sysdig

クラウドセキュリティ入門

CSPM、CIEM、CWPP、CNAPP
に関する基礎知識

目次

今日の現実を見据えたクラウドセキュリティ

IT環境がオンプレミスのデータセンターに限定されていた頃は、出入り口が1つだけの自己完結型の要塞であったため、セキュリティ運用は今よりずっとシンプルなものでした。しかし、最近では、ビジネスに不可欠なアプリケーションやデータをクラウドに移行する企業が増えており、サイバー犯罪者もすでにクラウドを通じて積極的に活動しているため、脅威を検知することは、古代の要塞を守ることではなく、ディズニーランドを守ることに似ています。遊園地のように、クラウド技術に基づく分散型のインフラストラクチャーは、多くのアトラクション、多様な消費者、無数のインタラクション、さまざまな入口と出口で構成されています。しかし、そこには、SecDevOps、DevOps、およびクラウドセキュリティオペレーションチームにとって、楽しいことは何一つありません。実際、そのような環境には、悪意あるアクターにとっての多くの誘惑と多くのリスクが存在しているため、それは高度にインテリジェントなセキュリティ技術と絶え間ない警戒を必要とする環境なのです。

企業の各事業部はすでに、顧客の要求に対応し、ビジネス目標を達成することで手一杯です。その一方で、脅威アクターの種類は多岐にわたっているため、企業規模や業種にかかわらず、あらゆる企業のシステムが標的にされることは避けられません。

唯一確かなことは、ある日突然、クラウドスタックの奥に潜む安全でない設定が大惨事を引き起こしたり、新たな脆弱性を悪用する新しいタイプの脅威が出現したりすることです。それは避けられないことです。では、クラウドセキュリティとは実現可能なものなのでしょうか、それともそれは単に絵に描いた餅にすぎないのでしょうか？

クラウドにおける責任共有モデル

クラウドセキュリティの計画を立案するための最初のステップは、責任共有モデルを理解することです。主要なパブリッククラウド（AWS、Azure、GCPなど）は、共有セキュリティの概念を用いて、クラウドプロバイダーが管理するセキュリティリスクと、顧客による対処が期待されるセキュリティリスクとを区別しています。

このモデルでは、クラウドプロバイダーは、VMインスタンスやストレージバケットをホスティングしている物理サーバーの保護などのように、いくつかのセキュアな側面を自らの担当業務として管理する責任があります。また、システムの定期的な監査も行います。その一方で、エンドユーザーがクラウド上に配置するリソースのセキュリティ確保は、そのほとんどがエンドユーザーの負担となります。クラウドプロバイダーは、最低限、ユーザーがアップロードするデータが、ユーザー自身のコンプライアンスフレームワークで義務付けられているアクセス制御により保護されていること、そしてユーザーがクラウドVMインスタンス上で動作するOSを確実に保護することを期待しています。.

クラウドプロバイダーの提供するセキュリティツールは十分ではない

この文書の目的は、クラウドサービスプロバイダーやプロバイダーが提供するツール（これらは、どちらも企業環境において大きな付加価値をもたらすものです）の持つセキュリティギャップを強調することではありません。むしろ、本文書は、クラウドプロバイダーにとってセキュリティは付加的なものであり、二次的な優先事項であることを読者に認識してもらうことを目的としています。クラウドプロバイダーは、クラウドコンピューティング、ネットワーク、ストレージなどのサービスを提供することに主眼を置いており、セキュリティに主眼を置いているわけではありません。

貴社がクラウドの導入を始めたばかりで、IaaSやSaaSのサービスを2つほどしか稼働させていない場合を想像してみてください。パブリッククラウドプロバイダーが提供するツールを使って、セキュリティポリシーを簡単に導入できるようになり、不審な動作があればプロバイダーは貴社のチームにアラートを発行します。そのようなプロバイダーの例としては、AWS Security Hub、AWS GuardDuty、Azure Security Center、Azure Defender、Google Security Command Centerなどが挙げられます。しかし、クラウドプロバイダー経由で利用するサービスの数が増えると、セキュリティを強化する必要性がより明らかに（そして緊急に）なり、その結果、これらのツールだけではクラウド環境を保護するのに十分でないと気付く可能性が高くなります。詳細な比較については、巻末の付録をご覧ください。

