sysdig

ホワイトペーパー

クラウドセキュリティにおけるアーキテクチャーの重要性

包括的なリアルタイムのクラウドセキュリティをエージェントレス型とエージェント型の両方を使って実現

最新のクラウド環境の複雑性と多様性に対処できるかどうかで、クラウドセキュリティプラットフォームの有効性が決まります。エージェント型とエージェントレス型のソリューションを組み合わせた統合的な戦略が必要です。最適化された設計とは、パフォーマンス、スケーラビリティ、そしてさまざまなワークロードや導入規模における適応性など、全ての側面を熟慮したものとなります。さらに、既存のテクノロジースタックとのシームレスな統合を通じて、重要なインサイトと実用的な結果を提供する能力も不可欠となります。

本稿では、異なるデータソースを統合し、収集したデータを充実させて、リアルタイムで価値あるインサイトを生成する高度で包括的なソリューションの必要性について探求します。

目次

03
クラウドセキュリティには、エージェント型とエージェントレス型の両方のインストルメンテーションが必要となる

07
すべてのエージェントが同じように作られているとは限らない

09
技術的になろう：エージェントに関する知識の核

14
クラウドセキュリティには柔軟でスケーラブルなインサイトが必要

クラウドセキュリティには、エージェント型とエージェントレス型の両方のインストルメンテーションが必要となる

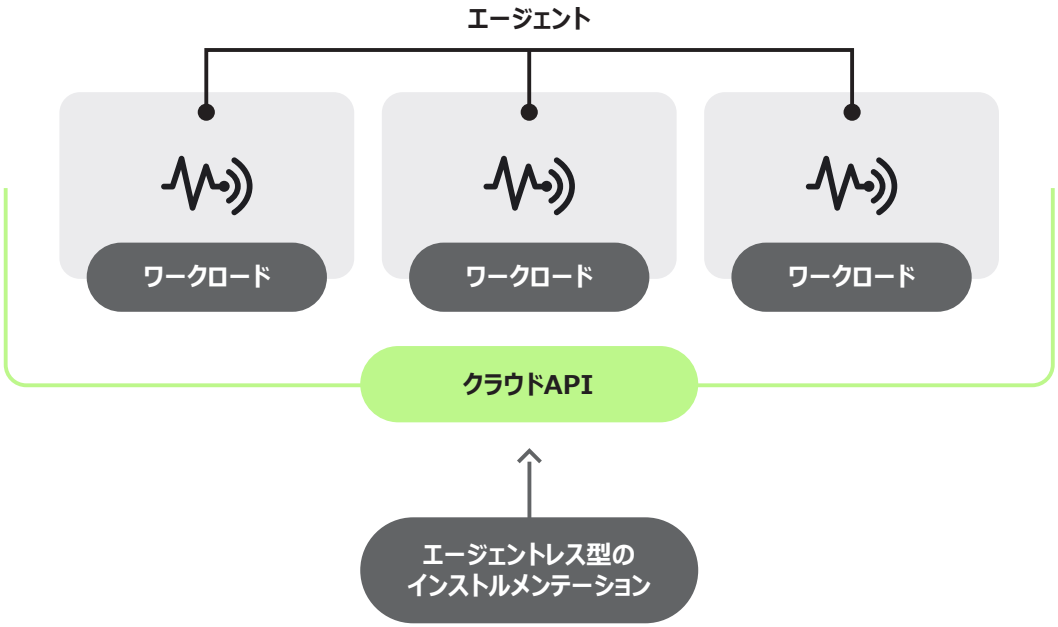
クラウド上でソフトウェアを開発し、効果的に展開することは、複雑なチャレンジを必要とします。高価なクラウドリソースの管理、進化するニーズやテクノロジーへの対応、そして、明確に定義されていないか、まったく存在しない境界線でそれらを保護することなど、多くの側面を含んでいます。このような複雑な状況でクラウドを保護するには、計算された戦略的アプローチが必要となります。すなわち、開発プロセスにおいてセキュリティを強化して保護するプロアクティブな「シフトレフト」型の方法論と、運用段階において潜在的な脅威から身を守るための検知および対応戦術の両方を採用しなければなりません。これらの異なる哲学を融合し、サイバーレジリエンスに焦点を当てた新たな規制要件と共存させるためには、クラウドセキュリティに対する組織的なアプローチを転換する必要があります。

クラウドセキュリティへの取り組みを始める際、セキュリティチームは、導入の容易さからエージェントレスのアプローチから始めることがあります。エージェントレスのセキュリティソリューションは、クラウドログ、API、ボリュームのスナップショットを活用し、クラウドセキュリティコントロールの監視、構成変更の検知、設定ミスや誤設定の特定、複数のクラウドアカウントにわたるドリフトの防御などを行い、実行時の可視性を提供します。エージェントレス型のセキュリティソリューションで必要となるのは、適切なIAM（Identity and Access Management）ロールが設定されたアカウントのみです。IAMロールはボタンをクリックするだけで簡単に作成できるため、これにより、初期設定プロセスを簡素化し、基本的なセキュリティ対策を迅速に導入できるようになります。

