Kaspersky Hybrid Cloud Securityによる仮想化セキュリティ - 機能ガイド

Light Agent or Agentless?

kaspersky

エグゼクティブサマリー

仮想環境には、それぞれ特有の課題があり、さまざまなセキュリティソリューションを評価する際に、考慮する必要があります。

仮想化は、産業界全体で広く取り入れられつつあり、それにはまっとうな理由があります。必要に応じて仮想マシン（VM）を起動できるため、リソースを大幅に節約することができます。これに対して、各マシンにフル機能のセキュリティエージェントを使用して、仮想環境に「従来型の」セキュリティアプローチを適用した場合、貴重なスペースが占有され、仮想化の費用対効果（ROI）が大幅に損なわれることになります。

この問題を解決する解決策としては、仮想デバイス上でエージェントが行う計算量やメモリ使用量を削減することです。Kaspersky Hybrid Cloud Security は、エージェントレス形式と軽量エージェント形式のふたつの異なるアプローチによって、これを実現します。

このガイドでは、これらふたつのアプローチが、それぞれどのように動作するか、また、それぞれの機能や利点についても解説します。

仮想化環境のセキュリティ対策 – その課題

仮想化がますます普及するにつれ、適切なセキュリティソリューションの必要性が、明らかになりつつあります。物理環境と同じように、サイバー攻撃の影響を受けやすくなっていますが、仮想環境には特有の課題があり、さまざまなセキュリティソリューションを評価するにあたり、考慮する必要があります。

企業は、同一のセキュリティソフトウェアを運用することで、物理マシンと仮想マシンの両方を保護することができます。ただし、適切なレベルの保護機能を提供する一方で、仮想環境用に特別に設計されていない標準ソリューションは、つぎのような問題を引き起こすおそれもあります。

- **保護された各VMでの定義データベースとアクティブなマルウェア対策エンジンのレプリケーションにより、リソース消費が過大**になります。
- **ストーム：**各VMで定義データベースの更新とアンチマルウェアのスキャンプロセスが同時に発生し、リソース消費が雪だるま式に増大することで、パフォーマンスが大幅に低下してサービスへの影響が発生する場合があります。これらのプロセスをスケジュール設定して問題を緩和しようとすれば、マルウェアスキャンが後回しにされることによって、VMが攻撃を受けやすくなる「脆弱な時間帯」が生じてしまいます。
- **インスタント・オン・ギャップ：**非アクティブなVMでは定義データベースを更新できません。このため、マシン起動時から更新プロセス完了までの間、VMは攻撃に対して脆弱になります。
- **非互換性：**標準のソリューションは、VMの移行や非永続ストレージなど仮想化固有の機能を扱うように設計されていないため、これらの機能を使用するとシステムが不安定になったり、停止したりする場合があります。

