DARKTRACE

Darktrace / EMAIL

従来のEメールセキュリティソリューションを超えたクラウドEメールセキュリティのマーケットリーダー

Eメール脅威ランドスケープは絶えず変化

2023年には、フィッシングがすべての侵害の1/3近くの初期アクセスベクトルでした[1]。 しかし敵は成功率を高めるためのイノベーションをさらに続けています。

フィッシングは攻撃型AIの先頭に立っており、ChatGPTのような大規模言語モデル（LLM）によって巧妙な標的型のフィッシング攻撃が大規模に実行できるようになるとともに、今や攻撃の45%をスピアフィッシングが占めています[2]。 フィッシング以外にも、他のEメール脅威が急速に進化しています。サイバー犯罪者は多段階型のソーシャルエンジニアリング戦術を使って信頼を構築した後にフィッシングメールを送る、あるいはリンクや添付ファイル等の従来のペイロードからの変化も見られます。特に、チャットツールの使用が増え続けており、QRコードのペイロードも59%増加しています[3]。

盗まれたまたは侵害された認証情報を使ったサイバー攻撃の数は2024年に71%増加しており[4]、BEC（Business Email Compromise）やサプライチェーン攻撃を含むアカウントベースの脅威が増えつつあることを示しています。 攻撃者は組織のコミュニケーションのあらゆる側面から侵入するマルチベクトル型のテクニックを使用しており、セキュリティチームの直面する課題は拡大する一方です。

既存のソリューションは過去を向いた状態から抜け出せない

従来のセキュリティソリューションはインパクトの低い一般的な攻撃の阻止には優れていますが、どれもBECのような高度な脅威に対応するための可視性が欠けています。

近年、MicrosoftやGoogle等のネイティブEメールセキュリティプロバイダーは多大な投資を行いましたが、その結果ゲートウェイを運用するセキュリティチームは、同様の能力に重複したワークフローと追加のコストを費やしていることになります。

AI駆動の検知を約束する、より新しいAPIベースのベンダーも最近の攻撃のデータに依存しており、高度な攻撃やゼロデイ脅威を見つけることができません。さらに、これらのツールにはデジタルエステート全体の可視性が欠けているため、Eメールとネットワーク、クラウド、エンドポイント間で攻撃を相関づけることができず、セキュリティチームが攻撃側の一歩先を行くことなどはとても無理です。 今日の脅威ランドスケープおよびビジネス環境において組織を保護するには、ネイティブセキュリティベンダーが提供する能力を強化し、インバウンド、アウトバウンド、ラテラルメール、そしてMicrosoft Teamsを含むメッセージングアタックサーフェス全体にきめ細かい分析を提供するプロアクティブなアプローチが必要とされています。

1 IBM Security X-Force Annual Threat Report 2023
2 Darktrace End of Year Threat Report 2023
3 Darktrace End of Year Threat Report 2023
4 IBM X-Force Threat Intelligence Index 2024

Darktrace / EMAIL

自己学習型AIによる業界で最も高度なクラウドEメールセキュリティ

これまでのEメールセキュリティやポイントソリューションを超えた視野により、従来型のセキュリティレイヤーを通過する脅威の58%を阻止することができます。[5]

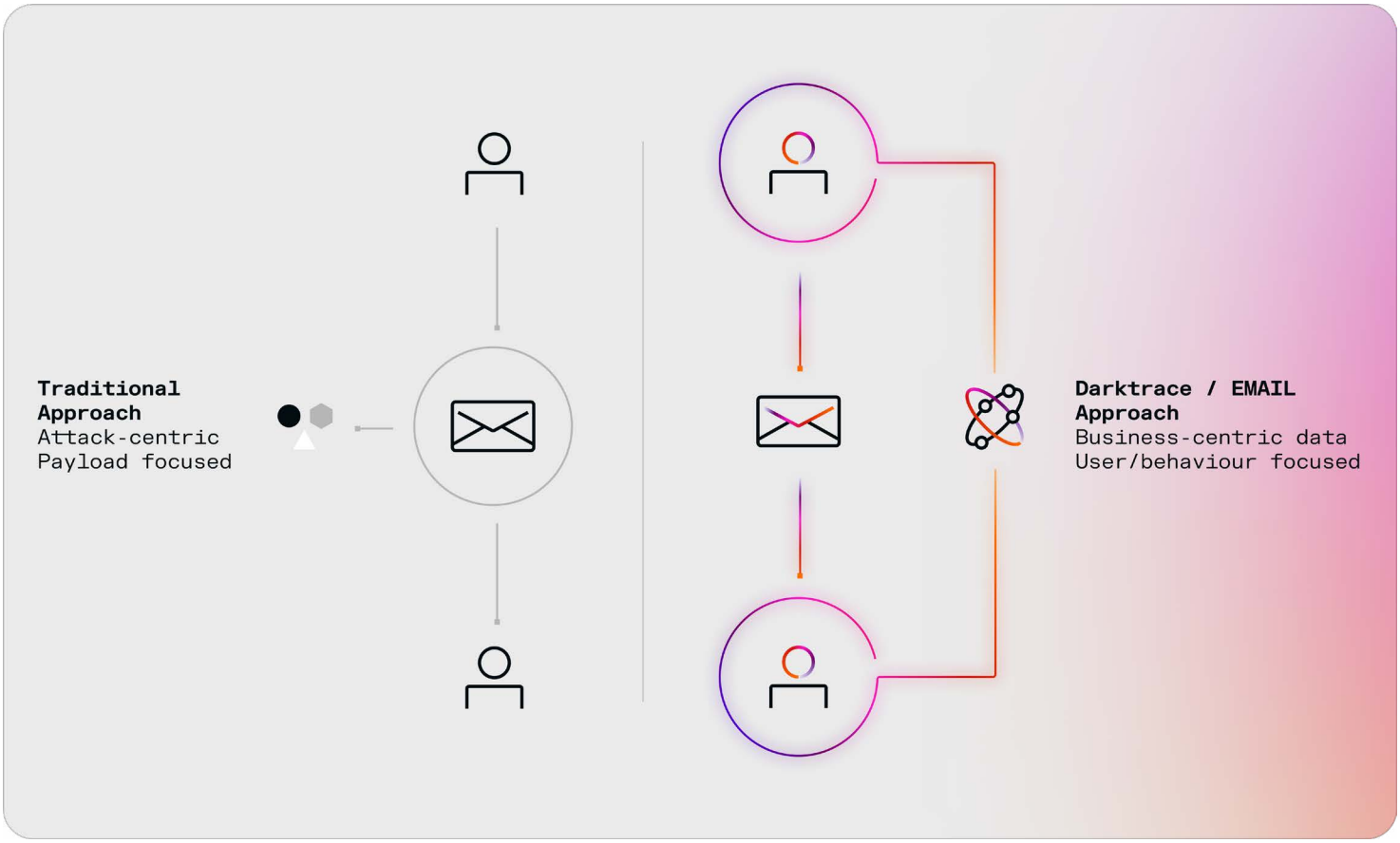
Darktrace / EMAILはEメールとTeamsの両方を含めたインバウンド、アウトバウンド、およびラテラルメッセージ全体に渡ってビジネスセントリックな動作異常検知を行い、ネイティブEメールセキュリティを補強します。

