VECTRA
SECURITY THAT THINKS.®

データシート

Detect for Office 365 and Azure AD

Member of
Microsoft Intelligent
Security Association
Microsoft

Microsoft Office 365は、組織において、電子メールだけではなく、OneDrive、SharePointの文書や機密データの保管場所としても機能するため、攻撃者にとっては、価値の高いターゲットです。

フィッシング対策のためのメールセキュリティや、アカウントを保護するための厳格なパスワードポリシー、さらには多要素認証 (MFA) の導入が進んでいるにもかかわらず、毎月30%の組織がアカウント乗っ取りの被害に遭っているなど、防御ツールだけでは不十分です。

Detect for Office 365 and Azure ADは、クラウドネイティブなアプローチをとることで、予防的なセキュリティに頼ることなく、既知および未知の攻撃を、侵害につながる前に検知・阻止します。

防御的なセキュリティでは不十分であるため、多くの企業は、環境内の攻撃者が拡散したり被害を及ぼしたりする前に発見して阻止することができる検知および対応ソリューションに投資しています。

業界初のクラウド向けネットワークの検知および対応ソリューションであるVectra Detect for Office 365 and Azure ADは、現在、パブリッククラウド、プライベートデータセンター、エンタープライズ環境からMicrosoft Office 365までを保護します。この受賞歴を持つアプローチでは、セキュリティ研究とデータサイエンスを組み合わせて活用し、Azure ADにおける実際の攻撃者の振る舞いやアカウント権限の乱用を理解するAIを作成しています。Detect for Office 365 and Azure ADは、クラウドネイティブなアプローチをとることで、防御的セキュリティに頼ることなく、既知および未知の攻撃を、侵害につながる前に検知して阻止します。

30%

メールセキュリティ対策にもかかわらず、毎月30%の組織がアカウント乗っ取りの被害に遭っています。

ハイライト

Office 365における攻撃者の検知と阻止：

Vectraは、攻撃者の振る舞いやアカウントの権限を理解するAIを活用することで、Office 365への攻撃ベクトルを幅広くカバーし、侵害に対して終止符を打つことを可能にします。

クラウドSaaSアプリケーションにおける侵害のリスクを低減：

連携したSaaSアプリケーションにおけるアカウント乗っ取りや特権の乱用を、エージェントレスで監視します。

セキュリティの主導権を取り戻す：

攻撃者はサイロ化した中だけで活動するわけではありません。それに対抗するセキュリティソリューションも同様であるべきです。Vectraであれば、Office 365とローカルネットワークの間を移動しながら進行する攻撃を追跡し、阻止します。

攻撃者はAzure ADアカウントにアクセスすると、簡単に動き回ることができるようになります。企業内ドメインを起点とした新たなフィッシング攻撃や、悪意のあるコードを含む共有ファイルは成功率が高く、Office 365とエンドポイントの両方を介して急速に拡散することになります。そこで、Vectraプラットフォームによってエンタープライズ全体をカバーすることで、企業はクラウドから現場まで、インフラ全体の可視性を取り戻すことができます。攻撃が進行しまった場合でも、エンドポイントとOffice 365の間を移動する際に、Vectraによって脅威のフルコンテキストに先手を打ち、迅速に対応することができます。

攻撃者の振る舞いを自動的に検知し、優先順位をつけ、調査を加速し、先を見越した脅威探索を可能できるVectra Detect for Office 365 and Azure ADによってMicrosoft Office 365のセキュリティを制御します。

Office 365における攻撃者のキルチェーン全体を幅広くカバー

Detect for Office 365 and Azure ADは、Office 365、Azure AD、SharePoint/OneDrive、Teams、Exchangeなどの複数のサービスからアクティビティログを取り込みます。Vectra AIは、Office 365アプリケーションのセマンティクスを深く理解し、教師あり・教師なしの機械学習モデルを活用します。ログイン、ファイルの作成・操作、DLP設定、メールボックスのルーティング設定と自動化の変更などのイベントを分析することで、キルチェーン全体にわたる攻撃者の振る舞いパターンを正確に発見します。その結果、異常アラートではなく、高精度の実用的な検知が行われ、これまでに見たことのない新しい攻撃者であっても、高い信頼性を持って正確に発見することができます。検知された結果は、関係するすべてのアカウントデバイスに関連付けられ、セキュリティチームに優先順位付けと迅速な行動のための情報を提供します。