課題への対応 – ふたつのアプローチ

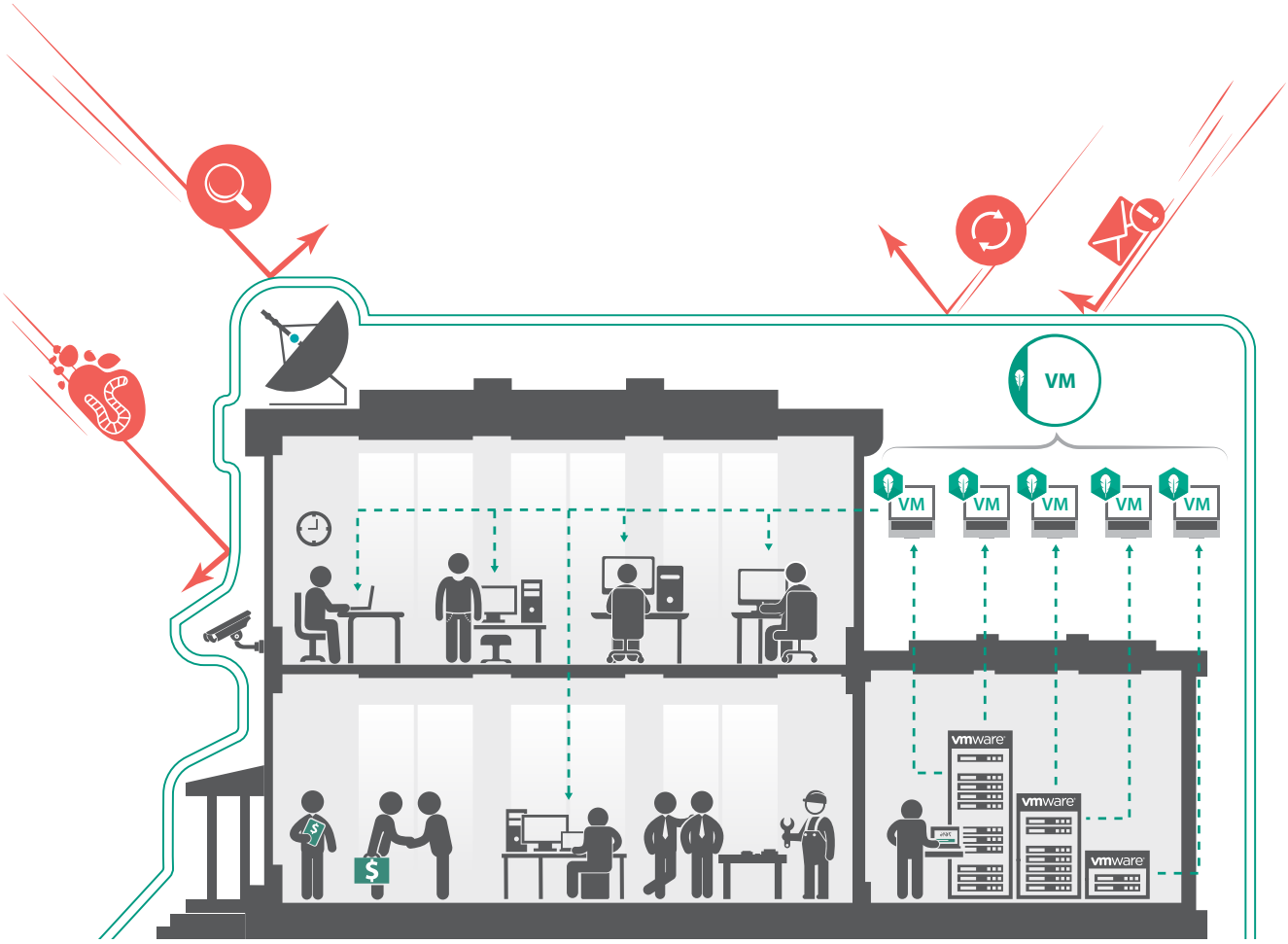
カスペルスキーの軽量エージェント形式のソリューションは、次のような様々なプラットフォームに対応しています。

- **Microsoft Hyper-V**
- **Citrix Hypervisor**
- **Citrix Virtual Apps and Desktops**
- **KVM**
- **VMware vSphere**
- **VMware NSX**
- **VMware Horizon**

仮想化テクノロジーの大手ベンダーである VMware は、仮想システムのセキュリティの重要性と、仮想化がもたらす独自機能について認識し、vSphere 仮想化プラットフォーム向けの、専用の防御レイヤーである vShieldエ ンドポイントテクノロジーを開発しました。このレイヤーが提供するサードパーティソリューション向けのセキュリティコネクタは、vShield EndpointやNSX Guest IntrospectionなどのVMware APIとネイティブ統合され、すべての仮想化資産を包含することで、適切に設計されたセキュリティソリューションによる効率的なアクセスが容易に行えます。