もう1つ注意点があります。クラウドサービスプロバイダー（CSP）が提供するセキュリティツールは、ベンダーロックインの大きな要因となります。なぜなら、ユーザーがCSPの提供するツールを使って自らのセキュリティ制御をカスタマイズしている場合、ユーザーはそのCSPを利用せざるを得なくなるからです。マルチクラウドの領域に移行すると、ユーザーは、すべてのクラウドに対応し、かつギャップを埋めるようなソリューションが必要となります。クラウドプロバイダーは、そのようなソリューションをカバーできませんし、また今後もカバーしようとはしないでしょう。

クラウドセキュリティソリューションの主要カテゴリー：CSPM、CIEM、CWPP

貴社のチームが、クラウドのセキュリティについて十分に理解していないとしても、それは貴社だけではありません。Gartner®によると、「組織の50%が、クラウドネイティブのDevSecOpsにおけるセキュリティについて社内の知識が不足していると回答している」とのことです[1]。そして、このような状況は、新しい用語、カテゴリー、および技術が日々表面化している中で起きているのです。しかし、新しいバズワードがどれだけ登場しようとも、クラウドセキュリティには、知っておくべき3つの確立されたカテゴリーが存在しています。すなわち、CSPM、CIEM、およびCWPPです。

CSPMとは？

CSPMとは、導入されたアカウントとリソースがセキュリティのベストプラクティスから逸脱した場合を検知する一連の制御機能のことです。CSPM制御の一部であるさまざまな標準を利用することで、ユーザーは、すべてのクラウドアカウントとワークロードを継続的に評価し、クラウドドリフトやプラットフォームの設定ミスの領域を迅速に特定できるようになります。また、CSPMは、組織のセキュリティポスチャーを改善したり維持する方法について、実行可能で規範的なガイダンスを提供します。

クラウドセキュリティポスチャー管理（CSPM）ツールとは、クラウド制御プレーンの保護（設定ミスの監視）、クラウドリソースの追跡、クラウドテナントの設定検証といったセキュリティ関連のユースケースを統合するものです。これらのツールは、安全でない設定を特定することでクラウドセキュリティを強化します。これにより、ギャップに対処してよりセキュアなアーキテクチャーを設計できるようになります。CSPMソリューションの中には、修復やその他の拡張機能を提供するものもありますが、ほとんどの企業や組織では、CSPMをコンプライアンス目的と監査にのみ利用しています。

「2025年までに、クラウド侵害の99%以上の根本原因が、エンドユーザーによる予防可能な設定ミスや誤りとなることでしょう。」[2]

[1] Gartner, “Emerging Technologies: Future of Cloud-Native Security Operations,” Mark Wah, Charlie Winckless, 17 November 2021.

[2] Gartner, “Hype Cycle™ for Cloud Security, 2021,” Tom Croll, Jay Heiser, 27 July 2021

CSPMツールは、クラウドの設定がベストプラクティスに合致していることを確認します。これにより、クラウドチームは、すぐに利用できるフレームワークコントロールとベンチマークをマッピングした上で、次のようなことに対処する時間を短縮できます。

