kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Security for Business

テクノロジーは、ビジネスを大きく変える力です。変化に対応できなければ停滞するだけです。しかし、テクノロジーは、犯罪への扉も開きます。エンドポイントは格好の標的です。そこで、御社にとって最も大切なものを守るために強固で信頼できるソリューションを導入することで、自らのサイトに取り込もうとするサイバー犯罪者の上を行く必要があります。

課題

攻撃者からのプレッシャーの増大

サーバー犯罪者が使用するツールが非常に安価になったことで、セキュリティイベントとリスクは劇的に増えています。ランサムウェア、ファイナンシャルスパイウェア、フィッシング、その他の脅威は、特にデジタル変革が進行中の場合、組織に深刻な損失をもたらす可能性があります。

多様な構成のインフラストラクチャの保護

リモートワーク、クラウドサービス、アジャイルプロセスが増加したことで、すべてのセキュリティ戦略は、ノート PC、ワークステーション、サーバー、モバイルデバイス、さらには業務に使用される個人所有デバイスを含むあらゆるエンドポイントデバイスをカバーすることが必要になりました。また、サポート対象である様々なオペレーティングシステムもすべて考慮する必要があります。

高度な複雑性への対処

複雑な IT インフラストラクチャとそれをサポートし、保護するために必要な専門知識のすべてにコストがかかります。時間、予算、スタッフ、特定のスキルの面で、変化する企業のセキュリティ要件を満たす適切なソリューションに対して、効果的に投資する必要があります。

ソリューション

俊敏な適応型セキュリティ

以下が可能であることが必要です：

- パフォーマンスに影響を与えずに、データ、従業員、インフラストラクチャを完全に保護する。
- 障害となる新しい脅威を検知し、それに対抗するために、最も信頼できる最新の脅威インテリジェンスを使用する。
- 脅威のふるまいのパターンを認識し、それによって未知の脅威であっても無害化する。
- エンドポイントとユーザーを操作できるアプリケーション、Web サイト、デバイスを管理して、攻撃サーフェスを縮小する。

あらゆるプラットフォームに対応する単一のソリューション

ソリューションには以下をもたらすことが期待されます：

- 設置または使用場所、組織の所有かどうか問わず、データを扱うすべてのワークステーション、サーバー、モバイルデバイスにとって最善のセキュリティ。さらに、脅威の侵入ポイントと、チームの負担を増やさずに Web およびメールゲートウェイを保護する方法についても考慮している。
- 単一のコンソールで操作できる単一のソリューションで、Windows、Mac、Linux、 iOS、Android などが混在した環境のすべての OS を保護できる安心感。

柔軟な管理とタスクの自動化

さらに、以下の方法でリソースを最大化することが望まれます：

- 高いレベルでの自動化：特に、パッチや OS の展開など、重要だが日常的な業務。チームの時間と専門性は非常に貴重なので無駄にはできません。
- リモート管理機能：在宅勤務環境でワークステーションをセットアップするか、または暗号化オプションでデータの安全を確保するか。
- 一元化：コンソール間の行き来がなく、自分の境界内またはクラウドで、統合された明快な単一の画面から管理できることが必要です。

データ侵害によるコスト

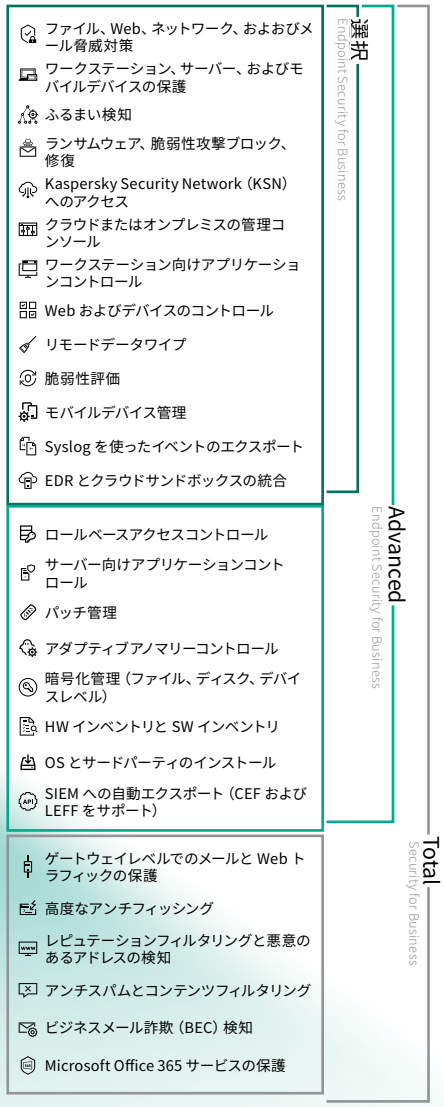
$105k（中小企業）　**$927k**（大企業）

$101k	▲	$105k		$1.09m	▼	$927k
2020年		2021		2020年		2021

出典：カスペルスキー IT セキュリティの経済レポート、2021

3 つの段階に分けた機能パック

Kaspersky Endpoint Security for Business のツールやテクノロジーは段階的なレベルのすべてにおいて賢くバランスが取られており、企業の成長に応じて進化するセキュリティや IT ニーズを満たします。



