製品カタログ

Deep Discovery™シリーズのご紹介

標的型攻撃に対する高度な脅威防御システム

概要

標的型攻撃や高度な脅威は、従来のセキュリティ対策を回避するようにカスタマイズされています。これらの攻撃は、その身を隠しながら、お客さまの組織やビジネスに関連するデータ、知的財産、そして通信データを盗み出すだけでなく、身代金と引き換えに重要なデータを暗号化します。セキュリティ分析者やセキュリティ専門家の間では、標的型攻撃や高度な脅威を検知するためには、企業のIT戦略の一環として、高度な検知技術を採用するべきであることが広く認められています。

トレンドマイクロのDeep Discoveryは、独自の検知エンジン、カスタムサンドボックス、およびTrend Micro Smart Protection Network™ によるグローバルな脅威インテリジェンスを活用することで、これまでの検知技術を回避する標的型攻撃を検知、分析、対応することができる高度な脅威防御製品です。そして、通常のセキュリティ製品では発見が難しい攻撃に対して、高い検知率を実現します。また、Deep Discoveryは、他のトレンドマイクロ製品や他社セキュリティツールと連携することで、組織全体に対する高度な脅威への保護を実現します。

主なメリット

高度な検知機能による未然の攻撃防御

独自技術による脅威検知機能により、被害が発生する前に攻撃を検知

脅威インテリジェンスによる迅速な対応

Deep Discoveryとトレンドマイクロのグローバルな脅威インテリジェンスで、迅速かつ効果的なインシデントレスポンスをサポート

他のセキュリティ対策との連携

Deep Discoveryと既にお使いのトレンドマイクロ製品および他社セキュリティツールの連携で、標的型攻撃を未然に防止

複合型の脅威からの防御

世代を超えた手法を取り交ぜることで、状況に合わせて適切なセキュリティ技術を利用
トレンドマイクロの侵入防御システムであるTippingPoint™と緊密に連携することで、既知、未知および未公開の脅威を検知、防御

Deep Discovery™ Inspector (以下DDI) は、全てのネットワークポートで100以上のプロトコルとアプリケーションのネットワークトラフィックを監視するネットワーク製品です。独自の検知エンジンやカスタムサンドボックスにより、マルウェアやC&Cサーバへの通信、攻撃の予兆を示す活動を検知します。そして、検知された情報は、お客さまによる迅速な対応を支援するだけでなく、エンドポイントなど他のセキュリティ製品と共有、連携することで、さらなる攻撃をブロックすることができます。

Deep Discovery™ Analyzer (以下DDAN) は、カスタムサンドボックスを採用し、お使いのセキュリティ製品のマルウェア検知能力の向上をサポートする、脅威分析ソリューションです。この製品は、多くのトレンドマイクロ製品と連携したり、手動での検体分析をサポートしたりするとともに、オープンなWebサービスインタフェースを介してその他の製品から検体を受け取り、その分析結果を共有することが可能です。またDDANは他のDeep Discovery製品の追加サンドボックスとして機能することで、トレンドマイクロおよび他のセキュリティ対策製品の機能拡張にもご活用いただけます。

DDIのXDR連携 (以下XDR連携) は、攻撃に対する重大さに応じて優先度を提供します。XDR連携は、DDIにより検知可能な明示的な攻撃と、ネットワークのメタデータを活用してネットワークアクセスのイベントを相互に関連づけて相関するルールを適用することで、攻撃のライフサイクル全体を可視化、分析を可能にします。

Sandbox as a Service for Deep Discovery™ Inspector Virtual Appliance (以下Sandbox as a Service for DDIVA) は、Deep Discovery™ Inspector Virtual Appliance (以下DDIVA) のアドオンであり、高度なクラウド型サンドボックスを提供します。組織のセキュリティチームは、このアドオンによる仮想型もしくはクラウド型のサンドボックスを活用することで、高度な脅威や標的型攻撃からお客さまの環境を保護できます。

