DARKTRACE

Darktrace / ENDPOINT

自己学習型AIで既知と未知の
エンドポイント脅威と戦う

リモートデバイスの可視性を維持

従業員の63%がハイブリッドベースでリモート勤務[1]する状況において、コーポレートネットワークやVPNの外にあるリモート勤務者のデバイスに対するネットワーク可視性を維持することはますます重要になりつつありますが、このことはほとんどのNDR（Network Detection and Response）やEDR（Endpoint Detection and Response）ソリューションでは対応されていません。

プロセスレベルのエンドポイントテレメトリーに基づくEDRやXDR等のソリューションのみに依存していたのでは、組織内にブラインドスポットが生じます。 ネイティブなネットワーク可視性を持たないこれらのソリューションは、従来の検知ルールを回避しネットワーク内の複数の場所を移動する攻撃を見逃してしまいます。

古いツールは新しい脅威に対して盲目

これまでに見られたことのない脅威や標的型の攻撃はEDRソリューションでは見過ごされてしまうか、検知が手遅れになることがあります。これらは過去の攻撃データや外部の脅威インテリジェンスに依存しているためです。 これらのツールが「既知の悪」に焦点を絞っていることは、新手のネットワーク攻撃や、その他の脅威、たとえば悪意ある内部関係者やサプライチェーン攻撃、データ抜き出しや、環境寄生型（Living off the Land）攻撃を検知できないことを意味します。

また、既存のソリューションは、エンドポイントデバイスに影響を及ぼしているネットワーク脅威に対して的を絞った対処アクションを取る能力が欠けています。これにより、脅威を封じ込めるためにエンドポイント全体が隔離される結果となることがしばしばあり、ユーザーとビジネスに混乱をもたらします。組織は効果的かつ的を絞った対処をマシンスピードで実行して脅威を封じ込める一方、通常のビジネスオペレーションを維持することのできるソリューションを必要としているのです。

SOCチームにかかるプレッシャー

SOCアナリストの70%以上が極度の疲労を経験していると報告しており[2]、結果に妥協することなくセキュリティチームにかかるプレッシャーを下げるためには、組織はサイバー脅威と戦う新しいアプローチを活用する必要があります。

組織の57%が、自社のSOCの集約および相関能力を強化する必要があると報告しており[3]、SOCチームは調査AI等、代替ソリューションを導入することでアナリストの負担を軽減し、アラート疲れを和らげ、セキュリティ業務をよりプロアクティブな状態に変革することを検討する必要があります。

1 McKinsey Global Institute, 2023.
2 Tines - Voice of the SOC Analyst, 2022
3 Gartner Peer Community One-Minute Insights - Modern Security Operations Center (SOC) Strategies, 2023

自己学習型AIによるリアルタイムの防御

検知

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、エンドポイントデバイス全体に渡り既知および新手のネットワーク脅威を検知します。シグネチャや過去の攻撃データに頼ることなく、エンドポイントやリモート勤務者のデバイスにネットワーク可視性と脅威検知機能を拡大することができます。

調査

Cyber AI Analystを活用してエンドポイントに影響するネットワーク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ができます。Cyber AI Analystは人間のアナリストが行うように自律的に仮説を立て、結論を導き出すことができ、SecOpsを変革しチームを強化します。

遮断

Darktraceの自己学習型AIは既知の脅威と新手の脅威のどちらに対してもリアルタイムかつ自律的に遮断し、組織についての文脈的理解および動作の理解に基づいて精密なアクションを実行し、業務に影響を与えることなく脅威を封じ込めることができます。

ビジネス上の利点

既知および新手の脅威からビジネスを保護
過去の攻撃データ、シグネチャ、脅威インテリジェンスあるいはクラウド接続に頼ることなく、リアルタイムに保護します。

完全なネットワーク可視性
VPN外のユーザーも含め、すべてのエンドポイントとリモートデバイスに完全な可視性を提供します。

AIでSOCチームを補強
セキュリティインシデントの調査とトリアージをマシンスピードで自動化し、時間とリソースを大幅に節約します。

ビジネスの中断を回避
ビジネスのコンテキストを理解し、精密なアクションを実行してリアルタイムに脅威を封じ込める自律遮断ソリューションにより、ビジネスに影響を与えません。

組織全体の情報を統合
エンドポイント、ネットワーク、クラウド、アイデンティティ、OTデバイス、からのデータを統一されたソリューションでコンテキスト化します。

Darktrace / ENDPOINTの主な機能

エンドポイント全体に渡り既知および新手のネットワーク脅威を検知

完全なネットワーク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

- エンドポイントデバイスに対する完全な可視性
- 異常なアクティビティをリアルタイムに発見
- 既知および新手の脅威を検知
- ローカルに展開される自己学習型AI
- 暗号化および復号化ネットワークトラフィックを分析

