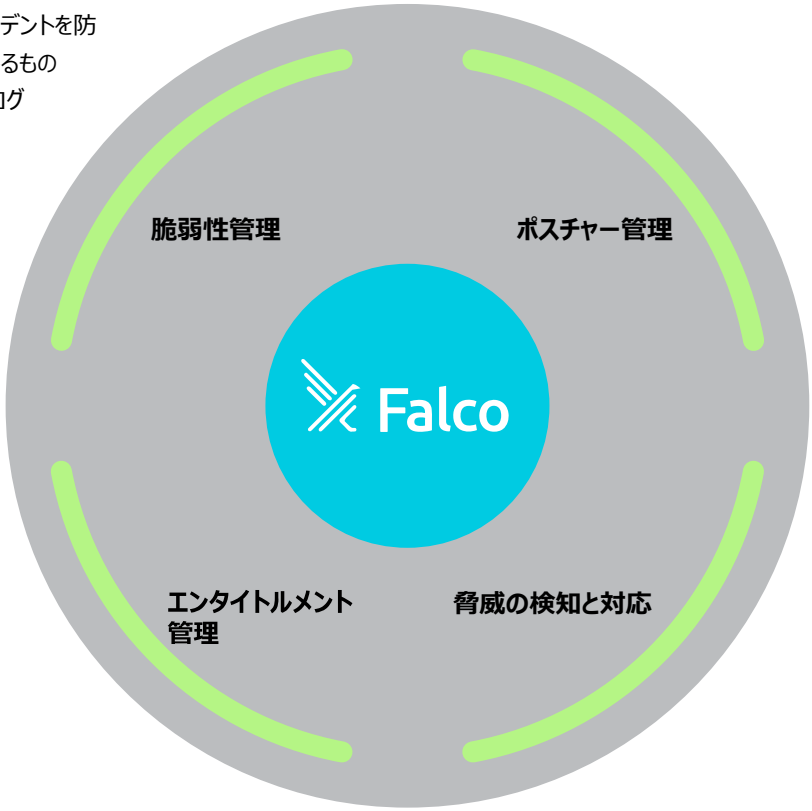
sysdig

ホワイトペーパー

ランタイムインサイトがシフトレフトセキュリティの鍵になる

クラウドセキュリティプログラムは、多くの場合、「シフトレフト」または「シールドライト」という2つのアプローチのいずれかを重視しています。シフトレフトアプローチとは、セキュアな設計と公開前のテストを促進するプロセスとツールに重点を置くものであり、セキュリティ上の問題が本番環境での問題になる前にそれを特定しようと試みるものです。シフトレフトアプローチとは、DevOpsのプラクティスと緊密に結び付いたものであり、セキュリティポスチャーを強化することで侵害を防ぐことを目的としています。一方、シールドライトアプローチとは、運用プラクティス、セキュリティ監視、およびランタイムセキュリティ機構に重点を置くものであり、セキュリティインシデントを防止し、発生したイベントを検知してそれに対応しようと試みるものです。どちらのアプローチも成熟したサイバーセキュリティプログラムには不可欠ですが、実際には、これらのアプローチはそれぞれ単独で実行されることが多いため、組織内にサイロ化をもたらしています。



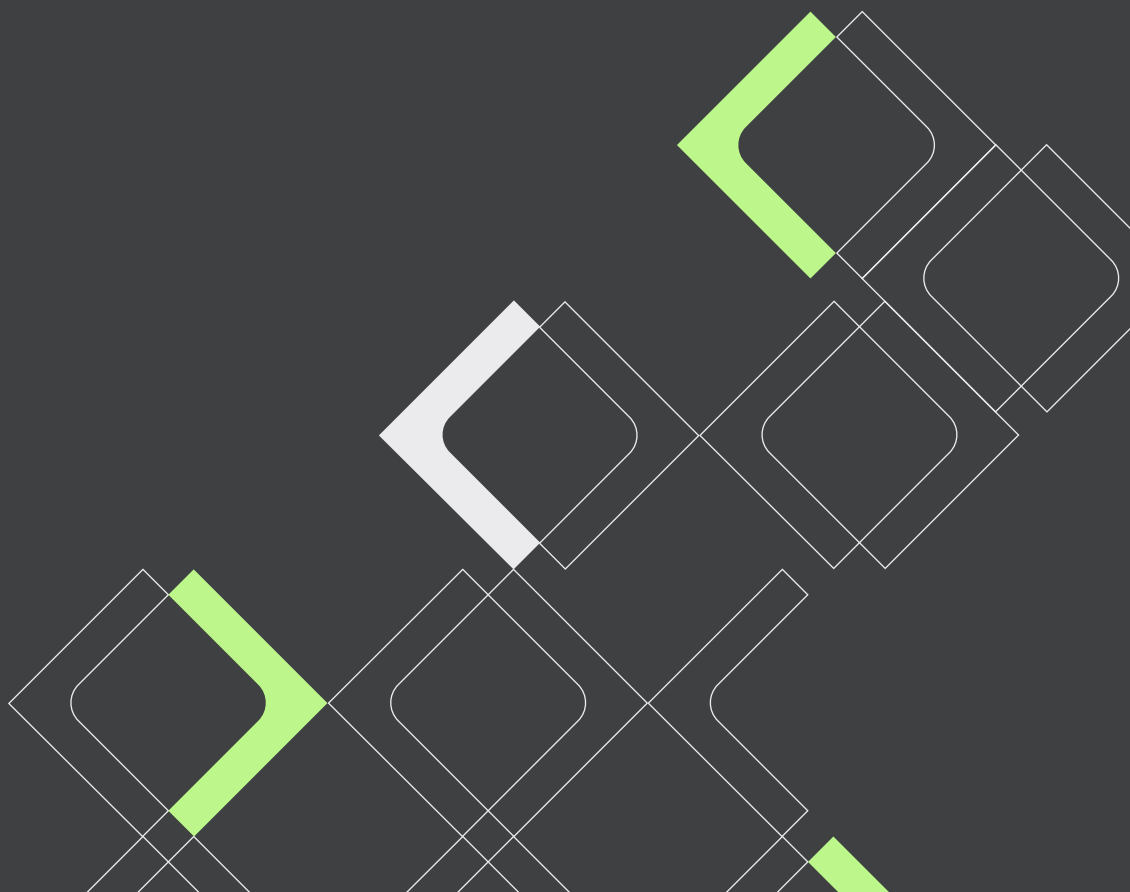
ランタイムインサイトは、これら2つのアプローチをつなぐものであり、ランタイムインサイトを使うことで、クラウド攻撃のスピードと高度化に後れず、サイバーセキュリティの範囲を拡張できるようになります。ランタイムインサイトを組み込んだセキュリティアプローチを適用することで、リスクの優先順位付けと軽減、脅威のリアルタイムでの検知と対応、そして環境全体にわたるリスクのある組み合わせの特定が可能となります。この文書は、シフトレフトアクティビティや予防的セキュリティにおけるランタイムインサイトの重要性を解説し、クラウド環境における攻撃を回避するのに役立ちます。

