DARKTRACE

Darktrace / CLOUD

マルチクラウド環境をリアルタイムに保護するために開発されたアダプティブAIによるサイバーレジリエンスの実現

急激に変貌しつつあるクラウドセキュリティランドスケープ

組織がますます多くのワークロードとデータをクラウド環境に移行させるなかで、セキュリティチームがしばしば直面する課題として、脅威をリアルタイムに検知、対処すること、すべてのアセットやアクティビティに対する明確な視界を維持すること、一貫したセキュリティポリシーを徹底することなどがあります。

多くの組織はクラウドアーキテクチャに対する可視性不足に悩まされ、マルチクラウド環境全体に渡ってデータを追跡しアクセスすることが難しくなっています。 この可視性不足はクラウドサービスの分散型の性質、および複数のプラットフォームを使用することによるもので、データがどこに保存され、どのようにアクセスされているかがわかりにくい場合があるためです。

また、クラウド環境はセキュリティチームにとって、特に脅威への対処において特有の問題があります。 リソースが絶えずスケールアップあるいはスケールダウンされ、コンフィギュレーションも頻繁に変更されるクラウド環境の動的な性質は、脅威をリアルタイムに検知し、対処することを難しくします。

異なるクラウドモデル（パブリック、プライベート、ハイブリッド）およびサービス（SaaS、PaaS、IaaS）の組み合わせにより、複雑な、管理の難しいセキュリティランドスケープが作り出されます。 この複雑さにより一貫したセキュリティポリシーの徹底が難しくなるだけでなく、クラウドセキュリティインシデントの主要な原因となる設定や権限の間違いが起こる可能性が高まります。

既存のソリューションはサイロ型で、保護のギャップが生じる

クラウド環境の動的な性質とその規模に対して、複数のクラウドプラットフォームおよびサービスを効率的に管理または統合するように設計されていない、サイロ型のセキュリティツールでは対応しきれません。クラウド環境の複雑さにより、脅威をすばやく検知および対処し、統一されたセキュリティポリシーを徹底して設定ミスを速やかに見つけることが難しくなります。

また、オンプレミスとクラウド環境の両方をセキュアにすることは、インフラのあらゆる部分に対して一貫した保護と可視性を保つ上できわめて重要です。 完全な可視性と一貫したセキュリティ戦略がなければ、オンプレミスとクラウド環境の間にギャップが生じ、その脆弱性を悪用して不正なアクセスを取得するチャンスを攻撃者に与えてしまいます。

現在のクラウドセキュリティソリューションは、カバレッジのギャップとサイロ型のアプローチにより、多くの場合リアルタイムの検知と対処、可視性と複雑性の問題に十分に対応できていません。これらのギャップに対応するには、リアルタイムの脅威検知および対処、コンテキストの認識、そしてプロアクティブなポスチャー管理を含む包括的なクラウドセキュリティ戦略が必要です。 統一されたマルチクラウド型セキュリティは、進化し続けるサイバー脅威に対して強固な保護を実現する上で不可欠です。

Darktrace / CLOUDでリアルタイムのクラウドセキュリティを実現

リアルタイム検知と自律遮断

組織にとって何が正常な状態であるかを理解する自己学習型AIにより、クラウドエステート全体で既知および新手の脅威をリアルタイムに検知し遮断します。Cyber AI Analystを活用してクラウド内のアラートを継続的に調査しコンテキストを理解することにより、調査プロセスを簡素化し加速することができます。

動的なクラウド可視性と監視

組織の複雑なクラウドフットプリントを解明し、すべてのクラウドアセットおよびアーキテクチャに対するリアルタイムの可視性を持つことができます。展開されたクラウドアセットをリアルタイムに追跡管理し、自動的に生成されたアーキテクチャダイアグラムをレビューすることにより、DevOpsとセキュリティチームが共通のコンテキストで作業することができます。

プロアクティブなクラウド保護とリスク管理

セキュリティ運用をリアクティブな状態からプロアクティブな状態にシフトし、攻撃に先手を打つことができます。露出したアセットを特定し、内部への攻撃経路を確認することにより、クラウド環境全体に渡って最もリスクの高い経路を動的に把握することができます。

ビジネス上の利点

クラス最高のクラウドセキュリティ
業界をリードするクラウドセキュリティにより既知と未知および新手のクラウド脅威をリアルタイムに検知し、正しい脅威検知を60%向上[1] させることができます。

ピンポイントの精度でリアルタイムに遮断
業界唯一の自律的脅威遮断を高精度かつマシンスピードで実現し、検知された脅威への対処に費やす時間を90%短縮[2] することができます[2]。

調査プロセスを簡素化し加速
あらゆるアラートを自動的に分析およびトリアージしてセキュリティ運用プロセスを変革し、データ侵害の防止とダウンタイム短縮によりROIを85%向上[3] させることができます。

クラウドインフラの全貌を解明
業界唯一の動的かつリアルタイムのアーキテクチャモデリングにより組織のインフラを明確に描き出し、クラウドアセットに対する可視性を30%向上[4] させることができます。