ひとつのホストで必要なセキュリティ仮想アプライアンス（SVA）は、アンチマルウェアスキャンエンジンとシグネチャ定義データベースを含む専用仮想マシンがひとつだけで済み、個々の仮想マシンに負担をかけることなく、リソース消費を大幅に減らすことができます。企業にとって、このアプローチの最大のメリットは、VMwareのエコシステムとの円滑なネイティブ統合にあります。

もうひとつのアプローチは、保護対象の各VMのOS内部で最適に動作する軽量エージェントを活用する、API独立型（仮想化プラットフォーム独立型）のソリューションです。この場合も、ファイルスキャンエンジンと定義データベースはセキュリティ仮想アプライアンス（SVA）で一元管理され、「軽量エージェント」テクノロジーにより、従来のフルエージェントソリューションよりも要求されるリソースは大幅に少なくなります。このソリューションは、リソース消費の点で、エージェントレス・ソリューションと従来型のフルエージェント・ソリューションの中間に位置しますが、さらに重要なことに、VMwareテクノロジーに縛られたり制限されたりすることがなく、他の一般的なプラットフォームでも使用できます。



どのように選択すべきか
Kaspersky Hybrid Cloud Security は、エージェントレス形式と軽量エージェント形式の両方を提供しており、どちらをどこに導入するか、お客様自身で選択することができます。

ソリューション - オンプレミスとクラウドの両方を提供

Kaspersky Hybrid Cloud Security は、仮想化された企業資産のための、統合型セキュリティ対策／制御を提供します。オンプレミスとパブリッククラウドのいずれにも実装でき、単一のコンソールで操作できます。

仮想化に関する費用対効果（ROI）を高めつつ、リソースとワークロードを保護するための主な方法のひとつとして、セキュリティエージェントによる各VM上のリソース使用量を最小限に抑えることが挙げられます。

Kaspersky Hybrid Cloud Security は、これを異なるふたつの方法で実行します。どちらも、同一ソリューションの一部として提供されます。

- 弊社のエージェントレス・ソリューションは、VMware環境が提供するセキュリティアーキテクチャを活用することにより、導入を簡易にするとともに、パフォーマンスを大幅に向上させることができます。
- 弊社独自の軽量エージェント・アーキテクチャは、従来のセキュリティエージェントよりもはるかに少ないリソース使用量で、仮想環境における包括的な多層型セキュリティ対策を実現します。また、主要な仮想化プラットフォームと互換性があります。

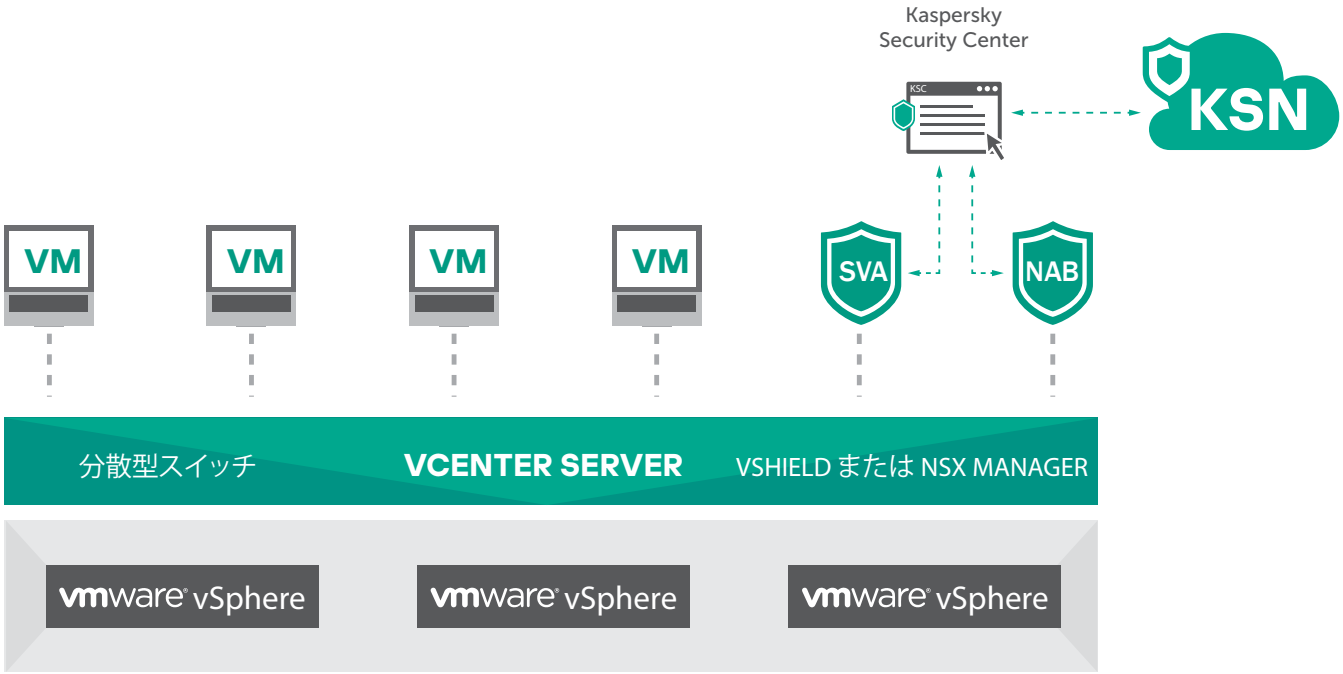
Kaspersky Security for Virtualization Agentless

