sysdig

チェックリスト

最新のCSPMソリューションに不可欠な5つの機能

チェックリスト：最新のCSPMソリューションに不可欠な5つの機能

クラウドの導入は、顧客に継続的なイノベーションを提供する上で最も重要です。しかし、クラウドネイティブ環境への移行は、企業が十分に認識していないセキュリティやコンプライアンス上の問題を引き起こします。このような問題には、ソフトウェアの脆弱性、過度に寛容なアクセス権限、データ侵害を引き起こす潜在的なクラウドの設定ミスなどが含まれます。さらに、これらの問題には、多額のコンプライアンス費用のリスクが伴うことは注目に値します。セキュリティインシデントが発生した場合、企業は多大な損害を被る可能性があります。

クラウドセキュリティの分野では、このような問題に対処するために、それぞれ異なる角度からアプローチする多種多様なツールが多く採用されてきました。クラウドセキュリティポスチャー管理（CSPM）はその一例です。企業や組織はその規模にかかわらず、自社のクラウドセキュリティおよびコンプライアンス要件に対応できるポスチャー管理ソリューションを求めています。一方、従来のCSPMソリューションは、当初の要求が変化し続けるクラウドセキュリティ環境への対応に苦労している状態です。

従来のCSPMソリューションは、エージェントレス手法を活用することで、簡単な導入とスムーズな統合を実現しています。エージェントレス環境は、使いやすい反面、対応に時間がかかりがちで、時代遅れのセキュリティ情報を提供しがちです。結果として、このような制限により、企業や組織が抱えるクラウドネイティブ環境内のセキュリティスタンスに関する正確な評価が妨げられ、悪意ある活動が覆い隠されることになります。

クラウドにおける攻撃は動きが速く、数分で発生します。Sysdigの『2023年度版クラウド脅威レポート』によると、日和見的な攻撃の場合、公開された認証情報を見つけるまでにかかる時間は平均2分未満、認証情報の発見から攻撃開始までにかかる時間は21分とのことです。

このため、コンテキスト化された情報、スピード、そして対応の優先順位付けに対する要求が非常に高まっています。

現代的なCSPMソリューションは、戦略としてランタイムインサイトを活用しています。これは、静的なチェックをリアルタイム検知で補強し、使用中のコンテキストを使用してより良い優先順位付けを行うものです。これらのインサイトは実用的なデータを提供し、リアルタイムの運用情報を活用することで、クラウドネイティブ環境内で影響度の高い問題を特定できるようにします。意味のある攻撃分析を提供すると主張する従来のCSPMソリューションとは対照的に、現実には定期的なリソーススキャンにより取得した設定ミス、ネットワークエクスポージャー、暴露されたシークレット、脆弱性、または過度に寛容なIDを相互に関連付けると、多くの場合偏った結果がもたらされます。従来のCSPMソリューションが提供できるのは潜在的な攻撃経路だけであり、最新のデジタルエコシステムの効果的な保護に必要な精度とリアルタイムの認識が欠けています。

リアルタイム検知から得られるランタイムインサイトは、ポスチャー管理の観点から最も価値のあるリスク関連のインサイトを提供します。この視点は、環境内における現在の活動を正確に描写し、使用中のデータを通じて、誰が、どこで、何をしたかに関する最新の情報を補足します。これにより、静的なスナップショットと比較して、何が使用されているかに関する最新の情報を通じて、静的なセキュリティ制御に命を吹き込むことが可能となります。その結果、セキュリティチーム、開発チーム、エンジニアリングチームは、予防と防御のユースケースに、より確実性とプロアクティブなマインドセットを持って、効果的に対処できるようになるでしょう。

