DATASHEET

WatchGuard Endpoint Security 360

自律型のゼロトラストエンドポイント保護

最小限の運用負荷で保護機能を最大化

現代のサイバー攻撃は、従来のエンドポイントセキュリティツールが検知できる速度をはるかに上回るスピードで展開されます。攻撃者は、ファイルレス攻撃の手法、正規のソフトウェアを利用した悪意のある動作、侵害された信頼できるアプリケーション、および水平移動をますます多用し、従来の防御を迂回しようとしています。WatchGuard Endpoint Security 360は、こうした高度な脅威を自動的に阻止するように設計されています。デフォルトで未知のアプリケーションをブロックする自律型のゼロトラストEDRを提供し、侵害された信頼できるソフトウェアを検知し、ネットワーク全体における水平移動を防止します。AIを活用した検知機能と自動化された調査／レスポンス機能を組み合わせることで、Endpoint Security 360は攻撃者の潜伏時間を劇的に短縮すると同時に、運用負荷を最小限に抑えます。

保護効率を最大限に高めたい組織向けに設計されており、より強力な保護、より迅速なレスポンス、そしてセキュリティ管理の負担を大幅に軽減します。

自律的な保護機能によるリスクの排除

WatchGuard Endpoint Security 360は、ゼロトラスト実行制御機能を備えた高度なエンドポイント検知／レスポンス（EDR）機能を提供し、信頼性が高く検証済みのアプリケーションのみが実行されるようにします。これにより、組織は継続的な人的介入に頼ることなく、リスクを低減し、攻撃を早期に阻止することができます。

Endpoint Security 360は、未知の活動を自動的にブロックし、信頼できるソフトウェアを継続的に検証することで、ファイルレス攻撃、環境寄生型攻撃（LotL）、悪意のあるスクリプトなど、最近のセキュリティ侵害で用いられる多くの攻撃手法を排除します。

Endpoint Security 360は、侵害された信頼の置けるアプリケーションの検知、水平移動の封じ込め、自動化された脅威ハンティング、インシデントレベルの調査など、さらなる保護階層を追加することで、リスクをさらに低減し、高度な攻撃手法を防止します。

MSPにとっては、これにより人員を増やすことなく、より効率的に業務を行い、より多くの顧客を保護できるようになります。また、エンドユーザーにとっては、懸念事項を減らし、より充実した保護態勢が得られることを意味します。

WatchGuard Endpoint Security 360には、ウォッチガードのAIを活用したEDRプラットフォームの全機能に加え、自律型のゼロトラスト保護機能が搭載されています。

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
- マルチベクターのマルウェア対策とオンデマンドスキャン
- URLフィルタリングとWebブラウジング
- 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
- 水平移動を封じ込め
- 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
- 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）

最新の脅威に対応した自律型保護機能

未知のアプリケーションをデフォルトでブロック

今日のサイバー犯罪者の動きは、エンドポイント保護ツールが追いつけないほど迅速になっています。そのため、WatchGuard Endpoint Security 360には独自の「ゼロトラストアプリケーションサービス」が搭載されており、デフォルトで拒否する制御を実装することで、検証済みのアプリケーションのみがエンドポイント上で実行されるようにしています。未知のアプリケーションは、信頼できるものと分類されるまで自動的にブロックされるため、最新のマルウェアやランサムウェア攻撃の大部分を、実行される前に排除することができます。

巧妙な攻撃の検知と封じ込め

高度な行動検知機能により、エンドポイント全体の活動を継続的に分析し、最新のサイバー攻撃に関連する不審な行動パターンを特定します。悪意のある活動が検知されると、隔離、封じ込め、修復などの自動化されたレスポンス措置により、攻撃がネットワーク全体に拡散する前に阻止します。

作業不可を削減して効率性を改善

WatchGuard Endpoint Security 360は、保護機能と効率性を向上させるためのさまざまな自動化機能を提供します。不審な活動を自動的に調査し、シグナルを関連付けてインシデントとして特定し、未知の脅威をデフォルトでブロックすることで、アラートのノイズや調査にかかる労力を大幅に削減します。その結果、運用負担を軽減しつつ、より強力な保護を実現します。

MSPの規模と効率性に合わせて設計

WatchGuard Endpoint Security 360は、現代のマネージドサービスプロバイダー（MSP）をサポートするために構築されています。マルチテナント型のクラウド管理により、MSPは単一のコンソールから、複数の顧客にわたるポリシーの適用、保護状況の監視、セキュリティ管理を行うことができます。ゼロトラスト型の実行制御、自動化された調査、インテリジェントなレスポンス措置により、MSPはより多くのエンドポイントを保護しつつ、調査時間とアラートの発生数を大幅に削減することができます。

この自動化により、サービスプロバイダーは、運用効率と収益性を向上させながら、より強力なエンドポイントセキュリティサービスを提供できるようになります。MSPにとっては、健全なサービスマージンを維持しつつ、強力なエンドポイント保護を効率的に提供できることを意味します。

ウォッチガードのUnified Security Platform（統合型セキュリティプラットフォーム）で、強力かつシンプルなセキュリティを実現

ウォッチガードのUnified Security Platformアーキテクチャは、最新のセキュリティ対策の提供を強化するための単一プラットフォームです。ウォッチガードのプラットフォームアプローチにより、あらゆる脅威ベクトルに対して強力なセキュリティサービスを提供できるほか、拡張性とレスポンス速度を向上させつつ、運用効率の向上と収益性の向上を実現します。

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
 作成日：2026年7月