KASPERSKY SECURITY FOR VIRTUALIZATION

仮想化環境向けに高度な保護とパフォーマンスを両立するために最適化されたライトエージェント型セキュリティ製品

企業の IT インフラストラクチャや社内の各部門が保有するサーバーやデスクトップの仮想化が急速に進む中、サイバー攻撃の脅威からビジネス、従業員およびサービス利用者を守る必要があります。また、サイバー攻撃からの保護と同様に安定したシステムの運用が IT 管理者にとって大きな課題となっています。

Kaspersky Security for Virtualization | Light Agent は、IT の仮想インフラストラクチャ特有の要件を満たすために開発された製品で、サーバーやデスクトップの仮想化、企業が保有するデータセンターの仮想化環境向けに提供します。軽量でシステムリソースの消費を最小限に抑えたエージェントを搭載したアンチマルウェア製品である Kaspersky Security for Virtualization | Light Agent は、優れたセキュリティシステムを実現し、高度な脅威から仮想サーバーや仮想デスクトップ環境(VDI)を保護します。すべての仮想マシンを強力に保護すると同時にシステムパフォーマンスへの影響を最小限に抑え、Kaspersky Security Center の統合管理コンソールから仮想化されていない他のエンドポイントやモバイル端末などまとめて効率よく管理できます。さらに、システムの信頼性を高める機能を組み込んでいるため安定したセキュリティシステムの運用を実現します。これにより IT システム管理者やセキュリティ管理者の作業負担を軽減するとともに IT インフラストラクチャの費用対効果（ROI）を向上させます。

Kaspersky Security for Virtualization | Light Agent の特長

強力な保護機能

- 脆弱性攻撃ブロック(Automatic Exploit Prevention)やシステムウォッチャーなどのさまざまなアンチマルウェア技術によって、未知の脅威に対する監視し仮想マシンを保護します。
- クラウドベースの Kaspersky Security Network(KSN)と連携し最新の脅威情報をリアルタイムに取得し、迅速に仮想マシンを保護します。
- ネットワーク攻撃防御、ファイアウォール、ホスト型侵入防止システム(HIPS)、アンチフィッシングなどのテクノロジーと連動しネットワーク上の脅威から仮想マシンを保護します。

高いパフォーマンス

- 共有キャッシュテクノロジーによって各仮想マシン間における重複ファイルのスキャンを回避します。セキュリティレベルを低下させることなく、システムの負荷を軽減してパフォーマンスを向上させることができます。
- 一斉ウイルス検知によって発生する「アップデートストーム」、「スキャンストーム」によるパフォーマンスの低下を抑制します。また、仮想マシン間で定義データベースに差異が生じる「インスタント・オン・ギャップ」を解消するため仮想デスクトップ環境(VDI)を安全な状態で利用できます。

高い信頼性

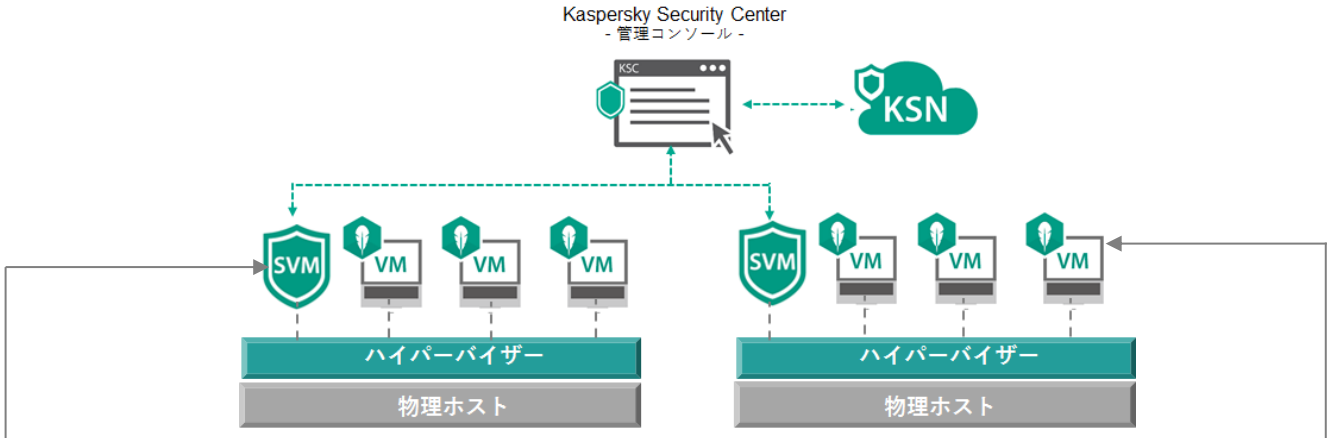
- セキュリティ仮想マシン(SVM)が停止した場合は、セルフモニタリング機能により異常が発生したプロセスの再起動を試行します。また、プロセスを再起動できなかった場合や仮想マシンと SVM 間の通信が遮断された場合は、仮想マシンのライトエージェントが他のハイパーバイザー上で稼働している SVM を検索し、自動的に接続して仮想マシンを継続的に保護します。
- 他のハイパーバイザー上の SVM を検索する際、接続されている仮想マシンの数や負荷が最も低い SVM に自動的に接続します。また、停止していた SVM が復帰すると仮想マシンは自動的に元の SVM に接続します。