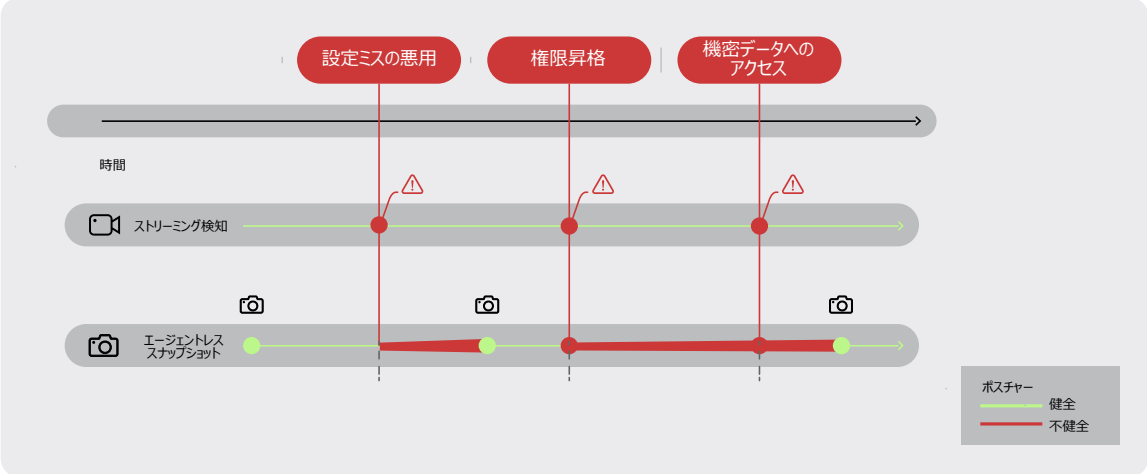

図1：CSPMに対する最新のアプローチ

このようなランタイムインサイトは、配信前のスキャンだけに頼るソリューションとは対照的に、導入されたアプリケーションとシステムに関する可視性を高めます。これは、セキュアな設計とセキュリティテストに対するアプローチでは達成できないものです。エージェントレスとエージェントベースのインスツルメンテーションの両方を備えたハイブリッド導入アプローチを使用するCSPMソリューションは、より多くのユースケースをカバーできるため、それぞれの機能を強化することができます。

プロアクティブなリスク評価と強固な軽減戦略の実施により、エンタープライズクラウドセキュリティアプローチのシームレスな拡張に必要な、CSPMソリューションの主な属性を下記に紹介します。

01
ライブインベントリの データベースを維持する

クラウド化が進むにつれ、ITチームはますます多くのクラウドネイティブサービスを活用するようになるでしょう。クラウドで発生するイノベーションへのシフトに伴い、設定ミスが必ず発生します。設定ミスは、攻撃者に狙われやすく、悪用されやすい「露出の入口」となります。クラウド内のサービスはスピンアップやスピンダウンされるため、セキュリティチームがクラウド環境に実際に何があるのかを常に把握することは困難です。不要な設定変更から企業や組織を安全に保つために、クラウド資産のライブインベントリを保持し、かつそれに対応するセキュリティポスチャーを維持することが最善の方法です。

インベントリデータベースを備えたCSPMソリューションを採用することで、企業や組織は、ランタイムインサイトによる危険なリソースの検索（たとえば、「読み取りアクセスがあり、インターネットに公開されており、PCI標準に違反しているストレージバケットをすべて見つけること」など）が可能になるほか、深刻度の高い設定ミス、コンプライアンス違反、脆弱性にさらされていないかどうかを素早くチェックできるようになります。

- 効果的なCSPMツールは、すべてのクラウド資産のライブインベントリを提供します。これは次の操作により可能となります。
- クラウド環境で稼働しているシステム、アプリケーション、サービス、ワークロードを特定する。そして、それらが安全でコンプライアンスに準拠しているかどうかを判断する。
- アカウント、仮想プライベートクラウド、リージョン、ストレージバケット、リレーショナルデータベースサービスなどのクラウド資産を、対応するInfrastructure-as-Code（IaC）マニフェストへとマッピングする。
- 機密性の高いデータ（たとえば、顧客データやコンプライアンス規制で管理されるデータ）がどこに保存され、処理されているかを把握する。
- 複数のクラウドサービスにまたがるクラウドアクティビティを可視化する。
- メタデータ、設定情報、コンプライアンス違反、ドリフト分析（IaCとランタイムの比較）、脆弱性、脅威イベント、リソース履歴などの機能を含める。

これにより、すべての資産に関するランタイムのインサイトと最新情報が提供され、現在の運用状態のベースラインが確立されます。その結果、セキュリティチームは、最も重大なリスクを抱えるサービスに優先順位を付けた上で、スピーディに修正に着手できるようになります。

02
Infrastructure as Code（IaC）の保護

アプリケーションとサービスの基盤となるインフラストラクチャを強化することは、すべてのセキュリティチームにとって基本です。不要なクラウドサービスや既知の脆弱な設定は、理想的にはIaCやpolicy-as-code型のアプローチを使用して、最初から無効化するべきです。設定を継続的に検証することで、古い設定ミスが再び環境に忍び込まないことを保証できます。

