cisco
The bridge to possible

Cisco Hypershield

AI スケール | クラウドネイティブ | 高度分散

AI スケールのデータセンター向けセキュリティ

AI は変革をもたらし、生産性を大幅に向上させます。AI の原動力であるデータセンターは、AI 革命によって大きく成長し、2 つの点で根本的に変わりました。1 つ目は、**インフラストラクチャ**がグラフィック処理ユニット（GPU）やデータ処理ユニット（DPU）などの高度なコンピューティングシステムに進化していることです。2 つ目は、データセンターで実行される**アプリケーション**が、従来の 3 層アーキテクチャから、仮想マシン（VM）またはコンテナで実行される複数のマイクロサービスを使用するように進化したことです。

AI スケールのデータセンターを保護するには、セキュリティを再定義する必要があります。従来のアプライアンスでは対応できないからです。

Cisco Hypershield は、初めての真の分散型 AI ネイティブ セキュリティ アーキテクチャです。ネットワーク上で実行されるすべてのアプリケーションのすべてのソフトウェアコンポーネント、すべてのサーバー、パブリッククラウドまたはプライベートクラウド環境など、セキュリティが必要なすべての場所にセキュリティを導入できます。

Cisco Hypershield には、セキュリティポリシーのライフサイクルとセキュリティ インフラストラクチャのアップグレードを自動化する、AI を活用した管理機能があります。また、テスト、記録、レポート機能を使用して信頼を得ることで、快適な自律性レベルをお客様が決定できるように設計されています。独自のルールを作成、テスト、展開し、それらのルールをライフサイクル管理できるネットワーク セキュリティ ソリューションを考えてみてください。Cisco Hypershield そのものをアップグレードすることも可能です。

Hypershield は、従来はデバイスの機能として提供されていたネットワークセキュリティ機能をネットワーク自体に組み込み、シスコだけが実現できる方法でセキュリティとネットワーキングを緊密に統合します。

Hypershield はフェンスというよりもファブリックであり、必要な場所にセキュリティを適用することが可能です。パブリッククラウドでは VM または Kubernetes クラスタに、プライベートクラウドでは VM と高性能サーバー DPU にセキュリティを組み込むことができます。シスコのビジョンは、スイッチなどのネットワーキングデバイスで実行されるハードウェアアクセラレータに Hypershield を拡張し、データセンターだけでなく IoT/OT 環境にもセキュリティを提供することです。病院では間もなく、Hypershield を使用して医療機器やその他の OT デバイスを保護できるようになるでしょう。製造業者は、工場の現場にある機器に関して、同じことができるようになるでしょう。

