

Cisco Secure Cloud Web Application Firewall (WAF) サービスプラン

2023 年 11 月

目次

1. はじめに	3
2. サービスプラン	3
2.1 Essentials プラン	3
2.2 Advantage プラン	3
2.3 Premier プラン	4
2.4 Web DDoS 保護	4
2.5 サポートおよび Premier/Enhanced サポート	5

1. はじめに

- Cisco® Secure Cloud Web Application Firewall (WAF) は、Radware のクラウド WAF サービスに基づく Cisco Secure OEM ソリューションであり、完全に管理されたクラウドベースの Web アプリケーション ファイアウォール サービスを提供します。
- このサービスは、Web アプリケーションベースの攻撃から完全に保護するもので、Radware の AppWall¹ と、レイヤ 7 の分散型サービス拒否攻撃 (DDoS) 保護用の Radware DefensePro で構成される Radware の攻撃緩和ソリューションに基づいています。¹
- 完全に管理された Cloud WAF サービスはセットアップが簡単で、ユーザーがソフトウェアをダウンロードまたは設定する必要はありません。
- お客様は、クラウド WAF サービスにオンボーディングすることで、Web アプリケーション、モバイルアプリケーション、および API エンドポイントを完全に保護できます。オンボーディングプロセスには、アプリケーション情報と証明書の追加、保護機能の有効化、およびトラフィックを Cloud WAF サービスにリダイレクトするための DNS レコードの編集が含まれます。
- Secure Cloud WAF は、一般的な Web 攻撃と高度な Web 攻撃の両方、および DDoS 攻撃を包括的にカバーします。

2. サービスプラン

Secure Cloud WAF Protection は、お客様のすべての要件を満たすように設計された 3 つのサービスプランで利用できます。また、各サービスプランは、さまざまなサイバーセキュリティのニーズとリスクに対応し、お客様のニーズを満たすレベルのマネージドサービスを提供するように設計されています。

2.1 Essentials プラン

Essentials プランは、アプリケーションの業界ベンチマーク保護を提供するエン트리レベルのパッケージです。Essentials には、Cloud WAF 保護、API 保護、ゼロデイ攻撃保護、1 Gbps のネットワーク DDoS 保護、標準サポート、優れた SLA が含まれます。

2.2 Advantage プラン

Advantage プランは、高度で未知の攻撃からの保護を必要とするお客様に高度な保護を提供することで、アプリケーションのセキュリティを次のレベルに引き上げます。Essentials に含まれる機能に加えて、Advantage プランではポジティブセキュリティ モデル エンジンを利用して、より巧妙な未知の攻撃やゼロデイ攻撃から保護する Advanced WAF (表 1 を参照) が提供されます。Advantage には、10 Gbps のネットワーク DDoS 保護、JavaScript サプライチェーンのマッピング、モニタリング、およびクライアント側保護のための攻撃検出も含まれています。

さらに、Advantage にはインテリジェンスフィードである ERT² Active Attackers Feed (EAAF) が含まれており、既知の悪意のあるアクティブデバイスを自動的にブロックします。また、Advantage パッケージに含まれるオンボーディングサポートと継続的なポリシーレビューも利用できます。

¹ AppWall および DefensePro は Radware, Inc. の登録商標です。

² Radware Emergency Response Team (ERT)

2.3 Premier プラン

Premier プランは、アプリケーション環境全体に包括的なセキュリティを提供します。Essentials プランと Advantage プランのすべての機能に加えて、Premier プランには、動作ベースのマルチレイヤ検出と緩和、自動化された API 検出と API セキュリティポリシー生成、クライアント側保護の適用、リアルタイム自動 Web DDoS 保護を備えた高度なボットマネージャが含まれています。

2.4 Web DDoS 保護

DDoS 攻撃が進化し続けるにつれて、従来のネットワークレイヤ 3、レイヤ 4、または単純なレイヤ 7 の検出および緩和ソリューションでは検出できない、より高度な新しいタイプの DDoS 攻撃が開発されています。Web DDoS Tsunami 攻撃として知られる新しい Web DDoS 攻撃は、トラフィックパターンが非常に似ているため、従来の DDoS および WAF ソリューションによって正当なトラフィックと誤解されることがよくあります。