完全なネットワーク可視性

Darktrace / ENDPOINT は軽量なエージェントを使ってあらゆるネットワークパケットおよび接続からのデータポイントを分析し、リモートデバイスやVPN外のユーザーも含めて、通常と異なるアクティビティをリアルタイムに発見します。

データをクラウド上で処理する、あるいはグローバルにトレーニングされるモデルの一部として処理する他のベンダーとは異なり、業界をリードするDarktraceの自己学習型AIはローカルに展開され、クラウド接続の必要なく組織のデータのみでトレーニングされます。これによりプライバシーに妥協することなく組織専用のセキュリティが実現されます。

既知と未知の攻撃を検知

Darktrace / ENDPOINTは他のセキュリティベンダーとは根本的に異なるアプローチにより、既知のマルウェアシグネチャや外部インテリジェンス、過去の攻撃データに頼ることなく脅威を検知します。DarktraceのAIは組織のネットワークにとって何が正常な状態であるかを理解し、異常なアクティビティや既知および新手の脅威を検知します。

ネットワーク内のあらゆるエンドポイント接続が継続的に分析、マッピング、モデル化され、組織のデバイスの全体像を作り出します。Darktraceの自己学習型AIはビジネスの中断を引き起こす可能性のあるあらゆるネットワーク動作を識別することで、既存のEDR（Endpoint Detection and Response）ソリューションを補完し、ゼロデイからサプライチェーン攻撃、内部関係者による脅威に至るまで、外部と内部双方の脅威を照らし出します。

正確な脅威検知

Darktraceの自己学習型AIは自身を自律的に最適化してノイズを排除し、純粋な、優先付けされたセキュリティインシデントを素早く提示します。これにより偽陽性を大幅に削減し、人手により絶え間なくアラートを調整する面倒を解消できます。

希望する場合には、ユーザーが運用を完全にコントロールし、直感的なモデルエディターを使ってAIの出力結果がどのように処理されるかを管理することも可能です。熟練したユーザーはあらゆる設定を直接変更または無効にすることができ、開発のコストをかけずにカスタムの検知を容易に作成することができます。

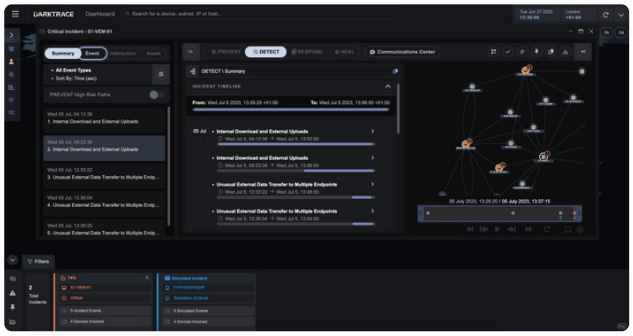


図 01: Darktrace / ENDPOINTは組織のエンドポイントデバイスにとって何が正常なネットワーク動作であるかを学習し、異常なアクティビティを検知して、ビジネスの中断を引き起こしかねないあらゆる問題についてそれらの優先度を判断します。

検知モデルの例

Darktrace / ENDPOINTはMITRE ATT&CKの14のカテゴリーすべてに対するカバレッジを提供し、過去のデータや静的なルール、あるいはシグネチャベースの手法に頼ることなく攻撃ライフサイクルのあらゆる段階で、エンドポイントに影響するネットワーク脅威を検知します。 以下はネットワーク内の異常な動作や脅威を検知するのにDarktrace / ENDPOINTが使用することのできる検知モデルの一部の例です：

水平移動

デバイス / 複数の水平方向移動モデル違反

特異な接続/ 通常と異なる管理者RDPセッション

デバイス / SMB 水平移動

コンプライアンス / SMBドライブ書き込み

C2通信

異常なサーバーアクティビティ / サーバーからの送信

特異な接続 / 新しい外部TCPポートへの複数の接続

特異な接続 / 珍しい外部SSL自己署名

デバイス / 疑わしいドメイン

ファイル暗号化

侵害 / ランサムウェア / 疑わしいSMBアクティビティ

特異なファイル / 内部 / SMBファイルへの拡張子の追加

特異な接続 / 疑わしい読み取り/書き込み比率

侵害 / ランサムウェア / 身代金要求文書の可能性

データ流出

通常と異なるアクティビティ / 通常と異なる外部データ転送（強化）

特異な接続 / 珍しいドメインへのデータ送信

通常と異なるアクティビティ / 通常と異なる外部データ転送

コンプライアンス / FTP / 通常と異なるアウトバウンドFTP

“Darktraceは本物のAIです。本当に自己を自律的にトレーニングし、私は一切モデルに手を加える必要がありません。 このシステムは驚くほど正確です。”

