sysdig

チェックリスト

マルチクラウド インフラストラクチャーを 保護するための 5つのステップ

マルチクラウドインフラストラクチャーを保護するための5つのステップ

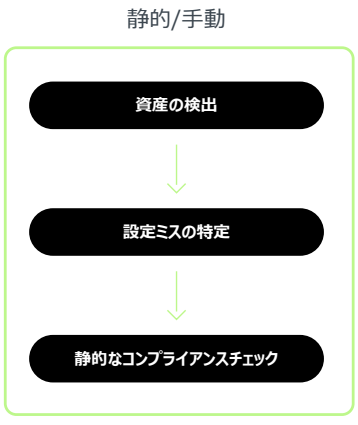
クラウドの導入が加速するにつれ、変化し続ける環境におけるセキュリティリスクを管理する必要性が高まっています。企業や組織は、自社で保護しなければならないクラウドサービスの多さに圧倒されるかもしれません。たった1つのサービスの設定ミスが重大なデータ漏洩につながる可能性もありますが、現実にはヒューマンエラーを避けることは不可能です。セキュリティギャップとリスクを常に把握するためには、自動化が必要となるでしょう。

Gartner®社は、「2025年までに、クラウド侵害の99%以上は、設定ミスが根本的な原因で起こることになる」と予測しています。また、同社では、「2025年までにワークロードの70%がパブリッククラウドでホスティングされるようになり、企業の50%がマルチクラウドを採用するようになる[1]」とも予測しています。

ここで、てっきりプライベートだと思っていたバケットから、何者かがユーザー情報をスクレイピングしていることに気付いたというシナリオを想像してみてください。セキュリティエンジニアが数時間調査したところ、特定のバケットへのパブリックアクセスを許可するような変更が手動で行われていた事を発見したとします。そして、さらに悪いことに、セキュリティエンジニアは、それ以外にも予定外のストレージ設定の変更を多数発見したとします。このような場合、セキュリティエンジニアは、複数の変更のひとつが調査のきっかけとなったことを幸運に思うでしょう。

継続的に行われるクラウドサービスへの追加や変更を追跡するには？マルチクラウド環境全体で、設定ミスや不審なアクティビティにフラグを立てるには？真の脅威を知らせるアラートに焦点を当てるには？ポスチャー管理ポリシーによる定期的なスキャン結果の相互関連付けや、複数のクラウドソースから収集したデータのコンテキスト化は、クラウドを採用しようとしている企業や組織にとって大きなギャップとなっています。これらの課題は、クラウドインフラ管理、権限管理、コンプライアンスニーズに影響を与えます。このようなクラウド特有のセキュリティリスクに対処するには、ランタイムインサイトを使用した可視化が必要です。