クラウドでソフトウェアを開発し、効果的に展開することは、さまざまな側面を含む**複雑な課題**です。

企業や組織がクラウドセキュリティへの移行をさらに進める中で、より強力な管理とより深い可視性へのニーズが高まっており、その結果として、エージェントベースのアプローチを通じてエージェントレス型のソリューションを強化するというニーズが高まっています。エージェントレス型のソリューションは、基本的なポスチャー管理と脆弱性管理を実現するためのシンプルで迅速なアプローチを提供するものであり、ランタイムの可視性も提供する場合があります。しかし、エージェントベースのソリューションと比較すると、エージェントレス型のソリューションには、システムレベルのアクティビティやリアルタイムに発生している事象のコンテキストに対するきめ細かな可視性が欠けています。エージェントレス型のみのソリューションは、広範な種類のクラウドメカニズムに依存しています。これには、通常3〜6時間間隔のスケジュールで変更を報告する定期的なスキャン、クラウドログのパーシング、または解析、分析、検知のためにSIEMにクラウドログを渡すことなどが含まれます。

クラウドコンピューティングのワークロードにソフトウェアエージェントを導入することで、プロセス、ユーザー、ファイルのアクティビティ、ネットワーク接続、およびその他のシステム固有の詳細について、より包括的なインサイトを得ることができます。これにより、振る舞い分析や機械学習アルゴリズムなどの高度な手法を含む、より効果的なクラウド脅威の検知と対応が可能となります。



エージェントレス型のアプローチとエージェント型のアプローチの両方を採用することで、Sysdigは、初期導入の容易さと、顧客がクラウドセキュリティへの移行を進める中で必要となるより深い可視性とより強固なセキュリティを両立させています。この柔軟で包括的なアプローチにより、より大規模な保護が可能となり、組織におけるクラウドのプレゼンスが成熟するにつれて進化を続けるセキュリティの課題に、効果的に適応できるようになります。 このことは、市場動向からも確認できます。Gartner社は、今年初めに発表した**「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）マーケットガイド（英語）」**の中で、最も先進的なCNAPPソリューションはエージェントが収集したデータを強化するために、エージェントレス型のインスペクションを使用していることを強調しています。

エージェントレス型のアプローチは、過去を振り返るためのものではなく、リアルタイムに対応したものでなければならない

クラウドサービスプロバイダが公開している強力な管理APIとスナップショットサービスは、セキュリティインストルメンテーションへのエージェントレス型のアプローチを可能にします。これらのサービスとプロバイダが提供する追加コンテキストを利用することで、導入されたリソースとその構成に関する意味のあるハイレベルな情報を収集できます。これにより、脆弱性評価、資産の検出、「静的な」クラウドセキュリティポスチャー管理などのユースケースを満たすことができます。さらに、クラウドイベントログを利用することで、セキュリティチームは、エージェント型のインストルメンテーションが利用できないサービスに関してもインサイトを収集することが可能となり、サードパーティサービス向けの脅威検知を実装できるようになります。

エージェントレス型のインストルメンテーションは、通常、スナップショット、API、ログ/イベントという3つの異なる方法で導入されます。

スナップショットでは、ワークロードの実行を妨げることなく、ポイントインタイムのイメージをリモートストレージへと転送し分析することが可能となります。これにより、ユーザーはディスクの内容をスキャンして、脆弱なパッケージ、マルウェアの痕跡、およびその他の侵害の痕跡（IoC）を見つけることができます。スナップショットをスキャンすることで、PIIやHIPAAなどの機密データや規制対象データを探すためのオーバーヘッドの少ないデータの検出と分類が可能になります。しかし、スナップショットベースのスキャンには、次のような重大な欠点があります。

- → スキャンはディスクの内容に限定されるため、オープンなネットワーク接続や実行中のプロセスなどのようなランタイムコンテキストは存在しないこと。
- → かなりの時間がかかるため、頻度を減らしてのみ実行可能となること（通常12時間または24時間ごと）。このため、検知時間をできるだけ短くする必要がある脅威検知のユースケースには適していません。
- → スキャナソフトウェアを実行するためのリソースが必要となること。これらのリソースが顧客の組織内でホスティングされる場合には、自社のクラウド支出が増すことになります。一方、これらのリソースがセキュリティツールプロバイダーのクラウド上でホスティングされる場合には、信頼できるサードパーティにスナップショットを送信する必要があるため、ユーザーの支出が増すことになります。

