SOPHOS

パブリッククラウドの保護：7つのベストプラクティス

ソフォスホワイトペーパー 2019年 6月

目次

パブリッククラウドの保護：7つのベストプラクティス

パブリッククラウドにあるアプリケーションを保護することで、達成しようとしている目標は何でしょうか。

データ流出を起こし、ニュースに大きく取り上げられてしまうことを避けることでしょうか？それとも、適切なレベルの保護を提供するために、自社のクラウドインフラのフットプリントを把握することでしょうか？または、コンプライアンスの監査に問題なくパスすることかもしれません。もしくは、サイロ化しているコンプライアンス部門と開発部門の連携を強化して、セキュリティやコンプライアンスに関する問題を解決することかもしれません。

目標が何であろうとも、このガイドをお役に立てていただけるはずです。ここでは、パブリッククラウドの保護において最も重要な 7つのステップについて説明しており、ベストプラクティスとしてすべての企業が実践できることです。このガイドには、サイバー犯罪者がクラウドベースのインスタンスを攻撃対象にする頻度に関して、SophosLabs が実施した脅威解析の結果も含まれています。また、Sophos Cloud Optix を使用して、企業がどのようにセキュリティと可視性に対応しているかについても説明します。

Amazon Web Services (AWS)、Microsoft Azure または Google Cloud Platform (GCP) で新しいインスタンスをスピンアップすることは簡単です。運営 / セキュリティ / 開発 / コンプライアンス部門にとって難しい点は、このような環境でデータ、ワークロードおよびアーキテクチャの変更を追跡記録し、セキュリティを万全にすることです。

パブリック クラウド ベンダーは、クラウド環境のセキュリティ (データセンターの物理的なセキュリティ、および顧客環境とデータの隔離) に対して責任がある一方、クラウドにアップロードするワークロードとデータの安全を確保する責任は、すべて利用者側にあります。オンプレミスのネットワーク上のデータを利用者が保護する必要があるのと同じように、クラウド環境も保護する必要があります。この責任の分担を誤解している例はよくあり、その結果、クラウドベースのワークロードに発生するセキュリティギャップは、最新技術に精通している今日のハッカーの新たな攻撃対象になっています。

クラウドセキュリティの難題を解決

パブリッククラウドはシンプルでコスト効果が高いため、より多くの企業が Amazon Web Services、Microsoft Azure、Google Cloud Platform などに依存しているのは驚くべきことではありません。新しいインスタンスはわずか数分でスピンアップでき、必要に応じてリソースのスケールアップ / ダウンが可能なだけでなく、使用した分だけに利用料を払い、導入時に高価なハードウェア費用を払う必要もありません。

パブリッククラウドの使用によって従来の IT リソースへの負担が緩和される一方、新たな問題が引き起こされます。クラウド環境で効果的なサイバーセキュリティ対策を実施する秘訣は、企業全体のセキュリティ体制を強化することです。アーキテクチャの適切な保護と構成、およびアーキテクチャの可視化、特にアーキテクチャにアクセスしているユーザーの可視化を実現することが重要です。

これは一見簡単なことのように見えますが、実際は難しいことです。

クラウドの使用が急激に増えたことにより、データはあちこちに分散し、ワークロードは多種多様なインスタンス (企業によってはプラットフォーム) に存在するようになりました。企業は平均で、2種類のパブリッククラウドでアプリケーションを実行しており、さらにテスト環境での使用数は平均 1.8種類です[1]。このマルチクラウドアプローチは、プラットフォームからプラットフォームにジャンプしてクラウドベースの管理サイトの全体像を把握が必要なITチームに可視性の課題を与えます。

クラウドベースのワークロードにおける可視性の欠如は、セキュリティとコンプライアンスの両方のリスクにつながります。

露出の増加

製品とサービスにおけるスピード、市場参入への時間の改善は、企業がパブリッククラウドに移行を考える大きな動機となります。その際には、通常 DevOps (開発・運用) アプローチのスピードと応答性が求められます。ほとんどのケースでは、開発と製品リリースに対するこの新しいアプローチでは、異なるタイムゾーンで複数のプラットフォーム間で作業をする何人かの開発者を必要とします。

