DATASHEET

WatchGuard Endpoint Security Prime

巧妙化した脅威を予防、検知、レスポンス

あらゆる組織向けに高度なエンドポイント防御を実現

長きにわたり、包括的なエンドポイント防御は、上位モデルや法外な価格の壁に阻まれてきました。WatchGuard Endpoint Security Primeは、あらゆる顧客が手の届く範囲でエンタープライズグレードのEDRを利用できるようにすることで、この状況に終止符を打ちます。AIを活用したエンドポイント検知／レスポンスソリューションは、高度な脅威検知、エクスプロイト対策、攻撃対象領域の縮小など、EDRの総合機能を提供し、MSPがエンドポイントセキュリティに対して予防的なアプローチを取れるよう支援します。Primeは、ファイルレス攻撃、ランサムウェア、環境寄生型（LotL）攻撃などの最新の脅威に対してより強力な保護を提供し、シンプルで手頃な価格、かつMSP向けに最適化された、軽量なクラウド管理型パッケージとして提供されます。

手頃な価格でセキュリティを強化

ウォッチガードは、今日のデジタル社会において、エンドポイントにおけるセキュリティの確保がますます複雑化していることを、身をもって認識しています。サイバー犯罪者が手口を進化させ、新たな戦術を駆使する中、エンドポイント検知／レスポンス（EDR）ソリューションに及ばない対策では不十分です。しかし、多くの組織では、基本的な次世代アンチウイルス（NGAV）やエンドポイント保護プラットフォーム（EPP）以上のソリューションを導入する余裕がなく、これらは現代の脅威から保護できず、また、高コストで複雑なエンタープライズグレードのツールを管理するためのリソースも不足しています。.

ウォッチガードは、あらゆる組織が不要なコストや複雑さを伴わずに、効率的かつ効果的なエンドポイントセキュリティを利用できるべきだと考えています。Endpoint Security Primeは、中堅／中小企業（SMB）およびMSP向けに特別に設計されたEDRソリューションです。AIを活用した検知／レスポンス機能と多層防御技術を組み合わせることで、最新の脅威が被害をもたらす前に阻止します。

マルウェアやランサムウェア対策、エクスプロイト対策、フィッシング対策、およびファイルレス攻撃や環境寄生型攻撃に対する防御機能など、ビルトインの保護機能により、組織は単一のクラウドコンソールからリスクを低減できます。行動分析やシグナルの相関分析と組み合わせることで、Endpoint Security PrimeはAIを活用したEDRの総合機能を提供し、パートナーがより強力でスケーラブルなエンドポイント保護を実現できるよう支援します。

Endpoint Security Primeは、AIを活用したEDR機能を網羅した包括的なソリューションを提供し、あらゆる規模の組織を高度なサイバー脅威から、より効果的に保護します。

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
- 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
- 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）

戦略的メリット

すべてのデバイスが対象

セキュリティ侵害は、サイバー犯罪者がバックドアや適切に保護されていないデバイスを通じて侵入することで発生することがよくあります。そのため、セキュリティエージェントがインストールされていない、あるいは管理対象から外れてしまったネットワーク上のデバイスを検知して特定することが極めて重要です。

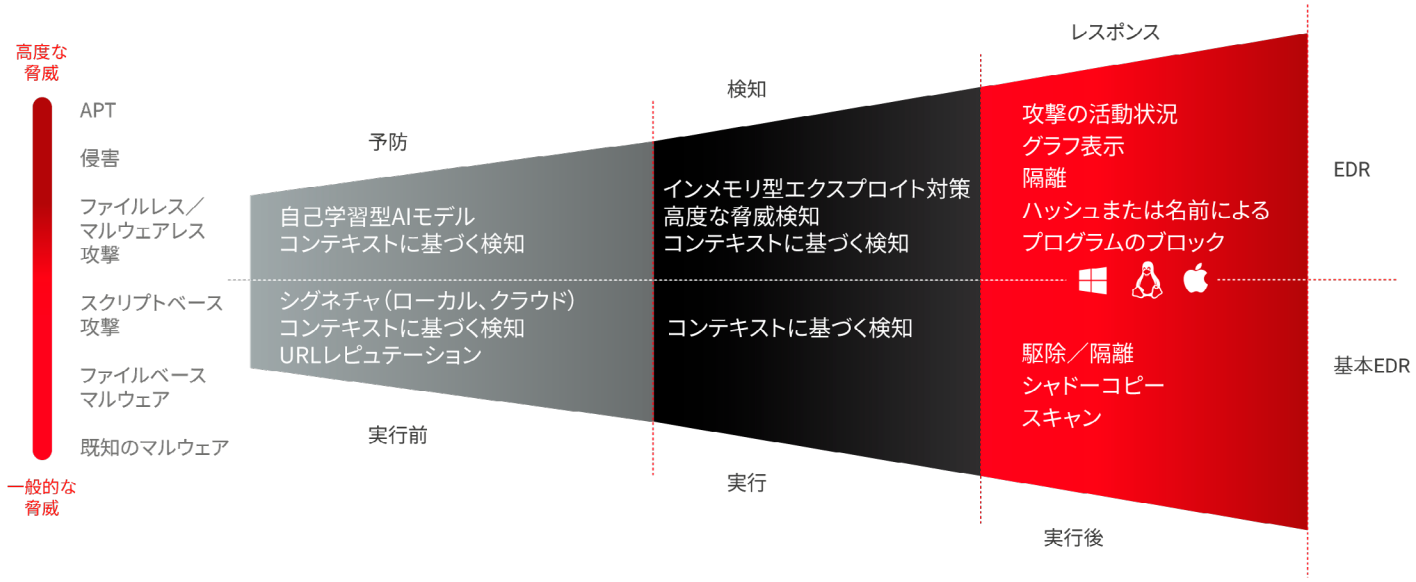
こうした管理対象外、あるいは「不正」なエンドポイントは、攻撃者にとって一般的な侵入経路となっており、セキュリティ上の死角を生み出しています。これらを自動的に検知、管理することで、組織は重大なセキュリティ上の脆弱性を解消し、すべてのデバイスを確実に把握することができます。Endpoint Security Primeを導入することにより、ネットワークがこれらの保護されていない侵入経路を継続的に検知し、フラグを立てるため、担当チームは先手を打って脆弱性を解消し、ネットワークのセキュリティをより強固に保つことができます。

継続的な保護サイクル

新たな脅威に対して最速のレスポンスを実現するため、ウォッチガードはクラウドとエンドポイント間の自己学習型AIループを活用しています。クラウド上では、高性能なAIがアクティビティを分類し、継続的に新しいモデルを学習させます。これらのモデルは精錬されてエンドポイントに適用され、軽量なAIエージェントがオフライン時であっても瞬時に判断を下します。その後、エンドポイントからクラウドへインテリジェンスがフィードバックされ、日々賢くなっていく絶え間ない保護サイクルが形成されます。

包括的なEDRセキュリティで見逃されていた脅威を排除

Endpoint Security Primeでセキュリティを強化し、NGAV技術と最先端のEDR機能を組み合わせることで、高度な脅威に先手を打つことができます。自動化された検知、レスポンス、そして継続的な監視機能を備えたEndpoint Security Primeでは、デバイス、ユーザー、データの包括的な保護を可能にし、今日から明日の安全を確保することができます。



WatchGuard Endpoint Security Primeの詳細については、ウォッチガードの営業担当もしくは各販売代理店にお問い合わせください。

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