データシート
Cisco Public

Cisco Hypershield

AI スケール | クラウドネイティブ | 高度な分散型

目次

製品の概要

Cisco® Hypershield は、分散型の AI ネイティブ セキュリティ アーキテクチャです。シスコのビジョンは、必要な場所（ネットワーク、サーバー、およびパブリッククラウドやプライベートクラウドの展開で実行されるあらゆる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）にセキュリティを配置することです。

Hypershield は、以前は専用のボックスで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に組み込むことで、セキュリティとネットワーキングを独自に組み合わせます。また、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 搭載の管理を提供します。同時に、お客様は、テスト機能やレポート機能を使用して信頼を獲得し、希望する自律性のレベルを選択できます。

Hypershield を使用すると、単一のポリシーフレームワークや管理システムから、ワークロードやネットワーク内にセキュリティを組み込むことができます。

今日のセキュリティの課題を克服する独自の機能

- **AI ネイティブセキュリティ：**Cisco Hypershield は、追加機能として AI を追加しているのではなく、その中核に人工知能を使用して設計されています。たとえば、Hypershield は、環境の監視を開始した瞬間から大量のセキュリティデータを自動的に分析し、インテリジェントな推奨事項を提示し、インサイトを生成できます。このシステムは、人間による監視を維持しながら、複雑な分析プロセスと意思決定プロセスを自動化することで、セキュリティチームがより効率的に作業できるようにします。
- **カーネルレベルの適用：**Hypershield は、ワークロードの優れた可視性と、Linux カーネルにネイティブであるオペレーティング システム レベルでの適用を提供するため、アプリケーション プロセス アクションやセキュリティアクションに必要なサージカルコントロールを高性能で詳細に可視化できます。
- **自己検証型アップデート：**セキュリティには、高い確実性と慎重なアクションが求められます。Hypershield は、変更に対して自己アップグレードおよび更新するように設計されています。管理者は、ライブの実稼働環境に対してテスト済みのポリシー更新および Hypershield ソフトウェアアップグレードをプレビューすることで、ターゲットのセキュリティ態勢を迅速に実現できます。

詳細については、**cisco.com/go/hypershield** を参照してください。

使用例

自律セグメンテーション

現代のセキュリティの課題に対応するには、従来のツールで提供できる以上の機能が必要です。現在のセグメンテーションツールは、アプリケーション（アプリ）に関する深い理解が欠けており、アプリケーション固有のイベントや新しいリリースごとにアプリがどのように進化するかを考慮せずに、経時的なネットワークフローの観察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。従来のアプローチではアプリケーションの変更を見逃す可能性があり、結果としてアプリケーションの脆弱性が高まります。そのため、組織は攻撃対象領域を減らすために、より効果的なセグメンテーション アプローチを必要としています。

Hypershield の**自律セグメンテーション モジュール**は、アプリケーションの動作やその他の重要な入力に対する深い理解に基づき、動的でインテリジェントなセグメンテーションモデルでこのプロセスを変革します。このモデルは、観測内容とお客様定義のポリシーに基づいて継続的に適応され、従来のセグメンテーションに伴う時間と複雑さを軽減します。

Distributed Exploit Protection

セキュリティパッチの適用は、今日の組織にとっての課題です。パッチのインストールは事業運営を中断する可能性があり、企業はダウンタイムを回避するために重要なセキュリティ更新を数か月にわたって遅らせることがあります。別の軽減策の場合、分析、導入、テストに多くの手作業が必要になり、アプリケーションの稼働時間に関する重大なリスクも伴います。

Hypershield は、**Distributed Exploit Protection モジュール**を使用して、新しい脆弱性に対する保護にかかる時間を短縮することでこの問題に対処します。このモジュールは、検出、優先順位付け、制御の評価からテストと展開まで、プロセス全体を自動化し、アプリケーションを中断することなく、スムーズに実行を継続できるようにします。

製品のアーキテクチャ

Tesseract Security Agent。この安全で高性能なエンフォーサはワークロードに存在し、extended Berkeley Packet Filter（eBPF）を介してプロセスおよびオペレーティング システム カーネルとインターフェイスをとります。このエンドシステムエンフォーサは、Kubernetes 環境で簡単に展開できるように最適化されており、Kubernetes 以外の設定でも完全に機能します。また、ワークロード内での優れた可視性と適用、ネットワーク接続、ファイルとシステムコール、およびカーネル関数のモニタリングを提供し、イベントベースのテレメトリを生成します。

