DARKTRACE

ネットワークセキュリティソリューションのバイヤーズガイド

NDRの先へ進む

目次

02 **従来のNDRソリューションでは最新のネットワーク攻撃に対応できない**

ステップ 1 可視性のギャップを解消

ステップ 2 リアルタイムに異常を識別して対処

ステップ 3 プロアクティブな状態へ移行

07 **ネットワークセキュリティのオペレーションパフォーマンス向上**

ステップ 4インテグレーションの容易化

ステップ 5 コストと複雑性の削減

ステップ 6 コンプライアンスと報告の効率化

08 **セキュリティツールを統合するのに最適なプラットフォームを選択**

09 **その道のりはここから始まります**

従来のNDRソリューションでは最新のネットワーク攻撃に対応できない

サイバーセキュリティはそれぞれのサイロで進化してきました ーしかし攻撃はそうではありません。今日のネットワーク環境はかつてないレベルで活発に変化し、相互に接続されています。攻撃者はこの複雑性を悪用し、エンドポイントやクラウド環境を標的として、ネットワーク内の水平移動により従来の NDR をすり抜けています。

従来の NDR ソリューションがこれに対応できないのは、明確な境界を持った静的なネットワークを念頭に設計されているためです。それとは対照的に、今日のネットワークは流動的であり、データとユーザーが複数の環境を行き来し、新たな脆弱性を生み出しています。こうした環境の複雑性と規模に対して、ネットワークセキュリティへの新しいアプローチが求められています。

より幅広い保護を提供するために EDR（Endpoint Detection and Response）ソリューションが出現しましたが、これらは多くの場合 NDR ツールとのシームレスな統合が欠けています。断片化により可視性に致命的なギャップが生じ、攻撃者はそこを悪用します。

この課題を解決し、セキュリティチームを支援するために XDR（eXtended Detection and Response）ソリューションが開発されました。

XDR はネットワーク、エンドポイント、クラウドからの疑わしいイベントを相関づけることができますが、最初の感染のほとんどの発生源である E メール等、重要なエリアに対する十分なドメインカバレッジが欠けています。さらに、人手による検証、優先付け、トリアージを必要とします。

しかし、これらのソリューションはすべて、セキュリティオペレーションに対して基本的に受け身のアプローチを取っています。効果的なネットワークセキュリティを実現するには、組織はリアルタイムの検知および対処以外にも、プロアクティブにリスクを削減して攻撃が発生する前に予防することも考えなければなりません。

組織は NDR の枠を超えて、NDR と EDR の機能を統合し包括的な可視性および対処機能をネットワーク環境全体に提供すると同時に、準備度の向上とサイバーリスクの削減を重視したソリューションを検討する必要があります。

複雑なサイバーセキュリティスタックはリスクを不明瞭にしリソースを枯渇させる

個別の課題に対応するために複数のセキュリティソリューションを積み重ねても、思ったような成果は得られません。

たとえ IT チームが既存の NDR 機能を強化する追加の検知および対処ツールを管理するリソースを持っていたとしても ーほとんどの組織にはありませんが ー あまり多数のサイロ型ツールからのデータを監視しようとすると、セキュリティを強化するよりもむしろ弱体化させる、複雑で、分離した、冗長なワークフローが作り出されます。

これによりさまざまなセキュリティ上の欠陥やワークフローの非効率が生じます：

- 統合されていないツール間のギャップによりネットワーク可視性に危険なブラインドスポットが生じる
- あまりにも多数のツールを使用するとアラート疲れにつながる
- インシデントのトリアージがツールごとに順次行われるプロセスとなり、複数の攻撃ベクトルに渡る対処の調整ができず、脅威の優先付けが難しくなる
- 「意味付けまでの時間」が長くかかるため脅威への対処と封じ込めが遅れる
- サイバー攻撃が複数のネットワークドメインに渡って進行する状況を追跡できない

効率の低下に伴ってコストは上昇します。競合するツールやサービスを管理することはセキュリティチームを疲弊させ、運用にかかる費用が増大し、サブスクリプションや更新のコストも上がります。また、セキュリティチームもイベントを調査しインシデント対応（IR）を調整するのに複数のベンダーと連絡を取り、度重なる対話を行う必要が生じます。断片化したアプローチでは、NDR が本来目指していた、ネットワーク全体に対して明確でアクション可能な情報をリアルタイムに提供するという効果が損なわれ、その結果、隙間から侵入する高度な攻撃に対して組織は脆弱なままとなります。