Darktrace / EMAILは組織とあらゆるユーザーアカウントにとっての「正常」を理解する自己学習型AIの上に構築された業界初のEメールセキュリティソリューションであり、BEC、ランサムウェア、フィッシング、サプライチェーン攻撃等の高度な脅威を、既存の機能と重複することなく、また従来のルールやシグネチャ、ペイロードの分析に依存することなく、迅速に識別します。

ネイティブEメールプロバイダーの利点をベースに能力を強化するようゼロから設計されており、より多くの脅威を阻止できるだけではなく、Eメールセキュリティ管理を変革しセキュリティチームへの負荷を劇的に削減することができます。 他のソリューションよりも13日早く脅威を阻止し、既存のネイティブEメールプロバイダーとセキュリティリソースからのROIを最大化できるのは Darktrace / EMAIL だけです。

■ Digimax

以前のEメールセキュリティソリューションと比較して、Darktrace / EMAIL は20-25%多くの疑わしいメールをブロックしました。



DarktraceはEメールセキュリティに対して、ユーザーにフォーカスした、ビジネスセントリックなアプローチをとります。
SEGのアタックセントリックなルールやシグネチャを使用したアプローチとは対照的です。

5 2023年9月1日から12月31日までの間に、Darktrace/Emailは顧客ベース全体で1040万通のフィッシングEメールを検知しました。
これらのEメールの58%はすべての既存のセキュリティレイヤー（Darktrace以外）をすべて通過しています. Darktrace End of Year Threat Report, 2023

6 Darktrace Press Release, April 2023

ビジネス上の利点

クラス最高のEメールセキュリティを利用
他のEメールセキュリティレイヤーを通過したとDarktraceの調査により確認された新手のソーシャルエンジニアリング脅威を、ビヘイビア分析による異常検知で38%阻止[7]

セキュリティスタックのコストの重複を回避
ネイティブEメールセキュリティプロバイダーの提供する機能を置き換えるのではなく、それらに追加して機能強化

ROIを最大化
ネイティブEメールセキュリティのワークフローを共有し、強化する高度なEメールセキュリティを導入

従業員に対するフィッシングの成功率を低下させる
ユーザーがフィッシングの疑いを報告するとリアルタイムのフィードバックが得られ、良性のEメールが報告されるのを60%削減[8]

エンタープライズにおけるユーザーのさまざまなコミュニケーションを保護
インバウンド、アウトバウンド、ラテラルメールに加えてMicrosoft TeamsおよびSaaSアプリケーションまですべての脅威をキャッチ

セキュリティチームの負荷を軽減
Cyber AI Analystの説明可能性を利用してトリアージの時間を90%削減[9]し、メールボックスの修復を自動化することで70%多くの悪意あるリンクを阻止[10]

Eメールからの情報をセキュリティサーフェス全体と統合
Darktraceプラットフォーム全体からの情報を相関づける、統一されたトリアージおよびレポート生成エンジン

Darktrace / EMAILの主な機能

市場をリードするメール保護

他のEメールセキュリティレイヤーを通過したとDarktraceの調査により確認された新手のソーシャルエンジニアリング脅威を38%阻止[11]

