Cisco Tetration Analytics プラットフォーム

メリット

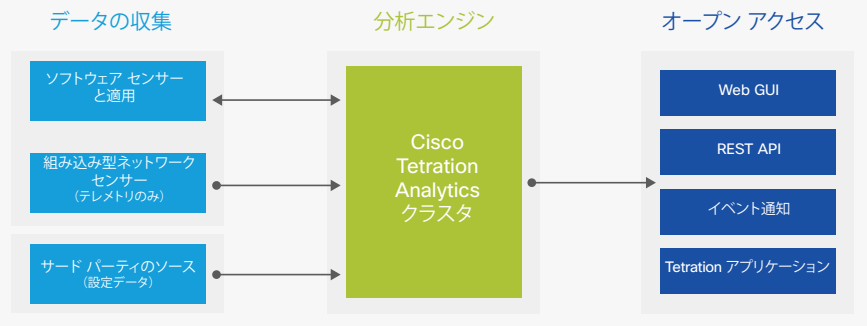
- ふるまいベースのアプリケーションの情報により、自動化されたホワイトリスト ポリシーを提供します。
- 自動化されたアプリケーション セグメンテーションにより、効率的かつ安全なゼロトラストの導入を可能にします。
- オンプレミス データセンター、およびプライベート クラウドとパブリック クラウドの環境全体で一貫性のあるポリシー適用を実現します。
- アプリケーションの動作の変更やポリシーの遵守違反をほぼリアルタイムに特定します。
- 異種環境での包括的なテレメトリ処理をサポートすることにより、実用的な情報を数分で提供します。
- 詳細なフォレンジック、分析、およびトラブルシューティングのデータを長期間保持します。

ふるまいベースのアプリケーションの情報とゼロトラスト ポリシー

さまざまなアプリケーションによって、データセンター インフラストラクチャは方向付けられています。現在のアプリケーションは非常に動的で、仮想化、コンテナ化、マイクロサービス、ワークロード モビリティ技術が使用されています。しかも、アプリケーション コンポーネント間の通信パターンは常に変化を続けています。現在、データセンター トラフィックの 76 % は East-West トラフィックです。これは過去のトラフィック パターンから根本的に変化しています。技術面でのこのような変化により、攻撃対象が増加し、適用インフラストラクチャにおけるギャップが広がっています。ネットワークとセキュリティの運用チームは、今日のダイナミックなアプリケーションに効果のあるセグメンテーションを実装するのに困難を抱えています。この課題に効果的に対応するために、ネットワークとセキュリティの運用チームにはアプリケーションに関するさらに詳細な情報が必要であり、また、必要なホワイトリスト ポリシーの生成と適用を自動化する必要があります。

Cisco Tetration Analytics™ プラットフォーム（図 1）は、人手を介さない機械学習、動作分析、アルゴリズム的アプローチを使用してこれらの要件に対応します。データセンターで実行されているアプリケーションとその依存関係、および異なるアプリケーション階層間にあるポリシーを正確に特定する、すぐに使えるソリューションを提供します。さらに、アプリケーション ワークロード内でのポリシーを正規化し自動化するとともに、ポリシーの遵守違反を追跡し、アプリケーションの動作の変更に応じてアプリケーション セグメンテーション ポリシーを最新の状態に維持します。このアプローチにより、Cisco Tetration Analytics プラットフォームは、パブリック クラウドとプライベート クラウド、およびオンプレミスのデータセンターで動作する、仮想化された、あるいはベアメタル ワークロードにわたって、一貫性のあるアプリケーション セグメンテーションを提供します。

図 1. Cisco Tetration Analytics プラットフォームのアーキテクチャ



このプラットフォームは、データセンター インフラストラクチャ全体に導入されたハードウェア センサーとソフトウェア センサーの両方を使用して、既存の環境（ブラウンフィールド）と新規展開（グリーンフィールド）の両方をサポートできます。ソフトウェア センサーは、アプリケーション セグメンテーションのエンフォースメント ポイントとしても機能します。

Cisco Tetration Analytics プラットフォームは、ビッグデータ テクノロジーを活用してデータセンター規模の環境をサポートします。センサーから受信した包括的なテレメトリ情報を、ほぼリアルタイム（毎秒最大 200 万件のテレメトリ イベント）で処理できます。このプラットフォームは、数万台のサーバで実行される多数のアプリケーションにわたって一貫性のあるポリシーを適用できます。また、長期にわたってデータを保持するよう設計されており、保持されたデータから数百億件のテレメトリ レコードを検索し、1 秒以内に実用的な情報を返すことができます。

動作分析を使用した、情報に基づく運用上の意思決定

Cisco Tetration Analytics プラットフォームは、人手を介さない機械学習と動作ベースのアルゴリズム的アプローチを使用した、すぐに使用できるソリューションです。

