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

人工知能 (AI) は変革をもたらし、企業全体の生産性を大幅に向上させるとともに、人工知能のエンジンであるデータセンター内で爆発的な成長を促進しています。**インフラストラクチャ**は、グラフィック処理ユニット (GPU) やデータ処理ユニット (DPU) などの高度な計算システムに進化しています。また、データセンターで実行される**アプリケーション**も、従来の 3 階層アーキテクチャから、仮想マシン (VM) やコンテナ上で実行される複数のマイクロサービスを使用するものへと進化しています。

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するという明確なビジョンがあります。

このソリューションは AI を活用しており、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します。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。また Hypershield は、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。

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。

このソリューション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 にセキュリティを組み込むことができます。Hypershield のスケーラブルな独自のアーキテクチャにより、さまざまなタイプの適用ポイントをサポートできます。たとえば将来的には、Cisco Hypershield はスイッチなどのネットワークデバイスで実行される高性能サーバー DPU やハードウェアアクセラレータに展開でき、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します。

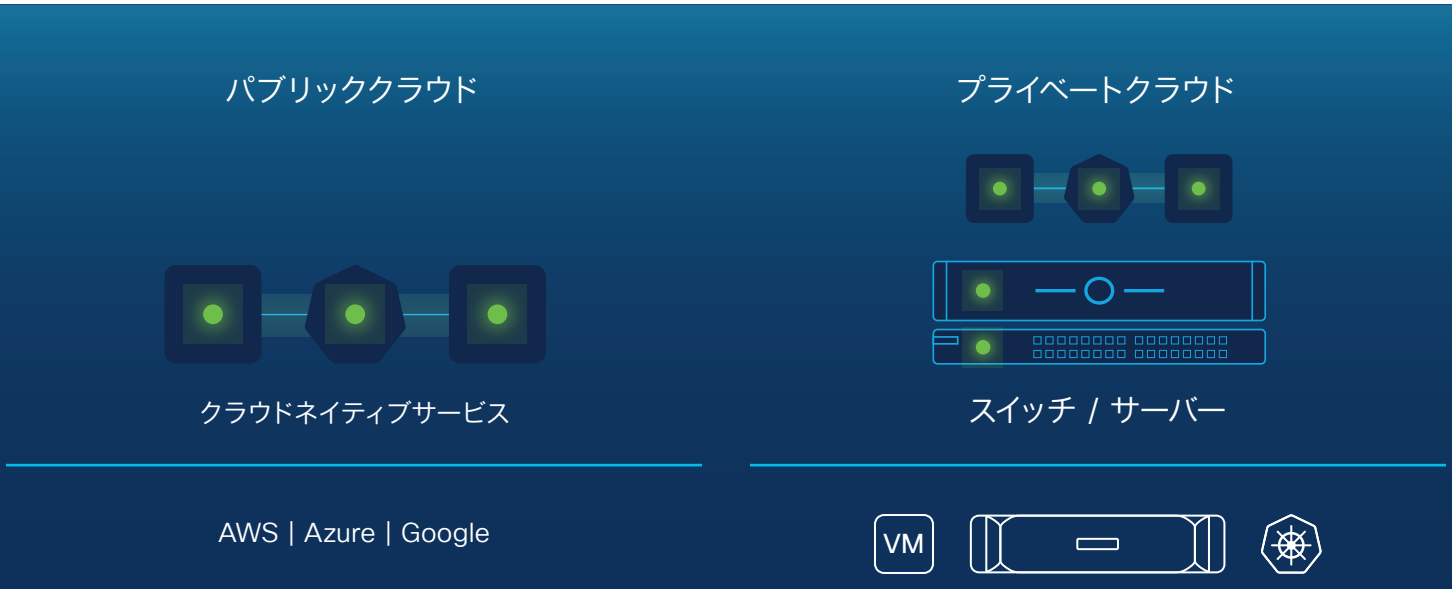

図 1. 必要な場所でセキュリティを実現できる Hypershield

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、AI ワークロード専用に構築された独自のアーキテクチャにより、セキュリティを刷新します。

Hypershield は、既存のハードウェアに追加される構成可能な**サブスクリプションベースのソリューション**です。ソリューションのコア機能上に構築された**モジュール**は、セグメンテーションや脆弱性のエクスプロイトからの保護など、特定のセキュリティユースケースを提供します。

