Cisco Cloud Application Security

目次

アプリケーションのトレンド

クラウドアプリケーションは、デジタルビジネスの未来です。実際、2025 年までに、組織は現在の約 3 倍に相当する 7 億 5,000 万を超えるクラウドアプリケーションを実行するようになると予想されます。さらに、85% 以上の組織がクラウド開発の原則の採用を計画をしており、これらの新しい環境を保護するために必要なアプリケーション アーキテクチャの標準と、セキュリティプラクティスを再定義しています。

クラウドアプリケーションはそれぞれ異なる方法で構築されているため、それらを保護するための革新的なアプローチが必要です。クラウドアプリケーション：

- ローカル企業のデータセンターの固定サーバーハードウェアで実行するのではなく、サーバーレス インフラストラクチャでホストされている。
- モノリシックコードの大きなブロックで構成されるアプリケーションとしてではなく、相互に依存する小規模なサービスとして設計されている。
- 特定のアプリケーション用に作成されたカスタム プログラム サブルーチンのライブラリではなく、API（アプリケーション プログラミング インターフェイス）とオープンソースコードを再利用可能なアプリケーション構成要素として使用する。

新しいセキュリティアプローチが必要

API とオープンソースコードは、繰り返し使用できるクラウドアプリケーションの「構成要素」であり、アプリケーション開発時間を短縮します。この再利用は、時間の節約と開発のアクセラレータとして優れていますが、組織がサードパーティのアーティファクトに組み込まれた汚染されたコードにさらされる可能性があります。多くの場合、これらのアーティファクトの発生源を検証するのは困難です。つまり、適切なツールを持たない組織は、ある時点で無意識のうちにアプリケーションに不正なコードをインポートすることになります。このリスクによって、開発からクラウドの導入までのクラウド アプリケーション プロセス全体をセキュアにするために、複数の異なるテクニックを使用し、**攻撃者のように考える**統一されたセキュリティプラットフォームを中心としたセキュリティ戦略に重点を置くことが重要になります。

Cisco Cloud Application Security の概要

Cloud Application Security は、クラウドセキュリティ態勢管理（CSPM）、クラウドワークロード保護（CWPP）、API セキュリティ、および Infrastructure as Code（IaC）セキュリティを統合する統合セキュリティ プラットフォームであり、可視性のギャップを最小限に抑え、中央管理を提供します。現在一般的な複数のセキュリティポイント製品を使用するのとは異なり、Cloud Application Security はシスコのオールインワン セキュリティ ソリューションであり、次の方法で生産性を向上させながら、リスクとコストを大幅に削減するように設計されています。

- **コードからクラウドまでの包括的なカバレッジ。**1 つまたは複数のクラウドでアプリケーションを構築して実行するかどうかにかかわらず、Cisco Cloud Application Security は、アプリケーションのライフサイクル全体と、Kubernetes クラスタを含むすべてのクラウド資産をカバーする包括的な保護を提供します。

- **コンテキストに応じたリスクの優先順位付け。**Cloud Application Security の攻撃経路エンジンは、設定不備、ネットワークの露出、秘密、脆弱性、マルウェア、および過度に寛容なアイデンティティを積極的に分析し、環境に侵入して横方向に移動するために使用される可能性のあるエクスプロイト可能な経路を見つけます。これらの攻撃経路は重大度によって優先順位付けされ、無数のアラートでオペレータを圧倒することなく、最大の脅威を明確に示します。
- **動的修復ガイダンス。**Cloud Application Security は、環境で検出された脅威を迅速かつ効果的に修復するためのガイダンスを動的に生成します。このガイダンスには、修復手順と各手順の特定のコマンドが含まれています。このガイダンスを既存の問題管理システムとワークフローに統合して、デベロッパーやエンジニアが問題を迅速かつ効果的に解決するためのチケットを作成できます。

機能と利点

Cloud Application Security の主な機能と利点を以下に示します。

表 1. 機能とメリット

機能	利点
エージェントレススキャン	• エージェントレステクノロジーは、Azure、AWS、GCP、OCI、Kubernetes、またはそれらの組み合わせなど、あらゆるクラウド環境をスキャンします。
API セキュリティ	• ワークロードで使用される信頼できない外部および内部の API に関連するリスクを分析します。 • 検査のために外部または内部 API 仕様を自動的にアップロードします。 • API トラフィック（外部と内部の両方）のトレース分析を実行して、リスクスコアに影響を与えるセキュリティ問題を特定します。
攻撃経路分析	• 攻撃者の視点から環境を見ることで、最も重大なリスクに焦点を当てます。 • 重要ではないセキュリティの検出結果を減らし、チームの生産性を向上させます。
CI/CD セキュリティ	• アプリケーション開発プロセス全体でセキュリティの自動化を促進し、デベロッパーがセキュリティリスクを評価して軽減できるようにします。 • コードの脆弱性、IaC の設定不備、API セキュリティなどのリスクを軽減します。
クラウドセキュリティ態勢管理（CSPM）	• コンプライアンス標準とベストプラクティスをモニタリングすることで、セキュリティチェックがすべての監査に合格し、ビジネス目標を満たしていることを確認します。 • PCI-DSS、HIPAA、GDPR、SOC2、および CIS（Center for Internet Security）ベンチマークを適用します。 • すべてのクラウド資産のインベントリを作成し、すべての設定不備に加えて次のアイデンティティリスクを特定することで、コンプライアンスを超えます。 ◦ 一般的な設定不備 ◦ 危険なデフォルト ◦ ダングリングドメイン ◦ 公開された秘密の検出 ◦ 有効な権限の評価 ◦ 情報公開の特定 ◦ 無視されたリソース ◦ 危険な設定と脆弱な設定 ◦ 危険な権限 ◦ シャドウ管理者 ◦ サポート対象外のソフトウェア