- **アプリケーションの情報：**機械学習の手法を使用して、アプリケーションの依存関係や動作のベースライン設定を含むアプリケーション情報を提供できます。また、通信パターンとプロセス情報を使用して、アプリケーション コンポーネント クラスタ（例：データベース クラスタ）を自動的に特定し、グループ化します。このリアルタイムのテレメトリ データを使用して、アプリケーション セグメンテーションに必要なホワイトリスト ポリシーを自動的に生成できます。

「Cisco Tetration Analytics プラットフォームは、ネットワークとアプリケーションに対する優れた可視性を実現してくれました。また、従来のブラックリスト ポリシー モデルから、安全性がはるかに高い ACI ベースのホワイトリスト ポリシー モデルへ移行することができました」

– 医療分野のお客様

- **アプリケーションの動作ベースのポリシーに関する推奨：**Cisco Tetration Analytics プラットフォームは、高度なアルゴリズムを使用して、アプリケーションの情報に基づいて生成されたポリシーと企業のセキュリティ ポリシーの要件をマージすることができます。たとえば、実稼働データベース サーバがインターネットと通信しないようにポリシーを指定できます。このようなポリシーの正規化および階層型のマージにより、範囲が制限された管理者が上位レベルのビジネス ポリシーの意図をオーバーライドできないようにします。
- **ポリシーの影響分析：**「適用前に試行」モードをサポートしているため、ポリシーを実稼働ネットワークに適用する前に、ホワイトリスト ポリシーをシミュレーションしてその影響を分析できます。
- **自動化されたポリシー適用：**Cisco Tetration Analytics プラットフォームは、パブリック クラウドとプライベート クラウド、およびオンプレミスの導入全体にわたって、ソフトウェア センサーを使用して一貫性のあるポリシー適用を実現します。ポリシーはワークロード自体に適用されるため、仮想化環境とベアメタル環境の両方がサポートされます。また、アプリケーション コンポーネントがベアメタル サーバから仮想化環境に移行される場合でも、ワークロードとともにポリシーが確実に移行されます。
- **コンプライアンスおよび監査対応機能：**アプリケーション コンポーネントがネットワーク ポリシーに準拠しているか監視します。また、動作分析手法を使用してコンプライアンス違反を短時間で検出し、通知をトリガーできます。さらに、アプリケーションの動作の変更に応じて、適用ポリシーが自動的に更新されます。

- **データセンターに対する可視性、トラブルシューティング、フォレンジック用の検索エンジン：**このプラットフォームでは、フロー データを包括的に収集して保存します。可視性を高め、フォレンジックを行うためにデータセンター全体に対してフロー データを照会し、そのデータを使用してネットワークおよびアプリケーションの問題をトラブルシューティングすることができます。

Cisco Tetration Analytics プラットフォームは、業界のどの製品とも一線を画しています。すぐに使えるプラットフォームに高度な管理機能を搭載し、迅速に導入できます。構成要件はほとんどありません。機械学習機能によって、通信パターンを理解するために必要な手作業による入力の量が大幅に削減されます。ポリシー適用モデルにより、アプリケーション セグメンテーションを使用したアプリケーションの安全なゼロトラスト運用が可能です。自己モニタリングおよび自己診断機能を備えているため、ビッグデータの専門家がクラスタを運用する必要がなくなります。

Cisco Tetration Analytic サービスによる価値創出までの時間の短縮

Cisco Tetration Analytics サービスを活用することで、Cisco Tetration Analytics による価値創出までの時間を加速できます。サービスには、費用対効果の高い固定の範囲を指定されたセレクト サービス バンドルや、個々のお客様のニーズに応じてカスタマイズされるカスタム サービス、Tetration Analytics ソリューションを活用して最大限の運用効果を実現するための継続的なサブスクリプション サービスがあります。

データセンターにおける Tetration Analytics の迅速な展開と統合、個々のお客様の環境に固有の使用例の定義、検証済みのアプリケーション セグメンテーション ポリシーの展開を、サービス エキスパートが支援します。さらに、Cisco Tetration サービスでは、API、Tetration アプリケーション、カスタム通知を含め、カスタム統合の専門知識を提供します。Cisco Tetration サービスを利用することで、お客様は価値創出までの時間を短縮し、包括的な導入、ポリシーおよびアプリケーション パフォーマンスの最適化を実現できます。また、Tetration 向けシスコ ソリューション サポートは、1 つのサービスでハードウェア、ソフトウェア、ソリューション全体のサポートに対応し、Cisco Tetration Analytics と Tetration エコシステム パートナーの製品を対象とした一元的な問題管理と解決を図るグローバルなソリューションの専門知識を、1 日 24 時間年中無休で提供します。

詳細については、『Tetration Services At-a-Glance』を参照してください。
https://www-author.cisco.com/c/dam/en/us/products/collateral/data-center-analytics/tetration-analytics/at-a-glance-c45-738443.pdf [英語]

関連情報

Cisco Tetration Analytics プラットフォームの詳細については、http://www.cisco.com/go/tetrationanalytics を参照してください。

C45-737257-01 03/17