F5® Distributed Cloud Web Application Firewall

Managed Service

オンプレミスまたはクラウドのどちらのアプリケーションを保護する場合でも、F5 Distributed Cloud Web Application Firewall（WAF）Managed Service は、市場をリードするアプリケーションセキュリティを提供し、かつ、セキュリティオペレーションセンター（SOC）の認定エキスパートによる導入、および保守サービスで、社内リソースを増強し、運用コストを削減できます。

主な利点

OWASP アプリケーションセキュリティ
アプリケーションレイヤーへの攻撃からアプリケーションを保護し、各ポリシーを現在の脅威の状況に適応させます。

簡単な導入
F5 のセキュリティ専門家によるサポートによりアプリケーションをオンボーディングすることで、保護までの時間を短縮します。

SaaS 型、グローバルに利用可能、ビジネスへの影響も最小限
F5 グローバルネットワークおよび SOC アナリストを活用して、継続的なアプリケーションセキュリティと可用性を保持できます。

手頃な価格の参入および所有コスト
SaaS 型 の Managed Service F5 Distributed Cloud Services を 利用することで、必要なサービスを手頃な価格で取得して、総所有コストを最適化できます。

スタッフ増強、常時対応の WAF エキスパート、知識集約
お客様の社内チームは、F5 のセキュリティ専門家と協力することで、24x7 体制でサポートされ、F5 Security Incident Response Team（F5 SIRT）から脆弱性に関する最新情報を入手できます。

高可用性、専用プロキシ、トラフィックステアリング、ヘルスモニタリング
F5 のグローバルネットワークは、99.99% のアップタイム SLA、専用ロードバランサー、トラフィックシェーピング、継続的なバックエンドでのヘルスモニタリングと可用性監視を提供します。

DDoS 攻撃緩和
Managed WAF サービスには、最大 1.5Gpbs 規模の攻撃に対応できる DDoS 攻撃緩和が含まれています。また、容量増加のサブスクリプションもご利用可能です。

F5 Distributed Cloud Web Application Firewall（WAF）は、一般的な自動化されたアプリケーション固有のセキュリティ脅威を検出および軽減する SaaS 型の Managed Service です。Managed WAF Service は、Web アプリケーションやデータに接する組織のインターネットを保護して、PCI DSS などの業界セキュリティ標準への準拠を施行します。このサービスは、F5 のグローバルなセキュリティオペレーションセンター（SOC）が 24x7 体制で高度な専門知識を有するアプリケーションセキュリティの専門家によりサポートされます。この Managed WAF Service は、22 のメトロマーケットにある 23 のリージョナルエッジ（RE）を持つグローバルネットワークを通じて提供されます。現在の RE のリストと可用性については、F5 Distributed Cloud Status をご覧ください。

