FORTRA™

Beyond the Basics: Tripwire Enterprise ユースケース

はじめに

セキュリティ、コンプライアンス、IT運用のリーダーたちは、セキュリティ設定の構成ミスや侵害の兆候を正確に特定するための強力かつ効果的な方法を求めています。業界をリードするファイル整合性監視（FIM）およびセキュリティ構成管理（SCM）コンプライアンス監視ソリューションであるTripwire® Enterpriseは、コンプライアンスの枠を超越するセキュリティ機能を提供します。

皆さまは、Tripwire® Enterpriseがこの種のソリューションの中でも最も強力なFIMコンプライアンスソリューションであることを、既にご存じかもしれません。しかし、御社のセキュリティコンプライアンスプログラムの効果を最大化するために活用できる重要なユースケースはいくつも存在します。

このガイドでは、Tripwire Enterpriseの優れたセキュリティ機能と継続的なコンプライアンス確保を通じて組織を保護するさまざまな方法をご紹介します。

コンプライアンス確保のためのFIM

Tripwire Enterpriseの監視機能では、対象資産のファイル変更が、正常なものか不審なものかを識別できます。どのようなファイルの変更がコンプライアンスに影響するかが可視化されるため、迅速な対応が可能になり、システムをコンプライアンスに準拠した状態に戻すことができます。

FIMの生みの親であるTripwireは、20年以上にわたり、格段に幅広くきめ細やかな検出機能を開発し、次のような機能で企業を支援してきました。

- 「良い」変更と「悪い」変更を識別
- コンプライアンス監査人に周知されたソリューションで監査プロセスをスピードアップ
- 4,000以上の組み合わせからなるコンテンツライブラリで、さまざまなプラットフォーム、ポリシー、標準、規制、ベンダーのガイドラインを網羅

お客様事例

ある大手銀行では、PCI DSSの要件11への準拠を目的に、変更検知ソリューションの導入を必要としていました。この分野のリーダーとしての当社の評判を知っていた同行は、PCI対象資産の監視のためにTripwire Enterpriseを購入しました。当社製品の広範なプラットフォームとコンテンツライブラリをすぐに活用し、同行は最小限の時間と労力でコンプライアンスの確保を実現しました。Tripwire Enterpriseの継続的なコンプライアンスワークフローを使用することで、コンプライアンススコアの改善に向けて環境内の構成が更新される都度、管理者宛ての進捗レポートが継続的に提供されています。PCI監査の際、監査人はTripwireのソリューションをすぐに認識し、その運用についてほとんど質問することはありませんでした。彼らはその結果の正確さが信用に値するものであることを知っていたからです。

追加情報

操作を見る
コンプライアンス基準を知る

セキュリティ確保のためのFIM

FIMは、コンプライアンスに不可欠なセキュリティコントロールであるため、コンプライアンス確保の目的のみに使用するものだと誤解されがちです。しかし、Tripwire　Enterpriseを強化しているFIM機能は、高度なセキュリティユースケースに対応する高度なセキュリティ機能をサポートしています。標準的なプラットフォームセット以外にも、環境固有のソフトウェアやデバイスを監視対象に含めるようカスタマイズすることもできます（たとえば、境界を保護するだけでなく、データセンター内の脅威にも対応）。また、取得したデータは、SplunkやServiceNowなどの他のソリューションと統合して、全体的なセキュリティの状態を把握することもできます。

Tripwire Enterpriseが支援すること

- 経時的な変化を含む、エコシステム全体の広範な可視化を実現
- 高度なフォレンジック分析を活用した平均復旧時間（MTTR）の短縮
- 侵害や障害がもたらす評判の失墜や金銭的リスクを回避

お客様事例

ある保険会社では、Webサーバーを使用して顧客ポータルのホスト、決済の受付、アカウント情報へのアクセスを行っています。それらのシステムを、ポータルのセキュリティと整合性に影響を与える可能性のあるアクティビティから保護したいという意向から、Webサーバーアプリケーション、決済カード処理アプリケーション、および顧客情報データベースへの不正な変更を監視する目的でTripwire　Enterpriseを購入しました。同社は、Tripwire　Enterpriseを設定してフォレンジック情報を収集し、セキュリティチームが顧客データを保護して決済処理アプリケーションの整合性を確保するとともに、セキュリティ問題にリアルタイムで対応できるようにしました。同社の重要なシステムには、すでに成熟した変更管理・承認プロセスが導入されていたため、ServiceNowシステムと統合を行い、Tripwire Enterpriseで検出されたアクティビティと承認済み変更チケットとの照合を行いました。対応するチケットが存在しない変更が検出された場合には、インシデントチケットが作成され、ただちにレビューを行うようにSOCチームに割り当てられます。また、これらのシステム上で不正なアクティビティが発生した場合に適切な対応を行うための手順書も作成されました。

