Cisco AMP Threat Grid - アプライアンス

Cisco® Advanced Malware Protection（AMP）Threat Grid アプライアンスは、マルウェア分析およびコンテキストリッチ インテリジェンスという 2 つの優れたマルウェア対策ソリューションを組み合わせた製品です。その機能により、セキュリティに携わるプロフェッショナルは、サイバー攻撃に対してプロアクティブに防御し、攻撃時に迅速に回復できます。

製品概要

AMP 脅威グリッド アプライアンスは、詳細な脅威分析とコンテンツによるオンプレミスの高度なマルウェア分析を実現します。コンプライアンスおよびポリシーの制約がある組織は、サンプルをアプライアンスに送信することでマルウェアをローカルで分析することができます。

AMP Threat Grid アプライアンスでは、高度にセキュアな独自の静的および動的分析テクニックを使用してすべてのサンプルを分析できます。数億もの他の分析済みマルウェア アーティファクトの履歴およびグローバル コンテキストから抽出した侵入兆候に基づいて分析結果を関連付け、マルウェア攻撃、キャンペーン、およびその配布状況をグローバルで把握できるようにします。これは、高度なマルウェアからの標的型攻撃と脅威の両方に対して効果的に防御するのに役立ちます。AMP 脅威グリッドによる、重要な動作インジケータの特定や脅威スコアの割り当てなどの詳細なレポートを通じて、迅速に優先付けし、高度な攻撃から回復することができます。

機能と利点

AMP 脅威グリッド アプライアンスの機能と利点を表 1 に示します。

表 1. 機能と利点

機能	利点
Glovebox	ユーザ操作ツール。ネットワークが感染するリスクなくマルウェアを分析できる安全な環境を提供。アプライアンスに組み込まれているため、アナリストは、アプリケーションの起動やダイアログボックスのクリック、必要な場合は仮想マシンの再起動などを含め、分析中にサンプルを操作することが可能。
オンプレミス アプライアンス	安全性の高いオンプレミスでの静的/動的マルウェア分析によって、データの機密性を維持。既存のセキュリティ インフラストラクチャと簡単に統合。マルウェア分析結果の安全なオンプレミスのストレージを提供。
高度な分析	マルウェアの動作に関する包括的なセキュリティ情報を把握し、サンプル ソースと AMP 脅威グリッドの広範なデータベース内の関連する動作への直接リンクを提供。すべての情報、および詳細な調査のための分析結果に簡単にアクセスできる機能を提供。
高度な侵入兆候	700 を超える、非常に精度が高く、実用的で高度な侵入兆候を低い誤検出率で分析。多数のマルウェア ファミリおよび悪意のある動作にわたる高度な静的および動的分析によって包括的な指標を生成。脅威に関する最も広範なコンテキストを提供し、信頼性のある判断を迅速に下せるようにサポート。
脅威スコア	見つかった動作の確信度と重大度、履歴データ、頻度、クラスタリング インジケータ、サンプルを考慮する独自のアルゴリズムと分析によって自動的に脅威スコアを提供。確信を持って脅威を優先順位付けし、悪意のある動作の各サンプルのレベルを反映。脅威の優先順位付けが改善されるため、マルウェア アナリスト、インシデント対応担当者、セキュリティ エンジニアリング チームの効率、および AMP Threat Grid フィードを使用する製品の精度が向上。
リモート更新	論理境界内のすべての情報を維持するために、企業ポリシーや規制に関するポリシーを遵守しながら最新のナレッジ ベースに手動で更新する機能。
統合用 API	既存のセキュリティとネットワーク インフラストラクチャによる脅威インテリジェンスの迅速な運用を簡素化。AMP 脅威グリッドの Representational State Transfer（REST）API により統合を迅速かつ簡単に実現。多数のサードパーティ製品向けの統合ガイドを提供（ゲートウェイ、プロキシ、セキュリティ情報およびイベント管理（SIEM）プラットフォームを含む）。

包括的なオンプレミスのマルウェア分析

クラウドにマルウェアのサンプルを送信する際にコンプライアンスおよびポリシーの制限に直面する組織に対して、AMP 脅威グリッドは、そのフェデレーテッド脅威インテリジェンスのフルパワーでサポートされるローカル マルウェア分析専用のアプライアンスを提供します。AMP 脅威グリッドは、マルウェア攻撃、キャンペーン、およびその配布状況をグローバルに把握できるようにします。毎月何百万ものサンプルを分析し、何テラバイトものマルウェア分析を内容が豊富で実用的なインテリジェンスに抽出します。

セキュリティ チームは見つかったアクティビティおよび特性の 1 つのマルウェア サンプルを、他の何百万ものサンプルにすぐに関連づけて、履歴およびグローバル コンテキストの中でその動作を完全に理解し、高度なマルウェアからの標的型攻撃と脅威の両方に対して効果的に防御することができます。AMP 脅威グリッドの詳細なレポートは、脅威スコアとともに主要な動作インジケータを特定し、迅速な優先順位付けおよび高度な攻撃からのリカバリを、精度と速度を保ちながら行えるようにします。以下の分析機能があります。