クラウドリスクにプロアクティブに対応
露出したアセットを特定し、クラウド環境全体に渡って最もリスクの高い経路を動的に把握することができます。

セキュリティ体制を強化しコンプライアンスを維持
自動化されたクラウドポスチャ管理がクラウドの設定、脆弱性およびポリシー違反を継続的に評価します。

1 製造業のDarktraceクライアントにおける脅威検知の向上に基づく。
2 金融サービス業のDarktraceクライアントにおける時間節約の向上に基づく。
3 金融サービス業のDarktraceクライアントにおけるROIの向上に基づく。
4 不動産投資業のDarktraceクライアントにおける可視性の向上に基づく。

Darktrace / CLOUDの主な機能

オンプレミスおよびクラウド環境全体に渡って既知と未知の脅威を検知

完全なクラウドカバレッジを実現し、精密な脅威検知によってブラインドスポットを明らかにします。

概要

- 既知および新手の脅威を検知
- 異常なアクティビティをリアルタイムに発見
- マシンスピードでの自律遮断
- 完全なクラウド可視性と監視
- 自己学習型AIによるSecOpsの効率化

Darktrace / CLOUD は自己学習型AIを使用してマルチクラウド環境に完全なサイバーレジリエンスを提供するインテリジェントなクラウドセキュリティソリューションです。クラウド内でのリアルタイムの検知と自律遮断、継続的な可視性と完全なアーキテクチャ認識、そしてプロアクティブなクラウドポスチャ管理を、一元的なソリューションで提供することにより現代のクラウドセキュリティ課題を解決します。

組織の日々のクラウドオペレーションから継続的に学習する、業界をリードするAIプラットフォームの上に構築されたDarktrace / CLOUDは、この重要なビジネスコンテキストを適用してクラウドアセットの可視化と監視、調査プロセスの自動化を行い、クラウドベースの脅威を数秒で無力化します。Darktrace / CLOUDはマルチテナント、ハイブリッド、およびサーバーレス環境をサポートし、デフォルトでエージェントレスであり（強化されたリアルタイムアクションと深層的調査のためにオプションでエージェントを利用することもできます）、クラウドから数分で展開することができます。他のクラウドネイティブなセキュリティベンダーとは異なり、Darktraceはオンプレミスとクラウドワークロード両者の可視性とセキュリティを統一することで、クラウド移行への顧客の道のりをサポートします。

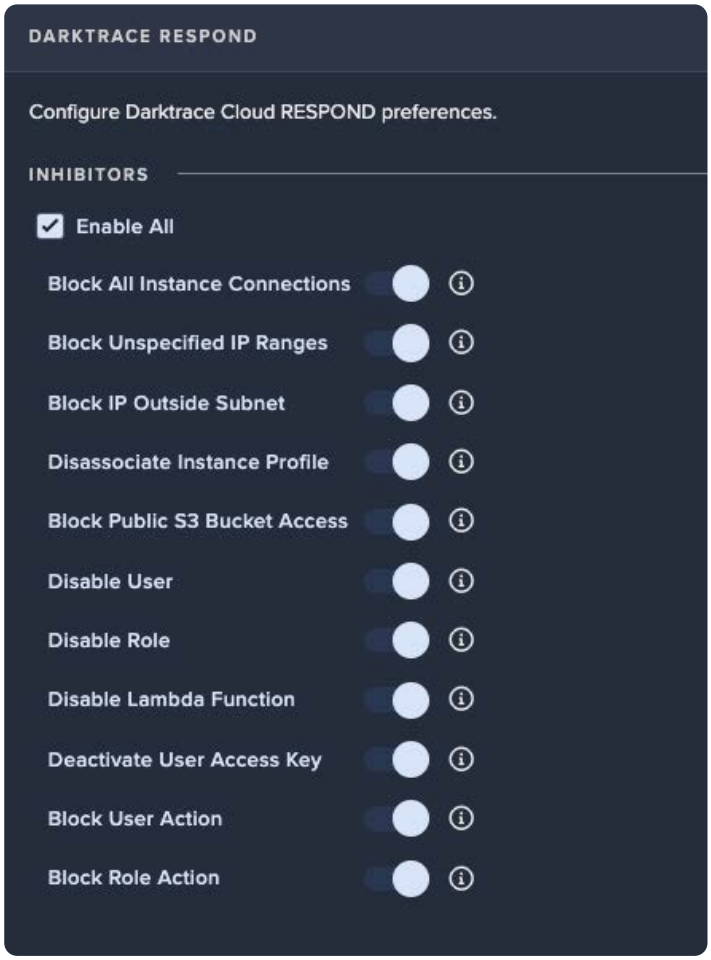

図 01: Darktrace / CLOUDの自律遮断アクションは組織の必要性に応じてカスタマイズでき、簡単に有効化または無効化できます。

クラウド上でのリアルタイム検知および遮断

クラウド上で自律遮断を行うことにより既知、未知および新手のクラウドベースの脅威を数秒で無力化します。Darktrace / CLOUDの自己学習型AIはクラウドアセット、コンテナ、API、ユーザーにわたるアクティビティを継続的に監視し、アイデンティティとネットワークに関する高度なコンテキストを用いて分析することにより脅威を迅速に検知し無害化します。さらに、攻撃経路モデリング機能により、セキュリティチームは攻撃経路が発生次第、それについて知ることができます。

