



Kaspersky Anti Targeted Attack



今日のサイバー犯罪者は、システムへの侵入と侵害を目的として、前例がなく斬新な方法を開発することに特化しています。脅威がますます進化し、より巧妙で破壊的なものに変化していく中、これらを短時間で検知し、最速かつ最も適切なレスポンスを行うことが、いずれも不可欠となっています。



脅威の特定とレスポンスに要する時間を短縮

脅威分析とインシデントレスポンスを簡素化

セキュリティギャップを解消し、攻撃の「滞留時間」を短縮

脅威の検知とレスポンスにおける手動タスクを自動化

ITセキュリティ担当者の作業負担を緩和し、より重要なタスクへの専念を促進

企業コンプライアンスを支援

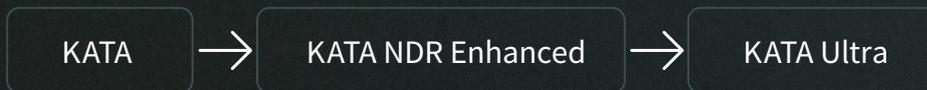
他の追従を許さないサイバーセキュリティ：APTと高度な脅威に先手を打つ

Kaspersky Anti Targeted Attack (KATA) は、APTのような脅威や標的型攻撃から企業インフラを保護し、企業コンプライアンスをサポートする信頼性が高い防御の構築を支援します。ITセキュリティリソースを新たに追加することなく、複雑なインシデントをすぐに特定、調査し対応できる環境を構築できます。また、自動化を最大限に使用し、成果の質を高める統合ソリューションにより、ITセキュリティチームやSOCチームを手動タスクから解放し、業務効率を向上させます。

Kaspersky Anti Targeted Attackは、APT攻撃に対する総合的な保護機能を搭載しており、あらゆる高度なサイバー脅威から組織や企業を保護します。基本的なNDR機能と高度なNDR機能から選択し、EDRソリューションと組み合わせてネイティブXDRのシナリオを作成することが可能です。これにより、ITセキュリティの担当者は、脅威を多面的なアプローチで検知する優れた機能、最先端技術の適用、効果的な調査、予防的な脅威ハンティング、高速で一元的なレスポンスの実現に必要なすべてのツールを手に入れることができます。

柔軟性の高い選択肢

APT対策を3つのレベルで実現：

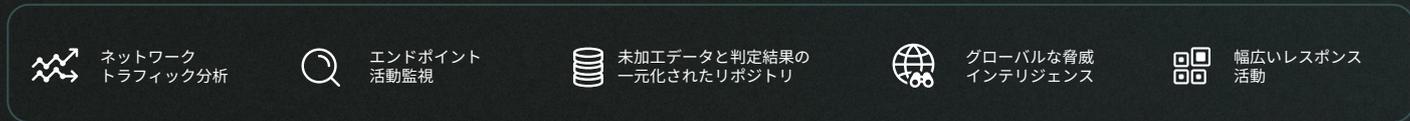


比較

	KATA	KATA NDR Enhanced	KATA Ultra
基本的なNDR機能			
・ ネットワークトラフィックの監視と高度な検知エンジン			
・ TLSフィンガープリンティング			
・ IDSアラートに関連するPCAP	●	●	●
・ URLレピュテーション分析			
・ IDSルール（外部-内部トラフィック）に基づく侵入検知			
・ ネットワーク誘導型レスポンス			
・ ゲートウェイレベルの自動レスポンスとICAP連携のブロックモード			
高度なサンドボックス	●	●	●
Kaspersky Threat IntelligenceとMITRE ATT&CKによるリッチ化	●	●	●
基本的なNDR機能			
・ プロトコルを定義するDPI			
・ IDSルール（内部トラフィック）に基づく侵入検知			
・ ネットワークセッションテーブル、ネットワークマッピング、インベントリモジュールによるネットワークの完全可視化			
・ ネットワークテレメトリ分析およびエンドポイント監視（EPP Linux、Windows）		●	●
・ ネットワークセキュリティリスク（未承認デバイス、ARPスプーフィングなど）からの保護			
・ 未加工のトラフィック（PCAP）の保存とレトロスペクティブ分析			
・ APIコネクター経由でのネットワークデバイスのレスポンス			
・ 異常検知			
・ シャドーITの検知			
高度なEDR機能			●
ネイティブXDRの機能			●

新たなレベルのセキュリティ対策

Kaspersky Anti Targeted Attackは、オールインワンのAPT対策ソリューションです。脅威インテリジェンスを搭載し、MITRE ATT&CKフレームワークに対応しています。ネットワーク、Web、メール、PC、ノートPC、サーバー、仮想マシンなど、脅威の侵入経路となる可能性がある、あらゆるポイントを管理下に置くことができます。



脅威の検知とレスポンスタスクの自動化

セキュリティ、インシデントレスポンス、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明快な連携

セキュリティレベルを全体的に向上させるとともに、従来のセキュリティへの投資も無駄なく活用することが可能です



完全な可視性

企業のITインフラを完全に可視化します



最大限の柔軟性

物理環境でも仮想環境でも、可視性と管理が必要なあらゆる場所への導入が可能です

Kaspersky Threat Intelligenceによるアラートのリッチ化



Kaspersky
Threat
Intelligence

1億個以上のセンサー、悪意のあるファイルと正当なファイルの膨大なリポジトリ、ダークウェブ、そして継続的な脅威ハンティングとインシデントレスポンス活動から収集された、包括的なインテリジェンスを使用できます。

Threat Intelligence Portalへは、KATAアラートから直接アクセスすることができます：不審なファイルの分析、その他の観察対象との関連性のチェック、実用的なコンテキストの追加などが可能です。

Kasperskyを選ぶ理由



世界的な認知度と国際的な評価



実証済みの技術的な実効性



透明性とコンプライアンス



世界トップクラスの豊富な経験と
専門知識



ITセキュリティ業界全体における
高評価



28年に及ぶ比類なき顧客保護
の実績



Kaspersky
Anti Targeted
Attack

[詳細はこちら](#)

www.kaspersky.co.jp

© 2026 AO Kaspersky Lab.登録商標およびサー
ビスマークは、各所有者の財産です。

#kaspersky
#bringonthefuture