VECTRA
SECURITY THAT THINKS.®

データシート

Vectra Recall：脅威のハンティングを支援する最も効率的なソリューション

Vectra®が提供するサイバー攻撃の検知と脅威ハンティングのプラットフォームのコアとなるVectra Recall™ は、クラウドやデータセンターのワークロード、ユーザーやIoTデバイスに対して、AIを活用して脅威のハンティングを実施する最も効果的な手段です。

Vectra Recallは、セキュリティ情報で強化したネットワークメタデータの包括的なソースを活用することで、経験豊富なセキュリティアナリストや脅威ハンティングのプロフェッショナルによる徹底したインシデント調査を支援します。

Vectra Recallのメタデータは、IPアドレスだけではなく、ホストとも関連付けられています。そのため、インシデントの発生時にそのIPアドレスを使用していたホストデバイスを特定するために、DHCPのログを追いかけたり、調査中に発生したIPアドレスの変更履歴をたどるなどの手間は不要になります。何よりもスピードが優先される調査においても、デバイスを直接検索できることによって、調査の時間が大幅に短縮されます。

また、Vectra Recallは、特権アクセス分析（Privileged Access Analytics）を活用して振る舞いを自動分析し、AIを利用して特権を持つエンティティを特定し、承認された使用と悪意を持つ使用を区別します。Privileged Access Analyticsは、Vectraプラットフォーム全体で活用でき、Vectra Stream™ とVectra Recallでは検索可能なセキュリティ強化機能として、Vectra Detect™ では検知機能として利用することができます。また、Vectra REST APIを通じてその属性にアクセスすることで、カスタムユースケースもサポートできます。

Vectra Recallによって、セキュリティチームはネットワークメタデータを使って、Vectra Detectあるいは他のセキュリティイベントや最新のインテリジェンスが提供する初期の兆候から、脅威の根本原因をたどることができます。セキュリティ情報で

Vectra Recallは、経験豊富なセキュリティアナリストや脅威ハンティングのプロフェッショナルによる徹底したインシデント調査を支援します。

ハイライト

- セキュリティ情報で強化したネットワークメタデータ、関連ログ、クラウドイベントをリアルタイムに収集、保存して、クラウドからエンタープライズに至るまで、サイバー攻撃に関する情報の高度な可視化を実現します。
- セキュリティ情報で強化したネットワークメタデータを使用することで、過去に遡って脅威のハンティングを実施することができます。
- セキュリティツールが検知したインシデントを詳細に分析することで、影響を受けた可能性があるホストデバイスやアカウント、また外部の関係者を特定することができます。
- クラウド上に必要なメタデータを無制限に保存し、検索することが可能です。

強化したネットワークメタデータは、ホスト名からでも検索することが可能です。

Vectra Recallは、クラウドからエンタープライズに対して行われる個々の通信のトランザクションレコードに似ています。しかし、パケットのペイロードではなく、メタデータの履歴を収集し保存することで、データのプライバシーを守り、GDPRなどの要件にも対応できます。

また、Vectra Recallは、クラウドサービスとして提供されるため、ビッグデータを扱うためのインフラストラクチャーの購入やインストール、管理などは一切不要です。ネットワークメタデータは、クリックするだけで簡単にVectraのクラウド環境へ転送することができます。

機能概要

- セキュリティ情報で強化したネットワークメタデータや関連ログ、クラウドのイベントをリアルタイムに収集・保存して、**脅威ハンターを支援**し、高度なサイバー攻撃に関する深い知識を十分に活用できるようにします。
- デバイスやワークロード、ホスト名を関連付け、IPアドレスに変更があった場合でも、**デバイスのアクティビティに対するインテリジェントな調査**が可能になります。
- 全てのクラウドやデータセンターのワークロード、ユーザーやIoTデバイスなど、**インフラストラクチャー全体のアクティビティを可視化**することができます。
- Vectraが管理する**クラウドインフラストラクチャーによって、必要なだけ無制限**にメタデータを保存し検索できます。

DetectとRecallの連携

セキュリティアナリストは、AIを使ったサイバー攻撃の検知および対応の自動化を支援するVectra Detectが提供する再現性に優れた実用的なインシデントを対象に、Vectra Recallでさらに踏み込んだ調査を行うことができます。

また、より上席のセキュリティアナリストは、サードパーティのセキュリティソリューションからのアラートに基づく脅威のハンティングや、最新の脅威インテリジェンスによる過去に遡った高度なハンティングを行うことができます。

	サイバー攻撃の検知	調査とAI支援による ハンティング
製品	Vectra Detect	Vectra Recall
目的	侵害されたホストを調査の 開始点として特定	手動での調査により 検出に失敗した脅威を見つける
対象範囲	初期検知 → 検証検知	完全な調査
ニーズ	リアルタイムで忠実度の高い シグナルそして自動化	履歴(ヒストリカル)メタデータの 360度ビューと効率的な検索

