VMware vShield Bundle

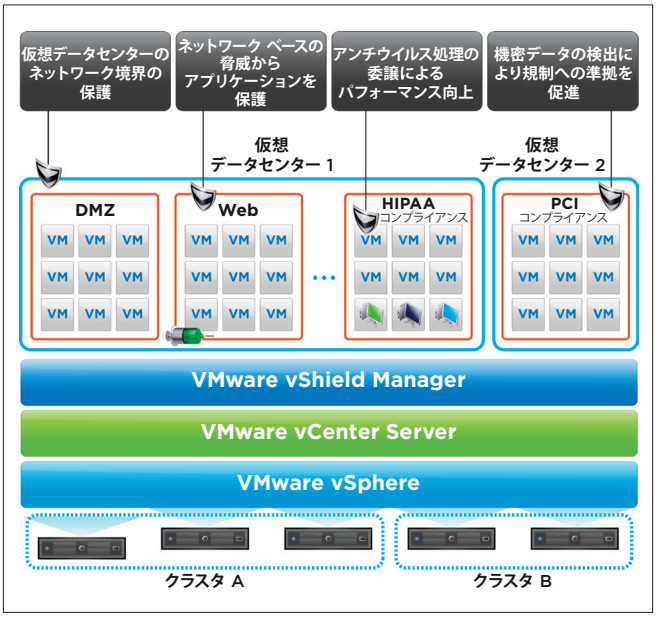
信頼性に優れたクラウド インフラストラクチャの基盤

概 要

VMware vShield™ Bundle は、信頼性の高いクラウド インフラストラクチャの基盤となります。vShield Bundle は、適応性と費用対効果に優れ、統合されたセキュリティ サービスと管理機能を提供します。これにより、仮想データセンターとクラウド環境があらゆるレベル（ネットワーク エッジ、アプリケーションとデータ、端末）で保護されます。vShield Bundle は、VMware vSphere®、VMware vCenter™ Server、および VMware vCloud™ Director と連携します。

主なメリット

- 仮想データセンターとクラウド環境をあらゆるレベル（ネットワーク エッジ、アプリケーションとデータ、端末）で保護
- コストおよび複雑性の低減
- エージェントを必要としない展開により、アンチウイルスとアンチマルウェアの「頻繁な起動」を排除
- 機密データの検出によって、規制への非準拠および企業イメージの悪化のリスクを低減
- 適応性の高いトラスト ゾーンを利用して、共通のセキュリティ ポリシーとアクセス要件を持つアプリケーションとデータのグループを形成



VMware vShield では、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できます。

VMware vShield Bundle の機能について

vShield Bundle のソリューションは、仮想データセンターの物理セキュリティよりも優れています。vShield Bundle には 4 つの vShield 製品の高度な機能が含まれており、適応性と費用対効果の高い、統合されたセキュリティ サービスと管理ソリューションが提供されます。これにより、ネットワーク境界から、端末を通じたアプリケーションやデータまで、仮想データセンターとクラウド環境が保護されます。

ネットワーク境界

vShield Bundle のエッジ ネットワーク セキュリティ ソリューションである vShield Edge は、仮想データセンターの境界を保護し、ネットワーク セキュリティ ゲートウェイ サービスなどの重要なセキュリティ機能と、パフォーマンスと可用性のための Web ロード バランシング機能を提供します。このソリューションは vSphere に直接組み込まれ、フォルト トレランスや高可用性などの vSphere の機能を活用して、比類のない回復性を実現します。

vShield Edge は VMware vCloud™ Director と連携しており、マルチテナント クラウド インフラストラクチャにおける仮想データセンターのプロビジョニングの自動化と安全性を強化します。また、セキュリティ管理者と仮想インフラストラクチャの管理者の業務を分離することにより、許可を受けたリソースのみにアクセスが制限されます。

vShield Edge は仮想アプライアンスとして展開され、ファイアウォール、仮想プライベート ネットワーク（VPN）、Web ロード バランサ、ネットワーク アドレス変換（NAT）、DHCP（Dynamic Host Configuration Protocol）サービスなどのネットワークセキュリティ ゲートウェイ機能を提供して、送信元および送信先の IP アドレスが含まれるパケットのヘッダを監視します。また、ポリシーに基づいて、接続の拒否または許可、VPN セッションの開始および終了、ネットワーク アドレスの変換、送信元および送信先のポートや TCP（Transmission Control Protocol）または UDP（User Datagram Protocol）などのプロトコル タイプ単位で、データの検査を実行します。

アプリケーションとデータ

vShield Bundle に含まれる vShield App with Data Security は、仮想データセンターに対し、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 ソリューションを提供します。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 コンテナ内の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、データセンター、クラスタ、またはリソース プール上で機密データの有無をスキャンすることにより、規制に準拠できるようになります。

vSphere に直接組み込まれた vShield App with Data Security は、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。また、管理者が業務に関連するセキュリティ グループを迅速に作成できるため、ポリシー管理が簡素化されます。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、ポリシーを作成および適用します。また、フロー監視機能が含まれており、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。

vShield App with Data Security では、機密データの検出の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。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、準拠していないファイルを修正できます。