目次

現在のシフトレフト戦略における課題

シフトレフトセキュリティには、ノイズの問題があります。スキャンツールを使って公開前のテストを開始しますが、あっという間に大量のスキャナー出力の対応に追われるようになります。アプリケーションリリースの合否を判断するための効率的な方法を見つけるのは大変な仕事です。脆弱性を見つけることは重要な事ですが、そのリスクに今対処するべきかどうかを判断することが困難なのです。

明確なリスクの優先順位付けができないままセキュリティ問題が山積している中で、ランタイムセキュリティが再び注目されています。多くの場合、次世代ファイアウォールやWebアプリケーションファイアウォールのような時代遅れのブロックメカニズムを使って作業を開始し、その後、セキュリティ情報やイベント管理（SIEM）を含むセキュリティ監視を強化することになります。これでは時間だけがかかり、問題は解決されません。

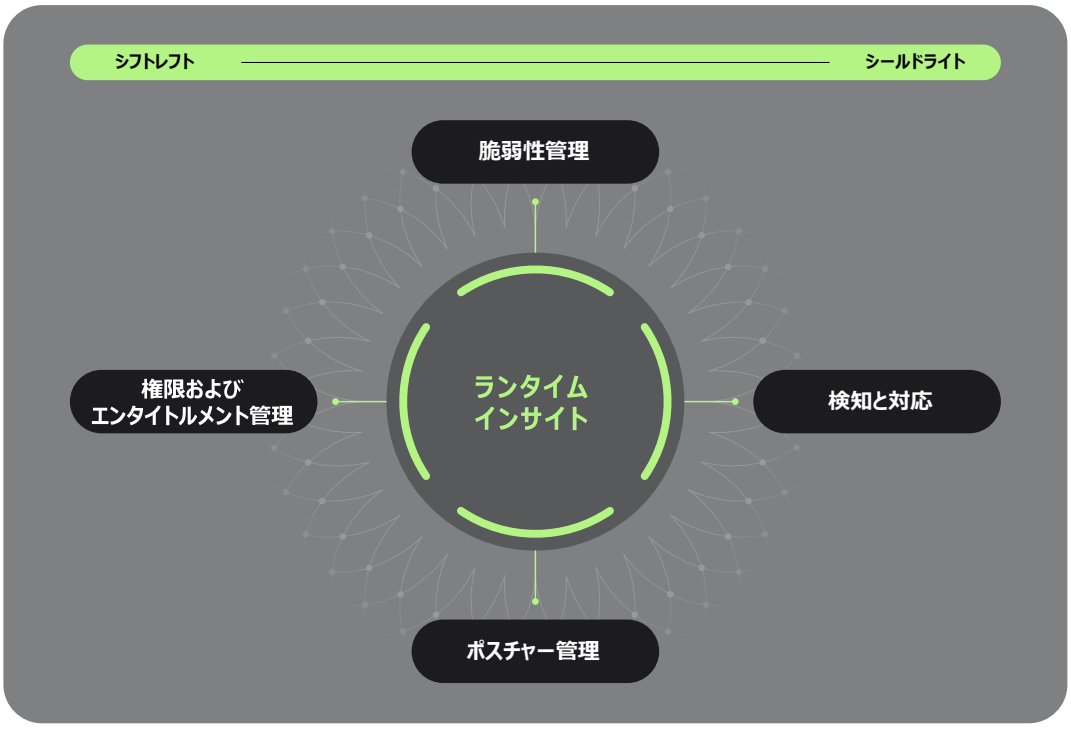


クラウドへの移行がセキュリティギャップをもたらしている

ビジネスプラクティスの大きな変化と同様に、チームの再編とプロセスの改良は、クラウド導入の重要な部分です。企業はDevOps、クラウドエンジニアリング、プラットフォームオペレーションなどの機能を持つように進化しています。また、クラウドセキュリティプロセスを監督し、環境を管理するようなSCoE（Security Centers of Excellence）を設立するか、またはエンジニアリングチームにセキュリティ人員を配置するなどの、異なる方向性を選択するものもあります。

また、クラウドセキュリティ戦略におけるギャップに対処するツールにも注目しています。予防に関しては多くの場合、ポスチャー管理、脆弱性管理、権限およびエンタイトルメント管理のためのポイントスキャンツールに焦点を当てます。防御に関しては、多くの場合、SIEMのような従来のツールを含むセキュリティ監視に焦点を当てます。しかし、これは完全にプロアクティブな保護的アプローチではなく、脅威の検知と対応に重点を置いたアプローチです。

