Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

サイバー犯罪者は、ますます洗練されてきており、既存の保護をうまく回避できるようになってきています。ビジネスのあらゆる分野がリスクにさらされており、ビジネスのうえで重要なプロセスが混乱させられ、生産性が損なわれ、運用コストが増大するおそれがあります。

カスペルスキーのEDRを用いることで、お客様の企業ではつぎのことが可能になります。

- マルウェアをかわして、効果的に脅威を**モニタリング**します
- 高度な技術を活用して、効果的に脅威を**検出**します
- 生データと判定を一元的に**集約**します
- 攻撃に対して迅速に**対応**します
- **発見された脅威による悪意あるアクションを阻止**します

…すべてを、直感的に操作できるWebインターフェースを通して操作できるため、調査や対応を行うのも簡単です。

カスペルスキーのEDRとIDCの「Endpoint Security 2020」報告*の要旨

- EPPソリューションが非力な場合、EDRツールの価値が損なわれます

  カスペルスキーは、単一のエージェントを通して、強力かつ完全なエンドポイント防御（EPP+EDR）を提供いたしております

- したがって、EDRツールの場合は、人と時間が新しいROI指標になります

  カスペルスキーは、複雑な問題についても高度な自動化を実現し、セキュリティを担当する専門職の拘束時間を減らすことができます

- EDRはエンドポイントの外部にあるデータを活用する必要があります

  カスペルスキーは、単一のツールを通して、メールベースおよびWebベースの高度な脅威の検出と可視性を改善することにより、EDRの有効性を向上させます。

まずはエンドポイントの防御を強化

サイバー犯罪者にとって、企業のエンドポイントは、データ、ユーザー、企業システムのすべてが集約されており、ビジネスプロセスが作られ実装される場所であるため、真っ先に攻撃のターゲットになります。このような企業のエンドポイントを保護し、インフラストラクチャへの入り口として利用されることを防ぐには、既存のセキュリティ対策を強化する方策を検討する必要があります。一般的な脅威を自動的にブロックすることから、複雑なインシデントに迅速かつ適切に対応することまで、エンドポイント防御サイクルのすべてを実装するには、高度な防御機能を備えた防御技術を導入する必要があります。

Kaspersky Endpoint Detection and Response（EDR）は、強力なセキュリティを実現しすることができます。これは、企業ネットワーク上のすべてのエンドポイントを包括的に可視化し、優れた防御対策によって、複雑な脅威やAPTのような攻撃を検出・優先順位付け・調査・無害化する定型タスクを自動化できるためです。

主な強化ポイント

- Kaspersky EDRは、もっとも試験され、もっとも評価されているフラグシップであるEndpoint Protection Platform（EPP）–**Kaspersky Endpoint Security for Business**–を強力なEDR機能で強化し、全体的なセキュリティレベルをさらに向上させています。単一のエージェントが、一般的な脅威を自動的に防御し、複雑な攻撃を高度に防御するため、インシデントの処理が簡素化され、メンテナンス要件を大幅に緩和することができます。エンドポイントへの負担が増えることも、コストが増えることもありません。ワークステーションやサーバーを、もっとも洗練された標的型攻撃の脅威から完全に保護することができます。
- カスペルスキーのEDRは、初期のエビデンス収集に必要な時間を短縮し、完全なテレメトリ分析を行って、EDRプロセスの自動化を最大化することにより、ITセキュリティのリソースを追加することなく、インシデントに対応するための時間を全体として削減することができます。
- カスペルスキーのEDRを、**Kaspersky Anti Targeted Attack Platform**のなかに取り入れ、EDR機能とネットワークレベルの高度な脅威検出を組み合わせることも可能です。エンドポイントレベルとネットワークレベルの両方で高度な多次元脅威を検出するために必要なツールがすべて揃っています。ITセキュリティ担当者はこのソリューションひとつで、最新技術を採用し、効果的に調査し、迅速かつ一元的に対応することができます。

* IDC PERSPECTIVE、Endpoint Security 2020:
The Resurgence of EPP and the Manifest Destiny of EDR

