



AVIRA クラウドサンドボックスサービス

Avira

()

GDPR

API

(IoC)

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初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に設計されています。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。



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援しており、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。



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



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	Americas	Asia/Pacific and China	Japan	China
Avira Kaplaneiweg 1 88069 Tettang, Germany Tel: +49 7542 5000	Avira, inc c/o WeWork, 75 E Santa Clara Street Suite 600, 6th floor San José CA 95113 United States	Avira Pte Ltd 50 Raffles Place 32-01 Singapore Land Tower Singapore 048623	Avira GK 8F Shin-Kokusai Bldg 3-4-1, Marunouchi Chiyoda-ku Tokyo 100-0005, Japan	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