APIベースのインストルメンテーションとは、クラウドプロバイダーが公開しているAPIを利用して、クラウドインフラストラクチャー上でデータの収集、相互関連付け、および統合を行うものです。クラウドリソースとその構成に関するメタデータを引き出すことで、インフラストラクチャーを確実にマッピングし、潜在的な脆弱性（古いソフトウェア、露出したエンドポイント、過度に寛容なロールなど）を特定できるようになります。このタイプのインストルメンテーションは、可視性の点でも、呼び出しや帯域幅の割り当ての点でも、クラウドプロバイダーのAPIにより制限を受けることになります。

ログベースの検知とは、クラウドプロバイ ダー、ホスティングされているOS、およびアプリケーションが公開している各種の監査ログソースを利用することにより、潜在的に重大なセキュリティイベントを検知するものです。Sysdigは、静的リスクの調査結果をリッチ化し、それにアクティブリスク情報を重ね合わせることで、優先順位付け、調査、修正を実現しています。静的リスクとアクティブリスクの組み合わせのうち最もリスクの高いものが、攻撃経路の可視化と共に最上位に浮かび上がるため、調査を迅速化できます。また、ワークフローに統合されたガイド付きの修正機能を利用することで、セキュリティチームは一刻を争う問題を迅速に修正できるようになります。さらに、外部のIAMプロバイダーなどのサードパーティシステムでは、ログが唯一のイベントソー スである場合もあります。

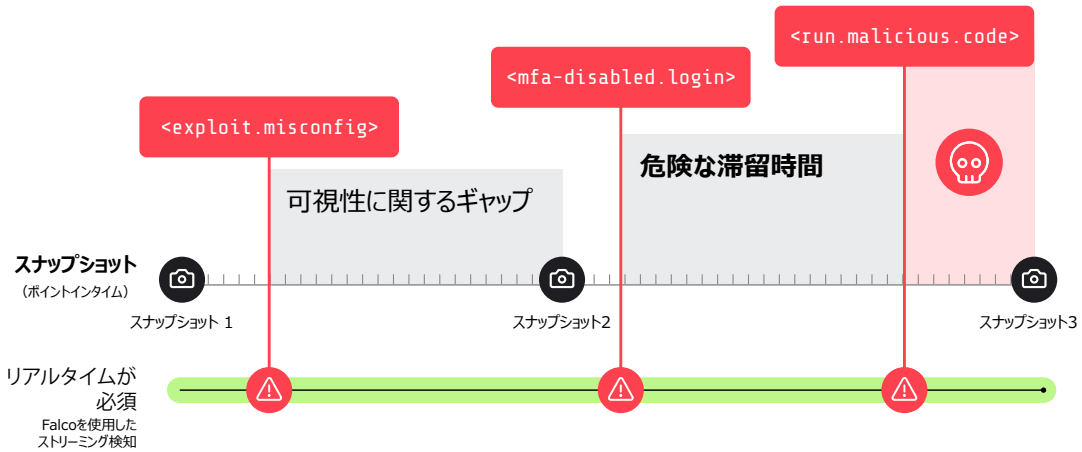
Sysdigは、イベントソースをリアルタイムで分析処理できる独自のエージェントレス型の実装を開発しています。Sysdigを利用すると、ユーザーはコンピュートワークロード以外のリソースを保護できるようになるほか、可能な限り攻撃経路の早い段階で脅威を特定できるようになります。Falcoをベースとしたこのユニークなストリーミング処理により、異種クラウド環境やオンプレミス環境も含めた全体においてリアルタイムの検知が可能になります。定期的なスキャンベースのアプローチや、後処理されたログ分析とは異なり、アクティブな悪意ある脅威を検知し特定するのに何時間も待機する必要はありません。

クラウドのリスクはアクティブです。
それにもかかわらず、なぜCSPMは静的なのでしょうか？

ポイントインタイム評価では、数時間以上の可視性に関するギャップが残る

静的なチェックは、アクティブな動きや動的な変化を見逃す

静的なチェックは、ランタイムコンテキストやアクティブな差し迫ったリスクを見逃す



ストリーミング検知は、悪意ある活動をリアルタイムで検知します。

すべてのエージェントが同じように作られているとは限らない

パフォーマンス、スケーラビリティ、精度、保守性に関する考慮事項

エージェントベースのソリューションについて議論する場合、パフォーマンスは第1の考慮事項となります。エージェントは、現実的なシナリオを通じてテストする必要があります。これには、さまざまなシステム負荷状況下において、ワークロード間でリソースを奪い合うことなく、重要なワークロードを保護することなどが含まれます。何が「許容できるパフォーマンス」を構成するかは、本質的に非常に主観的なものですが、エージェント型のソリューションは、トレースされるプロセスの適切な実行を妨げるものであってはなりません。