プラットフォームベースのネットワーセキュリティは スケール化および AI をフルに活用することが可能

変化しつづける今日の脅威ランドスケープにおいて、ネットワークセキュリティスタックの統合はリスクを回避し投資の無駄を最小限に抑える上できわめて重要です。

これらの機能を単一のプラットフォームに統合することで、組織はネットワークアクセスを保護するためのワークフローを効率化し、権限を管理し、脅威検知および対処を加速し、規制へのコンプライアンスを確実にすることができます。NDR、EDR、XDR のような受け身のアプローチを脱却して複数の予防テクニックを統合されたプラットフォームに組み込み、さらに検知と遮断にも情報を伝達する機能を備えたソリューションであれば、サイバーリスクをもっと効果的に緩和できるはずです。本ガイドでは、さまざまなネットワークセキュリティ機能をスケーラブルな AI 駆動のプラットフォームに統合し、以下のような効果を目指すためのベストプラクティスを紹介します：

- ネットワーク全体への包括的な可視性によりパフォーマンスを向上し、脅威に対してより高速な検知、およびより正確で自動的な対処を実現する
- ネットワーク運用を最新化および効率化し、コスト、複雑性、規制遵守の負担を軽減する
- プロアクティブなリスク評価によりセキュリティ体制を強化し準備度を高めることにより、より多くの攻撃を防止

組織の成長に伴って、ネットワークアタックサーフェスも必然的に拡大します。現代のネットワークはオンプレミスをはるかに超えて、仮想環境、クラウドおよびハイブリッドネットワークへと拡大しています。2029 年までにインシデントの 50% 以上がクラウドネットワークアクティビティ由来となる [1] ということは、デジタルエステート内のさまざまなエリアにわたる複雑な攻撃に対して、同じ土俵で対抗できるソリューションが必要となるということを意味します。

従業員の 63% がリモートまたはハイブリッドベースで勤務 [2] する状況において、リモート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、これは他の NDR や EDR ツールではカバーされていません。

1 Gartner Market Guide for Network Detection and Response, 2024
2 McKinsey Global Institute, 2023

AI はどれも同じようには作られていない

ほとんどのセキュリティソリューションは AI に関してはほぼ同じアプローチをとっています。それらは、教師付き機械学習、深層学習、およびトランスフォーマーの組み合わせを使ってシステムをトレーニングし、情報を与えています。その際、自社のデータがクラウド上のどこかにホストされている大規模なデータレイクに送出され、そこで他の数千の組織から得られた攻撃データと混合されます。その結果作成される均質化されたデータが AI システム（自社および他社すべての）のトレーニングに使われ、以前に遭遇した脅威に基づいて攻撃のパターンを認識します。

このような方法で AI を使うことは、従来手作業でこうしたデータを入力していたセキュリティチームの作業負荷を軽減することにはなりますが、同じリスクを生じさせることになります。つまり、既知の脅威でトレーニングされた AI システムでは未来の脅威に対応できないという点です。結局のところ、ネットワークをダウンさせるのは未知の脅威です。

この方法が考案された当初においては、サイバーセキュリティに対するアプローチとしてまずまず賢い方法でした。現在の脅威が過去の攻撃に似ているという仮定は、これまで長い間、有効でした。しかし、サイバー犯罪のコモディティ化により攻撃者の参入障壁が下がり、また生成 AI やその他のオープンソースツールにより高度な攻撃を大規模に実行できるようになった今、その仮定は成り立ちません。

Darktrace は組織内のデータに AI を適用します。情報がどこに存在していようとも、Darktrace の自己学習型 AI はすべてのデバイスの組織内の生活パターンにおいて何が「正常」であるかを理解します。その上で、システムはサイバー脅威の兆候であるかすかな動作の逸脱を識別します。この独自のアプローチにより、既知の脅威も新手の脅威も、それがネットワークのどこで発生しても、最初の遭遇時に特定することができます。

検知が優れていてもそれは戦いの半分に過ぎません。Darktrace はこれに加えて、進行中の攻撃がネットワークのさまざまな部分に害を及ぼす前にインテリジェントに阻止することができる、世界初の実証済み自律遮断テクノロジーを提供しています。ダウンタイムにつながる大規模な隔離を行う代わりに、侵害を受けたユーザーまたはデバイスに対して通常の動作を強制することにより、数秒で脅威を無害化することができます。また、インシデントサマリーが生成されるため、リソースが不足しがちなセキュリティアナリストもこれを使って即座にアクションを取ることが可能です。提供されるコンテキスト情報には、事前に定義されたプレイブックでは対応できない、新手の攻撃テクニックが使われたインシデントに対する考察も含まれています。