Web DDoS 攻撃は、アプリケーションの最大 1 秒あたりの要求数 (RPS) キャパシティを増やし、アプリケーションを正当なトラフィックに対して使用できなくすることで、システムのリソースを簡単に過負荷にすることができます。Web DDoS Tsunami 攻撃を検知するためには、トラフィックを解読する必要があり、特許を取得した新しい機械学習ベースの行動分析によってデータを解析し、悪意のあるトラフィックから有効なトラフィックを正確に識別し、アプリケーションの可用性を確保する必要があります。

表 1. Secure Cloud WAF サービスプラン

機能	Essentials	Advantage	Premier
WAF	●	●	●
API 保護	●	●	●
高度なルール	●	●	●
レート制限 (Rate Limit)	●	●	●
アクセス制御と IP Geo ルール	●	●	●
レポートと分析	●	●	●
DDoS 保護	1 Gbps	10 Gbps	10 Gbps
Standard サポート	●	●	●
Advanced サポート		●	●
高度な WAF		●	●
ERT Active Attackers Feed (EAAF)		●	●
クライアント側の保護：検出		●	●
クライアント側の保護：緩和			●
API ディスカバリ			●
ボットマネージャ			●
Web DDoS 保護			●

機能	Essentials	Advantage	Premier
データ保持 (Data Retention)	30 日間	60 日間	90 日間
無制限の DDoS	アドオン	アドオン	アドオン
CDN	アドオン	アドオン	アドオン
プレミアムサポート	アドオン	アドオン	アドオン

2.5 サポートおよび Premier/Enhanced サポート

Enhanced サポートはすべての CWAF サービスで利用でき、優先サポートを提供するホワイトグローブサービスと、ポリシーレビューと攻撃後の分析に関する定期的な更新を提供する専用のカスタマー サービス マネージャを提供します。Enhanced サポートは、お客様の組織内でスキルを使用できない場合に、WAF 管理、高度なポリシー作成、およびインシデントフォレンジックの専門的なサポートを必要とする組織に強く推奨されます。

デフォルトでは、Essentials を注文したお客様には Standard サポートが提供されます。Advantage または Premier を注文したお客様には、Advanced サポートが提供されます。サポートレベルを次の表に示します。

表 2. サポートマトリックス

カテゴリ	リスク/影響ベースの優先度	Standard サポート	Advanced サポート	Enhanced サポート
応答 SLA	P1 (電話)	40 分	30 分	10 分
	P1 (チケット)	3 Hours	2 時間	1 時間
	P2	6 Hours	4 時間	2 時間
	P3	16 時間	12 時間	4 時間
	P4	24 時間	24 時間	12 時間
チケットの更新	P1	48 時間	48 時間	24 時間
	P2	96 時間	72 時間	48 時間
	P3	120 時間	96 時間	72 時間
	P4	144 時間	120 時間	96 時間
マネージド サービス	証明書の管理と通知	非対応	対応	対応
	オンボーディングとポリシーの確認	非対応	対応	対応
	攻撃後分析	非対応	対応	対応
	四半期ごとのプレミアムセキュリティレポート	非対応	非対応	対応
	セキュリティ コンフィグ レビュー	非対応	6 ヶ月	3 ヶ月

カテゴリ	リスク/影響ベースの優先度	Standard サポート	Advanced サポート	Enhanced サポート
	拡張モニタリング	非対応	上位5つのアプリケーションでの外部モニタリング	すべてのアプリケーションでの外部モニタリング

シスコは、Radware とのグローバルな OEM パートナーシップを通じて、すべてのお客様のニーズを満たすように設計された、業界をリードするネットワークおよびアプリケーション保護ソリューションを提供しています。

Cisco Secure WAF と Bot Protection の詳細については、www.cisco.com/go/secure-waf を参照してください。詳細については、今すぐシスコにお問い合わせください。

シスコのアプリケーション セキュリティ ソリューションの詳細については、www.cisco.com/go/secure-waf 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。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)