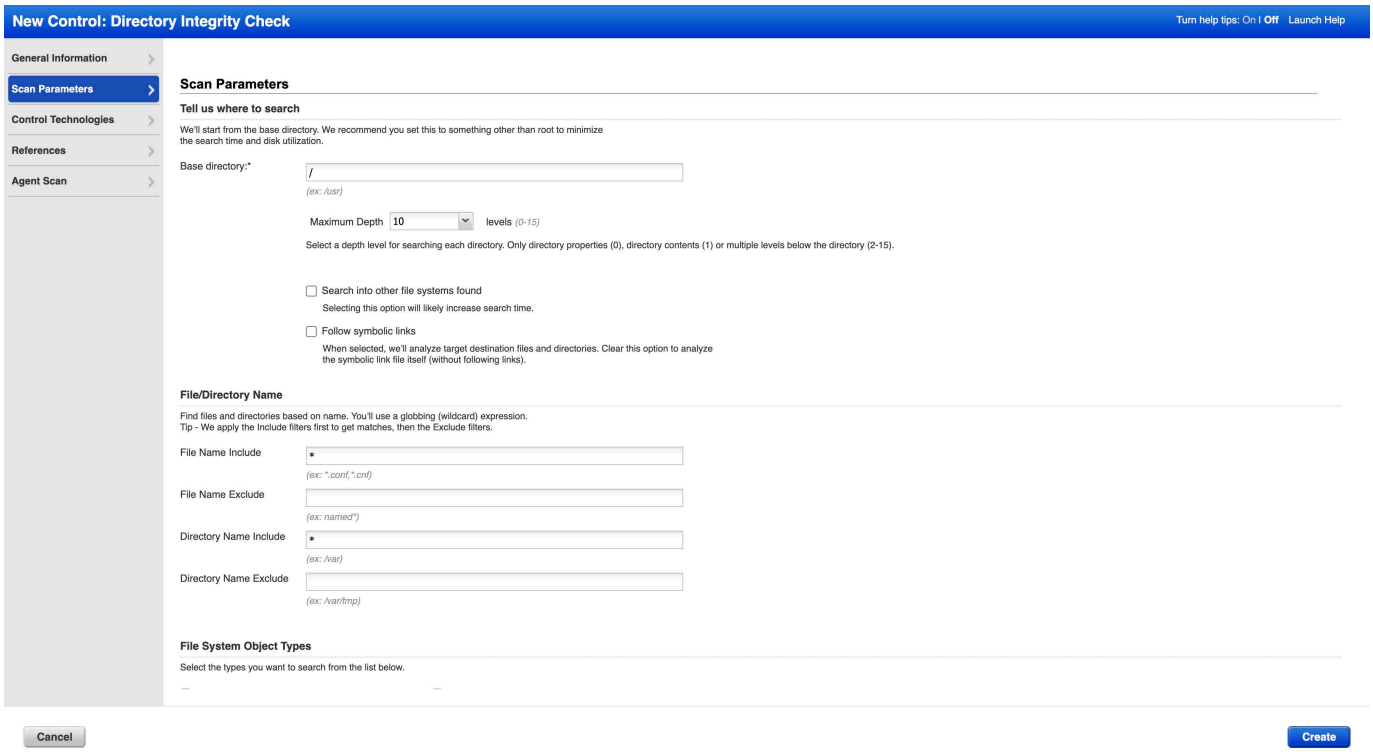
Qualysは、Solaris上でスキャンベースのFIMをサポートしています。Solaris上の重要なファイルに対する整合性チェックを容易に作成し、ハッシュベースのFIMを開始することができます。以下の技術は、「ファイル整合性チェック」および「ディレクトリ整合性チェック」のコントロールによってサポートされています（これらのコントロールタイプは、ディレクトリレベルでUnixファイルの整合性をチェックし、ハッシュベースのファイル整合性やスナップショットの更新状況を報告します）。

Solaris 8.x, 9.x, 10.x, 11.x

複数のハッシュタイプをサポート: MD5, SHA-1, SHA-256

整合性チェック（Integrity Check）ルールはきめ細かく設定されており、FIMイベント詳細の一部として網羅的なデータを収集します。ハッシュベースのFIMにおける整合性チェックルールをご確認ください。





詳細はこちらをクリックしてください

VIII. PCI DSS 4.0への対応

Qualys FIMは、PCI DSS 4.0の要件をサポートし、監査に対応できる体制を整えています。詳細については、以下のリンクをご参照ください。

- PCI DSS 4.0 FIM Requirements Simplified with Qualys File Integrity Monitoring
- Qualys Enterprise TruRisk™ Platform Extends FIM with Real-Time Monitoring of Unauthorized Access to Sensitive Data and Configuration Change Detection on Network Devices
- Qualys FIM Playbook for PCI 4.0

結論

監査での不合格、セキュリティ侵害、訴訟といった多大なコストを伴う事態を回避するためには、ファイル整合性監視（FIM）ソリューションに、ファイルアクセス監視（FAM）、ノイズ除去、エージェントレス・ネットワーク・サポートなど、7つの不可欠な機能が備わっている必要があります。Qualys FIMソリューションは、これらの機能を備えた軽量かつ拡張性の高いクラウドサービスであり、重要なファイル、フォルダ、レジストリ・オブジェクトに対する変更を継続的に監視します。

Qualys FIMは、PCI DSS 4.0、HIPAA 2023、CCPA、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 TruRisk Enterprise Platform」と包括的なFIMライブラリを活用することで、アラートのノイズを低減できるほか、イベントの重要度、すぐに使えるルール、統合された脅威インテリジェンスを組み合わせ、アラートに詳細なコンテキストを付加することが可能です。Qualys FIMは、他のほぼすべてのFIMソリューションと比較して、より低いTCO（総所有コスト）と優れたシステムパフォーマンスを実現しつつ、効率的な資産の可視化と監視機能を提供します。

Qualys FIMの詳細や、過剰なアラート（アラートノイズ）、監査不適合、サイバーセキュリティリスクの低減を当社がどのように支援しているかについては、下記ページをご覧ください。
詳しくは: **https://www.qualys.com/forms/file-integrity-monitoring**