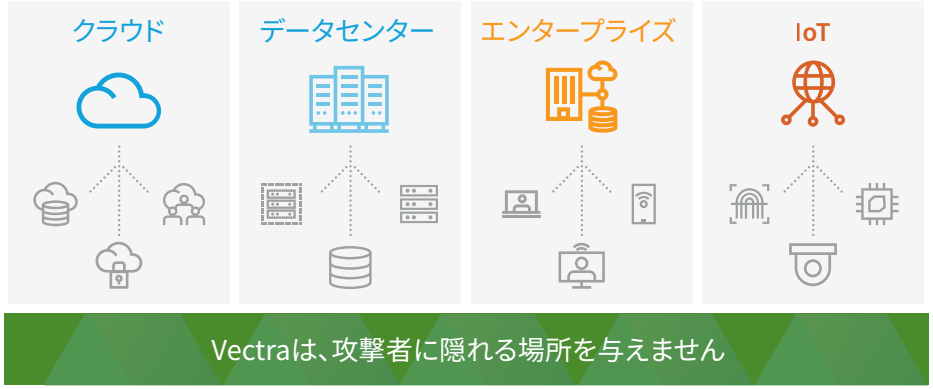
Vectra Recallの仕組み

企業の全貌を高い忠実性で可視化。Vectra Recallは、全てのパケットからメタデータを抽出し、検索や分析のためにクラウドに保存して、ネットワークトラフィックを可視化します。ネットワーク上でIPアドレスを使用する全てのデバイスを特定、トラッキングして、データをどのような時間の範囲でも保存しておくことができます。

取得したメタデータには、全ての内部（横方向）のトラフィック、インターネット（縦方向）とのトラフィック、仮想インフラストラクチャーのトラフィック、クラウドコンピューティング環境のトラフィックが含まれています。

このような可視化は、ラップトップやサーバー、プリンター、BYOD、IoTデバイス、またオペレーティングシステムやアプリケーション、さらにはデータセンターとクラウドの仮想ワークロード、SaaSアプリケーション間のトラフィックにまで及びます。

システムや認証情報、そしてSaaSのログを使って、ネットワークメタデータのコンテキストを強化し分析することで、システムやユーザーを正確に特定することができます。



Vectra Recallは、セキュリティ情報で強化したメタデータをクラウド、ユーザー、IoTのデバイスから収集します。

脅威のハンティング

AIを活用して高度な脅威のハンティングを支援するVectra Recallは、Vectra Detectが攻撃者を検知した場合や、セキュリティ分析によってデータ侵害のインジケーターや異常値が検出された場合に活用することができます。

侵害のインジケーターを使ったハンティング

セキュリティアナリストは、メタデータの全検索機能と無制限のデータストレージを持つVectra Recallによって、ユーザーのエージェントやIPアドレス、ドメインなど、メタデータに侵害のインジケーターが存在しないかどうかを判断できます。

また、リモートマシンからサーバーに対するPowerShellコマンドやリモートサイトからの特定タイプの接続の存在など、Vectra Recallはより詳細な情報を提供することで、効率的な脅威ハンティングを可能にします。

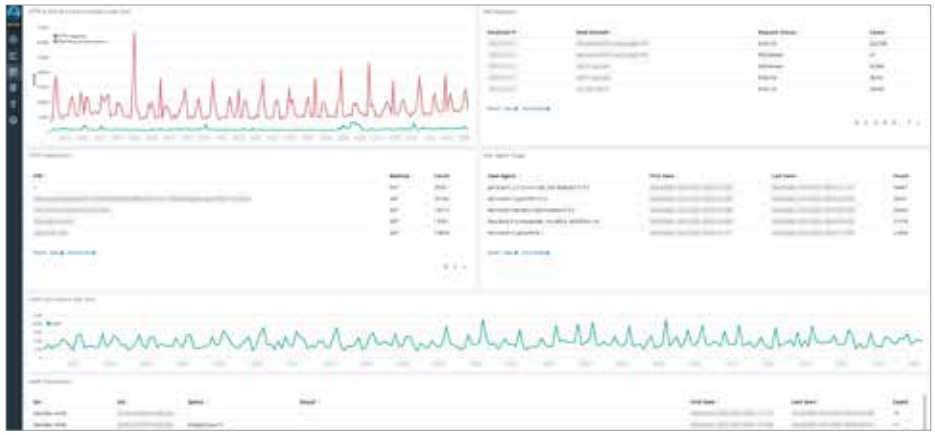
異常な振る舞いのハンティング

Vectra Recallは、脅威ハンティングのプロフェッショナルに対して、特定した異常な振る舞いに関する情報をわかりやすい視覚的なグラフで提供します。次のような異常な振る舞いが、Vectra Recallによって明らかになります：

- TCPやUDPのポートとアプリケーションの例外的な組み合わせ
- 異常に高い接続レート
- 試行錯誤を示すインジケーター
- 新たなビーコン活動
- 接続回数、ログインの失敗数、過度の内部および外部のデータ転送に対する量的なしきい値