効率的な運用

- 複数のハイパーバイザーに SVM を同時に配置できます。また、新しい仮想マシンが追加されると自動的に SVM に接続し、瞬時に保護を開始するため導入の作業効率が向上し、作業時間も大幅に短縮できます。
- 一元化された単一の統合コンソールから仮想化環境、物理環境、モバイル端末の保護状態を管理し、一貫したセキュリティポリシーを適用することができます。

Kaspersky Security for Virtualization | Light Agent の機能

仮想マシンには「ライトエージェント」と呼ばれる非常にコンパクトで軽量なソフトウェアエージェントのみがインストールされるだけで、高度なセキュリティ機能によって仮想化環境を強力に保護します。



Kaspersky Security for Virtualization | Light Agent の構成

信頼性のあるセキュリティシステムの運用

- **セルフディフェンス**
  マルウェアの攻撃からセキュリティ仮想マシン(SVM)とライトエージェントを保護
- **WatchDog による自己監視**
  SVM に問題が発生した場合、異常が発生したプロセスの再起動を試行
- **SVM の冗長性**
  SVM との通信が遮断された場合、ライトエージェントが他の SVM に自動接続し仮想マシンを継続保護

ユーザ環境を強力に保護

- **コントロール機能**
  - USB や周辺機器へのアクセスを制御
  - 特定の Web サイトへの接続を制限
  - アプリケーションの起動やレジストリなどへのアクセスを制御
- **ホストベース侵入防止システム(HIPS)とファイアウォール**
  アプリケーションの信頼レベルとファイアウォールと連動してアプリケーションの動作を制限
- **システムウォッチャー**
  疑わしいアプリケーションをブロック、被害を受けた場合は感染する前の状態に自動修復
- **脆弱性攻撃ブロック**
  最新の脅威に対するプロアクティブな保護
- **クラウドベースの保護**
  Kaspersky Security Network(KSN)と連動し、最新の脅威情報を活用してリアルタイムに保護

vmware PARTNER TECHNOLOGY ALLIANCE

対応プラットフォーム

ハイパーバイザー

VMware ESXi 5.5、VMware ESXi 6.0
Microsoft Windows Server 2012 R2 Hyper-V

ゲスト OS:

Windows 7 Pro / Enterprise SP1（32／64 ビット）
Windows 8.1 Pro / Enterprise（32／64 ビット）
Windows 10（32／64 ビット）
Windows Server 2008 R2 Standard SP1（64 ビット）
Windows Server 2012 （64 ビット）
Windows Server 2012 R2（64 ビット）
Windows 10（32 ビットまたは 64 ビット）

30 日間利用可能な無料試用版ダウンロード：http://www.kaspersky.co.jp/business-security/free-trials

最新情報はウェブサイトをご確認ください ► http://www.kaspersky.co.jp/business-security/virtualization

KASPERSKY

株式会社カスペルスキー

カスペルスキー Web サイト　www.kaspersky.co.jp/
ご購入相談窓口　jp-sales@kaspersky.com

製品・サービスに関するお問い合わせは下記へ

PMM-1011-201607