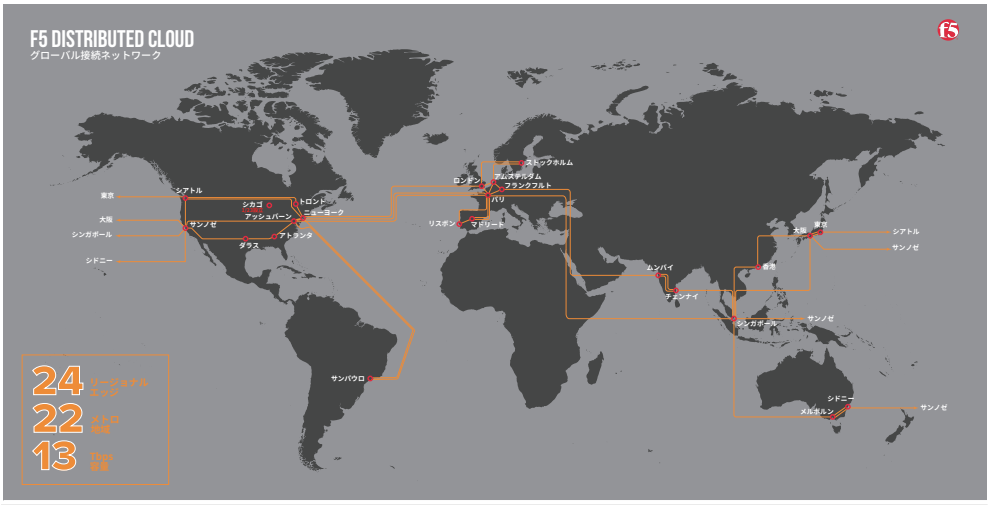

図 1：F5 Distributed Cloud のネットワーク

Managed Web Application Firewall

アプリケーションポートフォリオ全体に共通するマネージドセキュリティおよびパフォーマンスのポリシーを確立し、データ漏洩のリスクを軽減し、顧客体験を向上します

Web Application Firewall（WAF）ポリシーは、アプリケーションのオリジンへのアクセスをブロックまたは許可する必要があるトラフィックを決めるルール（または「ブロックモジュール」）のセットです。F5 SOC は、お客様と協力して、1 つ以上のアプリケーションを保護するために導入される特別な WAF セキュリティポリシーを作成および調整します。Managed WAF Service は、サービス拒否（DOS）などのネットワークレイヤー攻撃のリスクだけでなく、SQL インジェクション、クロスサイトスクリプティング、クロスサイトリクエストフォージェリ、悪意のあるボットトラフィックやその他のお客様のアプリケーション固有の脅威などのアプリケーション攻撃のリスクも緩和します。

F5 Distributed Cloud WAF Managed Service は、技術とソースを組み合わせて、悪意のあるトラフィックかどうか判別します。F5 Threat Labs や SOC のエンジニアにより保守される攻撃シグネチャセットは、既知の脅威をブロックするだけでなく、HTTP ヘッダー、パケットペイロードおよびその

F5 は、アプリケーション配信、および、セキュリティサービスのサービスカタログを提供いたします。このカタログは、専門家が保守しますが、SOC と協力して簡単に変更することができます。

他のお客様固有のリクエストパラメータに基づいてカスタムルールを定義および施行します。

以下に、構成に利用できる包括的な機能ライブラリのサンプルリストを示します。

- IP 拒否 / 許可リスト
- 高速アクセス制御リスト (ACL)
- ユーザー行動分析（WAF イベント / ログイン失敗 /L7 ポリシー拒否）
- WAF ポリシー管理
- サービスポリシー
- IP レピュテーション
- 脅威キャンペーン

F5 SOC のエンジニアは、お客様と協力してアプリケーションごとにどの機能を設定しプロビジョニングするかを決定します。Managed WAF Service は、正規トラフィックと悪意のあるトラフィックの両方を可視化しながら、アプリケーションソースコードを変更またはパッチ適用する必要なく、アプリケーションに仮想パッチを適用することで、攻撃を緩和します。

WAF Managed Service の構成要素

F5 Distributed Cloud Services を利用することで、アプリケーション境界の完全なセキュリティ管理を提供し、クライアントとの信頼関係を継続できます。

サブスクリプション

F5 Distributed Cloud WAF Managed Service は、1 年、2 年または 3 年契約のサブスクリプションを選択いただけます。サブスクリプションの合計コストは、導入する**ロードバランサー**の数と、ご希望の **Managed Service のカテゴリ（標準または拡張）**の2つの主要な要素を計算して決まります。

DDoS Protection

F5 Distributed Cloud プラットフォームは、ボリューム型攻撃の自動緩和機能や、レイヤー 3 ～ 4 のプロトコル攻撃やレイヤー 7 の特にアプリケーションを標的とした攻撃を防御する機能など、包括的な DDoS 防御を提供します。F5 Distributed Cloud WAF Managed Service には、回数無制限の攻撃に対する DDoS 保護が含まれています。

役割と責任

F5 Distributed Cloud WAF Managed Service には、F5 SOC のエンジニアによる WAF ポリシーの作成と保守が含まれます。お客様は、SOC のエンジニアによるポリシーの作成と保守の参考となるように、アプリケーションおよび Web サーバーテクノロジーの初期情報を提供する必要があります。

また、トラフィックが F5 ネットワークの F5 Distributed Cloud Services プラットフォームに送信（DNS 解決）されるようにルーティング構成を変更する必要もあります。

F5 Distributed Cloud Managed Services

Standard サービス
インシデントリクエストを介してオンボーディングのサポートや導入後のサポートを 15 分以内に提供します。

Enhanced サービス
セキュリティリスク、サイバー攻撃、修正アクティビティの可視化を強化し、優先順位付けされた個別のコンサルティング技術エンジニアリングサポートにより、迅速なトリアージと構成更新を実現します。

セキュリティとコンプライアンス体制を強化し、全体的な運用リスク要因を軽減します。

お客様のチームは、カスタムレポートを通じて、適切に関連付けられたデータに基づく実用的な修正により、WAF の脅威が阻止され、ポリシーの進化中における潜在的な WAF の脆弱性の特定と迅速なブロックが改善できていることを確認できます。また、データはさらになる法的措置のために法執行機関に提供されることもあります。