Darktrace ActiveAI Security Platform はセキュリティの隙間を見つけ出して解消することにより、インシデント対応を超えて、セキュリティオペレーションをプロアクティブな形に変革するよう設計されています。これにより攻撃による影響と損害を抑えることができます。

AI を使ったネットワークセキュリティパフォーマンスの強化

最新のベストプラクティスを取り入れ、先進的 AI を活用することにより、次のような形でネットワークセキュリティのパフォーマンスを大幅に高めることができます：

- ネットワーク全体の脅威およびリスクに対する包括的な可視性を一元的なビューで提供し、複数のドメインにわたりブラインドスポットを解消
- AI駆動による異常検知とビヘイビア分析により、過去の攻撃の知識に依存する必要なく、マシンスピードかつ大規模に脅威を検知し自律的に対処
- 高速で正確な自律遮断機能により水平移動の最初の兆候が発生した時点で脅威をブロックし、被害の可能性を最小化し対処にかかる時間を削減
- より多くの攻撃を防止するためのプロアクティブなリスク評価

■ ステップ 01

可視性のギャップを解消

脅威アクターはサイロ型のソリューションよりも大きな視野を持っています。
マルチベクトル攻撃は DDoS やランサムウェアなどのテクニックを組み合わせ、同時に実行することにより対処者を圧倒し、弱点が見つかればそこに付け入ります。サイロ型のセキュリティソリューションは、検知をトレーニングされた特定の攻撃を識別することができます。しかし、攻撃のライフサイクル全体を構成する複数のイベントをつなぎ合わせることは困難です。

脅威に対してネットワーク全体に渡る一元的な視野を持っていなければ、マルチベクトル攻撃に対する防御は至難の業です。
現代のサイバー攻撃はしばしば複数の環境を横断し、たとえば E メールなど 1 つのエリアから始まってネットワークを水平移動し、最終的にクラウドインフラや OT（Operational Technology）環境にも拡散していきます。従来の NDR システムが脅威を検知する頃には、既に被害は発生しています ― データの盗難、システムを人質にとった身代金要求、運転の中断などが起こってしまっているでしょう。

■ ユースケース

ネットワークのための自己学習型 AI

Darktrace / NETWORK はオンプレミス、仮想、クラウドおよびハイブリッド環境およびリモートデバイスからのネットワークトラフィックを受動的に取り込み、データポイントを抽出してあらゆる接続の暗号化および復号化パケットを分析し、通常とは異なるアクティビティをリアルタイムに見つけ出します。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 NDR 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個々の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を犠牲にすることなく組織専用のセキュリティが実現されます。

