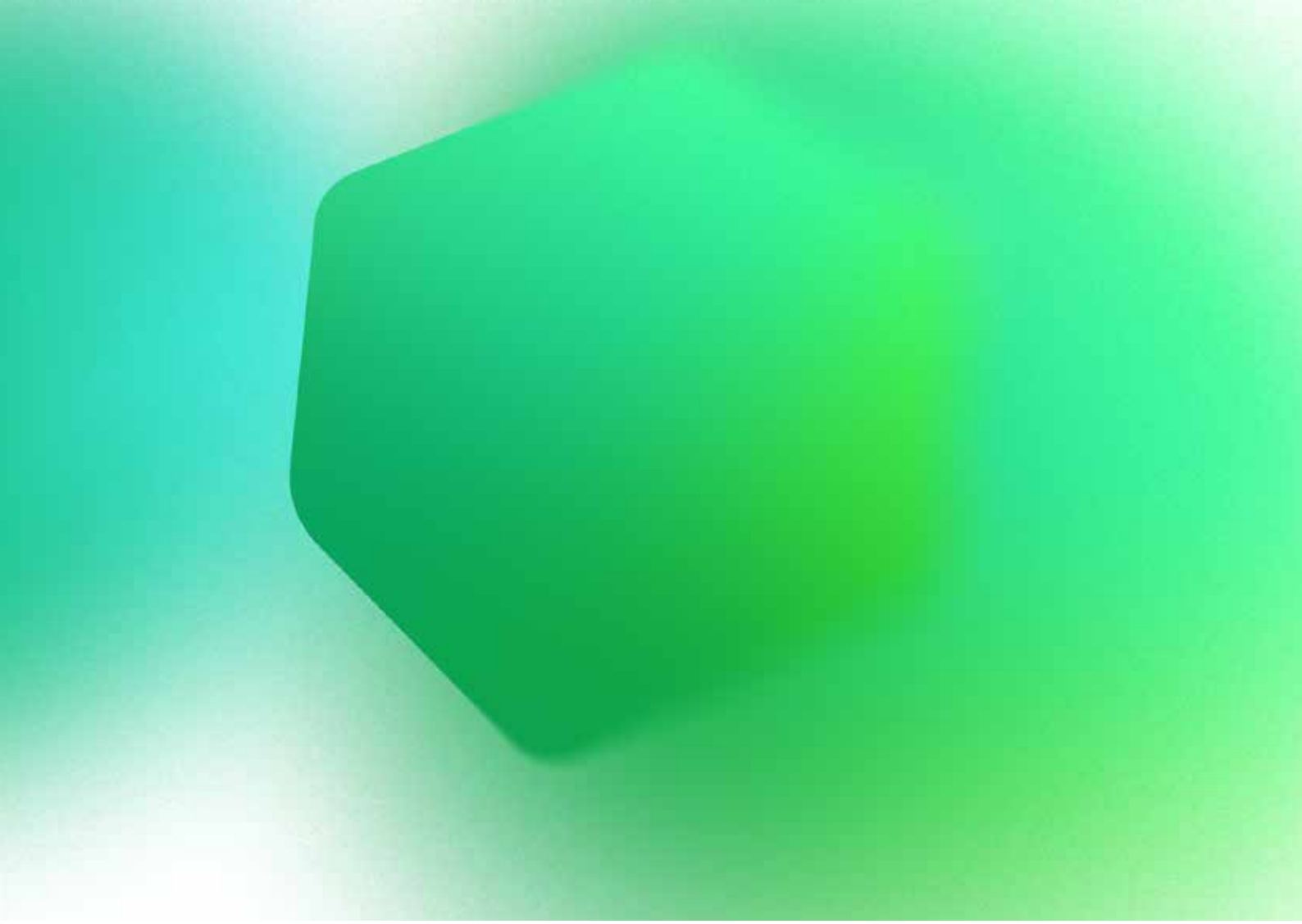


Protection where you need it: securing your move to the cloud

kaspersky

詳しくはこちら：www.kaspersky.co.jp

企業 IT の様相を一変させるデジタルトランスフォーメーション

企業は、デジタルトランスフォーメーションを推進してクラウド内にITインフラを構築する際、次の極めて現実的な問題に直面します。企業の資産に対するコントロールを保持できるでしょうか?それとも手放すことになるのでしょうか?移行の妨げとなる問題を解消して、恩恵を享受できるようにするにはどうすればいいでしょうか?このような変革を実行する際に、パフォーマンスへの影響を最小限に抑えつつ、多額の投資から最大限の利益を得るようにするためにはどうすればいいでしょうか?

