CISOのためのクラウドセキュリティガイド

マルチクラウドの世界で
新手の攻撃を防御

目次

概要

クラウドの広範な使用はビジネスを変革し続けており、サイバーセキュリティシステムの対応が急がれています。

動的なマルチクラウド環境の速度と規模はかつてない複雑な状況を作り出し、マルチベクトル型の、AI による攻撃も出現しつつある中、企業はビジネスを保護するために従来のセキュリティツールだけに依存することはできなくなりました。

脅威に対する従来の検知、分析、優先付け、対処のアプローチではあまりにも時間と労力がかかりすぎ、より高度な最新の標的型攻撃を発見し対応することができません。

ばらばらのツール、そして一時点のみの可視性では危険な視界のギャップが残ります。現在の攻撃者はこれを利用してクラウドベースのアセットを狙い、エンタープライズネットワークに潜み水平移動して攻撃を仕掛けます。

セキュリティチームは、もはや一時点での可視性や教師付き機械学習（ML）でトレーニングされたシステムに頼ってクラウドをサイバー攻撃や脆弱性、そして侵入につながる設定ミスから守ることはできないのです。

新しいクラウドセキュリティプラットフォーム、フレームワーク、およびベストプラクティス、たとえば、CWPPs（Cloud Workload Protection Platforms）、CIEM（Cloud Infrastructure Entitlement Management）、CDR（Cloud Detection and Response）、CSPM（Cloud Security Posture Management）、そしてCNAPPs（Cloud-Native Application Protection Platforms）などは、統合された可視性と AI のよりスマートな利用によりスケールとのバランスを取ろうとしていますが、自社のビジネスに適切なアプローチはどれなのか、どう判断すれば良いでしょうか？

本ガイドでは、現在のクラウドセキュリティの課題、リスク管理に対する CISO の選択肢、そして Darktrace / CLOUD が従来のアプローチに伴う限界を乗り越えてビジネスを既知の攻撃と新手の攻撃の両方からどのように保護することができるかをご紹介します。

クラウドの普及はまだ初期段階なのでしょうか？

大きな視点で見ればこの市場が膨大であることは明らかであり、まだまだ未利用の領域が大きく、現在の経済的混乱の後も続くと思われます。2023年には、クラウドの支出は6000億ドル、すなわち総IT支出の約12%に迫ると予測されています。

■ Forbes

クラウドが新しい機会、
そしてリスクへの扉を開く

企業はクラウドの潜在力をまだ利用し始めたばかりです。過去数年で10社のうち9社近くがクラウド利用の範囲を拡大していますが、アクセンチュア社のCloud Outcomes調査レポートではそのうち期待していた価値を引き出したのはわずか42%であることが明らかになりました。[1]

複雑な結果となった理由の一部は、2020年以降の予期せぬデジタル化の速度にあると思われます。無数のクラウド、ネットワーク、エンドポイント、アプリケーションに渡る複雑な環境が急速に拡大したのです。

■ 86%

企業の86%は、2020年以後クラウド化への取り組みの量および/または範囲が拡大したと回答

Accenture

セキュリティが導入を遅らせる

急激な変化に伴い、セキュリティに関する懸念が企業のクラウド移行戦略を再考させ、中核的ビジネスアプリケーションの混乱を遅らせようとする動きがあります。セキュリティインフラがビジネスを保護するためにクラウドも保護しなければなりませんが、クラウドの敏捷性でサイバーセキュリティの堅牢性が損なわれてはなりません。

動的なクラウド環境はワークロードの追加や削除、あるいは開発者がセキュリティチームに知らせることなく自由に移行を行うことなどから絶えず変化しています。

デジタル化やクラウド移行がサイバーセキュリティを損なうケースの例をいくつか見ていきましょう：

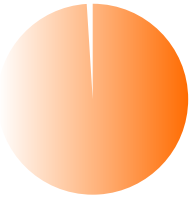
把握されていないデジタルアタックサーフェス

マルチクラウド環境により、企業のコントロールが及ばないところまで拡大された広大なアタックサーフェスが作り出されます。

クラウドドリブンのビジネスモデルは従来のIT、そしてセキュリティに「民主化」をもたらします。つまりユーザーが自由にサーバーやインスタンスを立ち上げ、その結果設定ミスや、公開のレポジトリにコードが露出するなどの事態を招く確率が高まります。

クラウドによる新しい攻撃の台頭

クラウドアーキテクチャや既知のセキュリティ脆弱性を狙うサイバー攻撃はマシンスピードで出現し、進行していきます。脅威のボリュームそのものが増大することに加えて、脅威アクターによるAIやMLの使用は高度なクラウド攻撃の自動化を容易にします。攻撃者は従来型の「一対多」攻撃と、標的型の「一対一」テクニックや新手の予知しにくい脅威を組み合わせる可能性さえあります。



■ 99%

顧客の責任となるセキュリティインシデントの割合は2025年までに99%となる

"Is the Cloud Secure?" ーガートナー社[2]

1: https://www.accenture.com/gb-en/insights/technology/maximize-cloud-value.
2: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure.

