Avira

AVIRA クラウドサンドボックスAPI

無制限の拡張と完全なプライベート

Avira クラウドサンドボックスAPIを使用すると、セキュリティベンダーおよびサービスプロバイダーは、ファイルを送信することで完全な脅威評価を含む詳細な脅威インテリジェンスレポートを受信できます。これは、セキュリティ業界で最も強力でスケーラブルなマルウェア分析サービスです。Aviraクラウドサンドボックスは、最先端のファイル分析、ディープインスペクション、受賞歴のある動的なデトネーション技術を利用して、詳細な脅威インテリジェンスを実現させます。

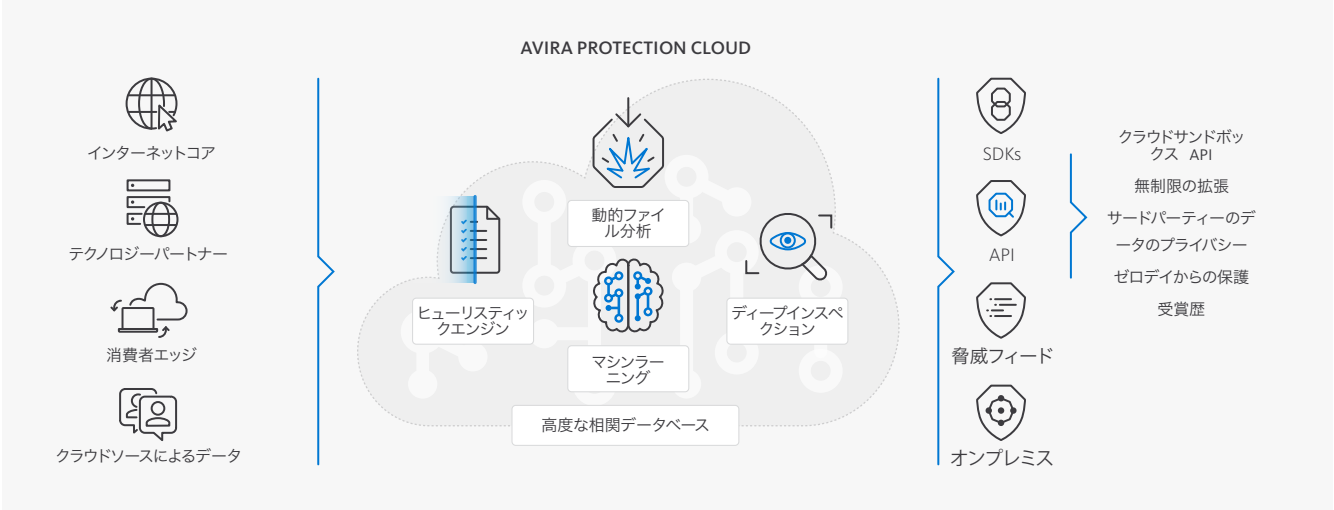
サイバーセキュリティ業界は、正確かつ詳細な脅威インテリジェンスに依存しています。このインテリジェンスは、サンドボックス(エミュレーションまたは仮想化を使用)からディープコンテンツ インスペクション、AI、マシンラーニングシステムに至る、高度なマルウェア分析システムによって作られています。ただし、このようなシステムは開発が難しく、ベテラン技術者による保守が必要であり、規模も限られています。

しかし、サイバーセキュリティベンダーは、攻撃の件数の急増と、複雑化を受け、それらからの保護に対する顧客の要求に応える必要があります。ベンダーは、拡張の制限がなく、費用対効果に対する顧客の期待に応えるだけでなく、データのプライバシーが最重要視されるさまざまな新規制へのコンプライアンスが必要となる社会の中で機能するマルウェア分析ツールにアクセスできなければなりません。

Avira のクラウドサンドボックス API:

- 効率的に拡張可能なマルウェア分析システムを提供します
- 企業の厳格なデータプライバシーの要件とEU一般データ保護規則 (GDPR) などの新規制に準じたマルウェア分析サービスを提供します
- ゼロデイ保護を保証し、 すべての疑わしいトラフィックから顧客を保護します

