VECTRA
SECURITY THAT THINKS.®

データシート

Detect for AWS

課題

常時接続型である現代のデジタル主体のビジネスにおいては、スピードと俊敏性が必須です。そのためにITチームは、従来オンプレミス型であったインフラストラクチャをクラウドネイティブアーキテクチャへと移行しています。その一方で、多くの場合、セキュリティが十分とは言えない状態です。

DevOpsの台頭、PaaS（Platform as a Service）やIaaS（Infrastructure as a Service）の利用が、デジタル主体のビジネスの基盤となっており、今では標準となっています。さらに、従来、セキュリティは専門のチームが担当していましたが、現在は開発者が担当することが多くなっています。その結果、スピードと俊敏性が高まると同時に、セキュリティ問題のリスクも高まっています。パブリッククラウド環境は非常に複雑で、常に変化し続けています。今の状況で、クラウドアプリケーションの安全なデプロイメントは不可能なのです。

2025年までに、クラウドのセキュリティ障害の99%は顧客に降りかかると言われています。[1]

2025年までに発生するクラウドセキュリティ障害の99%は、顧客自身の責任になるとガートナー社は予測しています。クラウドプロバイダーの責任は、可用性とインフラストラクチャーであり、ユーザー、アプリケーション、データのセキュリティに対しては責任がありません。たとえ専門のセキュリティチームを擁する企業であっても、レガシーな運用や従来のセキュリティ手法が、パブリッククラウドにうまく対応できないことにすぐに気がつくはずです。保護や監査が必要なクラウドの領域は常に変化しており、セキュリティのギャップ（死角）はますます拡大しています。

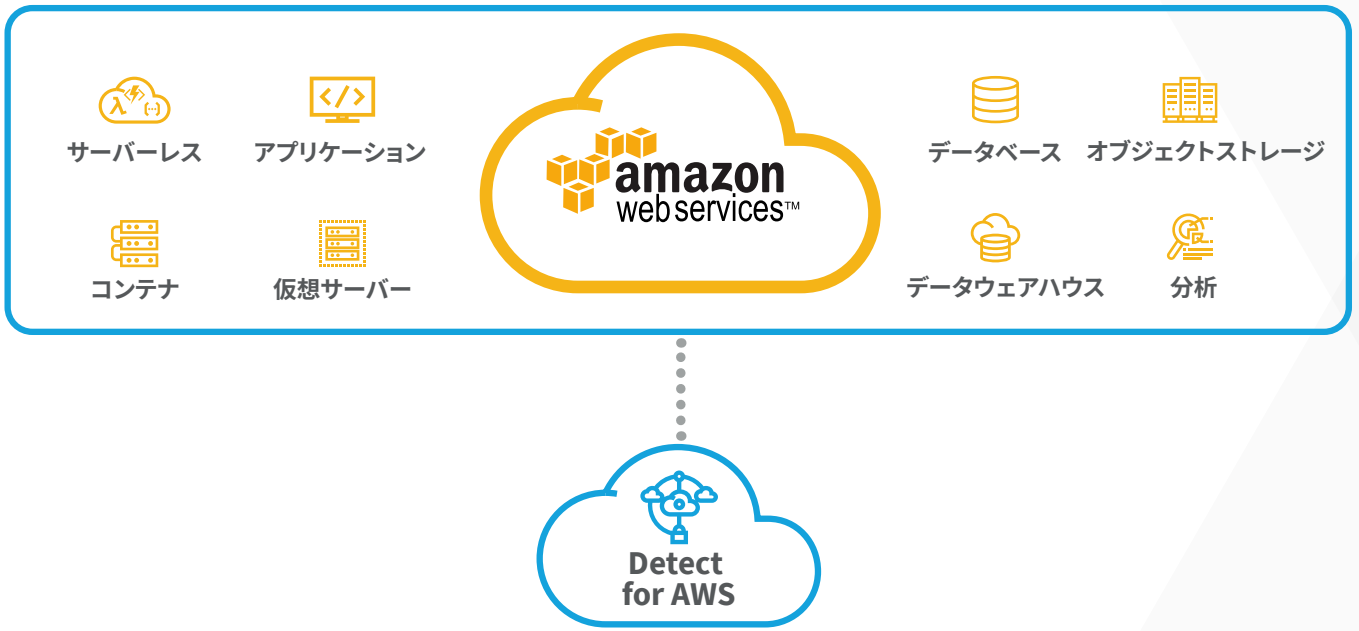
[1] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