実行時に設定ミスを検知することは、すでにサイバー攻撃にさらされていることを意味します。企業や組織は、IaCアーティファクトの保護などの予防策を適用する必要があります。IaCをスキャンしてセキュリティの設定ミスを検知することで、事後対応的な作業を回避できます。

- → ビルド統合、そしてIaCアーティファクトやファイルの迅速な分析を通じて、DevOpsパイプラインへの統合を実現します。
- → ランタイム修正とIaC修正の両機能を使うことで、すべてのリソースにおける設定や設定ミスを修正するポリシーを容易にかつ柔軟に作成できます。
- → IaC環境とランタイム環境で、セキュリティポリシーを一貫して使用できます。
- → AWS CloudFormation、Terraform、YAMLなどの一般的なフォーマットでIaC修正コードを生成するようなソリューションをいち早く利用できます。

ランタイムインサイトの利用は、IaCセキュリティを1つ上のレベルに引き上げます。CSPMツールがIaCアーティファクトをクラウド環境で実際に実行されているものにマッピングできれば、セキュリティチームはソフトウェアライフサイクルの早い段階で修正する必要があるものを把握できるようになり、その結果、予防と検知のセキュリティ手法の間に好循環を生み出せるようになります。

03
ガバナンスとコンプライアンスのためのフィードバックを即座に提供

ガバナンスとコンプライアンスに関する課題は、CSPMの導入でもよく見られます。DevOpsチームは、ガバナンス・リスク・コンプライアンス（GRC）チームにより設定された標準的なセキュリティ要件を満たすことが期待されています。しかしGRCチームは通常、ネットワークとセキュリティポリシーを理解しておらず、リソース消費に関する懸念の全体像を見逃しています。この結果、運用チームとセキュリティチームにとってガバナンス上の課題が生じます。ポリシー違反に関するフィードバックを即座に提供することで、アタックサーフェスの縮小と修復時間の短縮を実現します。

DevOpsチームのガバナンスとコンプライアンス管理を強化するために、CSPMツールは、次の事項でGRCチームとDevOpsチームのコラボレーションを可能にします。

- 自動化を実現し、手作業によるプロセスを排除する。自動化された修復によってコンプライアンスを強化する。さらに、本番環境における設定ミスをIaCアーティファクトへとマッピングする。
- コンテナ、Kubernetes、クラウド環境全体で、規制コンプライアンス標準（PCI-DSS、GDPR、NIST 800-53、ISO 27001など）を満たすためのコンプライアンスチェックを実施する。
- コンプライアンスに影響を与える可能性のある設定のドリフトがないかどうか、クラウドサービスを継続的に監視する。
- 定期的な評価と詳細なレポートにより、コンプライアンスの進捗状況を測定する。
- 重要なシステムファイルやディレクトリの改竄や、不正な変更を検知するためのファイル整合性監視を導入する。
- クラウドの監査ログとコンテナのフォレンジックデータを使用して、クラウドとコンテナのコンプライアンスを証明する。

単にセキュリティフレームワークに準拠しているだけでは、セキュアであることを意味しません。一貫性のある、再現可能で、セキュアなクラウド環境を確保するためには、DevOpsチームとGRCチームが共同作業を行う必要があり、CSPMソリューションはこのような共同作業をサポートするものでなければなりません。企業や組織は、タイガーチーム*（特定の問題を解決するために召集された専門家チーム）を導入することで、計画された安全な設定からの逸脱や、構築時および配信時に通常発生する環境の変化に対処できます。これは、ポリシー違反について即座にフィードバックを提供するランタイムインサイトを要として達成できるものであり、その結果として、アタックサーフェスを縮小し、修正時間を短縮できます。

04
ポスチャーのドリフトをリアルタイムで捕捉する

変化の速いクラウドネイティブシステムでは、アプリケーションの責任者は、新しいビジネス要件を満たせるよう製品を継続的に適応させるために、アプリケーションとその基盤に変更を加える必要があります。このような変更が発生すると、アプリケーションと基盤の設定を調整する必要も出てくるため、その結果として、システムが要塞化されたポスチャーから逸脱してしまう可能性があります。

CSPMは、設定およびポスチャーのドリフトを回避できるようにするために、下記の機能を提供します。

- → インシデントや侵害につながる悪用可能な状況が発生する前に、リアルタイム検知機能を使ってドリフトを捕捉する。
- → 一貫したセキュリティポリシーを適用することで、クラウドサービスやリソースが組織のセキュリティポスチャーから外れた場合にフラグを立てる。
- → 進化し続けるクラウド環境に後れずについて行きつつ、セキュリティ制御とポリシーの間に徐々に生じる不整合を常に把握する。
- → コンテキスト化された修正を提供し、プルリクエストを生成することで時間を節約する。
- → 「as-code」式のアプローチにより自動化を導入する。
- → ランタイムインサイトにより、設定ミスに関するアラートをリッチ化する。