Kaspersky Security for Virtualization Agentlessは、VMware vShield Endpoint テクノロジーの利点を全面的に活用できるよう、特別に設計されています。すぐに展開可能なセキュリティ仮想アプライアンス（SVA）で、受賞歴のあるカスペルスキー製のマルウェア対策エンジンを搭載しており、優れた検出率とパフォーマンスが期待できます。

クラウド支援型 Kaspersky Security Network（KSN）サービスにより、迅速な対応が可能で、0.02秒で新しいマルウェアの脅威を特定することができます。これにより、Kaspersky Hybrid Cloud Security は、最新の脅威からも仮想化環境を保護することができます。

VMware NSX 対応環境では、Kaspersky Security for Virtualization Agentless と VMware の NSX Guest Introspection とのネイティブ統合のメリットを享受できるため、セキュリティ・ソリューションがトポロジとインフラストラクチャの変更にシームレスに対応し、インフラを拡張することができます。

KASPERSKY SECURITY FOR VIRTUALIZATION AGENTLESS



高度なネットワーク保護機能として、VMware の vCloud Networking & Security コンポーネントと緊密に統合し、2番目のSVAを使用して「ネットワーク脅威対策」 機能を提供することができます。

考慮すべきふたつの重要事項

エージェントレスのアプローチには、いくつかの弱点があります。

まず、VMware vSphere は、中間的なセキュリティレイヤーである vShield エンドポイントを提供する、ただひとつの仮想化プラットフォームです。その他の仮想化プラットフォームでは、セキュリティソリューションは、マシンレベルでファイルスキャンタスクを実行するために、個々のVMのゲストOS内に、ある種のエージェントをインストールする必要があります。

