Kaspersky Next EDR Optimum

エンドポイント防御を
次のレベルに引き上げ、
回避型脅威に対処

kaspersky

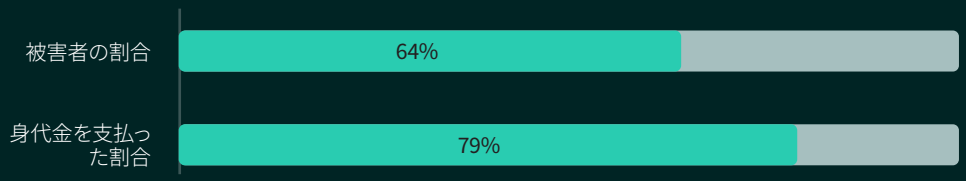
Kaspersky Next EDR Optimum

64% の組織が、既にランサムウェア攻撃の被害を受けています。

そのうち 79% が、攻撃者に身代金を支払っています。

How business executives perceive ransomware threats（Kaspersky、2022年5月）

今こそレベルを上げるべきです。従来の保護を回避するように設計された脅威を特定、分析、および無力化します。



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、攻撃に正規のシステムツールやその他の高度な技術を使用することで、従来の検知を回避する技術がますます洗練されています。

サービスとしてのランサムウェア

今日のハッカーは、安価な既成のツールを購入し、誰でも無差別で攻撃できます。それにより、データを盗み、インフラストラクチャに被害を与え、身代金を要求しており、身代金の額は増え続ける一方です。

リソースの制約

インフラストラクチャはますます多様化して複雑さを増し、その一方で時間、資金、人材といったリソースは不足しています。これは、高価なシェルフウェアが発生するうってつけの状況です。

「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 氏、CISO、NEO

事例を読む

お客様を支援するための方法

Kaspersky Next は、苦労せずに強力なセキュリティを構築することができるように設計された、カスペルスキーの主力製品ラインです。必要不可欠な EDR 機能を探しているお客様も、将来的な XDR の導入を模索しているお客様も、数回クリックするだけで、比類のないサイバーセキュリティの実績に支えられた Kaspersky Next の適応性が高く堅牢なクラウドネイティブ保護を利用することができます。

Kaspersky Next EDR Optimum は、使いやすい高度な検知、簡単な調査、自動対応機能を提供することで、回避型脅威を特定、分析、無力化に役立ちます。

高度な保護機能

カスペルスキーの高度な検知メカニズムには、ふるまい分析と機械学習が含まれます。

このすべてをシンプルな視覚的分析ツールおよび素早い対応アクションと組み合わせることで、脅威とその範囲を完全に把握し、損害が発生する前に攻撃を食い止めることができます。

クラウドの利用の検出とブロック機能および MS Office 365 のセキュリティにより、エンドポイントおよびクラウドで攻撃対象範囲を縮小できます。

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シンプルな 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。

クラウドまたはオンプレミスで、1 つのコンソールを導入して管理するだけです。

シンプルで効率的

Kaspersky Next EDR Optimum 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構築されています。対象となるのは、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お客様です。

大半のタスクを自動化および最適化しているため、お客様は重要な作業にのみ時間を費やすことができます。また、カスペルスキーでは、お客様と IT チームが新しいセキュリティ機能を最大限に活用するために必要なトレーニングを提供しています。

実行できること:

- サイバー脅威の事前防止
- 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
- シンプル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
- Pro ビューまたは Expert ビューコンソールを使用 – お客様が選択可能

提供されるもの:

- 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機能
- 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
- すべての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
- 十分な製品トレーニングを受けた IT セキュリティ担当者

いざというときに備えて、以下の質問に対する答えを用意しておきましょう

攻撃を受けているのか?

- **機械学習に基づく高度な検知**を利用する
- **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る

どのように発生したのか?

- 視覚的なプロセスツリーで脅威を確認**する**
- ドリルダウングラフで活動を追跡**する**
- **根本原因とインフラストラクチャへの侵入口**を把握する

脅威を無力化するには?

- **複数の対応オプションを使用**する (ホストの分離、ファイルの実行阻止、ファイルの削除などが可能)
- **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す
- **脅威 (IoC) の検知時にホスト全体にわたって自動的に対応を適用**する

他の脅威への対処は?

- **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
- **攻撃対象範囲を自動的に縮小し**、ポリシーを調整する
- **ユーザーが使用できるアプリケーションとデバイスを管理**する

今後同じ問題を防ぐには?

- **学習した情報を活用します。**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する
- **ルールを作成**し、今後同じような脅威を阻止できるようにする
- **クラウドを保護する。**許可されないクラウドリソース、サービス、インスタントメッセンジャーなどへのアクセスを検知して制限し、ブロックする
- **MS SharePoint Online、OneDrive、Teams を可視化し、制御**する

これを適切に行うには?