Darktrace / EMAIL は、インバウンド、アウトバウンド、ラテラルメール、そしてMicrosoft Teamsメッセージに対するビヘイビア分析およびコンテンツ分析を組み合わせ、アタックチェーン全体に渡り脅威を識別することができます。エンドユーザーの普段の行動を理解することにより高度な脅威をキャッチします。受信されたあらゆるメッセージに対して、言語、口調、感情、リンク、送信者のプロフィール、送信者と受信者の過去の振る舞い、そして彼らのデジタルアクティビティ全体を含む、何千ものデータポイントを分析します。 これらの分析と異常スコアに基づき、そのEメール全体を保留にするか、またはEメールの中の通常とは異なる要素だけを無害化するかの正確な対処を行い、生産性を維持しつつリスクを解消することができます。Darktrace / EMAIL は、リンクの書き直し、添付ファイルの削除、なりすまし送信者の実際のアドレス表示、ゴミ箱へ送る、等を含む様々な自律的かつ的を絞ったアクションを実行できます。 類似の悪意あるコンテンツを持つ攻撃が識別されると、Darktraceは遡及的にアクションを適用して完全な封じ込めを図ることができます（機能のリストについては表2を参照）。

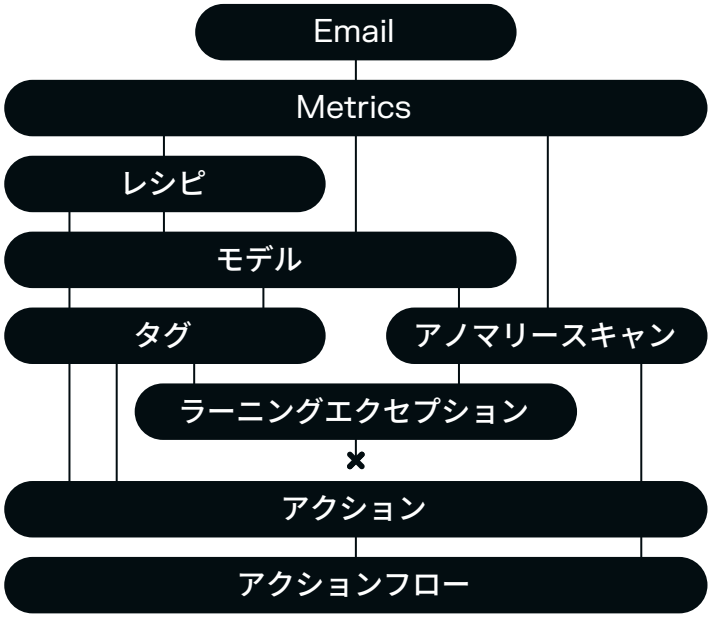


図 01: Darktrace / EMAIL はあらゆるメッセージに対して数千のメトリックを分析し、モデルと異常スコアを割り当てることにより、各コミュニケーションに含まれる具体的なリスクを識別します。

7 Darktrace End of Year Threat Report 2023
8 顧客が Darktrace / EMAIL Outlook Add-in を導入すると、間違って報告されるフィッシングEメールの減少が見られた。 2024年、Darktraceの社内調査
9 Cyber AI Analystが提供する説明可能なナラティブを通じて、セキュリティチームは脅威を理解し判断を行うまでの平均時間を短縮することができた。 2024年、Darktraceの社内調査
10 リンクを含むフィッシングをユーザーが報告すると、第2レベルのトリアージが自動的に実行されリンク分析のインフラにより分析対象のシグナルが展開される。 2024年、Darktraceの社内調査
11 Darktrace End of Year Threat Report 2023

既知および未知の脅威を平均13日早期に阻止[12]

