VMware vShield App with Data Security

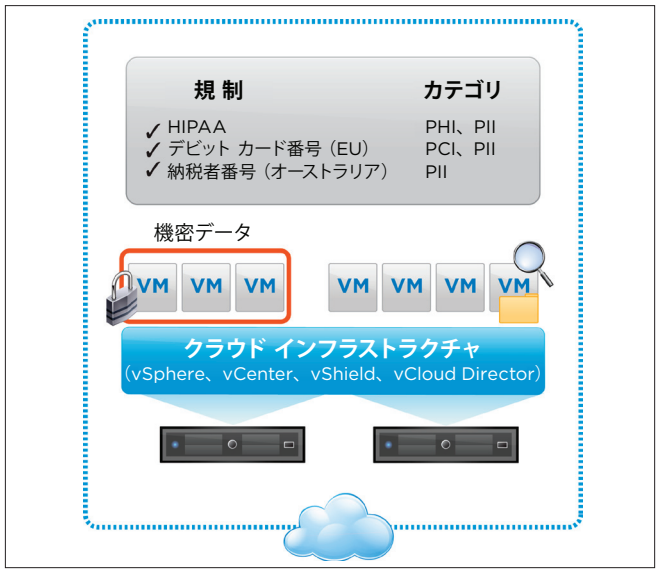
ネットワーク ベースのセキュリティ攻撃からの
アプリケーションの保護と機密データの検出

概 要

VMware vShield™ App with Data Security は、VMware vShield 仮想化セキュリティ製品ファミリの一部です。仮想データセンター内のアプリケーションやデータを、ネットワーク ベースの攻撃から保護します。これにより、仮想マシン間のネットワーク通信の視認性と管理性が向上します。また、仮想ワークロード内でクレジット カード情報などの機密データをスキャンし、PCI-DSS などの規制違反をレポートします。これにより、IT 部門は、世界中のさまざまな規制に対するコンプライアンス状態を迅速に評価できます。この製品には、ファイルのアンチウイルス スキャン処理の負荷を軽減し、アンチウイルスの頻繁な起動を最小限に抑える、VMware vShield Endpoint も含まれています。

主なメリット

- 仮想マシン間のネットワーク通信の視認性と管理性の向上
- 仮想マシン内の機密データを検出し、コンプライアンス違反のリスクを低減
- 各セキュリティ グループを分離するための専用ハードウェアと VLAN の必要性を排除
- ハードウェア リソースの使用を最適化しながら、強力なセキュリティを維持
- すべての仮想マシン ネットワーク アクティビティを包括的に記録する機能により、コンプライアンスへの準拠を簡素化



vShield App with Data Security は、セキュリティ グループを使用して、詳細にポリシーを適用します。

vShield App with Data Security について

vShield App with Data Security は、仮想データセンター向けに開発された、ハイパーバイザー ベースのアプリケーション対応ファイアウォール ソリューションです。このソリューションは、クレジット カード情報などの機密データを動的に検出する機能を提供します。これらの機密情報が、仮想マシン コンテナに格納されている構造化されていないデータ ファイル内にあっても検出可能です。管理者は、この製品を使用してデータセンター、クラスタ、またはリソース プール上の機密データの有無をスキャンすることによって、規制に準拠できるようになります。

この製品は VMware vSphere® に直接組み込まれ、社内ネットワーク ベースの脅威からアプリケーションを保護し、企業のセキュリティ境界内のポリシー違反を低減します。これを実現するため、アプリケーション対応ファイアウォールと、送信元および送信先 IP アドレスに基づく詳細なパケット検査および接続制御を使用しています。

業務に関連するセキュリティ グループを迅速に作成することで、ポリシー制御を簡素化できます。また、フロー監視制御機能により、仮想マシンのネットワーク トラフィック分析や、セキュリティ グループ ポリシーの動的な適用が可能となります。管理者は、vShield App with Data Security に含まれる vShield Manager コンソールを使用して、vShield App with Data Security 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。

また、ハードウェアや VLAN などの従来の制御方法に依存しないため、ハードウェアやポリシーの急増を抑制できます。これにより、物理的なセキュリティの制限を超える費用対効果に優れたソリューションが実現します。

vShield App with Data Security の仕組み

vShield App with Data Security では、機密データの検出ポリシーを管理するための管理コンソールが提供されます。管理者は適切な規制を選択してポリシーを作成し、これを使用して対象となる仮想マシン コンテナ（データセンター、クラスタ、およびリソース プール）全体のスキャンを行います。また、ファイルの拡張子、サイズ、または更新日で、スキャン対象のファイルをフィルタリングできます。スキャン結果には、選択したポリシーに準拠していないデータセンター、クラスタ、仮想マシン、およびファイル名が表示されます。管理者は REST（Representational State Transfer）API を使用して、規制に準拠していないファイルを修正できます。

vShield App with Data Security は各 vSphere ホストにインストールされ、ホスト上のすべてのネットワーク トラフィックを管理および監視します。これには、物理ネットワーク インターフェイス カード（NIC）を経由しないパケットも含まれます。物理的な境界や、アプリケーションの展開に関する静的な前提条件の代わりに、管理者が定義した業務に関連するセキュリティ グループに基づいて、ポリシーの作成および適用が可能です。

