VECTRA

Vectra Fusion

最新ネットワーク環境におけるシームレスなマルチクラウドの可視化

企業のクラウド導入が加速し、AWS、Azure、GCP、Oracle Cloud、IBM Cloudといった複数のクラウドサービスを横断して運用する中で、インフラおよび運用担当は可視性の欠如という課題に直面しています。

課題:

クラウドにおけるネットワークの可視化は、さまざまな要因によって困難が伴う

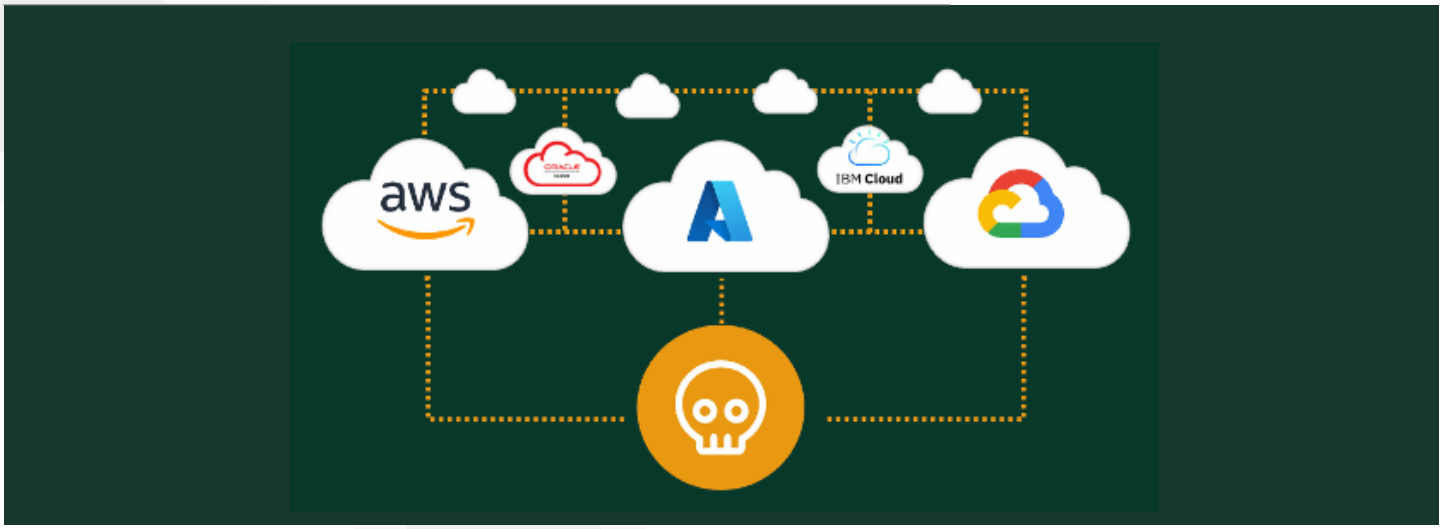
- **マルチクラウド環境における死角:** 従来のネットワーク監視ツールは動的なクラウドワークロードを十分にカバーできず、重要な東西方向トラフィックやクラウド間通信が隠れてしまいます。
- **コンテキストを欠いたインフラの複雑さ:** セキュリティ担当は数千ものアカウント、ワークロード、テナントを監視していますが、正常な状態と異常な状態を区別するための統一された可視性やコンテキストが不足しています。
- **アラートが生み出すストレスの深刻化:** プラットフォーム固有のツールは大量の区別不能なアラートを生成し、SOCチームはノイズに埋もれてしまい、真の脅威が検知されない状態に陥っています。
- **分散したツールの乱立:** 組織はネットワーク監視、クラウドセキュリティ、脅威検知、インシデント対応に別々のソリューションを導入しており、運用上のサイロ化とコストの増加を招いています。
- **検知とレスポンスの遅延:** 可視性と脅威インテリジェンスの可視性が欠如しているため、調査に数時間から数日を要し、その間に攻撃者がラテラルムーブを行い、目的を達成してしまいます。
- **クラウド成長に伴う拡張性の欠如:** センサー、タップ、エージェントに依存するレガシーアーキテクチャでは、一時的なワークロード、インフラの自動スケーリング、急速なクラウド拡張などに対応できません。