カスペルスキーのEDRは、企業が下記のことを望んでいる場合に最適です。

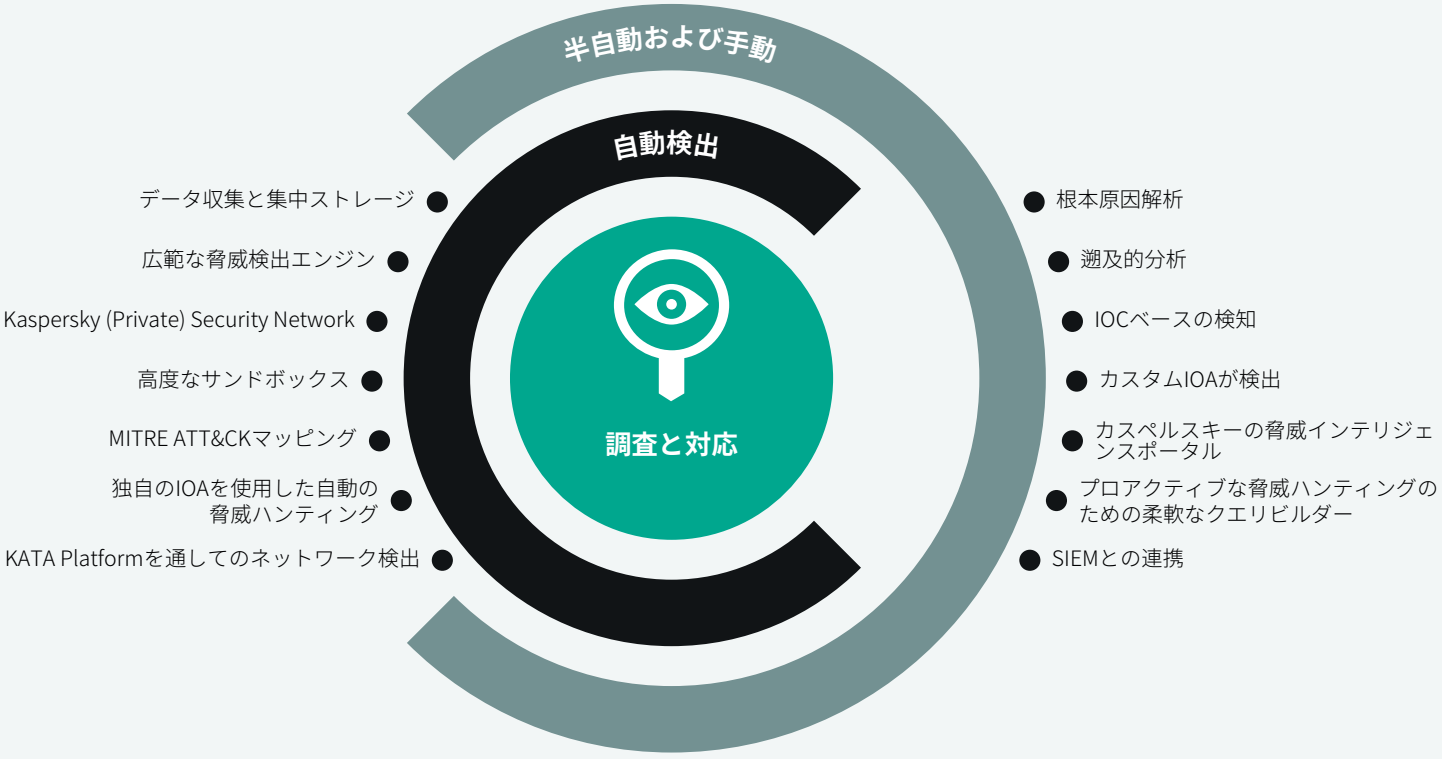
- インシデント対応のための使い勝手のよい企業向けソリューションでセキュリティをアップグレードしたい
- 脅威を特定して対応するプロセスを自動化し、調査中にビジネスが中断することを避けたい
- 高度な技術により、エンドポイントの可視性と脅威検出能力を強化したい
- 脅威アクターが目的を達成するために採用する具体的な戦術、技術、手順（TTP）を理解することで、より効果的な防御とセキュリティリソース配分を実現したい
- 効果的な統合型の脅威ハンティング、インシデント管理、対応プロセスを確立したい
- 無関係なエンドポイントログの分析に時間を浪費することを避け、社内SOCの効率を向上させたい
- エンドポイントログ、アラート評価、調査結果の文書化を実施することで、コンプライアンスを強化したい

