FORTRA

データシート(TRIPWIRE)

Tripwire Enterprise 9.0

優れたセキュリティ機能、継続的なコンプライアンス確保

セキュリティ、コンプライアンス、ITオペレーションのリーダーたちは、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。FortraのTripwire® Enterpriseは、ファイル整合性監視(FIM)とセキュリティ構成管理(SCM)機能を備えた、業界をリードするコンプライアンス監視ソリューションです。数十年にわたる経験をもとに、他のソリューションとは別次元の、高度なユースケースに対応します。

ポリシー遵守、システム整合性、レメディエーション管理機能を備えたこの完全統合型のソリューションスイートは、単にコンプライアンス準拠を目的とするものではありません。オンプレミス、クラウド、産業用資産を含む企業全体のセキュリティレベルを迅速に向上させることを可能にします。

仕組み:強力な統合型コントロール

Tripwire Enterpriseは、4つのコア機能を単一のインターフェイスで提供します。それらの機能が連携することにより、エンタープライズクラスのセキュリティ・コンプライアンスソリューションとして機能します。

システム整合性管理機能は、大規模な異機種混在環境全体をスキャンして脅威を検出し、設定上の脆弱性を即座に可視化します。それにより、構成の逸脱や不正な変更を抑制でき、エコシステムのセキュリティが向上します。Tripwire File Integrity Managerは、世界初の最高レベルのFIMソリューションです。スタンドアロンとして、緻密なエンドポイントインテリジェンスを提供することもできます。Tripwire Policy Managerと併用することで、変更をトリガーとした構成評価や、その他のシステム設定可能な対応を可能にします。これにより、「受動的」な構成評価機能が動的、継続的かつリアルタイムの防御ソリューションへと進化し、コンテキスト情報をカスタマイズして提供することにより、効果的な対応を加速します。

ポリシー管理機能は、プラットフォーム、セキュリティ、コンプライアンスポリシー、標準、規制、ベンダーガイドラインの4,000超もの組み合わせと突き合わせた継続的な構成評価を、エージェントベースおよびエージェントレスで実行します。Tripwire Policy Managerは、ポリシーのカスタマイズ、免除・例外管理、自動化されたレメディエーションオプションを提供するとともに、優先度ベースのポリシースコアリングにも対応します。さらに、コンプライアンス準拠のエビデンスを、監査官が確認しやすい形で提供するとともに、ポリシーの状態を可視化して、コンプライアンスチームがその後のアクションに生かせるようにします。

高度なユースケースにも対応可能になりました。これは、高度なカスタマイズが可能な監視オプション、最重要資産のリアルタイム変更検知、企業全体における新出の脆弱性(Log4J、Spring4Shell、Text4Shellなど)の検出、および厳しいハードニング基準に照らしたネットワークデバイスの継続的なレビューにより実現されます。高度なモニタリングのユースケースにおいて卓越した能力を発揮するTripwire Enterpriseが、御社のセキュリティエコシステムを強化します。

主な利点

- 整合性管理およびセキュリティ構成管理のための強力なワークフロー
- 構成ミスや不審な変更に対する比類のない可視性
- 数十年もの経験に裏打ちされたコンプライアンス監視機能
- 脅威の優先順位付けと、システムを安全かつコンプライアンスに準拠した状態に戻すためのガイダンス
- 規制ポリシー要件(PCI、NIST、CIS、その他多数)への準拠を監視し、監査対応のレポートを提供

主な連携

- Tripwire LogCenter®
- Splunk
- ServiceNow
- Active Directory
- SAML 2.0
- Cherwell
- Remedy
- JIRA
- Thycotic
- ChangeGear
- CyberArk

レメディエーション管理機能は、Tripwire Policy Managerと連携し、組み込みのガイダンスをITセキュリティチームとコンプライアンスチームに提供します。両チームは、正規の状態から逸脱したセキュリティ構成を修復できるようになるとともに、修復の実行に関するロールベースの管理、承認、サインオフが可能になります。これにより、オペレーションチームは、問題の箇所を把握し、システムを本番環境に対応できる状態に戻す方法を簡単に知ることができます。また、本番環境に復旧後もその状態を維持できます。

調査および根本原因の詳細分析によって、ITセキュリティチームとオペレーションチームは、何が起きたのかを迅速かつ効率的に特定できます。企業のスタッフ、プロセス、技術の絶え間ない変化に応じてシステムが変化することは、必然であると言えます。Tripwire Enterpriseでは、詳細なドリルダウン、サイドバイサイドの比較、ベースラインと比較の履歴などの機能により、「何が」、「いつ」、「誰により」、「どのような頻度で」、「どのように」変わったのか、といった調査チームが必要とする情報を迅速に提供し、環境への変化に関する詳細なフォレンジックデータを比類のない可視性をもって提供します。