Vectra Fusionのメリット

- **シームレスなオンボーディング:** エージェント不要のソフトウェアディファインドのカバレッジにより、ワークロードやアカウントの拡張に応じて柔軟に適応します。
- **低TCO:** 仮想アプライアンスやエージェントを不要にし、クラウドフローログに伴う非効率性を排除します。
- **統合されたワークフロー:** 予防的な可視化と事後対応のレスポンスを、分析担当者が使いやすい単一のプラットフォームに統合します。

成果:

現代の攻撃者は、制御プレーンとデータプレーンの死角を悪用し、マルチクラウドネットワークを横断的に移動する



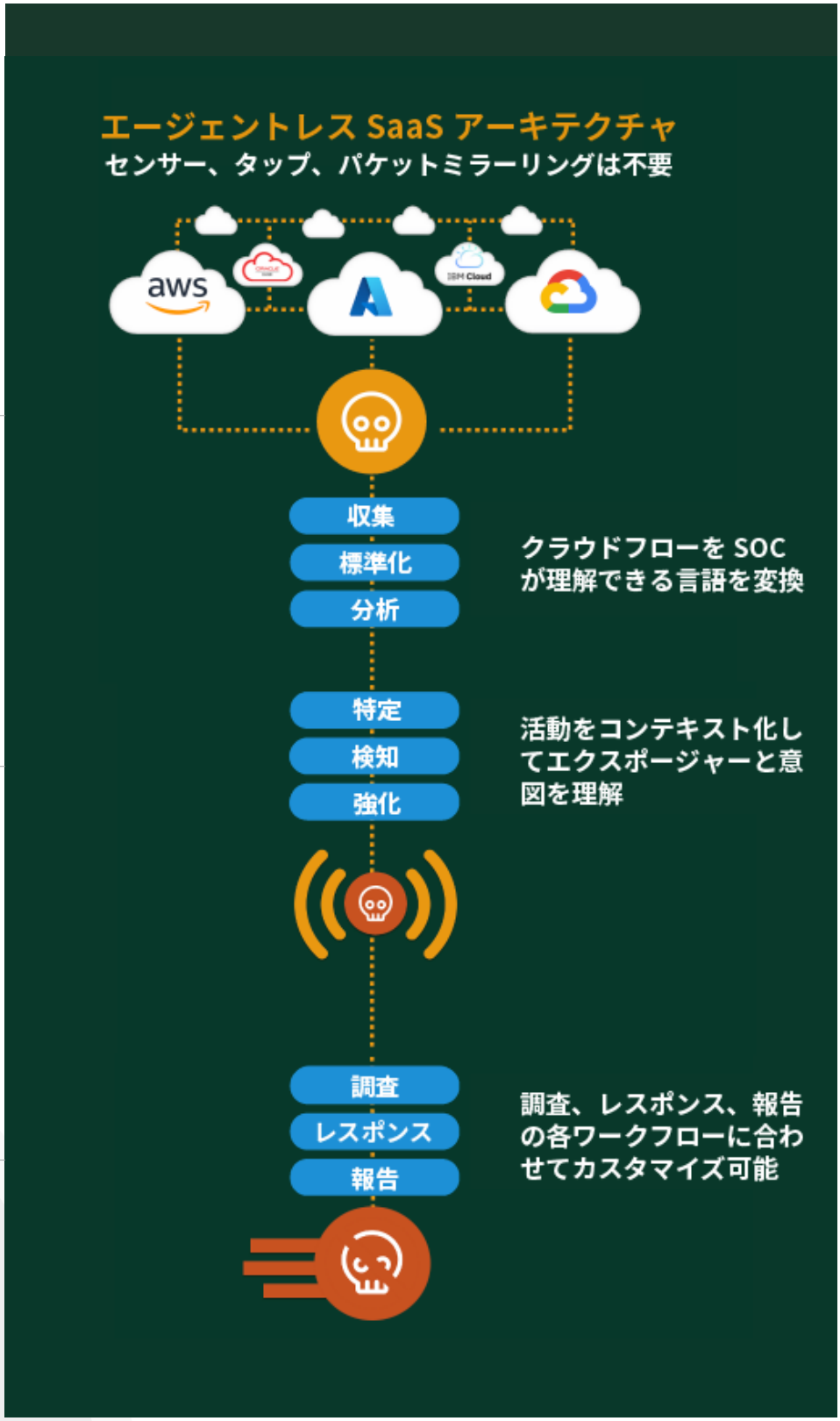
ソリューション:
Vectra Fusion

Vectra Fusionは、以下の機能によりマルチクラウドネットワーク防御を簡素化します。

- マルチクラウド環境のエクスポージャーと攻撃者の活動指標を、サイバーキルチェーン全体にわたって可視化する**カバレッジ**

- 攻撃のエクスポージャーと攻撃者の意図を、豊富なコンテキスト詳細と精度をもって可視化する**明確**な監視機能

- カスタマイズ可能な対応、修復、報告機能により、侵害前後の回復力を提供する**制御**機能



Vectra Fusionの仕組み

- **100% SaaSアーキテクチャ:**無制限のスケーラビリティを備えたソフトウェアデファインドの可視化。ハードウェアの展開が不要で、総所有コストを大幅に削減します。
- **マルチクラウドの可視性を統合:**ハードウェアやエージェントの展開なしに、AWS、Azure、GCP、Oracle Cloud、IBM Cloudを横断した完全な可視性を実現します。
- **クラウドフローログの取り込み:**ハイブリッドマルチクラウドネットワーク内のあらゆる場所から、VPCおよびVNetのクラウドフローログとDNSログをオーケストレーションし、正規化します。
- **コンテキストの強化:**クラウドプロバイダー、クラウドセキュリティプラットフォーム、エンドポイント保護プラットフォーム、その他のリソースからのコンテキスト属性でフローを強化します

Vectra Fusionがもたらす成果