ワークロードの追跡記録は、開発サイクルが数か月または数年続いた時はそれほど問題ではありませんでしたが、そのような時代は終わりました。今日では、複数のリリースに （時には同じ日に） 対応する必要があります。激しい変化のあるアーキテクチャの変更、構成の更新、およびセキュリティグループの設定を24時間追跡し続けることはほぼ不可能です。これらは、脆弱性が即座に悪用されるサイバー脅威への露出を増加させる原因となります。

データ、知的財産、サービスに対する脅威

パブリッククラウドが提供する自動化のメリットを享受するのは、企業もサイバー犯罪者も同様です。クラウド環境を訪問する攻撃者は次第に増え、ネイティブ クラウド プロバイダー API を利用して、新しいインスタンスの展開を自動化し、オープンデータベースを侵害し、セキュリティの設定を変更することで正当なユーザーをロックアウトします。

問題を数値化するために、最近 SophosLabs は世界で最も人気のある10のAWSデータセンターに環境を設定しました。そして、解析により次の事柄がわかりました。

- ログインを試行した10人の攻撃者全員が、2時間以内に苦戦したということです。[2]
- 各デバイスでは1分あたり平均13回、1時間あたりでは757回のログインが試行されました。

これらの驚くべき結果は、サイバー犯罪者が自動化された高度な手法を使用して、クラウドベースのインスタンスを標的にしている頻度を浮き彫りしています。
セキュリティ部門の課題は、攻撃をされる前に潜在的な脆弱性を特定して保護することで、奇妙な動作（攻撃者）をリアルタイムで特定し、攻撃を即座に阻止します。

コンプライアンス基準の維持

インフラやデータが保持されている場所に関係なく、CIS、HIPA、GDPR、PCIなど関連のある法令の遵守、またはリスク規制違反を明示する必要があります。

クラウドにおける課題は、日、時間、分ごとで環境が変化することです。オンプレミスネットワークの時には有効だった週や月ごとのコンプライアンスチェックは、パブリッククラウドでは有効ではありません。コンプライアンスの継続的な分析が必要になることで、クラウド環境を手動、またはネイティブツールで管理するチームにとって膨大なリソースを使うことになるでしょう。さらに、コンプライアンスの問題が特定された場合、ほとんどの企業で、セキュリティ / 開発 / 運営 / コンプライアンス部門の役割が分裂する性質により、タイムリーに状況に対処することがしばしば困難になります。

パブリッククラウドの保護の 7 つのステップ

ステップ 1：お客様の責任について

当然のようですが、クラウドではセキュリティの扱いが少し異なります。Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform などのパブリック クラウド プロバイダーは、責任共有モデルを採用しています。つまり、プロバイダーがクラウドのセキュリティに対して責任があると同時に、ユーザー側もクラウドに保存したものに対して責任があります。

データセンターでの物理的な保護、顧客データおよび環境の仮想的分離などの対応についてはすべて、パブリック クラウド プロバイダーが責任を持ちます。

環境にアクセスするための基本的なファイアウォールルールの管理についてはユーザー側で行います。しかし、適切なルールを設定しない場合（例えば、ユーザーがポートをすべて開放したままの場合）は、お客様の責任となります。ですから、ユーザー側のセキュリティの責任について学習することは大切となります。

図1 で責任共有モデルの概要を説明 – もしくはビデオをご覧になりたい場合は、こちらからどうぞ。

セキュリティの責任共有モデル	オンプレミス	パブリッククラウド	理由
ユーザー	■	■	認証の実施、アクセスの制限、認証情報の使用状況追跡
データ	■	■	コンプライアンス基準を満たしつつ、データの損失を防ぎ、誰がどのデータにアクセスできるか権限を定義・適用
アプリケーション	■	■	ポリシー、パッチ、セキュリティの適用によりアプリケーションの感染を保護
ネットワーク制御	■	■/□	ネットワークのアクセス権の追跡と適用
ホストのインフラ	■	■/□	OS、ストレージソリューション、その関連システムの管理とセキュリティ対策を実施することで、未修正のセキュリティホールや権限昇格を防止
物理的セキュリティ	■	□	システムへの物理アクセスの制限と、冗長性の設計により、単一障害点 (SPOF) を防止