FORRESTER®
WAVE LEADER 2023
Network Analysis And Visibility

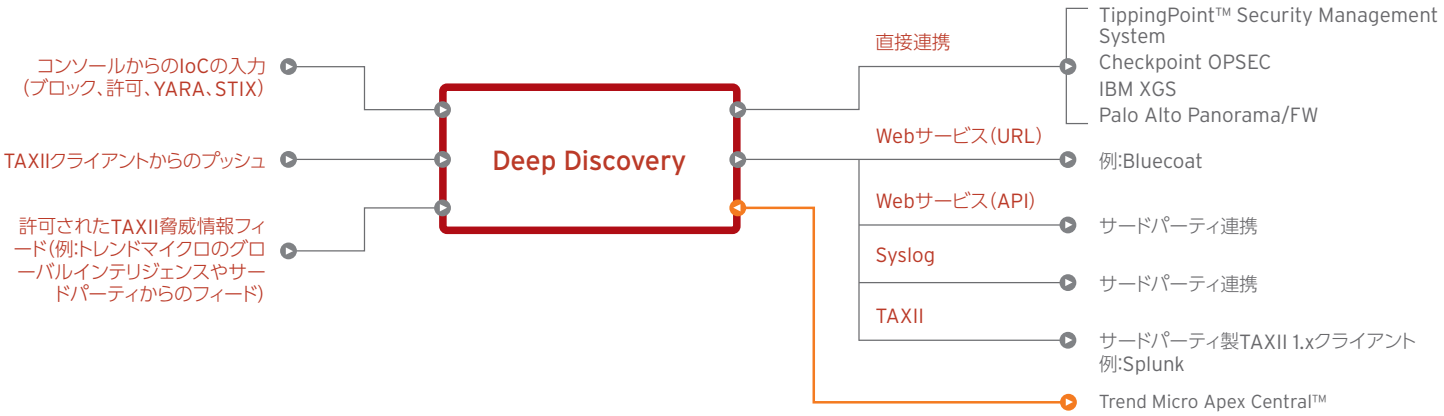
主な機能

- **ネットワークのコンテンツの検査**：DDIでは物理、仮想を跨がるネットワークの全トラフィック、100以上のプロトコルを監視。ネットワーク内部での横展開、C&C通信など、攻撃ライフサイクル全体に見られる攻撃者の活動に加えて、ネットワークで送受信されるトラフィックから、標的型攻撃、ランサムウェアを検知。
- **広範な検知技術**：ファイル、Web、IP、モバイルAppの各レピュテーション、ヒューリスティック分析、高度な脅威分析、サンドボックス、脅威情報の相関分析を活用し、ランサムウェア、ゼロデイの悪用などの攻撃活動を検知。
- **カスタムサンドボックスによる分析**：お客さまが利用するオペレーティングシステム (OS) 、ドライバ、アプリケーション、および言語を反映した仮想イメージを利用可能。一般的な仮想イメージを回避する高度な脅威、ランサムウェアを検知。

- **柔軟な配置**：DDANは単独のサンドボックスとしての利用に加えて、DDIを大規模に配備いただく場合に、個々のDDIのサンドボックス機能の拡張として利用可能。1台のアプライアンスで最大60のサンドボックスをサポートし、複数のアプライアンスをクラスタリングして可用度を向上、ホット・コールドスタンバイでの設定も可能。DDIはお使いの環境に合わせて、アプライアンスとバーチャルアプライアンスの2種類を提供。
- **拡張された検知と対応（XDR）**：XDR連携を、XDR機能をフル活用するためのSaaS型ソリューションとして利用可能。仮想もしくは物理サーバを通じて、オンプレミス環境でも、XDRソシューションの恩恵を享受。
- **高度な検知**：静的分析、ヒューリステック分析、挙動監視、Webレピュテーション、ファイルレピュテーションにより、迅速な検知が可能。DDIでは、外部への通信、不審なファイルからのC&Cへの度重なる通信、マルチステージマルウェアも検知。
- **脅威情報**：Deep Discoveryシリーズでは、STIX、TAXII、YARAなどの標準フォーマットを利用し、脅威情報を相関分析、共有可能。これによりネットワークに侵入する脅威の情報を先んじて入手、対応可能。
- **脅威分析**：わかりやすい脅威の可視化。優先度を上げて対応すべき脅威に加えて、ネットワークのどこから脅威が侵入し、どのようにネットワーク内を移動し、誰に影響を与えたかを一つのコンソールで確認。ネットワーク内部の攻撃の流れをビジュアルで再現して確認することも可能。トレンドマイクロのZero Day Initiative™ をサポートする15か所のグローバル研究センターと1万名を超える内外の研究者により、脅威状況の全体像を可視化。
- **統合**：Deep Discoveryシリーズは、サードパーティ、他のトレンドマイクロ製品と連携を前提に設計。製品独自の連携に加えて、豊富なAPIにより、レスポンスの自動化、Indicators of Compromise（IoC）の共有、高度な攻撃や標的型攻撃防止の自動化をサポート。