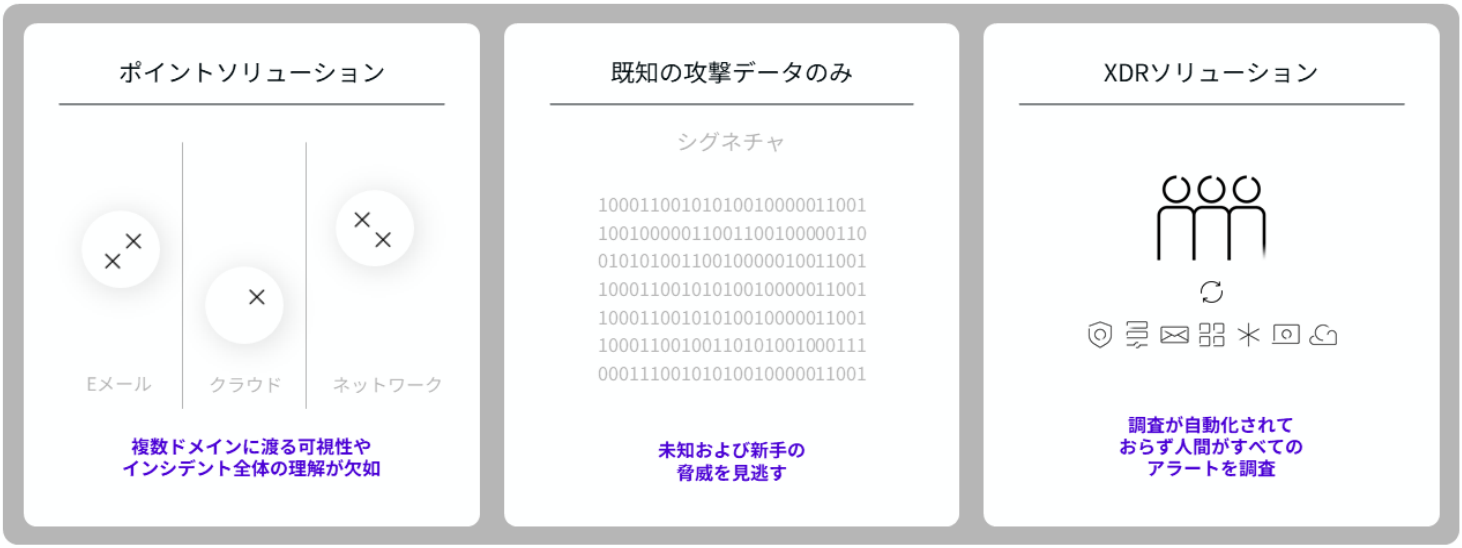

図 01: 既知の攻撃データに依存するXDRやポイントソリューションでは、マルチベクトル攻撃のスピードについていくことはできません。

プラットフォームベースのアプローチにより複数の領域に対するカバレッジを統合

組織の環境全体に渡るエンドツーエンドの可視性により、高度な脅威を効果的に優先付けするためのデジタルエステートに対する包括的理解を得ることができます。

Darktrace ActiveAI Security Platform は、組織内でデータが存在するあらゆる場所に展開することができ、コーポレートネットワーク、クラウド /SaaS アプリケーション、エンドポイント、E メール、そして OT ネットワークまでを含めた環境全体に渡る一元的なデータ、およびリスクに対する可視性を提供します。

その同じ UI に、E メール、Microsoft、Google、その他のアカウントアクティビティもまとめられ、簡単にアクセスできます。これは XDR ソリューションには欠けている機能です。この統合された視野により、脅威に対する分類と対処をより高速、より正確に行うことができ、ネットワークのすみずみまで重大な脅威を見逃すことはありません。

■ ステップ 02

リアルタイムに異常を識別して対処

ほとんどの NDR ツールは静的な機械学習テクノロジーを使ってリスクを認識するようシステムをトレーニングしています。この「バックミラー」的アプローチにおいては、各ツールの基準枠は過去に起こった既知の攻撃でのみ構成されています。このアプローチには、既知と未知両方の脅威を最初の遭遇時に識別するための重要なアドバンテージとなる、個別の組織にとっての不審なアクティビティを識別する能力が欠けています。

脅威の識別を過去のデータに頼るということは、これらのシステムでは過去に発生したインシデントに基づいてしかパターンや異常を識別できないということを意味し、新手の攻撃や高度な攻撃の検知が遅くなります。それと同時に、脅威を順番に処理して対処する形になりやすく、脆弱性に付け込む時間を攻撃者に与えてしまいます。

IBMの報告書によれば：

"セキュリティアプローチにおいてAIおよび自動化を広範囲に活用した組織では、平均して、侵害を発見し封じ込めるまでの期間が108日短縮されています。セキュリティAIおよび自動化は侵害を特定し封じ込めるためのコストを削減し期間を短縮するための重要な投資であることが確認されています。"

AI 主導のプラットフォームは自律的対処を促進

最新の AI 主導のプラットフォームは、異常をリアルタイムに、同期的に分析し、リスクを解決するためのアクションを自動的に実行することでネットワークセキュリティを革新しています。Darktrace ActiveAI Security Platform は個々のユーザーとデバイスの通常の動作パターンを学習し、異常なアクティビティを検知し、コンテキスト化します。一見無害なイベントも、ネットワーク内で深刻な脅威が発生しつつある兆候であることがあります。

Darktrace の持つ組織についての動的な理解は、真の自律的かつ正確なクラウドネイティブの対処を可能にします。あらゆるユーザーおよびデバイスの「正常」についての理解により、Darktrace は「正常」を強制することができます。つまり悪意あるアクティビティだけを切除し、通常の業務は機能を継続させることができるのです。ネットワーク内では、個別の、特定のポート上の異常な接続のブロックを意味することもあります。