本番環境におけるポスチャードリフトのような検知上の制御を使用する場合、本番環境で発生するに至った計画外の変更を見つけることができます。設定がセキュアな初期設定からずれた際にセキュリティチームに警告する必要がある場合は、リソースを継続的に監視する必要があります。ランタイムインサイトは、どこで不整合が発生したか、いつ不整合が発生したか、そしてドリフト変更の所有者は誰であるかを判断するために必要なコンテキストを提供します。

05
最小権限アクセスの実施

設定ミスの大半は、従来の基盤設定ではなく、権限やアクセス制御に関連しています。ユーザーは多くのグループに属しており、ユーザーとグループは多くのロールにマッピングされます。使いやすくするためにロールは過度に広く設定されており、その結果、きめ細かで厳密なアクセス制御が犠牲となっています。クラウドのリソースは、非常に多くあります。その一方で、機能の変更、従業員の離職、従業員の職務変更、顧客の減少、テクノロジースタックの変更などの結果として、権限は時間とともに変化します。クラウドサービスの利用が増えるにつれ、こうしたアクセス権や権限の制御と管理は複雑さを増しています。

最小権限の原則は、アクセス制御にとって絶対的に不可欠なものです。したがって、最新のCSPMツールでは、次のことが可能でなければなりません。

- クラウド資産とIDに関する包括的な可視性を確保した上で、過剰な権限を検知して削除する。
- 未使用のIDや過剰な権限をリスクの高いものとしてマークする。これらは、脅威アクターにより侵入口として狙われる可能性があります。
- 不正アクセスのリスクを減らし、データのプライバシーを確保するために、ヒューマンIDとノンヒューマン（マシン）IDの違いを明確に理解する。
- 必要なアクションを実行するための最小権限を与えるようなアクセスポリシーを実施すること。
- ランタイムアクセスパターンを活用することで、最初に修正すべき権限リスクに優先順位を付ける。
- 不審なアクティビティ（権限昇格など）を特定するために、エンタイトルメントや権限の変更を監視し、アラートを発行する。
- PCI、SOC2、FedRAMP、ISO 27001などの標準に対するコンプライアンス要件を満たすために、IDおよびアクセス管理の権限と制御を監査する。

ユーザー情報、ロール、パーミッション、認証メカニズムなどのIDおよびアクセス関連のメタデータを組み込むことにより、システムコールとクラウドのアクティビティを特定のユーザーまたはエンティティへと帰属させる。ランタイムインサイトは、このようなコンテキストに応じた情報を提供することで、監査やコンプライアンスを支援するほか、ユーザーの振る舞いに関連する潜在的なセキュリティ脅威の検知にも役立ちます。

> 実際に修正可能なもの、使用中のもの、悪用可能なものをフィルタリングすることで、軽減策や修正作業に対してより適切に優先順位を付けることができます。これにより、企業や組織に固有の環境やクラウドセキュリティアーキテクチャーの選択に照らして、リスクの高い設定ミスを優先することが可能になります。

まとめ

ランタイムインサイトを通じて次なる飛躍を実現

クラウド環境でセキュリティギャップが発生するのは明らかであり、クラウドセキュリティ戦略には徹底的な精査が必要です。現在導入されているツールが、すべてのクラウド環境に適しているとは限りません。それは特に、クラウドネイティブ環境の場合に顕著です。企業や組織は、ポイントソリューションで発生するような「ずれ」を回避するために、統一された機能やプラットフォームに目を向ける必要があります。

ランタイムインサイトがなければ、攻撃者は死角を突くことができ、長期間検知されないまま、悪意ある活動を妨害されずに実行できます。

クラウドセキュリティプログラムを強化するツールを探す際には、選択したソリューションがランタイムインサイトを備えており、エンドツーエンドの検知を提供することで、企業のクラウド環境を安全に保つものであることを確認してください。適切な CSPM ツールを選択することが、脅威の検出と深刻な損害の発生の分かれ目になります。

ランタイムインサイトの詳細については、https://sysdig.jp/why-runtime-insights/をご覧ください。

PB-029-JA REV. A 2/24