- インターネットに直接さらされているデータストレージ
- データベースにおける暗号化の欠如
- 重要なシステムアカウントにおける有効な多要素認証の欠如

CSPMツールは、違反が発生した際にチームに通知することで、チームが対応策を講じ、修正の優先順位付けを行えるようにします。

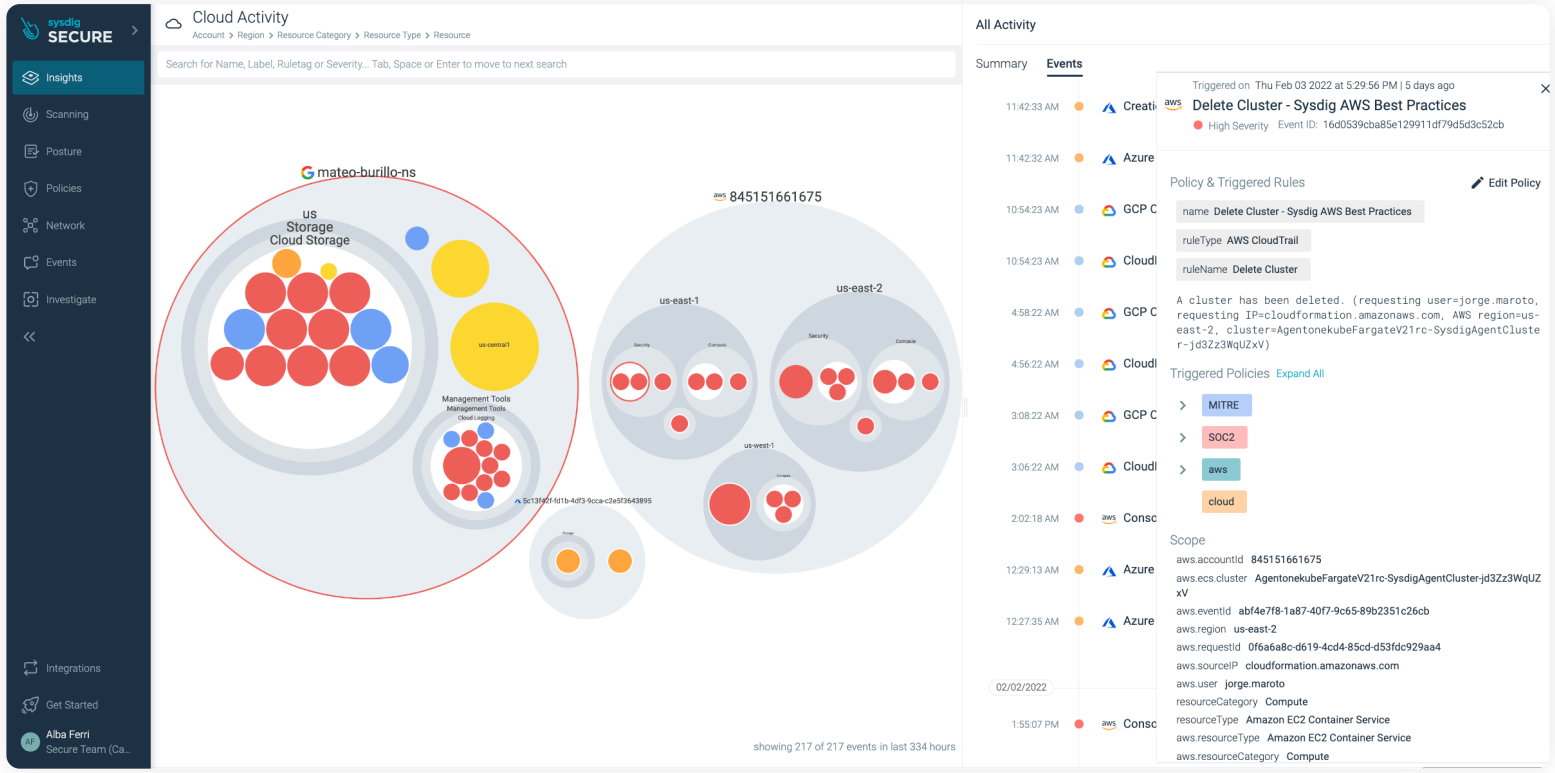

図1：SysdigのInsightsダッシュボードには、複数のクラウドとワークロードにまたがるリスクに関する単一ビューが表示されます。

CIEMとは？

クラウドリソースに過剰な権限やエンタイトルメントを付与することは、最もよくある設定ミスの1つです。クラウドIDは（人間用であれマシン用であれ）爆発的に増加しており、最小権限の原則を実装することは、動的なクラウド環境では非常に複雑になっています。さらに、クラウドプロバイダーがサービスや機能を追加し続ける中、最小権限の設定がどうなっているかを正確に把握することはますます困難になっています。

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（CIEM）ツールは、過剰な権限を与えられたアカウントやロール、未使用の権限、および未使用のアカウントを検知することにより、この問題に対処します。CIEMを使用すると、どの人間IDおよびマシンIDがどのリソースにアクセスできるかを知るだけでなく、日常的に使用している権限も知ることができます。この知識を活用することで、ユーザーは、最小権限アクセスを強制するようにポリシーを変更できます。