アカウント乗っ取り防止

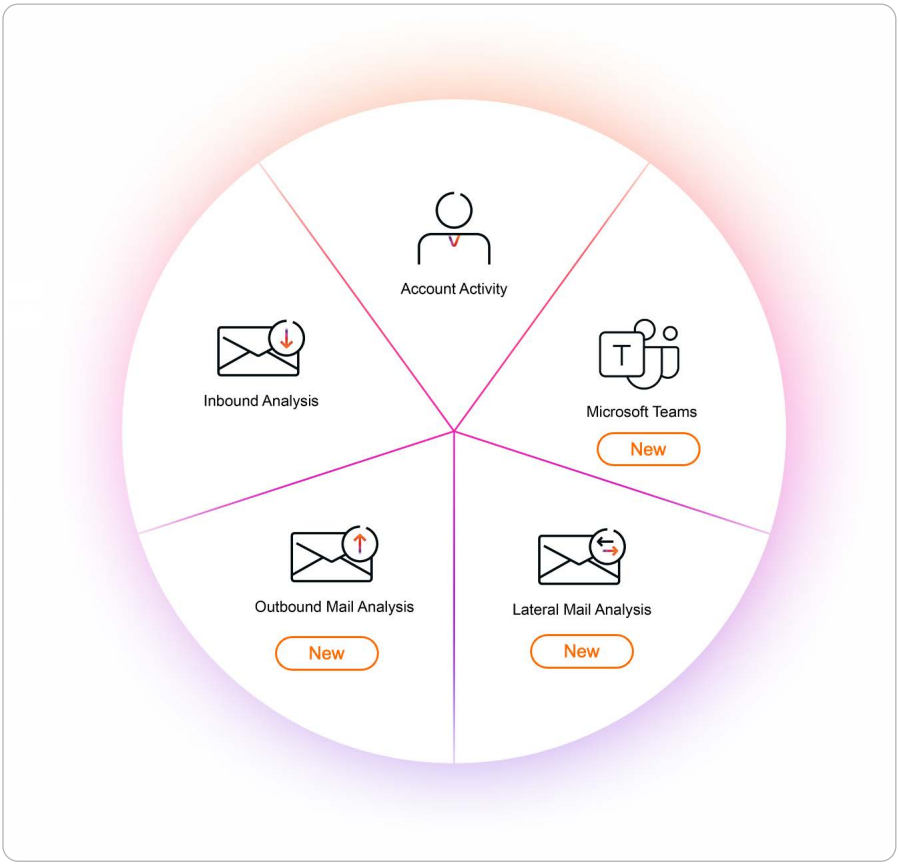
アカウント侵害の最も初期の症状を発見することにより真の深層的防御を実現

Darktrace / EMAILのアカウント乗っ取り保護は、クラウドSaaSアカウントのかすかな異常、たとえば普段と異なるログインパターンや管理アクティビティ等を識別することにより、セッショントークンの不正利用、中間者（Adversary-in-the-Middle）攻撃、認証情報詐取、データ抜き出しなどの高度な脅威をキャッチします。

この分析により、組織全体からのシグナル（ラテラルメール分析、DLP、およびMicrosoft Teamsを含む）で構成される個々のユーザーアカウントプロファイルが作成され、その従業員および組織全体にとって何が正常であるかの理解が構築されます。

検知を行うのにペイロード分析のみに頼る他のソリューションとは異なり、Darktraceはペイロードの投下やデータ流出が起こる前のソーシャルエンジニアリングなど、アカウント乗っ取りの初期症状を見つけ出すことができます。早期の検知により、企業やドメインがBECまたはサプライチェーン攻撃を実行する経路となるのを防ぎ、組織の評判を守ることが可能になります。

さらに、Darktrace / IDENTITYを利用してセキュリティチームはCyber AI Analystからのコンテキストを考慮した調査によるより深い考察を取得し、また自律遮断機能により脅威をマシンスピードですばやく封じ込めることができます。