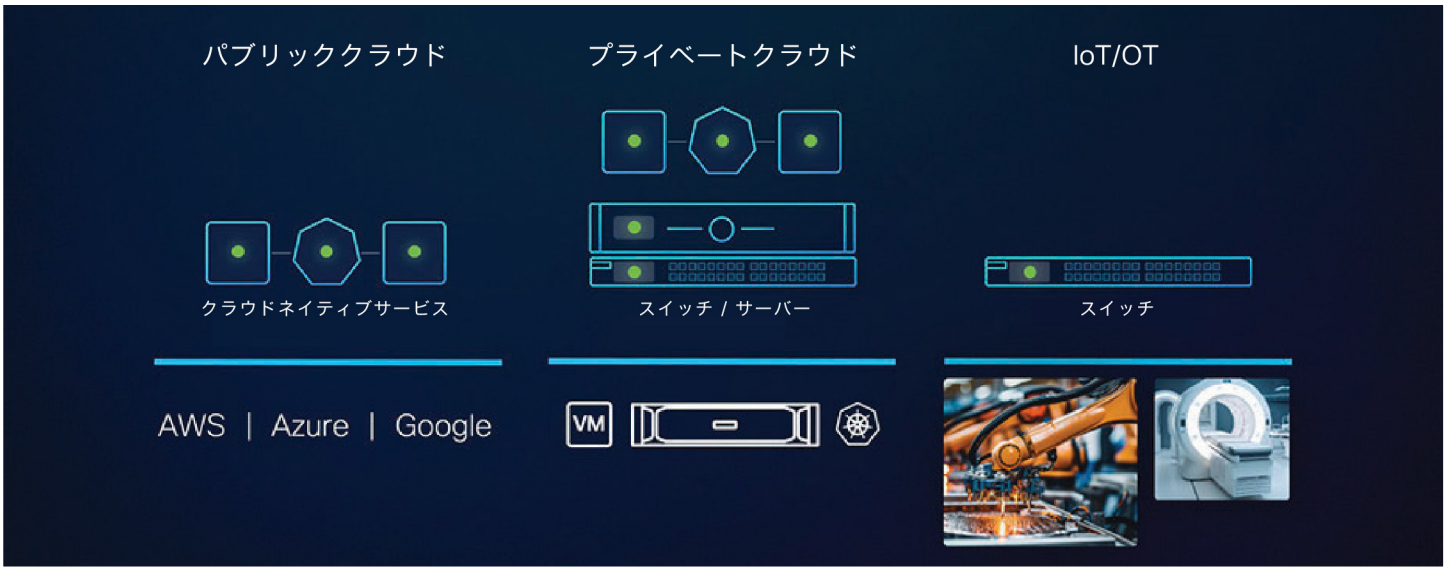

図 1. 必要な場所でセキュリティを実現できる Hypershield

何らかの既存製品の次世代ではなく、まったく新しい製品の第 1 世代

Cisco Hypershield は、そのソリューションの中核となる独自の機能によってセキュリティを再定義します。

- **AI ネイティブ：**Cisco Hypershield は AI の力を利用するように新しく設計されているため、他のセキュリティソリューションに比べて自律性が格段に高くなっています。実際、Hypershield は最初から AI 管理を中心に構築されており、従来の製品の上に AI レイヤを追加したものではなく、AI ネイティブだと捉えています。
- **eBPF の適用：**Hypershield は、オープンソーステクノロジーである eBPF を使用して、ワークロードレベルで詳細な可視性と適用を実現しています。近ごろシスコが買収した Isovalent 社が共同開発した eBPF は、最新のオペレーティングシステムに搭載されているソフトウェアフレームワークです。これにより、ユーザー空間のプログラムがカーネルを経由して安全に適用とモニタリングのアクションを実行できるようになります。
- **自己検証型アップデート：**Hypershield は、自身でアップグレードとアップデートができるように設計されています。分散型アーキテクチャを採用しているため、テレメトリを送信する eBPF エージェントは、特許出願中の設計を使用して適用ポイントとしても機能します。この設計は、ネットワーク、ワークロード、ファイル、プロセスのどのレベルであっても、クラウドの継続的な更新 CI/CD モデルをオンプレミスベースのシステムで実現するというものです。

これらのプラットフォーム機能に加えて、セグメンテーションや脆弱性エクスプロイトからの保護など、特定の効果をもたらす**モジュール**があります。これについては、次のセクションで説明します。Hypershield は、ハードウェアに追加される**サブスクリプションベースのソフトウェア製品**です。

図 2.　シスコの Hypershield アーキテクチャ

一元的なセキュリティポリシー

高度に分散した IT 環境が一般的になるにしたがって、複数のドメインにまたがるポリシーの管理と一貫した適用が課題となっています。企業内のポリシーの規模は膨大であり、何十万ものルールが存在しますが公開されることはありません。また、これらのルールを作成した人は、すでに組織内にいない可能性があります。このような複雑さを管理することは、今まで困難でした。しかし AI を活用した機能により、セキュリティ管理者が強力で一貫性のある動的なポリシーを大規模に実装できるようになりました。

Hypershield は AI を搭載しており、一元的で管理が容易な真のインテントベースのポリシーモデルを実装するための独自のアーキテクチャを備えています。適用されるポリシーは、フォームファクタや適用ポイントの場所に関係なく、Hypershield の管理コンソールによって一元的に整理されます。新しいポリシーが作成された場合や、古いポリシーが更新された場合は、ポリシーが「コンパイル」され、適切な適用ポイントへインテリジェントに配置されます。セキュリティ管理者は、適用ポイントでの分散の程度に関係なく、展開されたポリシーの概要を常に確認できます。オンプレミスからネイティブのパブリッククラウドへのワークロードの移動に合わせて、ポリシーを適用することも可能です。