AVIRA PROTECTION CLOUD



Avira

AVIRA クラウドサンドボックスサービス

Avira クラウドサンドボックスは、受賞歴のある拡張が無制限の自動マルウェア分析システムです。複数の高度な分析テクノロジーを組み合わせ、アップロードされたファイルから完全な脅威インテリジェンスレポートを提供します。サンドボックスのマルウェア分析モジュールにより、脅威の発生源および挙動を可視化します。ここでは、最も詳細かつ正確な脅威インテリジェンスを作成するために使用される貴重な情報のカスケードが抽出され、展開されます。これにより、研究者はマルウェアがターゲットのシステムを破壊する方法を理解できます。クラウドサンドボックスAPIは、価値のある実用的なインテリジェンスを含む詳細なファイル固有の脅威レポートを提供します。このレポートでは、ファイルの詳細な分類、脅威に含まれる技術、戦術と手順(IoC)に関する情報、ならびに、送られたファイルがどのように・なぜ「クリーン」、「悪意のある」、または「疑わしい」と識別されたのかについて説明が提供されます。

ファイルの分析中にデトネーションレイヤーがトリガーされると、レポートに追加情報が提供されます。これは、ファイルのデトネーション中にホスト上で行われた一連の変更(外部呼び出しやレジストリの変更など)の詳細を示します。このレポートは、セキュリティチームが脅威の性質を理解するために必要な情報を提供するものです。このサービスは当初から、個人データのプライバシーと規制に対する業界全体の懸念に対処するように設計されています。結果として、GDPRコンプライアンスが組み込まれており、サイバーセキュリティが直面する主要な課題、つまりサードパ ーティの個人データの処理方法にも対処しています。これは、規模、アクセシビリティ、プライバシーに妥協せず、業界のニーズに対処する、初めての自動マルウェア分析サービスです。

無制限の拡張:

Amazon Web Services (AWS) が提供する能力を活用して、単一の企業のニーズに留まらず、セキュリティベンダーの規模とコストのニーズを満たすように設計された始めてのサンドボックスシステムです。

データのプライバシー:

Avira クラウドサンドボックスは、顧客のデータを保護するよう設計されています。サードパーティのデータのプライバシーに対する顧客の要求を満たし、GDPRコンプライアンスの要件を満たすように特別に設計されています。

ゼロデイからの保護:

このサービスは、業界で最も高度なクラウドベースの分析モジュールを使用して、未知の脅威に対する保護を提供します。

セキュアで受賞歴のある技術:

Avira の動的デトネーション技術は、Amazon Web Servicesの厳格なセキュリティ要件を満たした初めての技術です。顧客のデータはプライベートのままであり、AWSネットワークは攻撃から保護されています。

Avira

クラウドサンドボックスフレームワーク

アーキテクチャ

クラウドサンドボックスは、Avira のクラウドセキュリティシステムである Avira Protection Cloud 内で開発された技術を活用しています。Avira Protection Cloudは、Aviraのマルウェア対策および脅威インテリジェンスソリューションを支えており、OEMパートナーシップを通じて、世界有数のサイバーセキュリティベンダーの多く利用しており、結果として世界各地で約10億人の人々を保護しています。Amazon Web Services (AWS)インフ ラストラクチャ上に構築された、受賞歴のある動的デトネーション レイヤー により、時間に対する要求が厳密なパートナーからのリクエストをクラウドサンドボックスで大規模かつ迅速に管理できるようになります。サービスへのアクセスと柔軟な統合は、セキュアなRestAPIを通じて有効化されます。このシステムは、Aviraの経験豊富なサイバーセキュリティエンジニアリングチームによって設計され、常に維持されています。クラウドサンドボックスのディープインスペクションおよび動的分析システムは、進化し続ける未知の脅威に対する最高レベルの保護とパフォーマンスを提供します。

