Kaspersky Endpoint Detection and Response Optimum

エンドポイント防御を次のレベルに引き上げ、面倒な作業なしで回避型脅威に対処できます。

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

今こそレベルを上げるべきです。お客様は、必要不可欠なアンチマルウェアテクノロジーを使用して組織を保護するだけでなく、従来の保護を回避してシステム内に深く身を潜めて最悪の事態を引き起こすべく身構えるよう意図的に設計された脅威を特定、分析、効率的に無力化する準備が整っています。

課題

脅威の回避の検知

回避型のマルウェア、ランサムウェア、スパイウェア、その他の脅威は、正規のシステムツールやその他の高度な技術を使用して攻撃することで、従来の検知メカニズムを回避する技術がスマートになっています。

サービスとしてのランサムウェア

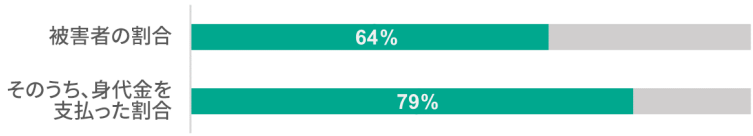
ハッカーは、既成のツールを安く購入し、誰に対しても攻撃できます。これにより、データを盗み、インフラストラクチャに被害を与え、金額が増大しつつある身代金を要求します。

限定されたリソース

インフラストラクチャは絶えず複雑化し、その普及範囲が広がっていますが、リソース（時間、資金、注意力持続時間）は減り続けています。ここには、シェルフウェアの余地はありません。

64% の組織が、既にランサムウェア攻撃の被害に遭っています。そのうち 79% が、攻撃者に身代金を支払っています。

カスペルスキー2022 年 5 月



「弊社は、カスペルスキーの包括的ソリューション、信頼性、迅速なサービスとサポートを高く評価しています。カスペルスキーは、弊社の IT 環境の可用性を保証してくれます。」

Marcelo Mendes CISO、NEO
事例を読む

お客様を支援するための方法

Kaspersky Endpoint Detection and Response（EDR）Optimum は、使いやすい高度な検知、簡単な調査、自動対応を提供することで、回避型脅威を特定、分析、無力化の役に立ちます。

高度な保護機能

弊社の高度な検知メカニズムには、機械学習、ふるまい分析、クラウドサンドボックスなどのテクノロジーが含まれます。

視覚的な分析ツールがシンプルであるため、脅威とその範囲を完全に把握できます。また、素早い対応アクションにより、損害が発生する前に、攻撃をその場で食い止めることができます。

1 つのソリューション

次世代のエンドポイントセキュリティが使いやすい EDR と統合されており、ノートパソコン、ワークステーション、サーバー、クラウドワークロード、仮想環境の高度な保護を実現します。

このすべての導入と管理が、単一のクラウドコンソールまたはオンプレミスコンソールを介して一元的に行われます。

シンプルで効率的

弊社は、小規模なサイバーセキュリティチームを念頭に置いて EDR Optimum を構築しました。これは、インシデント対応機能をアップグレードし、専門知識を養おうとしているが、そのために割ける時間があまりないユーザーが対象です。

弊社は、大半のタスクを自動化および最適化しています。このため、お客様が本当に重要な作業に費やす時間が増えます。

主な利点

- **複数のタイプの脅威を防止**
- **回避型脅威からシステムとデータを保護**
- **現在の脅威が活動する前に捕捉**
- **エンドポイント全体にわたって回避型脅威を認識**
- **脅威を把握し、素早く分析**
- **迅速な自動対応を使用して損害を防止**
- **1 つの簡易的なツールを使用して時間とリソースを節約**
- **すべてのエンドポイントを防御:**ノートパソコン、サーバー、クラウドワークロード

主な特徴

- **固有の次世代のエンドポイントセキュリティ**
- **機械学習を基盤とした高度な検知**
- **攻撃の痕跡(IoC)のスキャン**
- **視覚的な調査および分析ツール**
- **必要なデータをすべて単一のアラートカード内に保管**
- **組み込みの対応ガイダンスと自動化**
- **単一のクラウドまたはオンプレミスコンソールと自動化**
- **ワークステーション、仮想サーバーと物理サーバー、VDI 導入、パブリッククラウドのワークロードのサポート**

主な使用事例

私は攻撃を受けていますか?

- **高度な検知** – クラウドサンドボックスを含む機械学習を基盤としており、脅威を自動的に検知します。
- **securelist.co.jp またはその他のソースから IoC をダウンロードおよびスキャン**し、高度な脅威を見つけてください。

私が無力化できますか?

- **複数の対応オプションを使用してください** – ホストを分離し、ファイルの実行を防止するか、ファイルを削除してください。
- **その他のホストをスキャン**し、分析された脅威の兆候を探してください。
- **ホスト全体にわたって自動対応を適用**し、脅威(IoC)を発見してください。

どうすればスキルのトレーニングを受けられますか?

- **アラートカード内の対応ガイダンスを確認**してください。
- **Threat Intelligence Portal と最新の TI にアクセス**してください。
- **脅威を分析して対応する際に専門知識を養ってください。**

どのように発生しましたか?

