

Kaspersky Anti Targeted Attack Platform

今日のサイバー犯罪者は、システムに侵入し感染させるための、斬新な方法を独自に開発しようと、もっぱら取り組んでいます。脅威が進化を続け、さらに洗練されたものとなり、破壊的になるにつれ、迅速な検出と、迅速かつ適切な対応が、ともに重要になってきています。

企業は、IT関連のセキュリティについて、つねに見直しを続けることが重要になっており、

増大するサイバー脅威に対して一歩先んじるリードを保ち、経済的損失の発生を抑える必要があります。

統合型ソリューションにまとめられた比類なきサイバーセキュリティ

プロのサイバー犯罪者は、このところ、マルチベクトル型のアプローチを好んで採用しています。Kaspersky Anti Targeted Attack Platformは、ネットワークレベルの高度な脅威検出とEDR機能を組み合わせ、優れた多次元脅威検出処理、最先端技術の適用、効果的な調査の実施、脅威ハンティングのプロアクティブな実施、迅速で一元化された脅威への対応に必要なすべてのツールを、単一のソリューションにより、ITセキュリティを担当する専門職のために提供いたします。

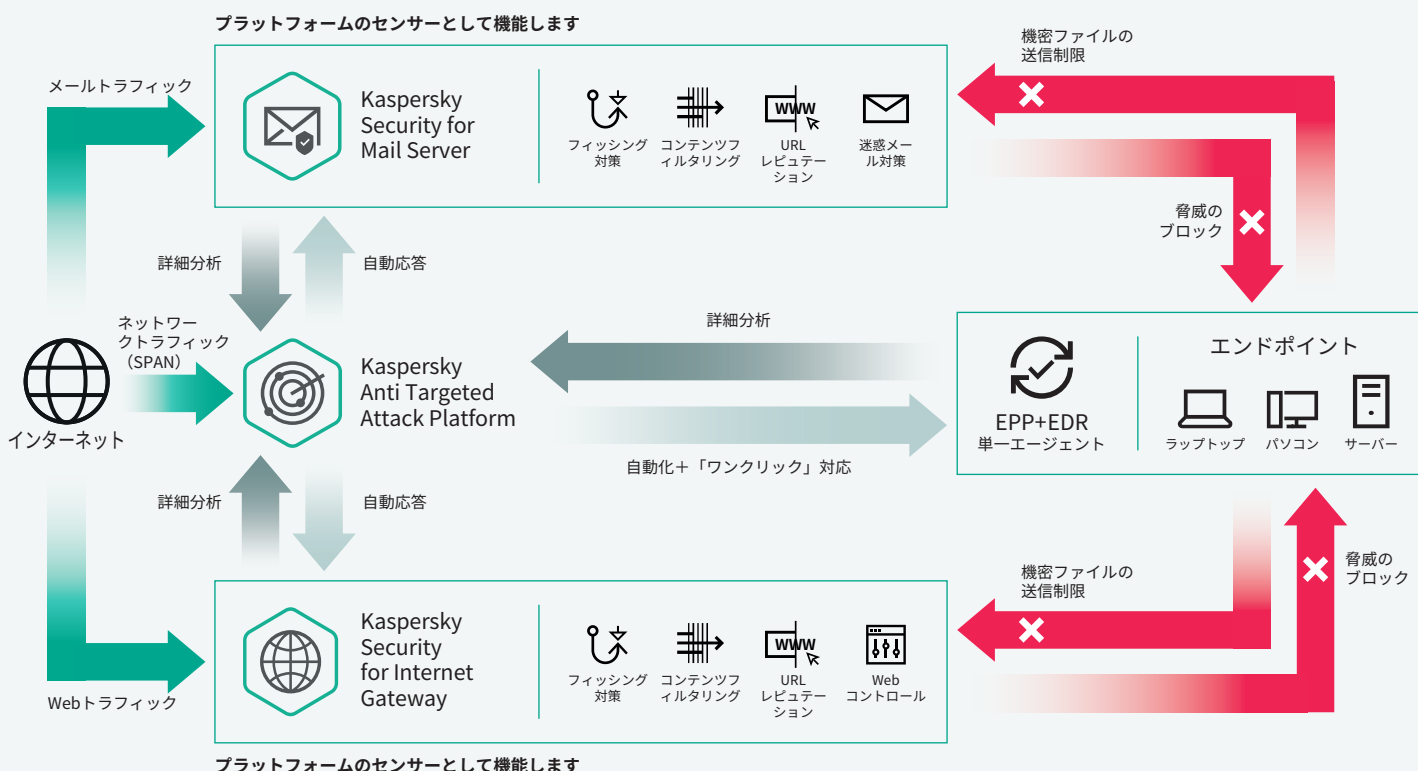
お客様の管理下で注目されるもっとも洗練された攻撃

このプラットフォームは、脅威の検出と対応が強化されたソリューションとして機能します。脅威に関する情報処理能力によって強化され、MITRE ATT&CKフレームワークにマッピングされた、オールインワンのAPT保護を実現します。すべての潜在的な脅威のエントリーポイント（ネットワーク、Web、メール、パソコン、ラップトップ、サーバー、仮想マシン）がお客様の管理下に入ります。