あるプロジェクトの一員であるユーザーグループがあるとします。これらのユーザーは、リポジトリへのイメージのアップロード、クラウドインスタンスでのコンテナの実行、およびいくつかのオートスケーリングアクションを担当します。これらのユーザーは、管理者の持つすべての権限を持つ必要はありません。そのようなアプローチが最も構成しやすいものだとしても、それを行うべきではありません。ユーザーはVPCを削除することがあるでしょうか？いいえ、それはユーザーのタスクではありません。CIEMツールを使って過剰な権限を排除することは、クレデンシャル窃取の被害を軽減するための重要なステップとなります。

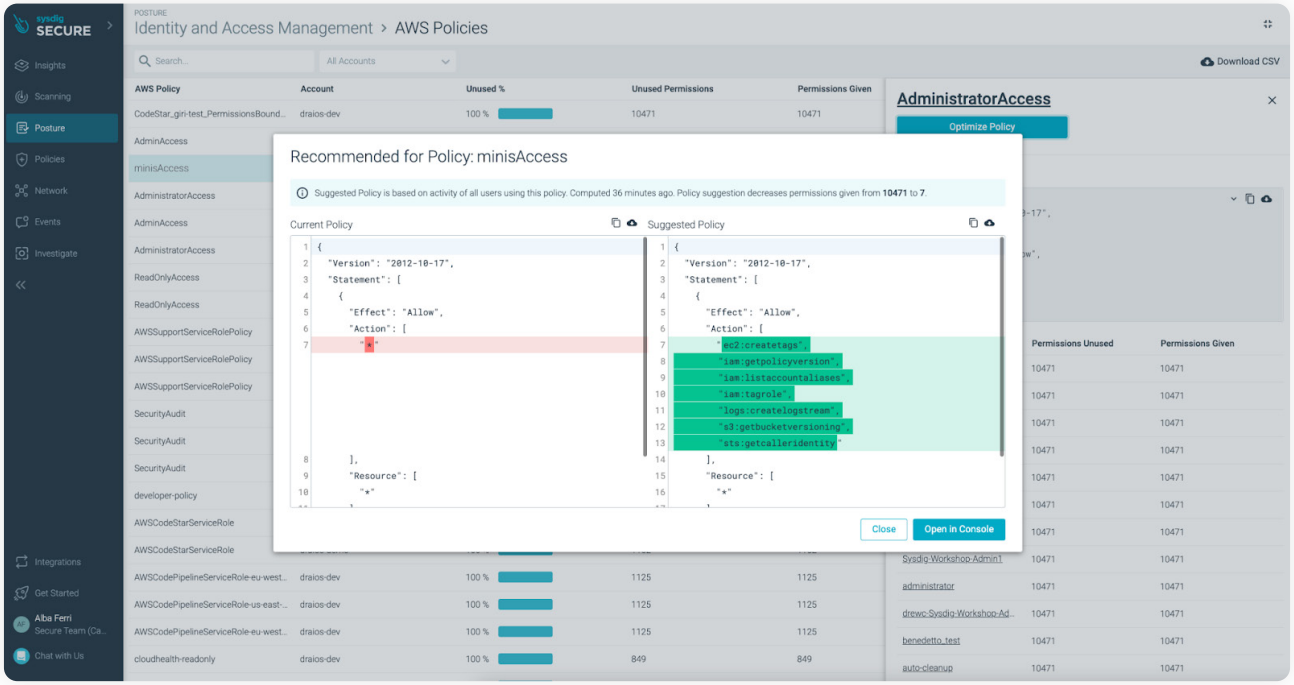

図2： CIEMダッシュボードは、最小権限を強制するためのポリシーを提案する。

CWPPとは？

クラウドワークロード保護プラットフォーム（CWPP）ツールは、ワークロードを保護します。このツールは特に、アプリケーションライフサイクル全体の保護に重点を置き、AWS、Google Cloud Platform（GCP）、Microsoft Azure、およびその他のクラウドベンダーのプラットフォーム上のインスタンスを保護するような、クラウドベースのセキュリティソリューションを提供します。CWPPソリューションは、次のような特定のユースケース向けに構築されています。

