Tufin Orca によるマイクロサービス アプリケーションのセキュリティ確保

ソリューション概要

DevOpsのスピードに応じたマイクロサービスのセキュリティ確保

さらなるビジネスの俊敏性が求められる中、コンテナやマイクロサービスベースのアーキテクチャを採用する DevOps 部門が増えています。このシフトにより、開発者は本番環境への変更内容を一日に数十回といった頻度で素早くビルドし、テスト、デプロイすることが可能になります。従来型のセキュリティツールやプラクティスを利用している IT セキュリティ部門は、いまや変更のペースについていくことができなくなっています。Tufin Orca は、自動的にアプリケーションの接続パターンを学習し、セキュリティポリシーを作成、実行時にセキュリティ確保を実現するクラウドベースのサービスです。

課題

マイクロサービス間の通信を安全に管理することは非常に複雑な作業であり、その内容は常に変化します。しかし、従来型のデータセンターとは異なり、Kubernetes のようなマイクロサービス環境は完全に自動的に運用されます。これにより、IT セキュリティを DevOps サイクルに完全に組み込まない限り、従来型のセキュリティサービスは増え続ける変更のペースに追いつくことが困難となり、組織がビジネスニーズにすばやく適応する上で阻害要因となります。そこで、IT セキュリティ部門は具体的に以下の内容へ適応する必要があります。

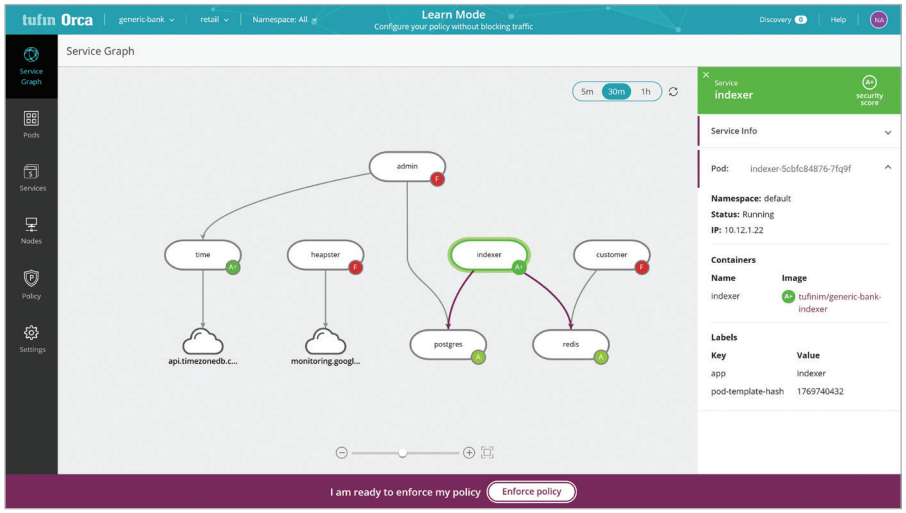
- マイクロサービス環境の可視化
- マイクロサービスおよびファイアウォール全体にわたるマイクロセグメンテーションの定義と適用
- セキュリティを CI/CD パイプラインに組み込むことによる DevSecOps の実現

可視性を取り戻す

マイクロサービス・アプリケーションは、クラウド上の Kubernetes や、オンプレミスの Red Hat OpenShift をはじめとするコンテナオーケストレーション・プラットフォームにデプロイされ、管理されます。

アプリケーションでは数百、時には数千のサービスが稼働していることもしばしばです。従来型のツールと異なり、Tufin Orca はマイクロサービス向けに設計されています。これにより、セキュリティマネージャーが全てのマイクロサービス・アプリケーションとそれらのコンポーネントの一覧を確認することが可能です。Tufin Orca は内部と外部におけるサービスの通信を正確に表示し、どのサービスが脆弱な状態にあり、どのようなセキュリティの問題が存在するかを示してくれます。

これにより、IT セキュリティ部門やクラウド運用部門が、ポリシーに準拠していない、またはリスクが高いために素早い対応が求められるリソースを迅速に特定することが可能になります。



主要機能とメリット

- マイクロサービスのセキュリティの可視化
- マイクロセグメンテーション・ポリシーの適用
- 継続的なコンプライアンス準拠とアラートの保証
- • DevOps ツールチェーンの統合によるセキュリティの自動化
- 無料アカウントの登録：tufin.io