次頁から紹介する5つのステップは、企業や組織がクラウドに移行する際に従うべきセキュリティ戦略の設定方法を示すものです。



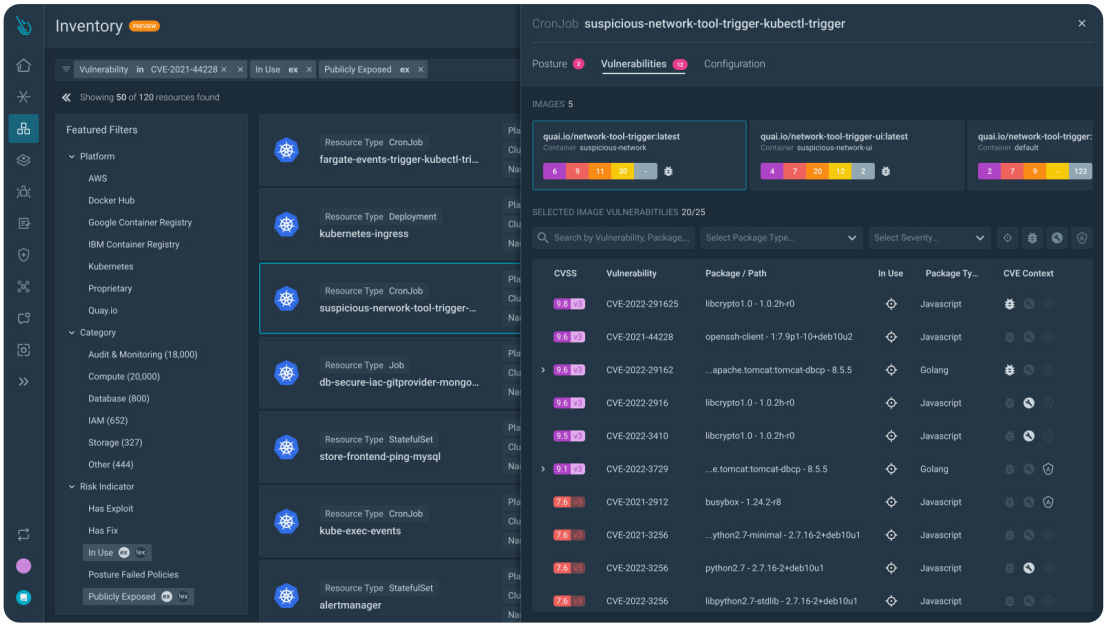
[1] Gartner, Risk-Based Evaluations of Cloud Provider Security, Charlie Winckless, Jay Heiser, 16 January 2023.

STEP 01

クラウド資産の検出

- 利用しているすべての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します。それらが安全でコンプライアンスに適合しているかどうかを判断します。
- アカウント、VPC、リージョン、ストレージバケット、データベースなどのクラウド資産を、対応するIaCマニフェストへとマッピングします。
- 機密データ（顧客データ、コンプライアンス規制で管理されるデータなど）がすべてのクラウド環境のどこに保存されており、処理されているかを把握します。
- 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します。
- クラウド資産を検出するための統一されたビューを提供します。クラウドプロバイダーごとに異なるツールを導入する必要はありません。

絶えず変化する広範なマルチクラウド環境において、強固なセキュリティとコンプライアンスを達成するには、総括的なアプローチが必要となります。これには、企業内あるいは組織内に存在するすべてのクラウド資産の特定とマッピング、機密データのロケーションに関する十分な理解が必要です。複数のプロバイダーにまたがるクラウドアクティビティに関する統一されたビューを利用することで、資産の検出を簡素化できるほか、セキュリティとコンプライアンス基準の遵守を保証できます。このような戦略的アプローチにより、複雑なマルチクラウド環境を正確、かつ自信をもってナビゲートしデータと業務を保護できるようになります。