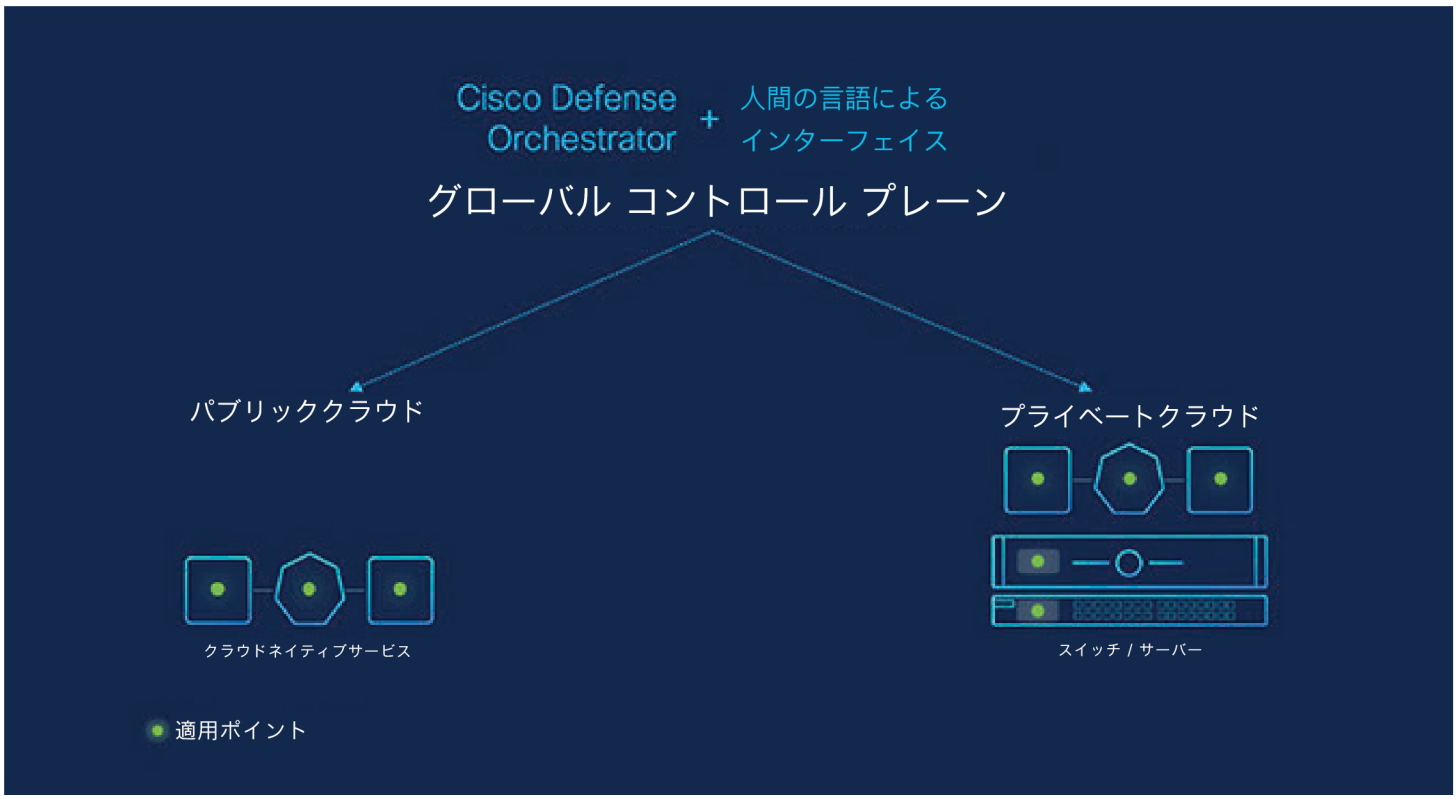

図 3. 分散型適用の中央管理

お客様の真の課題を解決

Cisco Hypershield は、組織が直面している重大な問題を解決することができます。

1. Autonomous segmentation（自律型セグメンテーション）

攻撃が発生した場合のラテラルムーブメントを防ぐために、企業は何十年にもわたってセグメンテーションを使用して、ネットワークのどの部分にどのワークロードとアプリケーションがアクセスできるかを詳細に規定してきました。しかし、セグメンテーションは困難です。1 つのアプリケーションのセグメンテーションルールを定義するのに 40 日以上かかるというお客様もいますが、これでは時間がかかりすぎです。現在のセグメンテーションツールはアプリケーションを深く理解していません。アプリケーション固有のイベントを考慮せずに、時間のみに基づいてアプリケーションの動作をベースライン化しようとしていますが、これは効果的ではありません。