複雑なクラウド環境においてスケーラビリティを実現するには、単一のマシンまたは数百から数千のノードを持つクラスターにおいて、数プロセスから数千プロセスにまで拡張できるように設計されたソリューションが必要となります。しかもそれは、検知ルールやパフォーマンスに不合理な制限を課すこともなければ、有効性を犠牲にすることもないソリューションでなければなりません。これが、スケーラビリティによりストリーミング型アプローチの重要性が強調される理由です。つまり、イベントはできるだけ早く評価され、消費される必要があるのです。バッチベースやスナップショットベースのアプローチでは、特に大規模な導入環境において、時間的な制約のあるイベントを見逃すことは避けられません。

クラウドは、動的で、複雑で、かつ多様な、まるで雲のような「インフラストラクチャー」です。そのようなインフラを保護する責任を負うソリューションは、誤検知のノイズを正確に減らし、最もリスクの高いアラートを効率的に目立たせることができる必要があります。クラウドインフラストラクチャーの利用が拡大するにつれ、組織全体で単一のセキュリティポスチャーを実装することはより複雑になり、その結果、脅威アクターに悪用される可能性のあるギャップを生み出すことになります。セキュリティアーキテクチャーを簡素化し、テクノロジーパートナー間のより緊密でシームレスな統合を活用することで、より一貫性のあるセキュリティポスチャーを構築する基盤ができるようになります。

たとえば、検知ルールを更新する際に複雑な再導入を必要とするようなソリューションは、必然的にライフサイクルの大半で時代遅れになり、本来提供されるはずのセキュリティが著しく制限されることになります。複雑な環境の保守、アップデート、トラブルシューティングは、きめ細かく適切な情報を提供する必要があり、かつ効率的でなければなりません。セキュリティソフトウェアの保守に費やす時間は、潜在的な侵害に対して窓を開くことになるため、保守はセキュリティにとって見過ごされがちではあるものの、実は重要な側面となります。クラウドアーキテクチャーを保護するセキュリティソリューションは、同ソリューションが保護するプログラムと同じように、迅速に適応しなければなりません。そうでなければ、セキュリティチームは永遠にキャッチアップを続けることになります。

クラウドの状況：インストルメンテーションに関するその他の課題

クラウドは、さまざまなリソースと、それらが提供する限られた可視性への適応に必要となる拡張性と柔軟性の両方に重要なリソースを保護する新たな課題とニーズをもたらします。最新のCNAPPソリューションが対応する必要がある各種のユースケースとしては、次のものが挙げられます。

- CaaS（Container as a Service）ソリューション：アマゾン ウェブ サービス（AWS）FargateのようなCaaSソリューションは、しばしば「サーバーレス」と呼ばれます。これらのサービスは、コンテナの実行を基礎となるホストから完全に分離して抽象化するため、ワークロードのカーネルレベルの可視性を維持するための新しい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のログ：主要なクラウドプロバイダーはすべて、監査ログやイベントソースへのアクセスを提供しており、ユーザー認証や権利認証、リソースのプロビジョニングや構成の変更、ネットワークトラフィックなど、クラウド環境内におけるある程度の可視性を提供しています。

- IAMサービス：IDサービスはクラウドの境界であるため、IAMサービスにおけるアクティビティを適切に監視し、実際のユーザーアカウントとマシンアカウントの両方から送られてくる異常なアクティビティを阻止することが極めて重要となります。

- IaC セキュリティ： IaCマニフェストをスキャンして、導入前に設定ミスやセキュリティリスクを特定し、ドリフトを防止します。

- 脆弱性管理/サプライチェーンセキュリティ：ソフトウェアのサプライチェーン（SCM、CI/CD、レジストリ、ランタイム環境）全体における脆弱性を特定し、優先順位を付け、修正を行います。

- 設定およびアクセス管理： クラウド環境（クラウドリソース、ユーザー、Lambdaのようなエフェメラルなサービス）全体における設定ミスや過剰なパーミッションを管理することで、セキュリティポスチャーを強化します。

- クラウドのワークロード、ユーザー、サービス全体における脅威の検知と対応：脅威インテリジェンスで強化されたルールとMLベースのポリシーを組み合わせた、多層型の検知アプローチです。フォレンジック/IRのための詳細な監査証跡を伴います。

- コンプライアンス：PCI、NIST、HIPAAなど、動的なクラウド/コンテナ環境におけるコンプライアンス基準を満たします。

- サードパーティのサービス：複雑なクラウド環境は、多くの場合、シークレット管理サービス、マルチクラウドオーケストレーターなど、サードパーティのツールやサービスに依存しています。包括的なクラウドインストルメンテーションアプローチは、これらのツールを統合して監視することにより、セキュリティポスチャーの全体像を提供できるようにする必要があります。

