クラウドセキュリティ状態の管理ソリューションを活用して、ソフォスは社内のクラウド環境を制御

ソフォスは、世界各地の 3,000名以上の従業員と 40万社の顧客のインフラとデータを保護しています。ソフォスの社内 IT およびセキュリティチームは、組織の日々のセキュリティ業務に、複数のソフォス製品を使用しています。この実環境は、ソフォスに貴重なテスト環境を提供しており、そこで得た洞察を活用して、ソフォスは製品ポートフォリオの継続的な改善と進歩に尽くしています。

ソフォス
アビンドン、英国

業種
情報セキュリティソフトウェア プロバイダ

Web サイト
www.sophos.com/ja-jp/

ユーザー数
3,000以上

ソフォスソリューション
Sophos Cloud Optix

「Sophos Cloud Optix を使用することで、大量の警告による疲弊を大幅に抑制することができます。Sophos Cloud Optix に組み込まれている強力な AI は、データを相関し、本当に意味のある対処が必要なものを表示します。」

Ross McKerchar
CISO, ソフォス

課題

- クラウド環境全体の可視性を確保する
- 大量の警告による疲弊を防ぎ、有効で対処が必要な警告のみを表示する
- クラウドアカウントとクラウドセキュリティを一元管理する
- 導入済みのセキュリティ対策が、想定通りに動作していることを再確認する

ソフォスは、世界各地の 3,000名以上の従業員と 40万社の顧客のインフラとデータを保護しています。ソフォスの社内 IT およびセキュリティチームは、組織の日々のセキュリティ業務に、複数のソフォス製品を使用しています。この実環境は、ソフォスに貴重なテスト環境を提供しており、そこで得た洞察を活用して、ソフォスは製品ポートフォリオの継続的な改善と進歩に尽くしています。

ソフォスは、社内のパブリッククラウド環境全体に対して、これまでにない可視性をどのように実現しているのか？

ソフォスの IT およびサイバーセキュリティチームは、社内のクラウド環境全体の可視性、セキュリティ、コンプライアンスを実現するツールを探していました。ソフォスのクラウド環境は、Amazon Web Services (AWS) の一部である Amazon Elastic Compute Cloud (Amazon EC2)、および Microsoft Azure を使用した、200件以上のパブリッククラウドアカウントで構成されています。ソフォスの CIS Global Operations Manager の Andy Joel とソフォスの Senior Red Team Lead の Dave Davison が主導した評価作業では、複数の製品に対して、概念実証の詳細な評価を実施しました。

評価したツールのなかには、限られたセキュリティ機能しかないクラウド管理ソリューションもありました。また、技術的に優れた単一の管理コンソールがあるものの、一度に数個のアカウントしか処理できない、というように拡張性に欠けているものもありました。「市場に出回っている各種のソリューションを検討する上で明確になるのは、クラウド管理ソリューションにはクラウドセキュリティが含まれていると考える傾向が組織にあるかもしれませんが、まったくそうではない、ということです。簡単な構成チェックを複数追加したからといって、それが、クラウドセキュリティと同等の役割を果たすわけではありません。犯罪者が攻撃に自動化と AI を使用している今日の動的な環境では、ネットワークトラフィックやユーザーアクティビティのログを分析して、潜在的な侵害をプロアクティブに通知する、高度なソリューションが必要となります。ソフォスでは、それを Cloud Optix に見いだしました。」と Davison は述べています。

評価チームは、すべての要件を本当に満たすことのできるソリューションは、Sophos Cloud Optix 唯一であるという結論に達しました。ソフォスでは、製品チームが開発目的でクラウドアカウントを頻繁に新規作成しており、システムの状況は急速に移り変わり、変化します。Joel にとって、このツールは最大の懸念の 1つに対処します。つまり、このような非常に流動的な運用環境全体を可視化し、安全性を確保することです。

直感的で使いやすい一括管理ハブを使用することで、非常に動的なソフォスのクラウド環境の全容を把握できます。ハブには、トラフィックフローも表示する、クラウドアーキテクチャを視覚化したダッシュボード、警告の概要と詳細、およびコンプライアンス状態などが表示されます。

「Sophos Cloud Optix は、クラウド環境全体にわたって、これまでにない最高レベルの可視性を提供してくれます。これは、他のクラウド管理ツールのほとんどで提供される可視性をはるかに超えます」と説明します。Sophos Cloud Optix は、すべてのクラウド環境にある組織のアセットを自動的に検出します。ネットワークトポロジの視覚化とアセットの継続的な監視により、セキュリティチームはセキュリティリスクに迅速に対応して修復することができます。