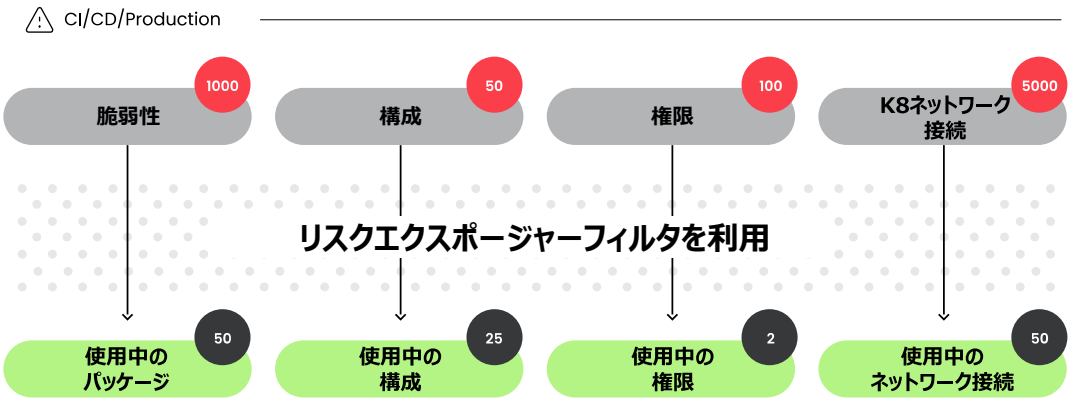
ランタイムインサイトの出現により、これらの領域のツールを統合するソリューションへの道が拓かれました。これにより、実行中のものに関するリアルタイム情報が提供されるため、セキュリティチームは、より高い信頼性で予防と防御を行えるようになります。次の図は、これらのセキュリティ活動が通常、シフトレフトとシールドライトのどの領域に位置しているかを示すものです。



ランタイムインサイトをセキュリティに適用する

ランタイムインサイトは、お客様の環境で最も影響を与える問題を優先的に解決するために実践的な情報を提供します。その情報は今まさに実行されているものに関する知識に基づいています。ランタイムインサイトは、実行環境で実際に起こっていることに関する「レンズ」を提供するものであり、これを利用することで、セキュリティチームや開発チームは、最も重要な問題に対処できるようになります。私たちはファイアウォールやIPSのような古い言葉は使わず、導入されたアプリケーションやシステムに関する可視性を高める機能を重視しています。もはや、配信前のイメージスキャンだけに頼ることはできません。多くの場合、セキュアな設計やセキュリティテストを中心としたアプローチでは不十分だからです。

下記の図は、シフトレフトスキャンにより、検知される環境問題の数がいかに増加するか、そして適切なリスクエクスポージャーフィルタを使用することで、実際のリスクに基づいて問題の数を、いかに対処可能な数へと減らせるかを示したものです。



ランタイムインサイトの主な特徴

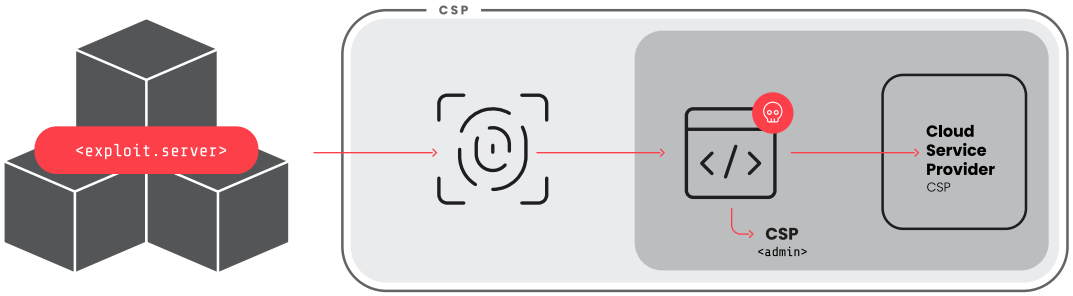
あらゆる種類の環境とワークロードを評価して保護するためには、ランタイム・インスツルメンテーションが不可欠となります。ランタイムインサイトの主な特徴として、次の4つが挙げられます。