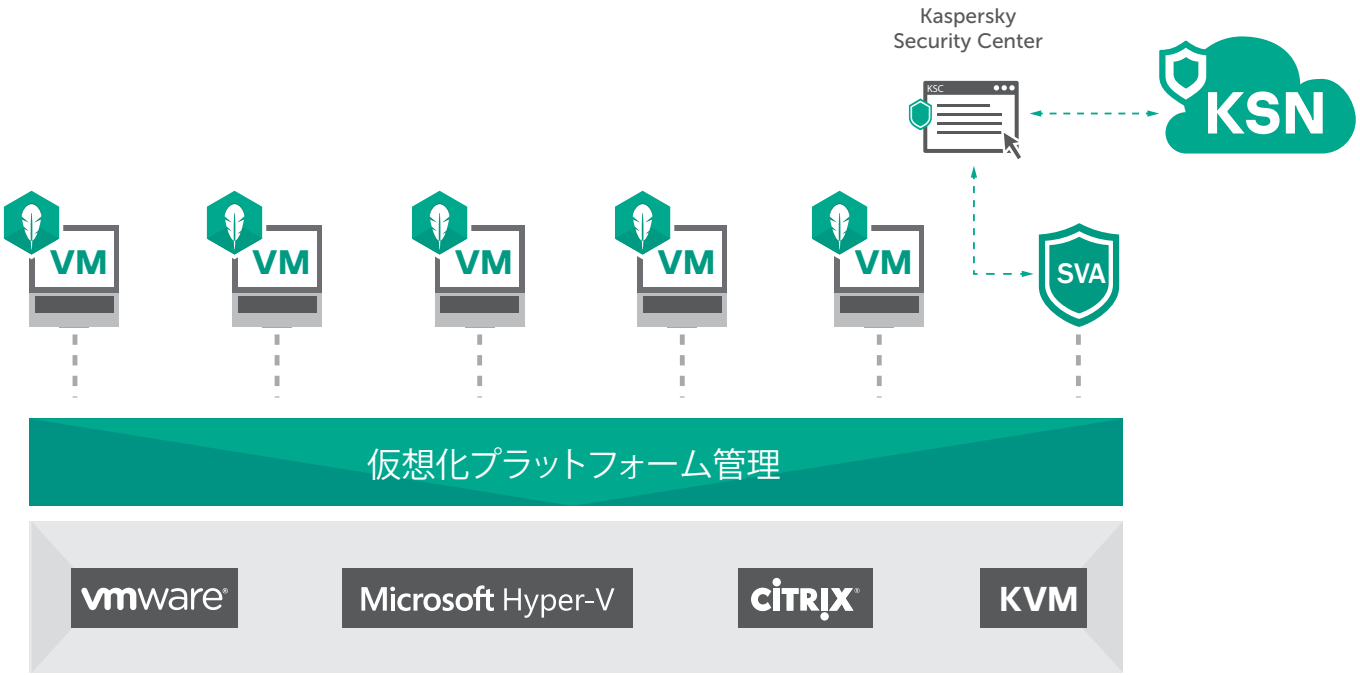
つぎに、VMware の設計の関係で、vShield Endpoint や NSX Guest Introspection などが本来備えている技術では、VMの内部プロセス、アプリケーション、Webトラフィック、または仮想化されたデバイスへのアクセスを提供することはできません。このため、インフラを保護する機能は、ファイルレベルのスキャンに限定され、個々のVMレベルで高度なマルウェアに対抗できるきめ細かい保護機能は大幅に低下します。

Kaspersky Security for Virtualization Light Agent

「軽量エージェント」によるアプローチでは、これらの制約を取り払うことができます。ファイルスキャンエンジンと定義データベースがセキュリティ仮想アプライアンス（SVA）上で一元化され、このアプリケーションのリソース使用量は、従来型のフルエージェント・ソリューションよりも少なくなります。各VM上の軽量エージェントにより、個々のVMメモリ、アプリケーション、内部プロセス、Webトラフィック、仮想化デバイスへのアクセスが可能になります。このアクセスにより、仮想化プラットフォーム全体の効率とパフォーマンスを維持しながら、高度なセキュリティ技術をVMレベルで展開することができます。

Kaspersky Security for Virtualization Light Agent は、仮想環境向けに特別に設計されており、Citrix Hypervisor、Citrix Virtual Apps and Desktops、Microsoft Hyper-V、VMware vShield、NSX、Horizon、KVMなどのもっとも一般的なプラットフォームをサポートしています。