■ 顧客　□ プラットフォームプロバイダ

図 1. ソフォスがまとめた責任共有モデルの見解です。各クラウドプロバイダーの詳しいバージョンについては、sophos.com/public-cloudをご覧ください。

ステップ 2：マルチクラウドの計画

マルチクラウドは、もはや単なる「望ましい機能」ではありません。むしろ、必須の機能となっています。マルチクラウドを使用する理由としては、可用性、スピードの向上、機能性など色々とあります。セキュリティ戦略を計画する際（現時点でなければいつか将来）は、マルチクラウドを実行するという前提で開始してください。これにより、長く使い続けることができます。

個別のシステムとコンソールにおいて、マルチクラウドプロバイダー全体のセキュリティ、監視、コンプライアンスをどのように管理するか考えてください。管理が容易であればあるほど、インシデントレスポンスの時間の短縮、脅威検出の増加、そしてコンプライアンス監査の悩みを軽減させます。大切な社員の保持につながることは言うまでもありません。

単一のSaaSコンソール内で、複数のクラウドプロバイダー環境を監視できるエージェントレス ソリューションを探すことで、複数のクラウドアカウントと複数の地域でセキュリティを管理するために必要なツール、時間、および人員の削減につながります。

ステップ 3：すべて可視化

目に見えなければ保護できない。そのため、正しいセキュリティ態勢において大きなバリアとなるのは、インフラを正確に可視化することです。

ホスト、ネットワーク、ユーザーアカウント、ストレージサービス、コンテナ、サーバーレス機能を含むすべてのインベントリの詳細表示を使用して、ネットワークトポロジーとトラフィックフローのリアルタイムな可視化を提供するツールを活用してください。

可視性を高めるために、アーキテクチャ内にある潜在的な脆弱性を特定するツールを使用することで、侵害される可能性のあるポイントを防御することができます。

潜在的な危険のあるエリアは以下：

- 攻撃者がアクセスする可能性のあるパブリックインターネットに対して開放されたポートを持つデータベース
- パブリック Amazon S3 (Simple Storage Services)
- 疑わしいユーザーログインおよびAPIコール – 同時に同じアカウントで何度もログインをしたり、同じ日に世界中のさまざまな場所からログインをするユーザーなど

ステップ 4：日々のプロセスにコンプライアンスを統合

クラウドにワークロードを移行すると、通常の開発リリースを伴うことが多く、より分散したネットワーク全体にコンプライアンス規制を満たすという課題が生じます。コンプライアンスを確保するには、クラウドフットプリントの正確なインベントリーレポートとネットワーク図を作成し、動的な環境においてコンプライアンスチェックリストが合っているか確認する必要があります。

監査の期限に間に合うように、企業は収益性の高いビジネスプロジェクトからリソースを流用するという短期的な修正に頼りがちです。しかし、これは長期的には持続可能ではなく、日々のスナップショットがすぐに古くなるよう、ISO 27001、HIPAA、GDPRなどの標準に必要である継続的なコンプライアンスモニタリングを提供しません。

ネットワークトポロジーのリアルタイムのスナップショットを提供することと、リアルタイムでクラウド環境への変更を自動検出することで、人的リソースを追加せずにコンプライアンスの準拠を向上させるソリューションを探します。また、セクターや業種の特定のニーズを合わせてポリシーをカスタマイズするオプションが必要となります。

もちろん、レポートすることはコンプライアンスの一面にすぎません。コンプライアンスの失敗にも対処できる必要があります。効果的なコラボレーションチャネル不足のため、運用、開発、コンプライアンスにおいて適切な人材を連係させることが難しいということが課題になっています。

コンプライアンスの失敗に対処するプロセスをスムーズに実行するためには、完了するまでの問題を作成、割り当て、追跡するために使用するアラート情報など、既存のチケットソリューションを統合するという方法を見つけ、重要なタスクがリリース中でも失われないようにします。

