Solution Brief

Trend Vision One - Endpoint Security™

エンドポイントやサーバ、クラウドワークロードに最適化された防御・検知・対処を提供

Trend Vision One – Endpoint Security™（以下、Endpoint Security)は、エンドポイントやサーバ、クラウドワークロード向けに脅威に対する高度な防御機能やEDR/XDR、および脅威インテリジェンスを統合した最先端のエンドポイント向けセキュリティソリューションです。

Endpoint Securityによって、セキュリティ運用の複雑さを軽減し、 オンプレミスやクラウド、マルチクラウド、ハイブリッド環境に必要なセキュリティをご提供します。

また、サードパーティ連携も可能な最新のサイバーセキュリティプラットフォームであるTrend Vision One™の一部として、 エンドポイントやワークロードのセキュリティを他のセキュリティ製品や脅威情報、SIEM、オーケストレーションツール、パイプラインツール、ASMなど、さまざまな機能と統合できます。

Endpoint Securityは、多様なIT環境をサポートし、ワークフローの自動化とオーケストレーションをご支援し、専門的なサイバーセキュリティのサービスもご提供することで攻撃をいち早く阻止し、サイバーリスクの低減に貢献します。

Trend Vision Oneに統合されたEDR

Trend Vision Oneに統合されたEDR機能にはさまざまなメリットがあります。

- リスクスコアが付与されたアラートと包括的なインシデントビューを提供
- Linux/Windowsの違いに関わらず、攻撃の根本原因と実行プロファイルを調査して、その範囲を明らかにしたうえで、対処を実現
- 強力なクエリからシンプルなテキスト検索まで、複数の方法で脅威を探索し、攻撃テクニックを特定し、環境内の疑わしい活動を検証
- トレンドマイクロの自動インテリジェンスまたはカスタムインテリジェンススイープにより、新たに発見されたIoC(Indicators of Compromise、侵入の痕跡)を継続的に検索

運用を考慮した単一ソリューション・単一コンソール

情報の可視化や製品の管理・運用、ライセンス管理、役割ベースのアクセス制御をひとつのソリューション、ひとつのコンソールに集約し、ユーザのエンドポイント、サーバ、クラウドワークロードを保護します。さらに、ひとつのコンソールからエンドポイントの把握や脅威の検出、脅威への対処、ポリシーなどを管理できます。

保護対象

- クライアントPC
- サーバ
- クラウドワークロード
- 物理マシン
- 仮想マシン

対応OS

対応OSの詳細は**こちら**

提供機能

- 高度な機械学習型検索による不正プログラム対策
- ふるまい検知/挙動監視による不正プログラム対策
- パターンマッチ型の不正プログラム対策
- ダメージクリーンナップ
- IPS(侵入防御)
- Webレピュテーション
- ファイアウォール
- 情報漏えい対策 (DLP)
- デバイスコントロール
- アプリケーションコントロール
- 変更監視
- セキュリティログ監視
- XDR