アナリストは、ポリシーがブロッキングモードに移行される前と後に、アプリケーションの脆弱性スキャンを実行します。

カスタマーサービスオンボーディング

F5 SOC は、最初の電話会議のスケジュールを決めて、アプリケーション設定、ポリシー導入（SSL 証明書アップロードを含む）、「モニタリングからブロッキング」への移行、および WAF ポリシー作成のためのアプリケーションとインフラストラクチャのアーキテクチャについて確認します。 F5 SOC は、Distributed Cloud プラットフォームへのトラフィックルーティングが開始された後で、必要に応じて電話で確認する場合もあります。

初回のオンボーディング会議では、以下のオポチュニティが提供されます。

- 導入成功までのステップを確認する
- F5 Distributed Cloud コンソールの概要を知る
- ロールベースのアクセス制御および管理のベストプラクティスを理解する
- 保護するアプリケーションを定義およびプロビジョニングする
- SSL アセットを導入および保護して、セキュリティプロファイルを定義する
- WAF 技術アンケート調査を実施する
- Managed Services としての WAF 運用の詳細について話し合う
- 保護のためのポリシー要素および機能について説明する
- 協力して必要なポリシー機能を定義する
- ラーニングおよびブロッキングフェーズの実行可能な項目に同意する（WAF ベストプラクティス）

導入

実装の成功は、お客様と F5 SOC の強力な関係の結果です。SOC は、シームレスな体験により保護機能を最大限活用できるようにプロセス全体でお客様をサポートします。ポリシー保護は一般的に以下のステップで実施されます。

- F5 SOC が、WAF ポリシーを作成して、そのポリシーがお客様により提供されるアプリケーション情報に基づいてアプリケーションに関連付けられるまで待ちます。
- お客様がコンソールまたは API を介してアプリケーション構成を作成します。
- お客様がコンソールまたは API を介してアプリケーションを Distributed Cloud プラットフォームに導入します。
- SOC がアプリケーション構成を完成させ、すべてが正しく機能することを確認します。

お客様は、F5 SOC との電話会議をオプションでスケジュールし、構成を確認し、Distributed Cloud プラットフォームへのルーティング変更をコミットできます。

主な利点

堅牢な攻撃シグネチャエンジン
Distributed Cloud WAF のシグネチャエンジンには、CVE だけでなく、F5 Labs が特定した既知の脆弱性や攻撃手法に対する 7,000 以上のシグネチャが含まれています。

脅威キャンペーン
F5 の脅威研究者によって開発された完全に検証された攻撃キャンペーンシグネチャにより、高度なマルチベクトル攻撃キャンペーンに対する保護を提供します。

高度なビヘイビアエンジン
WAF ルールのヒット数、禁止されたアクセス試行、ログイン失敗、エラー率などについて、他との比較により、クライアントのインタラクションが分析されます。

強力なサービスポリシーエンジン
さまざまなパラメータに基づいた許可/拒否リストの開発やお客様ルールの作成により受信リクエストに対応し、マイクロセグメンテーションを実現して、アプリケーションレイヤーでの高度なセキュリティのサポートを提供します。

IP レピュテーションサービス
既知の悪意のある IP アドレスに関する F5 のデータベースによって裏付けられた脅威カテゴリまたは脅威スコアに基づいて、IP アドレスを簡単に許可または拒否できます。

レポーティングと分析
アプリケーションの導入、健全性、パフォーマンスや、違反、攻撃アクティビティ、ソース、パスなどに関する詳細なリアルタイム情報のきめ細かいステータスを含む、すべてのアプリケーションのパフォーマンスとセキュリティに関する 360 度のビューを提供します。

WAF ポリシーの学習と構築

WAF のセキュリティポリシーは、F5 SOC が以下の 1 つ以上を使用して作成します。

- 保護対象となる特定のアプリケーションフレームワークに関連する既知の脆弱性に対して事前に設定されたベースラインセキュリティテンプレート
- サードパーティの WAF 脆弱性評価に関連する出力またはスキャン出力
- 他のベンダーの既存のポリシー

ポリシーの導入および調整タスクには、以下の脆弱性緩和の一部またはすべてが含まれる場合があり、これらは、F5 SOC とお客様との合意により実施される可能性があります。