最終的に最も難しい課題は、多種多様なリソースから発生するこれらすべてのイベントや検知を統合し、集約することです。多くのソリューションがこの点で十分な成果を上げていないのは、単一の限定的な焦点で構築された小規模なニッチソリューションを寄せ集めた結果であることが多いためです。

Sysdigは、クラウドを保護するためにエンドツーエンドのアプローチを採用してきました。当社は、Falcoをベースとした、単一の統合プラットフォームを構築しました。Falcoは、クラウドサービス、ワークロード、ID、サードパーティツール全体におけるエージェント型とエージェントレス型のインストルメンテーションから得られる多層的なインサイトを相互に関連付けます。当社のエージェントは、業界をリードするパフォーマンスを提供するように最適化されており、エンタープライズ規模で実証されています。これらのアダプティブな最適化により、カーネルレベルのソリューションと同様のパフォーマンスレベルを達成しつつ、ワークロードに関する優れた可視性を維持することが可能となります。

技術的になろう：
エージェントに関する知識の核

エージェント型のインストルメンテーション

ホスト上のインストルメンテーションは、ワークロードを損なわないよう、できるだけ控えめでかつ軽量でなければなりませんが、その一方で、それはシステム上で最高レベルの可視性を提供する必要があります。

このような可視性は、特権的な視点を必要とします。カーネルはオペレーティングシステムの中核であり、ハードウェアリソースを管理し、システムコール（略称：syscall）を通じてアプリケーションに基本的なサービスを提供します。syscallは事実上、システムアクティビティに関する究極の「真実を語るソース」であり、それらを監視することは、最新のインストルメンテーションの基本機能となっています。

プロセスをインストルメント化することでシステムコールイベントを収集する主な手法としては、次の3つが挙げられます。これらの手法は、精度とオーバーヘッドの点で、それぞれ異なっています。

ptrace

1つ目のアプローチは、ほとんどのデバッグツールで行われているように、ptraceや他の類似したシステムレベルのイントロスペクション手法を使用して、プロセスを一時停止して検査するものです。これらの手法は、カーネル自体によりエクスポートされた機能に基づいているため、精度が非常に高くなります。その一方で、それらはユーザースペースAPIに基づいているため、イベントデータを収集するために複数のコンテキストスイッチを必要とし、その結果、大きなパフォーマンスペナルティが発生します。また、ptraceのようなツールが、実行中のアプリケーションやワークロードのアクティブメモリをどのように変更するかに関連するリスクもあり、これは不安定性につながる可能性があります。

LD_PRELOAD

2つ目の手法は、ライブラリのダイナミックリンクを利用して、（LD_PRELOAD経由で）システムライブラリをインストルメント化されたバージョンに置き換えた上で、プロセスのシステムコールをトレースする方法です。これは比較的効率的ですが、精度が低いのが欠点です。なぜなら、この手法は、動的にリンクされたライブラリを使用しているプログラムに対してのみ機能するものであり、簡単に回避されてしまうからです。このアプローチには利点があるものの、LD_PRELOADを使用するエージェントは、監視しているシステムに不安定性をもたらす傾向があります。

カーネルレベルのインストルメンテーション

3つ目の手法は、カーネルレベルのインストルメンテーションです。これは、カーネルコンテキスト内にとどまってデータを収集するものです。このアプローチには、次のメリットがあります。

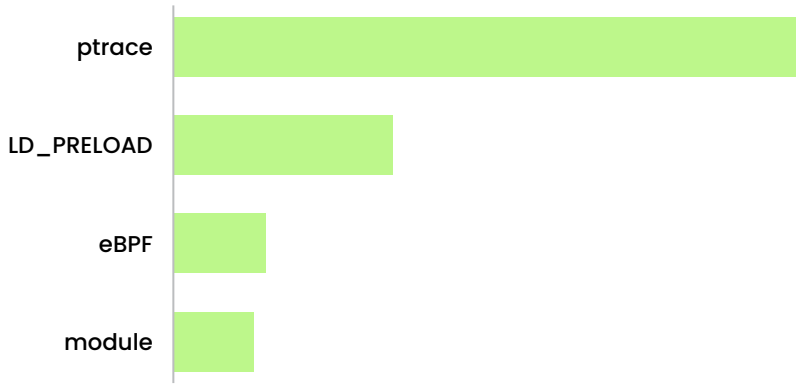
1. 可視性の向上：カーネルレベルのインストルメンテーションは、システムオペレーションに関する最も包括的な可視性を提供します。これにより、プロセスの作成、ファイルシステムのアクティビティ、ネットワークトラフィックなど、さまざまなイベントの監視とキャプチャが可能となります。このレベルの可視性を利用すると、効果的な脅威検知、パフォーマンス分析、そしてシステムの監視が可能になります。