最新の課題には
最新のアプローチが必要

今日の動的かつ非常に分散したマルチクラウド環境を保護する上での課題には次が含まれます：

- アーキテクチャのかつてない複雑性
- クラウドセキュリティについての専門知識が世界的に不足
- 連邦、州、業界レベルでの目まぐるしく変化するデータプライバシー保護関連規制への準拠圧力の高まり
- マルチクラウド環境全体に渡る一元的可視性の欠如

クラウドセキュリティに対する今後のアプローチは動的なものであるとともに、常に次の 3 つの根本的機能を提供しなければなりません：

1. リアルタイムの可視性

クラウドの侵害はほとんどのネットワーク侵害よりも急速に発生する可能性があります。ビジネスにとってクラウドを非常に有用なものとしている可用性、速度、拡張性といった特徴が、同時にサイバー攻撃者によるすばやい打撃に力を与えるものとなります。マシンスピードの攻撃テクニックは、リアルタイムの状況を把握し組織の環境と脅威ランドスケープについての正確な認識を構築することを困難にします。

ほとんどの従来型の、導入の容易なクラウドセキュリティツールは、リスクについての「一時点での」スナップショットを提供するのみで、現在のクラウドセキュリティに欠かせない一元的なリアルタイムの可視性が得られません。現代のクラウドセキュリティアプローチは、セキュリティ脅威を見つけ出す継続的かつリアルタイムの視点と、動的な DevOps パイプラインに対応した簡単な導入という 2 つの目標を満たす必要があります。

2. 複雑性の軽減

クラウド環境はサイロとして存在しているのではなく、ビジネスの複雑な構造に深く組み込まれています。多様な環境全体のリスクに対して統一された視界を持つことにより、新しいツールをよりスマートかつより高速に動作させることができ、新たなドメイン間のコラボレーションや知識共有を促進させることができます。単一の「信頼できる情報源」を持つことにより、情報の食い違いが起こる可能性が減り、アナリストがアクションを優先付けして実行するための冗長なあるいはサイロ化した作業が削減されます。

3. クラウドスケールでの脅威および露出管理

スキルを持った人材が慢性的に不足する状況下で、セキュリティチームはかつてなく幅広い範囲の既知および未知の脅威を検知し対処しなければなりません。サイバー防御はもはやこれまでの境界にフォーカスしたセキュリティに頼ることはできません。基本的な「検知と対処」アプローチでは、新手の、特定のビジネスを標的とした、AI による脅威が侵害を引き起こすのを見つけ出し防ぐことはできないのです。クラウドベースの脅威にはクラウドドリブンのセキュリティが必要です。幸いなことに ー不幸なことかもしれませんが ークラウドを保護するために CISO が選択することのできるベストプラクティス、プラットフォーム、そしてクラウドセキュリティのために一から設計されたポイントツールの数はますます増えています。

市場セグメントの分類

クラウドセキュリティに対する長期的な取り組みのビジョンを構築する上で、組織はすべての投資 – その道のりの一歩一歩 – がクラウドセキュリティインフラをより速く、よりスマートに、より拡張性を高くするものであるとの確証を必要とします。いくつかの新しいフレームワーク、プラットフォーム、およびプログラムは、一つの全体的かつ効率的アプローチの中で各コントロール間の点と点を結ぶあるいは統合することにより、クラウドセキュリティのレベルを引き上げることを目指しています。

広大なクラウドセキュリティ市場は、ガートナー社やその他の分析会社が定義するさまざまな – そしてしばしば重複した – 市場セグメントで構成されています。

CSPM（Cloud Security Posture Management）によるサイバー防御の強化

CSPM にはワークロードの保護を超えた機能があります。基本機能にとどまらない CSPM テクノロジーは、クラウド環境のセキュリティリスクや設定ミスを識別し、評価し、緩和に寄与することを目指しています。今日、CSPM は主としてコンプライアンス規制への準拠を助けるために運用されています。

CSPM ソリューションは一般に組織のクラウドインフラ、リソース、設定などのスナップショットイメージを提供し、セキュリティチームが脆弱性を識別し対策するのを支援します。

多くの場合、クラウドリソースへのアクセスをコントロールする CASB（Cloud Access Security Broker）または CIEM（Cloud Infrastructure Entitlement Management）ツールと組み合わせて使用されます。これらのツールは多様なデータソース、たとえばクラウドプロバイダーのログ、設定データ、脆弱性スキャンなどに依存していますがこれらは常に完全あるいは正確とは限らず、その結果すべてのセキュリティリスクを検知できない可能性があります。

CWPPs（Cloud Workload Protection Platforms）によるワークロードの保護

その名前が示す通り、CWPPs はあらゆるタイプのクラウドワークロード ー 物理サーバー、コンテナ、仮想マシン（VM）、サーバーレス ー をオンプレミスシステムおよびマルチクラウド環境で保護します。CWPPs が約束するものには、コンテナ保護、脆弱性スキャニング、設定管理、および脅威やエクスプロイトのより高速な検知および調査を目的としたその他の機能が含まれています。

クラウドベースの CWPPs はアプリケーションの保護、パッチの優先付け、外部脅威の検知に対して、一貫性のある統一されたフレームワークを提供します。CWPPs は環境を継続的にスキャンして、企業のセキュリティポリシーに違反するアクティビティや、アセットや規制への準拠をリスクにさらす不適切な設定などを探します。

