

SOPHOS

Security made simple.



サーバーアプリケーション のホワイトリスト化

シンプルで高度なサーバー保護を実現！

Tsailing Merrem、Senior Product Marketing Manager

企業サーバーを対象にした高度な攻撃に対処するには、強力なセキュリティソリューションが必要です。問題は、適切なレベルの保護を提供しながら、効率的でコスト効果に優れた方法で設定や管理ができるソリューションを見つけることです。アプリケーションのホワイトリスト化は、高度で未知の脅威がサーバーに到達することを防ぐことができますが、これまで、設定が複雑でコストがかかるという問題がありました。ソフォスは、企業環境でのアプリケーションのホワイトリスト化をクラウド経由で実現し、サーバーやサーバー上の機密データを最適な方法で保護します。

企業サーバー保護の課題

企業サーバーには、膨大で価値のあるデータが保存されているため、標的型マルウェア攻撃やゼロデイ攻撃の主要な攻撃対象になっています。サーバーの整合性や可用性、およびデータの機密性を保護することは、今日の企業にとって最も重要な課題です。これまで企業は、サーバーの保護にも、エンドポイントセキュリティソリューションの適用を余儀なくされてきました。しかし、エンドポイントセキュリティソリューションは、サーバーとエンドポイントコンピュータの特性を明確に区別できないため、詳細な設定や最適化を行う必要があり、非常に複雑な処理が必要とされました。

一方、サーバーアプリケーションのホワイトリスト化は、サーバーを高度な脅威や未知の脅威から保護するのに、より適切な方法として、企業により浸透しています。そのアプリケーションが脅威かどうかを判断して、脅威でないものへのアクセスをすべてデフォルトで許可するのではなく、アプリケーションをホワイトリスト化し、それ以外のアプリケーションへのアクセスは既定で拒否するというルールを作成することで、サーバー OS とそこで実行されるアプリケーションを保護します。この方法は、既知および未知の脅威に対して、シグネチャなしのプロアクティブな保護を提供し、IT 部門が許可したアプリケーションのみがシステムで実行されるようにします。

しかし、従来のアプリケーションのホワイトリスト化には、構築時の設定のみならず、メンテナンス作業や設定変更の管理にも過大な管理負荷が伴います。したがって、IT の知識や人的リソースに限りのある中小・中堅企業は、しばしば、導入をためらったり、高価なコンサルティング費用を払ったりする傾向にありました。

ソフォスのアプリケーションのホワイトリスト化 - シンプルで効率的なサーバー保護

Sophos Cloud Server Protection は、中堅中小企業や、規模に関わらず IT 環境がフィットする企業に、簡単に利用できるサーバーアプリケーションのホワイトリスト化を提供します。効果的なセキュリティ、最適化されたサーバーパフォーマンス、迅速な導入、および簡単な管理を実現します。また、アプリケーションのホワイトリスト化と、マルウェア対策およびホスト侵入防止システム (HIPS) 機能を強固に統合する業界唯一のソリューションです。インメモリ攻撃、DLL インジェクション、スクリプトベースの攻撃など、既知の脅威やゼロデイ攻撃に対して効果的なサーバー保護を提供します。

業界初のワンクリックのサーバーロックダウン機能で、マルウェアに対してサーバーを自動的にスキャンします。そして、検出したアプリケーションを識別し、適切なアプリケーションをホワイトリストに登録後、サーバーをロックダウンします。サーバーがロックダウンモードにある場合、登録済みのアプリケーションを置き換えたり、変更したりすることはできません。しかし、Sophos ServerAuthority は、登録済みのサーバーアプリケーションに更新が必要な場合など、そのアプリケーションにとって信頼できる更新 (たとえば Windows Update など) は、管理者が設定を変更せずとも実行できるように構成を自動的に変更します。また、高パフォーマンスを実現するため、ウイルススキャンの除外対象項目を自動的に設定します。このような機能によって、通常は手動による設定やルールの変更などの時間と労力がかかる作業が不要になります。さらに、コンテキストを活用するソフォスのセキュリティエンジンは、システムを常に監視して、コンテンツベースの攻撃から保護します。