Tufin 会社概要：

事業所：北アメリカ、ヨーロッパ、中東、アフリカ、アジア太平洋

顧客：50 カ国以上で 2100 社を超える顧客基盤

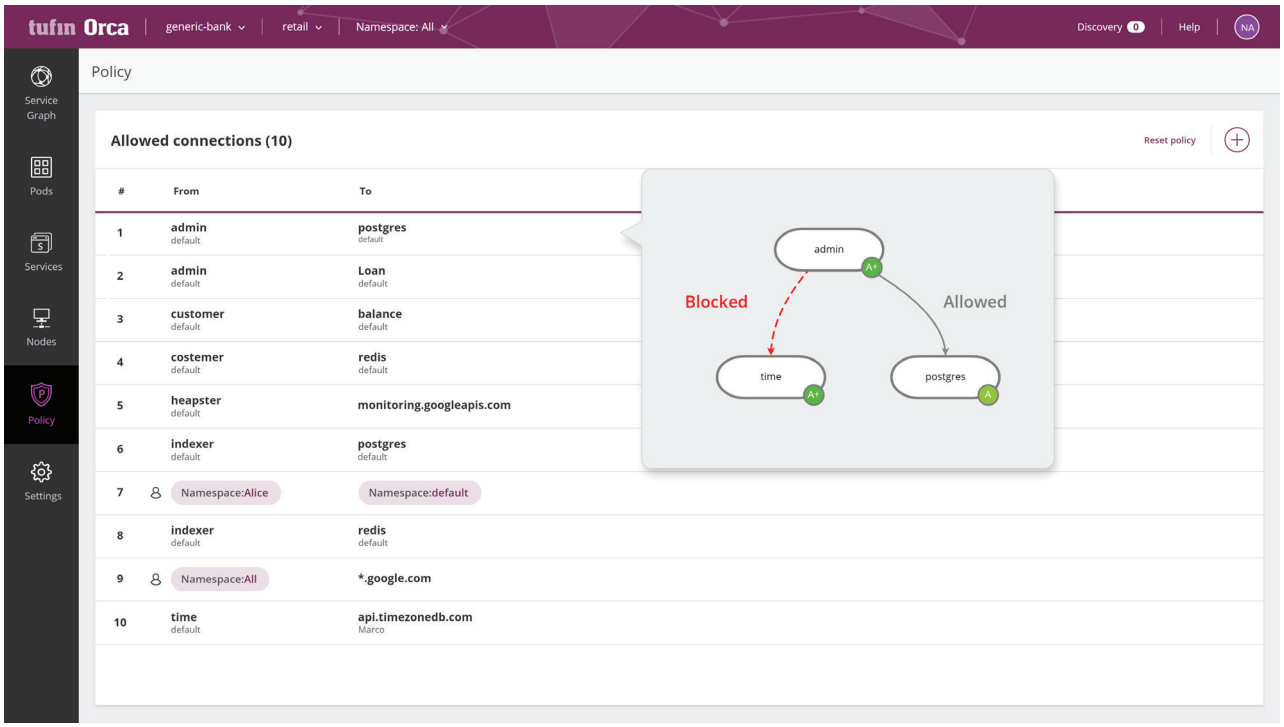
主要マーケット：金融、通信、エネルギー電気・ガス・水道、医療、小売、教育、政府、製造、運輸

チャネルパートナー：世界中で 150 以上のアクティブパートナー

テクノロジーパートナーおよび対応プラットフォーム：Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware and more

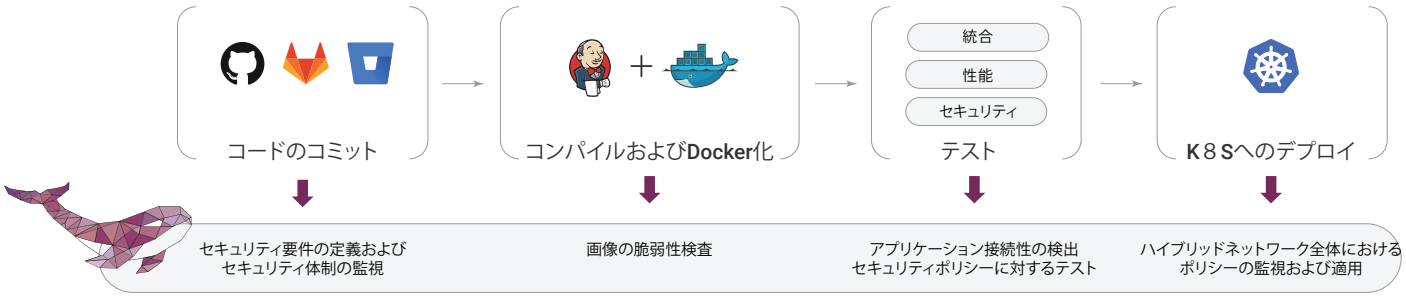
ハイブリッドネットワーク全体のセキュリティを自動化

セキュリティ部門は、業界、規制、業務要件に基づいたセキュリティポリシーの定義と適用を行うための手段を必要としています。Tufin Orca は通信の監視やセキュリティポリシーの自動作成によって、そのプロセスを単純化します。その後、セキュリティ部門は変化を続けるビジネスニーズに合わせてマイクロセグメンテーション・ポリシーを調整することができます。
Tufin Orchestration Suite との統合を通して、クラスター内部にポリシーを適用し、周囲のファイアウォールへ自動的に伝播させることができます。



CI/CD パイプライン内のセキュリティの自動化

これまで、セキュリティ対策はアプリケーション開発ライフサイクルの最後まで後回しにされてきました。実際、手作業のレビューを何週間もかけて行うことはよくあります。理想的には、セキュリティ問題は早期に発見され修正されるべきです。
一般的に「シフトレフト」と呼ばれるプラクティスです。Tufin Orca では、Jenkins などの一般的な CI/CD ツールを通してセキュリティポリシーが DevOps パイプラインに組み込まれ、本番環境前に容易にリスク判定やコンプライアンス検証を行うことが可能となります。



ぜひ無料トライアルをお試しください
Tufin Orca がどのようにコンテナやマイクロサービス・アプリケーションのセキュリティ確保を実現するのかご覧ください
無料アカウントのサインアップはこちら：tufin.io

tufin
www.tufin.com

SB-02-19

tufin Orca