より多くの賞を獲得し、お客様に評価されるセキュリティ

2013 年から 2021 年の間に、カスペルスキーの製品は第三者機関によるテストやレビューを 741 回受け、弊社の製品は 518 回、1 位になりました。詳しくは、次のサイトをご覧ください：www.kaspersky.co.jp/top3

ランサムウェアの脅威

これらの攻撃は個人または企業を標的にしています。近年で最もよく知られた攻撃のいくつかは大手ブランドに対するものでした。

過去にランサムウェア攻撃を受けた企業の 88% のエグゼクティブは、再度攻撃を受けた場合は身代金を払うと言っています。

ランサムウェアは、世界中の企業にとって大きな問題になりつつあります。ランサムウェアを使用した攻撃の数は、2021 年だけでほぼ倍になっています。この一因がパンデミックである可能性があります。これまでより自宅で働く人が増えたからです。しかし、ハイブリッドなワーキングモデルの継続が確実視されるため、ランサムウェア攻撃の可能性は存在し続けます。

カスペルスキーがもたらすもの

- 真のセキュリティ：**ファイルレス攻撃に対する保護**、ML ベースの**ふるまい分析**、さらにエクスプロイト、ランサムウェア、およびファイナンシャルスパイウェアに対する固有の保護といったカスペルスキーのテクノロジーの比類なきパフォーマンスにより、広く拡散する新しい脅威からすべてのエンドポイントを完全に保護します。
- プロアクティブな保護：攻撃が始まる前に攻撃を食い止めます。**アダプティブアノマリーコントロール**による実行前保護は、シンプルなブロックルールとふるまい分析に基づくスマートな自動チューニングを組み合わせています。
- IT セキュリティの成熟度の上昇に対応する完全なエコシステム：自動対応および分析では、EDR および **SIEM** ソリューションとの**統合**を活用します。
- コストパフォーマンス：弊社の多層的なアプローチでは、今すぐ必要な機能についてのみ支払い対象となります。
- 将来を見据えた提供体制：アップグレードは、レベルの変更だけでシームレスに行われます。拡張性に優れた弊社ソリューションは、御社の成長に合わせて**数千の管理対象デバイス**をサポートできます。
- **合理化されたクラウド導入：Microsoft 365** サービスを保護します。
- 柔軟性：**希望の展開オプションを選択**できます（クラウド、オンプレミス、エアギャップ、およびハイブリッド展開）。さらに、きめ細かいロールベースアクセスコントロール（**RBAC**）で、異なるチームメンバーに、様々なレベルのセキュリティシステムアクセスを割り当てます。
- 安心：すべての機密データが、ファイルおよびフルディスクレベル、および外部デバイスでの暗号化管理などの**データ保護機能設定**で、完全に保護されます。デバイスの紛失または盗難が発生した場合は、リモートデータ消去によってデータが削除されます。
- 境界防御：**Web およびメールベースの攻撃を防止**して主要な標的である従業員とエンドポイントを守ります。

使用事例

システムを自動的に防御

ふるまいベースの検知は、カスペルスキーの次世代技術を用いた多層保護アプローチの一部であり、ファイルレスマルウェア、ランサムウェア、ゼロデイマルウェアのような高度な脅威に対する最も有効な防御方法の 1 つです。

Kaspersky Security Network のデータを使用することで、新しい脅威に迅速に対応できます。また、保護コンポーネントのパフォーマンスが向上し、誤検知の可能性が低減されます。結果的に、高い検知率とアダプティブセキュリティの搭載によって、誤検知を最小限に抑えながら攻撃に迅速に対応できます。カスペルスキーは、最近の AV-Test による調査で、100% のランサムウェア保護率を示した唯一のサイバーセキュリティベンダーです。Advanced Endpoint Protection: Ransomware Protection test、AV-Test、2021 年 9 月 30 日

攻撃サーフェスの縮小

リモートデバイスを企業の IT セキュリティと連携させます。アプリケーションコントロールは、(ゲームアプリやソーシャルネットワークへのアクセスを制限するなどにより) 生産性とセキュリティの両方に影響を与えます。従業員はクラックされたアプリや疑わしい Web サイトでフィッシングやマルウェアの被害に遭う可能性があります。また、USB モデムを挿入しただけで、ネットワークプリンターから機密データの漏えいが発生する可能性があります。これらのすべての攻撃経路、そして人為的ミスによるリスクは、アプリケーション、Web、デバイスのきめ細かいコントロールを適用することで大幅に削減できます。

アダプティブアノマリーコントロールでは、ユーザーのふるまいに基づいて、一般のポリシーを強化したり、システムでどのようにルールが適用されているかを確認したりできます。

時間、労力、コストの最小化

Kaspersky Endpoint Security for Business は、Cloud コンソールから管理できます。

この SaaS ベースのアプローチでは、ハードウェアへの投資は不要です。弊社のクラウドインフラストラクチャがすべてに対応するので、アップデート、サポート、可用性に時間をかける代わりに、ビジネスイニシアティブに集中できます。