ステップ 5：セキュリティコントロールの自動化

プロセスの自動化が可能なことは、DevOps (開発・運用) にとって喜ばしいことです。ただし、チームがテンプレートやスクリプトのインフラの自動化導入を享受する間、開発時間を節約できるので、どのセキュリティコントロールを自動化するか検討する必要もあります。

DevOps (開発・運用)の協力体制において、セキュリティは責任を共有し、エンドツーエンドで統合されます。この考え方により、DevOpsイニシアチブに強いセキュリティ基盤を構築する必要性を強調する「DevSecOps (開発・セキュリティ・運用)」という用語が生み出されました。

サイバー犯罪者は自動化攻撃を活用する傾向が強くなってきたので、セキュリティの自動化は必須となります。たとえば、盗まれたユーザーアカウント情報を使用して、暗号ジャック、アカウント設定の変更、検出を回避するために正当なユーザーを無効化にするなどのアクティビティに対して、インスタンスのプロビジョニングを自動化します。実際、パスワード、セキュリティグループの設定、およびコードの脆弱性に対するクラウド環境の調査は今や一般的です。

パブリッククラウド環境で攻撃が成功する2つの主な理由は、アーキテクチャの構成が安全でないこと、脅威対応が攻撃者のペースに追いついていないことです。セキュリティコントールの自動化は、これらの問題に対処するための鍵となります。

パブリッククラウド環境のセキュリティの安全性を確保するには、以下のことが可能なソリューションを探してください。

- **ユーザーアクセスの脆弱性およびリソースの自動修復**
  （ポート上のソースからの侵入を利用したもの）
- **疑わしいコンソールのログインイベントおよび API コールの検出**
  （共有または盗まれたユーザーアカウント情報が攻撃者によって使用されているもの）
- **送信トラフィックにある異常を通報**して、クリプトジャッキングやデータの抽出などのアクティビティを組織に警告
- **非表示のアプリケーションワークロードを表示**して、ホストコンピューターのインスタンスの動作から隠された露出ポイント（データベースなど）を強調表示する

ステップ 6：すべての環境を保護 (Dev、QAを含む)

ニュースで取り上げられるパブリック クラウド データ流出は、組織の運用クラウド環境 （顧客が使用するもの） を攻撃する傾向がある一方、攻撃者はコンピュータを立ち上げた後（開発およびQA環境が立ち上がった後）にクリプトジャッキングなどのアクティビティに対して攻撃して来る可能性があります。

すべての環境 （運用、開発、およびQA）を反応的に先を見越して保護するソリューションが必要です。ソリューションは、ファイアウォールで望ましくないポートが開放している場合のようなすでに発生した問題を特定するためにアクティビティログ（VPC Flowログや CloudTrailログなど）を取り込めるようにすることです。同時に、先を見越して GitHu bなどのリポジトリから IaC （Infrastructure-as-Code） テンプレートをスキャンし、Jenkinsなどの CI / CD パイプラインツールと統合できる必要があります。これにより、コードに導入された脆弱性がサーバーに公開されるずっと前に検出され、不快なニュースの見出しに載ることを防ぎます。

ステップ 7：オンプレミスのセキュリティラーニングの適用

パブリック クラウド ガイドでは奇妙に聞こえるかもしれませんが、これは、長年にわたるオンプレミスでのセキュリティの経験と研究の結果によるものです。感染やデータ損失からクラウドベースのサーバーを保護する場合には、従来のインフラに対して既に何をしているかを考え、クラウドにそれを適応させることを始めてください。

- 次世代型ファイアウォール：クラウドゲートウェイに WAF（Web Application Firewall）を設置することにより、初期の段階でクラウドベースのサーバーに脅威が侵入しないようにします。また、サーバー/ VDIを保護するために、IPS（コンプライアンスに役立つ）およびアウトバウンド コンテンツ コントロールを含めることも検討してください。
- サーバープロテクション：クラウドベースのサーバーでも物理的なサーバーと同じように効果のあるサイバーセキュリティ対策を実行してください。
- エンドポイントの保護：ネットワークがクラウドにある場合でも、ノートパソコンやその他のデバイスは物理的に地上にとどまります。クラウドアカウントからユーザーアカウント情報を盗むのに必要なのはフィッシングメールとスパイウェアだけです。エンドポイントとメールのセキュリティをデバイス上で最新の状態に保つことで、クラウドアカウントへの不正アクセスを防ぎます。