KASPERSKY SECURITY FOR VIRTUALIZATION LIGHT AGENT



Kaspersky Security for Virtualization Light Agent は、強力な多層防御のペリメーター（境界線）を実現し、高度なマルウェアや最新の脅威でさえも排除することができます。ユーザーは、HIPS（ホストベースの侵入防止システム）、パーソナルファイアウォール、脆弱性攻撃ブロック、およびフルセットのエンドポイント制御といったテクノロジーの恩恵を受けることができます。ソリューションのアーキテクチャとしては、貴重なコンピューティングリソースを節約しつつ、攻撃対象領域を大幅に削減するというものです。

この軽量エージェントアプローチのおかげで、ハイパーバイザーのパフォーマンスに大きな影響を与えることなく、仮想サーバーやデスクトップ仮想化（VDI）などの仮想環境を保護することができるのです。したがって、マシンの集約率と使い心地の良さを維持しつつ、システムと機密性の高い企業データを完全に保護することができます。

カスペルスキーの保護テクノロジー 対仮想インフラを脅かす脅威

VMは、物理マシンと同じくらい脆弱であり、おそらくはさらに脆弱だと言えます。仮想化ネットワークの動作が超高速であるため、感染が破滅的な規模に広がる恐れがあるためです。このため、仮想インフラのセキュリティ上の弱点を特定し、高度な脅威への対応に特化した効率的なセキュリティソリューションを導入することが重要です。以下では、仮想システムにとっての潜在的な脅威に対抗するために採用されるテクノロジーについて解説します。

アプリケーションコントロールとホワイトリスト

信頼できるソフトウェアのみがVM上で実行を許可されるのであれば、マルウェアが実行される余地はありません。アプリケーションコントロールと動的ホワイトリストは、このような原理で、マルウェアが仮想化資産を破壊することを阻止します。Kaspersky Security for Virtualization Light Agent を使用すると、アプリケーションコントロールを含むエンドポイント制御を、個々のVM上で有効にすることができます。

脆弱性攻撃ブロック

システムコンポーネントや一般的なアプリケーションに見られる脆弱性を突くことは、いまなお非常に効果的な攻撃方法となっています。これらの侵入を阻止することは可能ですが、影響を受けるプログラムは高い特権レベルで動作しているため、その動作制御が制約を受ける恐れは存在します。

このような形の脅威に対処するもっとも効果的な方法は、標的となる脆弱性がエクスプロイトによって悪用される前に、未然に阻止することです。パッチ未適用によって脆弱性がもたらされる危険を迅速に回避するため、Kaspersky Security for Virtualization Light Agent は、脆弱性攻撃ブロック（AEP）テクノロジーを実装しています。脆弱性攻撃ブロックは、Adobe Reader、Internet Explorer、Microsoft Office および Java など、VDIのような重要の環境で標的になりやすいアプリケーションを集中的に監視し、追加のセキュリティ層によって未知の脅威に対する監視と保護を行います。

このテクノロジーの効率性は、MRG Effitas 研究所が実施した独自試験で立証されており、他のすべての保護コンポーネントをオフにしても、カスペルスキーの AEP テクノロジーはエクスプロイトを使用する攻撃に対して100%有効のままであったことがあります（Real World Enterprise Security Exploit Prevention、MRG Effitas、2015年3月を参照）。未知のゼロデイエクスプロイトでさえも、この優れたテクノロジーの前では、阻止されてしまいます。

MRG Effitas 研究所が実施した独自試験では、他のすべての保護コンポーネントをオフにしても、カスペルスキーのAEPテクノロジーはエクスプロイトを使用した攻撃に対して100%有効であったことがあります。

脆弱性診断とパッチ管理

Kaspersky Vulnerability and Patch Managementは、ネットワークに接続しているエンドポイントやアプリケーションに関する包括的な情報を提供します。導入されているソフトウェアのバージョンに関するデータが収集され、アップデートが必要かどうか、パッチの適用が必要な脆弱性があるかどうかを判断します。特定された脆弱性に対し、パッチはもっとも重大なものから、アップデートは重要性の高いものから適用されるよう自動的に優先順位が付けられます。このツールを利用して脆弱性がシステムに与える影響を正確に把握することができます。