エンドポイント向けのセキュリティ機能

自動化された高度なセキュリティ機能と業界をリードする最新の脅威インテリジェンスにより、増え続けるさまざまな脅威から保護対象を守ります。

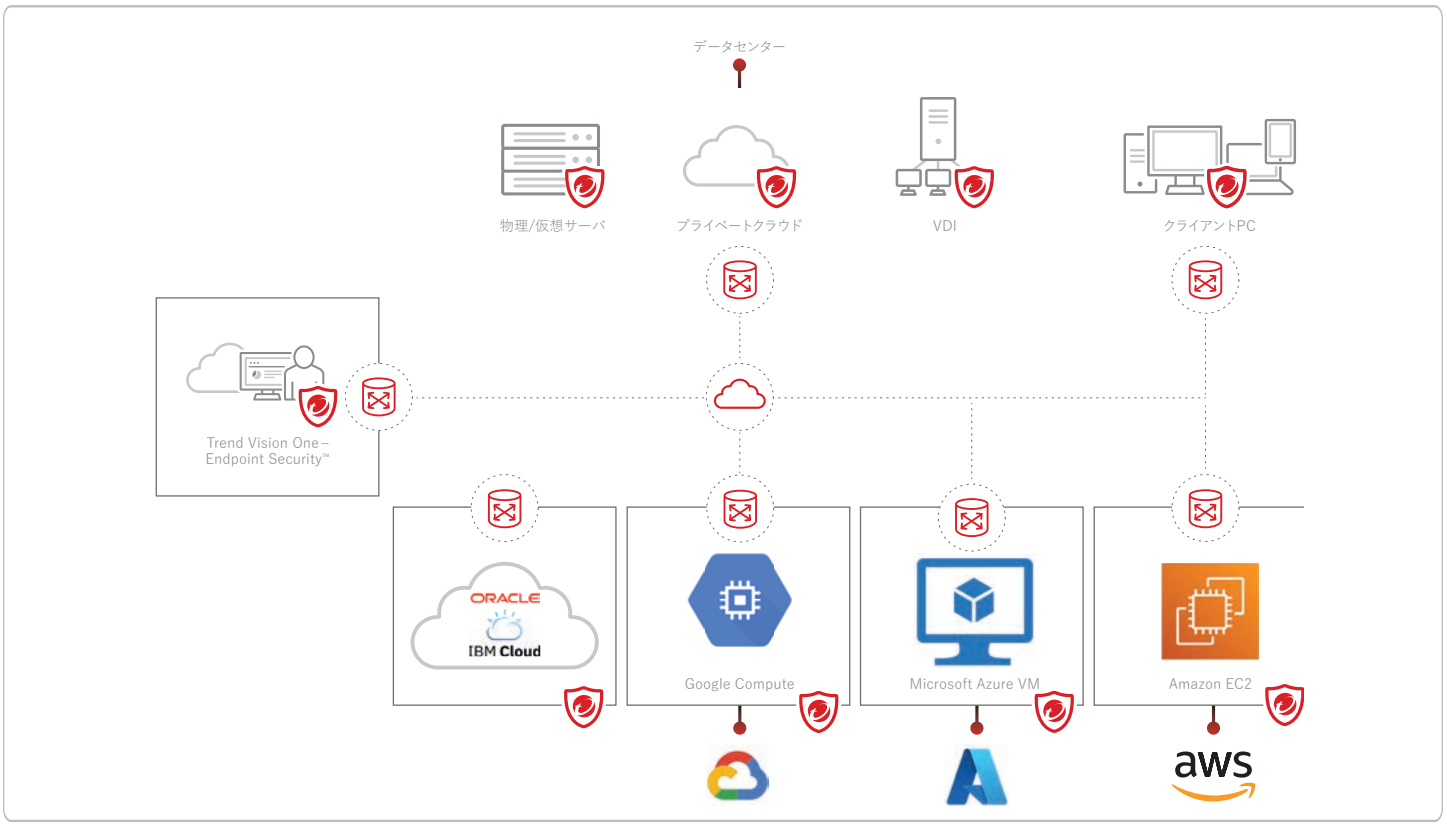
ランサムウェアを含む最新の不正プログラム対策やデバイスコントロール、ホストベースの侵入防御(IPS)、アプリケーションコントロール、機械学習/AIなどを利用した多層的な防御や検出、対処機能を備えているため、仮想デスクトップやサーバ、クラウド上のワークロードをリアルタイムで保護できます。

サーバやクラウドワークロードに必要なセキュリティ機能

「エンドユーザのクライアントPCは、メールやWebサイト、クラウドサービス、USBドライブなどを通じて日々脅威にさらされています。一方で、サーバやクラウド上のワークロードは、ソフトウェアや設定の脆弱性、システム内の横展開、さらには盗まれた従業員の資格情報などが攻撃者に悪用されます。このような脅威への晒され方の違いにより、エンドユーザの利用するクライアントPCとサーバ/クラウド上のワークロードにはそれぞれ明確なセキュリティ要件とセキュリティ方針が必要になります」とGartnerは評しています。(※1)