■ ジョセフ·ブッティンガー

コーポレートIT & セキュリティマネージャー、

EV Group

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 / ENDPOINT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劇的に短縮します。

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
- 詳細なネットワークフォレンジック
- 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重要な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はネットワーク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。一見無害なエンドポイントの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。

ネットワーク調査に対するこの包括的アプローチにより、Darktrace / ENDPOINTはゼロデイ攻撃や内部関係者による脅威その他多くの問題をすばやく見つけ出し、組織が「患者第一号」になることを防止するとともに、「既知の悪性」動作にのみ注目したソリューションよりも格段に優れた結果を提供します。

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重要な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デバイス、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 / ENDPOINT、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。

“自己学習型AIはエンドポイント上の動作を、Microsoft 365および当社のクラウド環境全体の動作と併せて調査してくれます。”

■ テリー・ライト
ITインフラ責任者、
Scope Markets社

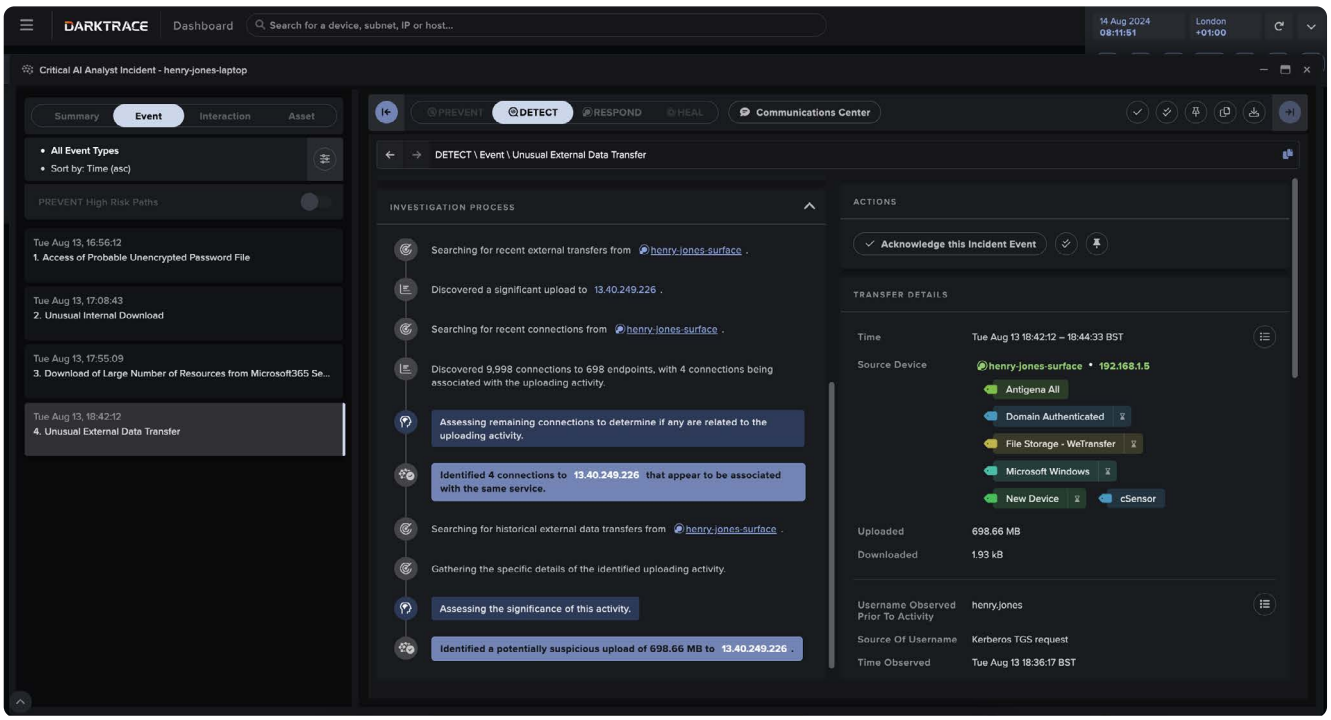


図 02: Cyber AI Analystは組織にとって何が正常な動作であるかについての理解に基づき、エンドポイントに影響するネットワーク内のあらゆる重要なアラートを継続的に分析しコンテキストにあてはめます。インシデントの詳細なタイムラインと完全なサマリーが提供され、チームは意味付けまでの時間を短縮することができます。

エンタープライズでの実効性が実証された業界初の自律遮断ソリューションでエンドポイント脅威を封じ込め

ビジネスオペレーションを中断することなく
リアルタイムかつ自律的に封じ込めおよび遮断

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
- 詳細なネットワークフォレンジック
- ビジネス全体のコンテキスト

自律的な脅威遮断

Darktrace / ENDPOINT 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 / ENDPOINT 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。また、リモートユーザーデバイスに対して、エンドポイントの場所に関わらず、またコーポレートネットワーク外にある場合にもアクションを実行することができます。

完全なコントロールを維持

Darktrace / ENDPOINTはネットワーク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対処アクションを選択できます。

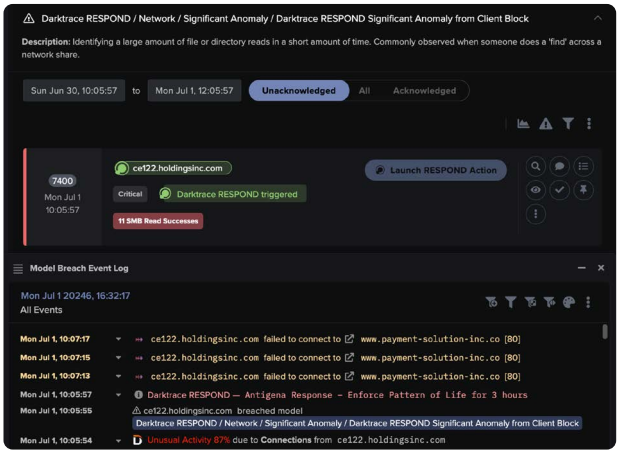


図 03: 各イベントとインシデントのつながり、またAIがどのように自律的に対処してビジネスを保護したかを完全に可視化

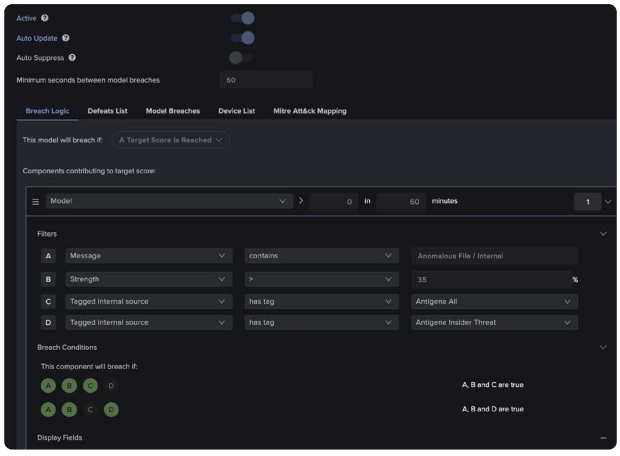


図 04: Darktrace Model Editorを使って対処ロジックを細かく調整することが可能

AIを既存のツールに拡大

豊富なネイティブインテグレーションとオープンなAPIアーキテクチャにより、複雑でコストのかかる開発は必要ありません。Darktrace / ENDPOINTは的を絞ったネイティブな対処アクションを実行して数秒で脅威を無力化すると同時に、サードパーティ製ファイアウォール、ZTNA、SIEM、SOAR、およびITSMソリューションとのインテグレーションにより、対処機能を組織の既存のテクノロジースタックに適用することもできます。 アラートは必要な任意の場所に送信して既存のワークフローを補完することができます。

また Darktrace / ENDPOINTは、Microsoft Defender、CrowdStrike、SentinelOne等のあらゆる主要なEDRプロバイダーとのインテグレーションも行われており、エンドポイントからのアラートを環境全体のテレメトリーのコンテキストに当てはめ、インシデントをより効果的に検知、調査および対応することができます。

“当社のチームがいないときにも、自律遮断機能がこれらの検知結果すべてを監視し対処してくれていると思うと安心できます”

■ リチャード・ロビンソン
ネットワーク管理者、LSUA社

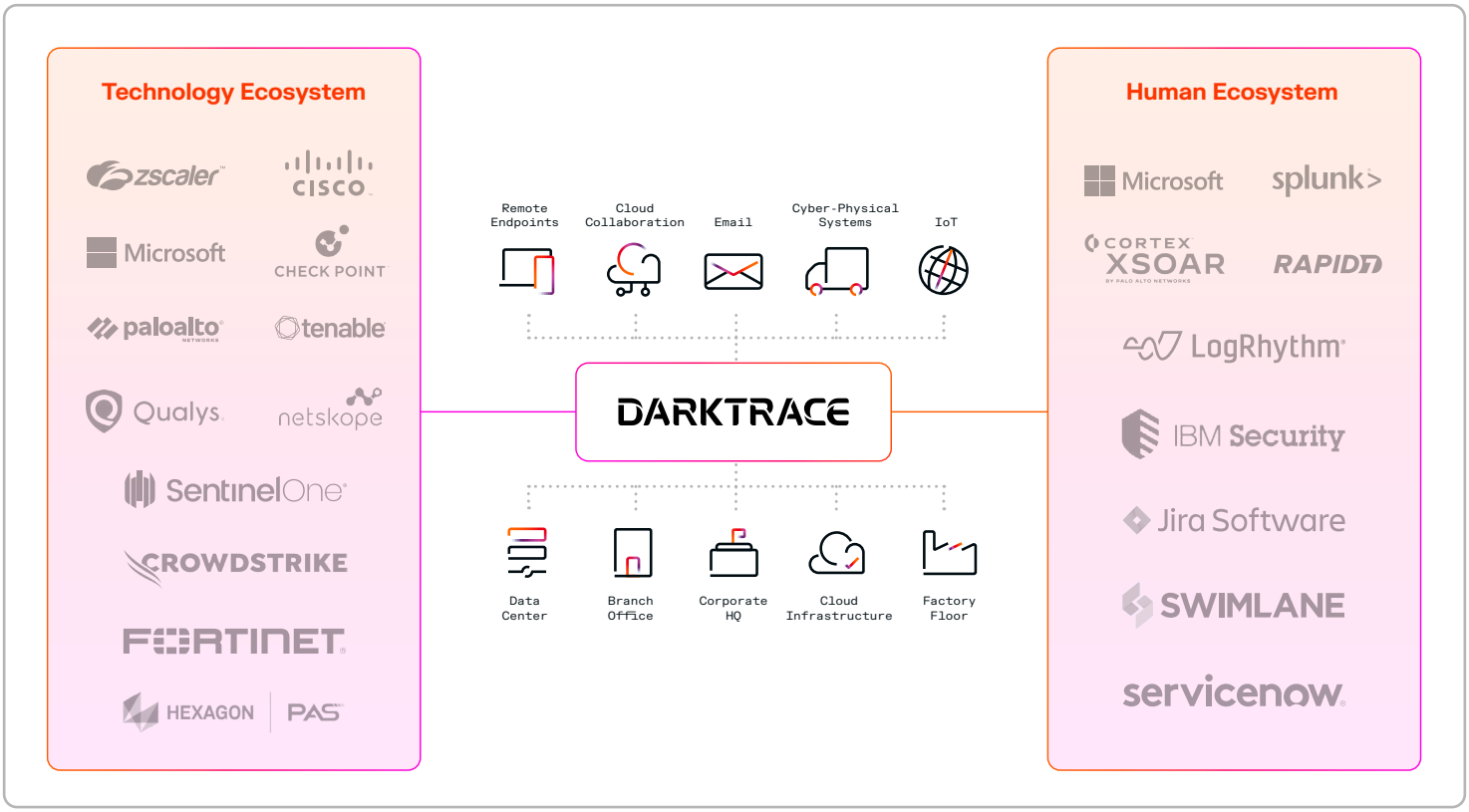


図 05: Darktraceと組み合わせることにより脅威検知、調査、遮断アクションを促進し業務ワークフローを効率化することができる多数のネイティブインテグレーション

Darktrace Mobile Appを使った人間の関与

Darktrace Mobile Appでは、効率的なユーザーインターフェイスを使って、どこにいても調査と対処が可能です。

検知された異常なエンドポイントアクティビティを調査する、人間の確認を待っている自律遮断アクションを承認する、同僚とアラートを共有する、またクリティカルな優先度のAI Analystインシデントが作成されたときには通知を受けることができます。

Darktrace Mobile App は Android と iOS で利用することができます。

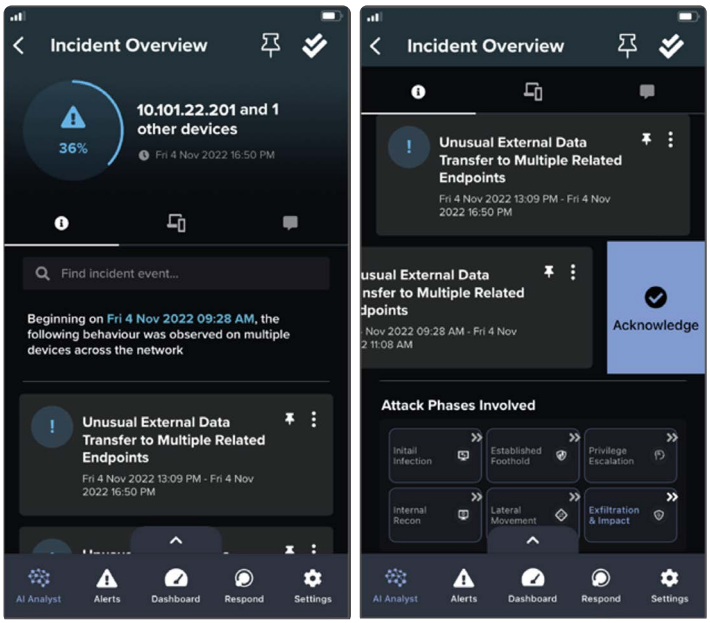


図 06: Darktrace Mobile Appのインターフェイス

Darktrace / ENDPOINTの導入

Darktrace / Endpoint cSensor エージェントは、ネットワーク可視性、検知および遮断機能をエンドポイントデバイスにも拡大します。これにはリモートワーク用デバイスや、バルクネットワークトラフィックミラーリングや既存のDarktraceセンサーを使って適切に可視化できないデバイスが含まれます。

