tufin The Security Policy Company.

Tufin SecureCloud ソリューション概要

ハイブリッド・クラウド環境全体のセキュリティ姿勢を可視化し、制御することができます。これにより継続的なコンプライアンスを保証します。妥協することなくゼロトラストを実現。

ビジネスにとってのメリット:

- ハイブリッドクラウドのセキュリティ姿勢をリアルタイムで可視化し、制御
- ハイブリッドクラウド環境全体にセキュリティポリシーを適用
- マイクロサービスの通信を安全に管理
- DevOps CI/CDプロセスへのセキュリティの組み込み
- セキュリティの変更を数日ではなく数分で実施
- 煩雑さや障害の無い適用 – アプリケーションコードの変更や設定を必要としないクラウドネイティブのエージェントレスソリューション
- ネットワークポリシー制御をKubernetesに統合

課題

ハイブリッド・クラウド環境は増加傾向にあり、それには正当な理由があります。企業はパブリック・クラウドの効率性、俊敏性、拡張性を活用して、デジタル・トランスフォーメーションの取り組みを進めています。グローバル規模のアプリケーションを迅速に構築して展開することができるため、企業は競争力を高め、市場の動きやビジネス・ニーズへの対応力を高めることができます。しかし、DevOps、クラウド、および IoT チームは、ほとんど、あるいは全くセグメント化されていない状態でアプリケーションを展開していることが多く、潜在的なリスクが発生しています。その結果、セキュリティ・チームは、複雑で断片化されたネットワークを管理・制御するために異なるソリューションを使用していることが多く、「ネットワーク上にはどのような資産が存在し、既存のセキュリティ・ポリシーを遵守しているか」といった単純な質問に答えることができません。セキュリティチームがアジャイル開発を妥協することなく、可視性や、コンプライアンスを保証するにはどうすればよいのでしょうか。

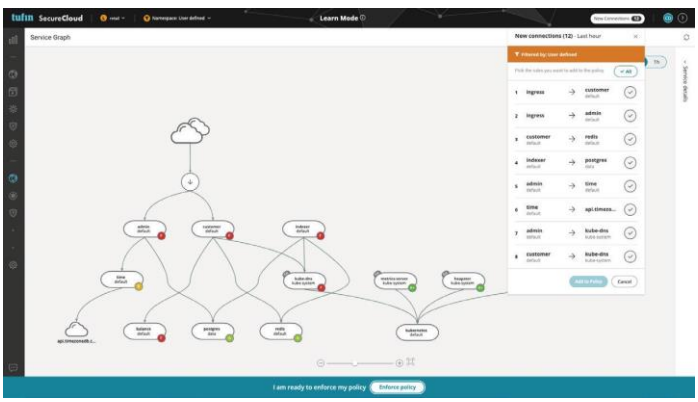
Tufin SecureCloud: クラウドネイティブな環境を安全に

Tufin SecureCloudは、ハイブリッドクラウド環境のセキュリティとコンプライアンスを保証するために必要な、リアルタイムでの可視性と制御を提供する、セキュリティポリシー自動化サービスです。Tufin SecureCloudはSecurity-as-a-Serviceとして提供されます。そして、自動化されたセキュリティポリシーのオーケストレーションにより俊敏性とセキュリティを最大化し、ネットワークの複雑さを管理し、セキュリティポリシーの変更を自動化します。SecureCloudは継続的なコンプライアンスを保証します。これによりゼロトラストを実現し、スピードや俊敏性を犠牲にすることなく、クラウドの導入とデジタルトランスフォーメーションを加速させます。

視認性とコントロールを取り戻す

ダイナミックなハイブリッド・クラウド環境でセキュリティとコンプライアンスを確保するために、セキュリティチームはリアルタイムの可視性、分析、レポート、介入ソリューションを必要としています。

- 自動ポリシー検出機能を使用して、ワークロードやネットワークオブジェクトを自動的に検出し、可視化します。
- アプリケーション中心のトポロジー ビューを使用して、適用されたすべてのアセット、構成、セキュリティ設定を可視化します。アプリケーションの接続先を把握して、ポリシー違反を検出し、信頼できるワークロードとトラフィックのみが許可されていることを確認します。