ネットワークベースのエンフォーサ。このエンフォーサには、ネットワークベースのアプライアンスまたは仮想マシン（VM）が搭載されています。従来の一元化された適用アプローチから脱却し、ネットワークベースのエンフォーサをワークロードの近くに戦略的に配置して、特定のアセットをより効果的に保護します。また、ネットワークベースの可視性、適用、およびデータプレーンのデジタルツインを使用したチェックと自己検証型アップデートを提供します。

> **デュアルデータプレーン**。インフラストラクチャやポリシーの変更に対する従来のソフトウェアアップグレードは、事業運営を中断させる高いリスクを伴います。そのような更新は、テストに多大な時間とリソースを必要とするため、通常は年に数回に制限されます。この更新サイクルが遅いと、組織の防御機能は古くなり、新たな脅威に対して脆弱になります。Hypershield は、ネットワークベースのエンフォーサを使用して、自己検証型アップデートをチェックし、デュアル データ プレーン テクノロジーでこの課題に対処します。このアプローチにより、ライブの実稼働トラフィックが現在のルールで動作し、同時に、実稼働トラフィックのコピーをネットワークベースのエンフォーサ内のシャドウデータプレーンに送信できます。このシャドウプレーンを使用すると、管理者は、ライブトラフィックを使用して、展開前に、実稼働環境に影響を与えることなく、新しいソフトウェアアップグレードやポリシーの変更をテストおよび検証できます。
>
> Hypershield のデュアルデータプレーンにより、IT およびセキュリティチームはより頻繁に自信を持って更新を展開できるため、ビジネスプロセスを中断することなく、最新の脅威に対する堅牢な防御を確保できます。

統合クラウド管理。適用ポイントのフォームファクタや場所に関係なく、Hypershield はインテントベースのポリシーモデルを実装するように設計されており、一元化されて管理しやすくなっています。新しいポリシーや更新されたポリシーはコンパイルされ、インテリジェントに適用ポイントに配布されます。Cisco Security Cloud Control（旧 Cisco Defense Orchestrator）SaaS 管理を利用したこのシステムにより、展開先がパブリッククラウドか、プライベートクラウドかに関係なく、管理者は展開されたすべてのポリシーの包括的な概要を維持できます。

統合コントロールプレーン。Hypershield は、セキュアなコントロールプレーンを使用してエンフォーサをクラウド管理システムにリンクし、環境全体でのスムーズなポリシーの配布を可能にします。エンフォーサはシスコのクラウドサービスに外部接続し、展開とファイアウォールのセットアップを簡素化します。両サイドで相互の ID を確認して、不正アクセスが防止され、コントロールプレーンにより双方向通信が可能になります。エンフォーサは、セキュリティイベントとパフォーマンスデータを送信しながら、ポリシーと更新を受信します。コントロールプレーンで

は、多くの場所にまたがる数千のエンフォーサを管理でき、ネットワークの問題が発生した場合にバックアップから復元できます。このセットアップにより、Hypershield のコンポーネントがワークロードからクラウドに結び付けられます。また、セキュリティポリシーと脅威情報をすばやく拡散し、どこでも一貫したセキュリティを維持できます。

AI ネイティブセキュリティ。AI を統合して新たに設計された Hypershield は、適切なレベルの自律性、レポート、および制御を通じて信頼を獲得し、高い有効性、迅速な対応、継続的な保護を実現します。システムはポッドやコンテナなどのワークロードオブジェクトを自律的にグループ化し、そのルールをテスト、展開、および管理できますが、ユーザーは完全な制御権限と最終権限を持ちます。また、AI アシスタントが分析、観察された動作、推奨事項などを説明してくれます。

グローバルグラフエンジンHypershield の中核となる強力なグラフエンジンは、リアルタイムのテレメトリデータを処理して、ネットワークアクティビティとシステム運用の複雑な動作モデルを構築して分析します。これは、ネットワークベースのエンフォーサからのトラフィックフローデータとともに、Tesseract Security Agent からのプロセス、ファイルアクセス、ネットワーク接続、およびプロセス間通信を収集および解釈することで実現されます。Hypershield では、このような大量のデータをバックエンドに送信して処理する代わりに、テレメトリをエッジで直接処理することによって動作グラフが作成されます。動作グラフは、アプリケーションのフィンガープリントを有効にし、脅威検出に情報を提供するために使用されるネットワーク動作の動的モデルです。Hypershield は、動作グラフを使用してデータの負荷を最小限に抑えることでリアルタイムの判断を下せるため、組織は脅威検出時間と応答時間を短縮できます。