エージェントはエンドポイント上のネットワークアクティビティを監視し、主要なデータおよびメタデータを中央のDarktrace Threat Visualizer環境に送信し、必要な場合には、異常な接続をシステムレベルで制限する自律遮断アクションをトリガします。

Darktrace / ENDPOINT は Darktrace / NETWORK と共に展開するのが最適であり、完全なネットワークカバレッジとともに検知および遮断機能を提供することができますが、希望する場合にはスタンドアロン製品として導入することも可能です。

展開オプション

エンドポイント

Darktrace cSensorはWindows、MacOSまたはLinuxエンドポイントデバイス向けのインストレーションパッケージとして提供されます。 インストレーション時に、エージェントに対してクラウドベースのcSensorインフラと安全に通信するための一意の認証情報が与えられます。

cSensorで監視するデバイスはネットワークトラフィック監視のためにHTTPS/443ポートを介してcSensorインフラに接続できなければなりません。

サポートされるオペレーティングシステム：

- **Windows：**Windows 365、11、10； Windows Server 2022、2019および2016
- **macOS：** macOS 12、 macOS 13、 macOS 14
- **Linux*：**Ubuntu 18.04+；RHEL/Centos 7+；Debian 9+；openSUSE 15.0+/SUSE Linux Enterprise 12.4+；Fedora（保守対象バージョン）

ホスト使用率：

- 帯域幅使用は最小限であり、平均で1kB/s未満。
- 無視できる程度のCPUへの影響であり、RAM使用率は40MB未満。
- インストレーションパッケージ：MacOS 30MB未満、Linux（すべてのフォーマット）30MB未満、Windows 30MB未満
- 最大40MBのディスク容量が必要

分析

Darktraceはさまざまな方法で展開して組織の物理および仮想ネットワーク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することも、物理ハードウェアアプライアンスを使用することもできます。環境内の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両方のネットワークロケーションに対応できます。 必要に応じて、Darktrace / NETWORK は Darktrace / ENDPOINT を補完するソリューションとして、ハードウェアアプライアンスをネットワークに対してパラレルに設置することにより、生のネットワークトラフィックを受動的に取り込むように展開することもできます。これは通常、Darktraceアプライアンスをコアスイッチに対してSPANセッションを使って接続することにより実現されます。

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。

* cSensorはカーネルバージョン4.6 以上のほとんどのLinuxベースのディストリビューションと互換性があると思われ、上記に明示的にリストされている以外のディストリビューションでも有効な場合があります。 サポートされるアーキテクチャはx86_64 のみです。

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全体のローカル「プローブ」（仮想または物理）からネットワークデータを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Deep Packet Inspection（DPI）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。

エンドポイントデバイスにインストールされると、cSensorはネットワークインターフェイス上で送受信されるネットワークトラフィックを分析し、この情報をクラウドベースのインフラを通じてDarktrace環境に伝達します。エンドポイント上のDPI分析（帯域幅消費を最小限に抑えるため関連するメタデータだけを転送）と、クラウドベースの処理が組み合わせて実行されます。すべてのデータはお客様のDarktrace環境に固有の認証情報を使って、暗号化通信モードで安全に転送されます。

vSensorは軽量な仮想プローブであり、パブリッククラウドVPCトラフィックミラーリングにおいて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、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、Darktrace / NETWORK の一部とし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。 お客様それぞれの環境に対して、特に大規模および/または分散型ネットワーク構成の場合には、ダークトレース担当者が最も適した展開方法をご提案することができます。

Darktrace / ENDPOINTはDarktrace / NETWORKの拡張としてシームレスに統合され、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 / EMAIL、Darktrace / IDENTITY、Darktrace / CLOUD等のDarktrace製品からのデータを収集することができます。

OT

検知および遮断機能を、お使いのOT（Operational Technology）デバイスにも適用することができます。Darktrace / OTはITとOTをネイティブにカバーし、OT、IoT、ITアセットの可視性を一元的に提供します。

Darktrace / OTは外部の接続を必要とせずエアギャップで隔離された環境にも展開することができ、Purdueモデルのすべてのレベルに渡りOTおよびITデバイスに対する 優れた可視性を達成しています。

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

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

Darktrace / ENDPOINTはDarktrace / NETWORKを補完するのに最適です。Darktrace / NETWORK の機能をエンドポイントにも拡大することにより、かつてないネットワーク可視性、精密な脅威検知と自律遮断を既知および未知の脅威に対して実現できます。