- **実行中：**リスクの優先順位付けを行い、セキュリティプログラムを効果的に拡張できるようにチームを支援します。組織とそのシステムで実際に使用されているものを特定することで、誤検知や重大度の低い問題を追いかける負担を軽減できます。
- **マルチドメイン相関：**機密データへの攻撃経路をもたらすような、環境全体におけるリスクのある組み合わせを特定します。また、予防制御の一種として、環境構成にギャップが存在する場所を目立たせるような、データの可視化を強化します。
- **リアルタイム検知：**継続的かつリアルタイムな検知を実現します。クラウド環境は常に変化しているため、ポイントインタイム式の環境評価やスキャンでは不十分です。また、データ収集や分析の遅延に対する許容度は極めて低いものとなります。なぜなら、それらの遅延は非常に長い「露出期間（Windows of Exposure、WoE）」をもたらすからです。
- **エンドツーエンドの検知：**ホスト、コンテナ、クラウドサービス、サーバーレス機能で構成されるクラウド環境において、さまざまなアプローチ（ルールベースの検知、振る舞いベースの検知、MLベースの検知など）を通じて、あらゆるものを検知します。詳細については、「**エンドツーエンドの検知によりクラウドを保護**」をご覧ください。

ランタイムインサイトを利用した攻撃チェーンの検証

ランタイムインサイトを使ってシフトレフトとシールドライトのアクティビティを通知することで、**SCARLETEEL**のような脅威における複雑な攻撃チェーンで悪用される問題を防止、検知、修正できます。この攻撃チェーンは、Sysdig脅威リサーチチームにより発見されたものであり、下図に示すように、他の攻撃よりも洗練されていました。この攻撃は、Kubernetesコンテナへのハッキングから始まり、被害者のアマゾン ウェブ サービス（AWS）アカウントへと拡散しました。この攻撃チェーンには多くの側面があり、それはクラウドベースのインフラを保護することの本質的な複雑さを浮き彫りにしています。配信前のスキャンと脆弱性管理だけでは、このシナリオのリスクをすべて軽減することは不可能です。ランタイムインサイトを利用することで、検知を加速し、可視性を高め、攻撃経路を明らかにすることが可能となります

実際に使用されている権限を明らかにすることで、過剰な特権（S3バケットへの書き込み権など）や、不要なインフラ構成のドリフト（ビルドパイプラインをバイパスして新しいコードを本番環境に直接デプロイする権限など）をもたらす可能性がある特定の役割を最適化できます。また、既知の脆弱性を持つパッケージがどのようにデプロイされ、使用されているかをアドバイスすることで、起こりうるインシデントや侵害を防ぐための修正に優先順位を付けることに、チームの力を集中させることができます。



ランタイムインサイトがセキュリティを強化する3つの方法

このセクションでは、ランタイムインサイトと、それが持つ主要な属性が、先に述べた3つのシフトレフトのセキュリティ活動（脆弱性管理、ポスチャー管理、権限およびエンタイトルメント管理）にどのように適用されるかについて、より深く掘り下げてみましょう。

1. 脆弱性管理

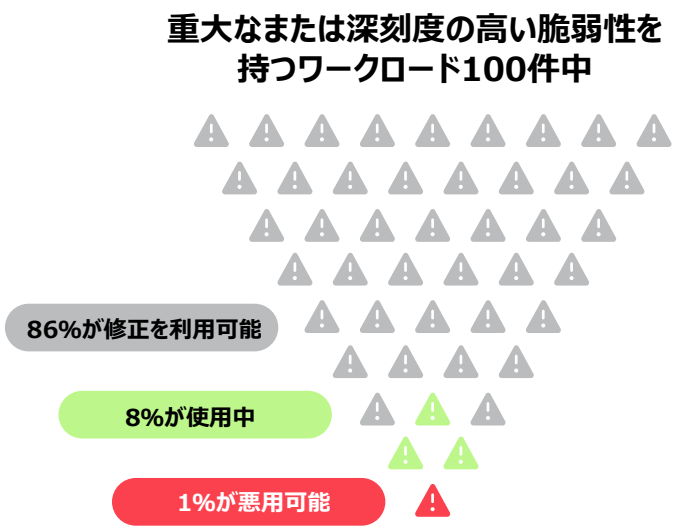
セキュリティチームやエンジニアリングチームは、分類すべき脆弱性があまりにも多すぎるために疲弊しています。2023年5月現在、CVEデータベースには1万件以上の新しい脆弱性が登録されており、これらが**21万件以上の既存の脆弱性プール**に追加されています。ヘビーなシフトレフトアプローチが使用されるクラウド環境では、設計、コードコミット、ビルド、配信などの異なる段階でスキャナーが脆弱性を検知するため、同様の問題が繰り返し発見されることがあり、その結果としてリリースの判断が複雑になります。攻撃者に悪用される前に修正や依存関係の変更を優先できるよう、影響を受けるすべての資産を正確かつタイムリーに把握する必要があります。残念ながら、これらの要件は、迅速なリリースサイクルや加速するリリース速度とは相容れないものです。

