DARKTRACE

クラウドフォレンジックとインシデント対応に関する5つのコア機能

目次

新たなクラウドリソースがスピンアップされるスピードと規模は、無秩序な運用、設定ミス、セキュリティリスクを引き起こす原因になっています。その結果、セキュリティチームは、従来型のオンプレミス環境からクラウドへと迅速に移行するビジネスのセキュリティを確保するために奔走しています。多くの企業は予防と検知の機能をクラウドへと首尾よく拡大しましたが、現在新たな重大なギャップに直面しています。それが、フォレンジックとインシデント対応です。

問題が識別されても、実際の範囲と影響を理解することは、ほとんど不可能な場合もあります。さまざまなクラウドプロバイダーにわたるクラウドリソースの急激な拡大と、コンテナ機能やサーバーレス機能の追加により、複雑さはさらに増しています。クラウドインシデント対応を管理するよりよい方法が組織に必要とされていることは明らかです。

セキュリティチームは、自社開発のソリューションやオープンソースのツールから先に進み、本格的なクラウドフォレンジック機能を組み込もうとしています。しかし、クラウドフォレンジック機能に関する話題が高まる中で、本物のクラウドフォレンジックと、“faux-rensics”（疑似フォレンジック）を見分けることは難しいかもしれません。

本ホワイトペーパーでは、クラウドフォレンジックおよびインシデント対応ソリューションを評価する際にセキュリティチームが検討すべき次の5つのコア機能について説明します：

01 データの深度

02 証拠保全の連鎖

03 自動収集および隔離

04 使いやすさ

05 インシデント準備度

コア機能01

データの深度

セキュリティコミュニティでは、クラウドフォレンジックとは単なるログ分析なのか、という議論が多く交わされてきました。ログに重要な情報が格納されているのは間違いありませんが、効果的なクラウドフォレンジックには、ログ分析をはるかに超えたデータの深度が必要になります。実際のところ、まとめて分析できるデータソースが多ければ多いほど、調査の精度は上がります。この意味をもう少し深掘りしてみましょう。

フォレンジック調査には、クラウドプロバイダーのログに加え、「コンテンツ全体」のデータがきわめて重要になります。このデータはクラウドインフラ内のディスク、ネットワーク、メモリに分散しており、インシデントの根本原因と影響範囲を特定するために不可欠な情報を提供します。

たとえば、EC2インスタンスを実行しているKubernetesクラスターに関連するインシデントを調査している場合、bashの履歴をクラウドログから得ることはできません。インスタンスからのホストとメモリの情報がなければ、攻撃者が実行したbashコマンドを確認しようがありません。

別の例として、SSHキーの無許可使用を伴う攻撃シナリオがあります。クラウドログだけを分析しても、疑わしいアクティビティを確認することはできません。しかし、ホスト情報にアクセスできれば、使用されたSSHキーと接続の詳細が簡単にわかります。

ホストベースの解析には、セキュリティチームが過去の状況を把握できるという利点もあります。多くの場合、システムがスピンアップされてからの重要なできごとを分析する機能は、発生したインシデントの実際の影響範囲を理解するために非常に重要です。また、インシデント発生前にシステムに検知ツールが導入されていなかった場合にも、きわめて重要となります。

適切なツールがないと、さまざまなデータソースと証拠アイテムにアクセスして内容を取得する作業は非常に複雑になり、時間がかかります。マルチクラウド環境であればなおさらです。各CSP（クラウドサービスプロバイダー）には数百ものサービスがあり、それぞれに固有のベストプラクティスやデータソースがあります。

さらに、コンテナベースリソースやサーバーレスアーキテクチャなどのエフェメラルリソースの場合、調査に必要なデータの取得はほぼ不可能になります。絶えずスピンアップ、スピンダウンされるこれらの一時的なリソースは、セキュリティチームにとって大きなハードルとなります。リソースのスピンアップやスピンダウンの間に悪意のあるアクティビティが発生した場合、重要な証拠は永久に失われ、調査は不可能になります。