- **アラートカード内の対応ガイダンスを使用**する
- **Threat Intelligence Portal と最新の TI にアクセス**する
- **脅威を分析して対応することで、専門知識う**
- **組み込みのトレーニングと認定を活用**する (シュミレーション環境での対話式の課題を含む)

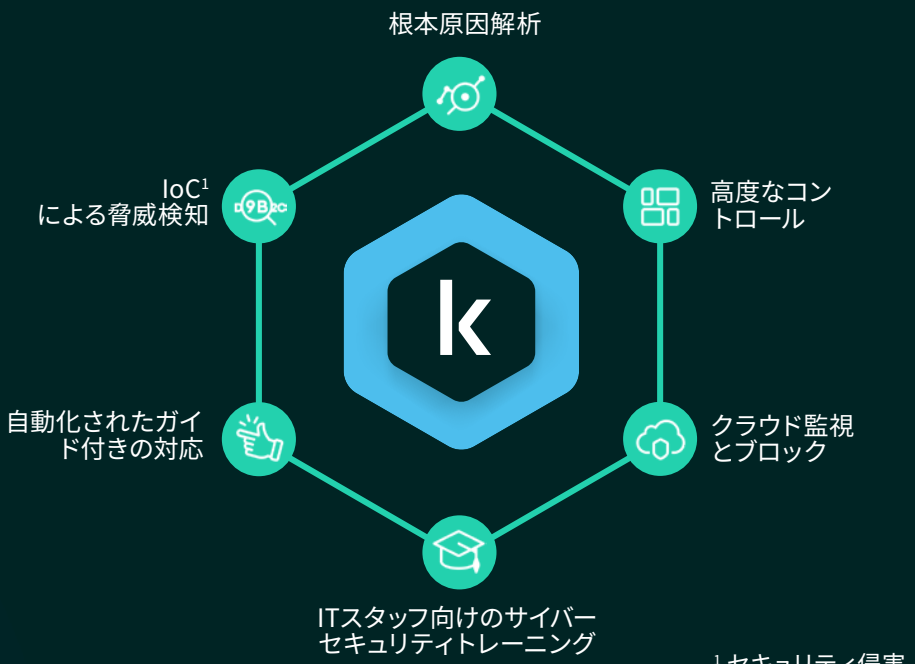
このすべてを行う時間を確保するにはどうすればよいか?

- **脆弱性とパッチ管理を自動化** – エンドポイントの状態をセキュアに保つための重要な方法
- **すべての従業員が企業のデータを安全に保つことができるように、リモートでネイティブの暗号化を管理**
- **時間のかかるセキュリティと IT の管理タスクを自動化**

Kaspersky Next
EDR Optimum

防御能力を強化
調査とレスポンスの基本機能でセキュリティを強化

対応するニーズ
- 可視性と対応能力の強化
- クラウドセキュリティの強化
- エンタープライズ水準のコントロール



[1] セキュリティ侵害インジケーター

Kaspersky Next – 将来を見据えたセキュリティ

Kaspersky Next EDR Optimum は、最も重要なサイバーセキュリティのニーズに応じて、強力なエンドポイント保護と制御に、EDR の透明性とスピード、XDR の包括的な可視性と強力なツールを組み合わせて、3 つのシンプルな構成で提供している、Kaspersky Next 製品シリーズの一部です。ニーズの高まりに応じて簡単にレベルを切り替えて、セキュリティ機能を迅速にアップグレードできます。

Kaspersky Next の構成

Kaspersky Next の各レベルの機能をご紹介します。

Kaspersky Next EDR Foundations

サイバーセキュリティの強固なコアを手軽に構築できます。

- ML ベースの強力なエンドポイント保護
- 自動修復
- 複数の自動化機能
- 柔軟なセキュリティコントロール
- EDR の根本原因分析ツール

Kaspersky Next EDR Optimum

回避型脅威への防御能力と専門知識を強化します。

- 可視化、分析、対応を実現する基本的な EDR 機能
- 強力なエンドポイント保護
- コントロール、パッチ管理、クラウドセキュリティの向上
- IT 向けのサイバーセキュリティトレーニング

Kaspersky Next XDR Expert

最も複雑で高度な脅威からビジネスを保護します。

- 既存のセキュリティインフラとシームレスに統合
- 脅威に対するリアルタイムの可視性と深い見識
- 高度な脅威の検知
- 資産を横断する関連付け
- 自動での対応

カスペルスキーを選択する理由

弊社は、世界中に数千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

さらに詳しくご確認ください

Kaspersky Next EDR Optimum がお客様のセキュリティチームを支援し、リソースに負荷をかけることなくサイバー脅威に対処する方法について詳しくは、https://go.kaspersky.co.jp/next をご覧ください。

Kaspersky Next EDR Optimum についてさらに詳しく

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations　詳しくはこちら

Kaspersky Next XDR Expert　詳しくはこちら

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

kaspersky.co.jp

Kaspersky Next について詳しく：
https://go.kaspersky.com.jp/next

対話型のツールで簡単なアンケートに答えて、最適な製品レベルを選びください：
https://go.kaspersky.com/Kaspersky_Next_Tool