デジタルトランスフォーメーションには、さまざまな形態があります。クラウドに新しい IT 機能を一から構築する方法もあれば、既存のサーバーやアプリケーションを移行する方法もあります。また、クラウドへの移行により、古いハードウェアの使用停止を促進する方法もあれば、サービスの自動スケーリングを実現し、働き方の急速な変化に対応するなどの方法もあります。

今まさに、かつてないほどの意味を持つクラウドへの移行

クラウド導入が利用者にとってどのような意味を持つかが、今まさに実感されつつあると言えます。

2020 年は、新型コロナウイルスの感染拡大を受けてリモートワークへの移行が一気に進みましたが、パブリッククラウドプロバイダーはノードを猛スピードで稼働させることで、急激な需要増加にも円滑な対応ができています。また、在宅勤務により、企業活動のあらゆる面において中断のないオンラインアクセスと通信にいかに依存しているか、またハードウェア層に物理的にアクセスしなくても、ITインフラをいかに容易に管理できるか(あるいは管理できないか)ということが改めて認識されています。この最新の危機下にあって、クラウド導入をすでに実現している企業はその恩恵をまさに実感しており、クラウドプロバイダーは「影の立役者」と称えられています。[1]

新型コロナウイルスの感染が拡大する中で、勢いを増しているもう 1 つの技術は、VDI(デスクトップ仮想化)です。多くの企業では、リモートワークに必要なラップトップやコンピューターなどの機器を全従業員分は調達できないという事態に直面し、従業員に対して私物のデバイスを業務に使用するように求めせざるを得ませんでした。その一方で、VDI をすでに導入している企業では、従業員に対してさまざまなデバイスで仕事することを許可しながら、安全かつ制御された方法で業務を継続することが可能になっています。また、VDI では、万が一デバイスの動作が停止した場合にもさまざまなバックアップオプションが用意されているため、利用できる別のデバイスでほぼ即座に仕事を再開させることができます。

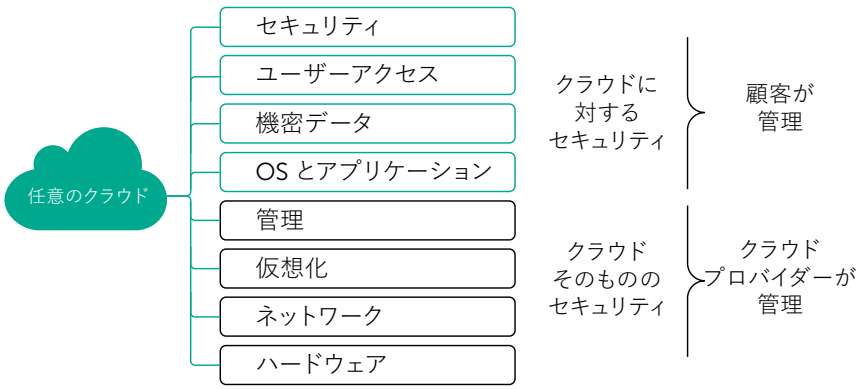
この困難な時期に、クラウドベースの業務形態は事業の継続性と回復力に関して明らかな恩恵をもたらすことが実証されたため、極めて多くの企業が今後いずれかの時点でクラウドに移行していくと言えるでしょう。ITインフラを変革してクラウドへの移行を進めるプロセスでは、物理、仮想、クラウドの異なるプラットフォームが混在する複雑なハイブリッド環境で作業をする移行途上の段階が生じます。このようなハイブリッド環境では、異なるプラットフォームの管理、調整、サポートを同時に行っていく必要があります。