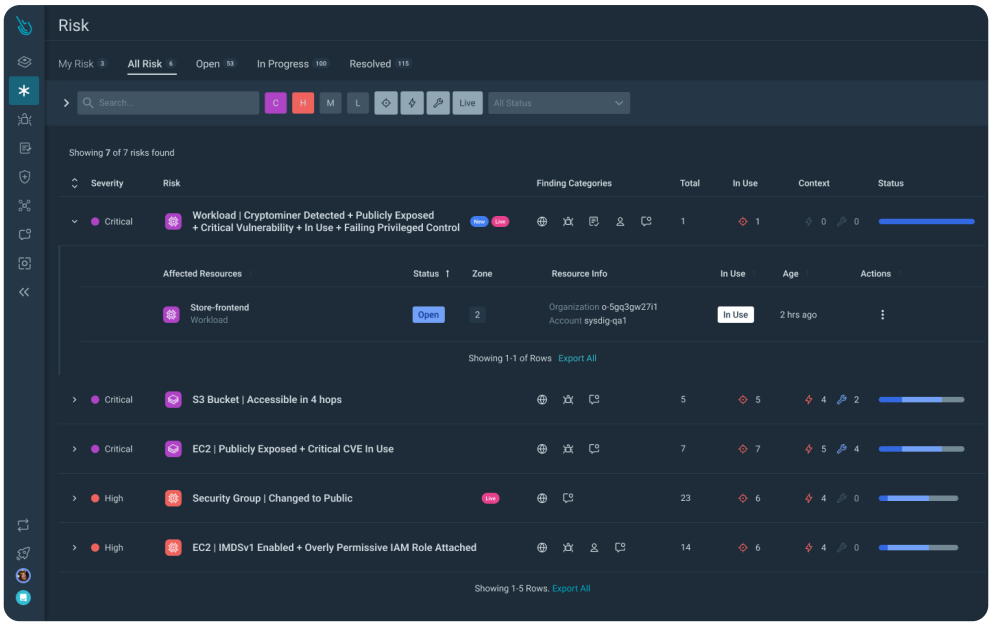


STEP 02

静的な設定リスクの管理（CSPM）

- リスク、不適切なプラクティス、設定ミスを特定し、マルチクラウド環境の現在のセキュリティポスチャーを可視化します。
- 保護されていないデータストレージ、過剰な権限、変更されていないデフォルトの認証情報や設定、無効化されたセキュリティ制御、ポートやサービスへの無制限のアクセス、保護されていないシークレットなどの設定ミスを検知します。
- お使いのクラウドとKubernetesの設定を保持しているGitリポジトリへのプルリクエストを自動的にオープンします。クラウドプロバイダーが提供するコンソールか、またはCLIコマンドを使用してセキュリティポスチャーを強化するための、実装ガイダンス付きの修正手順を取得します。
- クラウドサービスを保護するためのCISベンチマーク、コミュニティが提供するポリシー、またはお客様独自のセキュリティ基準に照らして、お使いのクラウド構成をチェックします。
- クラウドリソースの作成、削除、または変更時に、設定ミスやコンプライアンスポスチャーのドリフトを検知します。

保護されていないデータストレージからチェックされていないアクセス許可に至るまで、リスクをプロアクティブに特定すること（設定ミスを検知してそれに対処すること）は、最も重要な懸念事項です。クラウド設定を業界のベンチマークやカスタマイズされたセキュリティ基準に合わせることで、自社の全体的なセキュリティポスチャーを強化できます。さらに、Gitリポジトリを通じて修正手順を自動化することで、プロセスを合理化し、セキュリティを強化できます。マルチクラウド環境を保護するにあたって、これらのプラクティスを実施することで、総合的にリスクを軽減し、防御を効果的に強化できます。



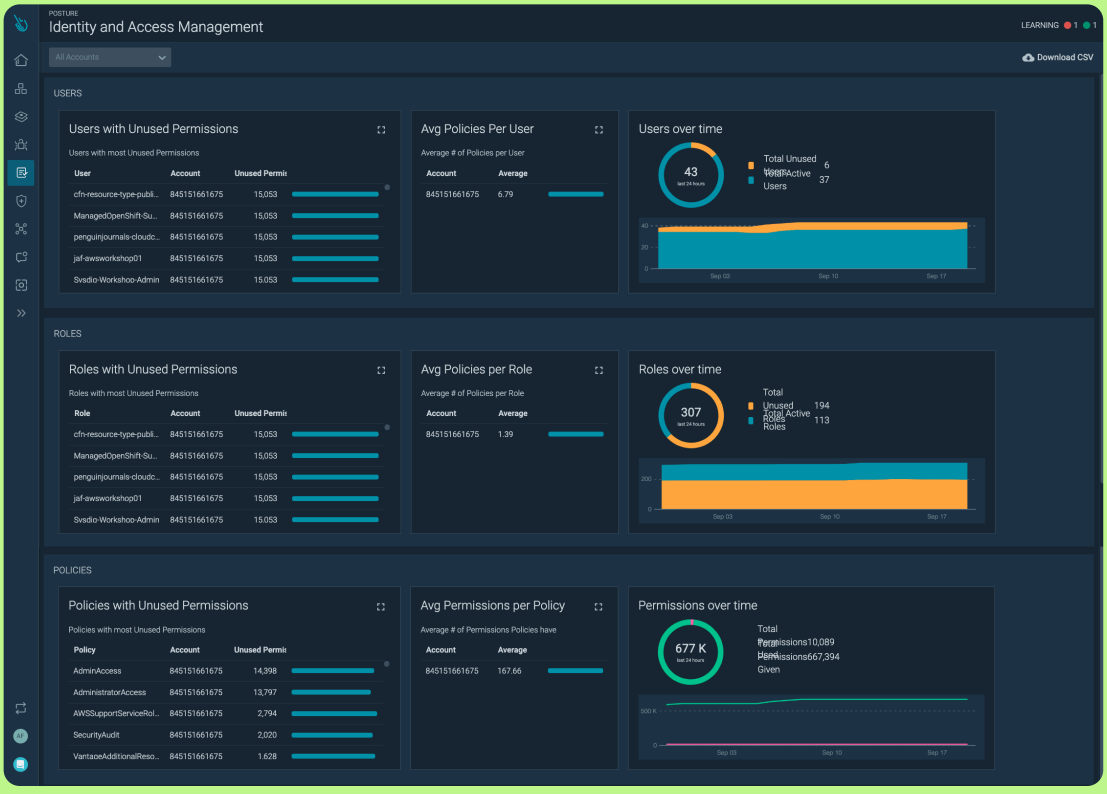
スタックランク式のリストにより、お使いの環境全体における最も懸念されている緊急性の高いリスクが明らかになります。