最新の脆弱性管理を成功させるためには、セキュリティチームが、実際のリスクに基づいて、脆弱性に優先順位を付ける必要があります。脆弱性の優先順位付けは、エンジニアリングチームの疲労を軽減し、反復的なアプリケーション開発を安全かつ高品質にし、迅速なリリースケーデンスを維持するために不可欠です。リスクベースの判断は、すべてのセキュリティプログラムの基礎となるものであり、脆弱性管理に関する基準としては、次のものが挙げられます。

- どのような脆弱性が悪用可能か？
- 既知のエクスプロイトや概念実証コードが利用可能な脆弱性にはどのようなものがあるか？
- ネット上や特定の業界で活発に狙われているものは何か？
- あらゆる環境、そしてあらゆる依存関係において、どこに脆弱性が存在するか？

『**2024年版クラウドネイティブセキュリティおよび利用状況レポート**』に掲載されている調査結果は、実行時にロードされる脆弱性のあるパッケージに修復作業を集中させることで、負担の大きい開発者に希望の兆しを与えています。イメージの大部分には重大なまたは深刻度の高い脆弱性が含まれていますが、実行時に実際のリスクをもたらすような脆弱性の割合ははるかに低くなっています。顧客の導入環境に見られた脆弱性の全体像を、次の図に示します。重大なまたは深刻度の高い脆弱性を含んでいるワークロードの割合は、次のようにようになります。

- 86%のワークロードが修正を利用可能です。
- 修正可能で、かつ実行時に実際に存在する脆弱性を含んでいるワークロードは、わずか8%です。
- 修正可能で、かつ実行時に使用中であり、かつ既知のエクスプロイトコードが存在している脆弱性を含んでいるワークロードは、わずか1.2%です。



実際に修正可能なもの、実行中のもの、悪用可能なものをフィルタリングすることで、軽減や修復の優先順位をより明確化できます。リスクの高い脆弱性には、組織独自の環境やアプリケーション設計の選択に照らして、より高い優先順位付けをすることができます。これらの脆弱性は、現実的かつ緊急の危険にさらす可能性が高いものとなります。

悪用可能な脆弱性を自社環境に残しておかなければならない場合、セキュリティチームは、ランタイムセキュリティ検知を実装することで、侵害のリスクを低減できます。ランタイム保護は多くの場合、ルールベースで実現されるますが、振る舞いの異常検知や、AIまたはMLベースの検知を組み込んだ多層的なアプローチも採用する必要があります。このようなアプローチにより、ゼロデイエクスプロイトや未知の脅威を検知し軽減する能力を向上できます。また、ランタイム保護メカニズムを調整することで、組織特有の環境内にある脆弱なワークロードを標的とする新しい脅威を検知できるようになります。

実際に修正可能なもの、実行中のもの、悪用可能なものをフィルタリングすることで、軽減や修復の優先順位をより明確化できます。リスクの高い脆弱性には、組織独自の環境やアプリケーション設計の選択に照らして、より高い優先順位付けをすることができます。

2. ポスチャー管理

アプリケーションやサービスを提供するインフラストラクチャのセキュリティを強化することは、すべてのセキュリティプログラム作業にとって基本となるものです。不要なクラウドサービスや既知の脆弱な構成は、理想的にはIaC（Infrastructure-as-Code）およびPaC（Policy-as-Code）式のアプローチを使用して、最初から無効化しておく必要があります。また、古い設定ミスが再び環境に忍び込むことがないように、設定を継続的に検証する必要もあります。セキュリティポスチャーを評価することは、非常に扱いにくい問題です。このため、組織は多くの場合、ネイティブのクラウドプロバイダーの管理コンソールや監査機構、監査用のシェルスクリプト、OpenSCAPのようなオープンソースツールなど、さまざまなアプローチを試しています。

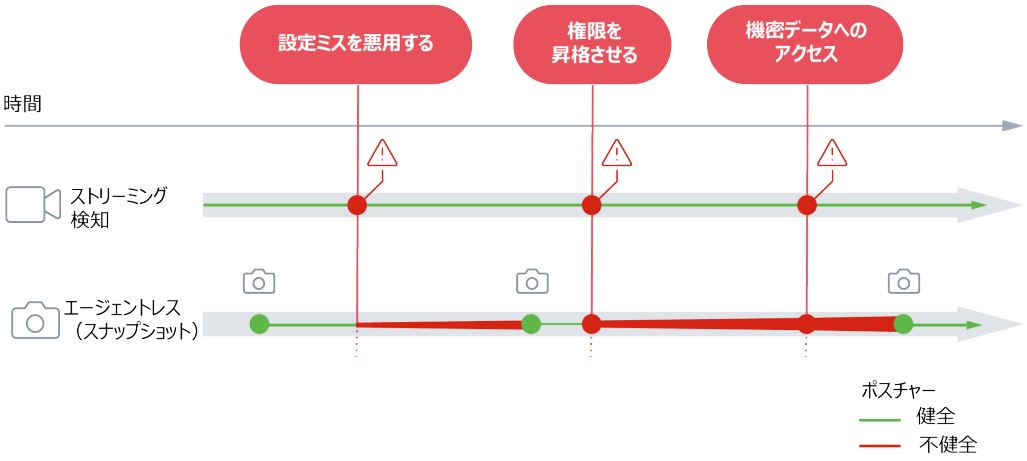
クラウドの導入が進んだ組織では、環境のスナップショットに基づいてテナントの設定ミスを監査して報告するような「クラウドセキュリティポスチャー管理（CSPM）」ツールを導入することが一般的です。