「異常な量」のデータが、「例外的なIPアドレス」を使って転送されているなど、異常値を前述の異常な振る舞いの組み合わせで表現する場合もあります。

Vectra Recallは、メタデータの全検索機能と無制限のデータストレージを提供します。



脅威ハンターは、Vectra Recallによって異常な振る舞いを特定できます。

確証性に優れたインシデント調査

Vectra Recallによって、セキュリティアナリストは、さらに詳細で徹底的なインシデント調査を、驚異的な効率で進められるようになります。

セキュリティアナリストは、Vectra Recallやサードパーティのセキュリティ製品が検知した一連の攻撃や、過去のネットワークメタデータにある検索可能で高品質な脅威インテリジェンスを容易に辿って活用することができます。

Vectra Detectやサードパーティのセキュリティ製品からイベントやアラートを受け取ったVectra Recallは、セキュリティアナリストが全てのワークロードやデバイスのアクティビティを全方位ビューで確認できるようにします。

セキュリティアナリストは、インシデントに関する完全なコンテキストや関連するデバイス、アカウント、ネットワーク通信に関する詳細などに基づいて、かつてないほど優れた効率でインシデントを調査することができます。

ホストベースの調査

Vectra Recallによって、セキュリティアナリストは脅威を検知した時間の前後におけるホストデバイスのアクティビティを特定し、ホストデバイス全体で振る舞いの変化を把握することができます。

Vectra Recallの視覚的なグラフや検索機能は、他のホストデバイスやアカウント、外部ドメインとIPアドレスなど、インシデント全体の状況を提示します。

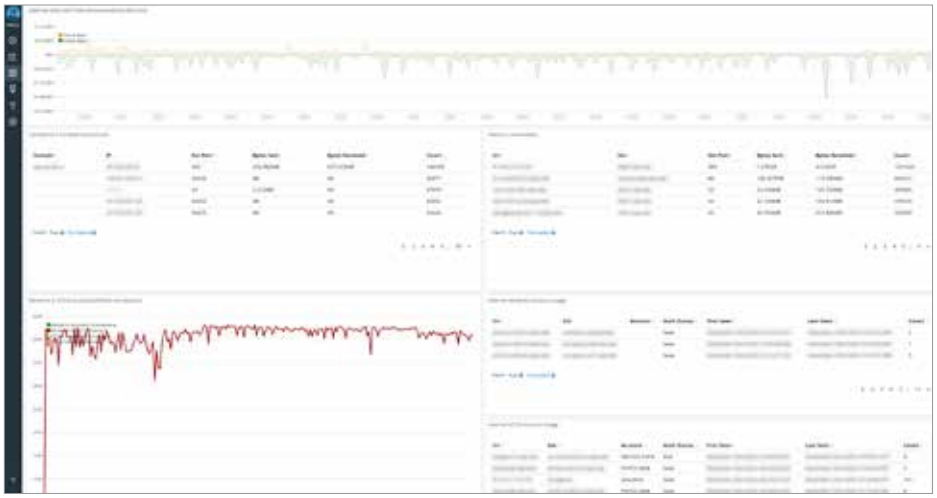
これにより、セキュリティアナリストは各種の不審な振る舞いを容易に順序付けして、他のホストデバイスに紐づく証跡を特定したり、その過程にある侵害のインジケーターを効率的に検索できます。

アカウントベースの調査

Vectra Recallは、特定の期間に侵害を受けた可能性のあるアカウントの全てのユーザーとアクションや、標的に対するアクションを特定するための詳細な情報をセキュリティアナリストに提供して、アカウントベースの調査を強化します。

また、セキュリティアナリストは、Vectra Recallが提示するサイバー攻撃全体の状況を参照しながら、他のホストデバイスに侵害されたアカウントが存在しないかどうかといった調査に役立てることができます。

Vectra Recallは、セキュリティアナリストが全てのワークロードやデバイスのアクティビティを全方位ビューで確認できるようにします。



Vectra Recallの提供する詳細な情報によって、アカウントベースの調査を強化することができます。

標的となるドメインとIPアドレスの調査

攻撃対象として大きな侵害を受けたホストデバイスが特定できたら、次に重要になるのが、その他のホストデバイスが攻撃に使用されている悪意あるドメインやIPアドレスと通信を行っていないかどうかという点です。

Vectra Recallは、全てのアウトバウンドとインバウンドの通信をトラッキングします。これによりセキュリティアナリストは、特定の期間に同じドメインやIPアドレスと通信を行っていたホストデバイスや、通信中に発生した内容を特定できます。

攻撃者の振る舞いに関する広範なコンテキスト

Vectra Detectが特定したサイバー攻撃の調査においては、インシデントの中で発生した全てのネットワークアクティビティの詳細を理解することが重要です。

セキュリティアナリストは、Vectra DetectとVectra Recallをワンクリックで切り替えながら、悪意あるネットワーク通信に関する詳細で有益なコンテキストを取得することができます。

Vectra Detectが、特定の攻撃の振る舞いや攻撃によって侵害を受けたホストに関する情報を提供すると同時に、セキュリティアナリストは、Cognito Recallによって、攻撃があった期間と同時に発生したネットワーク通信に関する保存データを検索できます。

Vectra Recallはホストデバイスからの、全てのアウトバウンドとインバウンドの通信をトラッキングします

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