Darktraceはメールフローおよび通信パターン全体からのさまざまなシグナルを統合しアカウント侵害の症状を判断

12 13日間とは、フィッシングペイロードの存在をDarktrace/Emailが検知してから、他のEメールセキュリティテクノロジーにより報告された16の独立した情報源の中で最も早い日との間の平均日数。Darktraceの社内調査：https://darktrace.com/news/darktrace-email-defends-organizations-against-evolving-cyber-threat-landscape

エンドユーザーおよびSOCワークフロー

エンドユーザーからのフィッシング報告の質的向上、および巧妙な悪意あるWebリンクの検知を 60%以上改善[13]

Darktrace / EMAIL はエンドユーザーによる報告を根本的に改善してセキュリティチームのリソースを節約します。他のソリューションではエンドユーザー報告を質の低いものと仮定していますが、Darktraceはエンドユーザーのセキュリティ認識の向上を優先づけることにより、報告の質の向上を実現します。

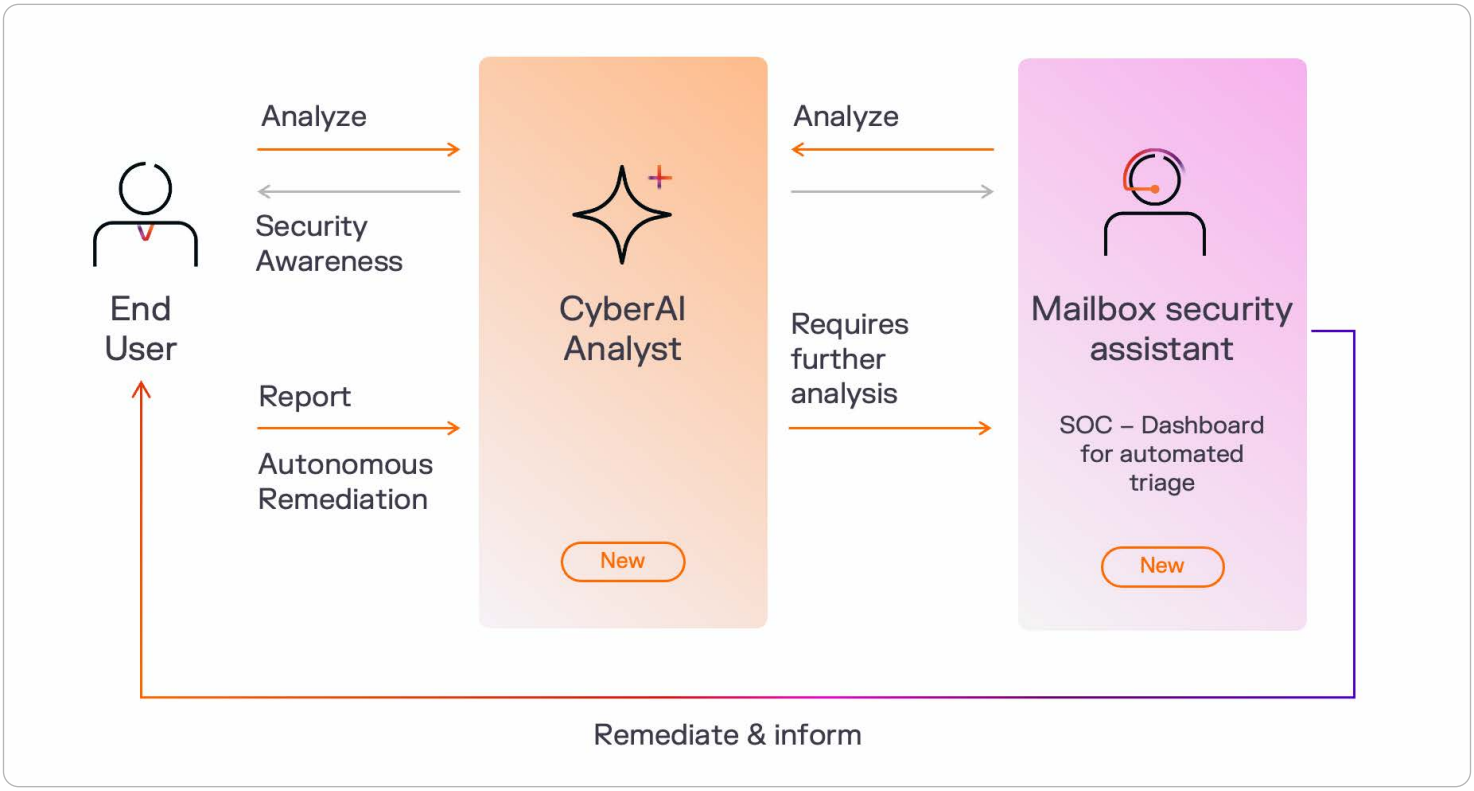
有害な可能性のあるEメールに対してCyber AI Analystが経緯説明を生成し、コンテキストに応じてバナーを表示することにより、ユーザーが疑わしいアクティビティを評価し報告する能力を高め、無害なEメールが報告される数を**60%削減することができます**[14]。