許可 HTTP メソッドの設定
許可 HTTP レスポンスコードの設定
拒否ファイルタイプの設定
攻撃シグネチャの設定
お客様の要件に基づき関連する攻撃シグネチャを設定します
お客様の環境に合わせてアーキテクチャベースの攻撃シグネチャを調整します
明示的なエンティティの設定
URL
パラメータ
セッションとログインの設定
（モジュールを有効にする前に通知が必要かどうかお客様と確認します）
ログオンページを構成します
ログインページに基づいたセッションアウェアネスの有効化
ヘッダーの設定
Cookie 実施
リダイレクションドメイン
オンボーディング電話会議時に同意した追加 WAF ポリシー機能の有効化
ブロック応答ページの設定

F5 SOC がポリシーとロードバランサーを関連付け、ラーニングフェーズを開始します。 SOC のエンジニアがお客様と協力してポリシーを調整します。ポリシー導入後、お客様と SOC が協力して違反確認および継続的な調整を行う場合があります。SOC のエンジニアがお客様独自の環境に合ったベストプラクティスを提案します。

移行、ポリシー調整、ログデータからの違反特定、偽陽性や偽陰性、追加ポリシーの構築や調整において生じたあらゆる問題について、メールまたは電話により F5 SOC に連絡して協力を依頼できます。また、F5 SOC がシステムのパラメータの調整や変更が必要となる問題を指摘する場合もあります。SOC は、必要に応じて参加を求めるサービスリクエストを通じ、お客様との連絡を開始いたします。

WAF 違反ブロックおよび施行

モニタリングフェーズのポリシー調整が完了すると、F5 SOC は、ポリシーをブロッキングモードに移行するための電話会議を設定します。お客様は、ポリシーをブロッキングモードに進めるか、そこから戻すかをいつでも選択できます。通常、1 フェーズまたは積極的な導入実装が選ばれますが、ポリシーの追加調整が必要な場合は、いくつかのステップによりポリシー導入まで漸進的かつ規律に従った方法で進める段階的実装が選ばれる場合もあります。

オンボーディング会議ではお客様は次のことが可能になります。

- ポリシーライフサイクルで使用される開発方法の理解
- 違反および攻撃タイプを是正するための SOC との協力方法を確立
- 必要に応じて、アプリケーションセキュリティのベストプラクティスの合同検証を協力して実施する
- Web アプリケーションの「ミッションクリティカル」なセクションを確認する
- システムの機能と防御に関するデフォルト設定とカスタマイズされた設定を確認する
- ポリシー導入を段階的または積極的に実施するか決定する
- ポリシー実施を始めるための一時的なメンテナンス期間を設定する

ポリシーの調整は、お客様または SOC が初期導入の追加調整の必要がないと判断するまで続く場合があります。

F5 SOC は、各導入フェーズのインシデントやポリシー状態の変化を追跡して最新情報を提供します。また、監査レポートを確認することで、ポリシーで実施された任意の措置を可視化できます。以下の場合は SOC と協力してメンテナンス期間を予定しておくことをお勧めします。

ブロッキングモードを有効にする
偽陰性と偽陽性を監視し、必要に応じてポリシーを調整する

2022 年版アプリケーション戦略の状況レポートはこちらからダウンロードしてご覧ください

ポリシー保守

F5 は、すべてのお客様のために継続的なポリシー保守を行います。

F5 SOC は、新しい観測結果があった場合はサポート / エスカレーションインシデントリクエストを介して通知します。お客様は、ポリシー調整の支援を SOC に直接依頼することもできます。F5 SOC は、問題を調査して、最善策を決定いたします。

攻撃シグネチャの保守 / 新たな脅威

F5 Distributed Cloud により提供されるアプリケーション保護は、ツールセットの組み合わせにより提供されます。これらのツールは、アプリケーション攻撃パターンシグネチャ、ボット特定シグネチャ、L7（アプリケーションレイヤー）サービス拒否（DoS）パターンなどを活用します。F5 SOC はお客様に代わりプラットフォーム全体でシグネチャを継続的に更新します。お客様は、F5 SOC と協力してポリシーを調整することもできます。この Managed Services は、お客様のアプリケーションが常に保護され、利用可能であることを保証する継続的な保護サービスを提供いたします。

参考情報 / 参考動画

以下のWebリンクより、WAFアプリケーションの推奨プラクティスに関する基本情報や、F5 Distributed Cloud Servicesでご使用可能ないくつかの機能を紹介するビデオをご利用いただけます。