追加情報

包括的な整合性管理を実現するFIM対応プラットフォーム

コンプライアンス確保のためのポリシー監視機能

Tripwire　Enterpriseは、FIMとセキュリティ構成管理（SCM）という2つの重要なセキュリティ管理機能を兼ね備えています。これらの機能を組み合わせて、監査対応のレポートを生成することで、システムが規制の枠組みに準拠していることを証明する際の組織の負担を軽減します。コンプライアンスフレームワークの適用範囲は、他のソリューションと比較して非常に広範かつ深いため、手作業の時間を取られることなく、複数の基準に同時に適合することができます。SCMのワークフローでは、事前定義されたポリシーを活用して免除およびレメディエーションのプロセスを簡素化しています。

Tripwire Enterpriseで実現できること

- ポリシーの内容を自動的に最新に保つ
- 明確なレメディエーションアドバイスを提供する、あるいはレメディエーションワークフローを自動化する
- オープンなポートやサービス、インストールされているソフトウェアを監視する
- 複数の規制を包括的に順守する

お客様事例

ある金融機関は、さまざまな業界の顧客と取引があり、サーバーをそれぞれの顧客と同じ規制に準拠させておく必要性がありました。その業種構成の特性により、同社のサーバーでは、PCI、SOX、さらにはHIPAA基準も順守しなければなりませんでした。ソリューションを検討したところ、Tripwire製品は、最も包括的にポリシーをカバーしていることがわかりました。Tripwire　Enterpriseを購入した同社は、データを収集し、社内の監査チームとGRC（ガバナンス、リスク、コンプライアンス）チームにレポートを提供しました。この強力なツール1つで、同社のサーバーがすべての関連規制に対し順守状態にあることを示すことができました。顧客側の監査に際して要求があった場合には、Tripwire　Enterpriseでより範囲を絞ったレポートを作成し、特定の基準に対するコンプライアンス準拠の証明を提供しました。日常的には、社内の監査チームとGRCチームに広範なレベルのコンプライアンスデータを提供し、自社のコンプライアンスを証明するためにTripwireのレポート機能を活用しています。

追加情報

ケーススタディを読む
Tripwireのコンプライアンス機能を探る

セキュリティ確保のためのポリシー監視

特に内部監査やコンプライアンス、GRC担当チームが置かれる組織のセキュリティにおいては、法規制の順守に加えて、ポリシーの監視が極めて重要です。法規制の順守を義務付ける根本的な目的は、最善のセキュリティ対策のための要求基準またはベースラインを設定して機密データを保護するところにあります。Tripwire Enterpriseでは、PCI DSS（PCIデータセキュリティ基準）などの基準以外にも、Center for Internet SecurityのCIS ControlやMITRE ATT&CKフレームワークなどのセキュリティフレームワークのポリシーコンテンツも提供しています。

Tripwire Enterpriseが実現すること

- 社内用ポリシーコンテンツを、優先度の高いセキュリティフレームワークに対応するようカスタマイズして作成する
- 構成管理データベース（CMDB）とITサービスマネジメント（ITSM）チケッティング機能を統合して利用する
- セキュリティ機能の有効性を高め、侵害やサービス停止のリスクを低減する

お客様事例

ある地方銀行では、小規模なITチームが、数百の支店とATMを束ねるネットワークインフラの構成を外部委託しています。ネットワークデバイスの設定に矛盾があることに気づいたチームは、外部ベンダーが加える変更の可視性を高めたいと考え、それらのデバイスの設定を監視するためにTripwire Enterpriseを購入しました。ベンダーが適用するセキュリティ基準に一貫性がないことが判明したため、同行のチームはTripwire Enterpriseでカスタムポリシーを設定し、ネットワーク構成に特定のハードニング基準を適用するようにしました。そして、毎月のデバイスの再構成時に外部ベンダーによって生じるセキュリティギャップを特定するためにレポート機能を使用しました。これにより、自社チームが変更を直接コントロールすることができない状況にありながらも、セキュリティ体制を強化できるようになりました。Tripwire Enterprise Policy Managerによって、構成済みデバイスの日々のスキャン結果とハードニング基準とを継続的に比較することが可能になりました。これにより、リスク許容度で定義される妥当な遅延時間内に、セキュリティ上の問題を把握できています。