板金配送を行う工場アプリケーションの例を見てみましょう。従来のツールは、90 日間などの一定期間アプリケーションを監視し、その期間に観察された動作に基づいてセグメンテーションポリシーを策定します。しかし、この工場で 91 日目に板金を使い果たし、このイベントによってアプリケーションからさまざまなシステムへの通信がトリガーされ、新しい注文が行われた場合はどうなるでしょうか？これは正当な動作ですが、ランダムではないのにランダムであるかのように見えます。アプリケーションを継続的かつ詳細に把握する必要があるのは、このためです。

AI ネイティブの Hypershield の監視対象は、他の製品が重視しているネットワークフローだけではありません。監視対象の動作の全範囲について情報が提供されます。具体的には、Hypershield が保護しているすべての環境で何が起きているか、決して発生してはいけない動作について脅威インテリジェンスが何を知らせているか、最新の攻撃ベクトルと手法と脆弱性、お客様が推奨ポリシーをどのように変更するかをモデル化したベストプラクティスに基づきシステムが何を学習し監視したか、攻撃を受けたときにお客様が何を行うか、という情報です。

システムは、環境内に何があり、どのような宛先と通信しているのかを理解することから始まります。それに基づいてガバナンス要件を把握し、ビジネスの安全を確保するためのマクロなガードレールが作成されます。Hypershield は、上記の属性に基づいて学習することで、ポリシーをさらに強化します。これは継続的かつ動的なプロセスであるため、アプリケーションが変更されたり移動したりするとセグメンテーションポリシーが緩和され、システムが新しい動作を学習すると、セグメンテーションポリシーを再度強化できます。

その結果、過去に起こっていた可能性のあることではなく現在起こっていることに基づいて、データに裏付けられた信頼性の高い推奨事項が提供されます。推奨事項はライブトラフィックに対して自動的にテストされ、ポリシーの有効性とパフォーマンスへの影響に関する結果とともにユーザーに提示されます。ユーザーが納得して推奨事項を受け入れると、初めて展開されます。システムは自律的でありながら、信頼を獲得し、継続的に学習します。

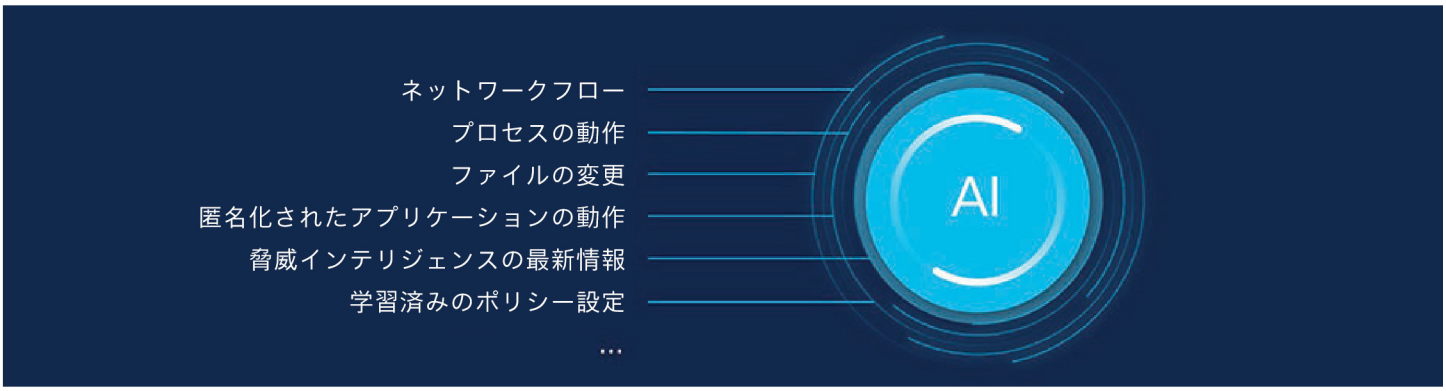

図 4.　セグメンテーションポリシー作成のための包括的な情報

2. Distributed exploit protection（分散型脆弱性対策）

攻撃者は、ログイン情報を盗んだり、アプリケーションのサービスを侵害したりして正規のアプリケーション経路を巧みに通り抜けすることができます。そこでユーザーは、アプリケーションを構成するサービスとその脆弱性を理解する必要があります。しかし脆弱性が特定されたとしても、パッチを適用するのは困難です。数週間から数か月かかり、場合によってはパッチが適用できないことがあります。一方、攻撃者は脆弱性が公開されてから数時間以内にエクスプロイトを開始します。

