VMware vShield Endpoint

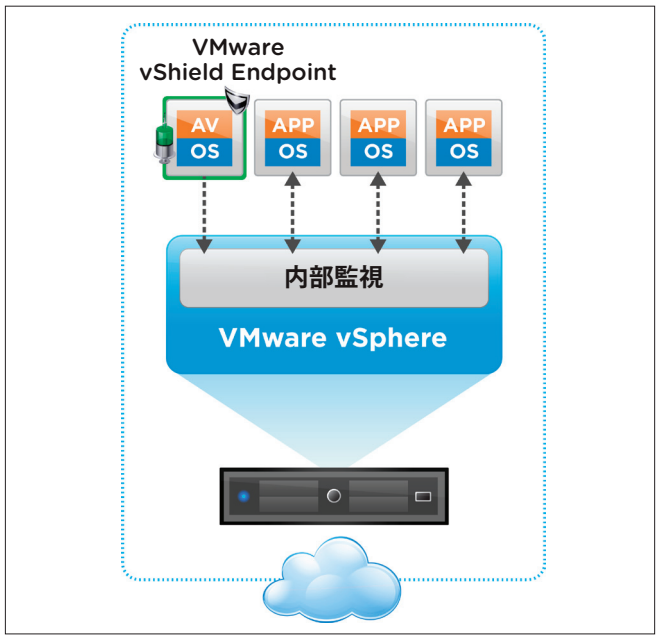
仮想データセンターにおける端末のセキュリティとパフォーマンスの向上

概 要

VMware vShield™ Endpoint は、仮想マシンのセキュリティを強化しながら、端末保護のパフォーマンスを飛躍的に向上させます。また、VMware のパートナーが提供する専用のセキュアな仮想アプライアンスに、アンチウイルスおよびアンチマルウェアのエージェント処理を委譲します。このソリューションは、既存の投資を活用できるよう設計されており、物理環境の保護に使用しているものと同じ管理インターフェイスを使用して、仮想環境用のアンチウイルスおよびアンチマルウェアのポリシーを管理できます。

主なメリット

- 仮想マシンのゲスト OS からアンチウイルス エージェントを排除することによる統合率とパフォーマンスの向上
- VMware の仮想化環境におけるアンチウイルスおよびアンチマルウェアの展開と監視を効率化
- アンチウイルス ソフトウェア エージェントを統合して攻撃の対象となる領域を縮小することで、セキュリティを強化
- アンチウイルスおよびアンチマルウェアのアクティビティをログに記録することで、コンプライアンスおよび監査要件への準拠が可能



vShield Endpoint により、仮想環境におけるアンチウイルスおよびアンチマルウェアのパフォーマンスと統合率が向上します。

vShield Endpoint について

vShield Endpoint は、ゲスト仮想マシンをウイルスやマルウェアから保護する方法を革新し、全く新しい考え方で対応します。このソリューションは、VMware vSphere® および VMware View™ 環境で使用される、アンチウイルスやその他の端末セキュリティを最適化するものです。

vShield Endpoint では、各仮想マシンが負担していたウイルススキャン処理を、1つのセキュアな仮想アプライアンスに委譲することで、パフォーマンスの向上を可能にします。仮想アプライアンスには、ウイルス スキャン エンジンが搭載され、アンチウイルスの署名が格納されています。このアーキテクチャでは、ゲスト仮想マシンにソフトウェア エージェントをインストールする必要がなく、システム リソースを占有しないため、アンチウイルスとアンチマルウェアの機能のパフォーマンスが向上します。また、定期的なスキャンや署名のアップデートなど、アンチウイルスを「頻繁に起動」することで、リソースが過負荷状態になるリスクを排除できます。ゲスト仮想マシンとは異なり、このセキュアな仮想アプライアンスはオフラインになることがありません。このため、アンチウイルス署名を頻繁にアップデートすることが可能となり、ホスト上の各仮想マシンは継続的に保護されます。また、新しい仮想マシン（またはオフライン状態の既存の仮想マシン）は、オンラインになると同時に最新のアンチウイルス署名で保護されます。

vShield Endpoint では、VMware のパートナーが提供する堅牢でセキュアな仮想アプライアンスを使用して、セキュリティを拡張することが可能です。また、vSphere のハイパーバイザーの内部監視機能により、アンチウイルスおよびアンチマルウェア サービス自体の脆弱性が低減します。

VMware のパートナーに提供される vShield Endpoint のインターフェイスにより、ファイルのスキャン機能だけでなく、メモリやプロセスのスキャン機能も実装できます。企業は複数のセキュリティ ソリューションを同時に使用することができます。たとえば、ある仮想アプライアンスで VMware vShield App with Data Security の機密データ検出機能を使用し、別の仮想アプライアンスでアンチウイルス ソリューションを使用することが可能です。