加えて、すべてのクラウドログがデフォルトで有効化されているわけではない事実に注意することが重要です。この点を考慮して、調査に必要なデータに確実にアクセスできるようにしておくことが不可欠です。また、ログに記録されている内容の正確な理解も大切です。その例として、ファイルストレージシステムのログ記録が挙げられます。ほとんどのシステムでは、成功または失敗したアクセス試行のみを記録するのがデフォルトです。しかし、ストレージの内容に加えられたあらゆる変更や、アクセスされた特定のファイルの記録も重要で、有効にするべきです。

統合分析の価値。クラウドログ、ホスト、メモリ情報を組み合わせることで、侵害の根本原因、範囲、影響を特定するための可視性が向上し、コンテキストが強化されます。

	クラウドログ	ホスト情報	メモリ情報	すべてを統合
過剰な権限の使用	●	○	○	●
脆弱なKubernetes API	◪	●	◪	●
無許可のSSHキー	○	●	◪	●
AWSコンソールへのアクセス	●	○	○	●
悪意のあるアプリまたはコンテナの実行	○	●	●	●
根本原因	◪	●	●	●
bash履歴	○	●	●	●
ネットワーク通信	●	◪	●	●
取得時の実行中プロセス	○	○	●	●

セキュリティチームには、クラウドプロバイダーのログ、ディスク、メモリといった多様なデータセットを自動的に収集できる、クラウドフォレンジックソリューションが必要です。

データ収集を自動化することで、セキュリティチームが直面する、クラウド環境特有のデータアクセスに関する障害の多くを取り除くことができます。たとえば、多くの企業では、クラウドリソースへのアクセス権限はクラウドチームが保有しています。そのため、アナリストはディスク全体の情報を取得しようとするたびに別部署を経由して手続きを行う必要があります。これにより調査の開始が数日から数週間遅れることも少なくありません。

さらに、今日のクラウドフォレンジックおよびインシデント対応ソリューションにおいては、複雑なセキュリティエコシステムに余分な負荷をかけないためのエージェントレスなアプローチが求められます。クラウドフォレンジックソリューションは本質的にクラウドネイティブであるべきで、カーネルエージェントを必要とせずに API を活用し、可視性を確保するものである必要があります。

徹底的な調査に求められる深度のデータへアクセスできることが第一歩ですが、クラウドフォレンジックソリューションには、さまざまなデータソースすべてを単一のビューにシームレスに統合し、調査を効率化する機能も重要です。複数の CSP（クラウドサービスプロバイダー）にクラウドリソースを展開している企業にとっては、特にこの点が重要です。この場合、証拠アイテムを一元的に集約し、統合されたビューとして提示できる機能が不可欠です。

コア機能02

証拠保全の連鎖

証拠保全の連鎖（Chain of Custody）は、クラウドにとどまらず、フォレンジックや調査の世界において重要な概念です。しかし、クラウド環境では、この連鎖を途切れさせずに維持する上でクラウド特有の困難さがあります。そのため、フォレンジック証拠の完全性を確保するには革新的なソリューションが求められます。

まず、「証拠保全の連鎖」とは何でしょうか、そしてなぜ重要なのでしょうか。証拠保全の連鎖とは、証拠の保管、管理、移動、分析の履歴を記録し、法的手続きにおける証拠の信頼性と採用可能性を保証する仕組みです。簡潔にいえば、証拠保全の連鎖は次の2つの要素で構成されます。

01 証拠に関与またはアクセスしたすべての人物、実施した操作、および保管場所を明確に示す記録（いわゆるペーパートレイル）

02 それ以外の誰も証拠にアクセスしていないことを絶対的に保証すること

証拠が厳密な検証に耐えられるようにするためには、証拠保全の連鎖を途切れさせてはなりません。これは非常に重要です。なぜなら、証拠保全の連鎖に関する文書の提示はいつ求められるかわからないからです。

調査を開始した当初は取るに足らない事案だと思っていても、後になってはるかに深刻な事態が判明する場合があります。しかし、調査の初期段階、すなわち証拠の収集を始めた時点から証拠保全の連鎖を維持していなければ、せっかくの証拠も法的手続きで採用できず、何の役にも立たなくなってしまいます。このような状況は、特に世界中で報告義務が厳しくなる一方の状況下で、決して望ましいものではありません。

証拠保全の連鎖がクラウド環境で特に大きな課題となるのは、クラウド環境ではデータやリソースへのアクセス経路が無数に存在するためです。従来型の環境では、限られた数の人員によるアクセスや操作を記録することで証拠保全を行います。

