DATASHEET

WatchGuard Endpoint Security Elite

セキュリティ担当チーム向けの高度なEDR

詳細な可視化と高度な脅威調査

成熟したセキュリティプログラムを有する組織や、高度なセキュリティサービスを提供するパートナー企業にとって、詳細な可視性と調査能力が不可欠です。セキュリティチームは、社内環境の脅威を調査し、対処するための予防、検知、レスポンスのソリューションを必要としており、これによりセキュリティ態勢を次のレベルへに引き上げ、攻撃者の潜伏時間を最小限に抑えることができます。

WatchGuard Endpoint Security Eliteは、充実したテレメトリ機能、高度なクエリツール、AIを活用した調査機能を備えた、フル機能のEDR（エンドポイント検知／レスポンス）プラットフォームを提供します。これにより、セキュリティチームは複雑な攻撃を迅速に把握し、エンドポイント間のイベントを相互分析し、的確にレスポンスすることができます。強力な分析機能と自動化されたレスポンス、そしてデータに関する広範囲の可視性を組み合わせることで、Endpoint Security Eliteは、セキュリティチームがエンタープライズ規模で高度な脅威を検知、調査、阻止するために必要なツールを提供します。

セキュリティ運用向けに構築された高度なEDR

WatchGuard Endpoint Security Eliteは、より詳細なセキュリティの可視化と高度な調査機能を必要とする組織やマネージドセキュリティサービスプロバイダー（MSSP）向けに設計されています。ウォッチガードのAIを活用したEDR基盤を元に、充実したテレメトリ、履歴の広範な可視性、および高度な脅威検知ツールを提供し、セキュリティチームが高度な攻撃をより効果的に検知、調査、レスポンスできるようにします。

詳細なエンドポイントテレメトリとインシデントのコンテキストデータを活用することで、アナリストは攻撃のタイムラインを把握し、根本原因を特定し、攻撃者がシステム間をどのように移動しているかが理解できます。統合されたMITRE ATT&CKマッピングと自動化された行動相関分析により、攻撃者の戦術、手法、手順に関する明確な洞察が得られ、セキュリティチームが脅威の優先順位を迅速に決定し、確信を持ってレスポンスできるよう支援します。

高度な調査ツールには、STIXおよびYARAベースの脅威検知機能に加え、アナリストが自然言語でセキュリティデータを検索できる組み込み型の生成AIアシスタントが含まれます。これらの機能により、調査ワークフローが劇的に加速し、セキュリティチームは隠れた脅威を特定し、脅威の潜伏時間を短縮し、全体的なセキュリティ態勢を強化することが可能になります。

MSPや高度なセキュリティサービスを提供する組織にとって、WatchGuard Endpoint Security Eliteは、分散したツールによる複雑さを伴わずに、現代のセキュリティ運用を支えるために必要な詳細な可視性と分析能力を提供します。

高度な調査ツール
- テレメトリデータを照会する生成AIアシスタント
- STIX形式の攻撃指標（IoC）およびYARAルールによる検知
- ファイル情報（動作、文字列、インポート、エクスポート）を分析するCAPAツール
- MTTRおよび潜伏時間を短縮するためのリモートシェル

WatchGuard Endpoint Security Eliteは、セキュリティ運用チーム向けに、高度な調査およびレスポンス機能を統合しています。

攻撃対象領域の削減
- カスタマイズ可能なエンドポイントリスクダッシュボード
- 管理対象外のエンドポイントの検知
- 脆弱性評価

ビルトインの予防技術
- ファイアウォール、IDS、デバイス制御
- 複数の攻撃ベクトルに対する保護（Web、メール、ネットワーク、デバイス）
- シグニチャファイル、実行前ヒューリスティック、コレクティブインテリジェンス
- 悪意のあるインストーラーやスクリプトを特定／ブロックするAIを活用した検知
- フィッシング対策
- URL/Webフィルタリング
- ネットワークトラフィック分析による検知
- デフォルト拒否の実行制御

検知／レスポンス機能
- エンドポイントの継続監視
- コンテキストに基づく行動分析機能を備えた自己学習型AIにより、ファイルレス攻撃や環境寄生型（LotL）攻撃を検知／遮断
- デバイス上のアクティブなプロセスにおける脆弱性を悪用しようとする試みを自動的にブロック
- インターネットに公開されているサービスの脆弱性に対するネットワーク攻撃対策
- RDP攻撃の自動検知／防止
- 水平移動の封じ込め
- MITRE ATT&CK®フレームワークに基づいてマッピングされたアラートを伴う、攻撃の自動検知／相関分析
- 包括的な根本原因分析（RCA）のための、インタラクティブなマルチシグナルインシデントビュー
- 詳細なコンテキスト情報と、リアルタイムのコンピュータフォレンジックテレメトリによる調査の迅速化
- ThreatSync（XDR）との連携による可視化と修復
- コンピュータおよびネットワークのリアルタイム隔離、スキャン、再起動
- 暗号化されたファイルの復元（シャドーコピー）

サポートされているOS：Windows（IntelとARM）、macOS（IntelとARM）、Linux、iOS、Android

戦略的メリット

調査の迅速化を実現する詳細なテレメトリ

Endpoint Security Eliteは、充実したフォレンジック用テレメトリへのアクセスと長期的なデータ保持機能を提供し、アナリストが攻撃活動を長期的に分析し、エンドポイント全体にわたる攻撃者の行動を再現することを可能にします。