Hypershield は、インベントリ全体を把握し、既存の脆弱性ツールと統合します。しかし、毎週約 500 ~ 1,000 件の CVE が公開されているため、それらの脆弱性に優先順位を付けて修正することは困難です。Hypershield は搭載されている AI 機能とアプリケーションに対する深い理解により、次の 3 つの重要な質問に基づいて、組織の環境に固有の最も重大な脆弱性の優先順位付けを支援します。

- 脆弱なコードモジュールがメモリ内で実行されているか
- 脆弱性は理論上のものなのか、実際に脆弱性がエクスプロイトされているのか
- 脆弱性は価値の高い資産に影響を与えているか

アプリケーションチームが時間をかけてパッチを検証している間に、Hypershield はアプリケーションのパスに正確な補完コントロールを適用してエクスプロイトを防止します。パッチが適用されると、補完コントロールは自動的に削除されます。

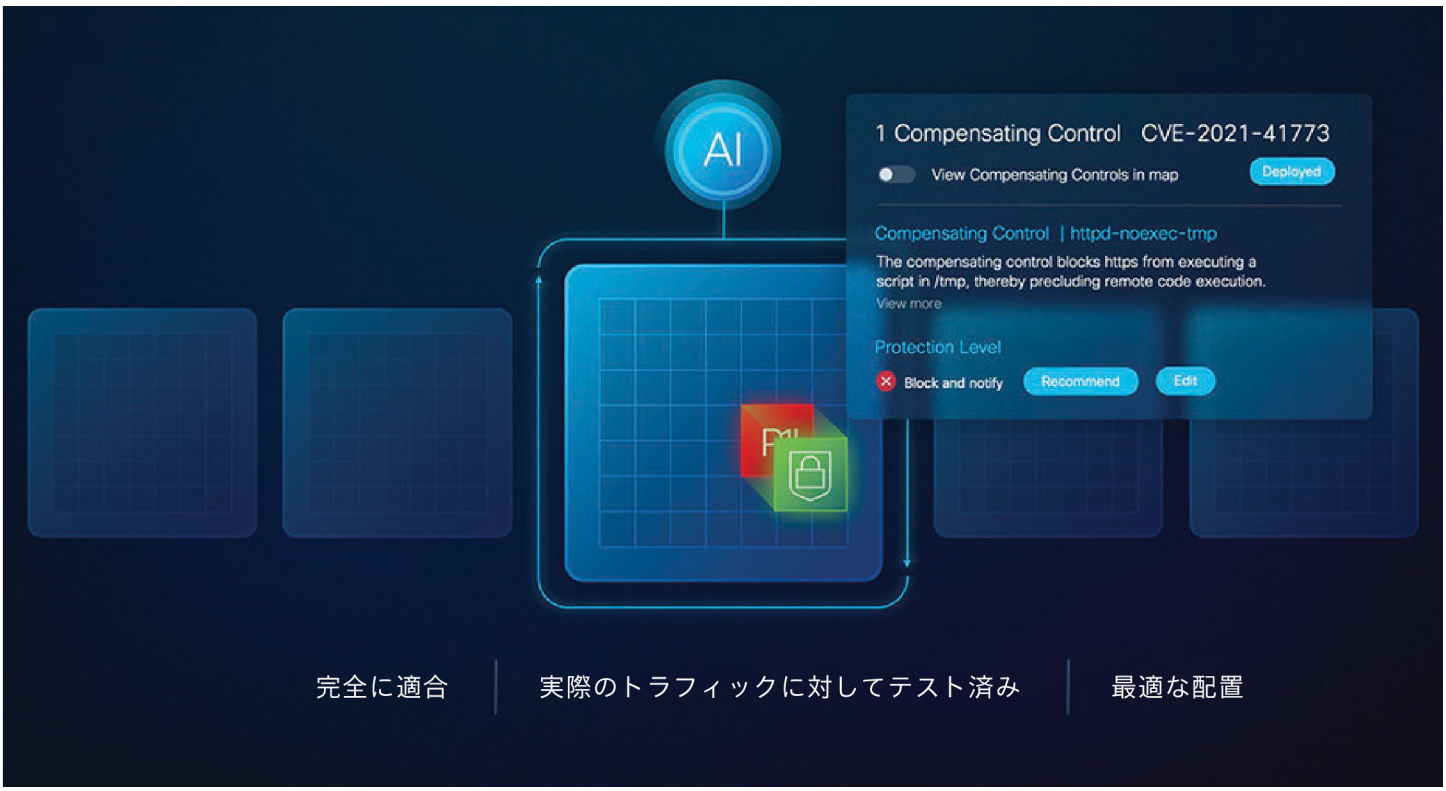

図 5. Hypershield が補完コントロールを適用して脆弱性のエクスプロイトから保護

3. Self-qualifying updates（自己検証型アップデート）

セキュリティ管理はその性質上、すぐに古くなる傾向があります。新しいソフトウェア アップデートがリリースされることで古くなることもあれば、新しいアプリケーションやビジネスプロセスによってセキュリティポリシーの変更が必要になることもあります。従来は、どちらのシナリオにも適用ポイントが十分に対応できませんでした。どちらの場合も IT インフラストラクチャが中断し、ビジネスリスクが生じる可能性があるため、引き受けたがるセキュリティ管理者はほとんどいません。ソフトウェアとポリシーの更新を正常かつ無停止で行うメカニズムが求められています。

Cisco Hypershield には、まさにこのニーズに対応する**デュアルデータプレーン**と呼ばれるメカニズムがあり、このメカニズムではプライマリデータプレーンとシャドウデータプレーンの 2 つのデータパスをサポートしています。実際のライブトラフィックは、プライマリデータプレーンとシャドウデータプレーンの間で複製されます。これはラボやシミュレーションではなく、環境内のすべての適用ポイントで実行されるデジタルツインです。ソフトウェア アップデートは、最初にシャドウデータプレーンに適用されます。ユーザーが十分に検証して承認すると、プライマリデータプレーンとシャドウデータプレーンのロールが切り替わります。同様に、新しいセキュリティポリシーを最初にシャドウデータプレーンに適用し、すべてに問題がなければ、シャドウデータプレーンがプライマリになります。