Endpoint Securityは、サーバとクラウド上のワークロード環境向けに設計された高度なセキュリティ機能を提供し、サーバとクラウド上のワークロードを脆弱性やマルウェア、不正な変更作業から保護します。サーバやクラウド上のワークロード向けの高度なセキュリティ機能には、サーバ用の侵入防御(IPS)や変更監視、セキュリティログ監視、コンテナ保護も含まれます。

さらに、AWS、Microsoft Azure、Google Cloudなどのクラウド上で稼働するワークロードを自動的に検出する機能により、クラウド上で増減するワークロードをシームレスに保護します。



[1] Gartner, Prioritizing Security Controls for Enterprise Servers and End-User Endpoints (Evgeny Mirolyubov, Peter Firstbrook, January 2023)

主要なメリット

高度な脅威対策

- 侵入防御(IPS)や変更監視、機械学習、アプリケーションコントロールなどの高度なセキュリティ機能により、脅威や不正なソフトウェアの実行をリアルタイムで検出してブロック
- 侵入防御(IPS)が配信する仮想パッチにより、既知、および新たに発見された脆弱性から保護することで、ベンダーの正規パッチを適用するまでシステムを既知及び、未知の脅威から保護
- 疑わしいアクティビティ、または悪意のあるアクティビティが検出された場合は、アラートを送信し、プロアクティブな防止策を提供
- トレンドマイクロのグローバルドメインレピュテーションデータベースからWeb レピュテーション用の脅威インテリジェンスを使用して、Webサイトの信頼性を検証し、リスクのあるサイトからユーザを保護
- ボットネットと標的型攻撃のC&C通信を特定してブロック

ハイブリッドクラウド向けの最新のクラウドネイティブなセキュリティ

- クラウド上のワークロードは何もしない状態だとインスタンスを起動した瞬間から脆弱な状態になるため、Endpoint SecurityはワークロードAWSやAzure、 Google Cloud、VMware、Microsoft Active Directoryと連携して、 ワークロードが作成された瞬間から保護を提供
- 環境ごとに異なる製品を導入するコストを削減し、単一コンソールで物理サーバ、仮想サーバ、クラウド、コンテナ、およびユーザのクライアントPC環境全体で一貫したセキュリティを実現
- 変更監視とセキュリティログ監視機能で DockerとKubernetes上の変更と攻撃を監視
- 侵入防御(IPS)によるコンテナの脆弱性対策、リアルタイムのマルウェア対策、およびコンテナ間のトラフィックの検査を通してコンテナのランタイムを保護

クライアントPCとサーバ、およびそこで稼働するアプリケーションに対する脆弱性対策と侵入防御

侵入防御機能は、既知、またはゼロデイの脆弱性を狙った攻撃やSQLインジェクション、クロスサイトスクリプティング、その他のWebアプリケーションの脆弱性を狙う攻撃からお客さまの環境を守るのに役立ちます。

トレンドマイクロの脆弱性対策と侵入防御は、ベンダーの正規のパッチを適用するまでの間、既知の脆弱性を保護するための仮想パッチを提供します。こうした機能は、世界をリードするバグ報奨金プログラムである、Trend Micro™ Zero Day Initiative™(ZDI)によって裏付けられています。

変更監視

変更監視機能は、レジストリ値、レジストリキー、サービス、プロセス、インストールされているソフトウェア、ポート、ファイルに対する予期しない変更を検出します。

ベースラインとなる安全な状態を比較対象として、変更監視モジュールがスキャンを実行し、予期しない変更を検出した場合はイベント（およびオプションのアラート）をログに記録します。