さまざまな業界の組織が、可視化とシグナルの明瞭さの融合から既に測定可能な成果を上げています。

- **FICO社**:高コストなNDRアプライアンスをFusionのSaaSモデルに置き換え、完全なハイブリッド可視性を実現するとともに、検知までの時間を短縮し、運用コストを削減しました。
- **Mercury社:**クラウドファーストのフィンテック企業は、Fusionを活用してアプライアンスの乱立を解消し、コストを削減するとともに、AWS環境全体でのリアルタイム可視性を実現しました。これにより、同社のSOCは、正常なトラフィックと悪意のあるトラフィックを確信を持って区別できるようになりました。
- **グローバルB2B SaaSプロバイダー:**Fusionの自動オンボーディングを活用し、数千の新規VPCおよびVNetをカバー。監視対象外のワークロードをゼロにし、侵害の可能性を大幅に低減しました。

業界の専門家もこのアプローチの価値に気がついています。アナリストは、NDR (ネットワーク検知とレスポンス) がパケット検査を超えて、フローログ、クラウドテレメトリ、アイデンティティデータを含むべきであることを強調しています。ソートリーダーは、可視化と検知の融合こそが、SOCがハイブリッドおよびマルチクラウド企業を防御する新たなモデルであると述べています。

Vectra Fusion の詳細

Vectra AIについて

Vectra AIは、現代のネットワークを最新の攻撃から保護するAI主導のサイバーセキュリティを提供しています。高度なサイバー攻撃が既存の制御を回避し、検知を逃れて顧客のデータセンター、キャンパス、リモートワーク、アイデンティティ、クラウド、IoT/OT環境にアクセスした場合、Vectra AI プラットフォームは攻撃のあらゆる動きを監視し、リアルタイムで点と点を結び付けて、侵入を阻止します。また、当社はAIセキュリティに関する35件の特許を取得し、MITRE DEFENDで最も多くのベンダーリファレンスを誇ります。他のツールでは検知できない攻撃を見つけ、阻止するために世界中の組織がVectra AIを活用しています。詳細については、 https://ja.vectra.ai/ をご参照ください。

ja.vectra.ai/　　お問い合わせ:info-japan@vectra.ai