高度な脅威検知

セキュリティチームは、エンドポイントのテレメトリを分析して侵害の兆候や不審な動作を検知する高度なツールを活用し、新たな脅威をプロアクティブに探知することができます。STIXやYARAといった構造化された検知フレームワークに対応しているため、セキュリティチームは隠れた脅威を洗い出し、環境全体にわたる活動を調査することができます。

豊富な視覚的攻撃コンテキスト

インタラクティブなタイムライン、プロセスツリー、水平移動マップにより、エンドポイント間で攻撃がどのように展開されるかを理解するための明確な視覚的コンテキストを提供します。これにより、セキュリティチームは根本原因を迅速に特定し、攻撃者の行動を把握し、調査を加速させることができます。

AIを活用したセキュリティ分析

ビルトインの生成AIアシスタントにより、アナリストは自然言語でセキュリティデータを検索できるため、迅速に調査を進めることができ、複雑なクエリは不要でインシデントの把握にかかる時間を短縮できます。

きめ細かなポリシー制御

Endpoint Security Eliteにより、管理者はエンドポイント全体において、アプリケーションの実行、デバイスへのアクセス、システムの動作を制御する詳細なセキュリティポリシーを適用できます。こうしたきめ細かな制御により、攻撃対象領域を縮小すると同時に、ユーザー、デバイス、環境を問わず一貫したセキュリティ対策の実施が可能になります。

マネージドセキュリティサービス向けに設計

Endpoint Security Eliteは、MSPが高付加価値のセキュリティサービスを提供するために必要な、詳細なテレメトリ、調査ツール、および自動化機能を提供します。一元化されたマルチテナント管理と高度な調査機能により、複数の顧客環境にわたる脅威を効率的に監視、調査、レスポンスすることができます。

ゼロトラストモデル：多層防御

ウォッチガードのエンドポイントセキュリティプラットフォームは、単一の技術だけに依存しているわけではありません。脅威アクターが攻撃を成功させる機会を減らすため、複数のツールを組み合わせて多層防御を実現しています。これらの技術は連携して動作し、エンドポイントのセキュリティ機能を活用することで、侵害のリスクを最小限に抑えます。

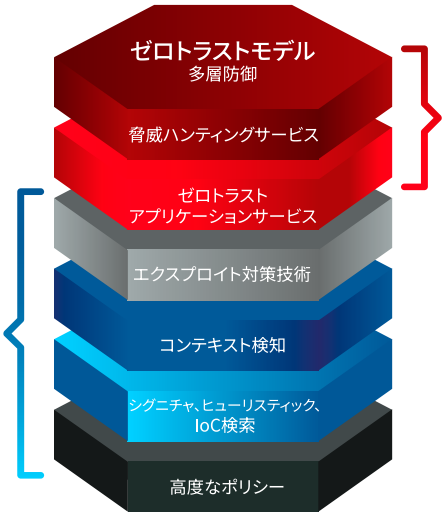
エンドポイントレイヤー

レイヤー1 / 高度なセキュリティポリシー
一般的な攻撃手法の実行を検知またはブロック

レイヤー2 / シグネチャファイル、ヒューリスティック技術、STIX IoC検索エンジン
ハッシュ、ファイル名、パス、C2ドメイン、IP、YARAルールに基づいて、最近公開された攻撃を検索

レイヤー3 / コンテキストに基づく検知
PowerShell、WMI、Webブラウザなどの正規のツールを悪用する、マルウェアを伴わない攻撃を特定

レイヤー4 / エクスプロイト対策技術
脆弱性を悪用するように設計されたファイルレス攻撃を検知



レイヤー5 / ゼロトラストアプリケーションサービス
プロセスを実行前にすべて分類し、信頼できると認定されるまで実行を中断

レイヤー6 / 統合型の脅威ハンティングサービス
侵害されたエンドポイント、IoA、初期段階の攻撃、および不審な活動を検知し、IoAは、関連するテレメトリデータとともにクラウドベースのコンソール上でコンテキスト情報とともに表示されるため、セキュリティアナリストは潜在的な攻撃の試みを調査することが可能

ウォッチガードについて

ウォッチガードは、マネージドサービスプロバイダー（MSP）向けに設計された統合型サイバーセキュリティ分野におけるグローバルリーダーです。30年以上にわたり、MSPが大規模なセキュリティ対策を提供する方法を確立し、脅威情勢のあらゆる大きな変化に先んじるべく、絶えず革新を続けてきました。AIを活用した「Unified Security Platform®」により、ゼロトラストに対応したネットワーク、エンドポイント、アイデンティティ保護機能を単一の統合プラットフォームで提供し、複雑な運用の軽減、対策成果の向上、ビジネスの効率的な成長を可能にします。世界中で150万社以上の顧客を保護する25,000社以上のMSPに利用されており、パートナーが世界中の顧客に対して、強力かつ測定可能なセキュリティの成果を提供できるよう支援しています。

ウォッチガード・テクノロジー・ジャパン株式会社　〒106-0041 東京都港区麻布台1-11-9 BPRプレイス神谷町5階
TEL：03-5797-7205 Email: jpnsales@watchguard.com　www.watchguard.co.jp