

kaspersky



Kaspersky Optimum Security

お客様のリソースに負担をかけること
のない EDR¹/MDR² を最大限活用して
回避型脅威の先手を打ちます。



Kaspersky
Optimum
Security

成功したサイバー攻撃のうち 30% で
正当なシステムツールが利用されて
います

Kaspersky Incident Response
Analyst Report, 2020 年



増加する高度な攻撃

現在の回避型脅威は、従来のエンドポイント保護を効率的に回避できるよう設計されているため、すべてのビジネスに重大なリスクを新たにもたらします。検知されない脅威がインフラストラクチャに入り込めば、ビジネスに以下のような大きな損害が生じ、利益が損なわれる結果となります。

- ビジネスの重要なプロセスの中断とデータの損失
- 信用の大きな毀損と顧客の喪失
- 罰金、違約金、利益喪失

攻撃の 45% は、疑わしいファイルまたは疑わしいエンドポイント活動が原因で検知されているため、これらを検知することが最優先です

上記と同様



最適な保護

エンドポイント保護の基盤となるのは自動的な保護機能ですが、より危険度の高い回避型脅威にも対応するためには高度なツールも備えている必要があります。

Kaspersky Optimum Security は、**機械学習**に基づく高度な検知と迅速な対応の機能を備えており、すべてがクラウドから提供されます。このソリューションを使用することで、かつてはお客様のチームが夜通し対応していたような脅威にも迅速かつ確実に対応できます。

課題

ランサムウェア、マルウェア、金融スパイウェアはすべて、検知を回避する能力を高めており、ダークウェブを介して簡単に安く購入できます。このため、現在、多くの組織にとって最悪の事態を引き起こしています。



強化が必要なエンドポイント保護

これらの最新の攻撃は、正規のシステムツールや、その他の簡単に使用できる手法とテクノロジー内に潜むことで**検知を回避**し、これらを使用して**お客様のインフラストラクチャにアクセスして生き残り続け、悪意のある活動を検知されずに高速に実行**します。

そして、リモートワークの存在があります。これにより、伝統的にインフラストラクチャへの最も魅力的な侵入口であったエンドポイントに一層注目が集まっています。



不足するリソース

お客様に今求められる競争力を強化するには、適切なインシデント対応能力を組織内で育む必要があります。

しかし、このようなプロジェクトには多大なコストと時間がかかる可能性があります。

- 全体としてのソフトウェアとハードウェアのコストが非常に高額になります。
- ツールおよびプロセスがサイロ化され、分断されているため、セキュリティの効率性が損なわれます。
- 定型化されたタスクに時間を費やすこととなります。

ソリューション

Kaspersky Optimum Securityは、24時間365日のセキュリティ監視、自動化された対応と脅威ハンティング、カスペルスキーのエキスパートからのサポートとガイダンスにより、効果的な脅威の検知と対応を実現するソリューションです。



最適な投資

専門家を雇用したり、スタッフを再トレーニングしたり、あるいは複雑な導入に奮闘することはありませぬ。Kaspersky Optimum Security は、重要なインシデント対応プロセスを組織のニーズに応じて簡単に導入して自動化できる柔軟性を備えています。

ニーズに応じてオンプレミスとクラウドのオプションを使い分けることができるほか、すぐに使える拡張性の高いセキュリティツールセットが備わっているので、IT システムの複雑性を低減し、ユーザーの生産性を高めるとともに、導入コストの透明性も確保できます。



最適にバランスのとれたセキュリティ

シンプルさと効果、人間のインテリジェンスと自動化、効率性と機能の最適なバランスをとることができるため、山をかけることなく確実な保護を実現できます。

Kaspersky Optimum Securityにより、利益、顧客、信用を失うリスクを低減するとともに、新たな脅威、未知の脅威、回避型脅威に対する防御能力を強化できます。そのため、現在の急速に進化し続ける脅威の状況にも対応できます。