お客さまのSOCを強化

脅威がどこから侵入し、どのように阻止できるかを理解することが、セキュリティ担当者には求められています。これは攻撃者優位な状況下で割りに合わない作業に思われるかもしれませんが、非常に重要な作業です。Deep Discoveryシリーズでは、STIX、TAXII、YARAなど、脅威情報の取り込みやカスタマイズのための標準的なフォーマットを利用。最新、高度な脅威情報やIoCを取り込み、SOC担当者や他のセキュリティ担当者が最新の脅威へ対抗するサポートを提供します。さらにネットワーク内のトレンドマイクロおよびサードパーティのセキュリティソリューションにIoCを共有することも可能です。このIoC共有の仕組みを構築することで、Deep Discoveryシリースでは、未知の脅威を接続されたすべてのセキュリティ対策製品によって検知できるようにするとともに、高度な脅威にも迅速に対応できるようになります。



サンドボックス製品であるDDANは、他のセキュリティ製品から自動的にIoCを取得し、それを起点にして分析を行うとともに、結果を自動的に返信します。これにより、この分析結果をさらなる対応に活用することができます。また、手動で登録、解析依頼された検体に対して、DDANにより潜在的な脅威や疑わしいファイルなどに対する回答を提供、スレットハンティングをサポートします。

対処の優先順位付けとシンプル化

セキュリティ対策製品は組織を攻撃する脅威の検知、警告、ブロックには長けている反面、製品が発する警告には、インシデントレスポンスに直接利用できるものと、さらなる分析が必要なものも含まれています。1日数千もの警告やログから有効な情報や今対応が必要な本当の脅威を見つけ出すことは、セキュリティ担当者の手腕にかかっています。

XDRとの連携により
攻撃の重要度を簡潔に表示：

攻撃の端緒は?

攻撃は組織内の誰に影響?

攻撃はどこに情報を送出(C&C)?

XDR連携により提供されるサンキーチャート（上図）によって、セキュリティ担当者は6ヶ月前まで遡り、実行された攻撃の全てのステップを確認できます。XDR連携は、ネットワークのトフラフィックから継続してメタデータを取得。これらのイベントをデータベースで相関分析し、リアルタイムで可視化します。これにより、少ないリソースで迅速な対応を可能にするとともに、影響を受けた機器など、攻撃の全体像を把握できます。ある攻撃は今日開始されたように見えることもありますが、実際にはネットワークへの最初の侵入は数週間前に行われていたということもあります。XDR連携では、データを相関分析、攻撃の全てのステップをマッピングし、適切な対応、将来の攻撃への適切な予防の考え方を提供します。

Trend Vision One™ の重要なパーツ

Trend Vision OneのXDR機能は、メール、エンドポイント、サーバ、クラウドワークロード、ネットワークの領域を超えて、ネットワークのレイヤーをまたがる検知を可能にします。またより広範な可視化、専門家によるセキュリティの分析を提供することで、より少ない警告と信頼性の高い検知による、攻撃の早期ステージにおける迅速な対応を提供します。トレンドマイクロのXDRにより、お客さまは脅威に効率的かつ効果的に対処するとともに、組織に対する攻撃の深刻度、影響範囲を最小化することができます。DDIのXDR連携は、XDRソリューションの重要な構成要素であり、エンドポイント対策などの対策を徹底しづらいパートナー企業やサードパーティのシステム、IoTやIIoT機器、複合機、さらには従業員のBYOD端末といった管理対象外のシステムからの重要なログを収集、システム全体の可視化を提供します。

トレンドマイクロ株式会社

お問い合わせ先

www.trendmicro.com

TREND MICRO、Trend Micro Smart Protection Network、Deep Discovery、Deep Discovery Inspector、Apex One、Apex Central、ZERO DAY INITIATIVE、およびVision Oneは、トレンドマイクロ株式会社の登録商標です。本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。記載内容は2023年9月現在のものです。内容は予告なく変更になる場合がございます。
Copyright © 2023 Trend Micro Incorporated. All rights reserved.

BR-DD-045