kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

自動化された即時対応および根本原因の簡単な分析により真の多層防御を構築

2019 年にサイバー攻撃の影響を受けた企業は、全企業の **91%** に上ります。そのうち標的型攻撃を受けた企業は **10** 社に **1** 社の割合に達しています[1]。

問題

複雑な脅威が引き起こす中断

単純なマルウェアの時代は過去となり、脅威はますます複雑化しています。これらの脅威は長期間にわたり検知されないまま、企業に対してより頻繁に中断を引き起こし、さらに大きな損失を与えています。

攻撃対象になる可能性の高まり

複雑な脅威をより安価に実行できるようになっていることから、攻撃が頻発化しています。攻撃の標的になる可能性が高いと考える組織は、今すぐ対策を講じる必要があります。

効率化が喫緊の課題

状況をさらに難しくしているのが、組織が抱えるリソース不足の問題です。多くの組織では時間や熟練スタッフなどの重要なリソースが不足しています。

解決策

«効果が低い EPP ソリューションは、EDR ツールの価値を損ないます»[2]

«このため EDR ツールでは、人員と時間が新しい ROI 指標になっています»[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum は、高度な検知、調査の簡素化、自動対応の提供を通じて、複雑で高度な脅威からの保護を支援します。

必須機能にオプションを追加

脅威を検知するだけでなく、その全容と発生源を明らかにして瞬時に対応し、事業の中断を回避するために、詳細な可視性、シンプルな調査ツール、自動対応のオプションを提供します。

真の多層防御

使いやすく高度に自動化された検知および対応ツールキットと、Kaspersky Endpoint Security for Business の比類のないエンドポイント保護機能および高度な検知を組み合わせることで、単一の統合ソリューションを形成しています。

インテリジェントなツールにより効率性を確保

一元化されたシンプルな管理機能と高度な自動化を提供することで、無駄な時間を削減し、人的リソースと IT 部門のオーバーヘッドを最適化します。オンプレミスとクラウドの両方で、単一コンソールから効率化されたワークフローを使用できます[3]。

主な利点

- より頻繁で破壊的な、高度かつ複雑な脅威から保護
- シンプルな自動化ツールによって時間とリソースを節約
- ネットワーク全体で複雑な脅威の全容を確認
- 脅威の根本原因と、実際の発生の仕組みを把握
- 迅速な自動対応で損害の拡大を回避

重要な疑問への回答

- 警告の背景には何があるのか？
- 警告発生時にどのようなアクションが実行されたのか？
- 検出された脅威は今もなお活動中なのか？
- 他のホストも攻撃を受けているのか？
- 攻撃はどのような経路をたどったのか？
- 脅威の真の根本原因は何か？

脅威の全貌を把握

グローバルな脅威にさらされていることが判明した場合（規制当局から特定の不正アクセスの痕跡（IoC）に対するスキャンを実行するよう求められた場合など）は、次の方法で対応できます。

- 信頼できるソースから IoC をインポートし、定期的にスキャンを実行して攻撃の痕跡を確認
- 警告について徹底的に調査し、検出された脅威に基づき IoC を生成し、ネットワーク全体でスキャンを実行して、影響を受けたホストが他にないかどうかを確認

活発な攻撃を繰り広げる脅威に瞬時に対応

- すべてのエンドポイントにわたり、複雑な脅威に関連したファイルを自動的に隔離
- 急速に拡散する脅威に関連した IoC を検出した場合は、感染したホストを自動的に隔離
- 調査中に悪意のあるファイルが実行されてネットワーク全体に拡散されるのを防止

[1] Kaspersky グローバル IT リスクレポート（Kaspersky、2019 年）

[2] IDC、『Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR』（Doc # US45794219、2020 年）

[3] クラウドコンソール経由で管理できる機能の範囲については若干の制限があります。詳細については、https://kas.pr/epp-management-options をご覧ください。

EDR の重要なユースケース

脅威の全体像の確認

エンドポイントでセキュリティ警告を確認し、さらに詳しく分析して脅威の全容を把握することができます。これにより、インシデントを適切に処理し、エンドポイントから脅威を完全に除去することができます。

