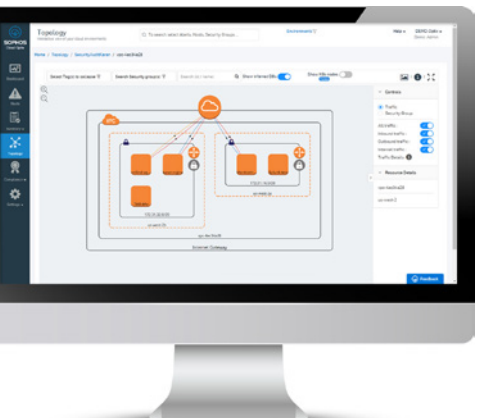
SOPHOS

Sophos Cloud Optix

AI と自動化テクロジーを組み合わせ、クラウド環境のセキュリティをシンプルに実現
Sophos Cloud Optix は、豊富なセキュリティ知見と AI 技術を併せ持ったエージェントレスの SaaS 型サービスです。クラウド環境のセキュリティ監視、分析、コンプライアンスオートメーションを、単一の使いやすいインターフェースで効率的に実施することができます。

主な特長

- エージェントレス、SaaS 型サービス。数分でセットアップ可能
- マルチクラウドのインベントリを管理
- ネットワークトポロジーとトラフィックフローを完全に可視化
- AI を活用したユーザー挙動やトラフィックの異常検知
- 継続的なコンプライアンス評価
- すぐに使える多様なコンプライアンスポリシー
- アラートの関連付けで修復にかかる時間を短縮
- 重要設定に加えられる変更の検知
- IaC (Infrastructure-as-Code) テンプレートを継続的にスキャン



すべて可視化、すべて保護

AWS (Amazon Web Services)、Microsoft Azure、GCP (Google Cloud Platform) 環境のユーザーのアセットを自動的に検出し、アセットを常時監視してネットワークトポロジーとトラフィック全体 (入口、出口、内部トラフィック) を可視化することにより、数分でセキュリティリスクに対応・修復することが可能です。

プロアクティブなクラウドコンプライアンス

ワークロードがクラウド環境に移行していくなか、適用すべきコンプライアンスプロセスを見極めるだけではなく、その施行方法を定めることは、ますます困難になっています。Sophos Cloud Optix は、すぐに使用できる各種テンプレート、カスタムポリシー、連係ツールなどの多彩な機能により、ガバナンスやリスク、コンプライアンスにかかるコストと手間を削減します。

コンプライアンスプロセスをスピードアップ

CIS、GDPR、SOC2、HIPAA、ISO 27001、PCI DSS などの規格に対応する事前設定済みテンプレートやカスタムテンプレートを使用して、コンプライアンス状態を常に監視します。

コラボレーションが簡単に

JIRA や ServiceNow などのサードパーティツールと連係し、コンプライアンスの管理と追跡を行うため、リリースの最中でも重要な課題を取りこぼすことがありません。

AI を活用したセキュリティ分析と監視

Sophos Cloud Optix は、クラウド環境におけるアセットのインベントリ、構成、ネットワークトラフィックを継続的に監視して学習を行います。AI を用いた高度な警告機能や、コンテキスト情報を活用して自動的に行われる警告の順位付けにより、レスポンスタイムを短縮し、セキュリティリスクをより迅速に修復できます。

- クラウド環境におけるアセットのインベントリ (Amazon Simple Storage Service (S3)、セキュリティグループ、ユーザーのアクセスキーなど)、構成、セキュリティグループのログを継続的に監視
- ユーザーの異常な挙動パターンを識別し、ユーザーアクセスキーの窃取やなりすまし従業員による自動化された高度な攻撃を検知
- セキュリティ設定に基づいてネットワークトラフィックの流れ方を予測 – 攻撃が開始される前に侵害される可能性があるポイントを防御
- ネットワーク設定の変更のミスおよび悪質な変更を防止、検出、修復するための予防対策を提供

スマートな DevSecOps

継続的デプロイに伴うインフラの変更のスピード化や、DevOps 手法の導入により、1日に何度もソフトウェアをリリースすることができますが、このような工程は、セキュリティチームに大きな負担がかかり、セキュリティが後回しにされてしまう可能性があります。Sophos Cloud Optix の API 指向アーキテクチャは、セキュリティを DevOps プロセスにシームレスに統合し、DevOps チームのリリース作業のスピード化とセキュリティ対策の両立を実現します。

設定変更の検出と予防対策

設定に加えられる変更を継続的に監視・検出し、組織をリスクにさらす可能性のある重要な設定の変更を防止します。

インフラ用テンプレートをプロアクティブにスキャン

Terraform、Github、Bitbucket などのソリューションからデプロイした IaC (Infrastructure-as-Code) テンプレートを継続的にスキャンします。脆弱性を持つインフラのプロビジョニングの原因となる設定ミスを検出します。

SIEM と DevOps ツールの統合

CI/CD (継続的インテグレーション / 継続的デリバリ) 用の SIEM や DevOps ツールなどのサードパーティのセキュリティ機能と統合して、セキュリティ対策を簡素化します。

簡単な管理と導入

エージェントレス型 SaaS サービスである Sophos Cloud Optix は、既存のビジネスツールとスムーズに連係します。

あらかじめ用意されている手順やスクリプト (ネイティブクラウド API で読み取り専用アクセスを作成) を使用して、AWS、Azure、GCP などのクラウドアカウントに簡単に接続できます。接続は数分で設定可能です。Sophos Cloud Optix を導入した後、すぐにお使いのクラウド環境にアクセスして重要な情報を確認することができます。

クラウド環境のセキュリティの責任共有

パブリッククラウドベンダーは、プラットフォームの高い柔軟性を提供します。しかし、データセンターの物理的なセキュリティや、データと環境の仮想分離は、ベンダーが責任を持つ一方で、ユーザーがクラウドにアップロードするものはすべてユーザー側の責任となります。

Sophos Cloud Optix は、継続的な可視性、コンプライアンス、脅威対応を実現します。ソフォスが提供するパブリック クラウド ワークロードのセキュリティ対策と次世代型ファイアウォール製品のラインナップは、sophos.com/ja-jp/public-cloud よりご覧になれます。

Sophos Cloud Optix の機能	
マルチクラウド環境を単一のコンソールから管理	✓
トポロジーの可視化	✓
ネットワークトラフィック可視化オーバーレイ	✓
セキュリティグループ可視化オーバーレイ	✓
異常検知 – ネットワークトラフィック	✓
異常検知 – ユーザーログインの挙動	✓
インベントリ – ホスト、ネットワーク、ストレージ、IAM	✓
インベントリ – AWS CloudTrail	✓
インベントリ – サーバーレス	✓
継続的なコンプライアンス評価	✓
コンプライアンス対応ポリシー (CIS、FEDRAMP、FFIEC、GDPR、HIPAA、ISO 27001、PCI DSS 3.2、SOC2、EBU R 143)	✓
CIS ベンチマーク対応ポリシー	✓
カスタムポリシー	✓
コンプライアンス/ベストプラクティスのアラートとレポート	✓
修復と予防対策	✓
DevSecOps スクリプト評価	✓

無料製品デモ、無償評価版

Cloud Optix の全機能を30日間無料でお試しいただけます
Sophos.com/ja-jp/cloud-optix

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2019/05/14 DS (PC)

SOPHOS