対照的に、クラウド環境では、ユーザー、サードパーティ、CSP など、複数のエンティティがデータにアクセスできるという複雑な状況が発生します。そのため、証拠保全の連鎖を途切れさせずに維持する難易度が大幅に上がります。

さらに、今日では多くの組織が、インフラの多様化や専門サービスの活用を目的としてマルチクラウド戦略を採用しています。しかし、このような多様化は証拠保全の連鎖をさらに複雑化させます。なぜなら、証拠が複数のクラウドプラットフォームやリージョンにまたがる可能性があるためです。

クラウドフォレンジックツールを評価する際には、そのソリューションが証拠保全の連鎖を自律的に扱えるかどうかが重要なポイントとなります。

クラウドフォレンジックツールは、ユーザーの介入を必要とせず、バックグラウンドでシームレスに動作しながら、証拠の完全性を維持する必要があります。証拠保全の連鎖を自律的に維持することができれば、ユーザー入力を介さずに証拠を一貫して記録・保護することにより、人為的なミスのリスクを軽減し、法的要件へのコンプライアンスを確保できます。

また、クラウドフォレンジックソリューションには、マルチクラウド環境における証拠保全の連鎖維持に伴う課題への対応も求められます。このようなソリューションは、異種環境間で証拠の未改変コピーを保持できる機能を含む、真のクロスクラウドサポートとフィーチャーパリティ（機能の等価性）を備えている必要があります。

証拠保全の連鎖をどのように保存および維持するかということも、重要な検討事項です。それには専用のストレージバケットなどの一元管理型証拠保管が、有効なソリューションとして注目されています。これにより、セキュリティチームは複数のクラウドプラットフォームで取得された証拠であっても、単一の場所に保管して証拠保全の連鎖を維持できます。証拠を一元管理することで、セキュリティチームは 1 つのバケットへのアクセスのみを管理すればよくなります。このアプローチにより、監査証跡を最小化し、証拠保全の連鎖を大幅に簡素化および効率化することにより、最終的に不正アクセスのリスクを低減できます。

コア機能03

自動収集と隔離

脅威を迅速に特定し、調査し、封じ込めることは、平均対応時間（MTTR）を短縮し、クラウド環境におけるリスクを低減するためにきわめて重要です。自動化によりデータ収集や攻撃の封じ込めを迅速化することは、リスク軽減の重要な要素です。多くの組織が直面している大きな課題として、フォレンジック調査に必要なデータへ迅速にアクセスできないことが挙げられます。先に述べたように、多くの大企業ではクラウドリソースへのアクセス権限がセキュリティ部門以外の別のチームによって管理されています。そのため、インシデントの証拠収集が、手作業の多い非常に時間のかかるプロセスになっています。

たとえば、セキュリティアナリストが特定のクラウドリソースを調査するとします。多くの場合、クラウドチームに対して人手でチケットを作成し、侵害の可能性のあるアセットへのアクセス権限を求める必要があります。