CIEM（Cloud Infrastructure Entitlement Management）によるアイデンティティ管理の強化

CIEM はクラウド内のコーポレートリソースへのユーザーのアクセスを決定する、権限の管理に対して包括的な一元化されたアプローチを提供します。CIEM はユーザーの資格、許可、アクセス権限に対する統一された可視性により、社内ポリシーの徹底およびコンプライアンスをクラウドインフラ全体で改善します。

CIEM はどのユーザーがどのアクションを取ることができるのかを可視化することで、セキュリティチームおよびビジネスリーダーがユーザーの役割と責任に基づいて許可をきめこまかく管理できるようにし、権限の不正な使用を最小化することによりアイデンティティおよびアクセス管理（IAM）を強化します。また CIEM システムは資格の付与および取り消しを自動化することによりサードパーティおよび非従業員のリスクを緩和し、監査証跡に使用するデータを生成してコンプライアンスを証明するのにも使われます。

CDR（Cloud Detection and Response）によるクラウドリスクの早急な排除

CDR は従来の「検知と対処」セキュリティを拡張しクラウドの動的な性質に合わせたものです。エンドポイント、ネットワーク、およびマネージド型の Detection and Response（EDR、NDR、MDR）同様、クラウドネイティブな CDR プロセスには脅威を封じ込めるまたは修正するための監視、検知、分析、脅威の優先付け、自動化されたステップの作成または実行が含まれます。

高度に分散したクラウドアーキテクチャのために設計された CDR は、各種ワークロード、API、および複雑なマルチクラウドサービスおよび環境全体に渡る可視性と自動化を提供します。CDR はクラウドに内在するリスク、たとえば設定ミスや複雑なマルチクラウド環境に対する統一された可視性の欠如などから生じる脆弱性を明らかにします。これらのソリューションはエージェントを使ったあるいはエージェントレスでのデータ収集を使って、エコシステム全体の継続的なリアルタイムの監視および分析を行います。

CDR は既知の脅威と新手の脅威をどちらも検知でき、また水平移動や権限昇格などが疑われる不審なアクティビティも検知できます。CDR は検知から一歩進んだ、深刻度に基づいたクラウドイベントの優先付け、偽陽性の削減、脅威のシミュレーション、脅威アクターの振る舞いの理解にも役立てることができます。リスクを識別すると、システムはワークロードの隔離や分離ゾーンの作成など自動化された対処をトリガすることができます。

CNAPP（Cloud-Native Application Protection Platform）による各種機能の統合

CNAPPs は調査・分析企業のガートナー社により、開発中および実運用中のクラウドネイティブアプリケーションを保護するための一元化され緊密に統合されたセキュリティおよびコンプライアンス機能のセット、と定義されています。

その意味で、CNAPP は CWPP、CDR、CIEM、CSPM のさまざまな要素および利点を組み合わせたものです。

野心的な統合のビジョンに基づき、ガートナー社はクラウドネイティブアプリおよびインフラのリスクを識別、優先付けおよび対処するための継続的なプロセスを定義しています。

CNAPP はランタイム保護、可視性、脆弱性管理を一つのプラットフォームに統合し、SecOps および DevOps チームに対して脅威の対処と回避のための統一された可視性を提供します。

CSPM と同様、CNAPP の構築を通じて企業は最小権限アクセスを徹底し、ゼロトラストセキュリティ態勢を作る取り組みを進めることができます。

エンドツーエンドの CNAPP が実現するその他の重要な機能には、コンテナ、VM、サーバーレス機能内の脆弱性の自動検知、および露出、マルウェア、Infrastructure as Code（IaC）を検出するためのスキャニングが含まれます。

最終的に前述のさまざまな略語やパズルのピースがすべて積みあがったものが CNAPP ですが、そこまでの企業の道のりは段階を踏んで進みます。その過程で CISO は常にビジネス固有の脅威環境、リスクの許容度、必須のデータプライバシー要件等に基づいた優先度の設定を続けなければなりません。

CNAPP は究極的には部分部分の合計よりも大きい価値を約束します。それは単一のツールまたはソリューションにより、ばらばらな分析や、アラート疲れ、冗長な調査、およびリスクを関連付け修正または回避するのにかかる時間と労力を削減する、クラウドセキュリティに対するプラットフォーム型のアプローチです。

■ 75%

ガートナー社は、2025年までに新しいCSPM関連の購入の75%は統合されたCNAPPの一部として行われると予想しています

Darktrace

いつ、どれを使うか？

これらのアプローチはすべて次を目指しています：

- AIを活用して検知と対処を改善し、脅威をより高速に発見および阻止する
- 新手の攻撃を自動的に回避し排除する
- セキュリティ対策をより積極的なものにする
- サイバースキルおよび専門知識の利用と保持を改善する

予算、スキル、およびサイバー保険等の要件、そしてクラウドを保護する上での課題の変化、これらがすべてCISOの投資判断に関係してきます。

課題には、適切なAIを適切な方法で適切な時に適用することにより、現在のセキュリティインフラをすり抜けるAI主導の新手の攻撃を阻止することも含まれます。[3]