主な利点

- 危険性の高い最新の回避型脅威による**損害や中断のリスクからビジネスを防御**
- 使いやすい Endpoint Detection and Response (EDR) ツールセットにより**独自のインシデント対応能力を整備**
- 面倒な作業を必要としない強力な Managed Detection and Response (MDR) を介して**検知を簡単に次のレベルに引き上げる**
- **従業員のトレーニングを通じたセキュリティ意識の向上により、感染リスクを大幅に低減**
- **運用の自動化と管理された保護により貴重なリソースを有効活用**
- 多様な機能を**クラウドまたはオンプレミスの単一のコンソールで管理**できるため、時間を短縮し労力を削減可能

攻撃の 55% は、検知するのに数週間以上かかりました

上記と同様



高度な検知

- 機械学習をベースにしたふるまい分析アルゴリズムにより、疑わしいふるまいを迅速かつ正確に見つけ出します。
- カスペルスキーのエキスパートによりサポートされた、カスペルスキー独自の攻撃の痕跡 (IoA) に基づく自動脅威ハンティングにより、身をひそめる複雑な脅威も見つけ出します。
- 攻撃サーフェスの縮小に役立つツールの設定をユーザーのプロファイルに合わせて自動的に調整する、アダプティブアノマリーコントロールを備えています。
- 組み込みのクラウドサンドボックスを含むクラウド検知。

主な機能

Kaspersky Optimum Security は回避型脅威に対する保護に必要な様々な機能を備えています。その中心となるのは、検知、分析、対応です。



簡単な分析

- インシデントに関するすべての情報が自動的に **1 枚のインシデントカード** にまとめられます。
- 視覚的でわかりやすい調査プロセスにより、特定の環境で生じたインシデントを迅速かつ効率的に分析して、さらなる対応が必要かどうかを判断できます。
- 同時に、攻撃の痕跡によって検知されたすべてのインシデントがカスペルスキーにより優先順位付けおよび調査され、お客様の環境に合わせて推奨事項が提示されます。



自動での対応

- 個別のインシデントへの対応を「**1 クリック**」で行い、すばやく封じ込めることができます。
- 弊社のエキスパートが持つ豊富な経験に基づく**ガイド付き対応**により、複雑で危険な脅威にも対応できます。
- 複数のエンドポイントにわたる自動での対応がサポートされているので、分析またはインポートされた脅威をネットワーク全体で検知して対応できます。

内容

Kaspersky Optimum Security は、24 時間 365 日体制の保護を実現するマネージドソリューションとして、または簡単に使える EDR ツールセットとして使うことができるほか、それらの使い方を組み合わせることができるので、カスペルスキーのエキスパートの経験と知識を利用しながら、社内の検知および対応能力も育てることができます。Kaspersky Optimum Security ソリューションには、複数の製品が統合されています。



Kaspersky
Optimum Security



Kaspersky
Endpoint Detection
and Response

脅威の可視性を高める
根本原因解析

自動での対応



Kaspersky
Security Awareness

従業員のサイバーセキュリティスキルを高めるオンライントレーニングプログラム



Kaspersky
Managed Detection
and Response

24時間365日 セキュリティ侵害に速やかに対応
マネージド脅威ハンティング

ガイド付きリモートレス
ポンスシナリオ



Kaspersky
Threat Intelligence
ポータル

詳細なデータを調査

成功したサイバー攻撃のうち**31%**で悪意のあるメールが使用されていました。つまり、従業員が注意してさえいれば、これらの多くを防ぐことができました

上記と同様



ユーザーを教育しましょう

自分の不注意や単なる知識不足により、インフラストラクチャにサイバー攻撃を招き入れてしまうことを従業員に認識させるトレーニングが、攻撃サーフェスを狭めて、発生するインシデントの数を減らすための鍵となります。**Kaspersky Security Awareness** トレーニングにより、インフラストラクチャを保護するためにすべての従業員が必要とする知識とスキルを学ぶことができるので、サイバーセキュリティを意識した環境の維持に従業員が積極的に貢献できるようになります。



ハッシュ

最新情報を取得しましょう

脅威に関連するファイル、ハッシュ、IP、URLについての最新情報がサイバーセキュリティの専門家に提供されるので、より迅速かつ深く脅威を分析して把握することができます。これらの最新情報は、使いやすい **Kaspersky Threat Intelligence Portal** から追加の費用なしで手にすることができます。