自前のITインフラが無くなっていくとき

以前は、自前のネットワークの構築者であり、所有者でもある企業自身が、検出ツールを実行して、ワークステーション、サーバー、サービス、アプリケーションのインベントリを作成できた時代もありました。自前のネットワークに対するコントロールを有していたため、これは比較的容易なことでした。ケーブルをたどることが可能であり、ハイパーバイザーの設定を掘り下げてソフトウェア定義ネットワークの範囲を調べることも可能でした。

IaaS の世界では、そのようなことはできなくなっています。そしてこれは、いいことなのです。なぜなら、ハードウェア層はIaaS プロバイダーに任せることができるからです。

セキュリティ共有責任モデル



1 https://www.crn.com/news/cloud/in-coronavirus-crisis-public-cloud-is-an-unsung-hero-

そのような責任がなくなると同時に、利用者が自分でコントロールしたり、実際にその目で確認したりすることもできなくなりました。以前のやり方を続けることもまだ可能です。VPN を使用して各ITインフラに接続させることで、仮想化されたワークロードを扱うのとほぼ同じ方法でクラウドに移行された IT 資産を扱うことができます。しかし実際には、そうしないケースがほとんどです。なぜなら、新しいやり方ではなく以前のやり方を選択するたびに、新しいアプローチの利点もあきらめることになるからです。

新しい現実に対処するための新しいツール

ここでジレンマが生じます。以前のツールは、ハイブリッド環境では十分に機能しません。その一方で、新しいツールは移行面に重点が置かれているため、通常、ワークロードのセキュリティは、移行後の問題として処理されます。大半の利用者にとって唯一の選択肢は、ITインフラごとに、さまざまなセキュリティツールを使用することです。その結果、責任を負う領域が拡大し、可視性の問題が生まれ、管理不全の状態に陥って、サイバー犯罪者が好むセキュリティギャップが生じることになります。

デジタル化を進展させるには、使用するツールを変えて新しい現実に柔軟に対応し、オンプレミス、物理、仮想、「クラウド内」のいずれにあるかにかかわらず、さまざまなプラットフォームにわたり役立つ機能を取り入れる必要があります。「クラウド内にある」という概念は一般的なものになりつつありますが、「誰か他の人のコンピューター上」と捉えているユーザーもいます。

すべてのワークロードにわたる一貫した可視性

カスペルスキーでは、セキュリティギャップとそれを悪用した脅威について考慮しています。確かに、ITインフラ全体を管理することも、ポリシーを適用して構成の統一性を確保することもできないということは、オペレーティングシステムや業務アプリケーションの脆弱性よりも大きな問題です。ソフトウェアの脆弱性は、ソフトウェアベンダーやセキュリティベンダーによって修正されますが、複数のセキュリティ管理コンソールで設定にばらつきがあるために、関心を持つ攻撃者にとって格好の侵入口を生み出していることは、誰が見つけるというのでしょうか？

カスペルスキーでは、この問題を解決する最善の方法は、「単一画面」の管理コンソールであると考えています。環境における物理、仮想、モバイル、クラウドのすべての要素のセキュリティをシームレスに管理できれば、人為的ミスがセキュリティギャップにつながる可能性は極めて低くなります。

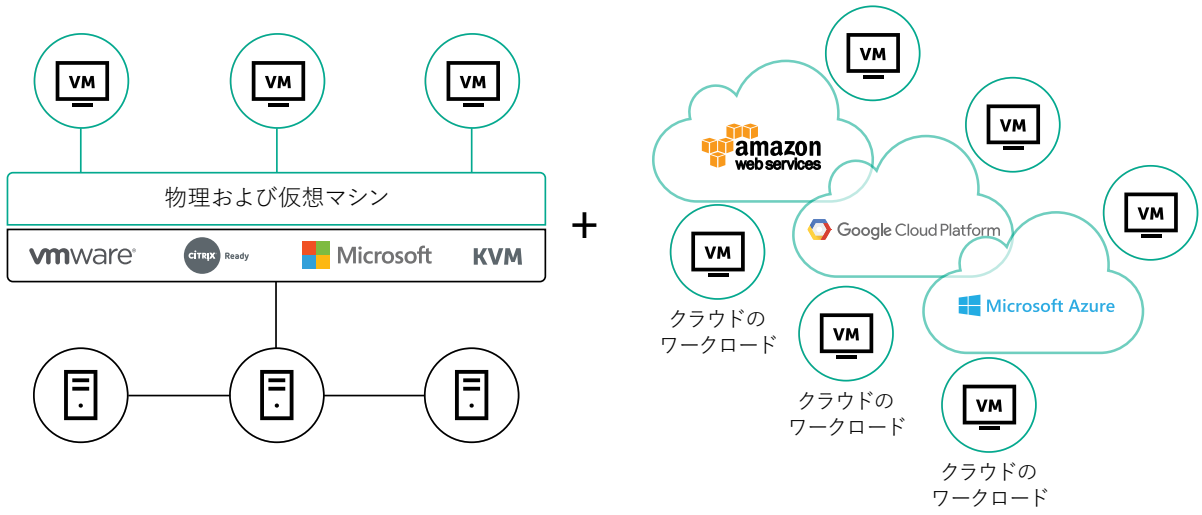
複雑なハイブリッド型環境向けのセキュリティ

Kaspersky Hybrid Cloud Security は、一貫性がある「単一画面」による可視性を提供し、移行プロセスの各段階とそれ以降にわたり、クラウドベースのワークロード、仮想環境、物理マシン全体を一元管理できるようにすることで、ハイブリッド 環境を保護します。システムのパフォーマンスに影響を与えることなく、要件に準拠した状態が維持されます。ポリシーが統一された単一の管理コンソールにより、管理の時間と煩雑さが軽減されて、セキュリティギャップを解消することができます。
パブリッククラウド – 可視性と利便性

Kaspersky Hybrid Cloud Security では、以下によって、パブリッククラウドへの展開に向けたオーケストレーションが簡素化されます。

- 任意の数のサブ環境に展開し、管理サーバー階層で体系化できる単一画面の管理コンソールにより、非常に複雑な構成にもギャップを生じさせることなく対応できます
- AWS、Microsoft Azure、Google Cloud プラットフォームとの API 連携
- Windows ワークロードと Linux ワークロードの保護
- クラウド環境のインベントリ、およびセキュリティエージェントの自動セキュリティプロビジョニング容易化

自動検出と展開



クラウド API と連携することで、自動化と柔軟な管理を実現します。管理コンソールでは、指定されたアカウントで実行されるすべてのインスタンスを確認し、その情報をセキュリティエージェントのデプロイやセキュリティポリシーの適用に活用できる必要があります。新しいインスタンスが作成されると、IAM ロールまたはスクリプト展開のメカニズムを使用して、インスタンスが作成された直後からすぐに保護されるようにすることができます。

自動スケーリンググループのサポート

Kaspersky Hybrid Cloud Security では弾力性のある設定が可能なため、新しいインスタンスが作成されてクラウドで実行されることにより負荷が増加した場合にも、ソリューションが自動的に対応します。API と自動スケーリングポリシーによって、各自動スケーリンググループに含まれるすべての新しいインスタンスに対してセキュリティをデプロイし、組織で設定されたポリシーが順守されるようにします。

コンテナー用セキュリティ

パブリッククラウドの重要なユースケースの 1 つに、DevOps があります。コンテナー・テクノロジー（Docker など）が導入されて幅広く（管理が厳格でないことが多い）使用されることにより、セキュリティ管理者は課題を抱えることになります。Kaspersky Hybrid Cloud Security では、Docker コンテナーと Windows コンテナーをセキュリティで保護し、攻撃者によって脆弱なコンテナーや悪意のあるコンテナーコンポーネントが組織内部に侵入する足がかりとして利用されることを防ぎます。コンテナ化におけるホストメモリの保護、コンテナーおよびイメージスキャンのタスク、スクリプト可能なインターフェイスによって「コードとしてのセキュリティ」アプローチが可能になり、CI/CD（継続的インテグレーションと継続的デリバリー）パイプラインにセキュリティタスクを統合できます。

仮想化 – データセンターのセキュリティと効率性のバランスを確保

パブリッククラウドによって IT の様相が一変する可能性がある一方で、オンプレミスの仮想化とプライベートクラウドに大きな変化は見られません。企業のリスクを管理するということは、すべての仮想マシン（VM）と仮想ストレージをセキュリティで保護することを意味します。ただし、パブリッククラウドとプライベートクラウドでは、セキュリティの目標（サイバーリスクを軽減および管理すること）は同じでも、移行プロセスで直面する課題は異なります。

オンプレミスのハードウェアリソースを最大限に活用して、物理マシンで達成できる以上のことを実現することが仮想化の目的です。そのため、仮想環境を保護するように特別に設計された適切なセキュリティを適用することで、仮想化への投資の見返りとしてパフォーマンス上の恩恵を受けられるようにする必要があります。効果的な仮想化セキュリティでは、セキュリティタスクを一元化し、入手できる情報を再利用して重複を排除し、VM 間の負荷を分散し、仮想プラットフォームによって提供される可能性を生かしてパフォーマンスに対する影響を最小限に抑えながら最大限の保護を実現する方法を見つける必要があります。

仮想サーバーと VDI の保護

Kaspersky Hybrid Cloud Security は、仮想環境での使用向けに特別に設計されており、余計な処理やデータが排除されていることから、従来型のエンドポイントセキュリティソリューションを使用する場合と比べて、仮想ハードウェアのリソースが最大 30 % 削減されます。このソリューションは環境について学習すると、多くの場合、追加のサイクルに時間を費やすことなく、即座に判断を下します。豊富で柔軟なシステム堅牢化機能により、攻撃対象領域が大幅に縮小されると同時に、サーバーで任意のコードが実行されるのを防ぎ、エクスプロイトをブロックします。これらは、リソース消費量をほとんど増加させることなく行われます。

仮想デスクトップでは、従来型のエンドポイントセキュリティソリューションと比べてログイン時間が大幅に短縮されます。また、拡張により仮想ホストが限界に近づいている場合に、一時的な中断やボトルネックが解消されます。Kaspersky Hybrid Cloud Security では、物理エンドポイント向けのソリューションと同じ充実したセキュリティ機能セットをデプロイすることで、迅速な対応が提供される安全なユーザー環境を生み出します。これによりファイルレスマルウェア、ランサムウェア、エクスプロイトなどの標的になるリスクが解消されて、ユーザーは集中して業務に取り組むことができます。Kaspersky Hybrid Cloud Security では、デプロイの複雑さ、プラットフォームの統合とサポート、リソース使用の最適化、機能セット、セキュリティレベルに関して、お客様のニーズに最適な複数のオプションを用意しています。

エージェントレス型セキュリティ

VMware は、vSphere 仮想プラットフォームで「エージェントレス」なファイルレベルのセキュリティを実現する API を備えています。これにより Kaspersky Hybrid Cloud Security は、vShield Endpoint や NSX Guest Introspection などの VMware エコシステムと連携でき、すべての仮想資産がシームレスかつ即座に網羅されるようになります。各ホストには、アンチマルウェアスキャンエンジンとシグネチャデータベースを持つ特別な VM であるセキュリティ仮想マシン（SVM）が 1 つのみ必要です。個々の VM の負担が取り除かれるため、リソースの消費が大幅に低減されます。

ライトエージェント型セキュリティ

Kaspersky Hybrid Cloud Security には、「ライトエージェント」アプリケーションによるもう 1 つのアプローチが含まれています。これはプラットフォームに依存しないソリューションであり、保護されている各 VM の OS 内で動作するように最適化されたライトエージェントを利用します。「ライトエージェント」テクノロジーでは、ファイルスキャンエンジンとデータベースは SVM に用意され、フルエージェントを使用した従来型のソリューションと比較して、大幅に少ないリソース消費を実現します。このソリューションは、リソース消費に関しては、「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間に位置付けられますが、VMware 技術に縛られたり、制限されたりすることがないため、Microsoft Hyper-V、Citrix Hypervisor、KVM などの普及しているプラットフォームでも使用することができ、はるかに高いレベルのセキュリティを実現します。