Sophos Cloud Optix の提案

すべて可視化、すべて保護

可視性は、すべてのパブリック クラウド セキュリティポリシーとアクティビティが構築される基盤となります。Sophos Cloud Optix は Amazon Web Services (AWS) アカウント、 Microsoft Azure サブスクリプション、Google Cloud Platform (GCP) プロジェクト、 Kubernetes クラスタ および 開発コードリポジトリ などの複数のクラウドプロバイダー環境の管理を容易にします。この優れた可視性は、コンプライアンスと DevSecOps （開発・セキュリティ・運用）） ポリシーの制御と警告を階層化しており、チームが自信を持ってクラウドセキュリティ戦略の制御、構築を可能にします。

Cloud Optix は、ネイティブ パブリック クラウド プロバイダー APIを統合するエージェントレスの Saas型サービスです。ホスト、ネットワーク、ユーザーアカウント、ストレージサービス、コンテナ、サーバーレス機能などのインベントリの詳細やリアルタイムにネットワークを可視化するトポロジーを含んだアーキテクチャの全体像を構築します。

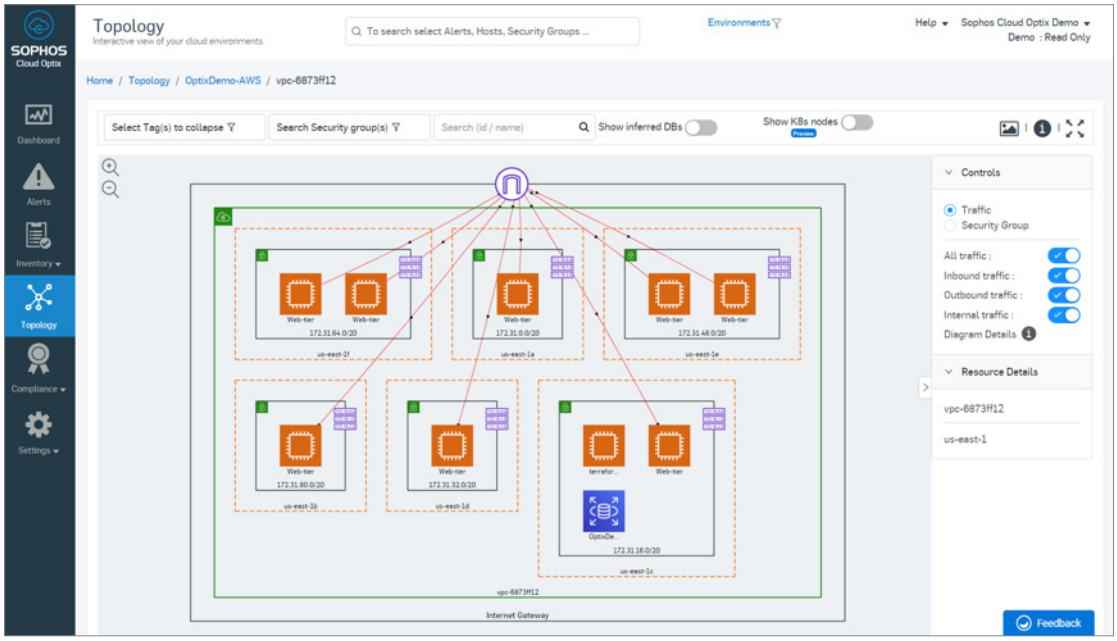

図 2. Sophos Cloud Optix のネットワークトポロジの可視化でAWS環境内の入力、出力、内部トラフィックを表示している図

コンフィグレーションを単にチェックする以上のもの

Cloud Optixは、機械学習のAI技術を使用して、ネットワーク、リソースの構成、ユーザーのログインイベントおよび APIコール、コンプライアンスの状態、IaC（Infrastructure-as-Code) リポジトリなどを監視しながら、ネットワークの設定で誤ってもしくは悪意的に変更されたものを自動的に修正するガードレールとしてプラットフォーム全体における異変とセキュリティの脆弱性をチェックします。