業界を率いるセキュリティおよびコンプライアンス対応機能

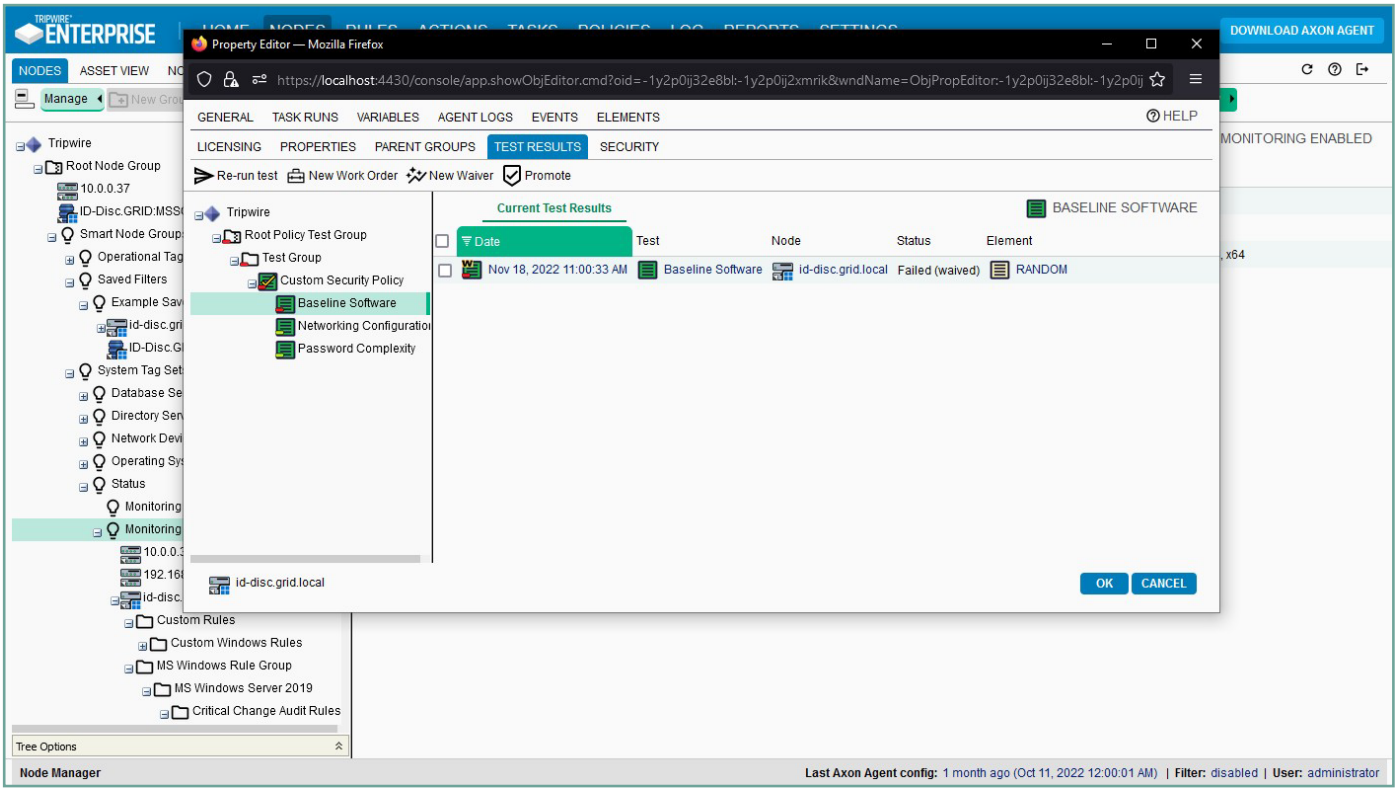
セキュリティとコンプライアンスの課題の変化に対応すべく、Tripwireは常に新機能を追加しています。Tripwire Enterpriseには、産業機器の保護機能と、MITRE ATT&CKフレームワークを使用して環境内の攻撃的なふるまいの証拠を発見する新機能が追加されました。

レポート機能と連携

監査対応のレポート、高度なセキュリティユースケース、およびServiceNowやSplunkなどの主要プラットフォームとの連携を提供するTripwire Enterpriseは、セキュリティの詳細とビジネスコンテキストを効率的に結びつけます。現在のセキュリティの状態（とその傾向）を常に把握し、リスクの低減に向けた企業目標を達成することを可能にします。組織全体から事業部門や個々の部署に至るまで、企業全体のセキュリティとリスクの傾向を視覚化します。