71% **AWSのお客様の71%が、4つ以上のAWSサービスを利用しています。**

ハイライト

- 脅威を検知して優先順位をつけることができる初の振る舞い型AIを用いて、**AWSのIaaS、PaaS上で稼働するエンタープライズ向けアプリケーションやデータに対する脅威を迅速に検知**します。
- シグネチャや仮想タップ、静的なポリシーに依存しないエージェントレスなカバレッジにより、**数分でデプロイメントが可能**です。
- 過去のセキュリティデータを利用して**攻撃を調査し、関係するロールやアカウントを特定**します。これによりチームは、すべてのロールやアカウントを通じて攻撃の進行を追跡きるので、広範囲の障害を引き起こすことなく、攻撃を開始した場所に戻って停止することができます。
- **AWS上で動作するアプリケーションに対する攻撃への対応**を、AWSのネイティブ機能や他のセキュリティソリューションとの統合を用いて**自動化する**ことで、エージェントに頼ることなく、また業務を中断することなく、脅威を軽減することができます。

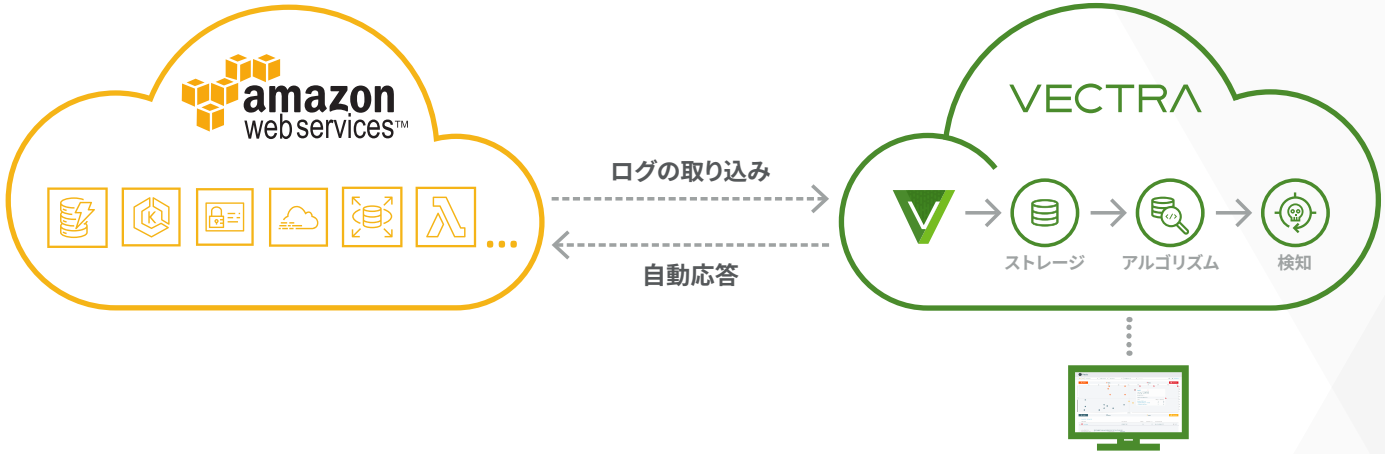
Vectra AIによってセキュリティギャップを解消



クラウドネイティブなVectra Detect for AWS SaaSは、セキュリティギャップを解消します。Detect for AWSは、攻撃者の振る舞い、クラウドID、ロール、アクセスポリシー、そしてストレージ、コンテナ、サーバーレスなどのワークロードのデプロイメント構成を観察し、理解することで、運用を中断することなく攻撃を発見して、阻止します。