Cyber AI Analystはあらゆるアラートを自動的に分析およびトリアージすることで調査プロセスを簡素化および加速し、時間を節約してセキュリティ運用を変革することができます。Cyber AI Analystはネットワーク、アイデンティティ、Eメール、クラウド全体に渡って相関づけられた何千ものデータポイントに基づいてインテリジェントに判断を行い、自動的にアラートを調査することで時間の節約につながります。

プラットフォームネイティブな自動遮断、およびAI駆動の動作封じ込め機能により、悪意あるアクティビティをピンポイントで無害化する一方、クラウドインフラやサービスの中断を回避することができます。 悪意ある動作が進行した場合、Darktraceの自己学習型AIは何千ものデータポイントを相関づけることで普段とは異なる動作を識別し、特定の接続をブロックして通常通りの動作を強制することにより、即座に遮断することができます。

動的なクラウド可視性と監視

組織のクラウドインフラ全体にリアルタイムの可視性を得ることで、複雑なハイブリッドおよびマルチクラウド型クラウド環境の全貌を解明することができます。ネットワーク、コンフィギュレーション、IAM接続に基づいて、クラウドアセットの列挙および動的なアーキテクチャのモデル化を行い、インフラの進化に伴って変化するアーキテクチャの明確な全体像を描き出し、リアルタイムの検知情報を表示します。

自動的に生成されるアーキテクチャダイアグラムと継続的なアセット監視により、DevOpsチームとSecOpsチームは効果的に共同作業することができます。理解を統一し、共通のコンテキストに基づいてより短時間に、より多くの情報に基づいた判断が可能になります。

継続的なネットワークトラフィック分析により、Kubernetes等のコンテナ化された環境を含め、ワークロードを大規模に監視し保護することができます。 展開方法は柔軟で、デフォルトではエージェントレス、ディープパケットインスペクションを行う場合にはオプションでエージェントを使用することもでき、サイバーレジリエンスの確保と既存のワークフローを補完するシームレスな統合が可能です。 可視性の共有により組織内の各チームを連携させ、クラウドへの移行を加速させると同時にオンプレミスおよびクラウド環境全体のセキュリティを維持することができます。

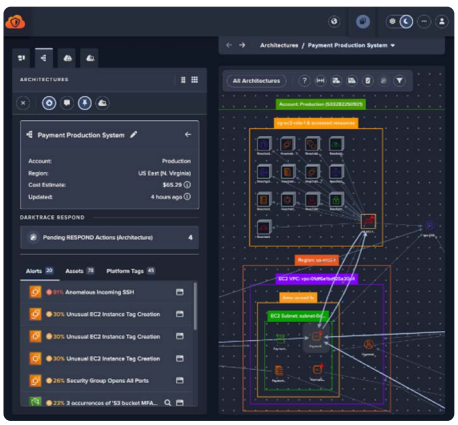

図 02: 動的なアーキテクチャモデリングにより継続的にリアルタイムの監視を提供します。

プロアクティブなクラウド保護とリスク管理

攻撃経路モデリングにより、攻撃者に先手を打つことができます。 露出したアセットを特定し、内部への攻撃経路を確認することにより、クラウド環境、ネットワーク環境、そしてその間を含む全体に渡って最もリスクの高い経路を動的に把握することで、セキュリティチームは組織のビジネス固有のリスクに基づいた優先付けを行い、ギャップに対策を施して将来の攻撃を防ぐことができます。

組織のビジネス固有のコンテキストに基づいて設定ミスやリスクの重大性を判断し、対応を行うことがクラウドセキュリティ体制の強化につながります。各ロールの権限とアクセス設定をセキュアにすることで内部関係者による脅威と水平移動を防御し、セキュリティ運用をリアクティブな状態からプロアクティブな状態にシフトさせ、攻撃に先手を打つことができます。 自動化されたクラウドポスチャ管理がCIS等の規格に照らしてコンフィギュレーションを継続的に評価し、脆弱性およびポリシー違反をリアルタイムに見つけ出します。

Darktrace / CLOUDは変化するリスクに基づいてその焦点を動的に調整し、設定ミスや異常なアクティビティを分析して攻撃の可能性を防止します。 エンタイトルメントの列挙により、すべてのアイデンティティ、ロール、権限に対する可視性を確保し、動的に調整を行って内部関係者による脅威を阻止することができます。

