The bridge to possible

Cisco Hypershield の概要

データセンターとクラウド向けの AI ネイティブセキュリティ。いかなるときも、どんな場所でも。

AI スケールのデータセンターの時代には、人間の力だけでセキュリティ管理を行うことはできません。ワークロードは通常、複数のデータセンターとクラウドに分散されているため、ポリシーがバラバラになって保護範囲が曖昧になり、問題やインシデントが発生した際の修復が遅れてしまいます。同時に、攻撃者はこれまで以上の速さであらゆる脆弱性を悪用するようになっています。AI の導入が進むにつれて、この傾向は加速するでしょう。最新のアプリケーションと動的なコンピューティング環境を保護するには、まったく新しいアプローチが必要です。

Cisco Hypershield は、オンプレミス環境とクラウド環境の両方でセキュリティに革命をもたらし、企業が最新のアプリケーションをより効果的に保護できるようにします。この画期的な製品を特徴付けるのは新しい分散アーキテクチャであり、ネットワークとワークロードの適用ポイントを一元化された管理システムに統合します。Hypershield により、企業は堅牢で拡張性に優れた保護を実現し、セキュリティ境界を従来のインフラストラクチャからクラウドにシームレスに拡張できます。

メリット

- **あらゆる場所を保護。**ネットワークのすべての領域に及ぶ超分散型セキュリティアプローチを導入し、以前は到達できなかったさまざまなワークロードやネットワークの適用ポイントを活用します。
- **エクスプロイトのギャップを解消。**このシステムは数分でアプリケーションのエクスプロイトをブロックします。数週間や数か月ではありません。最適な効果を得るため、本番環境のライブトラフィックに対し評価とテストが実施される高精度かつ補完的なコントロールを採用しています。
- **信頼性の高いセグメンテーション。**継続的に状況に適応し学習する効果的なセグメンテーションを実現します。時間経過とともに精度と信頼性を高め、正規表現のフィルタを作成するほどにその環境に特化したコントロールを適用することで、よりカスタマイズされたセキュリティを実現します。
- **信頼を獲得したら、あとは自律的に管理。**ネットワークとワークロード全体を一元管理できます。デュアルデータプレーン アプローチを使用してソフトウェアとポリシーの更新を自信を持って展開し、運用をリスクにさらすことなく、ライブトラフィックで安全にテストできます。

The bridge to possible

Cisco Hypershield の機能

以前は想像もできなかった成果を実現

Hypershield は、今日の現実に対処するためにゼロから構築されたまったく新しいアーキテクチャです。

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

今日のデジタル環境では、脆弱性がかつてない速さで悪用されています。AI を活用した攻撃によって数時間以内に悪用されることもあります。従来のパッチ適用では間に合わない状況です。パッチの適用には数週間から数か月かかることが多く、業務が中断されてしまったり、ダウンタイムを避けるために重要な更新を遅らせることを余儀なくされたりすることがあります。

Hypershield は、**Distributed exploit protection（分散型脆弱性対策）モジュール**でこの課題に正面から取り組み、新たな脆弱性に対する防御に要する時間を大幅に短縮します。このモジュールは、コントロールの検出、優先順位付け、評価からテストと展開に至るプロセス全体を自動化します。これにより、アプリケーションが中断することなくスムーズに稼働し続けるようになります。

主な特長

- **自動化されたワークフローによる迅速な対応。**シスコの AI ネイティブエンジンが脆弱性を迅速に検出して優先順位付けを支援し、最も必要とされるところに力を注げるようにします。さまざまなアプローチを評価し、お客様の環境に合わせて最も効果的なソリューションを提案し、継続的に信頼を構築します。
- **精度の高い補完コントロール。**ワークロードとネットワークの適用ポイントの分散メッシュに、カスタマイズされたコントロールが直接展開されるため、正確かつ効果的に脆弱性を緩和できます。
- **自信を持って更新。**すべての補完コントロールは、本番環境のライブトラフィックに対してテストされるため、アプリケーションを危険にさらすことなく、有効性を高め、配置を最適化することができます。

Autonomous segmentation（自律型セグメンテーション）

今日のセキュリティの課題は、従来のツールで対応できる以上のことを求めています。1 つのアプリケーションをセグメント化するのにかかる平均時間は 40 日を超えており、多くの場合、ルールを実装してもすぐに古くなってしまうため、企業は重大なセキュリティギャップに直面しています。攻撃者はこれらのギャップを突いてネットワークを横断し、リスクを急増させます。

Hypershield の **Autonomous segmentation（自律型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情報についての深い理解に基づく動的でインテリジェントなセグメンテーションモデルによって、このプロセスに変革をもたらします。このモデルは、観察結果とお客様によって定義されたポリシーに基づいて継続的に適応し、従来のセグメンテーションに要していた時間と関連する複雑さを大幅に削減します。

Hypershield の Autonomous segmentation（自律型セグメンテーション）により、アプリケーションをより効果的かつ先制的に保護し、攻撃者を寄せ付けません。

