kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

セキュリティを回避する未知の脅威から保護するための高度な検知機能 – IT セキュリティ専門スタッフが不足していても対応

今日の高度なサイバー攻撃には、企業の活動を停止させ、企業に金銭的な被害を与え、また企業イメージに大きな損害をもたらす力があります。複雑な脅威がもたらす、金融資産や営業秘密の窃取、サービス停止によるお客様からの信頼の喪失、その他多数の弊害によって、ビジネスの安定性と成功に深刻な影響が出ます。急速に進化するサイバー攻撃を防止するためには、ネットワーク境界部（ファイアウォール、メール / Web ゲートウェイ、プロキシサーバー）の保護、あるいはワークステーションやサーバーの保護（アンチウイルスによる保護や、基本機能を備えたエンドポイントプロテクションプラットフォームレベルのソリューション）を目的とした従来型のツールだけでは不十分です。そのため、企業は将来を見据えて、複雑なインシデントの検知、調査、対応のための専門ツールについて真剣に検討する必要があります。

Kaspersky Sandbox ソリューションの利用が最適な組織：

- 専門のセキュリティチームがなく、IT 部門が IT セキュリティの役割を担っている企業
- IT セキュリティリソースを割くことが困難な中堅中小企業
- インフラストラクチャが地理的に分散されており、オンサイトの IT セキュリティ担当者がいない大企業
- 自社の IT セキュリティアナリストが重要なタスクに注力させる必要のある企業

Kaspersky は 20 年以上にわたって、あらゆる規模、業界、IT セキュリティ成熟度の企業向けに保護ツールを開発してきました。脅威のハンティング、調査、対応の分野で継続的な研究開発を行い発展を遂げてきたことで、現在も第一線でサイバー犯罪と闘い続けています。

複雑な脅威に対抗するための Kaspersky の製品およびサービスのポートフォリオには、以下の製品が含まれています：

- Kaspersky Anti Targeted Attack：複雑な脅威や標的型攻撃をネットワークレベルで検知、調査するための最先端のソリューション
- Kaspersky Endpoint Detection and Response：ワークステーションやサーバーを標的とする複雑なサイバー脅威の検知、調査、対応のためのソリューション
- カスペルスキー脅威インテリジェンスポータル：Cloud Sandbox やその他のサービスへのアクセス用ポータルであり、APT 脅威に関する分析レポートを表示可能

しかし、これらのソリューションやサービスを効果的に活用するためには、適切な経験と専門知識を持つ本格的な IT セキュリティ部門の設置が必要になります。複雑な脅威に対処できるように訓練された技術者が世界的に不足しており、人件費がかかることが、この種のソリューションやサービスの購入を妨げる主な要因になっています。

特許取得済みの技術（特許番号 US 10339301B2）を基盤とする Kaspersky Sandbox は、既存のエンドポイント保護製品を回避する機能を持つ複雑な最新の脅威に対抗するための製品です。Kaspersky Sandbox は、 Kaspersky Endpoint Security for Business の機能をさらに強化し、高度な専門知識を持つ情報セキュリティアナリストがいなくても、未知のマルウェア、新しいウイルスやランサムウェア、ゼロデイエクスプロイト、その他の脅威に対するワークステーションやサーバーの保護レベルを大幅に引き上げることができます。

そのため、中堅中小企業はそのような人件費の高い専門スタッフの採用や雇用にかかる費用を抑えることができます。また、分散ネットワークを展開している大企業も、セキュリティアナリストの手作業による負荷を軽減しながら、リモートオフィスを効果的に保護するためのコストを最適化することができます。

実装、展開：

Kaspersky Sandbox は ISO イメージとして提供され、このイメージには CentOS 7 とすべての必須ソリューションコンポーネントがあらかじめ構成されています。このイメージは、物理サーバーまたは VMware ESXi をベースとする仮想サーバーにデプロイできます。

統合：

- SIEM システムは、Kaspersky Sandbox による検知状況に関する情報を受信できます。この情報は、一般的なイベントフロー内では Kaspersky Security Center 経由で送信されます。
- 他のソリューションとの統合用 API が Kaspersky Sandbox に実装されており、スキャン用にファイルを Kaspersky Sandbox に送信し、ファイルのレピュテーションを Kaspersky Sandbox に対してリクエストすることができます。

スケーラビリティ

基本設定では保護対象エンドポイントが最大 1,000 台サポートされており、スケーリングも簡単で、大規模インフラストラクチャ向けに継続的に保護できるようになっています。

クラスタリング

複数のサーバーをクラスタリングして、より高い性能と高可用性を確保できます。

ライセンス

Kaspersky Sandbox はソフトウェアアプライアンスとしてライセンス提供されます。1 ライセンスで最大 1,000 ノードの Kaspersky Endpoint Security for Business ユーザーがサポートされます。

仕組み

Kaspersky Sandbox は、複雑な脅威や APT レベルの攻撃を撃退してきた Kaspersky のエキスパートのベストプラクティスを活用しており、Kaspersky Endpoint Security for Business と密接に統合されています。管理は、Kaspersky のポリシーベースの統合管理コンソールである Kaspersky Security Center から行います。