CSPMを導入しているにもかかわらず、ガバナンスとコンプライアンスに悩まされることはよくあることです。GRCチームは、標準的なセキュリティ要件を定義します。エンジニアリングチームは、新しいアプリケーションやシステムを導入する際に、これらの要件を満たすことが期待されます。そして、理想的には、これらのすべてが、認可されたリポジトリやレジストリに「ゴールデンイメージ」として保存されます。しかしここで、よくある2つの落とし穴が発生します。

1. 広範なセキュリティ要件（コンプライアンスや法的目的に有用）と、その要件を満たすための具体的な技術的導入の詳細との間にはギャップがあること。
2. ビルド、デリバリー、運用の全体を通じて通常発生する環境変化に伴い、計画されたセキュアな構成と、提供または維持されるものとの乖離が、時間の経過と共に発生すること。

多くの組織は、CSPMツールが導入されている場合でも、ポイントインタイム型の評価を利用しています。業界では、このようなタイプの検証のことを、しばしば「スナップショットアプローチ」と呼びます。侵入テストと同様に、このようなタイプの検証は、定期的なチェックを義務付けるコンプライアンス監査や規制要件を満たすために有用であると考えられます。しかし、このようなアプローチは、セキュリティにとってハードルの高いものではありません。スナップショットアプローチには、レイテンシーが高くかつ精度が低いという欠点があります。

このような最小形態のセキュリティは、誤った安心感をもたらします。静的な制御に対して一連のスケジュールされた監査を実行しても、近い将来、構成が変更されないことを保証することはできません。設定ミスは、攻撃者にとって長い「露出期間（WoE）」をもたらすものであり、定期的に標的とされ悪用されます。組織が持つクラウド資産とそれに対応するセキュリティポスチャーの一覧（インベントリ）をライブで保持することは、不要な構成変更から組織を守るための最善の手段です。下記の図は、ストリーミング検知とスナップショット式のアプローチを視覚化したものであり、エージェントレスオンリー式のアプローチがもたらす「露出期間（WoE）」を取り上げています。



たとえば、米国国家安全保障局は、クラウドの設定ミスは「最も一般的なクラウドの脆弱性」であり、「クラウドにおけるセキュリティは絶え間ないプロセスであり、顧客はクラウドリソースを継続的に監視し、セキュリティポスチャーの改善に取り組むべきである」と述べています。[1]

クラウドサービスのスケーラビリティと拡張性はイノベーションの原動力となるものですが、攻撃者はこのような拡張されたアタックサーフェスを利用して、最初のアクセス権を獲得した後、被害者の環境でラテラルムーブメントを実行します。クラウドの設定ミスは、他のリスクと組み合わさることで、攻撃者が機密情報にアクセスするために悪用できるような、隠れた攻撃経路を生み出す可能性があります。ランタイムインサイトを利用して、クラウドインフラストラクチャー内に存在する複数のドメイン間におけるリスクの組み合わせを特定することで、このような隠れたパスを可視化できます。実行時に組織のセキュリティポスチャーにおけるどの領域がリスクにさらされているかを確認することで、環境構成におけるギャップを特定し、その悪用を防ぐことが可能となります。

急激に変化しているクラウドネイティブシステムでは、アプリケーションオーナーは、新しいビジネス要件を満たすために、自社のアプリケーションと基盤となるインフラに変更を加えることで、製品を継続的に適応させる必要があります。こうした変更が発生すると、アプリケーションやインフラの構成を調整することが必要となります。これにより、システムが「要塞化されたポスチャー」状態ではなくなる可能性があります。これが、私たちが定義する「構成またはポスチャーのドリフト」です。

組織が直面するポスチャードリフトの課題とは、それをいかにリアルタイムで検知し、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、いかにしてそれを把握するかということです。「as-code」式のアプローチを適切にサポートするためには、検知はコンテキストに応じた修正を提供する必要があるほか、さらに無駄な時間を省くためにプルリクエストを生成する必要もあります。また、対応に柔軟性を持たせ、ノイズを減らすためにリスクの優先順位付けを行い、「as-code」式のアプローチによる自動化を受け入れ、設定ミスに関するアラートをランタイムインサイトで充実させることにより、ポスチャーの評価と実施に固有の「悩ましい問題」の多くを軽減できます。