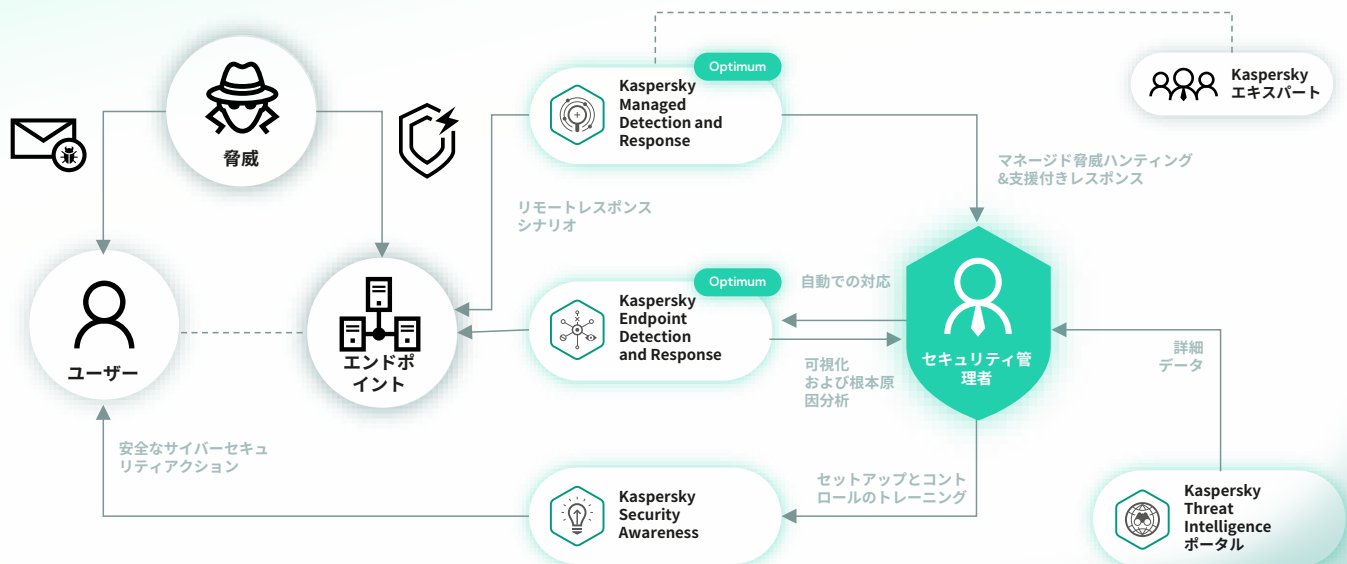
弊社にお手伝いさせてください。

つまり、ITインフラストラクチャの効果的な保護を確実なものにするには、ベストプラクティスとお客様のセキュリティ要件に基づいて、製品の実装、設定を適切に行うことが重要です。

Kaspersky Professional Services のエキスパートがお客様のセキュリティソリューションをヘルスチェック、導入、維持、最適化し、セキュリティ製品のROIを最大限に高め、性能をフルに引き出すことができます。

すべてが連携して機能する仕組み

Kaspersky Optimum Security では、保護、検知、分析、対応、従業員のトレーニングがすべて統合されています。任意のコンポーネントが独自の価値を持ち、個別に使用可能ですが、すべて連携して、回避型の脅威からのエンドポイントの保護に関するニーズをすべて単一の連携ソリューションで網羅します。



組織の44%は、ますます複雑化する環境をセキュリティで保護するコストが最優先の課題の1つであると考えています

IT security economics 2021、カスペルスキー



フルパッケージ

- カスペルスキーのセキュリティエコシステムに用意された様々な機能を利用して、セキュリティ基盤から、最適化された高度な機能まで、レベルに応じて防御力を強化できます。
- Kaspersky Optimum Security の様々な機能を単一のクラウドコンソールから管理できます。
- 多層保護により、コモディティ型と回避型の両方の脅威、および人為的ミスによるリスクに対処します。

