2020

Proven protection and borderless orchestration for your hybrid cloud

kaspersky

詳しくは kaspersky.co.jp
#truecybersecurity をご覧ください

Kaspersky Hybrid Cloud Security

今日、仮想化は、柔軟性や効率を高めようと考える企業が広く導入しています。次の段階は、クラウドコンピューティングです。クラウドコンピューティングは、複雑なインフラサポートの制約を緩和し、今までにない効率化を実現します。しかし、クラウド化にはリスクや複雑さがつきもので、それらのうち、いくつかは新しいもので、また、いくつかは従来のものと共通です。

Kaspersky Hybrid Cloud Security は、クラウド化のさまざまな段階やシナリオで一元的なセキュリティを実現します。クラウドへの移行とネイティブクラウドのどちらのシナリオにも適しており、オンプレミスやデータセンター、またパブリッククラウド環境においても物理と仮想の両方のワークロードを保護します。また、仮想化とサーバー機能の両方を念頭において開発されており、システムパフォーマンスを損なうことなく、既知および未知の高度な脅威に対抗できる、バランスの取れたセキュリティ対策となっています。

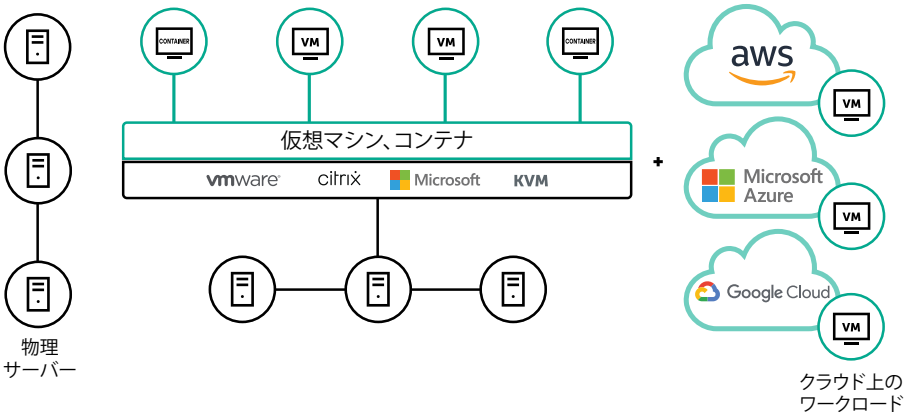
クラウドを採用した企業にとっての主な課題

- インフラがますます複雑になるにつれ、透明性が低下してしまう可能性
- 信頼性の高い安全対策の鍵となる多層アプローチを、単一の製品で実現している例は、多くない
- 従来の「重い」セキュリティエージェントでは、貴重なシステムリソースを浪費
- サイロアプローチにより、管理やセキュリティに関する課題が新たに発生
- マルウェアやランサムウェアは、物理的なエンドポイントだけでなく仮想エンドポイントも攻撃
- 個人データを保護するために適切なサイバーセキュリティ対策を実施しておかなければ、法的な問題に発展するリスクあり

Kaspersky Hybrid Cloud Security が選ばれる理由

- 物理、仮想、クラウド上のワークロード向けに設計
- さまざまなタイプのワークロードに対応できる統合型多層セキュリティ
- 機敏に動作し一貫性のある自動化セキュリティで、AWS Azure や Google などのパブリッククラウドに対応
- セキュリティのためのツールが充実しており、クラウドにおける共同責任の一助に
- ハイブリッドクラウド全体を網羅するシームレスなセキュリティオーケストレーション
- 複数の第三者機関によるテストに参加し、継続的に高評価を獲得[1]

主な利点



セキュリティのレベルを落とすことなく、安全なクラウド化を実現できます

- 特許取得済みのテクノロジーと、受賞歴のあるセキュリティエンジンにより、物理、仮想化、クラウドベースにおけるワークロードを保護することができます。
- 機械学習を活用した多層型でリアルタイムの保護機能により、データ、プロセス、アプリケーションを、新たな脅威から保護することができます。
- データ保護規制に関連する法的なリスクや、社会的評価に関するリスクを低減するのに役立ちます。