Darktrace / Incident Readiness & RecoveryはDarktrace / ENDPOINT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。

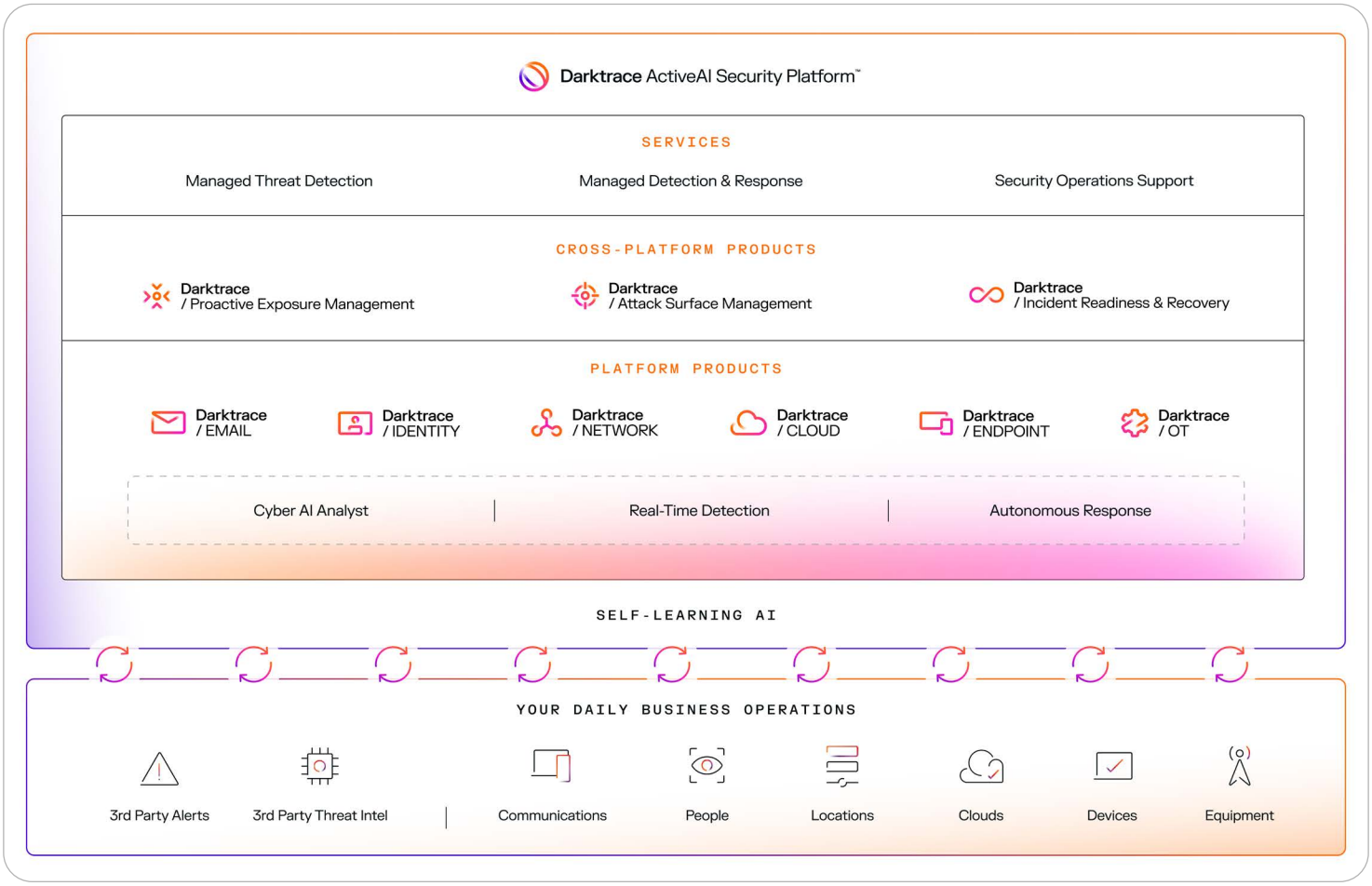


図 07: The Darktrace ActiveAI Security Platform.

