KASPERSKY SECURITY FOR VIRTUALIZATION と VMWARE NSX

Software-Defined Data Center (SDDC) 向けに高品質な保護を実現

データは企業にとってもっとも重要な資産です。そのため、データをどこで、どのように保管、処理、送信するかが、より高い競争力を得るだけでなく、運用効率の向上とビジネスの継続性を維持するためには大切なことです。

データの処理、ストレージ、ネットワーク運用のための優れたソリューションは多数ありますが、ネットワークソリューションは複雑で柔軟性に欠け、その基盤となるハードウェアプラットフォームに縛られ、制限を受ける場合がしばしばあります。そのような場合、データセンターの俊敏性や、日々変化するビジネス要件に対し十分に対応できません。

VMwareとカスペルスキーはこれらの問題を共同で解決するために、極めて効率的な Software-Defined Data Center (SDDC) を中心とする共同ソリューションを開発しました。このソリューションは、高度なセキュリティ機能を備え、社内外の脅威からの保護を高いレベルで実現します。

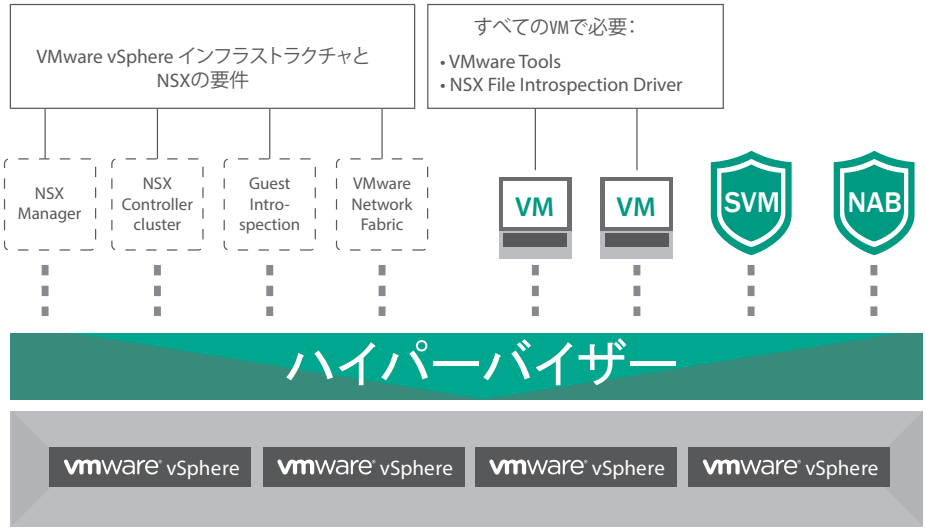
提供される VMWARE NSX サービス	
分散型ファイアウォール	仮想ネットワーク（VXLAN）
サーバーアクティビティ監視	VPN（IPSec、SSL L2VPN）
KASPERSKY SECURITY FOR VIRTUALIZATION	
アンチマルウェア	仮想ネットワーク IDS/IPS
セキュリティの自動化	ポリシーベースの統合
セキュリティタグの統合	電源オフの VM においてもすべてのインフラストラクチャをスキャン

Kaspersky Security for Virtualization | Agentless は、VMware vSphere 上に構築された Software-Defined Data Center（SDDC）をVMware NSX 技術を最大限に利用して保護するように設計された製品です。カスペルスキーのセキュリティソリューションは、プラットフォームのパフォーマンスにほとんど影響を与えずに、高度なセキュリティ機能を提供します。そのため、仮想マシン（VM）の集約率を維持しながら、最高レベルのアンチマルウェアソリューションのメリットを享受できます。

プラットフォーム統合の仕組み

VMware NSX は、ソフトウェア定義モデルを用いてデータセンターのネットワークを構築します。そのため、ユーザーは異なるネットワークリソースプールを操作して、わずか数秒でネットワークトポロジ全体を動的に作成または再構成することができます。その際には、常に検証する「ゼロトラスト」のセキュリティアプローチを利用します。