遮断アクションは、Darktrace がネイティブなメカニズムを通じて直接行うことも、組織に既にあるセキュリティコントロールとのインテグレーションを通じて実行することも可能です。

■ ステップ 03

プロアクティブな状態へ移行

効果的なネットワークセキュリティには、リアルタイムの検知および対処以外にも、プロアクティブにリスクを削減して攻撃が発生する前に予防することも必要です。これには、脆弱性を見つけ出し、攻撃の可能性をシミュレーションし、それに従って防御を準備するのを支援するソリューションが必要です。このプロアクティブなアプローチには、「攻撃者の視点で考える」ことにより脅威を予測し、組織の防御が試される前に強化しておくことが含まれます。

今日、予防的セキュリティ対策を構築しようとするセキュリティチームは、アタックサーフェスマネジメント（ASM）、攻撃経路モデリング、レッドチーム、侵入テスト、セキュリティ意識向上トレーニング、脆弱性管理、等の組み合わせを管理しなければなりません。これらのツールおよびプロセスは多くの場合相互に連携していることはなく、著しいオーバーヘッドが発生します。複数の予防テクニックを 1 つのプラットフォームに統合し、さらに検知と遮断もサポートするソリューションであれば、サイバーリスクを格段に効果的に緩和することができるでしょう。サイバーリスク軽減のためのより総合的なアプローチは、内部および外部両方のリスクについてのより一体的な視野を持つことから始まります。

$1.76M

■ **平均コスト節約額**

セキュリティにAIを使用している組織でのデータ侵害のコスト

(IBM)

エンドツーエンドのプラットフォームはより多くの攻撃を予防

Darktrace の Proactive Exposure Management 製品は組織内部および外部のアタックサーフェスを理解し、準備度の改善点を見つけ出すことにより、セキュリティチームはセキュリティの隙間やプロセスの潜在的リスクに先回りして対策することができます。その方法とはどのようなものでしょうか？

リスクに対する内部および外部からのビューを統合。Darktrace のエンドツーエンドのアプローチは、アタックサーフェスマネジメントと攻撃経路モデリングの両方を組み合わせて攻撃を予測し回避しようとするものです。これにより防御者は外部の情報（例：「このインフラのどのエリアが最も外部に露出しているか？」）を内部からの視点（例：「この組織の中で最重要情報に最もすばやく簡単に到達できる経路は？」）を組み合わせ、リスクについての包括的かつ対策が可能な理解を得ることができます。

予防策を検知および遮断機能と組み合わせる。リスクについての包括的な理解を検知および遮断メカニズムと組み合わせることでさらに効率を高めることができます。Darktrace / Attack Surface Management および Darktrace / Proactive Exposure Management は、最もリスクと可能性が高い攻撃経路をアナリストに提示します。この情報を検知および遮断システムと共有することによりこれらの経路にあるアセットを緊密に監視し、これらのアセットが関係する不審なアクティビティの調査を優先的に行うことができます。プラットフォーム内では攻撃予防テクニックから得られた情報が自動的に検知および遮断にフィードされ、その逆も行われます。たとえば、AI エンジンはネットワーク内の特に脆弱な経路および危険な状態にある注目されやすいアセットなどを警告し、検知および遮断システムは普段と異なるアクティビティについて警戒を高めることができます。

ネットワークセキュリティのオペレーションパフォーマンス向上

オペレーションパフォーマンスの向上には、AI を使って検知、遮断、予防を最適化することだけでなく、ワークフローを効率化し、ツールの管理を最適化することも必要です。ネットワークセキュリティ機能を、単一のプラットフォームで密接に統合することにより、組織はインシデント対処時間を加速し、セキュリティオペレーションの監視と管理をシンプルにすることができます。オペレーションパフォーマンスの向上により、罰金や賠償責任発生の可能性を最小化するだけでなく、堅牢かつ効率的なセキュリティ慣行を確実に実施することで、全体としてブランドの評価を強化することができます。

■ ステップ 04

インテグレーションの容易化

ネットワークセキュリティに対するエンドツーエンドのプラットフォーム型アプローチでは、1 つのツールが環境全体と統合され、冗長な設定や変換の手間がありません。柔軟なインテグレーションを通じて Darktrace ActiveAI Security Platform はクラウドシステムからエンドポイント、OT システムや従来のコーポレートネットワークに至るまでビジネス全体を隅々までカバーすることができます。Darktrace プラットフォームは組織の既存のセキュリティコントロールと連携し、CISO やセキュリティリーダーはこれまでの投資を最大限に活用して将来の攻撃に対応することができます。