- ランタイム検知：アプリケーションの不審な振る舞いをランタイムに検知します。また、脅威への対応を自動化します。
- システムのセキュリティ強化：潜在的な攻撃ベクターを排除し、システムのアタックサーフェスを縮小することで、セキュリティリスクを軽減します。
- 脆弱性管理：OSおよび非OSに関する既知の脆弱性を検知し、システムがあらゆる規制要件に準拠した状態を維持していることを保証します。
- ネットワークセキュリティ：コンテナやKubernetes内のネットワークトラフィックを視覚化し、Kubernetesネイティブのネットワークセグメンテーションを実施します。
- コンプライアンス：本番環境のワークロードが規制基準に準拠していることを保証します。
- インシデント対応：フォレンジックから得られる貴重な証拠を使ってセキュリティインシデントに対応することで、侵害を封じ込めます。

CNAPP：単なる頭字語ではない

クラウドネイティブアプリケーションの進化に伴い、より多くの可動部分が登場するのは避けられません。ありがたいことに、業界ではクラウドネイティブ技術と共に、モジュール式のアプローチを採用しています。これにより、既存のCI/CDパイプラインやランタイムプラットフォームを、より優れた手法が発見されるたびに拡張および更新できるようになります。

このようなモジュール方式の欠点は、複雑さです。合理的なレベルのセキュリティポリシーと施行を実現するために、アプリケーションライフサイクルに何を導入すればよいかを把握するのは非常に困難な仕事です。そこで登場するのが、**クラウドネイティブアプリケーション保護プラットフォーム**（CNAPP）です。CNAPPを活用することで、ユーザーは、自社環境のあらゆる側面における、詳細かつ多層的なエージェントベースおよびエージェントレスのカバレッジを実現できます。これには、ワークロードのプロアクティブな検証から、実行中のパブリッククラウドプラットフォームにおけるポリシー監査に至るまで、あらゆるものが含まれます。

CNAPPとは？

CNAPPとは、CSPMやCWPPに分類されるユースケースをカバーする包括的なセキュリティカテゴリーです。Gartnerは次のように述べています。

「クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）は、CWPP-CSPMコンバージェンス以上のものを提供します。CNAPPには2つの重要な原動力があります。1つ目は、CWPPベンダーがワークロードのコンテキストを提供するためのポスチャーに注目していることです。2つ目は、ワークロードへの「ドリルダウン」を行いつつ、より多くの可視性を提供することがCSPMの課題となっていることです。CNAPPは、CSPMとCWPPを統合してその両方を提供し、さらに付加的なクラウドセキュリティ機能によりそれらを補強できる可能性があります。」[3]

CNAPPがもたらす副次的なメリットとして、顧客とベンダーが、クラウドセキュリティスイートのもたらす価値を容易に確認できることが挙げられます。これは、苦労して統合する必要がある一連のポイントソリューションとは対照的です。

CNAPPは、開発から本番環境、そして開発に戻るまでのフェーズにおいて、5つのコア機能をカプセル化しています。これらは次の通りです。

- 開発アーティファクトのスキャン
- クラウドセキュリティポスチャー管理（CSPM）
- IaC（Infrastructure as Code)のスキャン
- クラウドインフラストラクチャーエンタイトルメント管理（CIEM）
- ランタイムのクラウドワークロード保護プラットフォーム（CWPP）