エンドポイント ソリューション

VMware のエンドポイント ソリューションは、革新的なアーキテクチャ上のアプローチを利用して、アンチウイルス、機密データの検出、および VMware のパートナーが提供する vSphere および VMware View™ の環境向けのその他の端末セキュリティ機能を最適化します。

vShield Endpoint のアンチウイルス実装環境では、各仮想マシンが負担していたウイルス スキャン処理を単一の安全な仮想アプライアンスに委譲することで、パフォーマンス向上を実現します。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、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 ソフトウェアを「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。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。新しい仮想マシンも、最新のアンチウイルス署名によって即座に保護されます。vShield Endpoint を使用すると、各仮想マシンにアンチウイルス エージェントを配置して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の管理者の作業が大幅に削減されます。管理者は 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、安全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。

vShield Endpoint では、VMware のパートナーが提供する堅牢で安全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 の堅牢で安全な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 のパートナー企業に提供されるインターフェイスでは、ファイル、メモリ、およびプロセスのスキャン機能を実装できます。このアーキテクチャは、複数のセキュリティ ソリューションを同時にサポートします。たとえば、あるセキュリティ仮想アプライアンスで機密データの検出を行い、別のセキュリティ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できます。

企業は、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

管理者は、付属の管理コンソールである vShield Manager を使用して、vShield Bundle を統合管理できます。vShield Manager 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 Bundle の活用

vShield Bundle を展開すると、セキュリティ サービスと管理ソリューションが提供され、仮想データセンターとクラウド環境をあらゆるレベルで保護できるようになります。

ネットワーク境界

vShield Bundle には、次のような重要な機能を提供する、エッジ ネットワーク ゲートウェイ セキュリティ ソリューションである vShield Edge が含まれます。

- **エッジ セキュリティ ハードウェアの統合：** 既存の vSphere リソースを使用してエッジ セキュリティ サービスをプロビジョニングできます。vSphere ホストを「エアギャップ」するための、専用のハードウェア アプライアンスは必要ありません。
- **仮想データセンターの境界を迅速かつ安全に設置：** 仮想データセンター環境の周辺に、ハードウェアに依存しない安全な論理的境界（エッジ）を容易に設置します。これにより、マルチテナント IT インフラストラクチャ内の共有ネットワーク リソースを容易に利用できるようになります。
- **共有ネットワーク上でデータの機密性を保護：** 256 ビットの暗号化を使用したサイト間の VPN 機能を提供しており、仮想データセンターの境界を越えて転送されるすべてのデータの機密性が維持されます。
- **Web サービスのパフォーマンスと可用性の保証：** 仮想マシン クラスタ間の受信 Web トラフィックを効率的に管理します。また、エッジ セキュリティとともに展開することも、単独で展開することも可能な、Web のロード バランシング機能を使用できます。

- **コンプライアンス管理の促進：** イベントの詳細なログ記録やフローの統計情報など、必要な管理機能を展開します。これらは、企業ポリシーや業界および政府の規制に遵守していることを証明するために必要な機能です。

アプリケーションとデータ

vShield Bundle には、次の目的に使用可能なアプリケーション対応ファイアウォールである vShield App with Data Security が含まれています。

- **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。
- **アプリケーション対応の保護機能：** 仮想ネットワーク インターフェイス カード（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：** 仮想マシンをホスト間で移行しても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：** ポリシーの定義を簡素化し、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、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：** ログの記録および監査制御機能により、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。これらの機能は、社内ポリシーや外部の規制要件へ準拠していることを示すために必要です。

エンドポイント ソリューション

vShield Bundle には、次の目的のためのエンドポイント機能である vShield Endpoint が含まれています。

- **アンチウイルスおよびアンチマルウェア展開の効率化：** エンタープライズ アンチウイルス エンジンと署名ファイルを vSphere ホスト上のすべての仮想マシンに展開する代わりに、1 つのセキュリティ仮想アプライアンスのみに展開します。
- **仮想マシンのパフォーマンスの向上：** 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のスキャンなどの処理の負荷を、個々の仮想マシンから各 vSphere ホスト上の 1 つのセキュリティ仮想アプライアンスに委譲することで、高い統合率を安全に実現します。
- **頻繁なアンチウイルスの起動とボトルネックの回避：** アンチウイルスおよびアンチマルウェアのスキャンとアップデートを 1 つのセキュリティ仮想アプライアンスで行うことで、頻繁なアンチウイルスの起動とボトルネックを回避できます。
- **アンチウイルス セキュリティ ソフトウェアを攻撃から保護：** 堅牢なセキュリティ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 クライアント ソフトウェアを展開して実行し、アンチウイルスおよびアンチマルウェア ソリューションを標的とする攻撃から保護します。

主な機能

vShield Bundle に含まれる主な機能とコンポーネントは次のとおりです。

ネットワーク境界向け

ファイアウォール

- 境界（レイヤー 3）ファイアウォール。ネットワーク アドレス変換（NAT）は不要
- ステートフル インスペクション ファイアウォール。次のパラメータに基づくルールを使用して、受信および送信接続を制御
  - IP アドレス：送信元および送信先の IP アドレス
  - ポート：送信元および送信先のポート
  - プロトコル：タイプ別（TCP または UDP）

