DATASHEET

WATCHGUARD EDR

エンドポイント検知／レスポンス

高度な脅威に対するサイバー防御

最新のサイバー攻撃は、従来のセキュリティソリューションによる保護をかいくぐるように仕組まれています。こうした攻撃は、ハッカーのテクニックが向上するにつれ、頻度が増し、より洗練されたものになってきています。また、このような現状は、システムに潜むセキュリティの脆弱性を修復していないことも起因しています。

このような状況の中、従来のエンドポイント保護プラットフォーム（EPP）では、企業ネットワーク上で実行されているプロセスやアプリケーションを詳細に可視化することができません。さらに、EDRソリューションによっては何も解決できず、セキュリティ担当者のアラート管理もままならず、手動で脅威を分類しなければならないため、ストレスが溜まり、作業負荷が増えてしまいます。

自動化されたEDRでセキュリティを向上

WatchGuard EDRは、コンピュータ、ラップトップ、サーバ向けの革新的なサイバーセキュリティソリューションであり、クラウド経由でサービスを提供します。現在および将来のあらゆる高度な脅威、ゼロデイマルウェア、ランサムウェア、フィッシング、インメモリエクスプロイト、マルウェアレス攻撃など、企業ネットワークの内外で防止、検知、封じ込め、レスポンスを自動化します。

WatchGuard EDRは、従来のソリューションを回避する不正な活動を監視・特定し、エンドポイントを総合的に可視化するように構築されています。既存のアンチウイルスソリューションに追加する形でインストールし、以下の自動化サービスを含むEDRのフル機能を提供します：

- **ゼロトラストアプリケーションサービス：アプリケーションを100%分類**
- **脅威ハンティングサービス：ハッカーや内部不正者を検知**

WatchGuard EDRは、以下の高度なセキュリティテクノロジーにより、脅威を効果的に駆逐し、悪意のある攻撃にレスポンスするための手段を提供します：

- EDRでエンドポイントを継続監視
- プロセスを100%分類するクラウドベースの機械学習（APT、ランサムウェア、ルートキットなど）
- 本番環境でのサンドボックス
- アンチエクスプロイト保護
- 自給自足型（LotL）攻撃を検知する振舞い分析や攻撃指標（IoA）検知を含む脅威ハンティング機能
- MITRE ATT&CKフレームワークにマッピングされた攻撃指標（IoA）
- RDP攻撃の検知・防止
- コンピュータの隔離やハッシュや名前によるブログラム防御など、封じ込めおよび修復機能

メリット

セキュリティ管理のシンプル化とコスト抑制

- マネージドサービスにより選任スタッフのコストを削減するとともに、アラートの誤送信を防ぎ、管理負荷を軽減します。
- 一元的にクロスプラットフォームのエンドポイントを管理します。
- 軽量エージェントとクラウドネイティブのアーキテクチャにより、エンドポイントのパフォーマンスへの影響を排除します。

自動化により検知に要する時間を削減

- セキュリティリスクを伴うアプリケーションを（ハッシュや名前に基づき）防御します。
- 各種の脅威、ゼロデイマルウェア、ファイルレス／マルウェアレス攻撃、ランサムウェア、フィッシングの実行を防御します。
- ハッキングの手法、戦術、手順を検知・防御します。

自動化によりレスポンス／調査時間を削減

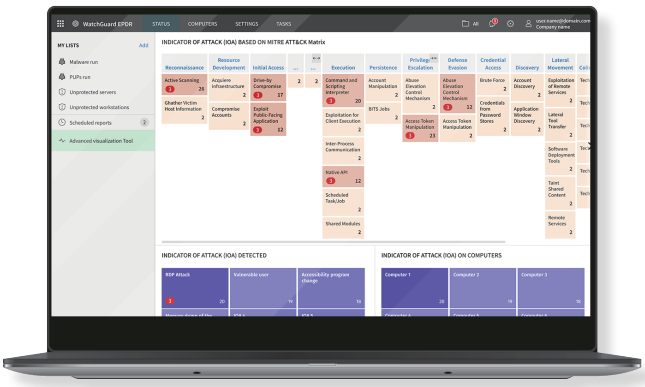
- 各攻撃の試みを徹底的に調査するためのフォレンジック情報と、その影響を軽減するためのツール（駆除）を提供することで解決およびレスポンス能力を高めます。
- 攻撃者とその活動を可視化し、高度な攻撃指標（IoA）調査を行うことで、各アクションを追跡します。
- フォレンジック分析により、セキュリティポリシーを改善・調整します。

