KASPERSKY SECURITY FOR VIRTUALIZATION と VMWARE NSX

* VMware NSX対応は2017年予定です

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、制限を受けるケースがしばしばあります。そうなると、データセンターの俊敏性や、日々に変化するビジネス要件への対応力が損なわれます。

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、社内外の脅威から高いレベルの保護を実現します。

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	侵入防止（IPS）
セキュリティポリシー統合	セキュリティタグ統合
自動配置	Software-Defined Data Center (SDDC)向けの多層型セキュリティ

カスペルスキーのエンタープライズポートフォリオでは、企業インフラストラクチャに対して業界をリードするセキュリティ機能を導入するための様々なソリューションを提供しています。データセンターについては、最適な効率性とシステムのパフォーマンスを維持しながら、自社のコアテクノロジーと緊密に統合できるセキュリティソリューションを選択することが必要です。

KASPERSKY

仕組み

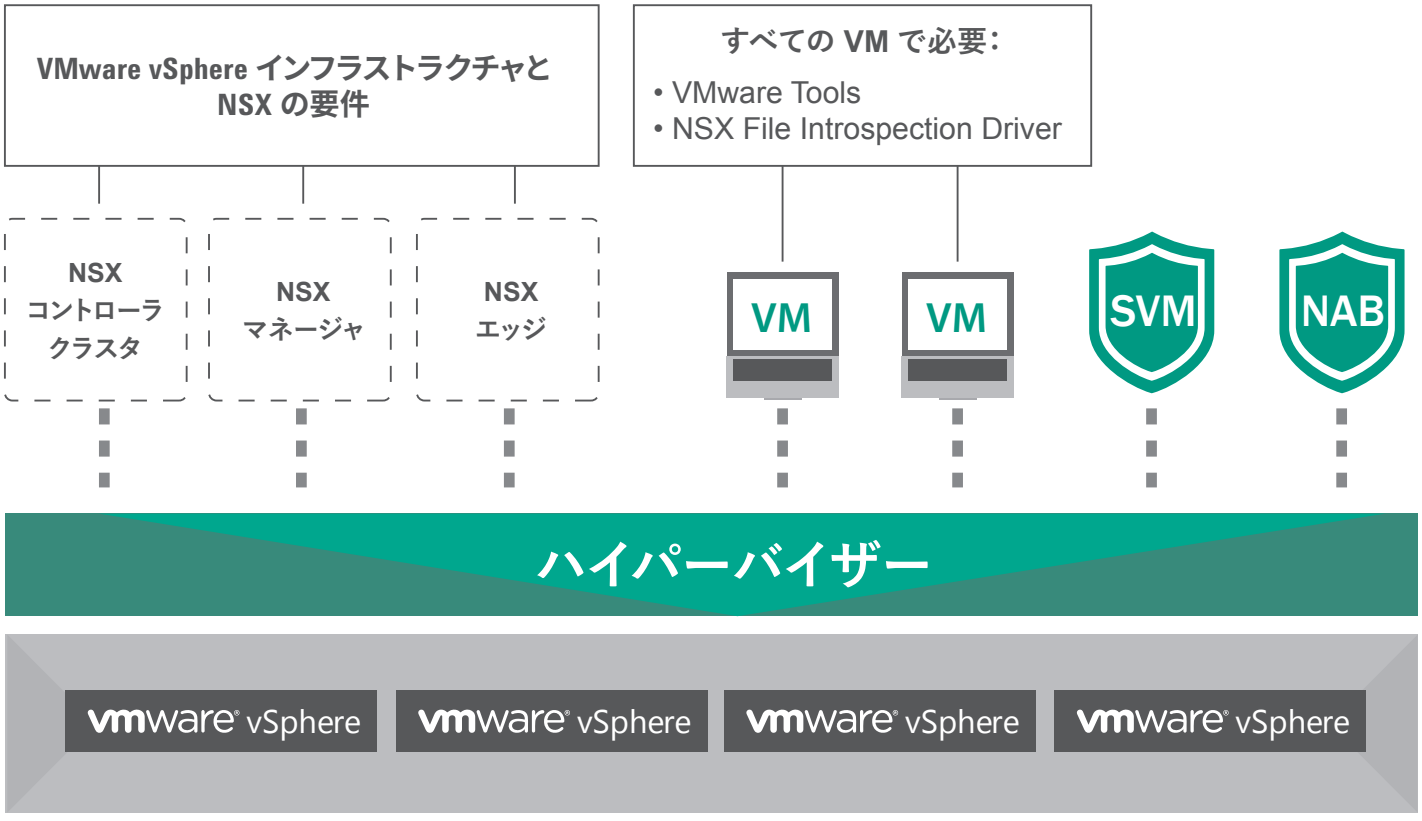
VMware NSX®は、ソフトウェア定義モデルを用いてデータセンターのネットワークを構築します。そのため、ユーザーは異なるネットワークリソースプールを操作して、わずか数秒でネットワークトポロジ全体を動的に作成または再構成することができます。その際には、「ゼロトラスト」のセキュリティアプローチを利用します。

VMware NSXプラットフォームとKaspersky Security for Virtualizationの緊密な統合によって、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、各VM（仮想マシン）と仮想化されたネットワークを最も高度な脅威から自動的に保護します。

カスペルスキーとVMwareが共同で、効率性やパフォーマンスに影響を及ぼすことなく、あらゆる規模のSoftware-Defined Data Center(SDDC)に対して強固でセキュアな基盤を確立します。

