

Sophos Cloud Native Security



クラウド環境、ワークロード、ID を保護

Sophos Cloud Native Security は、Amazon Web Services、Microsoft Azure、Google Cloud Platform 環境、ワークロード、ID 全体に包括的なマルチクラウドセキュリティを提供し、セキュリティリスクを検出して修正し、コンプライアンスを維持します。

さらに強化したセキュリティチーム

単一の統合クラウドセキュリティプラットフォームにより、効率性とインシデント対応時間が向上します。Sophos Cloud Native Security は、ワークロード、クラウド環境、エンタイトルメント管理のすべてのセキュリティツールを統合して、最高の可視性、セキュリティ、コンプライアンス成果を実現します。SIEM、コラボレーション、ワークフロー、DevOps ツールをすべて統合して、組織全体の俊敏性を高めます。

最小限に抑えた検出と対応の時間

強力な XDR (Extended Detection and Response) ツールを使用して、マルウェア、エクスプロイト、構成ミス、異常な動作を特定して阻止します。脅威をハンティングし、優先順位付けされた検出を受け取り、AWS、Azure、および GCP 環境全体で自動的に接続されたセキュリティイベントを利用して、調査と対応時間を最適化します。

サイバーレジリエンスを迅速に実現

サイバー犯罪者は賢くて巧妙です。お客様の組織とクラウド環境は、堅牢で、危険に晒されにくいこと、そして迅速に復旧できる必要があります。ソフォスの包括的で直感的なクラウドセキュリティと修正ツールは、お客様のセキュリティチーム、ソフォスパートナー、または Sophos Managed Threat Response サービスを通じて管理でき、今日のセキュリティインシデントに最適なサイバーレジリエンスを迅速に構築することが可能です。

チームを強化するパートナーシップ

Sophos MTR サービスは、Sophos Cloud Native Security を補完するのに最適です。この MDR サービスは、お客様と連携して、お客様の環境を年中無休で監視し、潜在的な脅威に対応し、感染の痕跡を検索します。いつ、どこで、なにが、どのように、なぜ起きたのかなどのイベントに関する詳細な分析を提供し、高度な脅威がデータやシステムを標的にするのを防ぎます。

統合されたハイブリッドな Cloud Security

ソフォスは、エンドポイント、モバイル、サーバー、ファイアウォール、スイッチ、安全なワイヤレス、メールセキュリティ、安全なアクセスなど、ソフォスのハイブリッドクラウドサイバーセキュリティテクノロジーすべてに対応する統合管理コンソールを使用して Cloud Native Security だけにとどまらないソリューションを提供します。Sophos Central は、製品間のリアルタイムの情報共有、Central の XDR データレイク、統合されたダッシュボードとアラートにより、サイバーセキュリティをより簡単かつ効果的にします。

主な特長

- ▶ AWS、Azure、GCP の環境とワークロードを保護
- ▶ Linux と Windows のクラウドワークロード保護
- ▶ クラウドのセキュリティ状態を管理
- ▶ Kubernetes セキュリティポスチャ管理
- ▶ Infrastructure as Code のセキュリティ
- ▶ クラウドインフラストラクチャエンタイトルメント管理
- ▶ クラウド支出監視

完全なマルチクラウド環境のセキュリティ 可視性、ガバナンス、およびコンプライアンス

マルチクラウド環境の可視化により攻撃対象領域を削減し、セキュリティリスクの検出、修正をし、コンプライアンスを維持します。

- ▶ 単一のコンソールで、AWS、Azure、GCP、Kubernetes、Infrastructure as Code、Docker Hub 環境全体にクラウドセキュリティポスチャ管理ツールを使用することで、効率性を高めます。
- ▶ すべて可視化。アセットのインベントリ、ネットワークの可視化、クラウド支出、および構成リスクを把握できます。
- ▶ コンプライアンス評価を自動化し、監査対応レポートを使用して数週間の労力を削減します。
- ▶ Infrastructure as Code とコンテナイメージのセキュリティにより、DevOps の速度を維持しながらリスクを軽減します。
- ▶ リスク評価と色分けされた警告により、リソースに優先順位を付けられるので安心です。

Cloud のワークロードとデータを保護

エージェントを使用した Windows 保護 および Linux 保護 (Linux は、軽量な API での保護もあります) により、ホストおよびコンテナワークロードを保護します。

- ▶ すべてを保護。クラウド、データセンター、ホスト、コンテナ、Windows、または Linux。
- ▶ カーネルモジュールを導入せずに、実行時に Linux の高度なセキュリティインシデントを特定します。
- ▶ Windows ホストとリモートワーカーをランサムウェア、エクスペloit、未知の脅威から保護します。
- ▶ アプリケーションの制御、構成のロックダウン、重要な Windows システムファイルへの変更の監視を行います。
- ▶ XDR により、脅威の調査および対応を合理化し、イベントの優先順位付けと関連付けを行います。

最小限の権限を実行

マルチクラウド環境全体にクラウド インフラストラクチャ エンタイトルメント管理で最小限の権限の実装をソフォスが支援することで、ID が悪用される前に管理します。

- ▶ すべての ID が、それぞれのタスクに必要なアクションのみを実行し、それ以上のアクションは行わないようにします。
- ▶ 複雑な IAM ロールを可視化して、過剰な権限を持つ IAM ロールを迅速に見つけ、防止します。
- ▶ 通常とは異なるユーザーアクセスパターンと場所を特定し、認証情報の悪用や盗難を特定します。
- ▶ Sophos AI を活用し、ユーザーの行動におけるさまざまなリスクの高い異常を関連付けて、侵害を防ぎます。

ネットワークとアプリケーションセキュリティに保護を拡張

Sophos Firewall でネットワークとアプリケーションを保護します。この統合ソリューションは、IPS、ATP、URL フィルタリング、WAF など、複数の最先端のセキュリティテクノロジーを 1つのソリューションに統合します。高可用性と柔軟性の高い SD-WAN と VPN 接続を備え、どこにいても誰とでも接続できます。自動スケーリングに対し、Sophos UTM Firewall は、非常に動的な環境に個別のソリューションを提供します。

サイバーセキュリティの調達を最新化

ソフォスのサイバーセキュリティ製品群は、信頼できるパートナーネットワークであるソフォスと AWS Marketplace より入手できます。これにより、お客様は調達プロセスを最適化するのを支援すると同時に、すでに実施されているクラウドプロバイダーの消費コミットメントにカウントされます。

詳細の確認、または営業担当者にご相談ください

sophos.com/cloud

ソフォス株式会社営業部
Email: sales@sophos.co.jp