使いやすさ

Kaspersky Optimum Security の管理は単一のコンソールから行えるため、運用がシンプルで、限りある時間とリソースを有効に活用できます。



管理が容易

- クラウド管理コンソールを通して、世界中のどこからでも迅速かつ効率的に管理できます。
- オンプレミスとSaaSのどちらのオプションでも、管理方法は変わりません。
- カスペルスキー製品の利用経験がなくても、簡単迅速に導入できます。
- お客様のチームが、すべてのツールを直感的に使用でき、簡単に管理できるので、長い時間をかけて使い方を学んだり、再トレーニングを受ける必要がありません。



時間とリソースの節約

- 管理された保護により、サイバーセキュリティのスタッフまたは専門知識が不足していても、関連するレベルのセキュリティ投資を行わずに検知機能と対応機能を構築できます。
- 重要なプロセスが自動化されているので、迅速、正確、効率的にインシデント対応を行うことができます。
- 従業員のセキュリティ意識を高めることができるので、防御をかいくぐる脅威の数を少なくして、処理が必要なインシデント数を減らすことができます。

実践

実際にすべてが連携して機能する仕組み

侵入

ユーザーがフィッシングメールを受信、または悪意のあるWebリソースにアクセスすることによりホストが感染

従業員のセキュリティ意識向上

攻撃サーフェスの縮小

自動的な脅威の阻止

インストール

最初の感染により必要なコンポーネントがインストールされてC&C¹と通信、環境が探索される

機械学習ベースのふるまい分析とクラウドサンドボックスを含む、高度な検知メカニズム

IoA²による自動の脅威ハンティング

自動化、ガイド付き、およびリモート対応シナリオ

ルーティング

様々なツールを使用して攻撃が継続化、必要に応じて水平移動を開始

根本原因分析とIoC³スキャン

1 Command and control (指令・制御)
2 Indicators of Attack (攻撃指標)
3 Indicator of Compromise (侵害指標)

各ステージに応じたカスペルスキー製品

セキュリティレベルに応じて、まず Kaspersky Security Foundations により信頼性の高い保護機能をベースに高い防御力を手に入れ、次の段階として Kaspersky Optimum Security にスムーズに移行して基本的なインシデント対応能力を獲得し、最終的に Kaspersky Expert Security の強力なツールを利用して非常に高度な脅威も防御できる体制を目指すといった、段階的な導入が可能です。お客様のステージに合ったソリューションをお選びください。



Kaspersky Security Foundations

大部分の脅威を自動的にブロックします。

» 詳しくはこちら



Kaspersky Optimum Security

回避型脅威への防御能力を強化します。

» 詳しくはこちら



Kaspersky Expert Security

複雑な APT 型攻撃に備えます。

» 詳しくはこちら

弊社について

弊社は、世界中に数十万ものお客様とパートナーを擁するグローバルなサイバーセキュリティの私企業であり、透明性と独立性の実現に熱心に取り組んでいます。弊社は 25 年間にわたり、**世界で最もテストを受け、最も多くの賞を受賞したテクノロジー**を使用してお客様の安全を確保すべく、ツールを構築し、サービスを提供してきました。

IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprises and SMB 2021 Vendor Assessment

メジャープレイヤー



AV-Test

Advanced Endpoint Protection: Ransomware Protection Test

100% の保護



Radicati Group

Advanced Persistent Threat (APT) Market Quadrant

トッププレイヤー



さらに詳しくご確認ください

セキュリティチームやリソースに負担をかけずに、Kaspersky Optimum Security によってサイバー脅威に対応する方法について詳しくは、以下をご覧ください：

www.kaspersky.co.jp/enterprise-security/edr-security-software-solution

¹ Endpoint Detection and Response

² Managed Detection and Response

サイバー脅威ニュース：securelist.com

IT セキュリティニュース：business.kaspersky.com

中小企業向けの IT セキュリティ：

kaspersky.co.jp/small-to-medium-business-security

大規模企業向けの IT セキュリティ：

kaspersky.co.jp/enterprise-security

kaspersky.co.jp