システム整合性の保証

これらのシステムは、アプリケーションコントロールおよびエクスプロイト防止テクノロジーと連携して、VMの状態や構成の変化を監視するために使用することができます。また、コンプライアンス上の理由から、必要になることもよくあります。

システム整合性保証テクノロジーには、ファイル変更監視、レジストリ整合性監視、仮想化 Windows Server のベースライン管理が含まれます。

ネットワークセキュリティ

ネットワークベースのサイバー脅威により、攻撃者はネットワークに関する重要な情報を入手し、標的となるシステムのリソースにアクセスして、重要なプロセスを妨害し、その円滑な運用に影響を与えるおそれがあります。これらの脅威には、ポートスキャン、DoS（サービス拒否）攻撃、バッファオーバーラン攻撃などの悪意のあるアクションが含まれます。弊社のエージェントレス・ソリューションと軽量エージェント・ソリューションでは、どちらにもネットワーク保護テクノロジーが組み込まれています。Kaspersky Security for Virtualization Light Agent は、組み込みのHIPS（ホストベースの侵入防止システム）と追加の独自技術を使ってネットワーク保護機能を拡張し、不透明な仮想化トラフィックに隠れている恐れのある脅威など、外部や内部からのネットワーク攻撃に対抗することができます。

Kaspersky Security for Virtualization Agentless もこの問題に対処し、VMware 統合を活用して、ネットワーク攻撃防御を実装します。これは、典型的な攻撃活動の兆候がないかネットワークトラフィックを監視するように設計された専用の仮想アプライアンスです。

ふるまいをもとにした保護

Kaspersky Security for Virtualization Light Agent は、仮想マシン（VM）のメモリへの侵入をブロックできる、さまざまなテクノロジーを備えています。これには以下のものが含まれます。

- プログラムの動作を監視し、システムイベントを追跡することができるシステムウォッチャー
- マルウェアのアクティビティに特徴的な動作パターンを識別することができるBehavioral Stream Signatures
- アプリケーションによるプロセスインジェクションを含め、一方的な変更を制限することができる特権制御

これらのツールを使用すると、ホストベースの侵入防御システム（HIPS）が、VMメモリ内の不正なプロセスを追跡し、停止させることができるようになります。

ファイルレスマルウェア対策

ファイルレスマルウェアはディスク上に本体を直接格納しません。このタイプのマルウェアは、その検知と修復が複雑化していることから、2017年にはより一般的になりました。近年、このような手法は標的型攻撃に限定されていましたが、現在の脅威の状況ではますます増大しており、カスペルスキーにはtrojan-clickerの新しいタイプまたはファイルレスコンポーネントをもつアドウェアも登録されています。

メモリ内のプロセスを監視し、疑わしく危険なアクティビティに関与しているプログラムを即座にブロックすることのできる、高度なマルウェア対策技術が必要です。

悪意のあるWebサイトに対する対策

一般的な感染源のひとつとして、悪意のあるWebサイトや感染したWebサイトを挙げることができます。これが仮想化サーバーに影響を与えることはめったにありませんが、VDI環境に深刻な脅威をもたらす恐れがあります。そして企業ユーザーが、このことを十分に理解していないことがあります。この対策として、カスペルスキーのWeb保護テクノロジーが有効です。

フィッシング対策では、Kaspersky Security Network（KSN）を介して情報が収集され、その情報は、世界中の何百万もの自発的なKSN利用者の協力により、絶えず更新されています。この情報にもとづいて、危険であると報告されたWebサイトには、ユーザーはアクセスできないようになっています。ロードされたページのソーステキストを分析し、悪意のあるコードの兆候を検出するヒューリスティックエンジンのおかげで、まだ発見されていないフィッシングサイトもブロックすることができます。