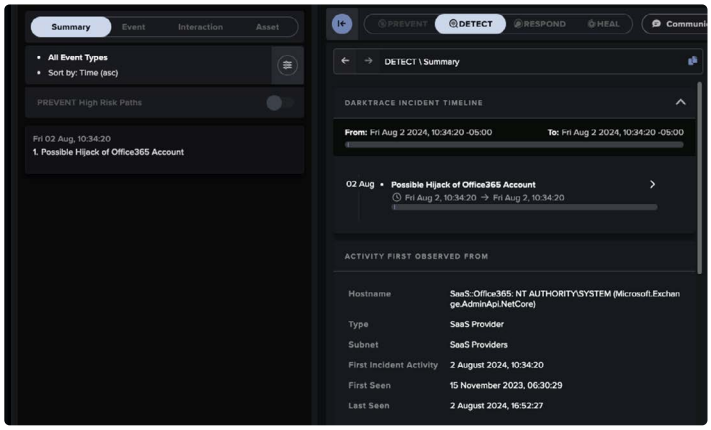

図 03: すべてのアイデンティティ、ロール、権限に対する可視性を確保し、進行中のラテラル攻撃や内部関係者による脅威を阻止します。

業界初のAI Analystにより環境内のすべてのアラートを調査

Darktrace / CLOUDはCyber AI Analystの力を活用して組織のデータにコグニティブオートメーションを適用し、トリアージの時間を92%[5]短縮します。

概要

- Cyber AI Analystの力を利用
- SOCチームを補強
- アラートのトリアージと調査を自動化
- 詳細なクラウドフォレンジック
- ビジネス全体のコンテキスト

SOCチームの能力を補強

単にインシデントのサマリーを作成するだけのプロンプトベースのLLMや、ベーシックなAI調査機能を提供する他のベンダーとは異なり、Cyber AI Analystは経験豊富な人間のアナリストのように実際に機能することができる市場で唯一のテクノロジーです。 セキュリティインシデントの調査をマシンスピードで自動化し、トリアージにかかる時間を劇的に短縮してSOCチームを支援します。

Cyber AI Analystは組織にとって何が正常な動作であるかについての理解に基づき、ネットワーク内のあらゆるアラートを継続的に分析しコンテキストにあてはめます。人間のアナリストが行うように自律的に仮設を立てて結論を導き出すことが可能で、SOCチームは時間とリソースを大幅に節約することができます。

詳細な調査により高度な脅威を解明

Cyber AI Analystはクラウド内のあらゆるアラートをインテリジェントに調査し、良性と見えるようなイベントを結び付けて高度な脅威を解明し、さまざまなアクティビティを相関づけて1つのインシデントを明らかにします。 一見無害な異常をつなぎ合わせることにより、Cyber AI Analystは悪意あるアクションのかすかな兆候も自律的に識別し、高度なネットワーク脅威を見つけ出してキルチェーン全体をリアルタイムかつ大規模に追跡します。

ビジネス全体のコンテキストを理解

組織の環境内のあらゆる部分から発生したアラートのコンテキストを理解することができます。 Darktrace Cyber AI Analystは、組織のネットワーク、エンドポイント、クラウド、アイデンティティ、OT、Eメールおよびリモートデバイス全体に渡って接続とイベントを追跡し、デジタルエステート全体を移動する最新の脅威の検知と調査に役立ちます。

Darktrace / NETWORK および Darktrace / CLOUD に既存のEDRを追加することで、元のEDRに限定されネイティブな機能に欠けるXDRベンダーと比較して、きわめて効果的なXDRソリューションの基礎を構築することができます。 セキュリティチームはActiveAI Security Platformを利用してプロアクティブな能力と修復機能を追加することができ、接続された1つのソリューション内でEメール、アイデンティティ、およびOTをカバーすることができます。