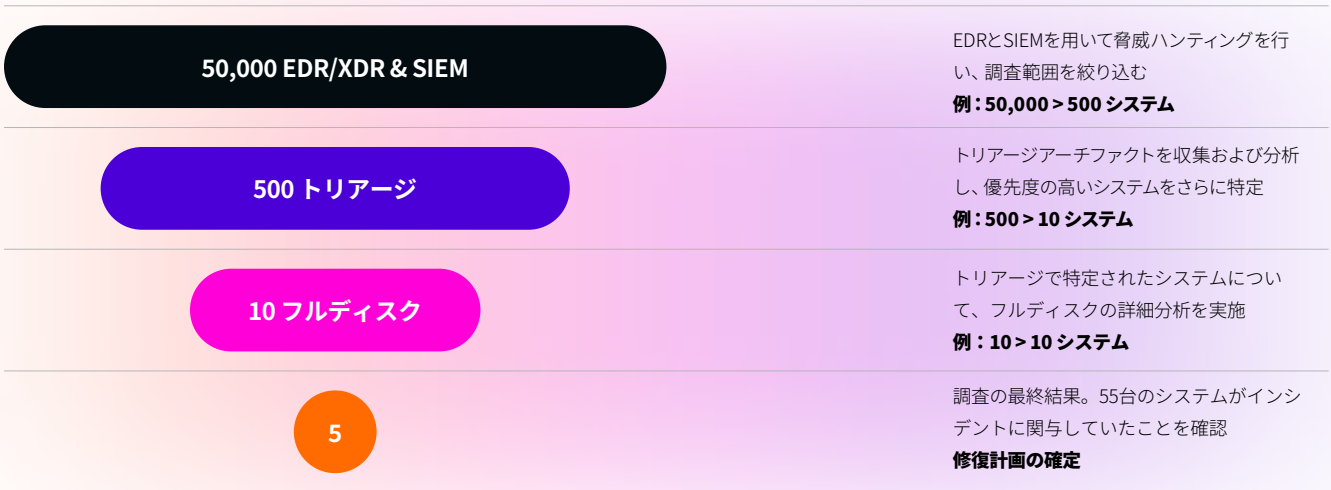
しかし、クラウド上でフォレンジック証拠に即時アクセスすることは可能であり、これはインシデント管理ツールとの統合や自動化ルールの組み込みによって実現できます。つまり、クラウドフォレンジックおよびインシデント対応ソリューションは、AWS GuardDuty、Microsoft Defender、XDR、CNAPP、SOAR、SIEM などの他のセキュリティプラットフォームとネイティブに統合され、インシデント検知の直後にさまざまな収集アクションを自動的にトリガーできる自動化ルールが組み込まれていることが重要です。データ収集を自動化することで、重要なインシデント証拠を保全し、ただちに調査に利用することができます。この機能は、悪意のあるアクティビティがエフェメラル環境で発見された場合に、特に重要です。

このような環境の特性上、アナリストがデータを迅速に取得して保全できなければ、サーバーがスピンダウンされたとたんにデータが消失してしまう可能性があります。

クラウドフォレンジックおよびインシデント対応ツールを評価する際にもう 1 つ重要なのは、セキュリティチームがデータ収集を実行する深度を選択できる機能を備えていることです。最初にトリアージキャプチャを自動化して調査範囲を絞り込み、どのシステムに詳細な分析が必要かを判断できれば、多くのケースでアナリストの時間を大幅に節約できます。その後、対象範囲がより細かく特定された段階で、絞り込んだリソースに対して自動的にフルディスクキャプチャを実行し、より深掘りした調査を行うことができます。

たとえば、5 万台のシステムがある環境で、新たに発見されたゼロデイ脆弱性の調査が必要になったとします。最初にトリアージキャプチャを自動的に実行する選択肢があれば、セキュリティチームは迅速に調査対象を絞り込み、修復までの時間を短縮できます。

同様に、システムの封じ込めなどの対応アクションを自動化できる機能も、効果的なインシデント対応プレイブックには欠かせません。たとえば、侵害の可能性のあるリソースに対して検知直後に自動的に封じ込めを実施できるようにすれば、セキュリティチームは被害の拡大を防ぎつつ、バックグラウンドでさらに詳細なフォレンジック調査を進められます。悪意のあるアクティビティが検知された時点でのデータ収集とシステムの封じ込めを自動化することで、クラウド、コンテナ、サーバーレス環境で発生中の脅威への対応時間を大幅に短縮できます。



コア機能04

使いやすさ

クラウド環境に内在する複雑さにより、セキュリティアナリストやインシデント対応担当者は、既存の業務に加えてクラウドの専門知識までも求められるようになっています。さらに、セキュリティチームのアラート疲れも深刻な問題となっています。大量のアラートに圧倒され、すべてを調査できなくなるという現象です。

加えて、業界全体にわたるサイバーセキュリティ人材の不足がこの問題をさらに悪化させています。セキュリティチームには、詳細な調査が必要なすべての事案に対応するための時間もリソースも十分にないのが現実です。最近の調査によると、クラウド関連のアラートの約23%は調査すら行われていません。

今日のクラウドフォレンジックおよびインシデント対応ソリューションには、使いやすさを中核に据え、セキュリティチームの対応力を底上げすることが求められます。

これにより、アナリストはより多くのアラートを適切にトリアージし、調査できるようになります。それだけではなく、あらゆるレベルのアナリストがクラウド特有の複雑さに対応し、かつては高度なインシデント対応スキルとクラウド知識を兼ね備えている必要があったクラウドフォレンジック調査のような高度な業務にも、これまで以上に取り組めるようになります。