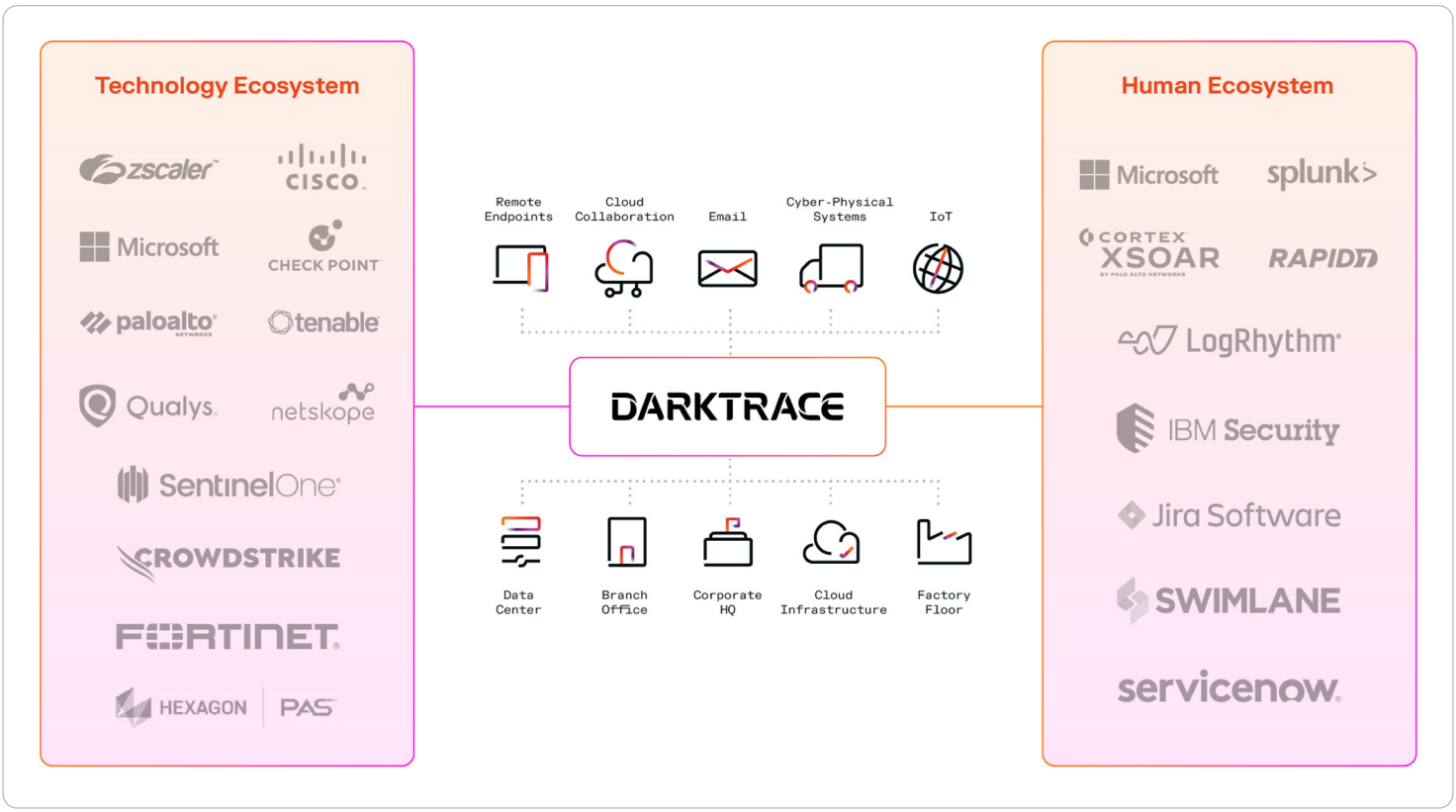

図 02: Darktraceはオープンアーキテクチャで設計されており、既存のインフラや製品を補完してエンドツーエンドのアプローチを実現

■ ステップ 05

コストと複雑性の削減

個別のポイントソリューションを購入して特定のネットワークセキュリティ課題に対応することは、最初はコスト効率が良いように見えるかもしれませんが、統合されたプラットフォームのもたらす長期的な利点は非常に大きいと言えます。