F5 Distributed Cloud Web Application Firewall

F5 Distributed Cloud Simulator でのマルチクラウド環境の構成

F5 Distributed Cloud によるレイヤー 7 コネクティビティ

F5 Distributed Cloud Services によるアプリ配信とセキュリティの最適化

新しい脅威は常に発見され続けており、新しい脆弱性から保護するためには、ポリシーを迅速に更新する必要があります。F5 SOC およびエンジニアリングチームは、F5 Security Incident Response Team (F5 SIRT) と協力して、これらの脅威に対応するための保護フレームワークを開発および実装します。これらは、F5 Distributed Cloud プラットフォーム内で、ポリシーに追加対策や他の攻撃緩和技術を追加することにより、新しいサービスポリシーとして導入できます。

可視化

F5 Distributed Cloud WAF Managed Services のサービス管理コンソールでは、構成を修正および更新できます。また、強化されたネットワークとセキュリティレポートにより、運用の詳細が可視化されます。

このコンソールは、WAF 違反（セキュリティイベント）、脅威キャンペーン、DDoS 攻撃アクティビティ、上位の攻撃ソース、攻撃パスなどの詳細なリアルタイム情報を提供します。コンソールのユーザーおよび管理者は、ユーザー情報 / 役割に基づいて関連情報を表示するカスタムダッシュボードを作成できます。

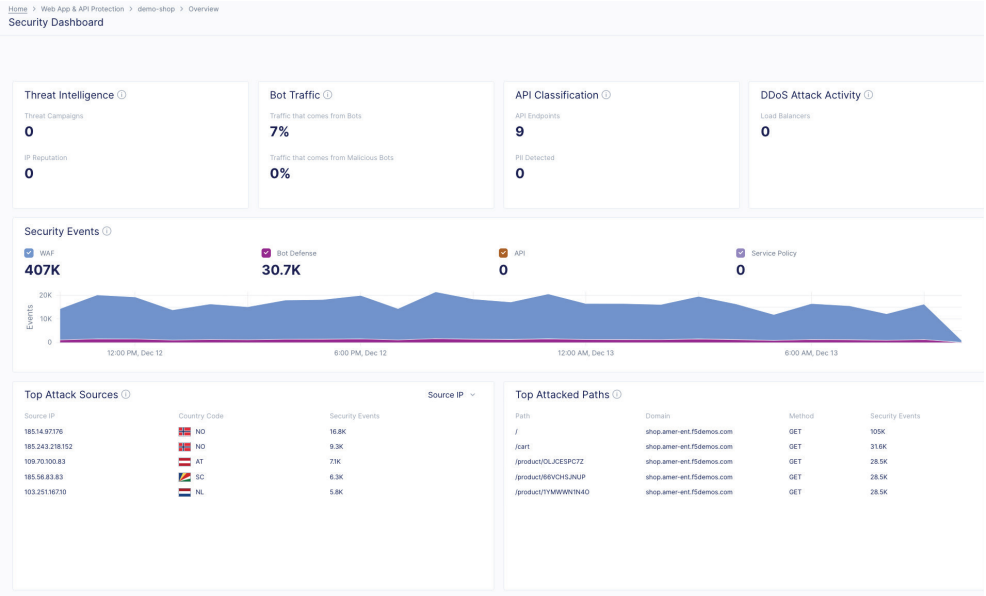

図 2：F5 Distributed Cloud 管理コンソール

自動化

F5 Distributed Cloud Services RESTful API を使用することで、新しいロードバランサーの作成、拒否リスト IP アドレスの更新、SSL 属性の設定などのタスクを、プログラムを使用して完了できます。API の詳細については、こちらをご覧ください。

脅威キャンペーン

脅威キャンペーンシグネチャは、最新の脆弱性を悪用する現在の「野生」の攻撃、または古い脆弱性を悪用する新しい攻撃方法に基づいています。脅威キャンペーンシグネチャには、攻撃の性質

と目的に関するコンテキスト情報が含まれています。F5 Distributed Cloud では、SOC と協力して、脅威キャンペーンを管理し、シグネチャを選んで適用して最も重要なアプリケーションを保護できます。