Sophos Cloud Optix は、どのようにしてセキュリティプロセスを改善しつつ、既存の対策に対する安心感を与えてくれるのか？

Sophos Cloud Optix の活用の例として、ソフォスでは、社内ポリシーに反して多要素認証が有効化されていないユーザーアカウントが数個発見されました。このポリシー違反は、多要素認証を有効化するプロセスがソフォスで実行されていたにもかかわらず発生しました。Sophos Cloud Optix のおかげで、プロセスが想定通りにうまく動作していないことが判明し、それに応じて調整されました。

「環境で何が起きているかを完全かつ継続的に把握できていない場合、疑わしい、悪意のある、またはコンプライアンス違反の可能性のあるアクティビティを把握することはできません。Sophos Cloud Optix は、すべてを把握し、すべてを保護し、適切なアクションを取るために役立てることができます」と Joel は述べています。

Sophos Cloud Optix の導入によって明らかになったもう 1つの事実は、Sophos Central 管理プラットフォームの運用環境のアカウントも含めて、クラウド環境全体で優先度の高い警告の数が少なく、深刻度の高い警告がゼロである、ということです。Joel は次のように指摘しています。「これは運用環境を設計し、構築した人の実績の真の証です。Sophos Cloud Optix は、適切な場所に適切な制御が揃っており、それが想定通りに機能しているという自信と安心感を与えてくれます。」

Sophos Cloud Optix の警告機能が、競合テクノロジーの中で際立っている点は何ですか？

Davison はまた、セキュリティチームに数千件もの警告を送信する競合製品とは異なり、Sophos Cloud Optix は、AI を活用して監視、検出、セキュリティ分析を実行していると指摘しています。この結果、正確かつ実用的で、優先順位付けされた相関性のある「スマート警告」が生成されます。コンテキスト情報を活用した警告の自動ランキングにより、ソフォスチームは、セキュリティリスクをより迅速に修復できます。大量の警告による疲弊を防ぎ、最も関連性の高い警告にセキュリティチームが集中できるようになります。

「警告は多ければ多いほどよいと、お客様を説得しようとするベンダーもありますが、実際はそうではありません。何百件という優先度の低い警告から重要なものを探し当てるのは理想ではありません。この点においても、Sophos Cloud Optix の機能は非常に的を得ていると思います。重大な警告は、管理者が対処したいものである傾向があります。」と Davison は述べています。

警告や修復を自由に設定できる柔軟性は、ソフォスのような組織にとって大きな利点です。ソフォスには、それぞれに独自のセキュリティ要件がある、さまざまなグループがあり、それによってクラウドワークロードが構成されています。たとえば、同じ警告でも、一部のアカウントでは「重要」に分類され、別のアカウントでは「中」に分類される場合があります。

ソフォスの CISO の Ross McKerchar は、この点についてさらに詳しく説明しています。「Sophos Cloud Optix を使用することで、大量の警告による疲弊を大幅に抑制することができます。他のソリューションは、警告の数で勝負しようとし、優先度に関わらず、セキュリティチームに大量の警告を送信します。Sophos Cloud Optix に組み込まれている強力な AI は、データを相関し、本当に意味のある、対処が必要なものを表示します。これにより、セキュリティの状態とリスクレベルを非常に正確に把握できるため、自動化されたプロセスを通じて、警告に優先順位を付け、プロアクティブに修復することが可能になります。正に、セキュリティ担当者が、セキュリティ担当者向けに構築したセキュリティ製品です。たとえ自社製品でなかったとしても、このテクノロジーを使用していると思います。」

絶えず変化するクラウド環境において、Sophos Cloud Optix は継続的なコンプライアンスの維持にどのように役立つのか？

Sophos Cloud Optix が満たしているソフォスの 3つ目の要件は、コンプライアンスです。すぐに使用できるテンプレート、自動化、カスタムポリシー、コラボレーションツールを使用して、標準的な外部コンプライアンス規制と内部ガバナンスの両方に対応し、組織のすべてのクラウドアカウントで一貫したベストプラクティスを実現します。クラウドでワークロードを作成する際、どのコンプライアンスプロセスが該当し、それをどのように実装すべきかを判断することは、多くの場合、容易ではありません。Davison の率いるチームは、近い将来、Sophos Cloud Optix を活用して、パブリッククラウド環境におけるガバナンス、リスク、コンプライアンスのコストと複雑さを軽減することを期待しています。

SOPHOS

「犯罪者が攻撃に自動化と AI を使用している今日の動的な環境では、ネットワークトラフィックやユーザーアクティビティのログを分析して、潜在的な侵害をプロアクティブに通知する、高度なソリューションが必要となります。」

Dave Davison
Senior Red Team Lead
ソフォス

Sophos Cloud Optix の全機能を無料でお試しいただけます。
www.sophos.com/ja-jp/cloud-optix