AIがユーザーから学習して検知を補強するのに加えて、何が正常であるかをAIが学習する際にユーザー間の相互のやりとりも情報として使われ、AIの意思決定と全体的精度を強化していきます。

次第に、AIはユーザーが受信した非生産的メールを整理するようになり、ユーザーが取り戻した**生産性により年間何百時間もの節約となります。**[15]

Eメールが報告されると、Darktrace / EMAILのMailbox Security Assistantは、さらに多くの動作シグナルを組み合わせた二次分析を行ってトリアージを自動化します。従来よりも20倍多くのメトリックを利用し、高度なリンク分析に基づき、巧妙な悪意あるフィッシングメールを70%多く検知することができます[16]。これにより、セキュリティアナリストが人手でトリアージを行う面倒な作業を直接的に軽減し、セキュリティチームに送られるEメールの数を減らすことができます。

Darktrace / EMAIL は自動化によりインシデントあたりの調査時間を短縮します。ライブインボックス表示により、セキュリティチームは直感的な検索機能、Cyber AI Analystレポート、モバイルアプリケーションによるアクセスを組み合わせた、一元化されたプラットフォーム上で対応することができ、**複数のコンソールを切り替える面倒を解消してインシデント対応を加速することができます。**

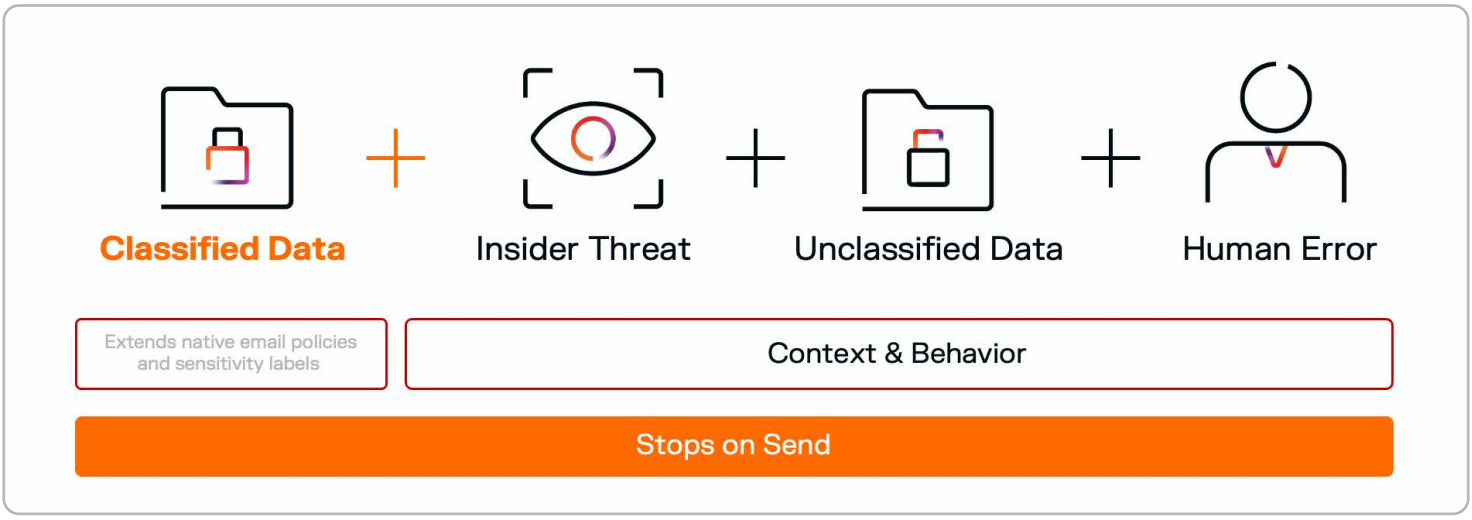


Darktraceはエンドユーザーを底上げしてセキュリティチームにかかる負荷を劇的に削減すると同時に、調査が開始された場合には分析を一元管理して高速化します

13 顧客が Darktrace / EMAIL Outlook Add-in を導入すると、間違って報告されるフィッシングEメールの減少が見られた。2024年、Darktraceの社内調査
14 顧客が Darktrace / EMAIL Outlook Add-in を導入すると、間違って報告されるフィッシングEメールの減少が見られた。2024年、Darktraceの社内調査
15 すべての受信箱に対して、それぞれの受信箱に対する動作に基づいてアクションが自動化され、UIには1ユーザーあたりの節約された時間数が表示される。2024年、Darktraceの社内調査
16 リンクを含むフィッシングをユーザーが報告すると、第2レベルのトリアージが自動的に実行されリンク分析のインフラにより分析対象のシグナルが展開される。2024年、Darktraceの社内調査

Darktrace / EMAILアドオン

データ損失防止（DLP）



ネイティブEメールのタグに基づいてあらゆるアウトバウンドメール脅威をブロックする自律的なデータ損失防止機能により、未知の、偶発的な、および悪意によるデータ損失を阻止

個別のユーザー、グループ、そして組織レベルでの正常についての理解に基づき、Darktrace / EMAIL はアウトバウンドEメールに対してアクションを実行し、未知の、偶発的な、あるいは悪意によるデータ損失を阻止 従来のDLPソリューションは、分類されたデータのみを考慮して各データに対する手動でのラベル付けに依存する、あるいはルールを作成してパターン一致を行い、特定のタイプのデータの組織からの流出を防止しようとするものでした。 しかしデータが常に変化を続ける今日の世界において、正規表現やフィンガープリンティングによる検知ではもはや不十分です。

- **ヒューマンエラー**
  それぞれのユーザーにとっての正常とは何かを理解しているため、Darktrace / EMAIL はEメール誤送信も識別することができます。データに正しくラベル付けされている、あるいは機密扱いではない場合にも、Darktraceはそのデータが送信されているコンテキストからデータ損失の可能性もあることを認識し、介入してユーザーにメッセージを表示します。
- **機密扱いされていないデータ**
  従来のDLPソリューションはユーザー定義のラベルに基づいて機密扱いのデータのみを対象にしているのに対し、Darktraceはラベル付けがまだ行われていない、あるいはラベル付けできない幅広いデータにも分析を広げ、すべてのEメールのコンテンツおよびコンテキストの理解を適用してデータ損失を検知します。
- **内部関係者からの脅威**
  悪意を持ったアクターがアカウントを侵害すれば、暗号化されたデータや知的財産およびその他のラベル付けされていないデータの抜き出しが行われ、検知を免れるかもしれません。Darktraceはユーザーの振る舞いを分析し、個々のアカウントからの不審なデータ流出をキャッチします。

Darktrace/ EMAILにより、これまでに行われた分類の作業を活かすことができます。DarktraceのAIはMicrosoft Purviewポリシーおよび秘密度ラベルを使用することができ、セキュリティチームは重複したワークフローの発生を回避できます。2つのアプローチを組み合わせることで、自社データに対するコントロールと可視性を維持することができます。

AIを使ってDMARCをすばやく展開

- **深い可視性とコントロール：** 業界初のAI支援によるDMARCにより組織のドメインを使用している第三者に対する深い可視性とコントロールを提供します。
- **スプーフィングとフィッシングを防止：** エンタープライズドメインからのスプーフィングとフィッシングを継続的に防止しながら、自動的にEメールセキュリティを強化しアタックサーフェスを縮小します。
- **コンプライアンスを簡単に達成：** GoogleやYahooからの要件を簡単に満たすことができます。
- **可視性を確保：** シャドーITや組織のブランドに代わってメールを送信するサードパーティベンダーに対する可視性を得ることができます。
- Darktrace / EMAIL-DMARC はDarktrace製品プラットフォーム全体と統合されており、情報を共有することでビジネスのセキュリティを高めるのに役立ちます。
- **Azure Marketplace での購入が可能**

MicrosoftとDarktrace ー相乗効果

Microsoft Azure上でホストされるDarktrace / EMAILは、自己学習型AIを使用してMicrosoftのセキュリティを補完し、多層的な防御を構築して脅威検知に対する攻撃セントリックなアプローチとビジネスセントリックなアプローチを融合します。

Darktrace / EMAIL はMicrosoftを考慮してワークフローや機能が重複しないよう設計されており、Microsoftの購入やリソースへの投資がDarktraceにも活かされます。