機能	利点
	• 脆弱性に関連する設定不備や、攻撃経路に関連するその他のセキュリティ問題を理解し、問題の優先順位付けをさらに高めることができます。
クラウドワークロード保護（CWP）	• 攻撃対象領域を最小限に抑え、管理者のエラーを防ぎ、一般的な攻撃ベクトルから保護します。 • セキュリティおよびコンプライアンスチームがポリシー主導のセキュリティ設定とガバナンスを適用できるようにします。 • 継続的なセキュリティリスクのアセスメントと修復により、クラウドアプリケーションに不可欠なオーケストレーションレイヤを保護します。
Infrastructure as Code（IaC）セキュリティ	• IaC ファイルをスキャンして、生産に展開する前に、セキュリティの脆弱性とインフラストラクチャの設定不備を検出します。
Kubernetes セキュリティ態勢管理（KSPM）	• セキュリティリスクとコンプライアンス違反について、Kubernetes クラスタの継続的な可視性とモニタリングを提供します。 • コンテキストマッピングを使用して Kubernetes オブジェクト間の関係を特定し、クラスタのセキュリティ態勢の正確な最新のビューを提供します。 • Kubernetes クラスタのセキュアな設定を保証し、脆弱性と設定不備を検出し、セキュリティ侵害のリスクを軽減します。 • マルチクラウド Kubernetes ワークロードの脆弱性や一般的な設定不備をスキャンすることで、実用的なインサイトを提供します。 • 宣言型ポリシーの自動化を有効にします。
根本原因分析	• 表面レベルのインサイトを超えて、複数の攻撃経路を可能にする単一の根本原因などの問題を見つけます。 • 分析にかかる膨大な手作業時間を削減します。
サーバーレスセキュリティ	• デベロッパーは、インフラストラクチャを管理することなく、クラウドの機能とサービスの開発と展開に集中できます。
ソフトウェア サプライ チェーンのセキュリティ	• 各イメージのソフトウェア部品表（SBOM）を生成します。 • 各レイヤの脆弱性を特定します。 • 設定リスクの展開テンプレートを分析します。 • CIS ベンチマークを通じてベストプラクティスへの準拠を確認します。 • アプリケーション デベロッパーが連邦政府の義務に準拠していることを確認します。 • CI/CD セキュリティ機能は、アプリケーション開発プロセスでセキュリティの自動化を促進し、デベロッパーが IDE、Terraform、および GitOps ツールからセキュリティポリシーを評価および構築できるようにします。

「Cisco Cloud Application Security を導入することで、クラウド アプリケーション エコシステムのセキュリティ態勢が大幅に強化されました。このプラットフォームをテスト環境と生産環境に統合することで、アプリケーションの展開プロセスを加速し、大きな競争力を得ることができました。」

– 金融サービス会社

Cloud Application Security のライセンスオプション

Cloud Application Security ソリューションは、スタンドアロン ソリューションとして、または Cisco Cloud Protection Suite の一部として使用できます。

- **Cloud Application Security ソリューション：**スタンドアロン ソリューションとして、単一のセキュリティ プラットフォームで DevSecOps のベストプラクティスを実現し、クラウドアプリケーションを開発からランタイムまで保護します。サブスクリプションには、仮想マシン（VM）、API、Kubernetes クラスタ、サーバーレス環境、およびデベロッパーのコーディング環境の包括的な保護が含まれています。これにより、デベロッパーは脆弱性を迅速に修正しながら、セキュリティチームがコンプライアンスを測定し、結果に優先順位を付ける能力を強化できます。
- **Cisco Cloud Protection Suite：**目的別にキュレーションされたセキュリティソリューションのグループで、複数のクラウドインフラストラクチャの採用や、従来のアプリケーションからクラウドアプリケーションへの移行に伴い、セキュリティ上の重大な課題が生じることが多いデジタル化のプロセスを通じて組織が移行する際に生じる特定のセキュリティ上の懸念事項に対処します。

注文情報

登録方法については、シスコパートナーまたはシスコ販売代理店にお問い合わせください。Partner Locator ツールを使用すると、お住まいの地域のパートナーを容易に検索できます。パートナーまたはシスコ販売代理店は、初期発注後のサブスクリプションの変更を支援することもできます。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、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。

Cloud Application Security の詳細

Cisco Cloud Application Security ソリューションが、クラウドアプリケーションとその基盤となるインフラストラクチャを保護するための包括的で導入しやすいソリューションを提供する方法の詳細については、シスコの営業担当者にお問い合わせいただくか、Cloud Application Security の Web ページを参照してください。

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 C78-4153002-00 04/24