CNAPPは、クラウドネイティブアプリケーションのライフサイクルをエンドツーエンドでカバーすることを可能にするフィードバックループを提供します。

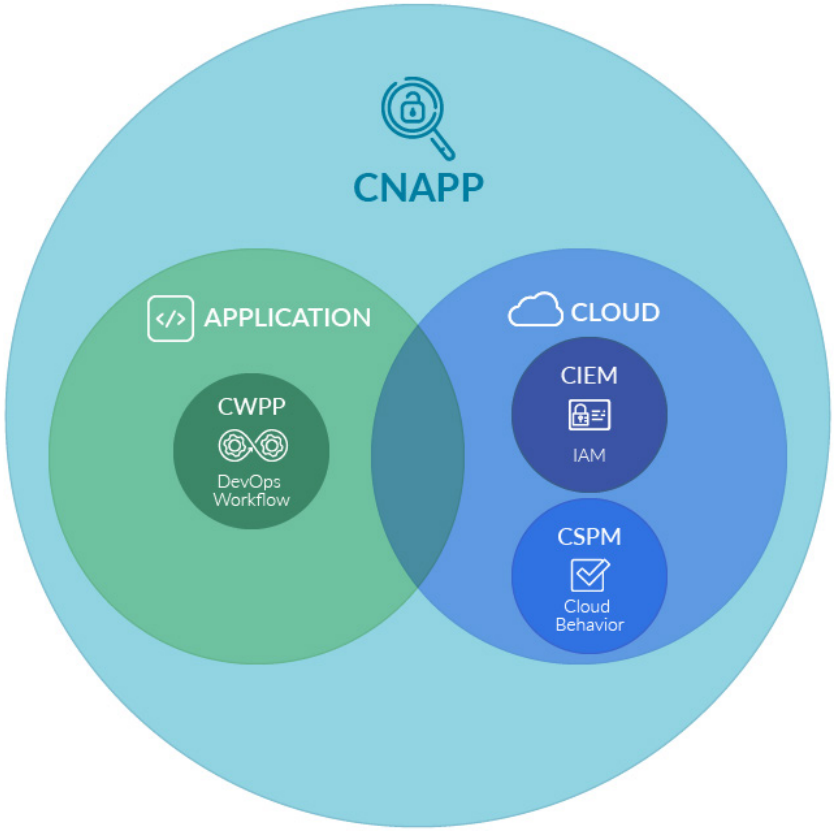

図3：主なクラウドセキュリティソリューション製品カテゴリー間の関係

[3] Gartner, Inc., How to Protect Your Clouds with CSPM, CWPP, CNAPP, and CASB, 2021, Richard Bartley, 6 May 2021

CNAPPによる包括的なカバレッジの実現

CNAPPを導入することで、ユーザーはクラウドネイティブなアプリケーションスタック全体の可視性と制御性を劇的に向上させることができます。CNAPP以外の代替案は、ポイントソリューションの寄せ集めとなります。それは、関連付けるために膨大な時間と労力を必要とするにもかかわらず、すべての領域がカバーされているかどうかの確証は依然として得られません。

CNAPPを使用すれば、包括的なカバレッジを実現できます。さらに、高い品質のCNAPPソリューションを使うと、さまざまなユースケースからのインサイトの相互関係を明らかにし、SecDevOps、DevOps、およびクラウドセキュリティ運用チーム間のコラボレーションを促進できます。CNAPPは、クラウド環境に関するリアルタイムの知識を提供すること、そして共通のワークフロー、データの相互関連付け、有意義なインサイト、および是正措置を取り入れることに関して、イコライザーとなりえます。

CNAPPを実装することで、クラウドネイティブなアプリケーションスタックのすべての主要な側面において、より高いレベルのセキュリティを実現できます。また、開発プロセスの初期段階から本番環境に至るまで、CNAPPセキュリティを組み込むことで、提供されるものが最高レベルのセキュリティと整合性を維持することを保証できます。

クラウドセキュリティソリューションを評価する際に考慮すべき5つのポイント

CSPが提供するセキュリティツールは、さまざまな機能を備えています。しかし、これらのツールのほとんどは、自社のクラウド環境に特化したものとなっています。特に多くの企業が行っているように、ハイブリッドやマルチクラウドのアーキテクチャーを使用している場合、すべてを統合するには、クラウドエンジニアやセキュリティエンジニア側で多くの作業を行う必要があります。このような場合、ネイティブのCSPツールではなく、サードパーティのソリューション（CWPPツールまたはCNAPPツール）の導入を検討するとよいでしょう。

サードパーティーソリューションを評価する際に考慮すべき5つのポイントを下記に示します。

その1：包括的な保護を実現するために、エージェントレスおよびエージェントベースのアプローチを選択すること

クラウド向けのセキュリティツールを評価する場合、クラウドプロバイダーから利用するサービス（IaaS、CaaS、PaaS、FaaSなど）により、エージェントレス、エージェントベース、およびその両方を組み合わせたアプローチに出会うことがあります。エージェントレス型のアプローチは簡単であり、最小限の管理オーバーヘッドで済み、パフォーマンスのオーバーヘッドもほとんどなく、エージェントを処理できないシステムにも対応できます。一方、エージェントベースのアプローチは、より深い可視性を提供し、より包括的なコンテキストとリアルタイムの検知を容易にすることで、より迅速なインシデント対応、封じ込め、および調査を可能にします。しかし、エージェントの管理はより困難であり、かつ時間がかかります。