2. 最も低いオーバーヘッド：カーネルレベルのインストルメンテーションでは、ユーザースペース手法と比べて、発生するオーバーヘッドがより少なくなります。システムが低レベルで動作することで、この手法は、より効率的にイベントをインターセプトして処理できるため、システム全体のパフォーマンスへの影響を軽減します。
3. より優れた機能：カーネルベースのエージェントは、アクセス制御ポリシーを実施し、悪意ある動作を検知して防止し、カーネルレベルのエクスプロイトや脆弱性からの保護を実現できます。カーネルに常駐することで、同エージェントは、より特権的なアクセス権を持ち、セキュリティ脅威を積極的に監視した上で、それに対応できます。

カーネルレベルでのインストルメンテーションには、主に2つの手法があります。すなわち、カーネルモジュール（従来の方法）を使うか、それともeBPF（extended Berkeley Packet Filter）プログラムを使うかです。eBPFプログラムは、カーネルレベルの仮想マシンで実行され、実行前に安全であることが検証されるため、カーネルモジュールよりも安全ですが、同じように優れた精度とパフォーマンスを提供します。ジャストインタイム（JIT）式のコンパイルのおかげで、これらのプログラムは、カーネルモジュールとほぼ同等の性能を発揮します。この効率性により、システムパフォーマンスへの影響を最小限に抑えつつ、リアルタイムの監視と分析が可能になります。

強力で柔軟なプログラミングフレームワークにより、eBPFは大きな人気を得ており、活発なコミュニティを有しています。eBPFのサポートの増加と絶え間ない進化は、特にパフォーマンスが重要な分野における新しいツールやライブラリの開発を促進しています。

カーネルレベルのインストルメンテーションにおけるパフォーマンス上のオーバーヘッド



カーネルレベルで動作するようにエージェントを設計し、特にeBPFを活用することで、強化された可視性、より低いオーバーヘッド、セキュリティの向上、安全性、パフォーマンス効率、およびプログラム可能性を提供します。これらの要素のおかげで、同ソリューションは、監視、セキュリティ、パフォーマンス解析のための堅牢で効率的なエージェントを構築するための優れた選択肢となります。

Sysdigのインストルメンテーションは、ランタイムセキュリティを実現するオープンソースソリューションであるFalcoに基づいています。Falcoは最先端のカーネルレベルのインストルメンテーションを使用しており、カーネルモジュールと最新のeBPFの両方を活用することで、業界をリードするパフォーマンスと新旧カーネルのサポートを実現しつつ、システムコールイベントに関する優れた可視性を提供します。

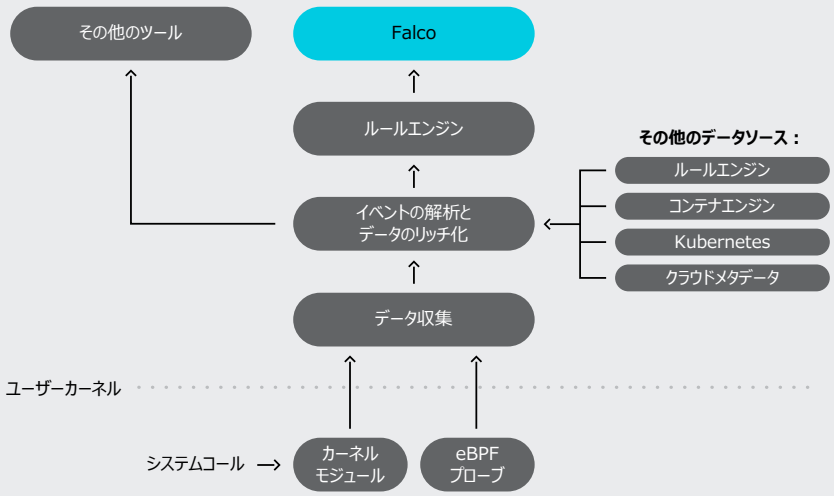
データ収集

セキュリティインストルメンテーションが提供するすべてのデータを収集することは、特にクラウド規模では困難な場合があります。さらに、収集されたデータを拡張および統合することにより、検知エンジンや人間がそれを利用できるようする必要もあります。

特に脅威の検知が主なユースケースである場合、データを収集し、利用できるようにすることは、一刻を争う作業でもあります。クラウド環境の拡張は、これらの目標を達成するためのさらなる課題となります。

セキュリティインストルメンテーションは、カーネルレベルとユーザーレベルの両方でデータを収集できる必要があります。syscallイベントから収集されたきめ細かい低レベルの詳細情報は、プロセス、ユーザー、コンテナ、Kubernetes名前空間に関する詳細情報、およびその他のすべての利用可能な相互に関連付けられたメタデータによりリッチ化される必要があり、しかも、そのリッチ化は、検知エンジンによるイベントの評価の前に行われる必要があります。さらに、データ収集は包括的でなければならず、かつ追加のデータソースをサポートするのに十分なほど強力でなければなりません。サードパーティ（たとえば新しいサービスのためのプラグイン）から送られてきたデータを取り込み、同データをリッチ化できることは、インストルメンテーションを将来も使い続けられるものにすること、そしてそれが技術的な進化がもたらす課題にも対処できることを意味します。