コンテキストアラートはセキュリティとコンプライアンスの問題の根本的な原因を特定する間、ユーザーは、問題内容の説明、復旧手順および影響を受けたリソースを使用してセキュリティの更新が必要な最も重要な領域に専念できます。

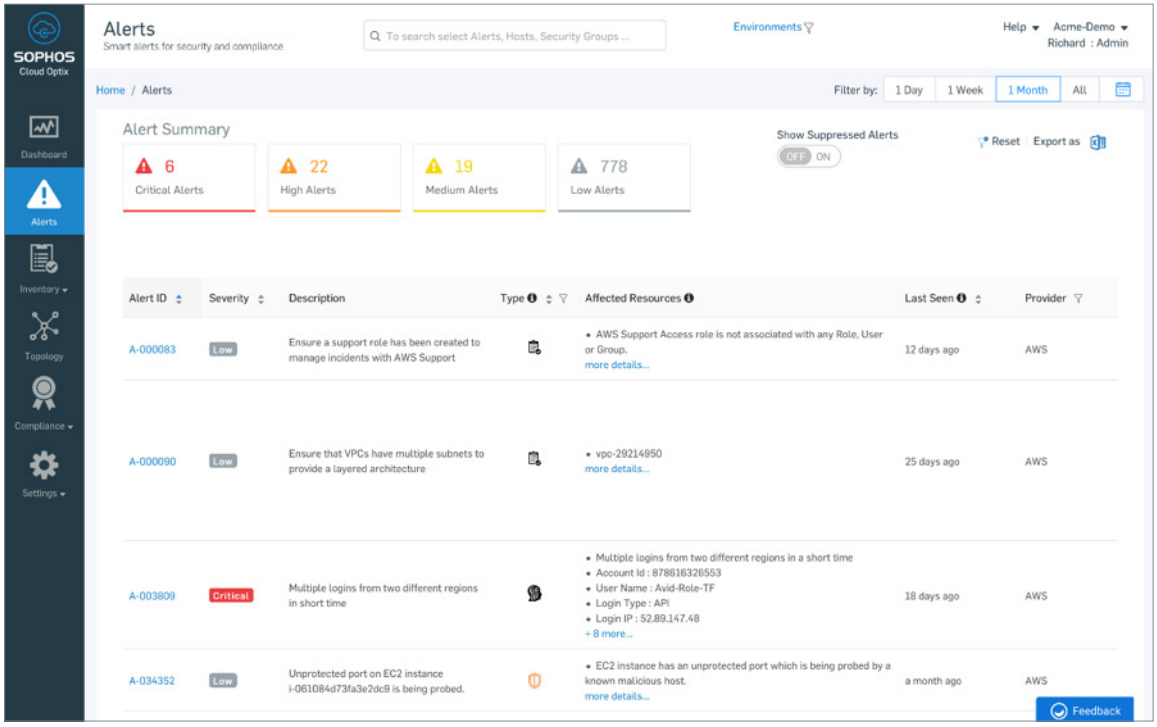

図 3. 同時に異なる地域から複数のアカウントでログインされたという重大レベルのアラートを示す図

それぞれのやり方で監視と対処

Cloud Optix は Rest API を提供し、Splunk、PagerDuty、および Amazon GuardDuty を統合して、必要な時にリアルタイムアラート情報を提供します。Jira および ServiceNow に組み込まれた統合のおかげで、アラート情報を使用してはチケット作成し、リリース中でさえも決して大事なタスクを失わないように保護しながら、それを完了まで追跡できる。

オンデマンドレポート上に一目でわかるダッシュボードでまとめられているので、クラウドセキュリティの状態の管理で数時間から数日の時間を節約できるでしょう。これにより、パブリッククラウドの保護において最も重要な７つのステップを達成しやすくなります。