ソフトウェアエージェントは、その欠点にもかかわらず、今後何年にもわたってクラウドにおいて重要な役割を果たすと思われます。エージェントレス型のセキュリティ方式は、APIベースで統一されたクラウド制御プレーンに容易にアクセスすることでて多くの種類の問題を特定し、迅速かつ容易なオンボーディングを可能にしますが、それはエージェントベースとエージェントレスの両方の技術を含む多層的な防御戦略の一部である必要があります。そうでなければ、可視性とソリューションの適用範囲にギャップが生じることになります。

エージェントレス型のアプローチは、チームが利用しているクラウドサービスのリストアップや、ソフトウェアの既知の脆弱性を特定するのに有効です。また、ログに基づいて脅威を検知することも可能です。一方、エージェントベースのアプローチでは、ランタイムの脅威、マルウェア、高度な持続的脅威をリアルタイムに検知できます。脅威を検知した後、エージェントが提供する詳細な活動記録とコンテキストは、インシデント対応、封じ込め、フォレンジック調査にとって不可欠となります。セキュリティリスクを効果的に管理するためには、両方のアプローチを使用する必要があります。

その2：構成と権限のリスクを管理

クラウド資産に対する完全な可視性を確保し、マルチクラウド環境における設定ミスとドリフトを特定します。最小権限の原則を導入することで、人間およびマシンのユーザーロールにおける過剰な権限を検知して削除します。すべてのアイデンティティとアクセス管理の役割とその権限設定を自動的に検知するだけでなく、過剰な権限を持つロールを検知し、適切な権限設定を推奨することができるようなツールを探してみてください。

その3：監査ログを通じたクラウドセキュリティ監視の実現

クラウドセキュリティ監視は、広大で多層的なクラウド環境における潜在的なセキュリティ脅威を追跡するための最初の重要なステップとなるものです。監査ログは、クラウド環境内のアクションを、そのアクションが行われた際に体系的に記録します。これにより、誰が何をしたか、いつ何が起こったか、そして何が変わったかを知ることができます。誰かがユーザーを作成したり、パーミッションを変更したり、新しいインスタンスを起動したりすると、これらのログを通じて、当該イベントが追跡されることになります。

主要なパブリッククラウドプロバイダーはすべて、監査ログを有効にし、ユーザーによるログの追跡に役立つネイティブサービスを提供しています。例としては、AWS CloudTrail、Cloud Audit Logs in GCP、Azureの監査ログなどが挙げられます。クラウド環境で起きていることはほとんどすべて、クラウド監査ログで追跡され、記録されます。これらの監査ログを分析することで、予期せぬ振る舞い、設定変更、侵入、データ窃取などを検知できます。しかし、これらのサービスは通常、個々のクラウドアカウントと個々のクラウドに対してのみ機能します。今日の93%の組織のように、複数のクラウドを同時に使用している場合、サードパーティツールが必要となります。サードパーティツールは、さまざまなクラウド環境からクラウド監査ログを集約し、それらを一元的に分析することで、あらゆるパブリッククラウド環境の監査データから疑わしいパターンを検知できます。

Falco、監査をさらに進化させる

ストリーム検知とは、動いているデータを収集し、分析し、レポートする連続的なプロセスです。その考えに基づいて、オープンソースコミュニティはFalcoと呼ばれるソリューションを提供しています。.

Falcoをクラウドの監査ログに接続することで、パーミッションやサービスのアクセス権に対する予期せぬ変更や、侵入者の存在やデータの流出を示すような異常な行動を特定できるようになります。脅威検知のためにログを外部リポジトリに送信する必要がないため、帯域幅の減少やストレージコストの上昇を招くこともありません。

その4：ランタイム検知と応答の実装

早期の「侵害の痕跡」に関して迅速に対処すること。ランタイムの脅威は現実的であり、巧妙さを増しています。攻撃者は、検知を回避するために複雑な攻撃を仕掛け、システムへの感染を通じて最大の利益を得ようとしています。リアルタイムのシグナルを見逃さないようにしましょう。イベントに関する詳細な可視性を確保することで、クラウド、コンテナ、Kubernetesにおける不審な振る舞いや悪意あるアクティビティを検知します。また、インシデントの発生後にコンテナが消失した場合に備えて、詳細なフォレンジック証拠を収集できるようにします。