Avira

分析モジュール

Avira のクラウドサンドボックスは、フレキシブルな多層自動マルウェア分析サービスを使用し、サイバーセキュリティ業界にディープインスペクションとレポートを提供します。主なモジュールとして含まれるもの: アップロードされたファイルを評価して、初期評価を行うファイル識別レイヤー。 このレイヤーに含まれる評価およびタグ付けシステムを利用することで、動的管理システムは、ディープインスペクション、動的分析、および行動プロファイリングレイヤーとのファイルの相互作用を最適化することができます。これにより、最も正確な分析と費用対効果の高いサービスが保証されます。ディープインスペクションレイヤーは、マルウェアの挙動に対してこれまでにない可視性を提供します。これには、Avira独自の強力なヒューリスティック、NightVision™ マシンラーニングシステム、お よびファイル固有の分析 モジュールが活用されていま す。このレイヤーには、脅威の始まりの表層に留まらず、ホスト全体をシミュレートする高度なデトネーション技術も含まれています。行動分析、プロファイリング、マシンラーニングが、それまで見えなかったメモリアーティファクトと隠されたコードレイヤーに対処します。また、インテリジェントなコード変換によって回避が無効化され、ほぼリアルタイムの分類が可能となります。

動的デトネーション分析レイヤーは、拡張無制限のAWS環境内で実行される分離されたデトネーションプラットフォームを使用します。このレイヤーのモジュールは、分析の対象となるサンプルが顧客の実際の状況と同じように動作することを保証するために、各種の高度なサンドボックス技術を利用しています 。また、システム内の痕跡分析を活用し、疑わしい挙動または悪意のある挙動を識別します。

行動プロファイリングおよびコンテキスト分析レイヤーは、システムモジュールによって開発された情報カスケードを相関させ、データに前後関係を付与します。マルウェアの新ファミリーを識別し、隠れた脅威パターンを明らかにするとともに、非常に洗練されたマルウェアの行動プロファイリングを提供します。その後、開発されたインテリジェンスが、専用のレポートモジュールを通じてユーザーに配信されます。

主な機能:

—分析中のすべてのシステムアクティビティを完全に監視することで、攻撃チェーンの完全な可視性が提供されます。

- 完全な外部ネットワーク接続の監視(FTP, TCP, HTTP, および DNS 要求など)
- ミューテックス操作と作成/変更されたサービス
- レジストリキーとそれに関連付けられた値の操作
- ファイルとフォルダの作成、変更、削除
- ドロップされた/ダウンロードされたファイルの実行分析
- メモリダンプ分析
- プロセス、コードインジェクション、API 呼び出しに基づく完全な実行チェーン

— コードの難読化とアンパックを促進する動的コード変更

—レピュテーション、侵害のインジケーターを含む実用的なインテリジェンス

—データ交換に使われるフォーマットや現在の業界標準形式のドキュメントまで、複数の形式で利用可能なレポート

—すべての分析レイヤーに含まれる高度なマシンラーニングメソッド

—休止中のコードから隠しコードまでのディープ コード分析により、コードブロックが未実行、非表示の場合でも識別可能

— コードの類似性のクラスタリングと分類

—分析を回避してくる脅威によって検出されないよう強化された分析環境

Avira

OUR AWARDS

FIND OUT MORE

Website: oem.avira.com
Email: oem@avira.com
Blog: insights.oem.avira.com
Social Media: @AviraInsights

Europe
Middle East, Africa

Avira
Kaplaneiweg 1
88069 Tettnang, Germany
Tel: +49 7542 5000

Americas

Avira, inc
c/o WeWork, 75 E Santa Clara Street
Suite 600, 6th floor San José
CA 95113 United States

Asia/Pacific and China

Avira Pte Ltd
50 Raffles Place
32-01 Singapore Land Tower
Singapore 048623

Japan

Avira GK
8F Shin-Kokusai Bldg
3-4-1, Marunouchi Chiyoda-ku
Tokyo 100-0005, Japan

China

中国北京市朝阳区东方东路19号
外交办公大楼D1座17层1727室
邮编：100016