- **AI ネイティブセキュリティ：**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。
- **カーネルレベルでの適用：**Hypershield は、Isovalent 社（現在はシスコグループ）の Tetragon と eBPF 上に構築された Tesseract Security Agent により、ワークロードレベルでの詳細な可視性と適用アクションを提供します。eBPF を使用すると、カーネル自体を変更したりシステムの安定性を危険にさらしたりすることなく、カーネル機能を安全に拡張できます。これにより、Hypershield はワークロードの動作を詳細に可視化し、きめ細かいセキュリティ制御を実装できます。また、ポリシーの更新を推奨、テスト、展開する際にアプリケーションは実行され続けます。
- **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。Hypershield の推奨ポリシーと独自のソフトウェアアップデートは、ラボやシミュレーションではなく、本番環境のトラフィックでテストされます。これらのテストの結果は、展開の確実性スコアと展開の有効性スコアを含むレポートとして表示されます。これによりセキュリティ管理者は、ビジネスを中断させることなく、自信を持ってアップデートを承認できます。承認されたアップデートは展開されます。

図 2.　Cisco Hypershield アーキテクチャ

図 3.　分散型適用の中央管理

一元的なセキュリティポリシー

高度に分散された IT 環境では、複数のドメインにまたがってセキュリティポリシーを管理および適用するための新しい方法が必要です。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。シスコは 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支援します。

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。

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時間がかかり、単一のアプリケーションのルールを定義するのに最大 40 日、もしくはそれ以上かかります。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、一定期間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。

たとえば、工場内の必要な場所に板金を配送するアプリケーションを想像してみてください。従来のセキュリティツールは、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 は、他のソリューションがトレーニングのために重視するネットワークフローの先を見据えています。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、環境内のアプリケーションとそれらがどのように通信して動作する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、学習するにつれて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。

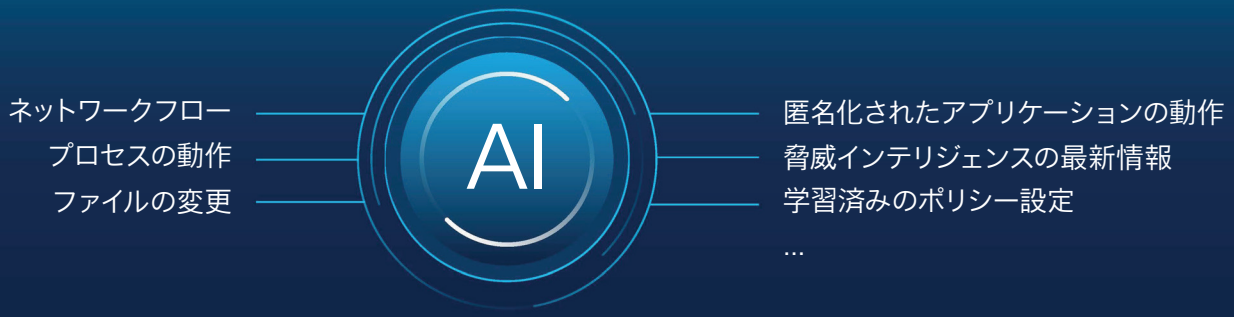

図 4.　Hypershield がセグメンテーションポリシーの作成に包括的な入力セットを使用

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、環境全体の脆弱性のある資産を把握します。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、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。これらの優先順位付けは、次の 3 つの重要な質問に基づいています。

- 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軽減コントロールや軽減シールド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、軽減コントロールは自動的に削除されます。

図 5. Hypershield が軽減シールドを適用して脆弱性のエクスプロイトから保護

図 6.　Cisco Hypershield のデュアルデータプレーン

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シームレスかつ無停止で行うメカニズムが必要です。

前述のように、Hypershield はアップデートを自己検証できます。これにより、ポリシーの更新とソフトウェアアップグレードに関連するリスクが軽減され、最新のセキュリティ態勢と大規模なポリシーライフサイクル管理が実現します。

ネットワークベースのエンフォーサは、**デュアルデータプレーン**を使用して自己検証型アップデートを実行します。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。これは実質的に、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。管理者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に加えて、エンドシステムエンフォーサ（Tesseract Security Agent を利用）にも同様の（ただし異なる）方法があり、アップデートを自己検証します。

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す。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、自己検証型アップデートにより、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。

同時に、お客様自ら 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。

関連情報

- 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。