追加情報

ポリシーカスタマイズ・エグゼクティブガイド
CISコントロール・エグゼクティ

高度なモニタリング機能

Tripwire　EnterpriseをIT環境内の強力な検索ツールとして使用することで、各マシンのどこにファイルが存在するのか（あるいは存在しないのか）を把握できます。重要なデータの迅速な収集を可能にするTripwire Enterpriseの柔軟な監視機能では、すべての監視対象資産を所定のファイルレベルまで迅速に検索できます。この機能は、たとえばLog4jなどの重大なセキュリティ上の脆弱性やマルウェアが新たに発生している場合、あるいは侵害の兆候が見られる場合に多大な効果を発揮します。また、デプロイ期間中に変更チケットをクローズする際に、マシンのセット全体の構成を容易に検証し、正しく更新されていることを確認することができます。

Tripwire Enterpriseで可能になること

- ・　任意のファイル名を指定すると、エージェントがインストールされた資産上で、そのファイルのすべてのインスタンスを検索する
- COCR（Command Output Capture Rules）を使用して任意のプログラミング言語でスクリプトを展開することで、アクセスしにくいデバイスの監視オプションを大幅に拡張できる
- 修正プログラムがリリースされる前であっても、Log4jなどの潜在的な脆弱性にさらされる可能性がないかを評価する

お客様事例

重大なセキュリティ脆弱性（Log4j、Spring4Shellなど）が新たに公表されたとき、ある政府機関は、Tripwire Enterpriseを環境全体に適用し、それらの脆弱性に関連するファイルを迅速にスキャンしました。その公表から1時間経たずして、カスタマイズが容易なルールと結果のフィルタリング機能を用いて、リスクにさらされているすべての領域を特定することができました。さらに、同組織の首脳部向けに、環境内の影響を受けたすべてのサーバーを示すレポートを提出しました。脆弱性管理製品のベンダーが、同脆弱性を検出するための新しいスキャンアップデートを公開した数日前に、同組織はこれらの対応を完了しています。

追加情報

ランサムウェアの予防と検知のためのベストプラクティス
Tripwire Enterpriseの概要を見る

高度な制御

Tripwire　Enterpriseでは、強力なエンドポイントデータ収集エージェント「Tripwire　Axon®エージェント」を使用して、監視対象の資産に対して任意のコマンドやスクリプトを実行できるため、システム管理機能のアドホックな運用が可能です。たとえば、サーバーの再起動や設定の更新、あるいは応答がない別のツールのサービスの再起動が必要な場合でもTripwire Enterpriseがそれを支援します。このように適用範囲が広く、拡張性の高い機能により、管理者チームが複数のリモートマシン上でアドホックなコマンドセットを実行しようとする場面などで、大幅な時間削減を実現できます。

Tripwire Enterpriseが支援できること

- 数千台のサーバーの設定を更新し、必要に応じてリブートする
- アドホックスクリプトを作成してデプロイ、実行、レポート作成を行う
- 複雑かつ多様なITインフラを柔軟に管理する

お客様事例

世界中にデータセンターを持つある保険会社は、業界規制へのコンプライアンスを確保するため、Tripwire　Enterpriseを購入しました。同社のエンドポイントモニタリングチームは、別のセキュリティソフトウェアのエージェントが何度もチェックインに失敗していることに気付きました。そのため同チームはTripwire　Enterpriseを使用して、他のツールのエージェントの同期失敗を特定するカスタムポリシーを作成しました。そして、Tripwire　Axonエージェントから他のベンダーにコマンドを送信してエージェントを再起動できるように、自動修復ワークフローを構成しました。このワークフローにより、エンドポイントチームは、すべてのセキュリティツールの機能を維持しつつ、何時間にもおよぶ遅延や、複数のシステム管理者チームとのインシデントチケットのやり取りを回避できるようになりました。

追加情報

操作を見る
Tripwire Enterpriseのデータシートをダウンロードする

FORTRA™

Fortraについて

Fortra は、他に類を見ないサイバーセキュリティ企業です。私たちはお客様のために、よりシンプルで強力な未来を創造します。当社の信頼できるエキスパートと統合されたスケーラブルソリューションは、世界中の組織にバランスとコントロールをもたらします。私たちはポジティブ・チェンジメーカーであり、サイバーセキュリティの旅路のあらゆる段階において、お客様の味方となります。 詳細については、fortra.com をご覧ください。

fta-tw-gd-ja-0922-r2-hm