チームがエンドポイントの強化、リモートデバイスの管理、OS 展開、パッチおよび暗号化管理に費やしていた時間を考えてみてください。Kaspersky Endpoint Security では、単一のソリューションと、すべてを管理できる単一の Web インターフェイスを提供して、これらすべてのタスクやその他のタスクを合理化し、自動化します。タスクやデバイスタイプごとに個別のコンソールや様々な製品を使用する必要はもうありません。

強力なデータ保護体制の構築

今日の攻撃では、脅威アクターは、合法なツールやアプリケーションを使用して、一般に普及しているアプリケーションの新たな脆弱性やゼロデイエクスプロイトを発見しています。自動パッチ管理で、データがこれらの攻撃を受けるリスクを大幅に低減します。また、データの暗号化で、正規ユーザーだけが特定の機密ファイルまたは外部デバイスにアクセスできるようにします。ハードドライブ全体を暗号化しておけば、デバイスの紛失または盗難が発生した場合にもデータを保護できます。

Kaspersky Total Security for Business で使用可能な統合では、Microsoft Office 365 コラボレーションおよびファイル共有も保護でき、PII (個人識別情報) 漏えい防止に役立ちます。

ご自身で体験してください

弊社の適応型保護をご自身で使用してみませんか?このページにアクセスして Kaspersky Endpoint Security for Business の 30 日間の無料評価版をお試しください。

段階ごとのアプローチ

適切な製品とサービスを選択して組織のセキュリティ基盤を構築することは、第一 歩にすぎません。企業における長期的な成功のためには、先見性を持ってサイバーセキュリティ戦略を策定することが重要です。

弊社のポートフォリオは、今日の企業のセキュリティニーズを反映し、組織の規模や IT セキュリティの成熟度のレベルを問わず、御社のニーズに対して、独自の段階ごとのアプローチを提供します。

このアプローチは、あらゆる種類のサイバー脅威に対抗する異なる保護層を組み合わせおり、脅威からの自動的な保護に役立ちます。その後、ビジネスの発展に伴って、より高度な脅威に対抗するための新機能や進化した機能を系統的かつ組織的に追加して強化します。セキュリティ全体の対処は弊社に任せて、恐れることなくイノベーションに注力できます。

---

* (個人を特定できる情報)

Kaspersky Security Foundations

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Embedded System Security
- Kaspersky Security for Storage
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Professional Services
- Kaspersky Premium Support and Professional Services

- 企業ユーザーおよびモバイルデバイスの保護
- ハイブリッド環境向けのサーバーセキュリティ
- 仮想デスクトップ (VDI) の保護
- 専門的なエンドポイントとレガシー PC 向けの保護
- 最も一般的な攻撃経路であるメールを保護
- ウェブベースの脅威に対抗する最先端の保護
- 展開、設定、保守の支援

カペルスキーエコシステムを最大限に活用

Kaspersky Security Foundations

弊社のクラウド管理による脅威保護段階では、すべての組織で、あらゆるデバイス、VDI、およびハイブリッドサーバーインフラストラクチャに対する、コモディティ化されたサイバー脅威を自動的に阻止できます。

- あらゆるデバイスを保護 (専門的なエンドポイントやレガシーエンドポイントを含む)
- あらゆる IT 資産を可視化して管理
- ユーザーのミスの防止および軽減に効果
- ニーズに応じたシステム管理の自動化を大きなコストをかけずに実現

Kaspersky Optimum Security

新しい未知の回避型脅威からビジネスを守るのに役立ちます。リソースに負荷をかけない、効果的な脅威検知・対応ソリューションです。24 時間 365 日のセキュリティ監視、自動化された脅威ハンティング、カスペルスキーのエキスパートのサポートによるガイド付き対応とマネージド対応を備えています。

- 回避型脅威に対するエンドポイントの保護をアップグレード
- 必要不可欠なインシデント対応プロセスの構築をサポート
- サイバーセキュリティリソースの使用を最適化

Kaspersky Expert Security

すべての IT セキュリティ成熟度の企業で、APT 攻撃や標的型攻撃といった最新の高度な脅威に対処する日常的なニーズを満たすように設計されています。

- 専門職のワークロードを最適化
- 知識とスキルを向上
- 御社の専門職をバックアップ

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/category/business/
中小企業向け IT セキュリティ:
kaspersky.co.jp/business
大規模企業向け IT セキュリティ:
kaspersky.co.jp/enterprise

kaspersky.co.jp

実証済みの品質、独立性、カスペルスキーは透明性を確保しています。弊社はテクノロジーが私達の生活をよりよくし、安全な世界を造ることをコミットします。そのために、世界中の誰もがテクノロジーの無限の恩恵を受けることができるよう、セキュリティサービスを提供しています。安心できる未来のために、サイバーセキュリティをお届けします。
詳しくは、www.kaspersky.co.jp/transparency をご覧ください。

Proven.
Transparent.
Independent.