シグネチャや静的なポリシー、エージェントによる運用上の影響に依存せず、振る舞い型AIを使用した初の脅威検知ソリューションなので、組織は安心してより多くのアプリケーションを大規模に移行、開発、デプロイメントできます。さらに、デプロイメント時にもたらされる、セキュリティ上の侵害リスクを最小限に抑えることができます。

Detect for AWSは、振る舞いモデルを用いて、業務を中断することなく攻撃を発見し、停止させることができる唯一のAI駆動型ソリューションです。

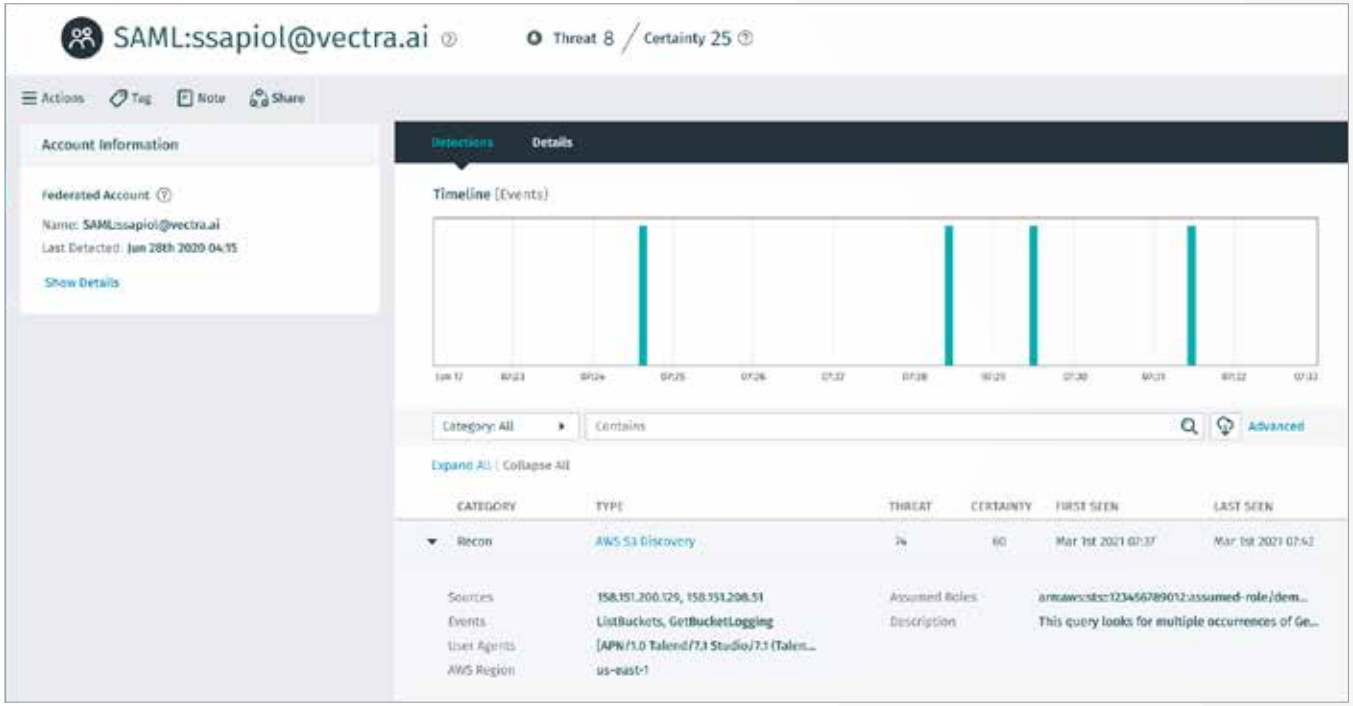


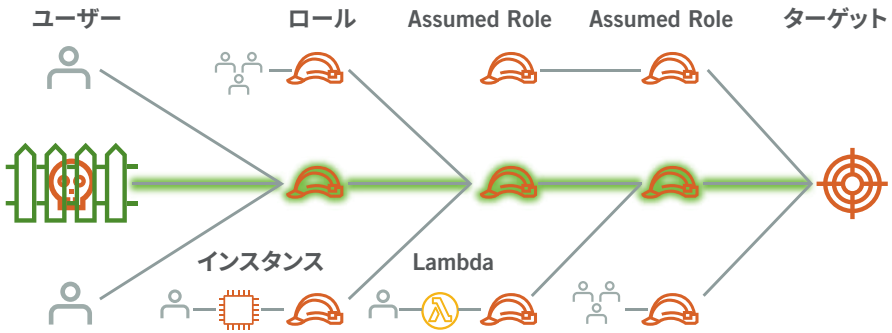
MITRE ATT&CKフレームワークを完全カバー

MITRE ATT&CKマッピング

- ネイティブAWSインテグレーションでは、EC2インスタンスの作成や削除、S3バケットの公開など、ユーザーやリソースとAWSサービスとのやり取りを監視します。
- 数分で終わるエージェントレスのセットアップにより、Vectra AIはアクティビティを分析し、特許取得済みのAI駆動型の攻撃者の振る舞いモデルを用いて、顧客のAWS組織の保護を開始します。
- 複数の地域にまたがるセキュリティビューを統合し、世界中の動きをまとめて把握することができます。
- ワンクリックですぐに調査ができることで、インテリジェントなクエリと履歴ログを提供し、調査を加速します。
- 使用量は、分析したアクティビティログ1GBあたりにライセンスされます。