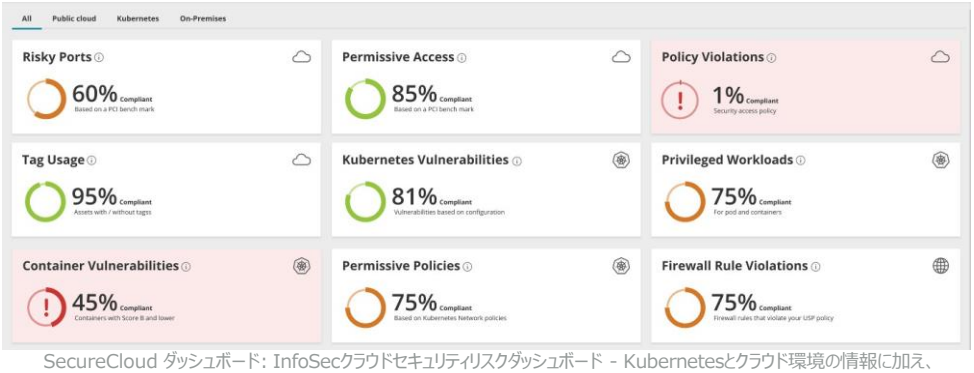


SecureCloud トポロジー:新しく見つかったすべての新規接続を含む、ハイブリッドクラウド全体のすべてのサービス、セキュリティ態勢のスコアや、トラフィックを完全に可視化します。

継続的なコンプライアンスを保証する

クラウド リソースとアプリケーションが適切に設定されることで、セキュリティ要件に準拠した形でリスクを最小限に抑えることができます。ポリシー違反の継続的な監視、検出、アラートを活用して、迅速かつ効果的な緩和を実現します。

- セキュリティ状況ダッシュボード–コンテナ、パブリッククラウドサービス、およびファイアウォールを監視して、セキュリティポリシー違反を自動的に検出し、リスクのある領域を強調し、寛容なアクセスポリシー、ルール違反、危険なポート、およびコンテナの脆弱性をピンポイントで特定します（既存の脆弱性スキャナーとの統合により）。
- CI/CD パイプラインでのシフトレフト（後工程の作業を開発工程に組み込むこと）を実現したセキュリティコントロール-ネットワークセキュリティを CI/CD パイプラインに統合し、エンドツーエンドの自動化を実現し、準拠したコードのみを確実に適用します。
- アクション可能な修復–アプリケーションの可用性と事業継続性を維持しながら、不正な通信を自動的に警告し、ブロックします。
- 統一されたセキュリティ管理–クラウド環境が従来のITと同じセキュリティコンプライアンス要件を満たしていることを保証します。必要なポリシーに合わせて必要なセキュリティ構成を自動化します。
- アプリケーションライフサイクルセキュリティ–構築、テスト、デプロイ、運用など、アプリケーションのライフサイクル全体にわたって、セキュリティリスクの発見、警告、修復を自動化します。



SecureCloud ダッシュボード: InfoSecクラウドセキュリティリスクダッシュボード - Kubernetesとクラウド環境の情報に加え、デプロイされたワークロードと資産のコンプライアンス状況も含まれています。

ゼロトラストを実現し、クラウドの選択を加速

可視性とセグメンテーションにより、ゼロトラストと安全なクラウドへの移行を可能にします。

- ポリシーをあらゆる場所で強化 - アクティビティを継続的に監視し、攻撃対象を減らすマイクロセグメンテーションを自動的に行うことで、大規模で複雑なクラウド環境でのゼロトラストを実現します。
- ポリシー生成の自動化 - 実際のトラフィックに基づいて自動的に学習、生成、マイクロセグメンテーションを確立し、攻撃対象を減らすために権限の付与を最小にし、アクティビティを制限します。
- ポリシーをコードとして生成 - 手作業によるエラーを回避し、時間を節約し、アプリケーションの変更とセキュリティポリシーの整合性を確保するために、ポリシーをYAML形式で自動的に生成します。
- プラットフォームAPI - APIを活用してポリシーの制御を自動化し、アジャイル開発を維持しながらアプリケーションセキュリティのオーナーシップを取得できるようにDevOpsを強化します。

全社的なセキュリティポリシー管理

クラウドおよびクラウドネイティブ環境でのセキュリティ管理は、大変に複雑な問題の一部に過ぎません。ワークロードやアプリケーションがクラウドに移行すると、一部のアプリケーションではオンプレミス環境へのアクセスが必要になります。クラウドネイティブのアプリケーションでも、従来のネットワークセキュリティデバイスで保護されたリソースへのアクセスを必要とすることがよくあります。Tufin Orchestration Suiteの一部であるSecureCloudは、ビジネスのスピードを損なうことなく、すべてのハイブリッドクラウド環境にわたって統一されたセキュリティポリシー管理ソリューションを提供します。

世界中のグローバル企業2,300社以上がTufinを信頼して、複雑なハイブリッド環境におけるセキュリティポリシー管理の簡素化と自動化を実現しています。