デュアルデータプレーンの概念により、セキュリティ管理者はビジネスの中断やパフォーマンスへの影響を心配することなく、適用ポイントでソフトウェアのアップグレードとポリシーの更新を実装できます。この重要な機能は、ポリシーの更新と補完コントロールをテストしてから展開することで、前述の自律型セグメンテーションと分散型脆弱性対策の成果を実現するのに役立ちます。

図 6.　Cisco Hypershield のデュアルデータプレーン

The bridge to possible

まとめ

Cisco Hypershield は、AI スケールのデータセンターに対するセキュリティを根本的に見直しました。Cisco Hypershield は、AI を活用した機能、カーネルレベルまでの詳細な可視性と適用、デュアルデータプレーンによる自己検証型アップデートにより、独自のルールを作成、テスト、展開し、それらのルールをライフサイクル管理する強力なネットワーク セキュリティ ソリューションとなっています。Cisco Hypershield そのものをアップグレードすることも可能です。同時に、AI 内で自律性レベルを調整することもできます。すべてをテスト、記録、レポートする機能によってシステムが信頼を獲得するにつれて、自律性が向上します。まるで魔法のようなこの驚くべき機能を実現できるのは、AI 管理機能で専用に構築されているからであり、これは AI ネイティブであることのもう 1 つの例です。

関連資料

- ソリューション Web ページ
- ビデオ：Unveiling a New Era of AI-native Security（Cisco Hypershield の発表イベント）
- ブログ：Cisco Hypershield でセキュリティを再定義、AI スケールのデータセンター向け超分散型セキュリティ（シスコ セキュリティ & コラボレーション ビジネス グループ EVP 兼 GM、Jeetu Patel）
- ブログ：A New Era of Distributed, AI-Native Security（シスコ セキュリティ ビジネス グループ SVP、Tom Gillis）
- ブログ：Reimagining Security（シスコ セキュリティ ビジネス グループ VP 兼 CTO、Craig Connors）
- ブログ：Our Vision to Combat Unknown Vulnerabilities（Craig Connors）
- 利用可能な製品、デモ、その他の最新情報を入手するには、こちら にサインアップしてください

C22-4442203-00 06/24