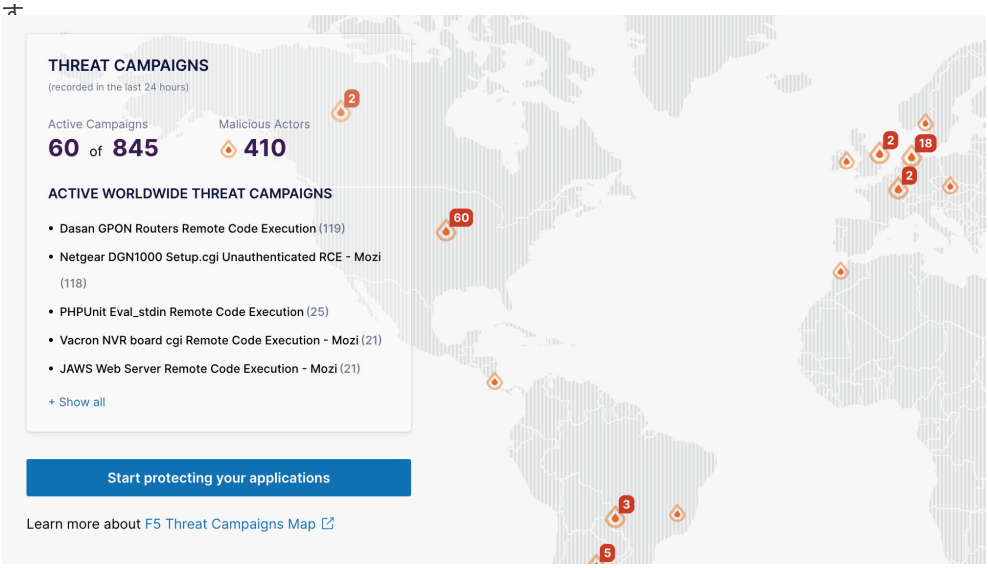

図 3：脅威キャンペーンの状況と現在の脅威

システムログ統合

ログ収集システムと接するインターネットに対し、WAF 違反データをリアルタイムで安全に送信して詳しく調査できます。F5 Distributed Cloud プラットフォームのロギング API により、アプリケーションがクラウド、オンプレミスまたはその両方にあっても、すべてのセキュリティイベントを一括表示できます。

システムステータス

F5 Distributed Cloud Service 運用に関するリアルタイムのステータス情報は、こちらのリンクからご利用できます。F5 は、通常保守作業に関する通知を、遅くても 15 営業日前までにご提供します。しかし、F5 は緊急保守をいつでも実施する権利を有します。サービス提供的にとして、緊急保守の通知は、保守作業の前に提供されます。

WAF Managed Service 階層

以下の表は、SOC が各サービス階層のサブスクリプションの一部としてどの Managed Service を提供するかを示しています。このリストは、最も一般的に要求されるタスクを表しています。お客様は、F5 アカウントチームに連絡して、このリストに含まれない追加のサービスを要求することができます。

サービス	標準	拡張
LB の設定、構成、トラブルシューティング	✓	✓
WAF ポリシーの評価と調整	✓	✓
L7 DoS の設定と調整	✓	✓
IP レピュテーション、脅威キャンペーンの設定	✓	✓
TLS 証明書のアップロードと更新	✓	✓
LetsEncrypt を使用した Autocert の設定	✓	✓
TLS ハンドシェイク問題のトラブルシューティング	✓	✓
ルーティングと遅延の問題のトラブルシューティング	✓	✓
標準サービスポリシーの設定	✓	✓
WAF の許可リスト / 拒否リストの設定	✓	✓
DNS 権威レコード変更の支援	✓	✓
コンソールでのユーザー管理	✓	✓
API トークン生成	✓	✓
SSO 設定	✓	✓
リモートログ設定	✓	✓
任命テクニカルアカウントマネージャー		✓
エスカレーション管理		✓
PIR/RCA レポート		✓
定期的な脆弱性スキャンとレポート		✓
サードパーティツールとの API 統合		✓
定期的な詳細ポリシーレビュー		✓
プロジェクト管理		✓
サービスポリシー作成の支援		✓
ビジネスレビュー	半年ごと	四半期ごと
ソリューション設計		✓
セキュリティレビュー		✓
製品トレーニング		✓
技術コンサルティング		✓

表 1：WAF Managed Service 階層

まとめ

WAF は、強力なセキュリティ対策の基礎的要素です。F5 Distributed Cloud WAF Managed Service は、悪意のあるアクターに対する保護および防御を提供します。組織は、このサービスを利用して、トラフィックがオリジンサーバーに到達する前にトラフィックフローを制御および監視できます。お客様は、ポリシーをすぐに導入して、トラフィックを検査し、ビジネス運営に悪影響を及ぼす可能性がある悪意のあるリクエストをブロックできるので、セキュリティ強化を瞬時に実感いただけます。

詳しくは、F5 の担当者または F5 の販売担当員にお問い合わせください。

DC 02.2023 | JOB-CODE-123456789