Darktrace のような統合されたプラットフォームは複数のセキュリティ機能およびリソースを単一のソリューションに一元化することにより、複雑性を軽減してベンダー管理をシンプルにすることができます。このアプローチによってサポートを効率化できるだけでなく、費用や予算の面での透明性も高めることができ、コスト管理とリソース配分を改善することができます。AI 駆動のプラットフォームは変化するセキュリティニーズに動的に適応することができます。新しい機能を必要に応じてアクティブ化することができ、追加のベンダーと契約し、テストし、統合する手間がかかりません。この柔軟性により管理オーバーヘッドを最小化し、ビジネスの拡大に応じてセキュリティインフラもスケールさせることができます。

■ ステップ 06

コンプライアンスと報告の効率化

Darktrace はコンプライアンスのためのカスタマイズ可能な機能を用意しています。これによりセキュリティコントロールを、関連する CISA、NIST、CIS-20、FERC、NIS2 などのベストプラクティスフレームワークにマッピングすることが可能です。クリティカルな攻撃経路上で発生しているイベントや異常には自動的にタグが付けられ、MITRE ATT&CK にマッピングされますので、監査やコンプライアンスの報告書作成に役立ちます。

Darktrace の Cyber AI Analyst は分かりやすい言葉で記述された詳細なレポートを生成し、エンジニア以外の担当者もガバナンスの記録に利用することができます。マシンスピードで生成される各種サマリーにはイベントがステップバイステップで解説されており、サイバーセキュリティインシデントについて短い時間内に当局に対し報告しなければならない（例：NIS2 では 24 時間以内の報告が求められます）要件を満たすのに役立ちます。

セキュリティツールの統合に最適なプラットフォームを選択

CISO がネットワークセキュリティに対してプラットフォーム中心型のアプローチを選択する場合、すべてのドメインに渡ってセキュリティを統合し強化できるソリューションを見つけることが課題となります。理想的なプラットフォームは以下を提供するものです：

- **包括的なカバレッジ：**ネットワーク、クラウドアプリケーション、OT（Operational Technology）システムを含めたデジタル環境全体に対して可視性、検知、遮断、予防機能を提供
- **高速な分析：**ネットワークの動作とセキュリティイベントに対してより高速かつより正確な分析を提供することにより、脅威の検知および遮断までの時間を短縮
- **正確な対処：**脅威に対して的を絞った自律的な遮断機能により、攻撃の影響を縮小し中断を最小化
- **AI駆動の予防機能：**組織の内部および外部の脅威サーフェスを分析し、エリアをピンポイントで特定して準備度を高めることにより、セキュリティギャップの解消と潜在的リスクの削減を支援
- **効率的なコンプライアンス達成：**規制へのコンプライアンスと報告プロセスを効率化し、データプライバシー規則やセキュリティ法規制への対応を容易化

過去にとらわれない AI

Darktrace は業界で唯一の自己学習型 AI を提供し、E メール、ネットワーク、クラウドアプリケーション、OT 環境に渡るユーザーの行動に対してプラットフォームを超えた理解を構築します。

お客様のビジネスについてその組織内からリアルタイムで学習することにより、他のプラットフォームでは見過ごされてしまう微細な脅威も認識し対応することができます。他のツールでは捕捉できないかすかな脅威も識別することにより、各攻撃段階を明確かつ包括的に可視化し、効果的な対処を可能にします。

正しいプラットフォームを使用することで防御者はあらゆる事態に備えることができます。現在のネットワークセキュリティニーズに応えるだけでなく新たな脅威にも適応することができ、自動化と人間の専門技術の両方を最適化することができます。従来の NDR やツールの組み合わせから脱却して多機能な AI 駆動のプラットフォームを選択することにより、堅牢、動的かつプロアクティブな、組織と共に進化するセキュリティ体制を実現することができます。

