SOPHOS
Security made simple.

Cloud Sandbox

動的なマルウェア分析と先進のDeep Learningでアンチウィルス防御を強化

ソフォスの次世代サンドボックス・プラットフォームは、高度なエミュレーションをベースにDeep Learningを加えた、マルウェア分析を迅速に統合するための完全なソリューションを提供します。クラウド・ベースのソフォスのサンドボックスは、未知または疑わしいプログラムやファイルを詳細に分析するためのスケーラブルで強力な環境を提供します。ソフォスのサンドボックスは、公開しているAPIを介してあらゆるメッセージングまたはWebセキュリティ製品に簡単に統合することができ、プレ・フィルタとしてソフォスのAntivirus SDKを含む、高度な脅威検出システムの実装に伴うコストと複雑さを軽減します。

特徴

- 未知のマルウェアとゼロデイ・マルウェアの高度な検知
- 様々なユースケースとビジネスモデルに応じた容易なインテグレーションが可能
- 任意のネットワーク規模に応じたスケーラブルなセキュリティを提供
- 柔軟でシンプルなライセンスによって費用対効果の高いインテグレーションが可能
- 強力なプレ・フィルタと事前に作成されたロジックがどのファイルに高度な検出が必要かを決定

業界の動向

捕捉できない新しいサイバー犯罪者が、より洗練された新しいマルウェアを開発することで、その感染を管理するためのコストと複雑さは、ますます高まっています。ゼロデイ・マルウェアはこれまで以上に蔓延しており、既存の技術や既存のセキュリティレイヤを迂回することが多くなってきています。

高度なマルウェア・セキュリティ・ソリューションを開発するには、膨大な研究開発費、カスタマイズ、インテグレーションが必要で、さらに高度な検出機能、ユーザ・エクスペリエンス、および費用対効果のバランスを取るために、どのファイルをサンドボックスで分析する必要があるか複雑な決定プロセスの作成が必要です。

ソフォスのサンドボックスを利用することで、セキュリティ・ベンダーは包括的なソリューションを簡単かつ迅速に導入することができます。その基盤となるのは、ソフォスの多くの受賞歴のあるマルウェア対策機能により補完され、SophosLabの脅威分析と緊密に連携した独自の検出プラットフォームです。

容易なインテグレーションと高度な検出

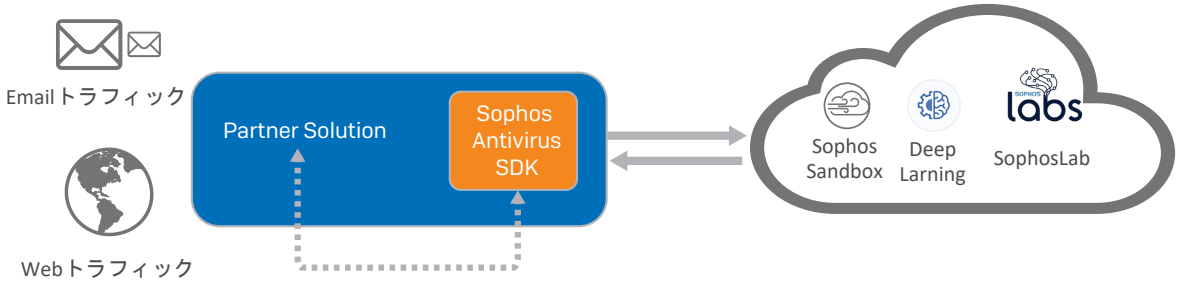
第4世代のソフォスのサンドボックスは、クラウド・サービスとして提供されます。最新の脅威分析と強力なエミュレーションツールを組み合わせて、リアルタイムの分析と包括的な検出技術を使用してファイルを確実に検査します。

包括的なAPIによって統合し、ソフォスAntivirus SDKと組み合わせることで、セキュリティベンダーは多様なユースケースのためのサンドボックス機能を、最も効率的な方法で展開し、時間とリソースを大幅に節約し、ヒューマンエラーの可能性を排除することができます。

高度な分析

業界初のDeep Larningを搭載したサンドボックスによって、シグネチャを利用することなく、誤検知を抑え、トップクラスの検知率を可能にします。
また、Antivirus SDKは、クラウド・サンドボックスを補完し、効率的なプレ・フィルタとして、第一線の防御機能を提供し、誤検知によって高度な分析のために送信されるファイルを削減します。そのため最適なパフォーマンスとユーザ・エクスペリエンスの向上、および疑わしいファイルの迅速な分析が可能になります。

ソフォスのSophos Labは、Synchronized Securityを通じて利用可能なデータ（エンド・ポイントとネットワーク・セキュリティの両方からの二重の分析）を提供し、包括的な階層型セキュリティ・ソリューションを提供するための検出機能をさらにサポートします。



より優れた検出機能とリスクの低減

ソフォスのサンドボックスは、ゼロデイ脅威と高度な攻撃を検出し、修復に必要なリスク評価と攻撃の詳細な情報を提供します。セキュリティ・ベンダーは、これらの検出結果と情報を利用して、是正措置が講じられるまでユーザの安全を確保するための予防措置を実施することができます。

最低限の所有コスト

ソフォスのサンドボックスは、コストを抑えながら高度な検出機能を提供することを目的としています。

- 強力なプレ・フィルタ検出と内臓ロジックにより、大部分のファイルを即座に分類することができます。クラウド・サンドボックスに送信されるファイルが少なくなるため、通信コストを最小に抑えることができます。
- インテグレーションの容易さとプラットフォームの拡張性により、セキュリティ・ベンダーはより早く収益を上げることができます。
- ユーザあたりのファイル数に制限のないサブスクリプション・ベースのモデルによってコストの予測が可能になります。

主な機能

パターンによる検出	検出不可能な標的型攻撃を目的とした多形性およびその他の偽装された脅威を含む悪意のあるファイルの発見をサポートします。
対サンドボックス・マルウェアの阻止	ソフォスのサンドボックスは、VM対応マルウェアの回避行動を検出し、「ヒープスプレー」などの他の一般的なメモリ・エクスプロイトからも防御します。
自動パターン・アップデート	急速に進化する高度な脅威に対する継続的な保護と最大限のパフォーマンスを保証します。
詳細な判定	安全な環境で脅威を分析することで、疑わしいWebサイト、ファイル、アプリケーションおよびイベントに関する決定的な証拠を提供します。
ソフォスの世界規模の脅威分析との統合	世界規模の基盤を活かし、包括的なクラウドソーシングの脅威分析を活用することが可能です。
クラウド基盤	日本国内のクラウド基盤を選択することが可能です。

評価に関して

ソフォスのサンドボックスを評価する際は
oem.sales@sophos.com
までご連絡ください。

For more information

Please visit
www.sophos.com/ja-jp/solutions/oem-solution

OEM Contact
Email: oem.sales@sophos.com

2017-06-23 DS-NA (NP)

SOPHOS