VMware NSX プラットフォームと Kaspersky Security for Virtualization との高度な統合により、各 VM（仮想マシン）と仮想化されたネットワークは、高度な脅威から自動的に保護されます。どの 仮想マシン（VM）にもセキュリティエージェントをインストールする必要はなく、仮想化プラットフォームのパフォーマンスに影響を及ぼすことなく、継続的かつ包括的な保護を実現します。



セキュリティ仮想マシン
- VMware NSX との高度な統合
- VMware NSX と vShield Endpoint のサポート
- システムリソースの消費を最小化
- 仮想マシンの電源オンまたはオフに関わらずスキャン

ネットワーク攻撃防御
- ネットワークの強力な保護
- URL スキャンによる Web トラフィックのコントロール
- ヒューリスティック分析によるアプリケーションの保護
- インフラストラクチャ全体の保護

仮想プラットフォームとセキュリティソリューションが高度に連携するため、Software-Defined Data Center（SDDC）は、インフラストラクチャ全体に対し、すべてのセキュリティインシデントにリアルタイムで対処できます。

VMWARE NSX のセキュリティに特化したに設計

- 業界で最も高く評価されたアンチマルウェアエンジンが、迅速に最新の脅威に対応し、ゼロデイ攻撃からの保護をより強固なものにします。
- VMware NSX の自動デプロイ機能により、セキュリティアプライアンス（セキュリティ仮想マシンまたはネットワーク攻撃防御）の配置を自動化できます。
- セキュリティポリシーとの統合により、各仮想マシン（VM）には、VM の個々の役割に基づき、お客様の企業ポリシーに沿ったセキュリティ機能が提供されます。
- セキュリティタグとの統合により、Software-Defined Data Center（SDDC）は、セキュリティインシデントにリアルタイムに対処し、必要に応じて仮想化インフラストラクチャ全体を自動的に再構成できます。
- クラウドベースの Kaspersky Security Network（KSN）が、高度な脅威に対するプロアクティブな防御を提供します。
- VMware NSX と vShield Endpoint を同時にサポートすることで、企業の IT 戦略とセキュリティ戦略をビジネス要件と完全に一致させた運用が可能です。

セキュリティと監視の自動化

- インフラストラクチャを完全にスキャンすることで、すべての仮想マシン（VM）は、電源がオンまたはオフの状態にかかわらず保護されます。これによりインフラストラクチャ全体を網羅したセキュリティシステムを実現します。
- すべての仮想マシン（VM）の定期スキャンのスケジュールを柔軟に設定できるため、ビジネス要件に沿ったセキュリティタスクの設定と実行を自動化できます。
- 高度な SNMP ベースの監視機能により、セキュリティ仮想マシン（SVM）を常時監視し、また SNMP をサポートするサードパーティのネットワーク監視ツールに情報を送信できるため、企業のネットワーク管理システムを利用してセキュリティ仮想マシン（SVM）のステータスを監視することができます。
- VMware vMotion とディザスタリカバリ機能により、ワークロードを ESXi 間で移動する際にセキュリティ保護が中断することがなく、安全に継続的なシステムの運用が可能です。
- VMware vCenter Server および VMware NSX Manager との高度な統合により、セキュリティ層はインフラストラクチャ層と連携し Software-Defined Data Center（SDDC）の自動化と保護レベルをさらに高めることができます。

保護とパフォーマンスの最適化

- 仮想化向けに設計された受賞歴のあるアンチマルウェア保護機能は、ファイルスキャンのタスクを個々の仮想マシン（VM）から専用のセキュリティ仮想マシン（SVM）に委譲するため、パフォーマンスが向上します。
- 仮想ネットワーク IDS/IPS（不正侵入検知・防御システム）は、エージェントレスモードで動作するため、仮想インフラストラクチャ全体がネットワークをベースにした最新の脅威から保護されます。
- 共有キャッシュ機能により、最近スキャンされたファイルが定期スキャン中に再度スキャンしないように制御します。
- システムリソースを効率的に使用するカスペルスキーのセキュリティソリューションは、システムのパフォーマンスを向上させ、コンピューティングインフラストラクチャに与える負荷を軽減します。