ネットワークアドレス変換

- 仮想環境で送受信される IP アドレスの変換
- 信頼できないサイトへは、仮想データセンターの IP アドレスをマスカレードして送信

DHCP（Dynamic Host Configuration Protocol）

- vSphere 環境内の仮想マシンに対する IP アドレス プロビジョニングの自動化
- 管理者が定義するパラメータ（アドレス プール、リース期間、専用 IP アドレスなど）

サイト間の VPN

- 仮想データセンター（またはエッジ セキュリティ仮想マシン）間の通信の保護
- IKE（Internet Key Exchange）プロトコルに基づく IPsec VPN（証明書認証および共有キーをサポート）

Web のロード バランシング

- Web トラフィック（HTTP）を含むすべてのトラフィックの受信ロード バランシング
- ラウンド ロビン アルゴリズム
- 「スティッキー」セッションのサポート

エッジ フロー統計情報

- テナントに起因する仮想データセンター リソースの使用率の測定
- REST API を介してアクセスでき、サービス プロバイダのチャージバック アプリケーションで利用される統計情報

ポリシー管理

- vShield Manager を使用した完全な管理機能。多くの機能が vCenter Server インターフェイスから利用可能
- REST API を使用した管理のための、カスタマイズ可能なインターフェイス
- 企業の IT セキュリティ管理ツールとの連携をサポート

ログの記録と監査

- 業界標準の Syslog フォーマットに基づく
- REST API および vShield Manager ユーザー インターフェイスを通じて利用可能
- 管理者は主なエッジ セキュリティ イベント（エラー、警告など）用のログ記録のオン / オフを次のレベルで定義可能
  - ファイアウォール：ルール レベル
  - NAT：ルール レベル
  - VPN：サイト間の接続名
  - Web ロード バランサ：プール レベル。URL やフォルダなどの特定の Web 要求
  - DHCP：サービス レベル。バインディング（リリースおよび更新）

アプリケーションとデータ向け

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
- 80 以上の規制テンプレート。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、およびアジアパシフィック地域の規制に対応
- 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のリソースを特定
- 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（Simple Network Management Protocol）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
- Oracle、Sun RPC（Remote Procedure Call）、Microsoft RPC、LDAP（Lightweight Directory Access Protocol）、SMTP などの広範なプロトコルに対応する、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。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
- 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）へのポリシーの適用
- REST 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

端末向け

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 Bundle ESX モジュールを使用して、セキュリティ仮想アプライアンスにウイルス スキャン処理を委譲します。セキュリティ仮想アプライアンスには、ウイルス スキャン エンジンを搭載され、アンチウイルス署名が格納されています。
- 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、仮想マシンから安全な仮想アプライアンスに委譲されます。
- EPsec（Endpoint Security）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、各仮想マシンと安全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、セキュリティ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（管理者が定義する規制のセット）は vSphere ホスト上のすべての仮想マシンに適用できます。

安全な仮想アプライアンスによる修正のトリガ

- パートナーのアンチウイルス エンジンのポリシーを保持し、削除や隔離など、悪意のあるファイルの処理方法を指定します。
- 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に使用します。

パートナーとの連携

- ハイパーバイザー レイヤーにおいてファイルのアクティビティを内部監視するための vShield Bundle EPsec API を使用すると、VMware のパートナーが提供するセキュリティ仮想アプライアンス ソリューションとの連携が容易になります。

vShield Manager、ポリシーの管理と自動化

- 完全な機能を備えたエンドポイント環境の構成を提供
- REST API により、エンドポイント機能をカスタマイズし、各ソリューションと自動的に連携
  - 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 標準に基づいてイベントのログを記録

サポートされるリリース

vSphere、ESX、および VMware View 環境でサポートされる製品リリースの詳細については、www.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 vShield Edge、ネットワーク ベースのセキュリティ攻撃からアプリケーションを保護し、機密データの検出を行う vShield App with Data Security、エンドポイント セキュリティと仮想データセンターのパフォーマンス向上を提供する vShield Endpoint、および vShield Manager があります。vShield Bundle には、vShield Edge、vShield App with Data Security、vShield Endpoint、および vShield Manager のすべてが含まれます。

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 製品の詳細については、
http://www.vmware.com/jp/products をご覧ください。

vShield Bundle には次のものが含まれます

- **vShield Edge：**仮想データセンターの境界をセキュリティ保護するネットワーク ゲートウェイ ソリューション
- **vShield App with Data Security：**vShield App に機密データの動的な検出機能を追加して、規制へ準拠するためのサポートを提供
- **vShield Endpoint：**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専用のセキュリティ仮想アプライアンスに委譲して、仮想マシンのセキュリティを強化し、端末保護のパフォーマンス向上を実現
- **vShield Manager：**サードパーティ製のセキュリティ サービスの管理、展開、レポート作成、ログ作成、および統合を中央から管理

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