Avira

ファイル レピュテーション API

ゼロデイ攻撃と高度な持続的脅威の検出

受賞歴のある Avira のセキュリティソリューションの中核にあるのが、Avira Protection Cloudです。これは、Avira の高度なマシンラーニングシステムである NightVision™ を搭載したグローバルなクラウドベースのセキュリティサービスです。

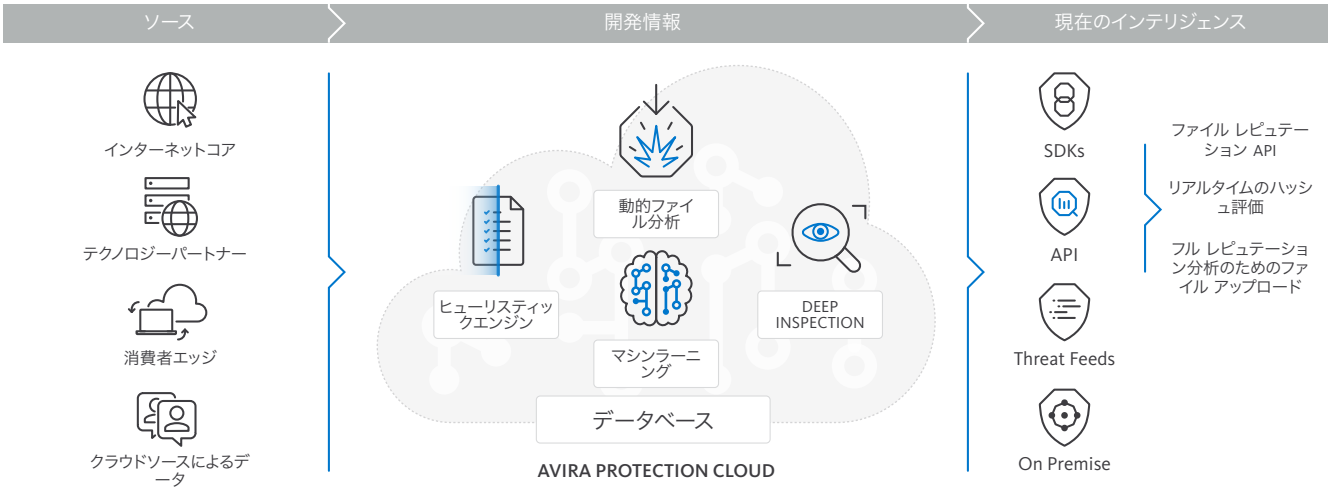
Avira Protection Cloud はファイル レピュテーション API 経由でアクセスすることができたり、Avira のマルウェア対策の SDK (SAVAPI) と組み合わせて使用することができます。Avira Protection Cloud は99.99% を超える確率で、デバイス、アプライアンス、サービスに潜むマルウェアを検出できます。ファイルレピュテーション API は、業界をリードするマルウェア対策機能を各社独自のソリューションに追加するための迅速で簡単かつ効果的な方法を、テクノロジーパートナーおよびサービスプロバイダーに提供します。REST APIはテクノロジーパートナーが評価を得るためにファイル ハッシュを送信することや、分析のためにAvira Protection Cloud にファイルをアップロードすることを可能にします。ハッシュが評価されると、数十ミリ秒以内に結果が返されます。ハッシュが認識されない場合、疑わしいファイルを完全な分析のためAvira Protection Cloud に送信することができます。アップロードされたファイルが評価され、分類を含む応答が返されます。使用されている分析技法には、配信前のジェネリックおよびヒューリスティックを使用したパワフルなクラウドスキャンエンジン、Avira の NightVision マシンラーニング システムによる分類、および革新的な動的ファイル分析技術によるマルウェアの展開と解析が含まれます。新しい分析方法が開発されると、それらは Avira Protection Cloud に統合され、オンラインで配信されます。この場合、テクノロジー パートナーによる対応は必要ありません。

主な機能:

- 使用しやすい REST API によりAvira Protection Cloud はさまざまなプラットフォームに対応。
- クラウドベースのサービスが可用性、信頼性、拡張性を提供。
- 強力なハッシュ評価技術と 10 億件を超えるエントリのデータベースにより、既知の脅威とのリアルタイムの比較が可能。
- ゼロデイ攻撃と高度な持続的脅威の検出。
- Avira の Cloud Scanning Engine は、強力で広範なルールを使用し、数秒以内にマルウェアを分類。
- 何千もの属性を含む疑わしいファイルおよび安全なファイルデータを、同時に複数のアルゴリズムで解析する高度なマシンラーニングシステム
- 他の分析手法から逃れる可能性があるマルウェアを解析するため、多くの主要な OS システムをサンドボックス化してエミュレートする仮想化環境。
- オンプレミスからクラウドへの統合と、クラウドからクラウドへの統合の両方を想定したアーキテクチャー。

Avira

統合



集成

Avira Protection Cloud には、REST API を介して直接アクセスするか、多くのセキュリティシステムに埋め込むことのできる Avira のアンチマルウェア SDK、SAVAPI からアクセスします。(セキュリティシステムの例：次世代ファイアウォール、UTM、Security as a Service、エンドポイント検出、IPS/IDS、電子メール ゲートウェイ、ファイル共有システムなど)。テクノロジーパートナーまたはサービスプロバイダーのセキュリティクラウド内で一次または二次評価を提供するために使用したり、リアルタイムで脅威を判定することができます。

Avira Protection Cloud は、ドイツにある Avira の施設内にホストされています。これには、Avira のテクノロジーパートナーにとっての大きな利点が 2つあります。1つは、世界の中でも最も厳しいデータプライバシー規制に準拠しているという点で、もう1つは、マルウェアの作成者にとってはそれが「ブラックボックス」に見えるという点です。「検出保護」と呼ばれるこのアプローチにより、マルウェアの作成者が Avira Protection Cloud に対してコードをテストするのが非常に困難となります。結果として、Avira Protection Cloud はマルウェア検出に対する従来のアプローチと違い、長期間にわたって優れた性能を発揮することができるようになります。

Avira

仕様

実装:
ファイルの送信およびハッシュ照会のためREST APIを介したアクセス

性能:
ファイルサイズ、脅威のタイプ、およびネットワークの遅延に応じ、100 ミリ以下から目標である3秒まで

リアルタイムの脅威報告:
Windows ファイルおよび実行ファイル、.pdf など

スキャンおよび検出:
実行ファイル: Windows (PE)、Mac、Linux (ELF)
ドキュメント: Office ファイル、pdf、js、vbs、画像など

再学習時間:
ハッシュおよびスキャンの更新は、15 ～ 30 分ごとに継続的に行われる NightVision の更新です

ファイル属性:
8600 以上の属性を分析に利用可能

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