SysdigとFalcoは最適な方法で効率的にデータ収集とリッチ化を実行します。syscallイベントは、関連するコンテキストにより補強されます。これには、実行中のプロセスやスレッド、それらが開いているファイル、コンテナ、そして関連するKubernetesオブジェクトが含まれます。これらのコンテキストはすべて、ルールエンジンと出力で利用可能となります。これにより、意味のある正確な検知器とルールを記述することが可能となるほか、インシデント対応者がリアルタイムのインサイトを利用して高リスクなイベントを迅速かつ正確に特定し、それらの優先順位付けを行えるようになります。また、Falcoはオープンソースであるため、このような強力な機能は、ユーザーやコントリビューターのコミュニティにより拡張されていくでしょう。データはエージェントの同じホスト上で収集され評価されるため、大規模なクラウド環境であっても水平方向のスケーラビリティを容易に達成できます。



多層的なリッチ化

システムコールからデータを収集することで、個々のプロセスやオペレーティングシステムの振る舞いに関する貴重なインサイトを得ることができます。しかし、生のsyscallデータは、適切なコンテキストと情報がなければ役に立ちません。イベントをセキュリティに関連付けるものとは、そのイベントが発生したコンテキストです。

クラウド環境の包括的でコンテキストに沿った理解を提供するためには、クラウドインフラストラクチャー、Kubernetes、コンテナランタイムなど、さまざまなソースから取得した追加のメタデータとコンテキストを通じて、このデータをリッチ化することが極めて重要となります。さらに、このリッチ化は可能な限り迅速かつ効率的に行われなければならず、検知時間とエージェントのフットプリントを最小限に抑える必要があります。

多層的なリッチ化が不可欠であるコンテキストとしては、次のものが挙げられます。

1. ローカルなリッチ化：システムからコンテキスト情報を追加することで、システムコールを通じて収集されたすべてのデータに意味を与えます。単なるID番号は、プロセス名、ユーザー、ファイルパス、コネクション、コンテナ名などに変換され、これにより、人間が読み取り可能な検知ルールを記述し、意味のあるセキュリティイベントを特定することが可能となります。
2. クラウド環境のコンテキスト：クラウド環境は、さまざまなサービス、仮想化されたリソース、ネットワーク構成を伴う、動的でかつ複雑なエコシステムを導入します。仮想マシン、ストレージ、ネットワーキング、IDサービスなど、クラウドインフラストラクチャーのメタデータを取り込むことで、エージェントはシステムコールデータを、より広いクラウドコンテキスト内で意味付けできるようになります。これにより、より適切な相互関連付け、依存関係の特定、そしてクラウド環境に特有の異常な振る舞いの検知が可能になります。
3. Kubernetesオーケストレーション：Kubernetesにより管理されるコンテナ化された環境では、Kubernetes固有のメタデータでsyscallsデータをリッチ化することが不可欠となります。これには、Pod、コンテナ、デプロイメント、サービス、ラベルに関する情報が含まれま。Kubernetesによりオーケストレーションされた関係と構成を理解することで、エージェントは、コンテナの動作、ワークロードの分散、リソースの利用、Kubernetes環境に固有のセキュリティイベントに関するより深いインサイトを提供できます。
4. コンテナランタイム：コンテナは、Docker、containerd、CRI-Oなど、特定のランタイムエンジンに依存しています。これらのコンテナランタイムからのメタデータを通じてsyscallデータをリッチ化することで、コンテナのライフサイクルイベント、イメージの詳細、コンテナネットワークの名前空間、およびリソースの利用状況に関するより詳細な可視性を実現できます。このコンテキストにより、コンテナ化環境内で、より正確な監視、セキュリティ分析、パフォーマンス最適化が可能となります。
5. IDおよびアクセスコンテキスト：ユーザー情報、ロール、権限、認証メカニズムなど、IDおよびアクセス関連のメタデータを取り込むことで、システムコール活動を特定のユーザーまたはエンティティに帰属させることができます。このようなコンテキスト情報は、監査、コンプライアンス、および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役立ちます。

