DATASHEET

WATCHGUARD EPDR

エンドポイント保護／検知／レスポンス

組織が抱えるサイバーセキュリティの課題

昨今のサイバー攻撃の主な標的としてエンドポイントが増加していますが、テクノロジーのインフラが複雑化するにつれて、組織はエンドポイントのセキュリティリスクを監視・管理するために必要な専門知識を持つ人材やソリューションを探すのに苦労しています。ではエンドポイントのセキュリティソリューションを導入する際に、企業はどのような課題を抱えているのでしょうか。

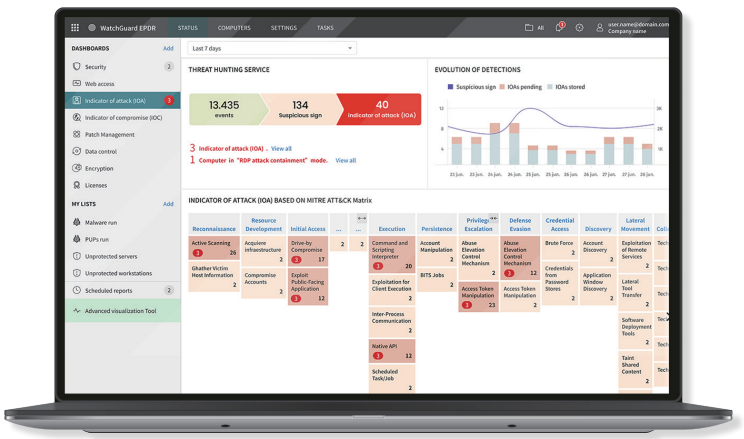
- **アラート疲れ：**組織は日々膨大な数のマルウェアアラートを受信していますが、実際に重要なものは19%程度で、4%しか調査されていないのが実態です。それでもサイバーセキュリティ管理者の3分の2の時間がマルウェアアラートの管理に費やされていると言われています。
- **複雑性：**セキュリティ担当者にとって、多様なテクノロジー、社内スキルの欠落、そして脅威を特定するために要する時間により、相互に連携されていない多くのサイバーセキュリティツールを管理するのは大変です。
- **低いパフォーマンス：**多くのエンドポイントセキュリティソリューションでは、監視しているコンピュータ、サーバ、ラップトップに必要となるエージェントのインストールと管理に手間がかかり、重大なエラー、パフォーマンスの低下、リソースの過剰消費の原因になっています。

従来のエンドポイント保護テクノロジーは、防御することにフォーカスしており、既知の脅威および不正な振舞いには有効ですが、高度なサイバー脅威に対しては十分ではありません。一般的な侵入経路から新たな脅威まで、攻撃者は常にIT部門の注意を逃れ、防御対策を回避し、新たな弱点を利用する方法を探しています。

防御からレスポンスまで - 自動化されたエンドポイントセキュリティ

WatchGuard EPDR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、クラウド経由で提供されます。防御、検知、封じ込め、レスポンスまで自動化し、企業ネットワークの内外における高度な脅威、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、ファイルレスおよびマルウェアレス攻撃などに対応しています。他のソリューションとは異なり、広範なエンドポイント保護テクノロジー（EPP）と自動化された検知／レスポンス（EDR）機能を組合わせています。また、ソリューションの特長として、ウォッチガードのエキスパートによって管理されている以下の2つのサービスも提供しています：

- **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 EPDRでは、従来のエンドポイントテクノロジーと、革新的かつ適応性に優れた保護、検知、レスポンステクノロジーを単一ソリューションとして統合しています。これにより、IT部門は以下の高度なセキュリティテクノロジーを含む、巧妙なサイバー脅威に対抗することが可能になります：

従来の防御テクノロジー

- パーソナル／マネージドファイアウォール（IDS）
- デバイス制御
- インテリジェンス共有
- 拒否リスト／許可リスト
- 継続的なマルチベクターアンチマルウェアとオンデマンドスキャン
- 実行前のヒューリスティック
- URLフィルタリング – Webブラウジング
- アンチフィッシング
- アンチタンパリング
- 修復とロールバック

高度なセキュリティテクノロジー

- 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・防御
- コンピュータの隔離やハッシュや名前によるプログラム防御など、封じ込めおよび修復機能

メリット

セキュリティをシンプルに強化

- 自動化サービスにより専任者の人件費を削減することが可能となり、誤検知アラートへの対応や手作業による設定時間などを排除することができます。
- インフラのインストール、構成、保守の管理を不要にします。
- 軽量エージェントおよびクラウドネイティブのアーキテクチャを採用しているため、エンドポイントのパフォーマンスに影響を与えることはありません。