33.2 億ドル

■ 2027までに予測されるCSPM市場の規模
CSPM市場は年平均成長率25.7%で成長すると予想されています。
"Is the Cloud Secure?" ーガートナー社

	CSPM	CWPP	CIEM	CDR	CNAPP
重点	セキュリティ体制の強化	イベント/インシデント	アイデンティティ	イベント/インシデント	統一されたアプローチの維持
強味	▪ 脅威に関するアクション可能なコンテキスト ▪ リスクを自動的に識別 ▪ 緩和措置をガイド	ワークロードの一元的表示	最小権限アクセスおよび認証ポリシーの推進	▪ アラート、偽陽性の削減 ▪ 検知のスピードアップ ▪ 対処を自動化	▪ 脅威に関するアクション可能なコンテキスト ▪ リスクを自動的に識別 ▪ 緩和措置をガイド
限界	進行中の脅威に対する検知、アクションができない	ワークロードへの対応が限定的	対象がアイデンティティに限定されている	インシデントに対する検知と対処が限定的	段階的な導入に時間がかかり専門技術が必要
セキュリティ体制への効果	▪ 一元的クラウド可視性を提供 ▪ コンプライアンスを改善	▪ サイバー損害賠償責任保険料の削減に寄与 ▪ 継続的な監視と検知を提供		▪ より高速な対処を促進 ▪ ゼロトラストへの取り組みを前進させる	

CISOが利用することのできる主なクラウドセキュリティの分類

3: https://www.gartner.com/en/documents/4295099

従来のクラウドセキュリティは限界に達した

従来のクラウドセキュリティツールはIAMやセキュリティリーダーに対して、彼らが本当に知る必要があること、つまりどユーザーがどのクラウドリソースにアクセスできるかをリアルタイムに教えてくれません。

既存のソリューションの限界の例をいくつか見ていきましょう：

動的な世界で静的な情報

動的なクラウド環境では、ほとんど誰もがただボタンを押すだけでサーバーやコンテナをスピンアップしアーキテクチャの変更を行うことができます。残念ながら、それは DevOps エンジニアがセキュリティチームを直前まで、あるいは何か不具合が起こるまで、つまりそうなってからでは遅いという段階まで、関与させないことを意味します。

今日の静的なクラウドセキュリティソリューションはインテグレーションおよびインストレーションを行う以前の脅威環境のスナップショットを提供してくれます。静的な情報は導入前のバリデーションおよびコントロールの設定に役立ちますが、クラウド移行に関係した本当のリスクはそれ以後に現れてきます。何かがうまく行っていない場合、セキュリティチームはどうやってそれを知ることができるのでしょうか？

セキュリティインシデントに対する「一時点の」情報を基にしたソリューションは脅威をリアルタイムに分析し相関づける能力が欠けています。アラートは環境から抽象化され、クラウドセキュリティプロフェッショナルはインシデントの診断および何が最も致命的かを理解する上で不利な立場に置かれます。

静的なアプローチはコンプライアンスを証明するのには役立ちますが、特に新手の予測不可能な攻撃の検知を強化するのにはほとんど貢献しません。“if/then” 型のシナリオに基づくルールを適用した後、静的なツールはアナリストがインシデントを調査する間、セグメントやコンテナの隔離など基本的な対処アクションを指示することもあります。事前に設定されたルールを適用する際には、アナリストはどの脅威がビジネスに最も大きなリスクとなるかを、それが実際に起こる前に知る必要があるのです。

実際の対処の欠如

組織にとってクラウドをこれほど便利かつ魅力的なものにしている、速度、敏捷性、可用性、規模といった特徴は、攻撃者にとっても同じ魅力を持つのです。クラウド内のサイバー攻撃が急激に展開するとき、単に攻撃を検知するだけでは不十分です。

今日のほとんどのクラウドセキュリティ製品は、何か間違いが起こったときにアナリストに警告することはできますが、実際の対処を開始する能力は欠けています。自動対処を標榜する比較的新しいソリューションも、大部分はチケットの作成を自動化する能力のことを言っています。

本当の対処には、実際の対処を開始するのにどのようなクラウドネイティブのメカニズムが利用できるかを含めた、クラウドアーキテクチャ全体の理解が必要です。

新手の攻撃をかわすことができない

先進的なサイバー犯罪者達は当然ながらAIを使った攻撃プロセスの高速化と効率化を考えています。生成AIと大規模言語モデル（LLM）ツールは参入障壁を下げ、初心者の脅威アクターでも高度な自動化された攻撃を仕掛けることが可能になります。

こうした状況から、Darktraceは新手の攻撃が急激に増加することを予測しており、一部のケースでは実際に確認しています。

これと対等に勝負するには、サイバーセキュリティリーダーもAIを適切な方法で適用し、必要なところには従来の教師付きAI機能を適用しつつ、これにビジネスを理解するAIを組み合わせて新手の脅威を阻止しなければなりません。

次のセクションでは、Darktraceの自己学習型テクノロジーがそれぞれのビジネスを理解する能力においてユニークであり、既知および未知の攻撃に対して防御側に強力なアドバンテージを与える理由を見ていきます。

