

ソフォスのクラウドセキュリティポスチャ管理



ソフォスのクラウドセキュリティポスチャ管理ソリューションである Sophos Cloud Optix は、AWS (Amazon Web Services)、Microsoft Azure、および Google Cloud Platform パブリッククラウド環境全体での未承認のアクティビティ、脆弱性、および設定ミスによるビジネスリスクをプロアクティブに削減します。

完全なクラウドセキュリティポスチャ管理

Sophos Cloud Optix は、マルチクラウド環境全体のクラウドリソースの全体像を提供します。コストの監視、安全でない構成と展開の検出、アクセスの異常、過剰な権限を付与された IAM ロール、および開発からライブサービスの継続的なセキュリティまでのコンプライアンス障害などです。

脅威をより迅速に特定して対応

サイバー攻撃で特定され、悪用される前に、最も重要なセキュリティの脆弱性に焦点を当てて修正します。Cloud Optix は、セキュリティ、コンプライアンス、クラウドの利用におけるリスクを特定し、リスクプロファイリングすることで、チームがより迅速に対応できるようにし、影響を受けたリソースを詳細な修復手順でグループ化するコンテキストアラートを提供します。

DevOps のペースに合わせたセキュリティ

Cloud Optix で、コンテナイメージと Infrastructure as Code テンプレートの脆弱性を本番環境への展開前にブロックします。開発のあらゆる段階でソフォスのセキュリティチェックとコンプライアンスチェックをシームレスに統合し、本番環境に脅威をもたらすことなく DevOps のペースを維持します。

権限が悪用される前に管理

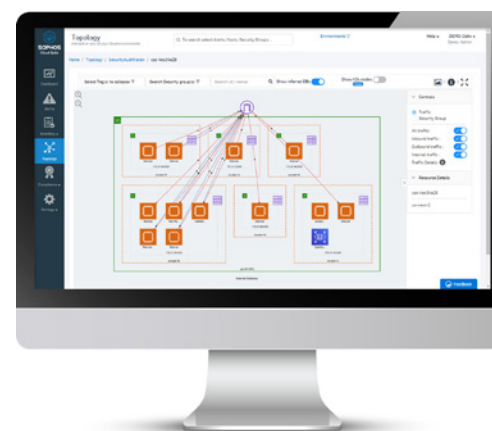
Cloud Optix は、複雑に混ざり合う IAM (Identity and Access Management) のロールを分析して関係を視覚化し、ユーザー、グループ、クラウドサービスの役割へのアクセス権限をより簡単に管理できるようにします。過剰な権限を持つ IAM のアクセスが悪用される前に、クラウドプロバイダーで IAM ポリシーを更新する場所を説明します。

コンプライアンスコストと複雑を軽減

Sophos Cloud Optix は、ユーザーの環境へ自動的にマッピングされるポリシーの準拠のコストと複雑さを軽減し、他のプロジェクトからリソースを変更することなく、監査準備の整ったレポートを作成します。コンプライアンスおよびセキュリティのベストプラクティスポリシーには、次のものが含まれます。GDPR、HIPAA、PCI DSS、SOC2、ISO27001、FIEC、EBU R 143、FedRAMP、AWS の CIS Benchmark Level 1 と Level 2、Azure、Google Cloud および Kubernetes。

主な特長

- ▶ AWS、Azure、Google Cloud、Kubernetes を監視
- ▶ 複数のクラウドのアセットとネットワークトラフィックの可視性
- ▶ ガイド付き修復機能により、セキュリティ問題のリスクベースの優先順位付け
- ▶ 消費を最適化し、異常なアクティビティを検出
- ▶ 過剰な権限が付与されたユーザーとロールベースのアクセスを特定
- ▶ DevOps 統合で導入前の脆弱性をブロックします。



SOPHOS

クラウドコストを最適化し、セキュリティを強化

クラウドサービスを同時に並べて追跡して可視性を向上させ、AWS、Azure の支出を最適化するための推奨事項を受け取り、不正使用やアカウントの侵害を示す異常なアクティビティを特定します。

シームレスに統合

クラウドプロバイダーのネイティブサービスと統合し、さらに大きな価値を引き出します。Cloud Optix は、AWS CloudTrail、Amazon GuardDuty、AWS Security Hub、Azure Sentinel などのクラウドサービスプロバイダーからのセキュリティアラートの分析とリスク優先順位付けを自動化し、セキュリティチームがイベントに迅速かつ効率的に対応できるようにします。Cloud Optix の機能に REST API を介してプログラムでアクセスしながら、SIEM や DevOps ツールなどの サードパーティーのサービスに統合し、セキュリティ運用を合理化したり、コラボレーションを向上させます。全ての統合については、soph.so/cloud-integrations を参照してください。

XDR を使用してデータソースを拡張

Cloud Optix を使用して、AWS、Azure、Google Cloud 環境の API、CLI、および管理コンソールのアクティビティを検出します。次に、EC2 インスタンスやクラウド内の仮想マシンのワークロード

で実行されている Sophos Intercept X for Server ワークロード保護エージェントの追加コンテキストを使用して、調査結果を調査します。Cloud Optix Advanced および Intercept X Advanced for Server with XDR が必要となります。

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接続します。

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、Google Cloud などのクラウドアカウントに簡単に接続できます。

Sophos Cloud Security Platform

Cloud Optix は Sophos Central の一部で、デジタル変革を可能にする単一の直感的なハイブリッドクラウドセキュリティ管理プラットフォームです。受賞歴を誇るソリューションは、導入、管理が簡単で、今日のサイバー攻撃を阻止するのに非常に効果的です。組織がクラウドアクセス、アプリケーション、インフラストラクチャを簡単に保護できるようにします。

業界で最も信頼されている統合クラウド セキュリティ プラットフォーム

| | | | |
|--|--|--|--|
|  <p>安全な接続</p> <p>認証情報を保護し、安全にサービスへアクセス</p> <p>アクセスを保護</p> <p>エンドポイントセキュリティ</p> <p>フィッシング攻撃対策</p> |  <p>ワークロードの保護</p> <p>ハイブリッドクラウドワークロードを検出、クエリ、保護</p> <p>ワークロード保護と EDR</p> <p>クラウドセキュリティポスチャ管理</p> <p>過剰な権限が付与された IAM ロールの検出</p> <p>脅威ハンティング、検出、対応を24時間年中無休で実施</p> |  <p>ネットワークの保護</p> <p>クラウド ネットワーク セキュリティと自動化された脅威対応</p> <p>ファイアウォール、WAF、VPN</p> <p>アプリケーションの可視化</p> <p>セキュリティの自動化</p> |  <p>DEVOPS との統合</p> <p>セキュリティを開発プロセスに組み込む</p> <p>CI/CD 統合</p> <p>コンテナイメージのスキャン</p> <p>脅威インテリジェンス API</p> |
|--|--|--|--|

無料製品デモ、無償評価版

Sophos.com/cloud-optix よりクラウドセキュリティとコンプライアンスの状態を今すぐ評価

ソフォス株式会社営業部
Email: sales@sophos.co.jp