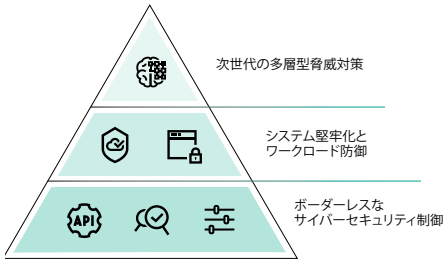
リソースと投資を最大限に活かします

- エージェントレス形式または軽量エージェント形式のセキュリティ対策でパフォーマンスを損なわず、物理ネットワークおよびSDN（Software Defined Networking）における仮想化された資産を保護することができます。
- パブリッククラウドとのネイティブな統合により、アプリケーション、OS、データ、ユーザーワークスペースを、小さなリソースで保護することができます。
- 物理リソースも仮想リソースも、ひとつの視点から管理するため、導入やメンテナンスにかかる工数を削減することができます。

1 これらのテストは、Kaspersky Hybrid Cloud Security と同じ脅威対策テクノロジーを使用している数々の他のカスペルスキー製品も対象としています。詳しくはこちらをご覧ください kaspersky.co.jp/top3

主な機能

主な機能	説明
多層型脅威対策 カスペルスキーの次世代のマルウェア対策には、プロアクティブに動作するセキュリティテクノロジーがいくつも組み込まれており、業務に重要なワークロードを脅かすサイバー攻撃から防御します	
グローバルな脅威インテリジェンス	脅威に関する状況に変化がみられてもリアルタイムで把握し、常に最新の保護を確保することができます。
機械学習	グローバルな脅威インテリジェンスのビッグデータは、機械学習アルゴリズムと当社エキスパートの連携によって処理され、誤検知を最小限に抑え、高い検出レベルを誇ります。
Web上の脅威やメールによる脅威から保護	仮想デスクトップやリモートデスクトップが安全に機能するよう、電子メールやWebからもたらされる脅威から、デスクトップを守ります。
Windowsイベントログ監視	サイバー攻撃の可能性がある異常な動作がないか、内部ログファイルを監視します。
ふるまい分析	アプリケーションやプロセスを監視し、ファイルレスのマルウェアやスクリプトベースのマルウェアなど、高度な脅威から保護します。
修復エンジン	必要に応じて、ワークロード内で行われた悪意のある変更をロールバックします。
脆弱性攻撃ブロック	OSやアプリケーション（Adobe ReaderやJavaなど）の脆弱性を悪用した攻撃の防御に特化したテクノロジーで、エクスプロイト特有の動作を識別してブロックします。
ランサムウェア対策	重要なビジネスデータを人質に取ろうとする試みに対抗して仮想化ワークロードを保護し、影響を受けたファイルを暗号化前の状態にロールバックし、リモートより試行された暗号化攻撃をブロックします。
ネットワーク脅威対策	ネットワーク攻撃を検知して阻止します。
コンテナ保護	侵入を許したDockerコンテナやWindowsコンテナを通して感染がハイブリッドITインフラに広がらないようにします。
システム堅牢化	
アプリケーションコントロール	ハイブリッドクラウドワークロードをデフォルト拒否モードでロックダウンして、システムを堅牢化し、動作するアプリケーションの範囲を正当で信頼できるものだけに限定できます。
デバイスコントロール	クラウドワークロードにアクセスできる仮想デバイスを制御します。
ウェブコントロール	仮想デスクトップとリモートデスクトップによるWebリソースの使用を制限することで、リスクを低減し、生産性を向上させます。
ホストベース侵入防止システム（HIPS）	起動されるアプリケーションに対して信頼カテゴリをあてはめ、重要リソースへのアクセスを制限して機能を限定することができます。
ファイル変更監視	重要システムのコンポーネントやその他の重要ファイルの整合性を確保できているか監視します。
脆弱性診断とパッチ管理	脆弱性診断、パッチとアップデートの配信、インベントリ管理、アプリケーションの展開など、セキュリティ、システム設定、管理に関する必要不可欠な作業を一元化し、自動化します。
ボーダレスな可視性	
セキュリティの一元管理	Kaspersky Security Center を活用することで、オフィス、データセンター、クラウドなど、インフラ、エンドポイント、サーバー全体を単一の視点から見渡すセキュリティ管理が容易になります。
クラウドAPI	AWSやAzureといったパブリックなクラウド環境とのシームレスな統合により、インフラの検出、自動化されたセキュリティエージェントの展開、ポリシーベースの管理が可能になるほか、インベントリやセキュリティのプロビジョニングが容易になります。
柔軟な管理	マルチテナンシー、権限ベースのアカウント管理、役割ベースのアクセス制御といった機能を備え、単一サーバーからの統合オーケストレーションの利点を維持して、柔軟性を実現します。
SIEMとの統合	イベント情報をSIEMにエクスポートしてSIEM上での一元的な蓄積・管理を可能にし、その情報を活かしてセキュリティ上の脅威となる事象をいち早く分析・検知できるようにします。