- マルウェアの動作について完全に理解できるようにする動的および静的分析エンジン
- ネットワーク トラフィックを含む、すべてのマルウェアのサンプル アクティビティの詳細な分析レポート
- セキュリティ オペレーション センター（SOC）アナリスト、マルウェア アナリスト、調査スタッフ向けに設計されたユーザ インターフェイス ワークフロー

ライセンス

AMP Threat Grid アプライアンスのライセンスは、表 2 に記載のとおり、1 日に分析されるファイルの最大数に基づきます。

表 2. モデルとライセンス

	Cisco AMP Threat Grid 5004	Cisco AMP Threat Grid 5504
1 日あたりの分析されるファイルの最大数	1,500	5,000

製品仕様

表 3 に製品仕様を示します。

表 3. 製品仕様

機能	Cisco AMP Threat Grid 5004	Cisco AMP Threat Grid 5504
フォーム ファクタ	1 ラック ユニット（1 RU）	1 RU
寸法	約 4.32 X 43 X 75.6 cm（1.7 X 16.9 X 29.8 インチ）（高さ X 幅 X 奥行）	約 4.32 X 43 X 75.6 cm（1.7 X 16.9 X 29.8 インチ）（高さ X 幅 X 奥行）
ネットワーク インターフェイス	1 GB 銅線 + SFP+ X 2	1 GB 銅線 + SFP+ X 2
CIMC インターフェイス	1 GB 銅線	1 GB 銅線
電源オプション	770 W AC または 1050 W DC	770 W AC または 1050 W DC

環境仕様

表 4 に環境仕様を示します。

表 4. 環境仕様

	Cisco AMP Threat Grid 5004	Cisco AMP Threat Grid 5504
温度：動作時	5 ～ 35°C（41 ～ 95°F）（動作時、高度 0 m、ファンの故障なし、CPU スロットリングなし、ターボ モード）	5 ～ 35°C（41 ～ 95°F）（動作時、高度 0 m、ファンの故障なし、CPU スロットリングなし、ターボ モード）
温度：非動作時	-40 ～ 65 °C（-40 ～ 149 °F）	-40 ～ 65 °C（-40 ～ 149 °F）
湿度：動作時	10 ～ 90 %（結露しないこと）	10 ～ 90 %（結露しないこと）
湿度：非動作時	5 ～ 93%（結露しないこと）	5 ～ 93%（結露しないこと）
高度：動作時	0 ～ 3,000 m（0 ～ 10,000 フィート）（最大周囲温度は、300m ごとに 1 °C 低下）	0 ～ 3,000 m（0 ～ 10,000 フィート）（最大周囲温度は、300m ごとに 1 °C 低下）
高度：非動作時	0 ～ 12,000 m（0 ～ 40,000 フィート）	0 ～ 12,000 m（0 ～ 40,000 フィート）

発注情報

Cisco AMP Threat Grid アプライアンスのご注文については、シスコ発注ホームページをご覧ください。表 5 に発注情報を示します。

表 5. 発注情報

製品番号	製品説明
Cisco AMP Threat Grid 5004 アプライアンスおよびサブスクリプション	
TG5004-BUN	Cisco AMP Threat Grid 5004 アプライアンスおよびサブスクリプション バンドル
TG5004-K9	Cisco AMP Threat Grid 5004 アプライアンス（ソフトウェア付属）
L-TG5004-1Y-K9	5004 モデル向け Threat Grid コンテンツ サブスクリプション ライセンス、1 年
L-TG5004-3Y-K9	5004 モデル向け Threat Grid コンテンツ サブスクリプション ライセンス、3 年
L-TG5004-5Y-K9	5004 モデル向け Threat Grid コンテンツ サブスクリプション ライセンス、5 年
Cisco AMP Threat Grid 5504 アプライアンスおよびサブスクリプション	
TG5504-BUN	Cisco AMP Threat Grid 5504 アプライアンスおよびソフトウェア バンドル
TG5504-K9	Cisco AMP Threat Grid 5504 アプライアンス（ソフトウェア付属）
L-TG5504-1Y-K9	5504 モデル向け Threat Grid コンテンツ サブスクリプション ライセンス、1 年
L-TG5504-3Y-K9	5504 モデル向け Threat Grid コンテンツ サブスクリプション ライセンス、3 年
L-TG5504-5Y-K9	5504 モデル向け Threat Grid コンテンツ サブスクリプション ライセンス、5 年

シスコとパートナーによるサービス

シスコおよびシスコ認定パートナーによるサービスでは、AMP 脅威グリッドのプレミアム脅威フィードおよび REST API との統合の計画および実装のお手伝いをします。計画および設計サービスでは、貴社の既存インストラクチャ、AMP 脅威グリッドのプレミアム フィード フォーマット、運用プロセスを調整して、高度な脅威フィードを最大限に利用できるようにします。

シスコ キャピタル

目標の達成を支援するファイナンス

Cisco Capital は、お客様が目標の達成と競争力の維持に必要なテクノロジーを導入できるよう支援します。お客様の CapEx を削減し、成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムにより、ハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に購入することができます。支払いが統一されるため、予想外の支払いが発生することもありません。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら

次のステップ

Cisco AMP Threat Grid 統合マルウェア分析および脅威分析に関する詳細については、http://www.cisco.com/web/JP/solution/security/advanced-malware-protection/index.html を参照してください。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-733667-04JA 17.06