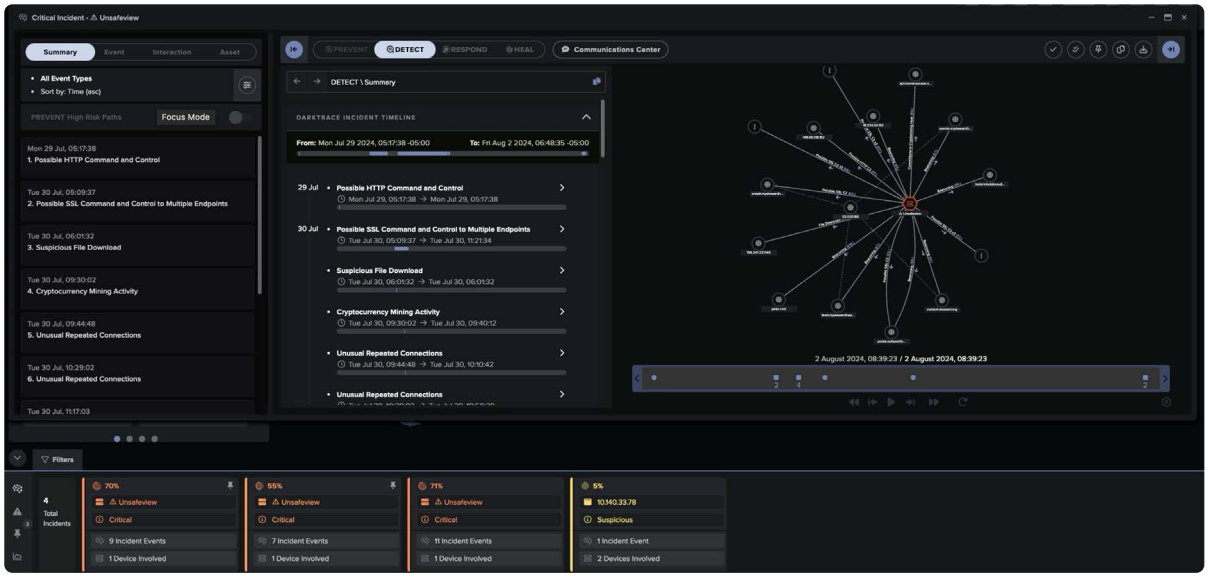

図 04: Cyber AI Analystは組織にとって何が正常な動作であるかについての理解に基づき、クラウド環境内のあらゆるアラートを継続的に分析しコンテキストに当てはめます。インシデントの詳細なタイムラインと完全なサマリーが提供され、チームは意味付けまでの時間を短縮することができます。

5 製造業のDarktraceクライアントにおける時間節約の向上に基づく。

自律遮断によりクラウドベースの脅威を数秒で無力化

ビジネスオペレーションを中断することなく攻撃をリアルタイムかつ自動的に封じ込め、遮断します。

まとめ

- 自律遮断
- 生活パターンと動作のコンテキスト
- 的を絞ったアクションにより中断を回避
- ネイティブな遮断アクション
- 完全にカスタマイズ可能

自律的な脅威遮断

Darktrace / CLOUD は過去の攻撃データに頼ることなく、環境の全体的コンテキストと、デバイスまたはユーザーにとって何が正常であるかについての詳細な理解に基づいて、脅威をすばやく封じ込め無力化します。Darktrace / CLOUD は単独のデバイス、またはそのピアグループにとって何が正常であるかに基づいて、生活パターンを自律的に強制することのできる唯一のCDR（Cloud Detection and Response）ソリューションです。

Darktrace / CLOUD は精密な遮断アクションをリアルタイムかつ自律的に実行することにより、ビジネスオペレーションを中断することなく、ネイティブに、またはサードパーティツールとのインテグレーションを通じて脅威を封じ込めます。

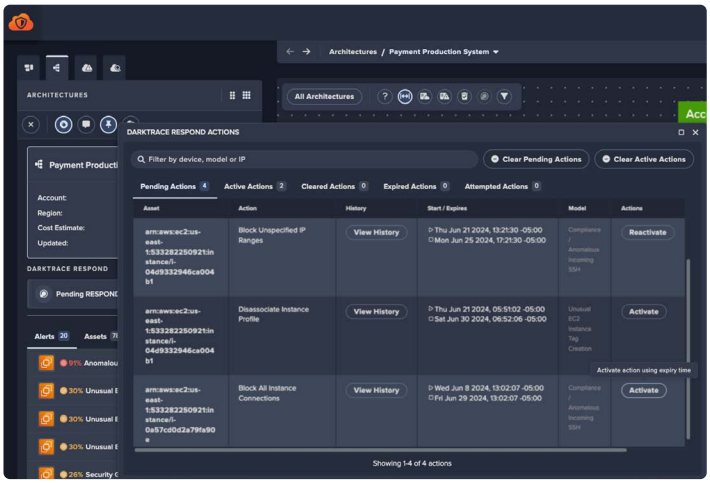

図 05: 各イベントとインシデントのつながり、またAIがどのように自律的に対処してビジネスを保護したかを完全に可視化

完全なコントロールを維持

Darktrace / CLOUDはクラウド脅威に対して最も効果的な対処を自律的に実行しますので、プレイブックの管理や運用環境を人手で調整する作業などに時間を費やす必要がありません。

遮断アクションを自分で調整したい場合には、直感的に操作できるモデルエディターを使ってカスタマイズすることも簡単です。あらゆるアクションと対処ロジックをきめ細かく調整して思い通りにチューニングすることができます。デバイスタイプ、IP範囲、業務時間、およびその他の無数のパラメータに基づいて異なる遮断アクションを選択できます。

クラウドの可視性をネットワークやリモートデバイスにも拡大

Darktrace / ENDPOINT

Darktrace / NETWORK

Darktrace / NETWORK により検知および遮断能力をネットワーク環境にも適用し、エンタープライズ全体のカバレッジを実現することができます。 プラットフォームネイティブな自律遮断アクションにより既知および未知のネットワークベースの脅威を数秒で無力化します。

Darktrace / NETWORK

Darktrace / ENDPOINT

Darktrace / ENDPOINT によりリモートデバイスのネットワーク可視性を維持し、自律遮断能力をエンドポイントに適用することができます。的を絞った対処アクションにより異常な接続をシステムレベルで抑制することが可能です。

Darktrace / CLOUDの導入

Darktrace / CLOUD は数分で導入でき、柔軟な展開オプションとマルチテナント、ハイブリッド、およびサーバーレス環境をサポートしています。Darktrace / CLOUD はデフォルトでエージェントレスであり、トラフィックミラーリングとAPIログの組み合わせを使用しています。またオプションで軽量なホストベースのサーバーエージェントを使ったディープパケットインスペクションも可能です。