運用上の利点

運用効率の向上
自律的に自己を調整する自己学習型AIにより偽陽性を大幅に減らし、人手による絶え間ない調整の必要性を解消します。

セキュリティチームに対する圧力を軽減
Cyber AI Analyst が関係のあるあらゆるアラートを自律的に調査およびトリアージし、最も重要なインシデントをチームに提示します。

AIを既存のワークフローに適用
ファイアウォール、EDR、ZTNA、SIEM、SOARおよびITSMソリューションを含む多数のサードパーティインテグレーションを通じてワークフローを統合します。

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。

エンドポイントセキュリティを超え
Darktrace ActiveAI Security Platformでプロアクティブにサイバー攻撃を予防し、セキュリティ体制を強化することができます。

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。

“自己学習型AIはエンドポイント上の動作を、Microsoft 365および当社のクラウド環境全体の動作と併せて調査してくれます。”

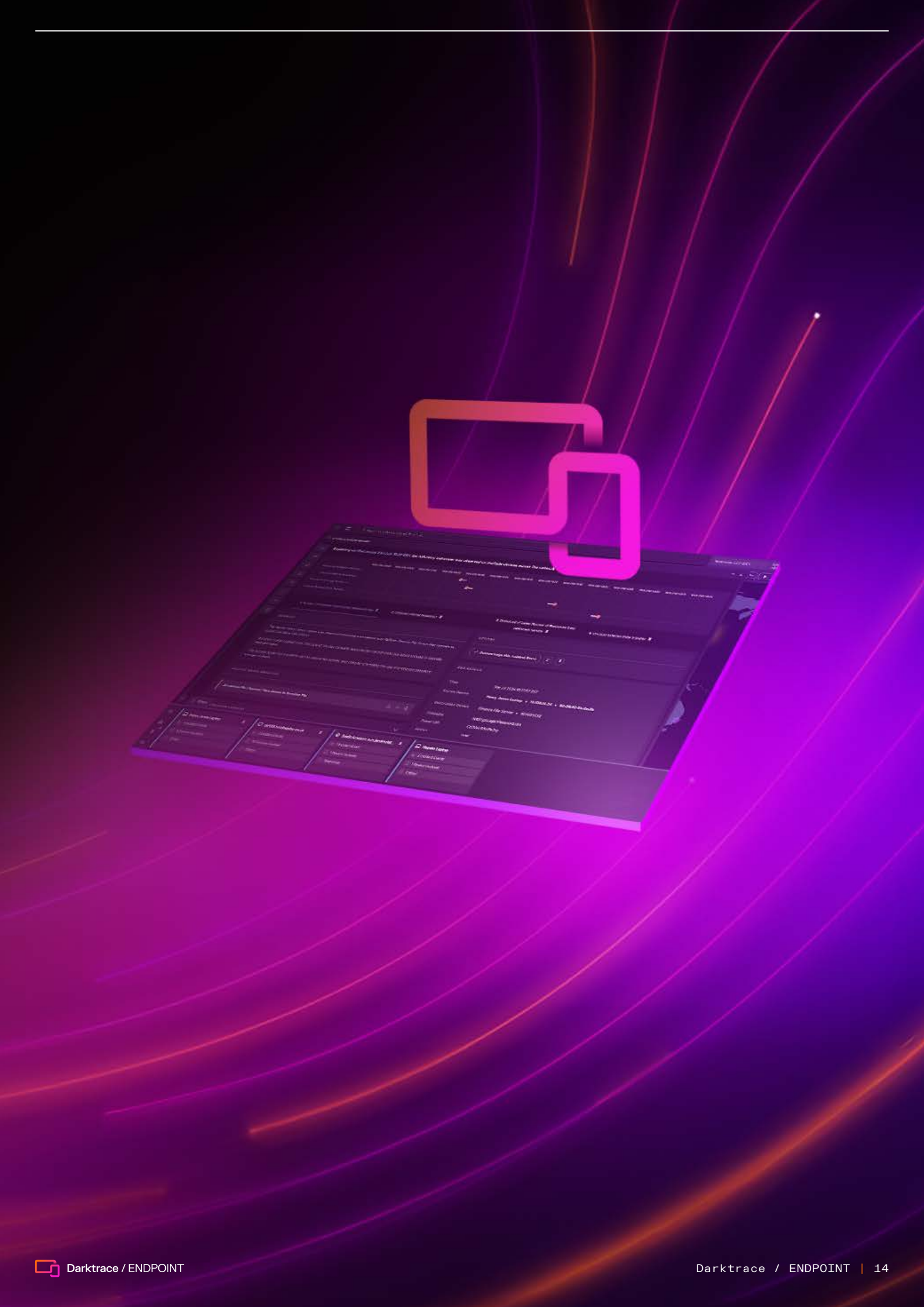
■ 脅威対処オペレーション担当シニアディレクター
Royal Caribbean Group社

“当社はMicrosoftを中心的に使用していますがDarktraceは既存のセキュリティプラットフォームおよびプロファイルにシームレスに統合できます。これは極めて大きな強みであり、一元的な可視性をもたらしてくれます。”

■ テクノロジー責任者
Community Housing Limited社

“Darktraceは導入が簡単で、当社の監視と対処のニーズにも効果的であり、必要なすべての情報を提供してくれます。”

■ 上級情報セキュリティアナリスト
AAA Washington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