さまざまなソースからの追加のメタデータとコンテキストでデータを充実させることが重要です。

このような追加的なマルチドメインコンテキストを利用することで、セキュリティチームは次のことが可能となります。

- スコーピング/パーティショニング：コンテキストによって、物理ビュー（ホストなど）と論理ビュー（アプリケーション中心のビューなど）の両方に基づいて、セキュリティイベントを細分化して分析できます。
- フィルタリング：イベントをフィルタリングできます。たとえば、ラボ環境のイベントを除外することで、アラートノイズを低減できます。
- 優先順位付け：正確なコンテキストを利用することで、最もクリティカルな環境におけるアラートを優先できるようになります。例としては、インターネットに接続しているクラスターや、厳しい規制の対象となる環境などが挙げられます。
- 柔軟なポリシーの適用：コンテキストを追加することで、同じオブジェクトに対して異なる環境で特定のポリシーを記述できるようになります。例としては、開発クラスタ（緩やかなポリシー）と本番環境（制限的なポリシー）の間でコンテナイメージを規制することが挙げられます。
- 所有権の割り当て：イベントが発生する環境だけでなく、イベントが発生する抽象化レベルも正確に把握することで、セキュリティ問題を関連する作業グループに割り当てることができます。

柔軟なプラグインアーキテクチャにより、Sysdig Secureはシステムコールと並行して他のデータソースを利用できます。たとえば、AWS CloudTrailのログをリアルタイムで監視し、クラウドリソース上で疑わしいユーザーアクティビティが存在した場合にはユーザーに通知できます。ワークロード、ID、クラウドサービスを完全に可視化することで、ソース全体を通じて相互関連付けを行い、イベントを追跡して攻撃者のアクションを正確にトレースできます。さらに、Falcoルールがトリガされると、ワークロード側で即座に対応することで、悪意ある振る舞いをリアルタイムで正確に阻止できます。 .

要約

クラウドセキュリティには柔軟でスケーラブルなインサイトが必要

近年、クラウドネイティブ状況は急速に進化しており、セキュリティはますます重要な関心事となっています。クラウドネイティブのアプリケーションとインフラストラクチャーの複雑さと規模が拡大し続け、セキュリティチームがクラウドセキュリティを統合する中で、効果的なセキュリティを確保するには、エージェント型のアプローチとエージェントレス型のアプローチを組み合わせる必要があることが明らかになってきました。セキュリティチームは、ベンダーが導入しているアーキテクチャアプローチを注意深く評価する必要があります。なぜなら、セキュリティを実現するには、単に網羅的に機能を実装するのではなく、最先端のインストルメンテーションが必要となるからです。

エージェントレス型およびエージェントベースという両方のアプローチの必要性は、クラウドネイティブ環境のコンテキストにおいて特に重要となります。そのような環境では、複雑で動的なシステムが、柔軟で適応性のあるセキュリティ対策を必要とするからです。エージェント型とエージェントレス型の両方のアプローチの必要性を補強するもう1つの進展として、LambdaのFaaSサービスのような新しいタイプの抽象化の急速な採用が挙げられます。このような特殊な環境はセキュリティを念頭に設計されており、効果的な保護を提供するためにはエージェント型とエージェントレス型のアプローチを組み合わせる必要があります。

さらに、新しいアプリケーションカーネルとサンドボックスが主流になりつつあり、このような厳重にサンドボックス化された環境では、インストルメンテーションへの異なるアプローチが必要となります。これらのサンドボックスは、アプリケーションが利用できる低レベルの機能を制限することで、セキュリティを高めているため、これらの環境を効果的にインストルメント化するには、新しい手法が必要となります。幸いなことに、SysdigやFalcoのようなソリューションは、新しい技術をサポートしており、その他のプロジェクトと統合するのに十分な柔軟性を持つように予め設計されています。Falcoのオープンな設計は、最新のプロジェクトとの統合を容易にしており、そのモジュラーアーキテクチャは、サードパーティのサービスのためのプラグインを活用することで、新しい技術が出現した際に適応できることを保証します。gs

さらに、新しいアプリケーションカーネルとサンドボックスが主流になりつつあり、このような厳重にサンドボックス化された環境では、インストルメンテーションへの異なるアプローチが必要となります。これらのサンドボックスは、アプリケーションが利用できる低レベルの機能を制限することで、セキュリティを高めているため、これらの環境を効果的にインストルメント化するには、新しい手法が必要となります。幸いなこと、SysdigやFalcoのようなソリューションは、新しい技術をサポートしており、その他のプロジェクトと統合するのに十分な柔軟性を持つように予め設計されています。Falcoのオープンな設計は、最新のプロジェクトとの統合を容易にしており、そのモジュラーアーキテクチャは、サードパーティのサービスのためのプラグインを活用することで、新しい技術が出現した際に適応できることを保証します。

クラウドにおける
効果的なセキュリティには、
最高レベルの柔軟性、
パフォーマンス、有効性、
スケーラビリティが
必要です。

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、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、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、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、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。

詳細は、**sysdig.jp**をご覧ください。

デモを依頼 →

sysdig

ホワイトペーパー

WP-007-JA REV. C 9/24