STEP 03

クラウドの権限リスクを防ぐ（CIEM）

- アクセスレビューに、アクティブおよび非アクティブのユーザー、およびそれらに関連付けられている権限の識別を含めます。
- コアタスクの実行に必要な権限だけを適用します。
- これらの権限を継続的に見直します。
- 主要なリスクをまとめたダッシュボードを使って、IAMセキュリティポスチャーの強化に向けた進捗を追跡します。

アカウントとロールに付与される過剰な権限は、クラウドの設定ミスにおいて多く見られるセキュリティ上の問題を表しています。この問題の複雑さは、IAMポリシーの中で、リソース、アクション、アイデンティティが融合されていることに起因します。最小権限アクセスの原則を実行することは、データ侵害のリスクを軽減するためだけでなく、権限昇格やラテラルムーブメントに関連する潜在的な脅威を阻止する上でも最も重要です。



STEP 04

クラウド脅威の継続的な検知と対応

- 資産とアクティビティを相互に関連付け、リソース全体におけるリスクと悪用可能なリンクを可視化します。.
- ランタイムインサイトから得られるコンテキスト（使用中の脆弱性や使用中の権限など）を、静的アセスメント（設定ミスや既知のセキュリティ上の欠陥を含む）と組み合わせることで、最も重要な事項に優先順位を付けることができます。
- クラウドリソース（ストレージ、データベースなど）、仮想サーバー用インフラポート、コンテナ、コンテナオーケストレーションプラットフォームの設定における変更を特定します。
- 予期せぬ振る舞いやリモートコード実行のプロセス実行パターンを検知します。
- 過去のインシデントのデータを調べることで、パターンを検知します。