135%

■ 2023年第一四半期における新手のソーシャルエンジニアリング攻撃増加*

Darktrace

* https://www.gartner.com/en/documents/4295099

最先端AIを
フルに活用できていない

多くの従来型アプローチおよびベンダーのソリューションは、教師付き機械学習（ML）を使ってセキュリティシステムをトレーニングします。教師付きMLでは、組織のデータをクラウド上の大規模なデータレイクに送出し、これを他の数千の組織からのデータを組み合わせてAIシステムをトレーニングし、この均質なデータセットに基づいて攻撃者のパターンやプロファイルを探させます。

このアプローチは、何らかの点で過去の攻撃と似ている将来のサイバー攻撃を検知するのにはとても有効ですが、すべてがこのようにいくとは限りません。新手の攻撃の増加は既知の攻撃のペースを超えており、特に攻撃者が設計にAIを利用するようになるにつれその傾向は顕著です。

自己学習型AIは教師付きMLとまったく異なる仕組みで機能します。文字通り、自己学習型AIは導入されたそれぞれの環境において自己をトレーニングして固有のビジネス環境の「生活パターン」についての変化する理解を構築します。

自己学習型AIでトレーニングされたシステムは、その脅威が以前に見られたことのあるものかどうかに関係なく、サイバー攻撃に伴う異常な挙動を見つけ出すことができます。教師付きMLに対する投資は引き続きその目的を達成すると思われますが、新手の、AIで補強された攻撃の時代を迎える現在、クラウドセキュリティはより新しいアプローチを必要としています。それはクラウドセキュリティのために設計された、自己学習型AIを使用してセキュリティスタックを進化させるアプローチです。

AIの力を利用してクラウド環境を新手の脅威から保護

静的な、「フリーサイズ」式の、一時点にフォーカスしたソリューションでは、今日のマルチクラウド環境を十分に保護することはできません。これらの懸念に対応するために、Darktraceは組織独自のクラウド環境および課題についての深い理解に基づく、動的で、統合された、ライフサイクル的アプローチを開発しました。

Darktrace / CLOUD™ はあらゆる段階でAIをよりスマートに利用することで予防から防御の積極的な強化まで組織のセキュリティ態勢を最新のものにします。システムは組織のビジネスについて自己をトレーニングしてパターンを識別し、脅威の優先付けを行い、異常な振る舞いを発生中または発生前に修復します。

リアルタイムの可視性によりリスクを明らかに

Darktrace / CLOUDは動的なパブリッククラウドおよびマルチクラウド環境全体に渡りあらゆるユーザー、ワークロード、コンテナ、アセットに対する統一されたリアルタイムの可視性を提供します。

単一のAI駆動ソリューションを使うことにより、Darktraceは包括的なカバレッジを提供し、進化し続けるマルチクラウド環境のどこで脅威が発生しようともそれらを見つけ出し調査することができます。

Darktrace / CLOUDはクラウドアーキテクチャ全体を可視化して資格情報や重大な不正利用および設定間違いをグラフィカルに指摘します。

組織のビジネスを学習するAI

自己学習型 AI を使うことにより、Darktrace / CLOUD はマルチクラウド環境に包括的なサイバーリジリエンスを提供することができます。クラウドの持つ動的な性質に合わせて設計されたこのプラットフォームは、組織のクラウドリソース、アイデンティティ、およびサービスの生活パターンを学習し、これらの情報を使って誰が何に対してどのようなアクセスを持っているかをモデル化し理解します。

Darktrace / CLOUD は組織独自のクラウド環境を、クラウドネットワークレイヤー、アーキテクチャレイヤー、マネジメントレイヤーにおいて学習します。権限についての深い理解に基づき、過剰な権限、使われていない役割やユーザー、過剰な許可を与えているポリシーなどを特定します。AI のよりスマートな使用により設定の間違いも削減され、脆弱性管理を改善し、対処のスピードを上げると同時にセキュリティポリシーおよび業界標準への準拠を維持します。

Darktraceの自己学習型AIの特徴:

- 「オンザジョブ」で、あらかじめ与えられた概念や、システムをトレーニングするためのセキュリティチームによる膨大な事前の作業を必要とすることなく根底から学習
- 確率論数学を使用して、行動についての仮定を絶え間なく見直す
- 人間の入力に頼ることなく最新の状態を保つ

Darktrace / CLOUD に含まれる Cyber AI Analyst™ はバックグラウンドで継続的に調査を行い、マシンスピードおよびスケールでの処理により複雑な多段階のインシデントについてアクション可能なレポートを生成します。

	シグネチャベース、既知の攻撃に基づくツール	DARKTRACE
AIのタイプ	教師付き機械学習	自己学習型サイバーAI
データソース	大規模なデータレイク	組織のビジネスデータ
速度	処理に伴い遅延が発生	リアルタイム ー 最小限の遅延

Darktrace / CLOUD は組織独自のビジネスデータでリアルタイムにトレーニングされ、あらゆるユーザー、デバイスおよびクラスターのタイプが通常どのように動作するかを理解します。組織についてのより深い理解は、セキュリティ体制内のウィークポイントを発生次第見つけ出し修正するのに役立ちます。