クラウドフォレンジックおよびインシデント対応ソリューションを評価する際に考慮すべき重要なユーザビリティ機能には、次のようなものがあります：

データエンリッチメント
収集されたデータは、サードパーティおよび自社の脅威インテリジェンスフィードと自動的に照合される必要があります。これにより、アナリストは収集データセット内で検知された疑わしい活動や悪意のある活動を即座に把握できます。これにより、調査全体を効率化できます。重要なイベントを基点としてアナリストが容易に調査の方向性を切り替え、そこからさらに生データを深掘りできるようになるためです。

検索の保存
調査中、特に初期の分析段階においては、セキュリティアナリストがさまざまなデータセットを横断的に探索したり、データセットを切り替えたりします。そのため、検索バーには多くのクエリが蓄積されていきます。クエリを保存できる機能があれば、次回のセッションで簡単に再実行したり、同僚と共有したりできるため、貴重な調査時間を節約できます。

ファセット検索
ファセットオプションは、イベントに含まれる主なデータタイプや属性を可視化し、セキュリティアナリストがデータセットを迅速かつ効率的に絞り込むのに役立ちます。

単一のタイムライン
統合されたデータビューは、複数のクラウドプラットフォーム、サービス、データソースから取得された証拠を容易に確認するために不可欠です。単一のタイムラインにアクセスできれば、セキュリティチームは重要なデータに対してシームレスにアクセスできます。たとえば、単一のタイムラインビューを使用することで、タイムスタンプ、イベントタイプ、ユーザーなどに基づいて調査を簡単に切り替えられます。

クロスクラウド調査のサポート
今日では、大半の企業がマルチクラウドアプローチを採用しているため、さまざまなクラウドプロバイダーから取得した証拠を、セキュリティチームが単一の画面と単一のタイムラインビューでシームレスに分析できる機能が不可欠です。

可能な範囲で自動化を活用し、一般的な調査タスクを繰り返し実行できるようにすれば、セキュリティチームの貴重な時間を節約でき、経験の浅いアナリストのスキル向上にもつながります。

クラウドの複雑さに、アラート疲れや人材不足といった要因が加わっている状況下で、セキュリティアナリストの日常業務を効率化するテクノロジーを採用することは、効果的で持続的なインシデント対応体制を構築する上できわめて重要です。

コア機能05

インシデント準備度

インシデントは「起こるかどうか」ではなく「いつ起こるか」の問題です。したがって、潜在的なクラウド脅威を調査して対応できる体制を整えておくことは、リスクマネジメントにおいてきわめて重要です。

クラウドフォレンジックおよびインシデント対応に対してプロアクティブなアプローチを取ることで、セキュリティチームはインシデントが発生する前に自社の準備状況を把握できます。これにより、実際にインシデントが検知された際に、セキュリティチームが迅速に根本原因を特定し、脅威を修復することが可能になります。

また、プロアクティブな姿勢を取ることで、セキュリティチームはインシデント対応プログラムに存在するギャップを事前に特定して是正し、プログラムを継続的に改善できます。そうすることで、いざインシデントが発生したときに貴重な時間を浪費せずにすみます。さらに、サードパーティのセキュリティサービス企業やインシデント対応企業と連携している場合でも、社内のセキュリティチームが外部ベンダーに調査をエスカレーションし、必要とされる証拠や回答を自信を持って用意できる体制を整えておくことは不可欠です。

準備の重要性を示す例の1つがランサムウェア攻撃です。

ランサムウェア攻撃について見落とされがちな論点は、実際のランサムウェア展開が始まるまでに準備段階が存在することです。近年の標的型ランサムウェア攻撃のほとんどは、スピアフィッシングによる初期侵入から始まり、続いてCobaltStrikeなどのマルウェアがインストールされます。その後、攻撃者はネットワーク内を水平移動し、暗号化で最大の影響を与えるためのペイロードを準備します。

この準備段階は数時間から数日かかる場合がありますが、ビーコニングや異常な水平移動などの初期兆候は数分以内に現れることもあります。ここで、リアルタイムの可視化と迅速な調査がきわめて重要になります。セキュリティチームがこれらの初期兆候を早期に特定して対応できればできるほど、ランサムウェアが展開される前に攻撃を阻止し、総合的なインパクトを最小限に抑えられる可能性が高まります。