Vectra AIは、人工知能（AI）を使って、同じAWSアカウントまたはクロスアカウント上で、ローカルまたはフェデレーションに関わらず、委任されたロールのチェーンを通じて攻撃者を追跡します。業界初のKingPinテクノロジーは、受信したすべてのアラートにおいて、どのプリンシパルが攻撃を仕掛けたかを明確に示し、調査と修復のための明確な次のステップを提案します。



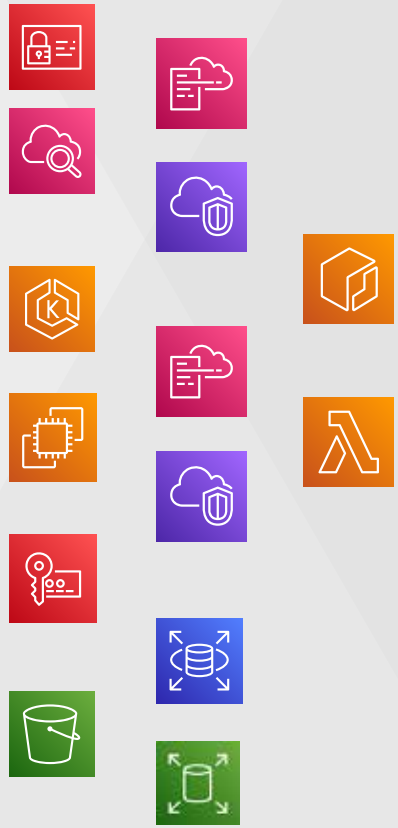


受信したすべてのアラートにおいて、どのプリンシパルが攻撃を仕掛けたかを明確に示し、調査と修復のための明確な次のステップを提案します。

AWSに対する攻撃への対応

戦術	攻撃例
初期アクセス	不審な認証の使用、Torからのアクセス、ルートアクティビティ
永続化	既存のユーザーやサービスの乗っ取り、外部からのアクセスの許可
権限昇格	ユーザーへの許可の追加、完全なコンソール制御への移行
回避	セキュリティツールの無効化、ロギングの無効化、セキュリティ制御の回避
認証情報アクセス	サービスから認証情報を取得
探索	ユーザー権限、組織の詳細とサービスの探索
収集	S3バケットとデータストアの検索
影響	ファイルを暗号化して身代金を要求する、クリプトマイニング
持ち出し	S3バケットからのダウンロード、インスタンスデータの一般公開

対象サービス例



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