1 The U.S. National Security Agency, **Mitigating Cloud Vulnerabilities**, 22 January 2020

3. 権限およびエンタイトルメント管理

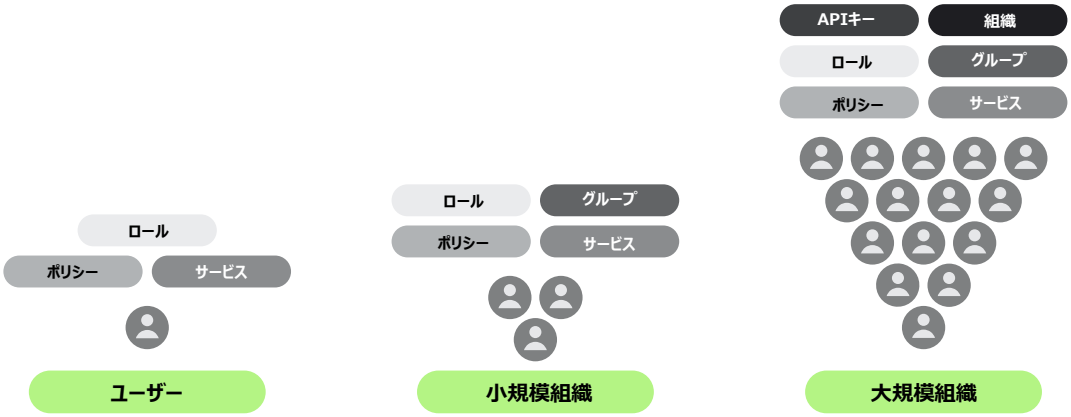
設定ミスは、依然としてセキュリティインシデントの最大の要因となっています。したがって、それは最大の懸念事項の1つとなるべきものです。

Gartner®は、「2023年までに、セキュリティ障害の75%は、ID、アクセス、および権限の不適切な管理に起因するものとなり、2020年の50%から増加する」と予測しています[2]。多くは最小権限の強制などゼロトラスト原則を話題にしていますが、当社のデータによれば、クラウド権限の90%が未使用のままであり、彼らがゼロトラスト原則を採用しているという証拠はほとんどありません[3]。

セキュリティ担当者としてアクセス制御の重要性を繰り返し学んでいるにも関わらず、IDやアクセス制御の誤操作は今もなお非常に多く見られます。なぜ、このようなことが起こるのでしょうか？実際には、システムは、裁量アクセス制御（DAC）や役割ベースのアクセス制御（RBAC）など、アーキテクチャに応じて、さまざまなアクセス制御の種類を組み合わせて使用しています。

IDをグループやロールに割り当てて許可や権限を与える方法は、アクセス制御の種類や技術スタックにより異なります。ユーザーは多くのグループに所属しており、ユーザーとグループは多くのロールへとマッピングされています。ロールは「広すぎる」定義であるため、きめ細やかさや厳密なアクセス制御を犠牲にすることで利用可能となります。クラウドリソースは数が多いため、複雑さや脆弱性を増やさないようにするために、アクセス制御の「粒度を粗く」することになります。また、機能の変更、従業員の離職や異動、顧客の減少、技術スタックの変更などが原因で、アクセス権は時間の経過と共に変化します。

IDおよびアクセス管理（IAM）チームの構造やプロセスにかかわらず、最終的な結果は部分的なカオスとなります。下図のように、IDと権限のポケットが急速に形成されます。しかし、これらの分散されたアクセス権の島々は、最新の設計の一部として接続され統合される必要があります。厳密なアクセス制御を実施することは、ほとんどの企業にとって、すぐに維持できないものとなります。



2 GARTNERは、米国および国際的なガートナー社および/またはその関連会社の登録商標およびサービスマークであり、許可を得て本書に使用しています。All rights reserved. Gartner, Best Practices for Optimizing IGA Access Certification, Gautham Mudra, 4 April 2022

3 **2024年度クラウドネイティブセキュリティおよび利用状況レポート**を発表, 2024年1月

最小権限の原則（PoLP）は、アクセス制御にとって絶対に不可欠なものです。開発者、セキュリティアーキテクト、コンプライアンス専門家がすべて、邪魔するものなしに自らの仕事を行えるようにする必要がありますが、その一方で、彼らがこの範囲を超える越えることができないようにすることも必要です。また、最小権限に従わなければならない独自の許可を持っているマシンIDやサービスアカウントも忘れてはなりません。クラウド環境では、抽象化、統合、自動化によって、マシンIDの数が、ヒューマンIDの数を上回ることがよくあります。

最小権限だけでは、もはや強固なアクセス制御には十分ではありません。企業や組織は、継続的に許可を検証する必要があるほか、与えられた環境が危険にさらされていることを常に想定しなければなりません。ID、アプリケーション、およびシステムの振る舞いを継続的に監視することを通じて、疑わしい活動を検知し、それに対応することを望んでいます。そのためには、効果的なゼロトラストアーキテクチャ（ZTA）を実現する必要があります。ある脅威アクターは、他のアカウントの乗っ取りやシークレットの取得に成功すれば、損害を引き起こすのに十分な権限を持つことができます。また、権限の昇格を行わず、設定ミスを悪用することもなく、損害を引き起こすことも可能です。