MITRE ATT&CKフレームワーク

MITER社が開発したATT&CKフレームワークは、攻撃者らのふるまいを提示し、リスクの軽減とセキュリティの向上のために取るべき対策を詳細に説明するサイバーセキュリティモデルです。ATT&CKのポリシーコンテンツをTripwire Enterpriseに適用すると、環境内の攻撃的なふるまいの検知とレポート生成が可能になり、御社のセキュリティ戦略に新たな防御層が追加されます。ただし、これはTripwireの包括的なコンテンツライブラリで利用できる数十のフレームワークのうちの1つに過ぎません。



ノードの詳細画面にノードのポリシーテスト結果が示される

主な機能と利点

ハイブリッド環境のサポート

» オンプレミスとクラウドの両方の環境において、セキュリティとコンプライアンスの状態を監視します。
» 単一のソリューションを両方の環境で使用できるため、コストを削減しながらも、優れた可視性を確保できます。

最新のデータ収集＆コミュニケーション

» プラガブルで拡張可能なエンドポイントデータ収集＆コミュニケーションプラットフォームであるTripwire Axon®上で、クラス最高レベルのセキュリティ、整合性監視、および構成＆コンプライアンス管理機能を提供します。

クラウド資産の自動オンボード/オフボード

» 動的な環境内で資産が接続されると、ただちに分類とスキャンを実行します。
» 資産のライフサイクルを通じて変化を監視するためのベースライン状態を(短期的なものであっても)即座に提供できます。
» 自動オフボーディング機能では、一時的な資産データを保持する期間を定義できます。

あらゆるIT構成を一元管理

» サーバー、デバイス、アプリケーション、複数のプラットフォーム、OSを含む物理および仮想ITインフラストラクチャ全体において、構成の一元管理を可能にします。

REST APIを使用した高度な統合

» Tripwire Enterpriseのプログラムによる自動化、収集した情報の抽出、他のソリューションとのカスタム連携を可能にします。
» 管理用APIでルーチンタスクの自動化を可能にし、Tripwire Enterpriseのワークフローを他のビジネスプロセスやツールと統合できます。

強力なAsset View

» Asset Viewでは、リスク、優先順位、地理的位置、規制ポリシーなどの業務用途に適したタグで資産を分類できます。
» 資産タグファイルを使用したプロビジョニング、多数の資産に対応する拡張性、他のTripwire製品との統合による資産タグのインポートなどの機能を提供します。

問題のある構成の管理のためのワークフローツール

» ロールベースのワークフローツールとして機能するRemediation Managerモジュールを提供し、安全性に問題のある構成や規則に準拠していない構成の手動/自動修復を、ユーザーが承認、却下、延期、または実行できるようにします。

変更管理システムとの連携

» ServiceNow、Remedy、Cherwell、JIRAなどの主要な変更管理システム(CMS)と連携できます。
» 検出した変更と変更チケット/リクエストとを自動的に照合します。

コンプライアンスに準拠したセキュアな状態を維持

» APCI、NERC、SOX、FISMA、DISAなどの業界規制/標準への準拠を自動化します。
» 構成評価機能とリアルタイムファイル整合性監視(FIM)機能を組み合わせて、変更の発生を検出、分析してレポート生成を行うことにより、構成を常にコンプライアンスに準拠した状態に保ちます。また、変更が深刻なデータ侵害を引き起こしたり、監査で不備を指摘されたり、あるいは長期間の機能停止につながったりする前に問題を修正できます。

迅速で簡単な監査準備

» 継続的かつ包括的なITインフラストラクチャベースラインとリアルタイムの変更検出機能を提供します。また、変更の影響を判定できるインテリジェンスも用意され、監査の準備にかかる時間と労力を大幅に削減します。
» 監査への対応を意識したレポートが提供されるため、自信を持って正当性を主張できます。

Active DirectoryとSAMLの統合

» Tripwire Enterprise を、Active Directoryまたはお好みのIDPと統合すると、ユーザー、グループ、ロールの自動作成が可能になり、管理オーバーヘッドの削減と、人的エラーの回避が実現し、安全かつ効率的なアクセス管理が行えます。

御社のITスタックに広く対応

監視対象が、ミッションクリティカルなサーバーである場合も、クラウド/仮想化環境やアプリケーションを含むITインフラストラクチャ全体である場合も、Tripwire Enterpriseがポリシーを評価、検証、実行し、ソースに関係なくすべての変更を検出する機能を提供します。次のような、エージェントベースおよびエージェントレスの革新的な監視機能をサポートします。