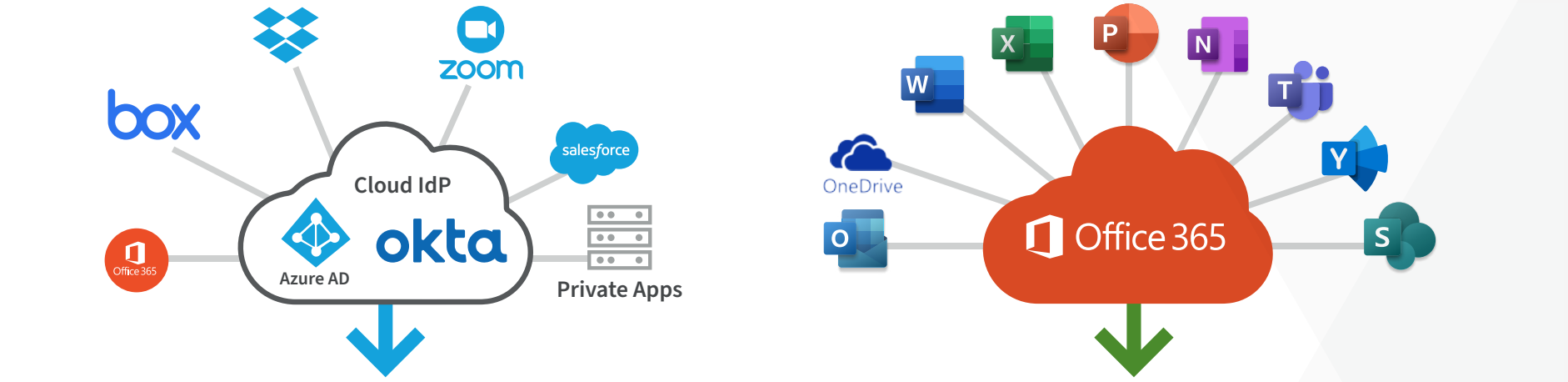
セキュアなAzure AD環境へ

Azure AD のような IdP は、急速に成長し、組織のインフラストラクチャの中で、最も重要な部分となっています。Azure ADは、SAMLやOpen ID Connect（OIDC）を介してユーザーやアプリケーションのための中央認証エンジンであるだけでなく、SCIMなどのプロトコルを使用してアカウントを追加または削除することができます。そのため、攻撃者にとって理想的なターゲットとなります。特権アカウントやIdP 自体を侵害すれば、攻撃者は管理されているクラウドやハイブリッド環境にほぼ無制限にアクセスできるようになるのです。

IdPは、MFAのようなアカウントへの防御的セキュリティの追加や、SaaSアプリケーションのオンボーディングとオフボーディングの自動化が主な目的であることから、それ自体への攻撃や特権アカウントの侵害を検知する能力に欠けています。

そこで、Vectraはアクティビティログを取り込むことでAzure ADを保護し、教師あり・教師なしの機械学習モデルを活用して、ログイン、構成および自動化の変更などのイベントを分析します。不可能な動きやVPNの使用のような単純な検知をはるかに超えて、認証トラフィックとユーザーの振る舞いから学習し、攻撃者の振る舞いパターン、悪用されたAPIやサービスアカウント、攻撃者のキルチェーン全体での異常なユーザーの振る舞いを正確に検知します。

Vectra AIは、Office 365アプリケーションのセマンティクスを深く理解し、教師あり・教師なしの機械学習モデルを活用します。



アクセス前	アクセス	固執	回避	発見	ラテラルムーブ	持ち出し	インパクト
ブルートフォース攻撃の試み	ブルートフォース攻撃	MFAの無効化	ログ無効化の試み	特異なeDiscovery検索	不審な操作	疑わしいメールの転送	ランサムウェア
無効化されたアカウント	不審なサインオン	信頼できるIPの変更	セキュリティツールの無効化	特異なコンプライアンス検索	リスクのあるExchange操作	外部チームへのアクセス	
	Tor活動	管理者アカウントの作成			内部スピアフィッシング	不審なダウンロード	
	特異なスクリプトエンジン	アカウントの操作			ファイルポイズニング	不審な共有	
	不審なOauthアプリ	冗長アクセス			DLLハイジャック	不審なSharePoint操作	
	不審なTeamsアプリ				Power Automate HTTP	終了前の持ち出し	
						eDiscovery持ち出し	
						不審な Power Automate Flow	

Office 365の検知
Azure ADの検知

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