ワークフローの簡素化

オンプレミスとクラウドの両方で、単一のコンソールから効率化されたワークフローを使用できます。また、詳細情報の視覚化、IoC スキャン、対応オプションなどのシンプルな EDR シナリオと管理を通じて、サイバーセキュリティの専門知識をそれほど必要とせず、時間をかけずに対処することが可能です。

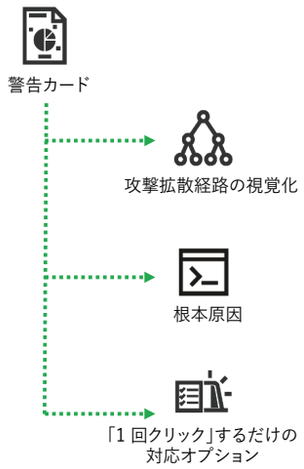
防御の強化

さらに Kaspersky Sandbox が追加されたことで、必要な機能がすべて揃った統合型エンドポイントセキュリティソリューションが生まれます。このソリューションは、商品化された脅威、複雑な脅威、回避型脅威に対して、シンプルかつ効果的な高度に自動化された多層防御を実現します。

情報が付加された警告データの分析

Kaspersky EDR Optimum ではインシデントの理解に必要な情報が付加されます。また攻撃拡散経路の視覚化を通じてさまざまなイベントの関連性を把握することができます。

インポートまたは生成された不正アクセスの痕跡（IoC）のスキャンにより、ネットワークに配置されたすべてのホストの可視性が提供されます。



自動的に対応

すべてのエンドポイントに対して、IoC スキャンによって脅威が検出された場合は自動的に対応するように設定できるほか、「1 回クリック」するだけのオプションを使用してインシデントが検出された場合に即座に対応することもできます。

対応オプションには、ホストの隔離、ファイルの隔離、ホストに対するスキャンの開始、ファイルの実行防止などがあります。

このサービスでできること
EDR の追加オプション

Kaspersky Endpoint Detection and Response Optimum は、当社が提供する、お客様固有のニーズにきめ細かく対応した EDR オプションの 1 つです。こちらもご検討ください。

Kaspersky Endpoint Detection and Response

業界および顧客から評価を得ているエキスパート EDR ソリューションとして、成熟度の高い IT セキュリティチームで構成された IT 組織に最適です。最も高度な標的型攻撃の根本的な原因を究明するのに役立ちます。脅威検知の強化、強力な調査、プロアクティブな脅威ハンティング、一元化されたインシデント対応を提供します。
https://www.kaspersky.co.jp/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

20 年以上にわたる絶え間ない脅威調査の卓越した実績に裏打ちされた、フルマネージドの検知、優先順位付け、調査、対応を 24 時間 365 日体制で個別のニーズに合わせて提供します。このソリューションを使用することで、独自のセキュリティオペレーションセンターを実際に設立しなくても、それを所有することで得られる主な利点がすべてもたらされます。
https://www.kaspersky.co.jp/enterprise-security/managed-detection-and-response

Kaspersky Endpoint Detection and Response Optimum を使用してサイバー脅威に対応しながらセキュリティチームとリソースの負担を軽減する方法について詳しくは、
https://www.kaspersky.co.jp/enterprise-security/edr-security-software-solution

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.co.jp

2020 AO Kaspersky Lab. All rights reserved.
.Kaspersky およびカスペルスキーは Kaspersky Lab の商標登録です。その他記載された製品名などは、各社の商標もしくは登録商標です。なお、本文では、TM、®は記載していません。

当社は実績を重ね、独立性、透明性を確保しています。そして、より安全な世界を築こうと励んでいます。テクノロジーが生活を向上させる、そんな世界を。世界中の誰もが、テクノロジーがもたらす終わりのないチャンスを手にできるように、私たちは保護します。もっと安全な明日のために、サイバーセキュリティを。

詳細はこちら：kaspersky.co.jp/about/transparency

Proven.
Transparent.
Independent.

PMM-1049-202006