アンチウイルスまたはアンチマルウェア サービスのアクティビティを詳細に記録することで、コンプライアンスへの準拠を実証し、監査要件を満たすことができます。

管理者は、vShield Endpoint に含まれる vShield Manager コンソールを使用して、vShield Endpoint を統合管理できます。vShield Manager コンソールは VMware vCenter™ Server とシームレスに連携するため、仮想データセンターの統合セキュリティ管理が容易になります。

vShield Endpoint の仕組み

vShield Endpoint は、次の 3 つのコンポーネントで構成され、プラグインとして vSphere に直接接続します。

- VMwareのパートナーが提供する堅牢でセキュアな仮想アプライアンス
- セキュリティ関連の負荷を委譲するための仮想マシン用シン エージェント（VMware Tools に付属）
- ESX® ハイパーバイザー レイヤーにおいて上記 2 つのコンポーネント間の通信を有効にする、VMware Endpoint ESX® ハイパーバイザー モジュール

たとえば、アンチウイルス ソリューションの場合、vShield Endpoint が、仮想マシン ファイルのイベントの監視やアンチウイルス エンジンへの通知を行います。アンチウイルス エンジンは、スキャンを実行してその結果を返します。このソリューションでは、ファイルへのアクセス時に行うスキャンと、オンデマンドの（スケジューリングされた）スキャンの両方がサポートされます。これらのスキャンは、セキュアな仮想アプライアンス内のアンチウイルス エンジンが実行します。

修正が必要な場合、管理者は既存のアンチウイルスおよびアンチマルウェア管理ツールを使用して、実行するアクションを指定します。vShield Endpoint は、ウイルスなどに感染した仮想マシン内の修正アクションを管理します。

vShield Endpoint の活用

VMware のパートナーが提供する管理コンソールは、セキュアな仮想アプライアンス内でホストされているパートナーのソフトウェアを構成および管理するために使用します。VMware のパートナーは、ポリシー管理を含む管理上の操作性が、専用の物理セキュリティ アプライアンスでホストされる管理ソフトウェアの場合とまったく変わらないユーザー インターフェイスを提供できます。

また、仮想マシンのアンチウイルス エージェントを管理する必要がなくなるため、仮想インフラストラクチャ管理者の作業量が大幅に削減されます。VMware のパートナー製の管理コンソールを使用して、エージェントの代わりに、セキュアな仮想アプライアンスを管理します。このアプローチにより、仮想マシンごとに、アップデートを頻繁に行う必要がなくなります。VMware Tools には展開に使用するシン エージェントが含まれており、また、ESX モジュールにより、ハイパーバイザーの内部監視が可能になります。

仮想インフラストラクチャ管理者は環境を容易に監視し、アンチウイルス ソリューションが正しく実行されているか判断することができます。

主な機能

アンチウイルスおよびアンチマルウェアの負荷の委譲

- vShield Endpoint は、vShield Endpoint ESX モジュールを使用して、セキュアな仮想アプライアンスにウイルス スキャンの負荷を委譲します。仮想アプライアンス上でアンチウィルスのスキャンが実行されるため、パフォーマンスが向上します。
- ファイル、メモリ、プロセスのスキャンなどのタスクの負荷は、シン クライアント エージェントとパートナーの ESX モジュールを通じて、仮想マシンからセキュアな仮想アプライアンスに委譲されます。
- vShield Endpoint EPSEC は、ハイパーバイザー レイヤーの内部監視機能を使用して、各仮想マシンとセキュアな仮想アプライアンス間の通信を管理します。
- アンチウイルス エンジンと署名ファイルは、仮想アプライアンス内でのみアップデートされます。ただし、ポリシーは vSphere ホスト上のすべての仮想マシンに適用できます。

修正

- vShield Endpoint は、削除や隔離など、悪意のあるファイルの処理方法を指定するアンチウイルス ポリシーを適用します。
- シン エージェントは、仮想マシン内のファイル修正アクティビティを管理します。

パートナーとの連携

- アンチウイルス製品を扱う VMware のパートナーは、EPSEC API を使用して、ハイパーバイザー内にファイル アクティビティの内部監視機能を提供することで、vShield Endpoint との連携が可能になります。この API を通じて、必要なアンチウイルス機能がサポートされます。

vShield Manager、ポリシーの管理と自動化

- vShield Manager により提供される、完全な機能を備えた vShield Endpoint 環境と構成
- REST（Representational State Transfer）API により、各ソリューションに合わせて vShield Endpoint 機能をカスタマイズし、自動的に連携
- 監視レポートの提供
- vShield Manager を vCenter プラグインとして利用可能

ログの記録と監査

- 業界標準の Syslog フォーマットに基づいてイベントのログを記録

サポート対象の製品

サポート対象の vSphere、ESX、および View 環境の製品リリースについては、http://vmware.com/jp/products を参照してください。

関連製品

vShield セキュリティ製品ファミリには、境界をセキュリティ保護する VMware vShield Edge、ネットワーク ベースの攻撃からアプリケーションを保護する vShield App、vShield App の機能に加えて機密データの検出を行う vShield App with Data Security、vShield Manager、およびすべての製品を含む vShield Bundle が含まれます。

詳細情報

製品仕様とシステム要件の詳細については、次の Web サイトで、『VMware vShield Administration Guide』（英語）を参照してください。
http://www.vmware.com/pdf/vshield_41_admin.pdf

vShield 製品の詳細な情報については、
http://vmware.com/jp/products をご覧ください。

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp