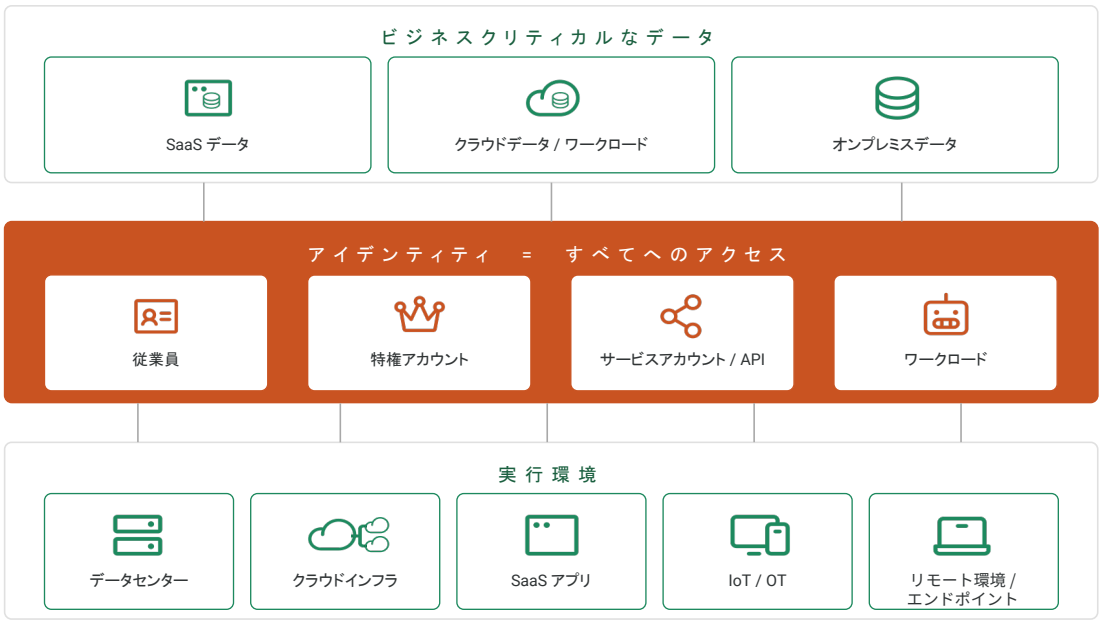
検知は効果的である。
ただし、不完全では無意味である。

攻撃者はどのように環境を横断しているのか。防衛側は何をすべきなのか。

現代の環境

企業は、単一の境界線の内側には存在しない

攻撃者は、レイヤーの間に境界線を見ていません。しかし、多くの検知スタックは境界ごとに分断されています。



セキュリティスタックに存在する3つのギャップと Vectra AIが提供すること

課題 1

異常が見えない

攻撃者はPowerShell、RDP、署名済みバイナリなど、正規のツールを悪用します。いわゆる「Living off the Land」（LotL：環境寄生型）です。操作自体はすべて通常業務に見えます。

VECTRA AI による分析

アイデンティティとネットワーク全体の振る舞いを分析し、こうしたツールの悪用をリアルタイムで検知します。

課題 2

認証が正常に見える

認証情報は正しく、MFAも承認されています。ログインそのものは正当です。ただし、その利用者は想定している本人ではありません。すべての認証チェックは「正常」と判断します。

VECTRA AI による理解

接続後のセッションの振る舞いを理解し、通常利用からの逸脱を検知します。

課題 3

移動が見えない

ラテラルムーブメントは、SaaS間連携、フェデレーション認証、OAuth、サービスアカウントなどの信頼された接続を経由して行われます。アーキテクチャ上、それらは見えません。

VECTRA AI による相関

東西方向の通信、クロスアカウントのAPI コール、SaaS 間のピボットを相関させ、ひとつの攻撃チェーンとして再構成します。

Vectra AIが提供すること

ネットワーク、アイデンティティ、クラウド全体にわたるリアルタイム検知

EDR、SIEM、IAMだけでは実現できない検知レイヤーを提供します。

1. **ネットワーク：**ラテラルムーブメント、暗号化通信を利用したC2通信、業務トラフィックを装ったデータ持ち出し、エージェント不要でリアルタイムに検知。
2. **アイデンティティ：**Microsoft Entra IDにおける特権悪用、フェデレーション操作、 OAuth悪用、セッショントークンのリプレイ攻撃、認証後の振る舞いを分析。
3. **クラウド：**AWSおよびAzureのコントロールプレーン活動、クロスアカウントAPIの利用パターン、サービス間のラテラルムーブメント、ログ集約ではなく、振る舞いベースで相関分析。

Vectra AIが実現する成果

2025年 Vectra AI 顧客調査より

391%	6 か月	$340万	40%	60%	69.4%	99.9%
3 年 のROI	投資回収期間	年間効果額	SOC運用効率の向上	アラート対応時間の削減	セキュリティ侵害の削減	生産性損失の回避

99 「Vectra AI導入前はアラートがまったくなく、レッドチームによる侵入は年次レポートで初めて知る状況でした。Vectra AI導入後の最初の1年で、当社はレッドチームを検知し、排除し、完全に阻止することができました。」

グローバル化粧品メーカー

自社環境で検証する3つの方法

Blue Team Workshop

ハンズオンセッション。実際の攻撃シナリオに取り組みます。3つのトラック：ハイブリッドネットワーク、AWS、M365 + Entra ID。CPEクレジット取得可能。

1.5〜3 時間

Offensive Security Assessment

当社のオフェンシブチームが、お客様の環境で実際の攻撃シナリオを再現します。現在の防御システムがどれだけの脅威を検知できるかを測定します。無料で提供。(本格的なレッドチームではありません。)

約 1 週間

Proof of Value

お客様の環境の一部にVectra AIを導入し、さらに攻撃的なセキュリティ評価を実施します。実際のデータ、お客様のネットワーク使います。

約 4 週間

Vectra AI について

Vectra AIは、AIネイティブのセキュリティと可視化のリーダーです。当社は、組織にネットワークのリアルタイムな可視性、重要な動作に関する明確な洞察、そしてリスクが影響を及ぼし始める前に対応できる能力を提供します。オンプレミス、マルチクラウド、ID管理、SaaS、エッジ、IoT/OTインフラストラクチャを接続することで、Vectra AIは組織の露出を減らし、検知とレスポンスを加速し、AIを活用してセキュリティ運用を自動化します。10年以上にわたるAIと機械学習のイノベーションと39件の特許におけるリーダーとしての実績を持つVectra AIは、セキュリティチームがAIを活用した新たな攻撃に先手を打ち、運用効率を高めること、そしてますます複雑化するAI主導の世界において回復力を発揮することを支援します。詳細は ja.vectra.ai をご覧ください。

お問い合わせ: info-japan@vectra.ai