これらのアプローチを通じて安全な仮想化を効率的に展開することで、次の問題が解決されます。

- 過剰なリソース消費：セキュリティタスクを一元化し、データベースの単一のインスタンスを使用し、判断をキャッシングすることで、保護されている VM ごとにシグネチャデータベースとアクティブなアンチマルウェアエンジンが重複するのを防ぐことができます。
- 「ストーム」：スマートキューによりSVMのバランシングやキャッシングが行われるため、各 VM におけるデータベースの同時アップデート、および/またはアンチマルウェアのスキャンプロセスによるストームの発生を抑制し、スキャンの遅れによって生じる「脆弱な時間帯」が生じるリスクを解消することができます。
- 「インスタントオンギャップ」：データベースやモジュールを非アクティブな VM でアップデートすることはできません。そのため、VM が起動されてからアップデートプロセスが終了するまでの間、VM は攻撃を受けやすくなります。常にオンの状態が維持されて、常に最新の状態にアップデートされる SVM を使用することで、この問題が解消されます。

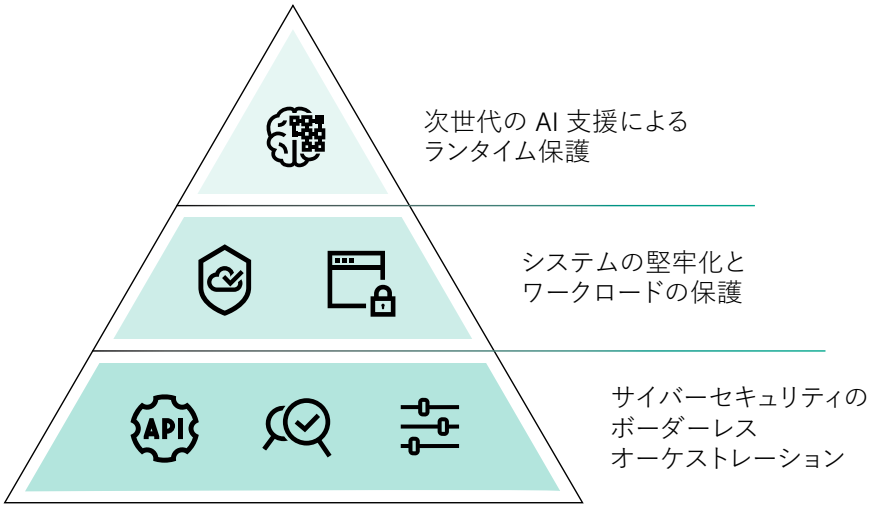
物理マシンとモバイルデバイス

物理サーバー、そして物理ワークステーションとモバイルデバイスにもセキュリティ対策が必要です。これは、カスペルスキーの別のソリューションである Kaspersky Endpoint Security for Business で対応しています。多層型の保護と管理をセキュリティプロセス自動化ツールと組み合わせることで、すべてのワークステーション、ラップトップ、タブレット、携帯電話のセキュリティステータスが可視化され、より広範なハイブリッド環境の一部として利用者の管理下に置かれます。またこれらすべてにカスペルスキーの受賞歴がある最高レベルの保護が適用されます。

最高レベルの保護機能

携帯電話、物理サーバー、仮想マシン、クラウド内のいずれでセキュリティが実行されている場合も、同じルールが適用されます。

カスペルスキーの製品とサービスでは、最高レベルを誇る保護機能が中枢的な役割を担います。リアルタイムの脅威インテリジェンスに関する業界トップクラスの情報源と機械学習を基盤とするカスペルスキーのテクノロジーは絶えず進化し、高度な脅威やランサムウェアからデータと共有フォルダーを安全に守ることで、最新のエクスプロイトからエンドポイントを保護します。



Kaspersky Hybrid Cloud Security では、物理または仮想エンドポイントやサーバー、パブリッククラウド内のワークロードのいずれを保護する場合も、業界トップクラスの同じ機能セットが利用されます。この機能セットには以下が含まれます。