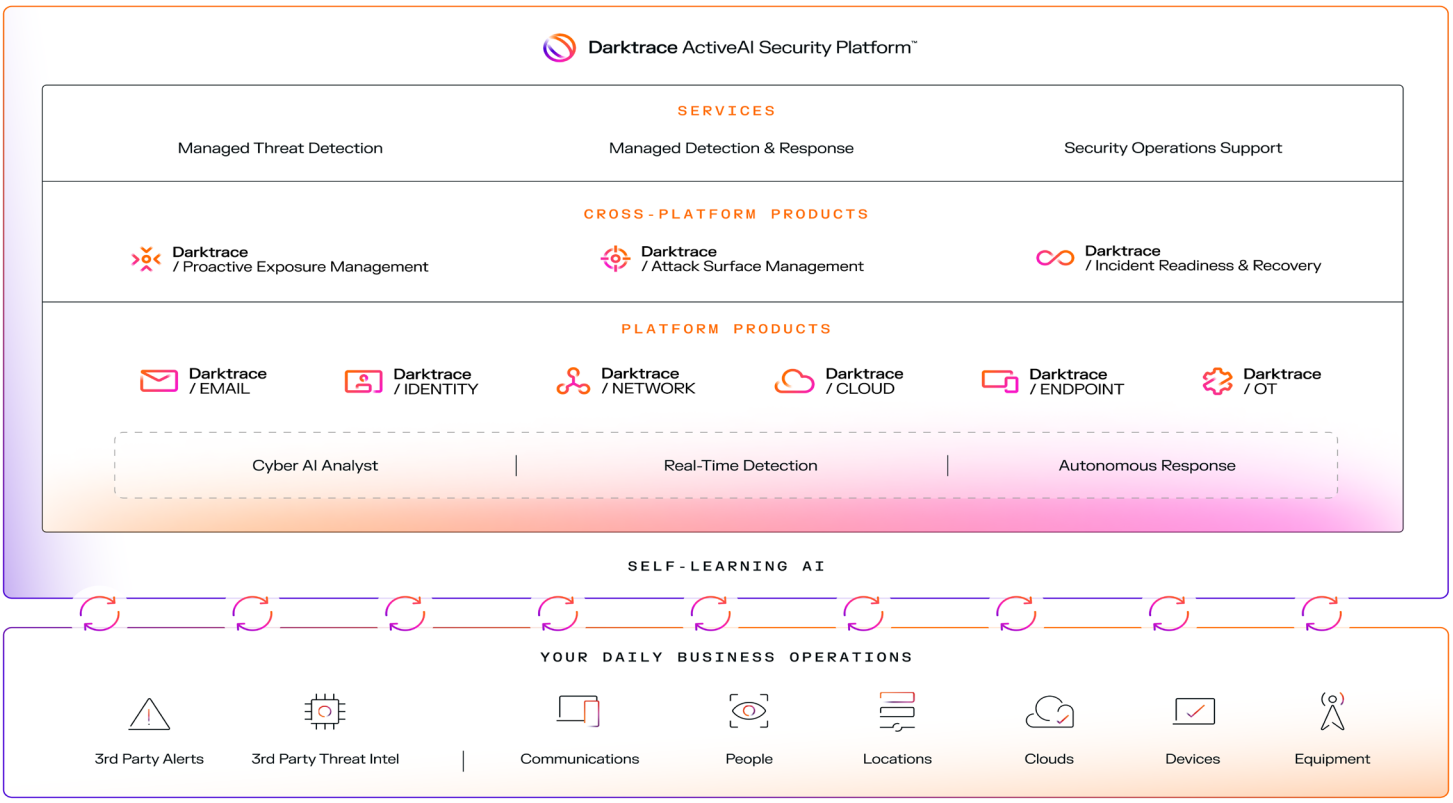

図 03: Darktrace ActiveAI Security Platformはセキュリティーオペレーションセンターをアラートのトリアージ作業から解放し、調査を行い、既知と未知の脅威に対して迅速に検知と遮断を行うとともに、組織内のテクノロジーとプロセスに内在するリスクの隙間を明らかにし、プロアクティブなサイバーアプローチへと移行できるように設計されています。

ダークトレースがお客様のビジネスにどう役立つかを今すぐご確認ください。

その道のりは ここから始まります

無償のデモを申し込む

Darktrace / NETWORK →

あるいは詳しい情報をチェック

Darktrace ActiveAI Security Platform →

■ **ダークトレースについて**

ダークトレースはAIサイバーセキュリティのグローバルリーダーであり、日々変化する脅威ランドスケープに立ち向かう組織を支援しています。2013年に英国ケンブリッジで設立されたダークトレースは、それぞれのビジネスからリアルタイムに学習するAIを使用して未知の脅威から組織を保護する、必要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。ダークトレースのプラットフォームおよびサービスは2,400名を超える従業員により支えられ、世界でおよそ10,000社の組織を保護しています。より詳しい情報については、http://www.darktrace.com/jaをご覧ください。

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