容易な操作・管理

- エンドポイントセキュリティのポートフォリオは、単一のWebコンソールから非常にシンプルな方法でエンドポイント保護のニーズに応えます。
- 設定が容易で、一元的にクロスプラットフォームでのエンドポイント管理を可能にします。
- 迅速に操作を習得できる、明快なユーザーインターフェースを採用しています。

EDRの自動化機能

- 被害を受ける前に、ハッキングの技術、手法、手順、および不正なインメモリ活動（エクスプロイト）を検知・防御します。
- フォレンジック情報により、各攻撃の試みを徹底的に調査し、被害を軽減（駆除）するためのツールを提供することで、解決とレスポンスを可能にします。
- 攻撃者とその活動に対する実用的な可視化機能を提供し、フォレンジック調査も実施することにより、各アクションを追跡します。

ゼロトラストモデル：多層型保護

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、複数のテクノロジーを採用することにより、攻撃者の侵入に対処しています。これらのテクノロジーを組合わせることで、エンドポイントへの攻撃リスクを最小限に抑えます。

ゼロトラストモデル：多層型保護

エンドポイントレイヤ：

レイヤ1／シグニチャファイルとヒューリスティックテクノロジー

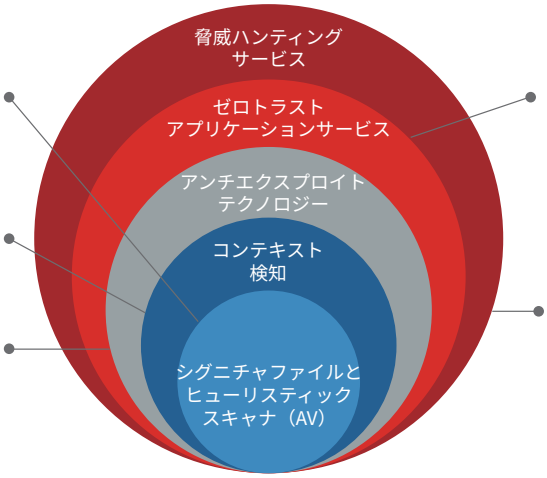
効果的に最適化されたテクノロジーにより、既知の攻撃を検知

レイヤ2／コンテキスト検知

マルウェアレスおよびファイルレス攻撃を検知

レイヤ3／アンチエクスプロイトテクノロジー

脆弱性のエクスプロイトを狙ったファイルレス攻撃を検知



クラウドネイティブレイヤ

レイヤ4／ゼロトラストアプリケーションサービス

前段階のレイヤが侵害された場合、侵害を検知し、すでに感染したコンピュータ、並びにネットワーク内の攻撃の拡散を抑止

レイヤ5／脅威ハンティングサービス

感染したエンドポイント、早期段階の攻撃、疑わしい活動の検知や、攻撃指標（IoA）による検知

シグニチャファイルとヒューリスティックテクノロジー：従来のエンドポイント保護（EPP）として知られており、次世代アンチウィルステクノロジーレイヤにより、多くの一般的な低レベルの脅威を防御します。特定のシグニチャ、ジェネリック／ヒューリスティック検知、不正URL防御を活用した既知の攻撃の検知に最適化されています。

コンテキスト検知：リソースやアプリケーションの異常な使用状況を調査し、マルウェアレスおよびファイルレス攻撃を検知します。スクリプトベース攻撃、PowerShellやWMIなどのOSツールを用いた攻撃、Webブラウザの脆弱性、およびJava、Adobeなどの一般的に標的となるアプリケーションに対して効果を発揮します。

アンチエクスプロイトテクノロジー：脆弱性をエクスプロイトするファイルレス攻撃を検知します。エクスプロイトされたプロセスの確実なシグナルとなる異常な振舞いを検索・検知します。アンチエクスプロイトテクノロジーは、パッチが当てられていないエンドポイント、およびサポートが終了しているOSを使用してるエンドポイントに大変有効です。

ゼロトラストアプリケーションサービス：プロセスを100%分類するとともにエンドポイントの活動を監視し、不正なアプリケーションやプロセスの実行を防御します。それぞれの実行に対して、悪意のあるものか正当なものか分類・判断し、不確実性を排除しつつ、ユーザーに判断を委ねることなくリアルタイムに情報を送信し、手作業を回避します。

脅威ハンティングサービス：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。

WatchGuard EPDR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