効果的なIAMには、アカウントやノンヒューマンユーザーへの権限付与におけるきめ細かさを維持するために、多くの異なるチーム間のコラボレーションとオーナーシップが必要となります。各チームは、自分の責任範囲と必要最低限のリソースを把握しておく必要があります。ITチーム、あるいはIAMチームが存在する場合は、クラウドプロバイダーが提供する制御を使用して最小権限の原則に従う必要があります。しかし、残念ながら、CloudOpsチームとPlatformOpsチームの両方が存在する場合、環境の運用から切り離されたチームにより設定された要件に基づいて、セキュリティが運用される可能性があります。この場合、義務化されたセキュリティ要件と具体的な技術的実装の間の不一致が、すぐに頭をもたげることになります。

アクセス制御を担当するチームは、多くの場合、クラウドのアクセス権限や、ヒューマンIDとマシンIDの混在に苦労しています。スケーラブルなデータセキュリティのアプローチでは、権限付与は、データ所有者や管理者に委託されることがよくあります。この場合、どのようなアクセス権が必要なのか、いつ必要なのか、そしてそれが実際に実行されているのかを判断することは、推測の域を出ません。このジレンマに立ち向かう唯一の方法として、どのようなIDがプロビジョニングされ、どのようなアクセス権が付与されているかを理解した上で、これをリアルタイムのアクセスパターン（または実行中のパーミッション）と組み合わせて、観測された振る舞いに基づいて権限を正確にモデル化することが挙げられます。この種のアプローチで確認することができる一般的なタイプの権限の誤操作には、未使用のパーミッション、未使用の管理アカウント、二要素認証のない特権アカウント、過剰な権限、本番環境のクラスターを壊すような破壊的な行動を行う特権ユーザーなどが含まれます。

最小権限だけでは、堅牢なアクセス制御にはもはや不十分です。継続的に承認を検証し、特定の環境が侵害されていると常に想定する必要があります。

ランタイムインサイトがアプリケーションをセキュアに保つ

クラウドでは明らかにセキュリティギャップが発生しているため、クラウドセキュリティ戦略には十分な検討が必要です。現在導入されているツールは、すべてのクラウド環境、特にクラウドネイティブな環境に適しているとは限りません。このようなギャップに対処するためのコアな特徴として、ランタイム・インスツルメンテーション、リスクの優先順位付け、リアルタイム検知を挙げています。ポイントソリューションで発生する分断を避けるために、統一された機能やプラットフォームに注目する必要があります。これは、シフトレフトやシールドライトの優先順位が定着する中で、より一層重要になっています。そのようなツールやプラットフォームは、最低限、次の機能を備えている必要があります。

- → 適切な環境とワークロードのシグナルを使ったリッチ化が行える
- → アプリケーションとサービスのコンテキストをホストコンテキストよりも優先して提供
- → 関連するイベントソースを取り込み、その場で処理できる
- → ワークロードの種類に応じて適切なインスツルメンテーションを使用できる
- → デリバリー前のスキャン結果とランタイム監視を相互に関連付ける
- → 各チームのワークフローやシステムとの統合を行い、分断を回避する
- → 組織独自の環境に対応するために、修正のカスタマイズやコンテキスト化が行える
- → 「as-code」式のAPIファーストアプローチにより自動化を促進

これらの機能は、これまでCSPM、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）、クラウドワークロード保護（CWP）など、他のツールカテゴリを通じて提供されていました。このようなツールを導入して運用することで、自然に対話が形成されるようになるため、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）という形で、新たな複合プラットフォームアプローチが登場することになりました。

クラウド環境が複雑化するにつれて、クラウドインフラストラクチャー内に存在するドメイン間で、コンテキストと調査結果を相互に関連付けることができるようなプラットフォームの価値が明らかとなっています。ランタイムの可視化により、マルチドメイン相関を通じて、サーバー、コンテナ、クラウドサービス、サーバレス機能、およびアイデンティティの全分野における最も重要なリスクを特定し、優先順位を付けることが可能となります。ランタイムインサイトを活用することで、セキュリティチームは潜在的な攻撃経路を可視化できるようになるほか、セキュリティポスチャーを強化し、攻撃を未然に防ぐために必要となるコンテキストを明らかにすることが可能となります。クラウドセキュリティプログラムを強化するツールの種類にかかわらず、クラウド環境を安全に保つためには、利用しているすべてのツールがランタイムインサイトを搭載しており、かつエンドツーエンドの検知機能を提供するものであることをご確認ください。

参考資料

本文中で紹介したレポート、ならびに内容に関するブログや学習コンテンツ、ガイドをここに紹介します。

- 【レポート】2024年度版クラウドネイティブセキュリティおよび利用状況レポート
- 【ブログ】Run Faster, Runtime Followers（日本語版）
- 【ブログ】なぜ企業はクラウドにおける最小特権にいまだ苦慮しているのでしょうか
- 【ブログ】脆弱性の優先順位付けによるデベロッパー疲労対策
- 【ブログ】クラウドでリアルタイムに脅威を検知する
- 【ブログ】SCARLETEEL: Terraform, Kubernetes, AWSを活用したデータ窃盗
- 【学習】クラウドネイティブを学ぼう（クラウドやコンテナのセキュリティに関するナレッジベース）
- 【ガイド】SANS CNAPPバイヤーズガイド（日本語版）

WP-006-JA REV. B 9/24