概要

ソフォスのアプリケーションのホワイトリスト化は、高度なマルウェア対策および HIPS を統合し、インストールと管理が簡単な、強力なサーバー保護機能を提供します。

特長

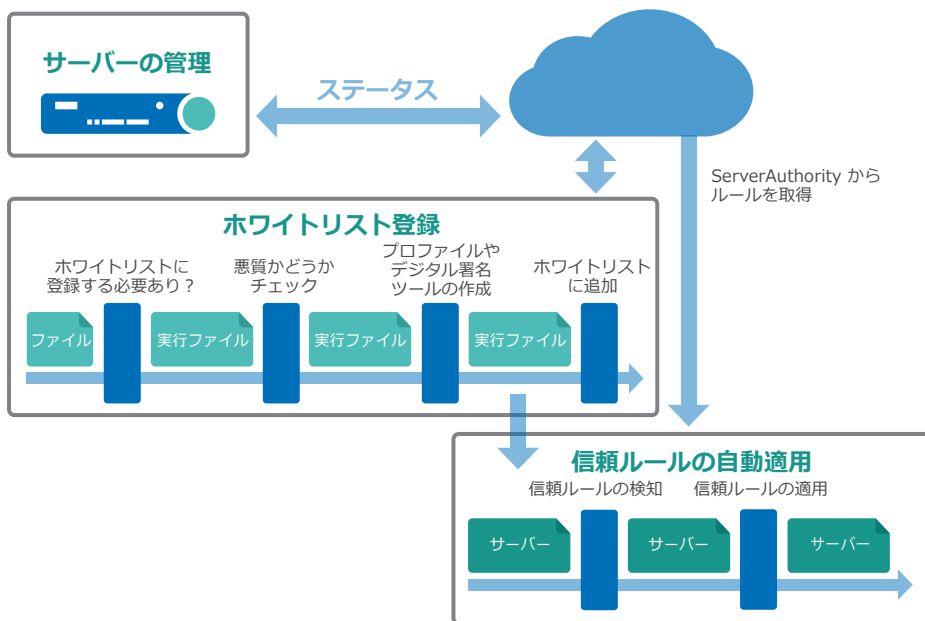
- ▶ ワンクリックでサーバーロックダウン
 - ▶ 自動信頼ルールを使用して、サーバー環境に応じた設定を適用
 - ▶ マルウェア対策および HIPS 機能と統合して、コンテンツベースの攻撃やゼロデイ攻撃から保護
 - ▶ ウィルススキャンから除外する項目を自動的に適用して、パフォーマンスを向上
 - ▶ クラウドベースの保護と管理
-

サーバーアプリケーションのホワイトリスト化

ソフォスのアプリケーションのホワイトリスト化は、アプリケーションだけでなく、DLL やスクリプトもホワイトリストに登録します。Sophos ServerAuthority は、アプリケーションと、それに関連付いている DLL やスクリプトなどのファイルとの関係を自動的にロックダウンし、メモリベースの攻撃から保護します。このような操作は、カスタムルールの作成なしで実行されるので、設定ミスを防ぐこともできます。

ソフォスのホワイトリスト化は、サーバーアプリケーションのパフォーマンスを最適化するように設計されています。また、作成されるカスタマイズ可能な警告やレポートには、統合されている Sophos Cloud の管理コンソール経由で場所を問わずアクセスできます。サーバーの管理者は、管理インターフェースを使って、単一のダッシュボードから、すべてのサーバー、アプリケーション、および保護ステータスを把握することができます。

ソフォス アプリケーションの ホワイトリスト化の構成について



ワンクリックでサーバーロックダウン

ソフォスのアプリケーションホワイトリスト化では、ワンクリックでサーバーをロックダウンできます。そして、物理サーバーの設定、ポリシーの設定、アプリケーションのインベントリの作成、変更管理のためのルールの作成などの作業は一切不要です。従来、何日、何カ月もかかった作業が、ワンクリックするだけで終わりです。ワンクリックすることで、システム全体のマルウェアスキャンが実行され、アプリケーションの一覧が作成され、アプリケーション、自動更新、およびシステム間の信頼関係が確立されます。

ServerAuthority を活用した自動信頼ルール

Sophos Server Protection は、Sophos ServerAuthority を活用して、サーバー環境に応じた適切な設定を適用します。ホワイトリストに登録済みのアプリケーションを検出し、信頼するソースのみが、そのようなアプリケーションを更新できるように必要な信頼ルールを適用します。これによって、アプリケーションの整合性が保護されるだけでなく、アップデートや修正パッチの適用が中断されることなくスムーズに行われます。

Sophos ServerAuthority は、ドメインコントローラー、Exchange Server、SharePoint などの一般的なサーバーアプリケーションの一覧を管理し、推奨されるウイルス検索の除外対象項目を自動的に適用して、パフォーマンスや安定性に影響を与える可能性のあるファイルやディレクトリを検索から除外します。

さまざまなセキュリティ機能を統合

ソフォスのアプリケーションのホワイトリスト化を Sophos Server Protection と統合し、サーバーの安全を確保するために両方のテクノロジーを使用することで、今日見られるさまざまな脅威に対する保護を提供します。同時に、クラウドベースで SophosLabs の脅威データをリアルタイムで参照する Live Protection も使用されます。

サーバー向けの高度な保護

Sophos Server Protection では、ユーザーポリシーとサーバーポリシーが明確に区別されます。デフォルトのサーバーポリシーは、サーバー OS のパフォーマンスと保護の最適なバランスを実現するように設定されています。ポリシーは、1台のサーバーのみに適用したり、Active Directory のグループに適用したり、管理コンソールから手動で適用したり、システム全体に自動的に適用したりできます。

まとめ

今日、既知の攻撃やゼロデイ攻撃から、企業サーバーを保護する緊急性と必要性は、共に増加しています。ソフォスのアプリケーションのホワイトリスト化は、シンプルかつ強力なサーバー保護を提供する業界初のソリューションです。ソリューションには、ワンクリックでのサーバーロックダウン機能、信頼する変更のソースを Sophos ServerAuthority が自動的に指定する機能、および統合されたマルウェア対策および HIPS などが含まれています。これによって、中堅中小企業や規模に関わらず IT 環境がフィットする企業に、使用や管理が簡単で、パフォーマンスの最適化と効果的なサーバー保護を実現するソリューションを提供します。

Sophos Cloud Server Protection

詳細は、次のサイトを参照してください。

<http://www.sophos.com/ja-jp/products/server-security.aspx>

ソフォス株式会社営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

英国、オックスフォード | 米国、ボストン
© Copyright 2015.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos は、Sophos Ltd. の登録商標です。その他すべての製品および会社名は、それぞれの所有者に帰属する商標または登録商標です。

06.15NOLA.wjpp