Darktrace / CLOUD により実現される効果

クラウドネイティブな検知および対処

組織固有のクラウドフットプリントを組織のビジネスの文脈で理解することにより、何か普段とは異なる、即座に対応が必要な事象が発生したときに、Darktrace / CLOUD はそれを検知できる独自の機能を持っています。AIを使って組織の環境を理解することにより、真に自律的かつ正確な、クラウドネイティブの対処を行うことが可能になります。「正常」についての理解は正確な対処を開始する能力を解放し、普段のビジネス活動は継続させつつ、異常なアクティビティだけに対処することが可能になります。

このプラットフォームは組織のクラウドアーキテクチャ全体を理解しているため、実際の対処を開始するのにどのようなクラウドネイティブのメカニズムが利用できるかを知っているのです。自動化されたリアルタイムの対処には、EC2インスタンスを分離しセキュリティグループを適用することによりリスクの高いアセットを封じ込める、といったクラウドネイティブのアクションが含まれます。

新手の攻撃を検知し排除

LLM、生成 AI、教師付き ML 等の他の AI 手法と組み合わせて使用される、Darktrace / CLOUD の自己学習型 AI は、その脅威が以前にも見られたものかどうかに関係なく、サイバー攻撃の出現をリアルタイムに識別します。ビジネス固有のフットプリントをすべてのレイヤーで理解する Darktrace / CLOUD のアプローチにより、幅広い範囲のセキュリティリスク – 設定ミスや脆弱性だけでなく、内部関係者による脅威や予期せぬデータ損失も含めた – を洗い出す能力が最大限に発揮されます。

危険な攻撃経路を優先付け、封鎖

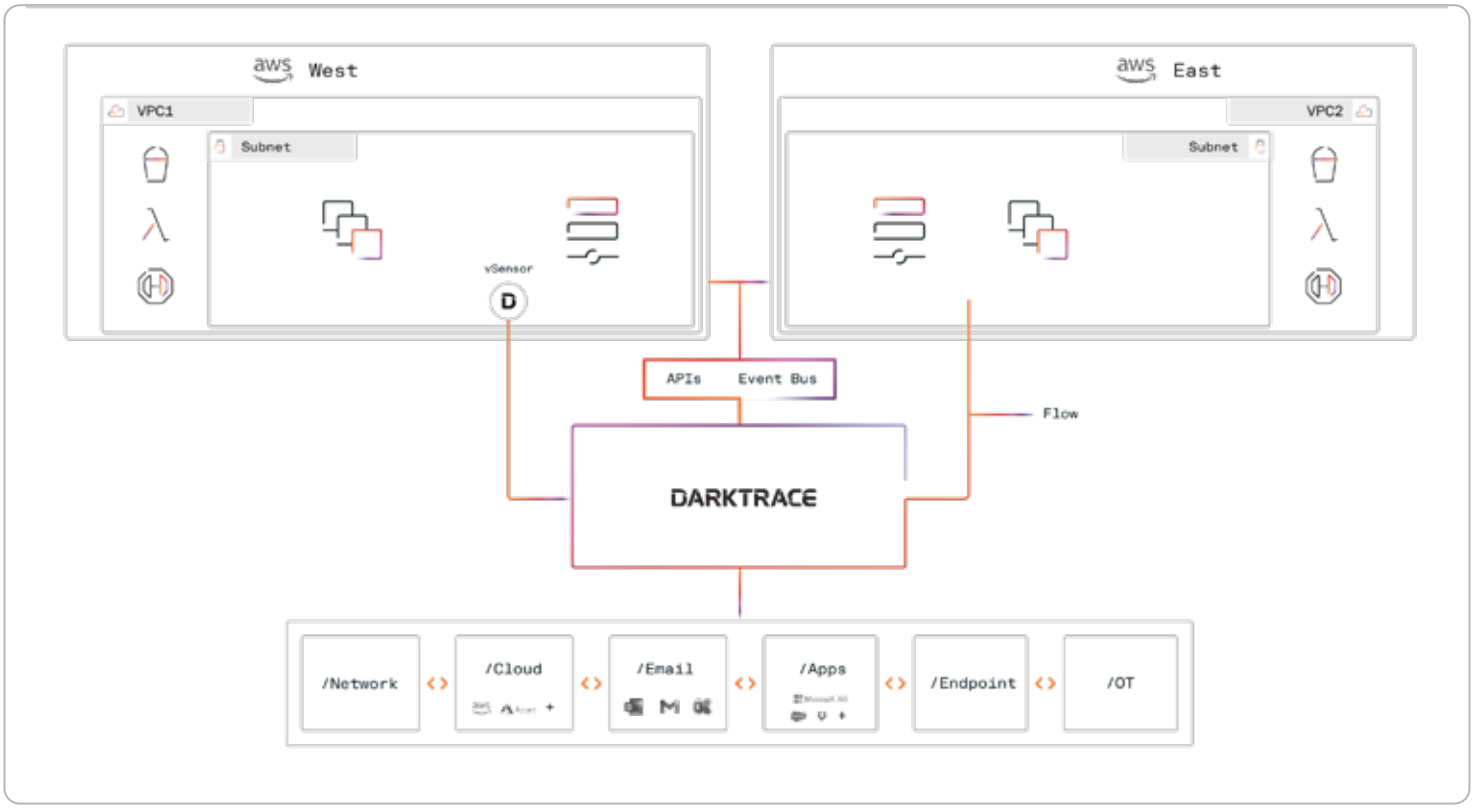
Darktrace / CLOUD では本物の攻撃者の手法を使った一般的な攻撃経路モデリングを行うことができます。従来のモデリングはクラウド間の攻撃経路に重点を置いていましたが、Darktraceは潜在的にリスクの高い経路や、アセットが攻撃を受けている可能性のある場所を特定することができます。