主な特長

- **継続的な適応。**ネットワーク自体がセグメント化され、現在の状況に合わせて動的に調整され、常に最新の状態で保護されます。
- **包括的なデータに基づく情報。**シスコのセグメンテーション戦略には、ネットワークフローにとどまらず、プロセスの動作やアプリケーションの更新などの多様な情報を取り入れています。この包括的なアプローチにより、きめ細かい効果的なセグメンテーションが可能になります。
- **全体的な保護ポリシーから始まる精密なコントロール。**広範な保護パラメータに始まり、特定の正規表現のフィルタ処理に至るまでコントロールを微調整することで、正確かつ効果的にリスクを軽減できます。

Self-qualifying updates（自己検証型アップデート）

従来の方法でのインフラストラクチャに対するソフトウェアアップグレードやポリシーの変更には、事業運営の中断という高いリスクがあります。これらの更新プログラムのテストには多くの時間とリソースが必要であり、通常は年に数回に制限されます。更新サイクルが遅くなると、企業は時代遅れの防御を使用することになり、新たな脅威に対して脆弱になってしまいます。Hypershield は、**デュアルデータプレーン**技術により、この課題に画期的なソリューションをもたらします。この革新的なアプローチにより、本番環境のライブトラフィックを現在のルールで運用しながら、トラフィックのコピーを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は、実際の本番環境に影響を与えることなく、新しいソフトウェアのアップグレードやポリシーの変更をテストします。

Hypershield のデュアルデータプレーンにより、IT チームとセキュリティチームは、これまでより頻繁に、より自信を持って更新プログラムを展開できるようになりました。ビジネスプロセスを中断させることなく、最新の脅威に対する堅牢な防御を実現できます。

主な特長

- **中断を伴わないテスト。**シャドウデータプレーンは、ライブトラフィックをミラーリングすることで新しいポリシーとソフトウェアアップグレードを評価し、本番運用に影響を与えないようにします。
- **継続的改善。**リアルタイムで更新をテストすることで、Hypershield は従来の更新に必要だった時間とリソースを大幅に削減します。
- **情報に基づく意思決定。**テスト後、Hypershield は詳細なレポートを生成し、新しい更新を展開すべきかどうかについて AI の支援による推奨事項を提示します。これにより、信頼が高まって業務効率が向上します。また運用担当者は、結果と推奨事項の説明を助けてくれる AI アシスタントを活用することで、信頼を高めることができます。

The bridge to possible

シスコの Hypershield アーキテクチャ

これは次世代のものではなく、第 1 世代の新製品です。

Hypershield は、ハイパースケーラ技術をあらゆる規模の企業が利用できるようにすることで、AI スケールのアプリケーション インフラストラクチャとシステムを保護する際に、優れた有効性、エクスペリエンスの強化、経済性の向上を実現します。**フェンスというよりもファブリックのような** Hypershield は、高度に分散された環境の必要な場所に、クラウドのスピードでシームレスにセキュリティを適用します。

このソリューション アーキテクチャの主なコンポーネントは次のとおりです。

Tesseract Security Agent（TSA）：この安全で高性能なエージェントはワークロードで動作し、拡張 Berkeley Packet Filter（eBPF[1]）を通じてプロセスおよびオペレーティング システム カーネルと連携します。TSA は Kubernetes 環境に簡単に展開できるように最適化されていますが、Kubernetes 以外の環境でも完全に機能します。ワークロードのアクションを完全に可視化し、ネットワーク接続、ファイルコールとシステムコール、カーネル関数をモニタリングし、異常なアクティビティがあればアラートを出します。

仮想マシンおよびコンテナベースのネットワーク適用ポイント。Hypershield には、仮想マシンやコンテナ内で動作するネットワーク適用ポイントが含まれています。

特定の資産をより効果的に保護するために、適用ポイントはワークロードの近くに戦略的に配置されます。集中的だった従来の適用アプローチとは一線を画すものです。

クラウドの一元管理。適用ポイントのフォームファクタや場所に関係なく、すべてのポリシーは Hypershield の管理コンソールで一元的に整理され、管理されます。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、適切な適用ポイントにインテリジェントに配布されます。このシステムにより、展開されたすべてのポリシーの包括的な概要をセキュリティ管理者が維持することができ、オンプレミス環境からパブリッククラウド、またはサーバー間で移動するワークロードへの動的な適応が可能になります。

AI ネイティブ。AI を統合してゼロから設計された Hypershield は、高い有効性、迅速な対応、継続的な保護を実現します。このシステムは、デュアルデータプレーンと、ネットワークとワークロード全体の広範な可視性を活用して、独自のルールを自律的に作成、テスト、展開、管理することができます。また、分析、観察された動作や推奨事項などの説明に AI アシスタントを利用することも可能なので、適切なレベルの自律性とコントロールによって信頼を得ることができます。

詳細については、cisco.com/go/hypershield をご覧ください

[1] 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。これを使用すると、ユーザー空間のプログラム（この場合は Tesseract エージェント）はカーネルを経由して適用とモニタリングのアクションを安全に実行できます。