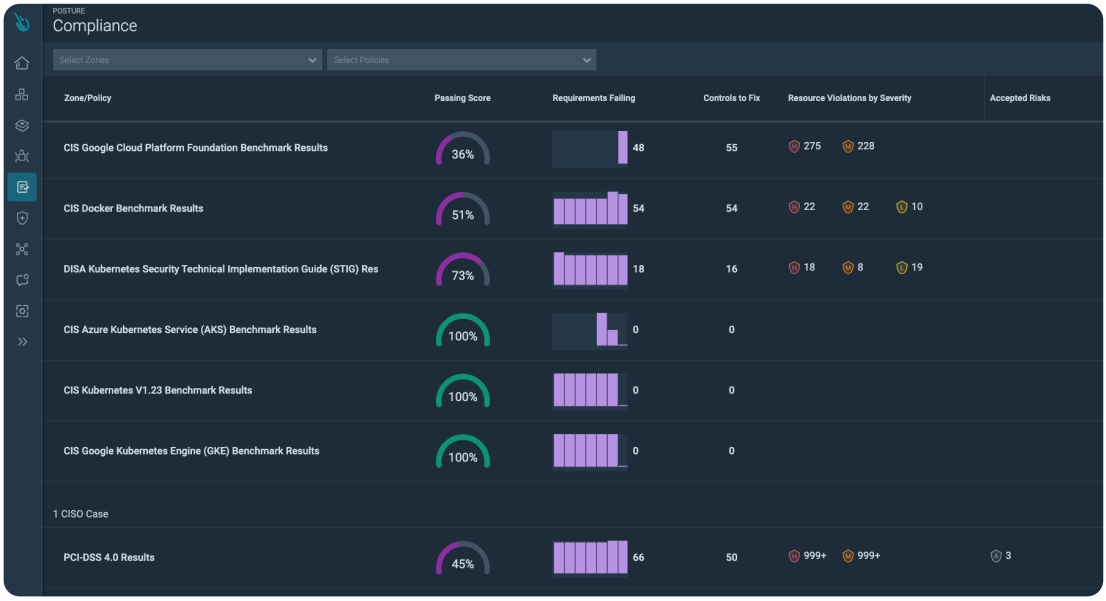
リアルタイムのクラウドアクティビティは、クラウドのコントロールプレーン内、ユーザー間、サービス間での異常なアクティビティを特定するために不可欠です。クラウド攻撃は、侵入後わずか10分以内に発生する可能性があるため、検知の有効性は、どこに焦点を当てるべきかを知っているかどうかにかかっています。これらの要素がなければ、マルチクラウド環境で活動する組織は、暗中模索に陥ってしまう可能性があります。チームは、情報過多により圧倒され、優先順位を見極めるのに苦労し、最終的にセキュリティポスチャーを弱めることになります。

STEP 05

クラウドのコンプライアンスとガバナンスを検証

- 各種のセキュリティ標準やフレームワーク（ISO/IEC 27001、NIST 800-53、PCI DSS、SOC 2、FedRAMP、MITRE ATT&CK®など）を実施するPolicy as Code（PaC）型のコントロールを採用することで、コンプライアンスポリシーを自動化します。
- ビジネスユニットや環境にリソースを戦略的に割り当てることで、セキュリティチームは、そのインフラストラクチャーに必要となるセキュリティポスチャーをより深く理解できるようになります。これにより、クラウドチームは、監査人や顧客向けのコンプライアンス検証を容易に行えるようになります。
- 詳細なレポートとセキュリティに関する調査結果を元に、フレームワークや標準に対するクラウドコンプライアンスの進捗を継続的に追跡します。ガイド付きの修正プレイブックと提案の採用で、平均対応時間（MTTR）を短縮できます。

現在、コンプライアンスを管理することは、義務的なもの、任意的なもの、地域固有のもの、重複するものなど、無数の基準や規制と向き合うことを意味します。これらの基準や規制を満たさない場合、評判の低下や多額の罰金など、大きなリスクが伴うことになります。



まとめ

クラウドでは1秒1秒が大切

攻撃は瞬時に進行するため、セキュリティチームは、ビジネスの減速を抑え、自社を保護しなければなりません。Sysdigは、ランタイムインサイトとオープンソースのFalcoを使用してリスクの変化を即座に検知することにより、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体のシグナルを相互に関連付け、隠れた攻撃経路を明らかにした上で、今対処が必要な真のリスクに優先順位を付けます。予防から防御に至るまでをサポートすることで、Sysdigは、企業がその最も重要な課題である「イノベーション」に集中できるようにします。

SysdigのAWS、GCP、Azureにおける継続的なクラウドセキュリティの提供について詳しく知りたい方は、当社までデモをご依頼ください。

デモを依頼 →