異常および脅威検知と連携した積極的な攻撃経路モデリングにより、攻撃者が水平移動する可能性がある経路や最初の侵入が発生する可能性のある場所を確認し優先付けすることができます。

Cyber AI Analyst™ を使って適切な判断をより高速に

DarktraceのCyber AI Analyst™ は検知からさらに先へ進んでインシデントを自動的に調査し、まとめ、セキュリティチームや他のシステムに提供します。

アナリストに大量のデータやアラートを浴びせる代わりに、Cyber AI AnalystはAIを使ってL1 SOCのワークフローを自動化し、リスクを優先付けし、技術者ではない対処担当者にも理解できるインシデントサマリーを生成します。



ツールとベンダーを整理および統合

クラウドインフラはもはや個々の区分に分離しておくことはできません。クラウドセキュリティについても同じことが言えます。Darktrace / CLOUD は他の Darktrace 製品と組み合わせて使用することができ、個別のポイントソリューションの機能を統合してアプリケーション、E メールシステム、エンドポイント、OT（Operational Technology）、およびオンプレミスの、またはハイブリッドおよびマルチクラウド環境に分散したその他のアセットをよりよく保護することができます。Darktrace / CLOUD はセキュリティスタックに含まれる他のツールと統合することが可能で、CrowdStrike や Carbon Black などのサードパーティソースから調査を開始させることもできます。また、インシデントについての情報も SIEM、SOAR およびチケット発行システムに直接エクスポートすることができます。

アーキテクチャモデリング

Darktrace / CLOUD はクラウドアセットおよびアーキテクチャ、そしてユーザーおよび権限に対するリアルタイムの可視性を含め、組織のクラウドフットプリントについての即時に近い理解を提供します。コスト情報によりリソース配分をよりよく理解し、リソースの文脈化に役立てることができます。

