Tufin Iris によるクラウドセキュリティの最新アプローチ

ソリューション概要

マルチクラウド環境のためのセキュリティポリシー運用自動化

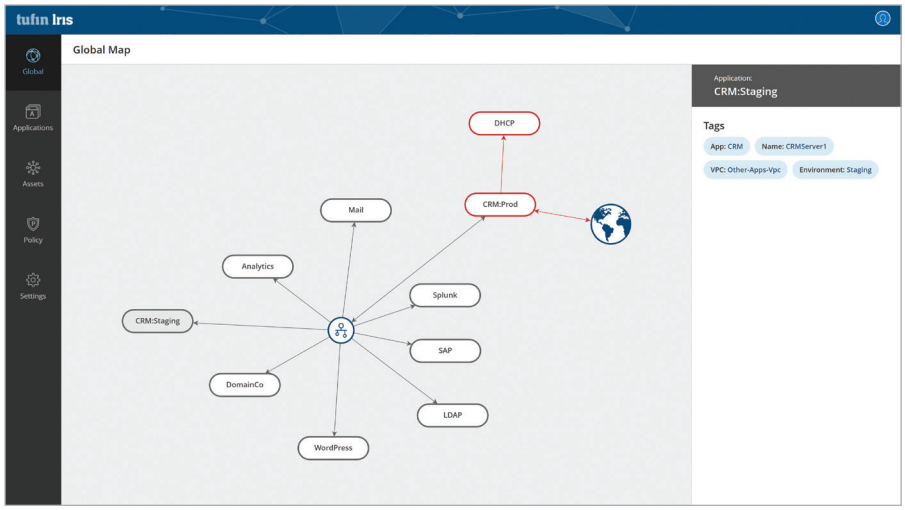
デジタル革命を支えるクラウドネイティブなプラットフォームは、ビジネスのフットワークを軽くし、イノベーションをさらに加速させています。クラウドファーストの世界では、機密情報の保護やアプリケーションのセキュリティ確保がこれまでになく重要性を増しています。
しかし、開発者が複数のクラウドプロバイダを利用し、アプリケーションのデプロイ頻度を高める一方セキュリティ対策はますます困難になってきています。
急速な技術革新に遅れをとらならないために、IT セキュリティ部門とクラウド運用部門は、新しいクラウドネイティブなソリューションによってミッションクリティカルなアプリケーションを保護する必要があります。
旧来のセキュリティソリューションは、物理インフラや仮想化環境を保護することを目的に設計されています。セキュリティ部門や IT 運用部門は Tufin Iris を利用することで可視性を取り戻し DevOps パイプラインと一体化した自動化技術により、クラウド内における柔軟なセキュリティポリシー制御を実現します。

課題

従来のセキュリティツールは、IP アドレスとポートに基づき、アクセスを許可または拒否することでアプリケーションを保護してきました。しかし、クラウドネイティブな環境において、IP アドレスはほんの一時的な情報に過ぎず、アドレスの代わりにユーザネーム等を使用してサービスにアクセスすることが多くなっています。さらに、アクセス制御ポリシーは、セキュリティグループと「ID とアクセス管理」（IAM）のロールとの組み合わせで定義されます。
したがって、ビジネスのコンプライアンス準拠を担保するためには、IT セキュリティ部門が可視化、制御、自動化を実現できる新しいソリューションが必要とされています。

可視性を取り戻す

ひとつのクラウド環境では数百、時には数千ものリソースが稼働している場合があります。
複数のクラウドアカウントやベンダーに分散していると、デプロイしているアプリケーションや、関連するセキュリティポリシーのコンプライアンス準拠を把握することは困難になります。
Tufin Iris はクラウドをインテリジェントに監視、全てのアプリケーションを検出して、簡単に全体把握ができるようマップに一覧表示します。
これにより、IT セキュリティ部門とクラウド運用部門がポリシーに準拠しないリスクをすばやく発見し、より安全で安定したシステム運用を実現します。



主要機能とメリット：

- パブリッククラウドのセキュリティ設定を可視化
- セキュリティ・ガードレールを用いて複雑なポリシー運用を回避
- マイクロセグメンテーション・ポリシーによるきめ細かなアクセス制御
- サービスとしてのエージェントレス・ソリューション
- DevOps ツールチェーンとの統合
- 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