分析

Darktraceはさまざまな方法で展開してハイブリッドマルチクラウド環境への完全な可視性を提供することができます。 いずれの展開方法もDarktraceの「マスター」インスタンスのプロビジョンから開始されます。これは仮想インスタンスとして展開されます。環境内のクラウドおよびネットワークデータはDarktraceマスターインスタンスにより処理および分析され、出力は Darktrace Threat Visualizerに表示されます。

DarktraceはクラウドベースのマスターインスタンスをDarktraceクラウド環境（AWSおよびAzure）内でホスティングすることにより完全に仮想化された展開も可能で、これにより仮想および物理双方のロケーションに対応できます。 複数のマスターが必要な場合、‘Unified View’を使用することで、すべてのマスターインスタンスに対して単一の一元化されたユーザーインターフェイスを提供することができます。必要に応じてHigh Availability（HA）オプションも使用できます。

収集

Darktraceマスターインスタンスはそれ自身で生のトラフィックを処理し、ネットワークデータをクラウド上のローカル「プローブ」（仮想または物理）から収集することができます。このトポロジーでは、Darktraceプローブが取り込んだデータに対してDPI（Deep Packet Inspection）を実行し、元のトラフィックと比較してごくわずかな帯域幅でマスターアプライアンスに対して絶え間なくデータを送り続けます。 パケットキャプチャデータ等の生データはプローブに保持され、マスターインスタンスのThreat Visualizer Webインターフェイスからオンデマンドで呼び出されます。

vSensorは軽量な仮想プローブであり、仮想スイッチからパケットを受信するスタンドアロン仮想マシンとして運用することも、パブリッククラウドVPCトラフィックミラーリング、Microsoft仮想ネットワークフローログ、あるいはVM上に展開されたホストベースのosSensorエージェントからパケットを収集することも可能です。 Darktraceは Kubernetes等のコンテナ化された環境と統合することもできます。

必要に応じて、ハードウェアプローブを物理的なロケーションに展開することも可能です。 ネットワーク内のトラフィックの量やデバイス数に応じて、さまざまなハードウェアアプライアンスが用意されています。

Darktrace / CLOUD はホストベースのClient Sensor、統合されたサードパーティサービス（SaaSやクラウドアプリケーション等）、および連携しているDarktrace製品からのデータも収集します。