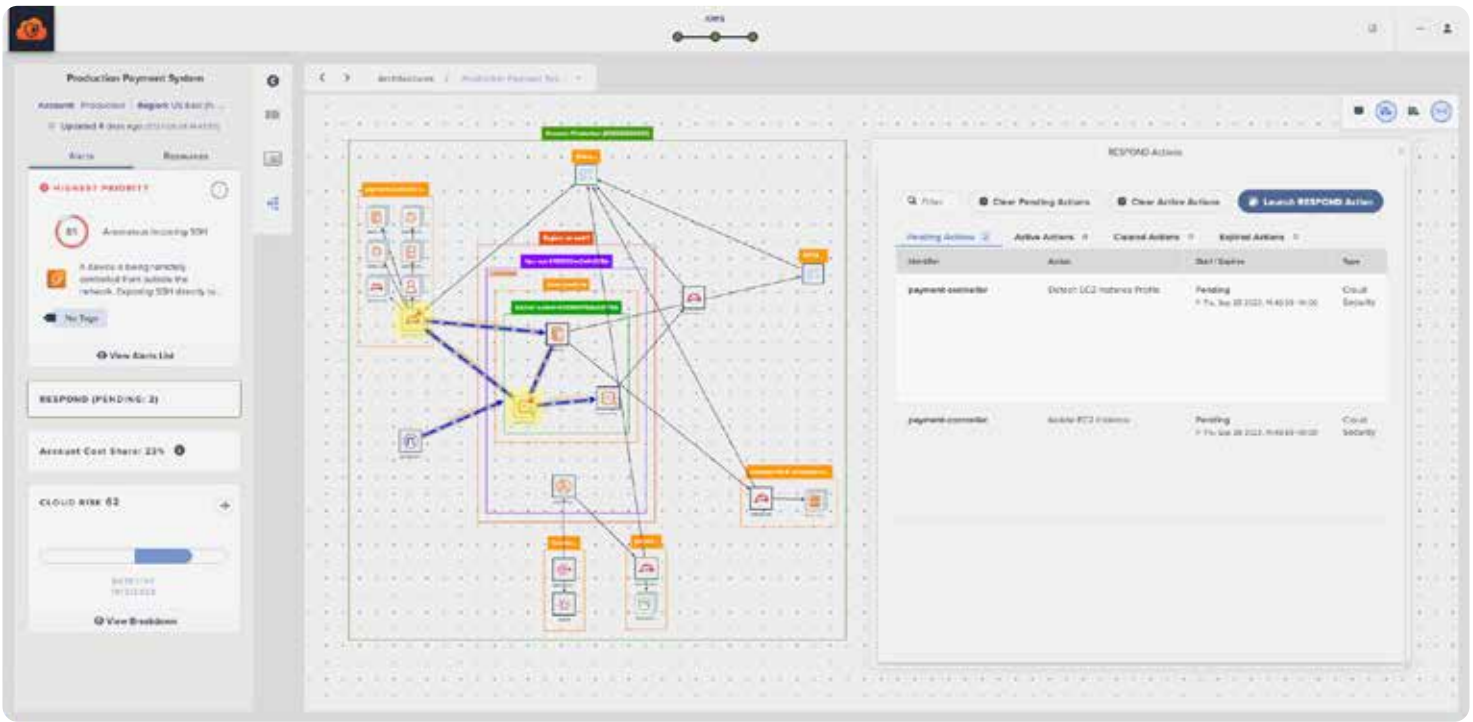
攻撃者の視点で見る

効果的なセキュリティとは、検知あるいは内部のリスク情報から開始する、あるいはそこで終わるものではありません。Darktrace / CLOUD には、セキュリティにきわめて重要な組織の外部からのビュー ー脅威アクターが攻撃を組み立てる際の視点となる ー を提供するアタックサーフェスマネジメント（ASM）も含まれています。

内部と外部のビューを組み合わせることにより、完全かつそれに対してアクションを取ることが可能な、露出の全体像が作成され、セキュリティチームは脅威を優先付けし攻撃経路を封鎖するのにこれを役立てることができます。環境に脅威が侵入した場合には、Darktrace / CLOUD の AI により生成されたプレイブックが迅速なトリアージ、修正、修復を助けます。

統一されたソリューションがクラウドの使用を最適化

- **柔軟な導入オプションを活用**
  Darktrace / CLOUD はデフォルトでエージェントレスであり、すばやいインストールが可能です。より複雑な環境においては、Darktraceの提供する動的なアーキテクチャの概要およびリスクコンテキストに基づいて、アナリストがリアルタイムエージェントの導入を選択することも可能です。
- **クラウドリソースの配分を改善**
  Darktraceのアナリティクスはクラウドリソースの使用と配分を最適化するための情報を提供します。豊富な情報を提供するダッシュボードおよびレポートにより、クラウドの処理能力が十分に利用されていない部分が分かりやすい言葉で説明され、DevOpsとセキュリティチーム間での知識共有やより緊密な連携が可能となります。
- **セキュリティワークフローの効率化**
  Darktrace / CLOUD はメッセージングプラットフォームを使ったセキュリティチームとDevOpsチーム間のコミュニケーションを推進し、JiraやServiceNowなどのツールを利用したオンデマンドのチケット作成にも対応しています。アラートや異常検知もSIEMやSOAR製品、またはDarktrace Mobile appに送信することが可能です。



適切なソリューション選択のためのガイド

クラウドセキュリティはクラウドの利点を体現したものであるべきです：

それは動的敏捷性、使いやすさ、そしてクラウド環境に対する組織の目標に基づいた運用の完全な柔軟性です。

理想的なアプローチとは、リスク、コスト、複雑性を同時に低減し、変化し続けるというビジネスの特性に応じて – ベンダーの統合、吸収合併、リモートワーク、デジタル化、および次にどのような変化が起こっても – スケールすることができるものです。

レディネスおよびリジリエンスを強化するには、クラウドセキュリティ戦略には次が含まれていなければなりません：

- クラウド内で誰が何を行っているかを知ることができる、リアルタイム可視性によるリスク削減とコンプライアンス維持
- クラウドの速度と規模で異常を検知する継続的な監視
- 自己学習型AIによるリスクの優先付け、既知および新手の攻撃に対する検知と対処の自動化、およびアナリストが調査しなければならないアラート量の削減
- リスク、複雑性、コストを削減するための統一されたライフサイクルアプローチ

クラウドセキュリティプラットフォームを評価するための10のチェックポイント

1. このソリューションは組織のビジネスを学習するのか、あるいはシステムをトレーニングするために膨大な事前の作業を必要とするか？
2. このソリューションは 100% リアルタイムの、エンドツーエンドの可視性を提供してマルチクラウド環境全体でリスクを検知し優先付けすることができるか？
3. リスクについての情報は静的な、一時点でのビューに限定されるか？
4. 可視性は組織のアタックサーフェス内部および外部のビューを統合したものか？ハッカーから見えているものがセキュリティチームにも見えるか？
5. このツールを使って防御者が攻撃経路および水平移動をモデル化できるか？
6. このソリューションは新手の攻撃を識別できるか？新手の攻撃に対する対処を導くプレイブックも提供されるか？
7. 柔軟な導入オプションがありエージェントを使用した運用とエージェントレスでの監視の両方に対応しているか？
8. このソリューションは適切な AI を適切な目的に対して適切なタイミングで使用しているか？
9. このアプローチは CWPP、CSPM、CNAPP の利点を単一のソリューションに統合することができるか？
10. このアプローチによりコンプライアンスの徹底が効率化され、最小権限およびゼロトラストへの取り組みが促進されるか？

■ ダークトレースについて

ダークトレース（ロンドン証券取引所上場、ティッカーシンボル：DARK）はAIサイバーセキュリティのグローバルリーダーで、サイバー破壊から世界を解放することを使命としています。ダークトレースの技術は「御社」についての知識を常時学習・更新し、その理解を適用してセキュリティオペレーションの変革およびサイバーリジリエンスの強化に貢献します。 ダークトレースの各研究開発センターにおけ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中です。従業員数は世界各国で2,400名を超え、9,700社以上の顧客を既知、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