- 脅威を**視覚的なプロセスツリーで確認してください。**
- 活動を**ドリルダウングラフで追跡してください。**
- **根本原因とインフラストラクチャへの侵入口**を理解してください。

どうすればもう一度発生しないようにできますか?

- **学習した情報を使用してください** – ブロックすべき IP と Web サイト、変更すべきポリシー、トレーニングすべき従業員を把握します。
- **今後このような脅威を防止するためのルールを作成してください。**たとえば、ファイルの実行を防止します。

コモディティ化した脅威に関してはどうですか?

- **次世代のエンドポイントセキュリティ**が、大半の脅威を即座に食い止めるために用意されています。
- **パッチ適用をステップアップ**するために、脆弱性とパッチ管理を活用してください。
- **攻撃サーフェスの縮小とポリシー調整を自動化**するためにエンドポイントコントロールを活用してください。

仕組み

簡単なデモについては、**こちらの動画**をご覧ください。

お客様はどれに該当しますか？

アンチマルウェアを装備しているが、それでは十分でない場合

エンドポイント防御をステップアップしましょう

カスペルスキーとサードパーティのどちらのエンドポイント防御を使用しているのであれ、今こそ EDR の導入を検討してみるべきです。

これは、高度な検知および防御機能に関することではなく、回避型脅威に備え、これを特定、分析、無力化することに関することなのです。

回避型脅威から保護する方法について詳しくは、**最適なレベルのセキュリティを実現するための購入者ガイド**をご覧ください。

既にカスペルスキーを使用している場合

セキュリティを最適化しましょう

弊社は製品を継続的に改善しています。このため、アップグレードを使用して弊社製品を最大限活用するようにしてください。またはクラウドに移行し、面倒な定型業務は完全に忘れてしまってください。

Kaspersky EDR Optimum の最新バージョンには、以下が用意されています：

- **アラートカード内のガイド付き対応！**
- **対応を適用する前のシステムの重要なオブジェクトの確認！**
- **アラートカード内の脅威インテリジェンスファイルレピュテーション！**
- **プロセスツリー分析の無制限の深さ！**

新機能について詳しくは、**こちら**をご覧ください。

カスペルスキーを初めて利用する場合

セキュリティを最適化しましょう

世界中の何千もの企業が Kaspersky EDR Optimum を使用していますが、その理由は以下の通りです：

- **単一の製品内の強力な EPP と基本的な EDR**
- **小規模なサイバーセキュリティチーム向けに設計された使いやすい EDR 機能**
- **クラウドまたはオンプレミスで導入する軽量で柔軟なソリューション**

EDR および MDR テクノロジーを基盤として回避型脅威に対処する複合ソリューションである **Kaspersky Optimum Security** をご確認ください。

段階に応じたアプローチを使用して前へ進む

使用するツールは、サイバーセキュリティとビジネス上のニーズ、およびチームとリソースに最適なものである必要があります。このため、弊社は、お客様の組織のプロフィールに応じた 3 つの異なるオプションを用意し、お客様の現在の主な焦点であるサイバーセキュリティのレベルを簡単に選択できるようにしました。

Kaspersky Security Foundations

大部分の脅威を自動的にブロックします。

- **一般的な脅威により生じるインシデントに対する多角的かつ自動的な保護の仕組みを提供し、大部分のサイバー攻撃をブロックします。**
- **あらゆる規模および複雑度の組織での連携セキュリティ戦略の基盤となるステージです。**
- **小規模な IT セキュリティチームを擁し、サイバーセキュリティに関する専門知識を学びつつある組織に、信頼性の高いエンドポイント保護を提供します。**

» 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。以下のような組織に最適です。

- **小規模な IT セキュリティチームを擁し、サイバーセキュリティに関する基礎的な専門知識を持っている組織。**
- **IT 環境が大規模化および複雑化しており、攻撃対象範囲が広がっている組織。**
- **高度な保護が必要であるにもかかわらず、サイバーセキュリティのリソースが不足している組織。**
- **インシデント対応機能を開発する必要性が高まっている組織。**

» 詳しくはこちら

Kaspersky Expert Security

複雑で APT のような高度な攻撃への対応を必要とする、以下のような組織に最適です。

- **IT 環境が複雑で分散している組織。**
- **成熟度の高い IT セキュリティチームまたは定評のあるセキュリティオペレーションセンター（SOC）を持つ組織。**
- **セキュリティインシデントやデータ侵害が発生した際のコストが高いためにリスク選好度が低い組織。**
- **法令の遵守が求められる環境で事業を営んでいる組織。**

» 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 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

トッププレーヤー

さらにセキュリティを強化する必要がある場合

強力な EDR ツールである **Kaspersky EDR Expert** をご確認ください。詳細な脅威ハンティング機能、広範なカスタマイズ、優れた検知メカニズムをお客様のエキスパートに提供します。

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

---

サイバー脅威ニュース：securelist.com
IT セキュリティニュース：blog.kaspersky.co.jp/category/business/
中小企業向けの IT セキュリティ：kaspersky.com/business
大規模企業向けの IT セキュリティ：kaspersky.com/enterprise

kaspersky.co.jp