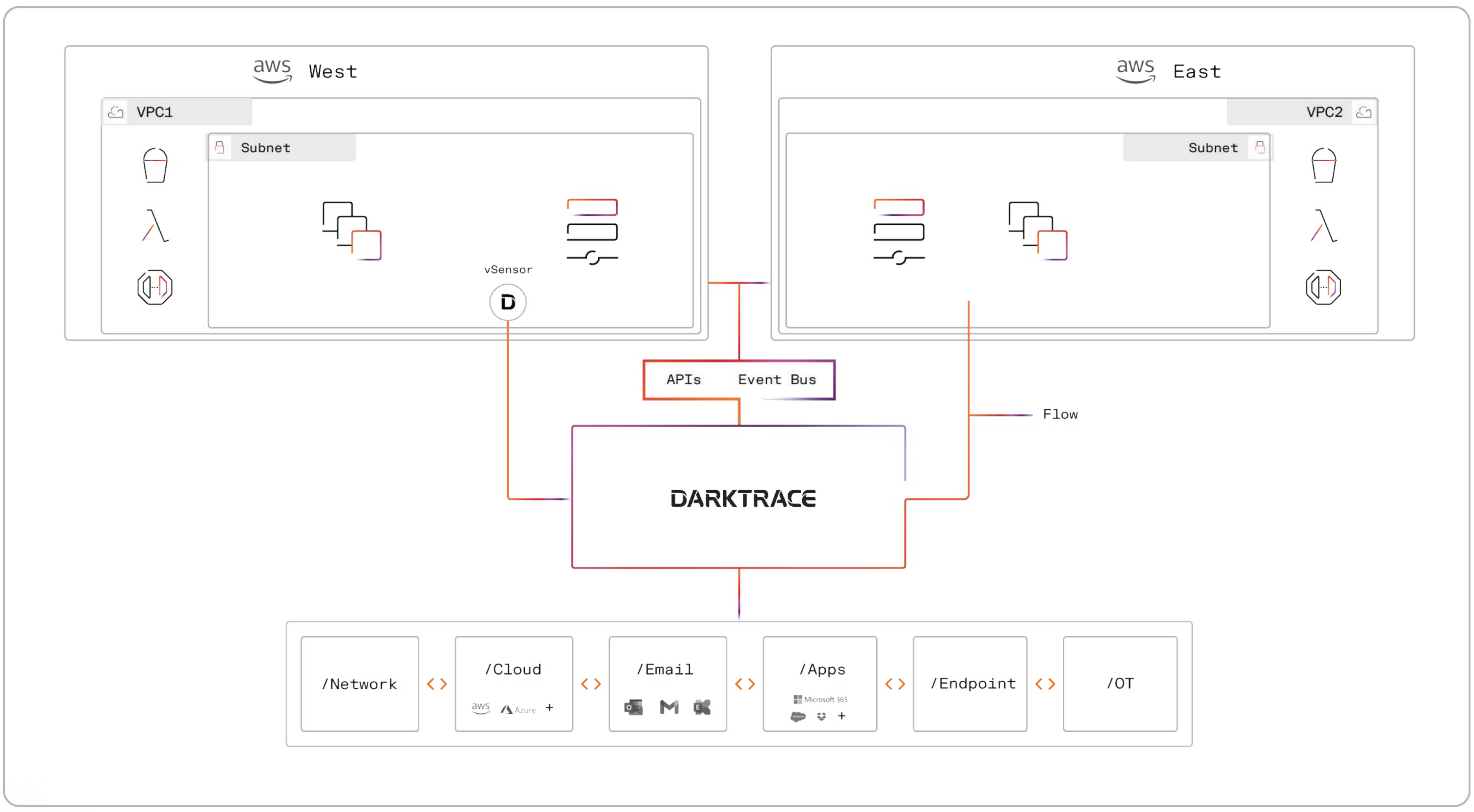

図 06: Darktrace / CLOUD の展開

Darktrace ActiveAI Security Platformでサイバーレジリエンスを実現

Darktrace / CLOUD はDarktrace ActiveAI Security Platformの一部であり、ネットワークセキュリティをデジタルエステートの他のエリアと組み合わせて、クラウド、エンドポイント、Eメール、アイデンティティ、およびOTデバイス全体に渡るセキュリティの可視性とコントロールを強化することができます。

Darktrace / CLOUD はDarktrace / Attack Surface Managementとの連携により、外部に露出したアセットに対する継続的な、カスタマイズされた検知を提供します。 Darktrace / Proactive Exposure Managementと組み合わせることにより、組織は内部と外部のセキュリティリスクに先手を打って識別、分析、緩和するためのアクションを実行することができます。

Darktrace / Incident Readiness & RecoveryはDarktrace / CLOUD ならびにActiveAI Security Platformの他のすべてのエリアから情報を受け取り、あらゆるサイバーインシデントを予測、検知、封じ込め、修復し、そこから学習するのに役立ちます。 それぞれの組織専用のプレイブックと効果的な修復は組織のネットワークと脅威ランドスケープについての深い理解に基づいており、現代の攻撃者からオペレーションの継続性を守ることができます。

Darktrace ActiveAI Security Platformはサイバー攻撃のプロアクティブな予防、インシデントからのすばやい修復、セキュリティ体制の継続的強化のすべてを1つのプラットフォームから実現することにより、組織のサイバー防御に革命をもたらします。