MicrosoftとDarktrace / EMAILは連携してアーカイブ等のEメール運用の基本的要素を提供するとともに、ペイロード投下前の初期段階のフィッシングの試みも含めた、市場をリードする既知および未知の脅威検知機能を実現します。

Darktrace / EMAILはMicrosoft 365および Microsoft Exchangeの両方と統合できます。

運用上の利点

最大30倍高速
オプションでジャーナリングを使用することによりAPIのみの運用のレイテンシを短縮

メールフローの中断なし
インラインでのインストレーションではなく、MXレコードのリダイレクト不要

数分で柔軟にインストール可能
APIのみまたはジャーナリングを追加

SOC業務の手間を60%削減
エンドユーザーによるフィッシング攻撃の報告に力を与え理解を高める

より多くの高度な不正URLおよびWebページを検知
先進的なビヘイビアWeb分析により他の大手クラウドEメールセキュリティベンダーよりも70%多くの高度な脅威を阻止

1つのコンソールで調査を完結
Eメールおよびメッセージングの脅威に対して包括的な検索、分析、レポート機能を提供

展開

柔軟な展開アプローチにより
最大30倍高速に脅威に対処[17]

- **パフォーマンスの向上：** SEGは中央管理されたデータに依存しています。つまり過去に見られた脅威しか検知できません。Darktraceはすべてのコミュニケーションに対して無制限の可視性を有しており、ビヘイビア異常検知と組み合わせてあらゆる既知と未知の脅威を阻止することができます。
- **保守作業の解消：** SEGはルールと検知方法の静的な集まりであり、攻撃者に遅れをとらないためには時間のかかる人手による調整を必要とします。Darktrace AIはユーザーの振る舞いに基づいて適応し、ブロックリストを更新する必要なく脅威を阻止することができます。
- **効率的な展開：** Darktrace / EMAIL はネイティブEメールセキュリティプロバイダーを置き換えるのではなく共存するように設計されているため、SEGのようにMXレコードのリルートを行う必要がありません。そのためネイティブセキュリティ機能はそのままに、Darktraceは重複することなくさらなるセキュリティを提供することができます。
- **コストを集約してROIを改善：** ネイティブEメールセキュリティプロバイダーと並行してSEGを運用する重複したコストを解消し、最適化されたワークフローで実現されるより強力な保護により投資効果を高めることができます。

■ 表1

DARKTRACE / EMAIL展開オプション

提供モデル	M365展開：Microsoft 365 （旧Office 365） Business Essentials ライセンスまたはそれ以上が必要 ハイブリッドExchange展開：Exchange Server 2016 およびそれ以上 オンプレミス展開：Exchange Server 2013 SP1、またはNTLM(v2)を設定したExchange Server 2016 / 2019 Google展開：Google Workspace EnterpriseまたはEnterprise for Education License（またはそれ以上）
展開オプション	APIのみまたはAPI+ジャーナリング
リテンション期間	最大90日間のログ、アクションを実行されたメールに対しては21日間、アクションされていないメールに対しては7日間、フラグを立てられたメールに対しては30日間

17 ジャーナリングを追加することにより、APIのみの展開の場合に発生するレイテンシが解消されます。Darktraceの調査による

Darktrace ActiveAI Security Platform

Darktrace / EMAILはDarktrace ActiveAI Security Platformの一部であり、Eメール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ネットワーク、クラウド、エンドポイント、アイデンティティ、およびOT全体のセキュリティの可視性を高めることができます。

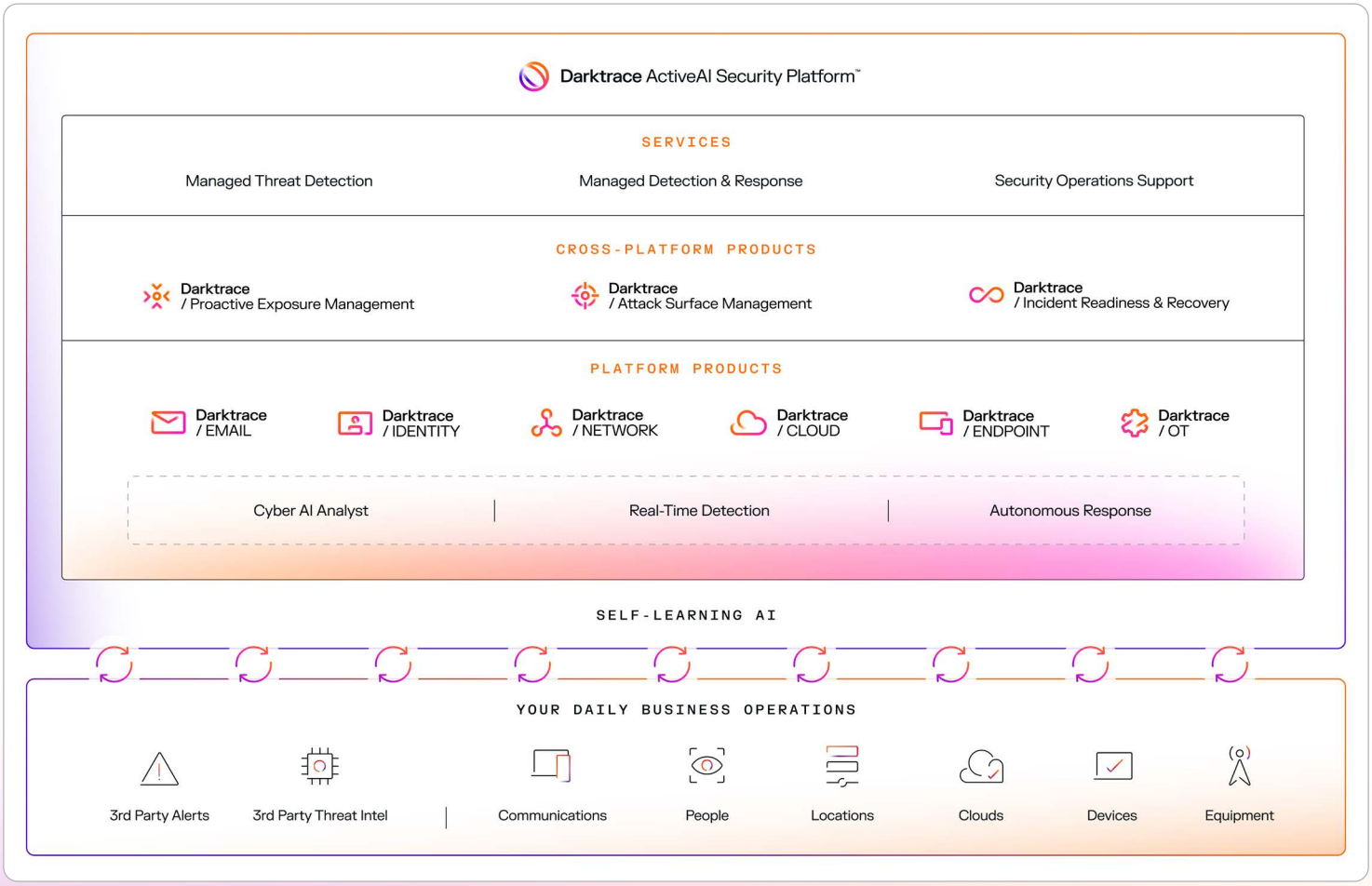
Darktrace / Attack Surface Management は、最もよく見られる攻撃ベクトルであるEメールに基づいて攻撃経路を想定します。またEメールからトリガされた検知は、Eメールによって運ばれてきた攻撃の結果発生したかもしれないネットワークまたはSaaSイベントの識別の強化にも使われます。

また、Cyber AI Analystもマルチドメイン攻撃の分析にEメールの情報を取り込むことで、手作業でデータを集めることなく完全な調査を実施することができます。 その一方で、Eメールの全体的アタックサーフェスもAIを使ったDMARCにより縮小され、スプーフィングやフィッシングの阻止により予防的に防御を強化することにつながります。

Darktraceは1つのホリスティックなプラットフォームで予防的なサイバー防御を提供するまったく新しいソリューションです。

これを実現するため、Darktraceは日々のビジネスオペレーションから継続的に学習し、Eメール、クラウド、OT、エンドポイント、アイデンティティ、アプリケーションおよびネットワークを含む組織内部のネイティブソース、そしてサードパーティセキュリティツールや脅威インテリジェンス等の外部ソースから取り込まれたエンタープライズデータのコンテキストを適用する、ActiveAI Security技術を市場に先駆けて開発しました。

このアプローチを通じて、Darktraceは個別のポイントに限定されるサイロ型のアプローチのような制限を受けることなくセキュリティインシデントの可視化と相関づけを行う能力を提供します。



Darktrace / EMAIL のアクションョン

ビジネスのフローを維持したまま、的を絞ったアクションによりリスクを削減

■ 表2

Darktrace / EMAIL のアクション

配信のアクション： メッセージを保留にするまたはゴミ箱に移動	Darktrace / EMAILは疑わしいコンテンツあるいは添付ファイルを理由にメッセージを配信せず保留するまたはゴミ箱に送ることができます。 保留にされたメッセージは調査後オペレーターが再処理およびリリースすることができます。
リンクをリライトする	URLはリライトされ、先に進む前にユーザーの確認を求めます。これにより第2段階のチェックを受けるようにします。疑わしいリンクには、ロックされている旨のメッセージを表示し、アクセスを防止するとともにユーザーの意図を記録します。リライトされた後、疑わしいリンクは分析され、ユーザーにアクセスさせてよいか、ブロックすべきかが判断されます。
添付ファイルに対するアクション： 添付ファイルを変換または削除	Eメールの1つまたは複数の添付ファイルが安全なフォーマットに変換され、通常は初期画像変換でPDFに変換することによりファイルが平坦化されます。これは添付ファイルを意図された受信者に配信しますが、リスクが大幅に軽減されます。または、フォーマットやリスクによっては添付ファイル全体を削除することもできます。
スプーフィングを見破る	「なりすまされた」名前を送信者のアドレスから削除し、通常の状況では受信者から隠されている実際の「エンベロープ送信者」で置き換えます。
バナーを追加する	アクション済みEメールの先頭にカスタムテキストのバナーを追加し、受信者に見えるようにします。バナーの色はアクションを設定するときに選択した深刻度によって決まります。複数のタグを同じEメールに追加して、検知された脅威プロファイルを表すことができます。Eメールにタグを追加することにより、エンドユーザーはそのEメールについて検知された潜在的脅威を知ることができます。

■ **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