- **受賞歴のあるアンチマルウェアエンジン**によって、コンピューター、VM、ワークロードを、アクセス時およびオンデマンドで、リアルタイムかつ自動的にファイルレベルで保護
- **クラウドベースのインテリジェンス**によって、新しい脅威を迅速に特定し、自動アップデートを実施
- **ふるまい検知**によって、アプリケーションとプロセスを監視し、高度な脅威やファイルのないマルウェアからも保護して、必要に応じて悪意のある変更をロールバック
- **脆弱性攻撃ブロック**によって、OSやソフトウェアの脆弱性を悪用した攻撃を検知し、ブロック
- **ランサムウェア対策**によって、クラウドワークロード、仮想および物理エンドポイント、共有ディレクトリを攻撃から保護し、感染したファイルを以前の暗号化されていない状態にロールバック
- **HIPS/HIDS** によって、物理およびクラウドベースの資産へのネットワークベースの侵入を検知または防止
- **アプリケーションコントロール**によって、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、さらに最適なシステムの堅牢化、および実行可能なアプリケーションとその場所、許可されるアクセス先の指定が可能
- **ウェブコントロール**によって、インターネットベースのサイバー脅威（従業員の認識の欠如やミスを悪用したものを含む）から保護し、ソーシャルメディアでのやり取りや業務に無関係な Web サイトの閲覧に費やす時間を削減することで生産性を向上
- **メールセキュリティ**（アンチスパムを含む）によって、クラウドワークロード内のメールトラフィックを保護
- **Web セキュリティ**（アンチフィッシングを含む）によって、潜在的に危険な Web サイトやスクリプトの脅威から保護

コンプライアンス

コンプライアンスは、すべての組織にとって重要な要件です。カスペルスキー製品では次のさまざまな制御と機能を通じて、コンプライアンス要件を満たすことができます。

- **管理サーバー階層：**ITインフラの複雑さに対応する柔軟性を提供
- **複数のデプロイオプション：**オンプレミスやクラウドに対応
- **レポートとWindowsイベントログ監視：**包括的で詳細な構成が可能で、監査を簡素化
- **ロールベースのアクセス制御（RBAC）**によって、組織構造や IT ポリシーに従って管理者グループごとにコントロール権を確実に分離
- **パスワードによるエージェントの保護とセルフディフェンス**によって、セキュリティシステムの改竄を防止
- **セキュアな通信**（すべてのソリューションコンポーネント間）
- **脆弱性評価と自動パッチ管理**によって、高度なマルウェアやゼロデイの脅威がパッチ未適用の脆弱性を悪用するのを防止
- **ユーザー透過的な FIPS 140-2 認定の暗号化**によって、ポータブルデバイス上およびオンサイトの機密情報を保護。統合された技術により、暗号化を一元的に再び適用することが可能
- **システムの堅牢化：**「デフォルト拒否」によりロックダウンを実行。またファイル変更監視（FIM）を通じて代替攻撃を防止
- **デバイスコントロール**によって、アタッチされた使用中のストレージ、カメラ、マイク、および他のハードウェアをきめ細かくコントロール
- **アンチマルウェア保護とパーソナルファイアウォール**によって、サーバーとワークステーションのセキュリティを強化

上記以外にも、可視化、十分な粒度、高いレベルの制御、および継続的な改善とリスク状況への柔軟な対応を実現する機能やメカニズムが提供されています。

セキュアなデジタルトランスフォーメーションを実現

デジタルトランスフォーメーションにより、利用者だけでなく、利用者を標的とするサイバー犯罪者にとっても、新しい機会が創出されます。カスペルスキーが提供する、ハイブリッド環境向けの統合された最善のセキュリティソリューションを導入することで、ビジネスの機会を最大限に活かすと同時に、攻撃者の機会を取り除くことができます。

製品情報：
www.kaspersky.co.jp/enterprise-security/cloud-security

ご購入相談窓口：
jp-sales@kaspersky.com

www.kaspersky.co.jp

kaspersky BRING ON THE FUTURE