製品の機能と利点

製品モジュール：各モジュールは、前述のアーキテクチャ コンポーネントを使用して、特定の使用例を解決するために開発されました。

モジュール	機能/利点
自律セグメンテーション	• **アプリケーションのフィンガープリント**：ワークロードの分類と優れたデータ衛生は、正常なセグメンテーションおよびワークロード管理を簡素化するための基盤です。システムは、すべてのプロセスとネットワークアクションの高性能の分散分析に基づいて、ワークロードの自律的な検出、タグ付け、およびグループ化を実現します。 • **ポリシー管理の簡素化**：複数のデータセンターにおけるポリシーの保守は、エラーが発生しやすく、時間がかかる場合があります。単一のポリシー管理により、パブリッククラウドとプライベートクラウドの複数の適用ポイントをセグメント化できます。 • **展開の確実性スコア**：ポリシー、保護、およびソフトウェアアップデートのパフォーマンスをリアルタイムで把握することで、自信を持って展開できます。[展開（Deploy）] を選択する前に、ライブの実稼働トラフィックに対する CPU 使用率、メモリ使用率、および遅延の変化を比較できます。
Distributed Exploit Protection	• **脆弱性の検出**：Common Vulnerabilities and Exposures（CVE）のデータベースに対してインストール済みのソフトウェアを自動的にスキャンすることにより、ワークロードの既知のセキュリティ脆弱性を特定します。 • **軽減シールド**：セキュリティ管理の的確な軽減策を実装することにより、既知の脆弱性からアプリケーションが保護されるため、アプリケーションチームは、システムを攻撃にさらすことなく、ソフトウェアパッチを適切にテストして展開できます。

製品アーキテクチャ：Cisco Hypershield アーキテクチャは AI を利用してゼロから構築されており、エージェントとエージェントレスの両方のフォームファクタを提供し、一元化されたクラウド管理プラットフォームによってすべて統合されています。

コンポーネント	機能/利点
Tesseract Security Agent	• **カーネルレベルの可視性と適用**：アプリケーションを中断または変更することなく、ワークロード内で実行されているすべてのプロセス、ネットワークフロー、システム I/O を完全に可視化し、制御します。
ネットワークベースのエンフォーサ（ネットワークアプライアンス/仮想マシン搭載）	• **ネットワークレベルの適用**：レイヤ 3 およびレイヤ 4 のネットワーク適用を備えた仮想マシンアプライアンスを使用して、East/West トラフィックを保護します。 • **自己検証型アップデート**（デュアルデータプレーン経由）：展開前に、ライブトラフィックを使用して新しいファームウェアのアップグレードまたはポリシーの変更をテストおよび検証するために、デュアルデータプレーンを使用することで、更新サイクル間の時間を最小限に抑えます。実際の実稼働環境に影響を与えることはありません。
統合クラウド管理（Cisco Security Cloud Control を利用）	• **統合されたポリシー管理とレポート**：適用ポイントのフォームファクタや場所に関係なく、一元化された場所からすべてのポリシーを整理および管理します。 • **簡素化されたスケーラブルなポリシー**：適用ポイント全体で大規模にポリシーをコンパイルして配布するインテントベースのポリシーモデルを使用して、ポリシー管理を簡素化および自動化します。 • **ポリシーのテスト**：展開前にライブトラフィックに対してポリシーを自己検証することにより、推奨されるポリシーの信頼性を高めます。
AI ネイティブセキュリティ（Cisco Security Cloud Control を利用）	• **AI を活用した分析**：ネットワーク、プロセス、プロトコル、ポート、ファイル検査、アプリケーション動作に至るまでのワークロードアクション間の関係を可視化します。 • **Cisco AI Assistant**：広範かつ大規模な Hypershield データにアクセスし、迅速な意思決定をよりインテリジェントにガイドし、情報を提供します。

サブスクリプション要件

Cisco Hypershield のサブスクリプション価格は、購入した保護ユニットの数に基づいています。保護ユニットは、ネットワーク内での Hypershield コンポーネントの展開を可能にする割り当ての単位です。アクティブなサブスクリプションには少なくとも 100 保護ユニットが必要です。お客様は、有効なサブスクリプション期間中にいつでも保護ユニットを再割り当てでき、追加の保護ユニットを購入できます。保護ユニットの割り当ては、Cisco Security Cloud Control にある Hypershield モジュール内でモニターできます。