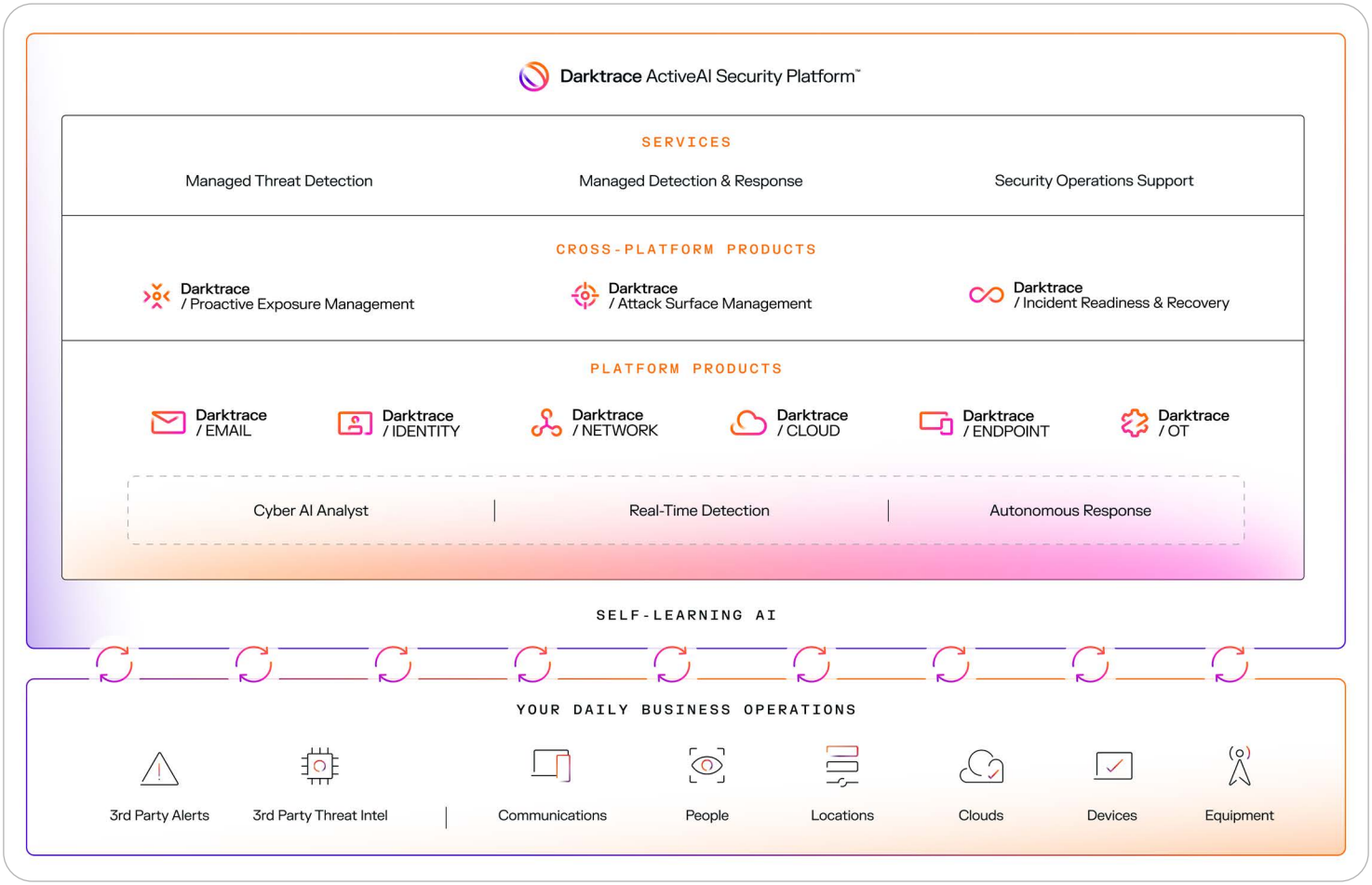

図 07: The Darktrace ActiveAI Security Platform

運用上の利点

運用効率の向上
自律的に自身を調整する自己学習型AIにより、人手による面倒なチューニングを行うことなく重大なアラートを通知させることができます。

セキュリティチームに対する圧力を軽減
人間のアナリストと同じように分析を行うCyber AI Analystを活用することにより、セキュリティインシデントの調査を自動化してトリアージにかかる時間を92%短縮[5] することができます。

完全なコントロールを維持
デバイスタイプ、IP範囲、業務時間、およびその他の無数のパラメータに基づく高度なカスタマイズオプションと対処アクションにより完全なコントロールを維持できます。

CDR（Cloud Detection & Response）を超えた機能
デバイスタイプ、IP範囲、業務時間、およびその他の無数のパラメータに基づく高度なカスタマイズオプションと対処アクションにより完全なコントロールを維持できます。

サイバー防御を最大化
Darktrace MDR（Managed Detection & Response）によりSOCチームから24時間、週7日のサポートを受け、セキュリティの成果に集中することができます。

“Darktrace / CLOUD は環境についてのコンテキスト、および実際に何が起こっているかに基づいて、セキュリティチームが彼らの貴重な時間をどこに優先的に費やし何に対処するかを決めるのに役立ちます。”

■ **CISO**
Domino’s社

“これまで異常の特定に時間単位、日単位の時間を要していたものが数秒で行えるようになりました。”

■ **金融サービス企業**
米国

“Darktraceではすべてのトラフィックに対しオンプレミスかオンクラウドかに関係なく同じセキュリティモデルを適用できました。”

■ **ICTマネージャー**
Dreamworld社

“クラウド環境に対するホリスティックかつリアルタイムの視野を持つことにより私達は現実的な方法で作業できるようになり、AIの使用を通じて管理にかかる時間を短縮してセキュリティリスクに対処しレジリエンスを強化できるようになりました。”

■ **サイバーセキュリティ責任者**
Sykes Cottages社

■ **ダークトレースについて**

ダークトレースは、日々変化する脅威ランドスケープに組織が自律対処できるように支援するAIサイバーセキュリティのグローバルリーダーです。2013年に設立されたDarktraceは、各顧客固有の生活パターンをリアルタイムに学習する独自のAIを使用して、未知の脅威から組織を保護するために不可欠なサイバーセキュリティプラットフォームを提供しています。Darktrace ActiveAI Security Platform™は、セキュリティ体制の完全可視化、リアルタイムの脅威検知、自律遮断機能により、サイバーレジリエンスに対して先手を打つアプローチを提供し、クラウド、Eメール、アイデンティティ、OT、エンドポイント、オンプレミスネットワークを含むあらゆるデジタル環境でビジネスを保護します。英国ケンブリッジとオランダ・ハーグの研究開発チームによる画期的なイノベーションにより、これまでに200件以上の特許を出願しました。ダークトレースの従業員数は世界各国で2,400名を超え、10,000社近くの顧客を既知、未知および新手のサイバー脅威から保護しています。

北米: +1 (415) 229 9100　ヨーロッパ: +44 (0) 1223 394 100　日本: 03-5456-5537　ラテンアメリカ: +55 11 4949 7696

darktrace.com/ja | japan@darktrace.com