DATASHEET

WatchGuard Endpoint Security Basic

最新のEDRで容易にエンドポイントを保護

今日、組織にとって強力なエンドポイント保護体制を整備することは極めて重要です。従来のウイルス対策ツールだけでは、現代のサイバー攻撃を阻止するにはもはや不十分ですが、多くの高度なエンドポイント検知／レスポンス（EDR）プラットフォームは、複雑で手間がかかり、管理が困難です。

WatchGuard Endpoint Security Basicは、こうした課題を解決するべく、最小限の管理でAIを活用した最新のEDR保護機能を提供します。複雑さを抑えつつ信頼性の高い保護を必要とする組織向けに設計されており、行動検知、ランサムウェア対策、攻撃対象領域の縮小を、軽量でクラウド管理型のソリューションとして集約しています。

手間入らずの強力な保護機能

ウォッチガードは、多くの組織において、専任のセキュリティチームを必要とせずに、ユーザーやデバイスを保護する信頼性の高いセキュリティ対策が求められていることを理解しています。

Endpoint Security Basicは、運用上の負担をかけずに強力な保護を必要とする組織向けに設計されており、インテリジェントなマルウェア対策、ランサムウェア対策、および攻撃対象領域の縮小機能を、軽量でクラウド管理型のソリューションに集約しています。リアルタイムのセキュリティ監視と運用上の負担の軽減により、頻繁な調整や手動による介入を必要とせずに、攻撃を早期に阻止します。

Endpoint Security Basicは、AIを活用した予防技術により、マルウェア、ランサムウェア、悪意のあるスクリプト、および新たな脅威に加え、ファイルレス攻撃や環境寄生型攻撃（LotL）などを自動的に検知／ブロックする、最新のエンドポイント保護機能を提供します。また、ビルトインのフィッシング対策、デバイス制御、URLフィルタリング機能により、脅威が定着する前に、一般的な攻撃の侵入経路を削減します。

本ソリューションは、一元化されたクラウドネイティブプラットフォームを通じて提供されるため、単一のコンソールから、ポリシーの適用、セキュリティ態勢の監視、およびすべてのエンドポイントにわたる保護管理を容易に行うことができます。結果として、運用上の負担を低く抑えつつ、脅威を早期に阻止する信頼性の高い保護を実現します。

Endpoint Security Basicには、攻撃を早期に阻止するように設計された、最新の予防／検知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）
- 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

検知／レスポンス機能

- エンドポイントの継続監視
- AIを活用した検知
- コンテキストに基づく行動検知
- 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
- エンドポイントのリスク監視
- 可視性を高めるThreatSync（XDR）との統合
- インシデントの攻撃経緯の自動生成
- 暗号化されたファイルの復元（シャドーコピー）

運用の手間をかけずに信頼できる保護態勢を実現

設定後は自動運用

Endpoint Security Basicは、バックグラウンドで目立たず動作するように設計されています。AIを活用した分類機能により、アクティビティを自動的に分析し、それが安全なものか悪意のあるものかを判断するため、頻繁な調整や調査の必要がありません。

この「静かな設計」のアプローチにより、アラート疲労や運用上の負担が劇的に軽減され、チームは継続的な監視に時間を割くことなく、強固な保護態勢を維持することができます。

デバイス制御の一元化

デバイスのカテゴリ全体（フラッシュドライブ、USBモデム、Webカメラ、DVD/CDなど）のブロック、デバイスの許可リストへの登録、および読み取り専用、書き込み専用、読み取り／書き込み両用のアクセス権限の設定により、マルウェアや情報漏洩を防止します。

エンドポイントのリスク監視

保護されていないエンドポイント、セキュリティ設定の不備、OSやサードパーティ製ソフトウェアの脆弱性、および適用されていないパッチを管理／監視し、侵害が発生する前にネットワークをプロアクティブに保護します。

マルウェア／ランサムウェア対策

Endpoint Security Basicは、動作やハッキング手法を分析し、ランサムウェア、トロイの木馬、フィッシングなど、既知および未知のマルウェアを検知／ブロックします。

リアルタイムの監視／レポート

包括的なダッシュボードと分かりやすいグラフを通じて、詳細かつリアルタイムのセキュリティ監視が行われます。保護状況、検知結果、およびデバイスの不正使用に関するレポートが自動的に生成／配信されます。

ビルトインの攻撃領域の削減

多くのセキュリティ侵害は、パッチが適用されていない脆弱性、許可されていないアプリケーション、あるいは安全でないWebアクセスから始まります。

Endpoint Security Basicは、統合された脆弱性評価、デバイス制御、および一般的な攻撃手法にさらされるリスクを予防的に制限するURLフィルタリングポリシーを通じて、こうしたリスクの軽減に貢献します。

脆弱性評価

脆弱性評価は、ITチームがアプリケーションやシステム全体のセキュリティ上の弱点を特定、評価、優先順位付けを行う上で不可欠なプロセスです。潜在的な脅威を理解／特定し、攻撃者に悪用される前に、リスクを軽減するための予防措置を講じることが重要です。

シンプルなクラウドネイティブ

Endpoint Security Basicは、ウォッチガードのクラウドネイティブ管理プラットフォームを通じて管理され、すべてのエンドポイントにわたる一元化されたポリシー、ダッシュボード、レポート機能を提供します。この統合コンソールにより、運用が簡素化され、管理負担が軽減されるほか、分散した従業員を場所を問わず保護できるようになります。

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