容易な導入と効率的な管理

- 単一の統合管理コンソールを使用することで、仮想化環境、物理環境およびモバイル端末を含むすべての コンピュータ 資産に対し一貫性のあるセキュリティポリシーを適用できます。
- 新たな仮想マシン(VM)の追加やインストールする際にシステムを停止することなく導入できるため、仮想マシン（VM）を再起動したり、ホストサーバーをメンテナンスモードにする必要はありません。
- スキャンタスクの高度な設定と実行の自動化により、ハイパーバイザーのリソース消費を最小限に抑えるため、プラットフォーム全体のパフォーマンスを向上させます。
- 豊富なレポートと監視機能を活用することで組織内でのセキュリティの管理と監視をより簡単に行うことができます。

その結果、卓越したパフォーマンスの効率と業界をリードするセキュリティが両立したエンタープライズレベルの柔軟な仮想化環境を構築できます。

Software-Defined Data Center（SDDC）の最適なセキュリティ

物理インフラストラクチャと仮想インフラストラクチャも、同じセキュリティの脅威に直面しています。サイバー犯罪者はこれらを区別しません。セキュリティとパフォーマンスについても最適化された環境を構築する必要があります。

1 サイバー脅威は過去のものに

業界で最も高く評価されたセキュリティエンジンを搭載する Kaspersky Security for Virtualization は、仮想化された IT 環境全体を高度な脅威と脆弱性から保護します。カスペルスキーのセキュリティソリューションは、仮想プラットフォームが提供する技術的な利点を活用するように設計されているため、最適なパフォーマンスとシステムリソースの消費を抑えながら、強力なセキュリティシステムを実現します。

2 VMWARE NSX 向けに設計および最適化

カスペルスキーのエージェントレス型ソリューションを VMware NSX プラットフォームと高度に統合することで、お客様の仮想インフラストラクチャをより効率的に運用することができます。カスペルスキーのエージェントレスは、VMware NSX のセキュリティポリシーおよびセキュリティタグと連携して動作することで、高度なセキュリティ機能をリアルタイムで VMware NSX プラットフォームに提供して自動的に保護するため、運用効率がより向上します。

3 エンタープライズレベルの可視性と管理の容易性

単一の統合管理コンソールを活用することで、IT部門の運用管理担当者は、すべて仮想マシン（VM）のセキュリティを、物理環境やモバイル端末上に導入されているカスペルスキーのセキュリティ製品と合わせて一括管理できます。仮想化、物理、およびモバイルプラットフォームを組み合わせたハイブリッドな環境を運用管理担当者が容易に管理できるようにすることで、仮想化プロジェクトをスムーズに展開できるとともに、IT リソースへの負荷を軽減し、ヒューマンエラーによるシステム障害の発生する可能性も低減できます。

Kaspersky Security for Virtualization は、VMware NSX プラットフォーム上に構築された企業のハイブリッド環境に、最先端のセキュリティ機能を提供します。また、このソリューションはシステムのパフォーマンスに影響を及ぼさないことから、最高レベルのセキュリティシステムを効率的に運用できます。仮想化環境に特化したカスペルスキーのセキュリティソリューションは、IT インフラストラクチャを透過的に統合して操作できる包括的な保護管理機能を提供します。ハイブリッドな仮想化環境は、Kaspersky Security for Virtualization とともに使用することで、さらなるメリットを享受できます。

株式会社カスペルスキー

詳細情報はこちら：http://www.kaspersky.co.jp/enterprise-security/data-center

ご購入相談窓口：jp-sales@kaspersky.com

KASPERSKY
Save the World from IT threats

PMM-1015-201702