費用対効果の高いコンプライアンスの実現

- ひとつに統合されたコスト効率の良いソリューションでGDPRやHIPPA、NISTなど主要なコンプライアンス要件への対応を支援します
- 攻撃に対する防御の状況と、コンプライアンスへの対応状態をまとめた詳細な監査レポートを提供します
- 監査に必要な準備時間や労力を削減します

Linux環境の保護

Endpoint Securityは、Solaris™、AIX、HP-UXを含むLinuxのビルドやカーネルを幅広くサポートします。

セキュリティログ監視

セキュリティログ監視機能は、OSやアプリケーションのログに埋もれている可能性のある重要なイベントの特定を支援します。セキュリティログ監視機能で実現できることは以下の通りです。

- 不審な挙動の検出
- 異なるOSやさまざまなアプリケーションを含む多様な環境全体を通したイベントの収集
- ディスク容量のひっ迫やサービスの開始/シャットダウンなど、エラーやイベント情報の表示
- 管理者のログイン/ログアウトやアカウントのロックアウト、ポリシーの変更など、管理者のアクティビティの監査証跡の作成・維持

Endpoint Security のセキュリティログ監視機能を使用すると、サードパーティ製品のログファイルもリアルタイムで分析できます。

セキュリティログ監視ルールとデコーダは、多様なシステムに渡ってイベントを解析、分析、ランク付け、相関付けるためのフレームワークを提供します。

Trend Vision One – Endpoint Security ライセンス別提供機能

	Core	Essentials	Pro
推奨環境	XDR要件なしの クライアントPC環境	XDR要件ありの クライアントPC環境	サーバ環境
Windows, Linux, and Mac OS	•	•	•
不正プログラム対策（パターンマッチ型）	•	•	•
不正プログラム対策（ふるまい検知/挙動監視）	•	•	•
不正プログラム対策(機械学習型検索)	•	•	•
Webレピュテーション	•	•	•
デバイスコントロール	•	•	•
DLP	•	•	
ファイアウォール	•	•	•
アプリケーションコントロール	•	•	•
侵入防御 – IPS（クライアントPC向け）	•	•	
侵入防御 – IPS（サーバ向け）			•
変更監視			•
セキュリティログ監視			•
EDR/XDR		•	•

Trend Vision Oneでできること

- マルウェアやランサムウェアからの保護： 不正プログラムやランサムウェア、悪意のあるスクリプトなどの脅威からエンドポイントを保護さらに高度な保護機能によって、ステルス性の高い未知の脅威からも保護
- XDRをひとつのコンソールで実現：メールやエンドポイント、サーバ、クラウドワークロード、およびネットワークなど、クロスレイヤーの検出や脅威ハンティングによってEDRを超えたXDRを実現
- タイムリーな仮想パッチの提供： 正規パッチを適用するまでの間、仮想パッチによって脆弱性対策を提供
- ランサムウェアからのロールバック：パターンマッチ型以外に、機械学習型検索やふるまい検知型の不正プログラム対策などによってランサムウェアを検出し、暗号化プロセスをブロック。さらにロールバックにより、検出前に暗号化された任意のファイルを復元
- 運用担当者が、複雑な脅威アクティビティを迅速に理解するために活用できる高度な生成AI機能・Trend Vision One – Companionも提供
- Trend Micro Zero Trust Risk Insightsが、脆弱性や設定不備、資産の重要性、XDR、異常、クラウドアクティビティに関するリスクを算出
- Trend Vision One は、多様なレイヤー向けに自社開発のXDRセンサーを提供
- Trend Vision OneのXDRとASMに対する自社製品を中心としたハイブリッドアプローチは、保護対象のレイヤー全体に対して検出データだけでなく、より多くのアクティビティデータを提供。これにより、より早期かつ正確なリスクと脅威の検出と、効率的な調査を実現