使用例に応じて、適用はネットワーク内の異なる場所で実行され、さまざまな数のユニットを使用できます。

エンフォーサタイプ	展開	保護ユニットコスト
Tesseract Security Agent	Linux ワークロード VM	展開ごとに 12 ユニット
	Kubernetes ノード（各 16 vCPU、64 GB RAM）	展開ごとに 36 ユニット
ネットワークベースのエンフォーサ	VM アプライアンス	展開ごとに 36 ユニット

導入モデルと規模

Hypershield は、適用のニーズに基づいて展開でき、柔軟に拡大/縮小できます。製品は、次のバリアントで展開できます。

エンフォーサタイプ	展開	仕様
Tesseract Security Agent	Linux ワークロード VM	Linux ワークロード VM に展開されたエージェント
	Kubernetes ノード（各 16 vCPU、64 GB RAM）	Kubernetes ノードに展開されたエージェント
ネットワークベースのエンフォーサ	VM アプライアンス	ネットワーク適用ポイントの仮想イメージ

ソフトウェア サブスクリプション モデル

Hypershield ユニットは、前述の適用ポイント全体で適用できます。

機能	Essentials
モジュール	
自律セグメンテーション モジュール	
アプリケーションのフィンガープリント	✓
簡素化されたポリシー管理	✓
展開の確実性スコア	✓
Distributed Exploit Protection モジュール	
脆弱性の検出	✓
軽減シールド	✓
アーキテクチャ	
Tesseract Security Agent	
カーネルレベルの可視性と適用	✓
ネットワークベースのエンフォーサ	
ネットワークレベルの適用	✓
自己検証型アップデート（デュアルデータプレーン経由）	✓
統合クラウド管理	
統合されたポリシー管理とレポート	✓
簡素化されたスケーラブルなポリシー	✓

機能	Essentials
モジュール	
ポリシーのテスト	✓
AI ネイティブセキュリティ	
AI を活用した分析	✓
Cisco AI Assistant	✓

サポートと互換性

Hypershield に推奨される Linux および Kubernetes ディストリビューション リリースを以下に示します。

Linux ディストリビューション	最小カーネルバージョン
Ubuntu 22.04 LTS	5.15
Ubuntu 20.04 LTS	5.4
Red Hat Enterprise Linux 9	5.14
Fedora 38	6.3
Debian 12	6.1
Debian 11	5.10
Arch Linux	6.4
CentOS Stream 9	5.14

Kubernetes ディストリビューション	Kubernetes の最小バージョン
Amazon Elastic Kubernetes Service（EKS）	1.23

AI とプライバシー

責任ある AI

シスコは、人工知能（AI）を活用することで、すべての人にとって包括的な未来を実現できることを理解しています。また、このテクノロジーを適用することで、損害発生の可能性を軽減する責任があることも認識しています。そのため、シスコは、透明性、公平性、アカウンタビリティ、プライバシー、セキュリティ、信頼性の 6 つの原則に基づく責任ある AI フレームワーク（以下「フレームワーク」）を遵守しています。シスコは、これらの原則を製品開発要件に取り入れ、最終的にはセキュリティバイデザイン、プライバシーバイデザイン、およびヒューマンライツバイ デザイン プロセスとともに製品開発ライフサイクルの一部を形成しています。

したがって、AI ネイティブソリューションとしての Cisco Hypershield は、透明性、公平性、アカウンタビリティ、プライバシー、セキュリティ、および信頼性を中核として構築されています。AI を利用するすべての機能とモジュールは、AI インパクト（AII）アセスメントの対象となります。AII インパクト（AII）アセスメントは、フレームワークの原則に対する機能の技術的基盤の適用程度を示すクラス最高水準のレビューです。

詳細については、Responsible AI Web ページ [英語] を参照してください。

データプライバシー

Cisco Hypershield Privacy Data Sheet [英語]

Cisco Security Cloud Control (previously Cisco Defense Orchestrator) Privacy Data Sheet [英語]

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用、拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

次の表に、環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

Cisco Capital

Cisco Capital® により、目標を達成するための適切な技術を簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 か国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

Cisco Hypershield の詳細については、https://www.cisco.com/go/Hypershield を参照するか、最寄りのシスコアカウント担当者にお問い合わせください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-4789245-01 01/25