クラウドの統合セキュリティ：
パブリッククラウド
- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud Platform

プライベートデータセンター
- VMware NSX
- Microsoft Hyper-V
- Citrix Hypervisor
- KVM
- Proxmox

VDI環境
- VMware Horizon
- Citrix Virtual Apps and Desktops

サーバーOS
- Windows
- Linux

デスクトップOS
- Windows
- Linux

aws

Microsoft Azure

vmware

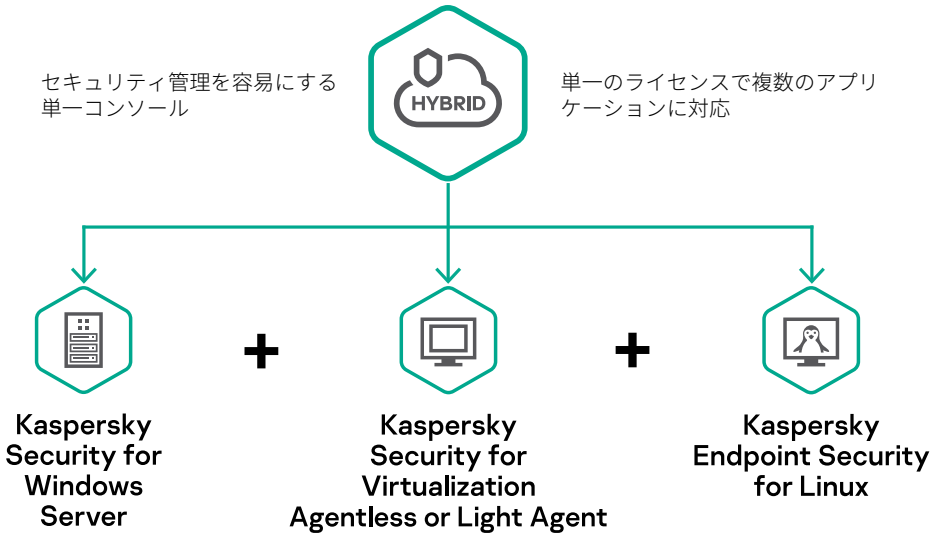
citrix

Google Cloud

KVM

ハイブリッドインフラ環境において、一貫した可視性と制御を実現します

- ハイブリッドクラウド全体で、容易なセキュリティのプロビジョニングとポリシーベースでの運用が可能になります。
- 管理性とセキュリティのオーケストレーションは、複数のクラウドにわたってシームレスに機能します。
- さまざまなロケーションの、さまざまなワークロードについて、最先端の脅威に対抗できる可視性、コントロール、全体的な保護を実現します。



Kaspersky Hybrid Cloud Security は、IT環境の変革を支援し、その簡素化を実現するため、受賞歴があり業界で広く認められているセキュリティテクノロジーを数多く採用しています。物理から仮想、仮想からクラウドへの移行を安全に行うことができ、可視性と透明性においてセキュリティオーケストレーションを実現することができます。

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.