また、vCenter Server を利用した統合インターフェイスを提供しているため、仮想データセンター内の複数の vSphere ホストにこれらのポリシーを一括で適用できます。

vShield App with Data Security の活用

- **仮想ホストに格納されたデータのコンプライアンスへの準拠：** REST API を使用することで、管理者は手動またはプログラムによるスキャンを実行し、選択したポリシーへ準拠しているかどうかを検証できます。
- **テンプレートの提供：** 管理者はテンプレートを選択してポリシーを作成し、これをスキャン対象となる特定の仮想リソースに適用します。
- **機密データのスキャン結果：** スキャン結果はレポートとして出力されます。このレポートは、コンプライアンスに違反した仮想マシンの特定や隔離に利用できます。
- **アプリケーション対応の保護機能：** 管理者は、仮想 NIC を経由するすべてのトラフィックに対し、詳細なポリシーを定義して適用することができます。これにより、社内の仮想データセンターのトラフィックに対する視認性が向上し、物理ファイアウォールへの迂回路が排除されます。
- **変更に対応した保護機能の維持：** vShield App では、ホスト間で移行しても仮想マシンは引き続きファイアウォールで保護されます。そのため、ネットワーク トポロジを変更してもアプリケーションのセキュリティには影響しません。
- **動的なポリシーを効率的に管理：** 変化するビジネス ニーズに応じて社内ファイアウォール ポリシーの定義や調整を行うための、豊富なコンテキストを管理者に提供します。
- **ボットネット攻撃によるリスクの低減：** 信頼できるアプリケーションに対する動的なポートの割り当てが可能なため、セキュリティ管理者はボットネットやその他の攻撃を防ぐことができます。
- **共有リソースへのアクセスの制御：** セキュリティ管理者はストレージやバックアップなど、vSphere ホスト上の共有サービスへのアクセスを IP アドレスに基づいて制限できます。
- **IT コンプライアンスへの準拠の促進：** 仮想マシンのネットワーク セキュリティの視認性と管理性が向上します。また、ログの記録および監査制御機能により、企業は社内ポリシーや外部の規制要件へ準拠していることを証明できます。

主な機能

機密データの検出

- ポリシー管理コンソールで、管理者はコンプライアンスのスキャンに使用する規制を選択
- 企業は、PII（Personally Identifiable Information）、PCI-DSS のカード保有者のデータ、PHI（Private Health Information）など、北米、ヨーロッパ、中東、アフリカ地域、アジア太平洋地域を含む、世界各地の規制に対応した 80 以上のテンプレートから選択可能
- スキャン後に作成されるレポートで、選択した規制に違反するデータ リソースを特定
- REST API またはオペレータ コンソールを使用して、機能のプログラミングが可能
- VMware vCenter Configuration Manager を使用して、ウイルスに感染した仮想マシンを隔離および修正

ファイアウォール

- ハイパーバイザー レベルのファイアウォール：ハイパーバイザーの検査により受信接続および送信接続を仮想 NIC レベルで制御し、マルチホーム仮想マシンをサポート
- レイヤー 2 のファイアウォール：透過型ファイアウォールとも呼ばれるレイヤー 2 のファイアウォールにより、パスワード スニフィング、DHCP スヌーピング、ARP（Address Resolution Protocol）偽装やポイズニング攻撃など、さまざまな種類の攻撃からの保護を実現。この機能により、SNMP トラフィックは完全に分離される
- ネットワーク、アプリケーション ポート、プロトコル タイプ（TCP、UDP）、またはアプリケーション タイプに応じて保護を適用
- 仮想マシン移行時の動的な保護を実現
- IP ベースのステートフルなファイアウォールおよびアプリケーション レイヤー ゲートウェイ：Oracle、Sun RPC（Remote Procedure Call）、Microsoft RPC、LDAP、SMTP などの広範なプロトコルに対応。ゲートウェイは、必要な場合にのみセッション（ポート）を開くことで、セキュリティを強化。サポート対象プロトコルの一覧については、『VMware vShield Administration Guide』（英語）を参照

フローの監視

- 詳細なレポート作成機能：管理者は、アプリケーション トラフィック（アプリケーション、セッション数、バイト数）の詳細なレポートにより、仮想マシン間のネットワーク アクティビティを確認し、ファイアウォール ポリシーの定義と変更、ボットネット攻撃の特定、およびビジネス プロセスの保護を実現

セキュリティ グループ

- 管理者は、業務に関連する仮想マシンのグループを仮想 NIC ごとに定義可能

ポリシー管理

- vShield Manager により製品の機能を管理。多くの機能は、vCenter Server インターフェイスから利用可能
- 管理者によるセキュリティ グループ、vCenter Server グループ、および TCP 5-tuple（送信元 IP、送信先 IP、送信元ポート、送信先ポート、プロトコル）へのポリシーを適用
- REST（Representational State Transfer）API は、管理およびポリシー適用のためのプログラム可能なインターフェイスを提供
- 企業のセキュリティ管理ツールとの連携をサポート

IP アドレス

- 複数のテナント ゾーンで同一の IP アドレスを使用するなど、柔軟な IP アドレス指定によりプロビジョニングを簡素化

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ログを記録
- REST API と vShield Manager により、ログおよび監査ツールが利用可能に
- ファイアウォールのログ記録のオンまたはオフを、管理者がルールレベルで定義可能

サポート対象の製品

サポート対象の vSphere 環境の製品リリースついては、
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、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、境界をセキュリティ保護する vShield Edge、端末のセキュリティとパフォーマンスを強化する vShield Endpoint、vShield Manager、およびすべての製品を含む vShield Bundle があります。

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 サイトから、『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 を参照してください。

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