データシート

AWS 向けサイバー AI セキュリティ

自己学習型 Cyber AI により、Darktrace はお使いの AWS クラウド環境にこれまでにないリアルタイムでの可視性と自律的な脅威検知、対応、調査機能を提供します。

主要な利点

- ✔ AWS を含むネットワーク全体のワークロードや管理アクティビティに対する完全なリアルタイムの可視性
- ✔ 自己学習型 AI はポリシーベースの防御をすり抜ける高度な脅威を検知、解釈、およびそれらに対処
- ✔「オンザジョブ」で学習し、ダイナミックに分散したワークフォースおよびワークロードと共に進化
- ✔ Cyber AI Analyst は脅威の調査を高速かつ大規模に自動化し、トリアージの時間を最大 92% 短縮

「Darktrace 導入以前、当社の AWS 環境はブラインドスポットでした。Darktrace により、分散したインフラ全体をリアルタイムに防御する Cyber AI テクノロジーで武装することができました。」

Innovating Capital

動的なワークフォースの自律的な防御

Darktrace の力により、リアルタイムの可視性を獲得し、重大な設定ミスから内部関係者による脅威まで、もっとも検知の困難な新種の脅威から防御することが可能になります。

Darktrace Immune System は Cyber AI を使って組織のすべてのユーザー、テクノロジーおよびリソースの通常の「生活パターン」を学習し、脅威の出現を示す最もかすかな異常も認識することができます。

図 1: Darktrace Immune System に表示された AWS 環境

新種の、および高度な脅威から AWS を保護

データ流出および破壊

- 異常なデバイス接続およびユーザーアクセス、および不審なリソースの削除、変更、移動を検知します。

重大な設定ミス

- オープンな S3 バケット、異常な権限変更、コンプライアンスに関連したデータおよびデバイス周辺の異常なアクティビティを特定します。

認証情報の漏えい

- ブルートフォース攻撃の試み、不審なログイン元および時間、さらにルールの変更やパスワードのリセットなどを含む不審なユーザーの挙動を特定します。

内部関係者による脅威および管理者権限の濫用

- 機密ファイルへのアクセス、リソースの変更、役割の変更、ユーザーの追加 / 削除を含め、悪意ある内部関係者による脅威のかすかな兆候を識別します。

VPC Traffic Mirroring の活用による可視性の強化

AWS VPC Traffic Mirroring により自己学習型 AI が粒度の細かいパケットデータにアクセスすることが可能になり、Darktrace Immune System は生データから何百もの特徴を抽出しお客様の AWS クラウド環境の詳細な動作モデルを構築することができます。

VPC Traffic Mirroring により得られる AWS 環境に対するリアルタイムの可視性は、Darktrace の Cyber AI がビジネスの変化に応じて絶えず適応を続け、「オンザジョブ」で学習するのを助けます。Darktrace はリアルタイムで学習する唯一のセキュリティソリューションを提供します。これはクラウドの進化のスピードと規模を考慮すれば極めて重要な機能です。

Darktrace Security Module for AWS はさらなる可視性を提供するとともに、AWS CloudTrail とのやり取りを通じて運用および管理アクティビティに対して AI を使った監視を行います。

クラウドで業務がどのように行われるかについてのこうした深い知識により、Darktrace は次を含む AWS サービス全体に渡るトータルなカバレッジを提供します：

- Certificate Manager
- Athena
- EC2
- IAM
- Lambda
- RDS
- Route 53
- S3
- VPC
- DynamoDB

Darktrace Immune System: 自律的サイバー防御

検知

高度な自己学習型 AI により、Enterprise Immune System は極めて巧妙なあるいは新しい脅威であっても、あらゆる弱い兆候を自律的に検知し、相関付けることができます。

AWS クラウド環境及び組織全体のアクティビティについてのリアルタイムかつコンテキストを含めた理解をベースに、Enterprise Immune System はポリシーベースのコントロールや他のセキュリティソリューションがまったく対処できない脅威を識別することができます。

対処

Darktrace Immune System プラットフォームは、Antigena の自動対処機能により AWS 内のデジタルデータ及びアセットに対して 24 時間、週 7 日の防御を提供します。

Darktrace Antigena はマシンスピードかつ正確に的を絞って人間の代わりに攻撃を中断できる市場唯一のテクノロジーであり、セキュリティチームが多忙を極めている、あるいはその場にいないときにも高度な防御を提供します。

調査

あらゆる脅威は Darktrace Cyber AI Analyst により自動的に調査されます。業界で初めて、Cyber AI Analyst はセキュリティインシデントを自動的にトリアージし、解釈し、その全貌をレポートします。

Cyber AI Analyst Incident Reports にはエグゼクティブにもわかりやすいイベントの概要や推奨される対応方法が記載されている他、措置に必要なあらゆる重要な情報が含まれています。 AI テクノロジーによりトリアージの時間を最大 92% 削減します。

エンタープライズ全体をカバーする一元的かつ AI ドリブンなセキュリティ

Darktrace Immune System は AWS を通じて、あるいはハイブリッド運用形態で簡単に導入することができ、お客様のクラウド環境、さらには SaaS アプリケーション、E メール、コーポレートネットワーク、産業用システム、リモートエンドポイントに対するカバレッジを提供します。

根本的に独自のアプローチをとる Darktrace Immune System は、組織全体の情報を相関づけリアルタイムに適応する業界唯一の自己学習型プラットフォームです。

これは、ビジネスとワークフォースがますます複雑化しダイナミックになりつつあるなかで特に重要な利点です。Darktrace の統一されたセキュリティプラットフォームにより、Cyber AI はインフラ内の別々のエリアで発生した不審な挙動の点と点を結び付け、クラウドセキュリティが組織のそれ以外の領域の監視から孤立するのを防ぎます。

「最近では AI ワークロードの大部分はクラウド内で処理されています。そのため、当社はインフラ面とクライアントのサポート面の両方において、AWS と緊密に協力しています。」

ダークトレース、グローバル CISO、マイク・ベック

[ダークトレース、グローバル CISO、マイク・ベックの AWS に関するインタビューを読む]

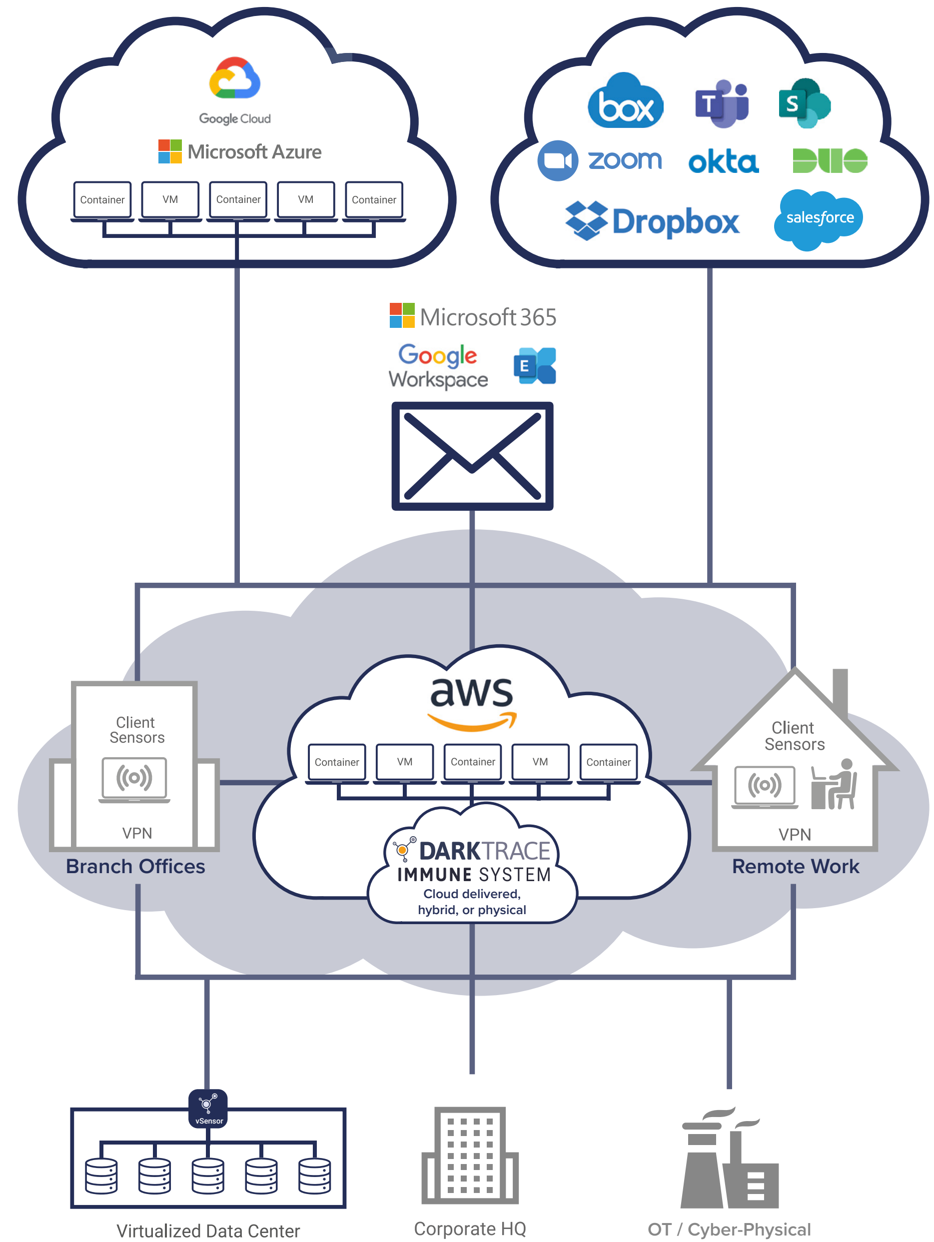

図 2: Darktrace の自己学習型プラットフォームは組織全体の防御を一元化