ウェブコントロールは、ネット利用を管理することができ、ソーシャルネットワーク(SNS)、音楽ファイル、ビデオファイル、社外との Web メール、コンテンツが不適切であったり組織方針に反している Web サイトへのアクセスをブロックすることができます。従業員の役割に応じてさまざまなポリシーを展開し、完全なブロックを適用するか、一定の期間だけアクセスをブロックするか、などの設定をすることができます。

マルウェア実行可能ファイルをブロック

巧妙に作られた添付ファイルが、電子メール、感染したマルウェアによって作成された一時的な実行可能ファイルを通して送られてくることがあります。このため、基本的な脅威に対処できるマルウェア対策が必要不可欠です。

強力なマルウェア対策エンジンは、Kaspersky Security for Virtualization のエージェントレス構成と軽量エージェント構成のいずれにおいても中核をなす存在ですが、保護されたVMのファイルにアクセスするためには、さまざまな手段が使用されます。

アンチルートキットと修復テクノロジー

ルートキットとは、悪意のあるコードとアクティビティが検知されないようにさまざまな技法を駆使し、アンチウイルスによる修復に対抗する悪意のあるプログラムのことです。アンチルートキットテクノロジーは、カスペルスキーの次世代型多層保護アプローチの一部であり、ルートキットプログラムによるアクティブな感染を検知して、この種の感染からシステムを修復します。

エージェントレス形式と軽量エージェント形式のどちらがよいか？

Kaspersky Security for Virtualization を使用すれば、仮想化環境に対して、単一のライセンスで適切にセキュリティを展開することができます。エージェントレス形式、軽量エージェント形式、または両方の組み合わせになります。

その答えは、どのような仮想化プラットフォームやプラットフォームを使用しているか、また、特定のインフラ、セキュリティターゲットによっても異なります。仮想化環境の構築に使用されたハイパーバイザーは問いません。Kaspersky Security for Virtualization Light Agentを使用して、仮想サーバーとVDI環境を保護することができます。また、最重要とまではいえない VMware ベースのサーバーについては、Kaspersky Security for Virtualization Agentless の使用をご検討いただくこともできます。

エージェントレス形式、軽量エージェント形式、または両方の組み合わせと、仮想化環境の各部分に、単一のライセンスで適切なアプローチを展開することができます。従来型のエンドポイントエージェントをアクティブ化することもでき、物理インフラから段階的に移行することもできます。

仮想化プラットフォームの組み合わせや、使用するアプローチに関わりなく、仮想マシンと物理マシン、およびパブリッククラウドのワークロードは、単一の統合管理インターフェイスである Kaspersky Security Center を通して一元的に容易に管理することができます。また、クラウドベースのセキュリティサービスである Kaspersky Security Network を利用することで、高度な脅威も、ほぼ瞬時に検出することができます。

Kaspersky Hybrid Cloud Security:
www.kaspersky.com/hybrid
サイバー脅威ニュース：www.securelist.com
ITセキュリティニュース：blog.kaspersky.co.jp
中規模企業向けサイバーセキュリティ：
www.kaspersky.co.jp/small-to-medium-business-security
大企業向けサイバーセキュリティ：
www.kaspersky.co.jp/enterprise-security

www.kaspersky.co.jp

カスペルスキーは実績があります。カスペルスキーは独立性を確保しています。カスペルスキーは透明性を確保しています。カスペルスキーは、テクノロジーが私たちの生活をよりよくすることを願い、世界がより安全になるよう取り組んでいます。カスペルスキーがセキュリティに取り組む動機はまさしくそこにあり、世界のどこにいても、誰もが、テクノロジーの限りない恩恵を受けられるようにしたいと願っております。より安全な未来のために、サイバーセキュリティをお届けいたします。

詳しくはkaspersky.co.jp/transparencyをご覧ください

Proven.
Transparent.
Independent.