インシデントへの備えができていれば、セキュリティチームは攻撃が進行中であってもただちに調査を開始し、次のような重要な質問に迅速に答えを出すことができます：

- 攻撃者はネットワーク内を水平移動しているか？
- データの流出は発生しているか？
- 初期侵入があった周囲で他のシステムとの接続が発生しているか？
- システム上にパスワードダンピングツールの痕跡はあるか？
- 侵害されたシステムに平文パスワードが保存されていなかったか？

インシデント対応をプロアクティブなアプローチへ転換することで、セキュリティチームの対応が迅速化し、攻撃の機会と潜在的な被害を大幅に縮小できます。

クラウドフォレンジックおよびインシデント対応ツールを評価する際には、セキュリティチームがクラウドインシデント対応準備度を継続的に評価できる機能を備えているかどうかが重要です。

たとえば、セキュリティチームは任意の時点で、クラウドフォレンジックソリューションを活用して次のような項目をプロアクティブに確認ができる必要があります。

- クラウド環境全体の重要な情報源から証拠を取得できるか。たとえば、適切なクラウドログがすべて有効化されているか。すべてのクラウドサーバーでトリアージキャプチャを実行できるか。
- 証拠を取得し、適切に対応するためのアクセス権限が正しく設定されているか。
- セキュリティチームは重要な証拠を復号化できるか。
- 組織の準備度の傾向が時間の経過とともにどのように変化しているか。たとえば、準備度が改善しているか、組織をよりよい状態に導くためにどのような手順が講じられたか、など。

新しいリソースやサービス、環境が次々と追加されていくため、セキュリティチームは自社のインシデント対応フレームワークがこれらの変化にシームレスに適応できるようにしておかなければなりません。そのためには、アクセス権の設定状況をプロアクティブに確認し、データ取得テストを実施し、XDR、SOAR、CNAPP、SIEMなどのサードパーティツールとの最適な統合を確保しておくことが重要です。こうした取り組みによって、セキュリティチームはあらゆるインシデントに包括的に備え、徹底的な調査を実施するために必要な可視性を実現できます。また、プロアクティブなアプローチを取ることで、セキュリティチームは常にリスク状況を理解し、どこにギャップが存在するのか、また露出を減らすためにどこに投資を集中すべきかを把握できます。

まとめ

企業によるクラウドテクノロジーの採用がますます進む中で、フォレンジックとインシデント対応の必要性は一層高まっています。クラウドテクノロジーと脅威は常に進化を続けているため、インシデント対応能力とプレイブックも継続的な適応と強化が求められます。

クラウドフォレンジックおよびインシデント対応ソリューションを評価する際には、宣伝に惑わされて“fauxrensics”（疑似フォレンジック）ソリューションを本物と誤認しないよう注意が必要です。このホワイトペーパーで紹介した 5 つのコア機能が、クラウド、コンテナ、サーバーレス環境におけるさまざまなフォレンジックおよびインシデント対応テクノロジーを評価する際の一助となれば幸いです。

Darktrace の活用法

Darktrace は単一のサイバーセキュリティプラットフォームでクラウドもカバーし、サイバーリジリエンスに対するプロアクティブなアプローチを提供します。Darktrace / CLOUD は、すべてのセキュリティチームと SOC がクラウドセキュリティを利用できるようにするために先進的 AI を用いて構築された、リアルタイム CDR（Cloud Detection and Response）ソリューションです。

さまざまな機械学習テクニックを駆使し、Darktrace はハイブリッドおよびマルチクラウド環境に前例のない可視性、脅威検知、調査、インシデント対応を提供します。Darktrace のクラウド製品は Cado Security Ltd. の買収によりさらに強化され、セキュリティチームはマルチクラウド、コンテナ、サーバーレス、SaaS、オンプレミス環境においてフォレンジックレベルのデータに即座にアクセスできるようになりました。

/ CLOUD

Darktrace / CLOUD について詳しく知る

AWS ↗

Azure ↗

Darktrace / CLOUD の仕組みを理解する

詳しくはこちら ↗

Darktrace の実際の動きをデモで確認

デモを予約する ↗

■ **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2,700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、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