Trend Vision Oneは、環境内のエンドポイントをはじめとするネイティブなセンサーから収集されたアクティビティデータをAIや豊富なナレッジによって分析し、誤検知/過検知が少ない精度の高いアラートを生成します。

トレンドマイクロの脅威インテリジェンスである Trend Micro™ Smart Protection Network™と、スレットエキスパートが日々更新する検出ルールを組み合わせて、AIの能力を最大限に活用し、
比類ない方法で分析モデルを作成します。

多層防御で防御力を最大化

Endpoint Securityは、保護機能を多層的に組み合わせてシステムを保護し、効率的に多様な脅威に対する保護を実現します。

さらに、XDRによって各レイヤーの情報をTrend Vision Oneに集約することで、環境全体を俯瞰した脅威の調査・検出・対処能力が大幅に向上します。

脅威に対する第1の対応

- シグネチャベースの技術により、既知の不正なデータを除外

脅威に対する第2の対応

- 機械学習やアプリケーションコントロール、および亜種対策機能により、未知のデータが実行される前に分析、ブロック

脅威に対する第3の対応

- 個別のランタイムの機械学習モデルが実行中のプログラム、スクリプト、ドキュメントなどを監視し、脅威や不審な動作を検出

クラウドサンドボックスは、連携した製品とユーザが送信したオブジェクトを管理、および分析する安全な仮想環境です。エンドポイントOSに特化した未知の脅威への対策を行います。

第三者評価

- The Forrester New Wave™: Extended Detection and Response (XDR) Providers, Q4 2021でリーダーの評価を獲得
- Gartner Magic Quadrant for Endpoint Protection Platformsで2002年から18回連続でリーダー・クアドラントの地位を獲得

- IDC Worldwide Cloud Workload Security Market Sharesでグローバルシェア No.1を獲得、2018年から5年連続してNo.1のシェアを獲得
- The Forrester Wave™: Endpoint Security, Q4 2023で12の評価項目で最高スコアを獲得

- Endpoint Protection Platforms分野のGartner® Peer Insights™において Customers' Choice 2023の1社に選出

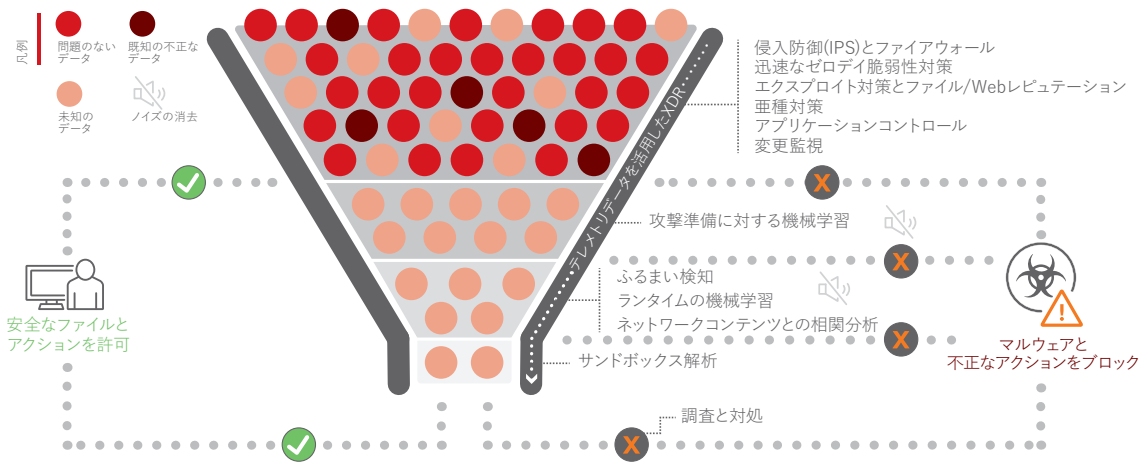


図1: Trend Vision One – Endpoint Securityの保護ステップイメージ図