もっとも洗練された脅威を迅速に発見し封じ込めたい

カスペルスキーのEDRは、高度なエンドポイント保護を実現し、SOCの効率を高め、高度な脅威を検出します。破壊されたエンドポイントにアクセスできなかったり、攻撃中にデータが暗号化されたりした場合も、時間を遡ってデータにアクセスすることが可能です。独自のIOA（攻撃の痕跡）、MITRE ATT&CKエンリッチメント、柔軟なクエリビルダー、および脅威インテリジェンスポータルのナレッジベースへのアクセスにより、調査能力が強化されています。これらすべてにより、効果的な脅威ハンティングと迅速なインシデント対応が促進され、損害の予防や抑制につながります。

使用事例

- ネットワーク全体をとおして侵入の証拠をプロアクティブに検索します
- 侵入者が重大な損害や混乱をもたらす前に、迅速に侵入を検出して修復します
- シームレスなワークフローにより、数多のエンドポイントにわたってインシデントを迅速に調査して集中管理を行います
- 他のセキュリティソリューションによって検出されたアラートと潜在的なインシデントを検証します
- 日常業務の自動化で、手作業を最小限に抑えてリソースを解放し、「アラートによる過負荷」の割合を削減します



Gartner peerinsights customers' choice 2020™

「Gartner Peer Insights Customers' Choice」で、2020年のEDRソリューションのトップベンダーにカスペルスキーが選出されました

2020年に、エンドポイントの検出と応答（EDR）ソリューションで、Gartner Peer InsightsのCustomers' Choiceに選出されたベンダーは、世界でわずか6つしかありません。カスペルスキーは、その6つなかのひとつであり、弊社のサービスやサポートは、他のどのベンダーよりも高い評価を受けております。これはカスペルスキーのEDRに対する、お客様からの最高の称賛です。

ガートナー免責事項

Gartner Peer Insights Customers' Choiceは、文書化された方法に対して出されたエンドユーザー個人の主観的な意見や評価、データに基づいたものであり、いかなる点でもガートナーまたはその関連会社の見解を表すものではありません。

MITRE | ATT&CK®

MITRE ATT&CK Evaluationによって立証された検出品質

複雑なインシデント調査におけるTTP（戦術、技術、手順）分析の重要性と、今日のセキュリティ市場におけるMITRE ATT&CKの役割

- Kaspersky EDRはMITRE Evaluationのラウンド2（APT29）に参加しており、今日の標的型攻撃の重要な段階で用いられるラウンド2スコープからの主要なATT&CK技術の検出において、高い性能を実証しています。
- Kaspersky EDRの検出は、攻撃者のTTPを詳細に分析するため、MITRE ATT&CKナレッジベースのデータにより強化されています。

詳しくは、kaspersky.com/MITRE をごらんください

カスペルスキーのEDRは、企業全体に対してつぎのようなビジネス上のメリットをもたらします

- セキュリティ上の隙をなくし、攻撃の「滞留時間」を短縮するのに役立ちます
- 脅威を検出して対応する際の手作業を自動化します
- IT担当者やセキュリティ担当者の拘束時間を短くし、他の重要な業務にあてることができます
- 脅威分析とインシデント対応を簡素化します
- 脅威を特定しそれに対応するために必要な時間を短縮します
- コンプライアンス強化に貢献します

お求めのものがもっとある場合はKaspersky Managed Detection and Responseをご利用ください

完全管理で、個別にカスタマイズされた24時間体制の防御をカスペルスキーのEDRに追加することで、IT関連のセキュリティリソースを節約することができます。これは、インシデント関連の処理タスクをカスペルスキーにオフロードすることで、具体的なシナリオを実行するのに十分な技能を持つセキュリティ専門職が社内チームに見あたらないときも、専門家の判断を仰いだり、他にはない脅威ハンティング専門技能を求めたりすることができるためです。

カスペルスキーのEDRについて詳しくは、こちらをごらんください。

kaspersky.com/enterprise-security/endpoint-detection-response-edr

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

www.kaspersky.com

実証済みの品質、独立性、透明性への取り組み。カスペルスキーは、安全な世界を作り上げ、テクノロジーを活かして人々の暮らしを良くすることを目指しています。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、kaspersky.co.jp/transparency をごらんください

Proven. Transparent. Independent.