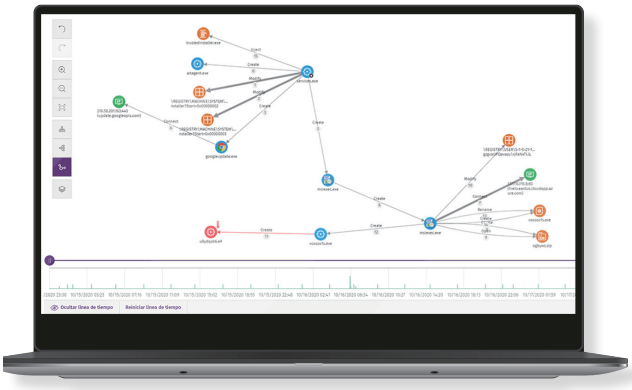
ゼロトラスと脅威ハンティング

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、1つのテクノロジーのみならず、攻撃者を阻むための複数のテクノロジーを採用しています。これらのテクノロジーを結集することにより、エンドポイントの侵害リスクを極力削減することに注力しています。

ゼロトラストアプリケーションサービスでは、プロセスを100%分類し、エンドポイントの活動を監視し、問題のあるアプリケーションや悪意のあるプロセスの実行を防御します。実行ごとに、リアルタイムに善悪を分類し、不確実性を排除して結果を送信します。また、セキュリティ担当者に判断を委ねることなく、手動によるプロセスを回避します。これらは、AIやクラウド処理における十分な容量、スピード、適応性、拡張性により実現しています。

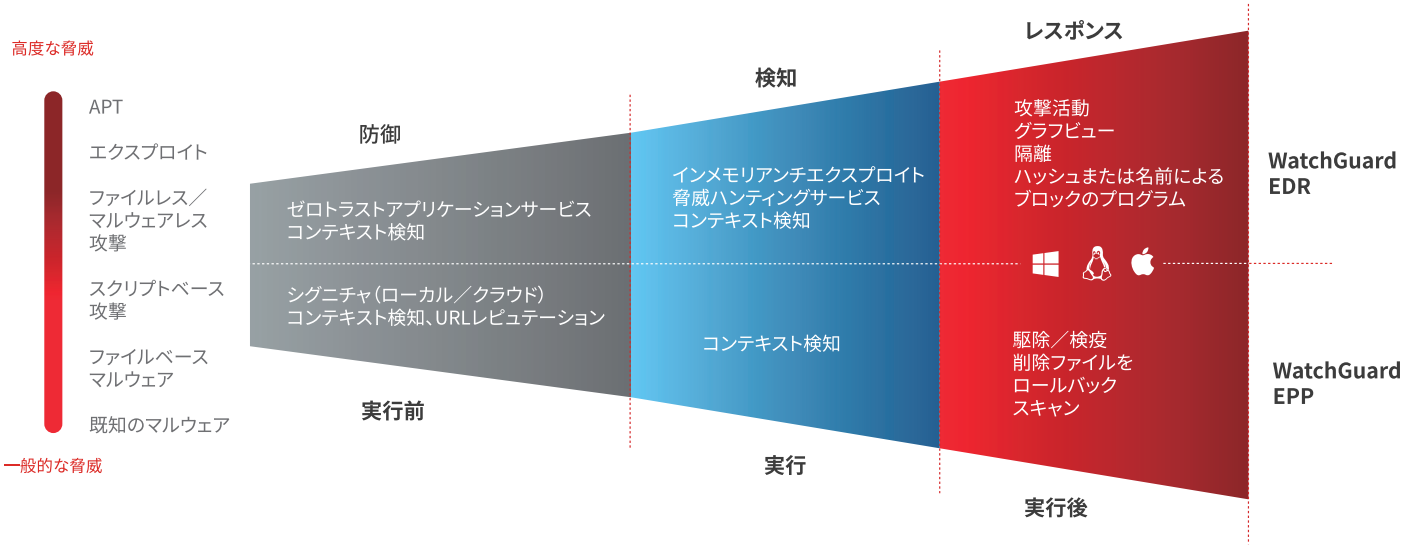
同サービスでは、ビッグデータテクノロジー、ディープラーニングを含むマルチレベルの機械学習技術、継続的な監視結果、そしてWatchGuardの脅威チームが蓄積した経験と知識の自動化を統合しています。





脅威ハンティングサービスは、サイバーセキュリティのスペシャリストにより作成された一連のハンティングルールに基づいています。テレメトリから収集された全データに対して自動的に処理する検知時間（MTTD）とレスポンス時間（MTTR）を最小限に止めるために、信頼度が高く、誤検知率が低い攻撃指標（IoA）を起動します。

これらの攻撃指標（IoA）は、高度なデータ分析、ウォッチガード独自の脅威インテリジェンス、そしてアナリストの専門知識を活用した攻撃者を発見するための継続的なプロセスの結果に基づいています。ウォッチガードのハンターたちは、組織は常に危険に晒されているという前提で取り組んでいます。



WatchGuard EDRがサポートするプラットフォームとシステム要件

サポートしているオペレーティングシステム：Windows（Intel と ARM）、macOS（Intel と ARM）、Linux、Android

レガシーシステムのサポート：
Windows XP SP3 および Server 2003 で起動するシステム

EDR の機能は、Windows、macOS、Linux で利用できますが、Windows プラットフォームで全ての機能を利用できます。

互換性のあるブラウザ：Google Chrome、Mozilla Firefox、Internet Explorer、Microsoft Edge、Opera

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　FAX：03-5797-7207　www.watchguard.co.jp