その5：MITRE ATT&CKフレームワークへのマッピング

主要なクラウドサービスプロバイダーは、自社のコンピュートサービスや環境を強固にするためのネイティブセキュリティツールを提供していますが、これらのサービスはそれぞれ微妙に異なっています。そのため、クラウドセキュリティについて語る際には、共通の言語が必要となります。統一されたセキュリティフレームワークを採用することで、セキュリティエンジニアはクラウドの侵害を管理しやすくなり、脅威モデルや方法論の基礎を提供できます。

MITRE ATT&CKフレームワークとは、主要な脅威を分類した包括的な知識ベースであり、これを使うことでサイバーセキュリティチームは自らのインフラストラクチャーを強化できます。また、同フレームワークは、高度な脅威アクターが攻撃に使用するすべての戦術、手法、手順（TTP）の分析も提供します。MITRE ATT&CKフレームワークは、脅威モデルや方法論の基礎となるものです。また、同フレームワークは、サイバーセキュリティチームやリスクチームが確立されたベストプラクティスに従うよう導くため、ユーザーはあらゆるコンプライアンス標準に関して競争相手の先を行くことが可能となります。

クラウド用のMITRE ATT&CKは、高度な脅威アクターがクラウド環境に対する攻撃で使用する可能性のある特定のTTPをマッピングしています。

Sysdigによるコンテナとクラウドの統合セキュリティ

Sysdigは、企業や組織が、コンテナ、Kubernetes、クラウドサービスなどを、自信を持って保護できるようにすることで、クラウドのセキュリティの標準を推進しています。Sysdigプラットフォームは、ビルドの保護、ランタイムの脅威の検知と対応、クラウドの設定、権限、コンプライアンスの継続的な管理を可能にします。Sysdigプラットフォームは、エンドツーエンドのクラウドインフラにおけるセキュリティを実現するための最適なソリューションです。

お客様のクラウドやコンテナ環境で、可視性とセキュリティの価値を実際に体験してください。

Sysdig Secureで始めるコンテナ＆Kubernetesセキュリティをご覧ください

30日間の無料トライアルはこちら

付録

下記の表は、3社の主要パブリッククラウドプロバイダーが提供するセキュリティ機能を比較したものです。

サービス	AWS	Azure	GCP
DevOpsライフサイクル			
CI/CD	AWS CodeBuild, AWS CodeDeploy, AWS CodePipeline	Azure DevOps, Github Enterprise	Cloud Build
プロビジョニングテンプレート	CloudFormation	Azure Resource Manager	Cloud Deployment Manager
サービスカタログ	AWS Service Catalog	Azure Custom Images, Azure API Management	Private Catalog
セキュリティアセスメント	Inspector	Security Center – Resource Security Hygiene	Cloud Security Command Center
サーバーレスコード	Lambda	Azure 機能	クラウド機能
インサイト	Systems Manager	Monitor	Stackdriver Monitoring
検知			
DLP	Macie	Azure Information Protection	Cloud DLP
異常検知	GuardDuty	Stream Analytics	Cloud Dataflow
脆弱性のスキャン	Inspector	Security Center	Scanner

サービス	AWS	Azure	GCP
保護			
DDOS	Shield	DDOS Protection	Preset
MFA	Multi-Factor Auth	Azure MFA	Cloud Identity Aware Proxy
ウェブアプリケーションFW	WAF	Azure WAF, Application Gateway	Cloud Armor
IAM	AWS Identity & Access Management Cognito	Azure AD/IAM	Cloud Identity and Access Management
暗号鍵管理	KMS	Azure Key Vault	Cloud KMS
監査			
ログ管理	CloudTrail	Azure Audit Logs	Cloud Audit Logs
構成管理	Config	Azure Security Control	Cloud Asset Inventory
コンプライアンス	CloudHSM	Azure Trust Center and Key Vault	GCP Security
サービスカタログ	Service Catalog	Managed Applications	Service Catalog
セキュリティ監視			
SIEM	CloudWatch and Amazon GuardDuty	Azure Sentinel and Azure Monitor	Stackdriver Monitoring/ Logging, Chronicle
クラウドコストの最適化	Trusted Advisor	Azure Advisor	Recommender

Sysdigについての詳細は www.sysdig.jp/

Sysdig Japan合同会社
〒107-0052 東京都港区赤坂7-9-4 赤坂Vetoro 3階
https://sysdig.jp/company/contact-us/

www.sysdig.jp