プラットフォーム統合

Kaspersky Security for Virtualization を自社のVMware NSXプラットフォームに統合することで、Software-Defined Data Center(SDDC)のインフラストラクチャ全体を最適なレベルで保護できます。どの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がなく、プラットフォームリソースに影響を及ぼさずに、継続的かつ包括的に保護します。



セキュリティ仮想マシン
- すべての VM に対するアンチマルウェア保護
- VM で従来型の（「重い」）エージェントが不要
- 効率とパフォーマンスを維持

ネットワーク攻撃防御
- 高度な侵入防止（IPS）
- Web トラフィックと URL の保護
- ネットワークのヒューリスティック分析

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。

KASPERSKY SECURITY FOR VIRTUALIZATION によって インフラストラクチャを完全に保護

Kaspersky Security for Virtualization は、高度なアンチマルウェア保護とネットワーク保護を導入することで、VMwareプラットフォームのセキュリティ機能を強化します。

永続的な保護

- 仮想サーバーとデスクトップのすべてに対しリアルタイムにアンチマルウェア保護を行います。
- 強力な仮想化IDS/IPSによって既知または未知の高度なネットワークベースの脅威を検知し、ブロックします。
- ダウンタイムなしにソリューションを導入できるため、ビジネス上重要なワークロードを継続的に運用し、保護することができます。

パフォーマンスの強化

- 仮想化環境向けに設計されたセキュリティによって、貴重なハイパーバイザーリソースを浪費せず、高い統合率を維持します。
- 専用のセキュリティ仮想マシン（SVM）をハイパーバイザーにインストールすることで、ファイルスキャンタスクをオフロードすることができ、VMの運用やパフォーマンスに与える影響を最小限に抑えます。
- 革新的な設計で特許を取得しているテクノロジーの1つであるキャッシュベースの最適化を利用して、可能な限り軽量のリソースフットプリントと最大限の密度を確保します。

効率性と保護機能の向上

- アップデートやスキャンの「ストーム」、脆弱性性、または「インスタント・オン」ギャップを解消します。
- コンパクトでしかも強力な IDS/IPS アプライアンスであるネットワーク攻撃防御によって、既知または未知のネットワークベースの攻撃（特定のエクスプロイトを利用するものを含む）を検知し、ブロックします。
- VMware NSXとの緊密な統合によって、インフラストラクチャおよびネットワークトポロジの変更に制限なくシームレスなソリューションを提供します。
- クラウドベースのKaspersky Security Network（KSN）と統合されたプロアクティブなセキュリティ機能によって、データセンター全体を最新の脅威から保護します。

優れた柔軟性と可視性

- 単一のコンソールによって物理マシンと仮想マシン、仮想化されたデスクトップとモバイル端末のすべてを一括して管理できます。
- 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がより簡単に行うことができます。

セルフディフェンステクノロジー

- SVMが自身の稼働状況を常に、自立的に監視することで、スキャンエンジンが利用可能な状態であり、いつでもア ンチマルウェアタスクを処理できる状態であることを保証します。
- セキュリティソリューションのコンポーネントおよび仮想化インフラストラクチャのノード間における通信にはSSL証明書を利用することで、サイバー犯罪者がインフラストラクチャの脆弱性を悪用することを防ぎます。

KASPERSKY

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も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。セキュリティや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。

VMware NSXとKaspersky Security for Virtualizationを利用することで、次のメリットが得られます。

- 分散型ファイアウォールとマイクロセグメンテーション機能によって、Software-Defined Data Center(SDDC)（SDDC）とそのビジネスワークロードのセキュリティレベルを強化します。
- インフラストラクチャ全体を、マルウェア、ランサムウェア、ネットワーク攻撃、「ゼロデイ攻撃」の脅威からも永続的に 保護します。その際に、システムのパフォーマンスや生産性に影響を与えることなく運用できます。
- カスペルスキーの侵入検知防止（IDS/IPS）テクノロジーによって、データセンター全体をネットワークベースの脅威から保護します。
- セキュリティポリシーを完全に統合し、NSXプラットフォームのコンソールから管理できます。
- 完全にスケーラブルで自動化されたセキュリティによって、ビジネスのより一層の柔軟性と運用効率を実現します。

Kaspersky Security for Virtualizationは、ネイティブのVMware仮想化プラットフォームテクノロジーと統合されます。それぞれのVMにエージェントをインストールする必要がないため、仮想プラットフォームのパフォーマンスに対す るシステムの影響はほとんど発生せず、管理業務を削減し、起動された各VMが瞬時に保護されます。

1 テクノロジー駆動型 インフラストラクチャ

- 仮想ネットワーク管理の自動化
- SDDC内での動的なマイクロセグメンテーション
- SDDCアーキテクチャコンポーネント間での統合

2 統合された 多層型セキュリティ

- SDDC、ネットワーク、VMの高度なセキュリティ
- VM内のすべてのファイル操作に対する高品質のセキュリティ
- ネットワークベース攻撃からの保護（IDS/IPS）
- 自動化されたスケーラブルなセキュリティソリューション

3 パフォーマンスと 効率性

- 特にVMware仮想化を念頭に置いて設計されたセキュリティ
- SDDC内のあらゆるVMやホストのパフォーマンスに影響なし
- VMの高密度化とシステム効率を維持

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

PMM-1012-201607