Kaspersky Endpoint Security for Business のエージェントは、Kaspersky Sandbox サーバーにある判定データ用の共有運用キャッシュから、不審なオブジェクトに関するデータを取得するようリクエストします。オブジェクトがすでにスキャン済みである場合、Kaspersky Endpoint Security for Business はその判定データを受信し、以下の 1 つ以上の修復オプションを適用します：

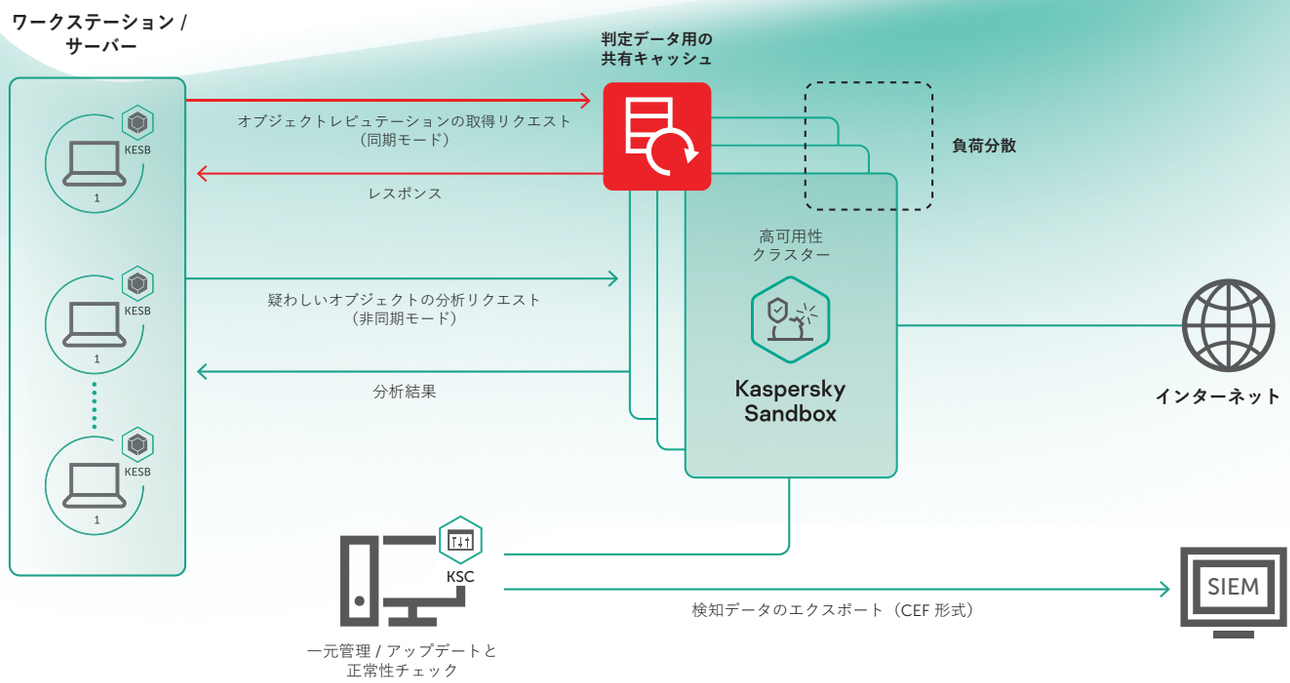
- 除去、隔離
- ユーザーへの通知
- 簡易スキャンの開始
- 検知されたオブジェクトを、管理対象ネットワーク内の他のマシンでも検索

オブジェクトのレピュテーションについての判定データをキャッシュから取得できない場合、Kaspersky Endpoint Security for Business のエージェントはその不審なファイルを Sandbox に送信して、レスポンスを待ちます。Sandbox はリクエストを受信してオブジェクトをスキャンし、この時点で、実際のインフラストラクチャから隔離された環境内で、そのテストオブジェクトが実行されます。

ファイルスキャンは、一般的な作業環境（オペレーティングシステムやインストール済みアプリケーション）をエミュレートし、各種ツールを配備した仮想マシン内で実行されます。オブジェクトの悪意のある意図を検知するために、ふるまい分析が実行され、アーティファクトが収集、分析されます。オブジェクトが悪意のある動作を実行している場合は、Sandbox はそのオブジェクトをマルウェアとして認識します。サンドボックス分析の実行中、オブジェクトに対して何らかの判定が割り当てられます。

オブジェクトのエミュレートプロセスが完了すると、判定結果がリアルタイムで判定データ用の共有運用キャッシュに送信され、Kaspersky Endpoint Security for Business がインストールされている他のホストもスキャン済みオブジェクトのレピュテーションに関するデータをすぐに取得できるようになります。同じファイルを再分析する必要はありません。このアプローチによって、疑わしいオブジェクトを迅速に処理して、Kaspersky Sandbox サーバーの負荷を軽減し、脅威に対する対応のスピードと効率性を高めることができます。

Kaspersky Sandbox は、Kaspersky Endpoint Security for Business をさらに強化します。リソースを追加せずに高度で複雑な未知の脅威が自動でブロックされるようになり、IT セキュリティアナリストが他のより重要なタスクに注力できるようになります。



サイバー脅威に関する最新情報：www.securelist.com
IT セキュリティに関する最新情報：business.kaspersky.com

www.kaspersky.co.jp

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-1047-201911