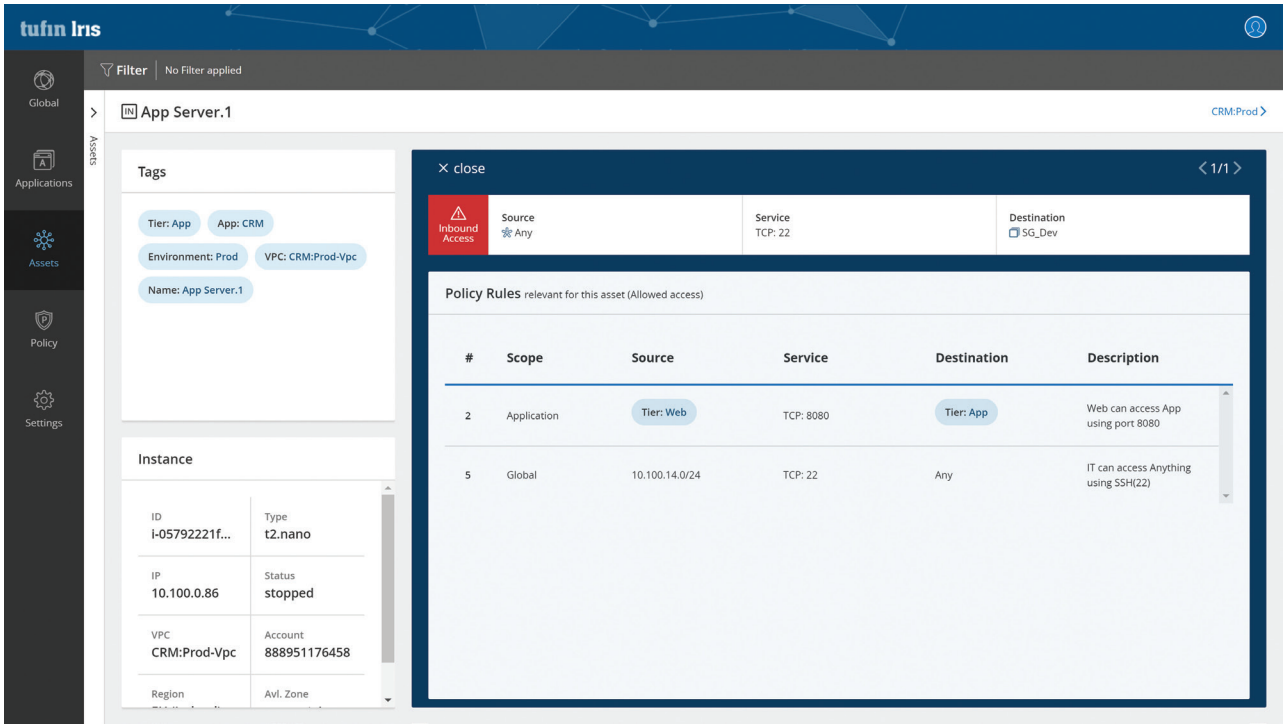
チャネルパートナー：世界中で 150 以上のアクティブパートナー

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

Azure　aws

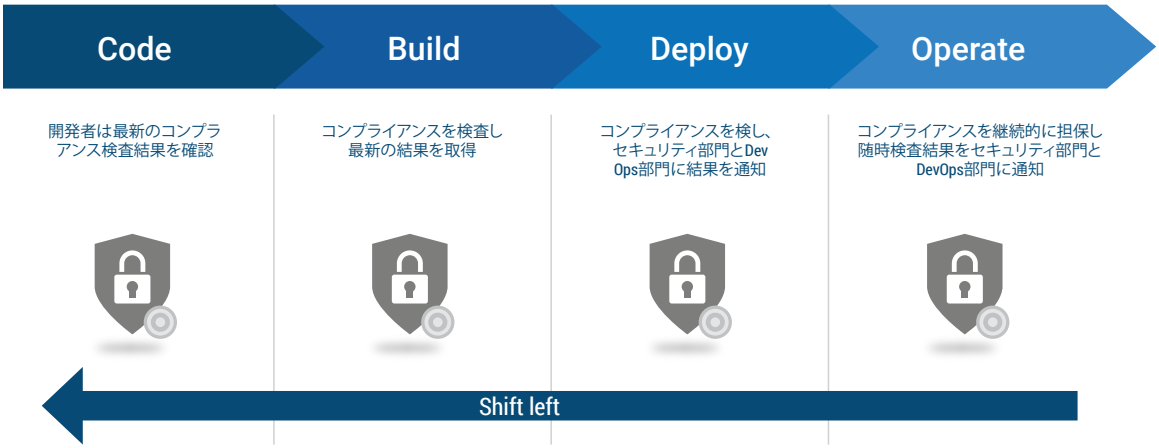
コンプライアンスの維持

セキュリティ部門は Tufin Iris を用いることで、業界、規制、業務要件に基づくセキュリティポリシーを手軽に定義することができます。また、セキュリティ・ガードレールを構築することで、複雑なポリシー運用やルールの肥大化に直面することなく、アプリケーションを保護することが可能です。そして、それらをグローバルに適用したり、一般的なリソースグループに対して適用することができます。例えば、ガードレールを利用することで、インターネットからのデータストレージへのアクセスがきちんと制限されているかどうか確認することができます。また、粒度の高い制御の例として、IT 部門がマイクロセグメンテーション・ポリシーを定義しアクセスを厳しく制限し、ミッションクリティカルなリソースを保護することができます。アクセス制限の対象は、顧客の個人情報を処理するサービスなどが想定されます。



セキュリティの自動化

クラウドにおけるセキュリティで、現在、最も効果的とされているのが「シフトレフト」といわれる早期予防策です。
セキュリティポリシー・レビューを開発ライフサイクルの最終段階に予定するのではなく、初期段階から全ての段階にわたって組み込みます。
Tufin Iris は Jenkins などの一般的な CI/CD ツールを通して DevOps パイプラインに組み込まれ、本番環境に入る前にリスク判定やコンプライアンス準拠の検証を行います



ぜひ無料トライアルをお試しください
Tufin Iris がどのようにマルチクラウド環境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 Iris