物理、仮想、クラウド、ハイブリッド環境: Tripwire Enterpriseは、プライベート、パブリック、ハイブリッドクラウドなどの物理および仮想環境内で動作します。Tripwire Enterpriseコンソールは仮想マシンとして動作可能であり、あらゆる仮想または物理エンドポイントをエージェント経由で監視できます。

ファイルシステムおよびデスクトップ: フォレンジックレベルのインサイトを活用して、物理/仮想サーバーおよびデスクトップファイルシステムの構成を評価します。これには、セキュリティ設定、構成パラメーター、権限が含まれます。

ディレクトリサービス: LDAPスキーマ、パスワード設定、ユーザー権限、ネットワークリソース、グループ更新、セキュリティポリシーなど、LDAP準拠のディレクトリサーバーオブジェクト/属性に対する独立したコンプライアンスポリシー管理を行います。

ネットワークデバイス: POSIX準拠のOSを実行するあらゆるデバイスをはじめ、業界で最も幅広いネットワークデバイスの構成評価に対応します。カスタムの接続パラメーターを使用して、ほとんどのデバイスを監視できます。

データベース: Oracle、Microsoft、およびIBMのデータベースサーバーとインスタンスが安全かつ高性能な状態を維持するのに役立ちます。

VMware: VMware仮想インフラストラクチャ全体に対する可視性を提供し、仮想環境の構成を継続的に制御できます。

アプリケーション: コンプライアンスポリシー管理機能とファイル整合性監視機能によって、サポートするアプリケーションがセキュリティ、コンプライアンス、機能、可用性の面で適切な構成になっていることを確認します。

カスタマイズ可能で柔軟なデバイスサポート: Tripwireは、すぐに使える4,000以上の設定を含むコンテンツライブラリを保持しています。設定不要のTripwire Axon®エージェントのカスタマイズ可能な監視機能を利用して、Tripwire Enterpriseは、一般的なプロトコルやAPIをサポートするほとんどのデバイスで動作することができます。これにより、御社の運営に不可欠な資産を柔軟に監視することが可能となり、社内資産や市場にはあまり出回っていない種類のカスタムソリューションにも対応します。

監視対象のシステム:

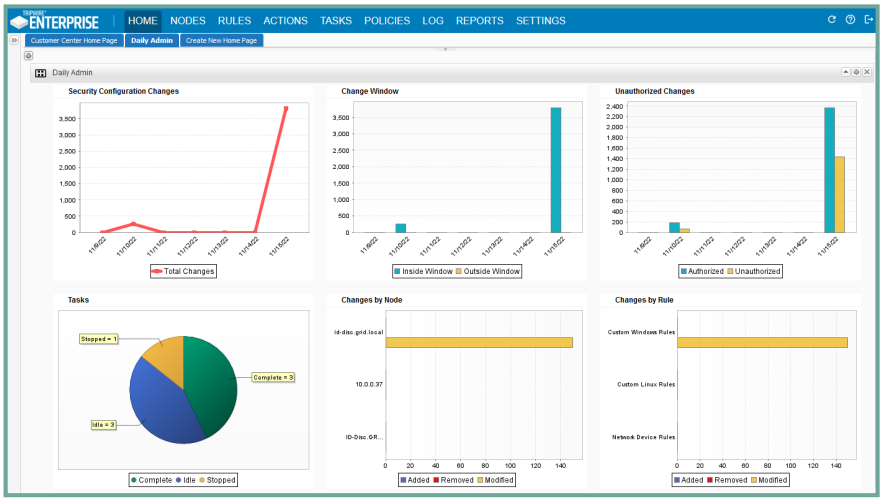
主要なOS: Windows、Red Hat、Oracle、AIX、SUSE、Debian、Ubuntu、Solaris、CentOS、Rocky、HP-UX

ディレクトリサービス: Active Directory、LDAP

ネットワークデバイス: ファイアウォール、IDS/IPS、ルータ、SSHデバイス

データベース: Oracle、MS SQL、DB2、PostgreSQL

仮想インフラストラクチャ: VMware



セキュリティと構成変更のコンプライアンス状態が表示されるTripwire Enterpriseのカスタマイズ可能なダッシュボード

さらに詳しい情報が必要ですか？

Tripwire Enterprise のレポート機能をはじめとする諸機能、利用可能なポリシー、対応プラットフォームなどの詳細については、tripwire.comをご覧ください。

FORTRA

Fortra.com

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、よりシンプルでより強固な未来をお客様のために創造しています。当社の信頼のおける専門家と、包括的で拡張可能なソリューションのポートフォリオが、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。常にお客様の味方であり、積極的な変革者である当社は、サイバーセキュリティの旅におけるすべてのステップを通じて安心を提供いたします。詳細については fortra.com.をご覧ください。