Kaspersky Anti Targeted Attack Platformは、**Kaspersky Endpoint Security for Business**と完全に統合され、単一のエージェントをKaspersky EDRと共有しています。また**Kaspersky Security for Mail Server**および**Kaspersky Security for Internet Gateway**の両方に統合されます。これらはプラットフォームのセンサーとして機能し、より複雑な電子メールやWebを介する脅威に対して自動的に対応します。

Kaspersky Anti Targeted Attack Platform

- 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
- 脅威分析とインシデント対応を簡素化します
- 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
- コンプライアンス強化に貢献します



プライバシーを完全に守ることができる信頼に足るセキュリティソリューション

すべてのオブジェクト分析がオンサイトで実行され、アウトバウンドのデータフローはありません。Kaspersky Private Security Networkは、企業データを完全な隔離状態に維持しつつ、インバウンドのレピュテーションをリアルタイムでアップデートします。

以下によりデジタル変革によるイノベーションを加速する統合型プラットフォームです。

- **統合による事業の継続。** 最初からセキュリティとコンプライアンスを新しいプロセスに組み込みます
- **企業のITインフラストラクチャを完全に可視化**します
- **このうえない柔軟性**により、現実の環境においても、仮想環境においても、可視性と制御が必要とされるあらゆる場所に展開できます
- **脅威を検出して対応する作業の自動化**により、お手元のセキュリティ、インシデント対応、SOCチームの費用対効果を最適化します
- **既存のセキュリティ製品との緊密で直接的な統合**により、セキュリティレベルを全体的に高め、レガシーセキュリティへの投資を無駄にしません

主な機能は以下のとおりです。



多層センサーアーキテクチャ - ネットワーク、Webおよび電子メールセンサー、エンドポイントエージェントの組み合わせにより、あらゆる面で可視化を実現します。



広範な脅威検出エンジン - ネットワークセンサー（ネットワークトラフィック分析）およびエンドポイントエージェント（EDR機能）からのデータを駆使して、迅速な判定を実現し、誤検知を減らします。



Advanced Sandbox - 脅威アクティビティの詳細分析のため安全な環境を提供し、OSコンポーネントのランダム化、仮想マシンでのアクセラレーション、回避技術対策、ユーザーアクティビティのシミュレーション、およびMITRE ATT&CKナレッジベースへの結果マッピングをサポートします。これらすべてが、行動ベースの検出の効率向上に貢献します。



遡及分析 - 感染したエンドポイントにアクセスできなかったり、データが暗号化されている場合でも、自動化されたデータ、オブジェクトと判定のコレクション、および一元化されたストレージを通じて遡及分析が行えます。



インタラクティブな脅威インテリジェンスの2つのモード - Kaspersky Security Networkからの地球規模のレピュテーションデータとの自動比較、および、Kaspersky Threat Intelligence Portalを介する手動脅威ハンティングと調査クエリ。



リアルタイムの自動脅威ハンティング - イベントは、カスペルスキーの脅威ハンターによって生成された攻撃の痕跡（IOA）の固有のセットと関連付けられ、MITRE ATT&CKマトリックスにマッピングされ、明確なイベントの解説や実例を提供して、推奨される対応を実行します。



強力で柔軟なクエリビルダーによるプロアクティブな脅威ハンティング - 分析者は複雑なクエリを作成し、非定型的な行動や疑わしいアクティビティ、およびお手元のインフラストラクチャに固有の脅威を検索することができます。

要点

今日、企業が長期間にわたって成長を持続させるには、確実なデータ保護、ITインフラストラクチャのセキュリティ、ビジネスプロセスの安定化、コンプライアンスの遵守が欠かせません。

Kaspersky Anti Targeted Attack Platformを利用すれば、他のITセキュリティリソースに頼ることなく、APTに類する脅威から企業インフラストラクチャを確実に保護する防御を構築し、コンプライアンスの遵守を支援し、成熟したITセキュリティを備えることができます。自動化を活用して質の高い成果を出す一体型ソリューションにより、複雑なインシデントに対して迅速に特定・調査・対応することで、ITセキュリティチームやSOCチームを手作業から解放し、効率性を向上します。

業界でもっとも効果的なソリューションであることが証明されています



SE Labsは、Kaspersky Anti Targeted Attack Platformに、さまざまなハッキング攻撃を加えて試験し、トリプルAの評価を与えました。



ICSA Labsによる独自試験「Advanced Threat Defense (Q3 2019)」では、Kaspersky Anti Targeted Attack Platformは検出率100%を示し、誤検出はゼロでした。



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

Radicatiグループは、持続的標的型攻撃 (APT攻撃) 対策部門のトッププレイヤーとして、カスペルスキーを選出しました (2020年Market Quadrant)。



「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つしかなく、カスペルスキーはそのひとつです。弊社の拡張EDRソリューションKaspersky Anti Targeted Attack Platformは、カスペルスキーのEDRを中核としており、お客様から最高の称賛をいただいております。

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

Kaspersky Anti Targeted Attack Platformの中核要素であるカスペルスキーのEDRは、MITRE評価のラウンド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主要なATT&CK技術の検出において高い性能を実証しております。

詳しくは、kaspersky.com/MITREをごらんください

Kaspersky Anti Targeted Attack Platformについて詳しくは、こちらをごらんください。

kaspersky.com/enterprise-security/anti-targeted-attack-platform

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

2020 AO Kaspersky Lab.
登録商標およびサービスマークはそれぞれの所有者に帰属します。



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。安心して未来のために、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.