詳細はこちら

Sophos Cloud Optix は、パブリッククラウドを使用中または移行を考えている企業にとって理想的なソリューションです。AIと自動化テクノロジーを組み合わせることにより、セキュリティおよび危険にさらされたままになりうるコンプライアンスの脆弱性を検出、対処、防止するために必要な継続的な可視性を企業に提供します。

Sophos Cloud Optix の詳細およびクラウド環境で購入義務を伴わない30日間無償評価版を始める場合、または今すぐにオンラインでもをお試しになる場合は www.sophos.com/cloud-optixをご覧ください。

まとめ

従来のワークロードからクラウドベースのワークロードの移行は、さまざまな規模の企業に大きな機会を与えます。ただし、サイバー攻撃からインフラや企業を守る場合は、パブリッククラウドの保護は必須となります。このガイドの７つのステップに従うことで、管理とコンプライアンスのレポートをシンプル化しながらも、パブリッククラウドのセキュリティを最大限に高められます。

責任の共同負担モデル：ソフォスを活用した対策

	オンプレミス	パブリッククラウド	理由	ソフォス製品の機能
ユーザー	■	■	認証の実施、アクセスの制限、認証情報の使用状況追跡	XG FirewallおよびSophos UTM ： シングルサインオン (SSO) および 2段階認証 (2FA) を使用したイン/アウトバウンド認証を実行し、アクセスに関する詳細になレポートを提供します。Sophos Cloud Optix は、アカウント認証情報の共有または不正使用を追跡します。
データ	■	■	コンプライアンス基準を満たしつつ、データの損失を防ぎ、誰がどのデータにアクセスできるか権限を定義・適用	Sophos Cloud Optix は、クラウド環境におけるコンプライアンスの自動化、ガバナンス、セキュリティ監視を実現。Sophos SafeGuard は、データ流出防止機能、Sophos Mobile は、データ保護とアクセス許可の設定します。
アプリケーション	■	■	ポリシー、パッチ、セキュリティの適用によりアプリケーションの感染を保護	XG FirewallとSophos UTM - IPS (侵入防止システム)、Sophos Server Protection - HIPS とロックダウン機能は、アプリケーションへの攻撃や意図しないアプリケーションの開示に対し防御します。
ネットワーク制御	■	◪	ネットワークのアクセス権の追跡と適用	XG Firewall および Sophos UTM は、使いやすいインターフェース、強力なパケットインスペクションであり、Synchronized Security (XG のみ) は ネットワークアクセスのセキュリティ対策と管理、ネットワークの権限を強化します。
ホストのインフラ	■	◪	OS、ストレージソリューション、関連システムの管理とセキュリティ対策を実施し、未修正セキュリティホールや権限昇格を防止	Sophos Intercept Xは、さまざまなエクスプロイトの手法を検知し、ゼロデイ脅威から防御します。Sophos Server Protection は、ロックダウン機能でランタイム制限を実行し、Sophos XG Sandstorm は、未知のコードの拡散を防止します。
物理的セキュリティ	■	■	システムへの物理アクセスの制限と、冗長性の設計により、単一障害点 (SPOF) を防止	XG Firewall と Sophos UTM は、物理アプライアンスおよびクラウドプラットフォームの両方に、HA 構成導入オプションがある。

■ 顧客　■ プラットフォームプロバイダ

図 4. ソフォスが クラウドの共有負担モデルをどのように支援しているかについての図

Sophos Cloud Optix は、リアルタイム管理、AWS環境に対する高度な可視化、および必要な設定のコンプライアンス状態をチームに知らせます。これにより、以前は単一ビューでは不可能だったレベルの監視と警告が可能になります。Sophos Cloud Optix の使用で、インフラアクティビティの全体像を把握でき、包括的な保護に専念できるようになりました。

Ryan Stinson
Manager of Security Engineering
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report from Flexera

2 自動化攻撃のデータソース：真相：クラウドハニーポットによるサイバー攻撃、Matt Boddy、ソフォス、2019年 4月

Sophos Cloud Optix をお試しください

www.sophos.com/ja-jp/cloud-optix

ソフォス株式会社営業部
Email: sales@sophos.co.jp

19-06-19 WP-JA (RP)

SOPHOS