DATASHEET | SOC

# WATCHGUARD ADVANCED EPDR

## サイバーセキュリティの課題

現在のサイバー攻撃は主にエンドポイントを標的としています。テクノロジーのインフラが複雑化する中で、組織は必死になってエンドポイントのセキュリティリスクを監視・管理するための専門知識を求めています。それ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上で、セキュリティチームはどのような課題に直面しているのでしょうか？

- **巧妙化し続ける脅威：**取って付けたようなセキュリティ対策を脱し、効率的でプロアクティブなセキュリティ対策を実践することにより、被害者にならずに済む場合があります。実践内容は、攻撃対象領域を減らすことから、実際に侵害される前に新たな脅威を発見することまで、多岐に渡ります。
- **アラートの頻発による非効率な業務：**セキュリティチームは毎週膨大な数のアラートを受信していますが、重要なアラートはわずか19%であり、4%しか調査されていません。セキュリティチームは3分の2の時間を手作業によるアラート管理および不審なファイルの分類に充てているのが現状です。
- **低いパフォーマンス：**エンドポイントのセキュリティソリューションは一般的に、監視対象の各コンピュータ、サーバ、ラップトップに複数のエージェントをインストールし、管理することが求められています。

防御を任務とするセキュリティチームは、敵の滞留時間を最小限に止めるためにセキュリティスタックを次のレベルに引き上げ、システム環境に潜む脅威を**容易に見つけ出し、対策を取るための自律的な予防、検知、レスポンス**のソリューションやツールを必要としています。

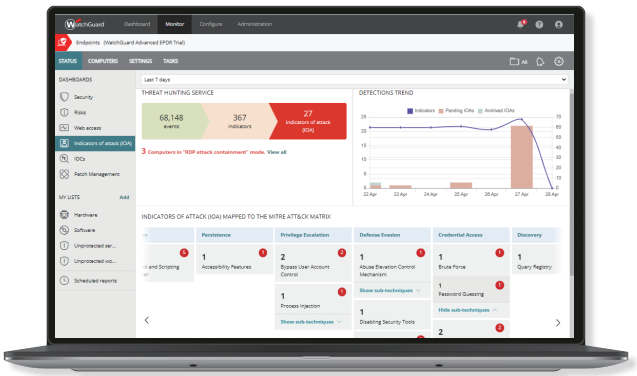
## サイバーセキュリティサービスをレベルアップ

WatchGuard Advanced EPDRは、コンピュータ、ラップトップ、サーバ向けのクラウド型の最先端サイバーセキュリティソリューションであり、企業ネットワークの内外に潜むあらゆる高度な脅威に対して予防、検知、封じ込め、レスポンスを自動化します。

WatchGuard Advanced EPDRは、以下の2種類のセキュリティサービスにより、予防およびEDR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：**クラウド型の機械学習により、全てのファイルを自動で分類します
- **脅威ハンティングサービス：**振舞い分析により、環境寄生型（LotL）攻撃を活用した脅威を明らかにします

WatchGuard Advanced EPDRは、迅速な調査とレスポンスを可能にするMITRE ATT&CKにマッピングされた高度なIOC（侵害指標）検索エンジン、IOA（攻撃指標）検知、そしてエンドポイントへのリモートアクセスなどのハンティングツールをテクノロジースタックに追加することにより、WatchGuard EPDRの機能を拡張します。



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

WatchGuard Advanced EPDRは、従来のエンドポイントテクノロジーとEDRテクノロジーをシングルソリューションとして統合しており、セキュリティチームは高度なサイバー脅威に対処することができます。

### 攻撃対象領域の削減ツール

- 一元化されたエンドポイントセキュリティリスクの検知／スコアリング
- 管理されてないエンドポイントのプロアクティブな自動検知
- OSおよび各種アプリケーションの脆弱性評価

### 従来の予防技術

- 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
- アプリケーション制御：拒否リスト／許可リスト
- 恒久的なマルチベクターアンチマルウェア／オンデマンドスキャン
- 実行前のヒューリスティクス
- 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
- ネットワークトラフィック分析による攻撃検知
- 自動修復／ロールバック
- シャドーコピーによる暗号化ファイルのリカバリ

### ハンティング／検知技術

- EDRによる継続的なエンドポイント監視
- ゼロトラストアプリケーションサービス／脅威ハンティングサービス
- 本番環境でのサンドボクシング
- アンチエクスプロイトプロテクション
- MITRE ATT&CKにマッピングされた攻撃指標（IOA）
- RDP攻撃の自動検知と封じ込め
- STIX侵害指標（IOC）とYARAルール検索
- 高度なセキュリティポリシーによる一般攻撃手法の実行拒否

### 封じ込め／修復ツール

- コンピュータ隔離／システムリブート
- クラウドからエンドポイントへのリモートシェル

## 特長

**コスト効率の高い運用 – 不審なファイルの調査を削減**

WatchGuard Advanced EPDRのゼロトラストアプリケーションサービスにより、他のソリューションのようにアラートを発信するのみで判断をスタッフに委ねることなく、不審なファイルのリバースエンジニアリングに要する時間を削減します。

**自社サービスに適した包括的なエンドポイントセキュリティ**

WatchGuard Advanced EPDRは、攻撃対象領域の削減、脅威の防止、検知、レスポンス、プロアクティブなハンティングツール、および正確なレスポンスを可能にするリモートエンドポイント接続など、エンドポイントセキュリティプログラムを強化するための広範な包括機能を提供します。

**使い勝手のよい高度なハンティングおよびレスポンス機能**

侵害指標（IOC）の一元検索機能により、WatchGuard Advanced EPDRでは、セキュリティチームが複雑なクエリに対応することなく脅威を発見することができます。また、脅威ハンティング機能では、さらなる調査のためにテレメトリでコンテキスト化された攻撃指標（IOA）を提供します。

**成長に合わせてマネージドセキュリティサービスを拡張**

**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）アーキテクチャ**追加コストのかからない卓越したプラットフォーム機能により、ネットワークからエンドポイント、Wi-Fi、認証まで包括的なセキュリティを提供します。サービスの導入が増えれば増えるほど、運用と業務効率を高めることができます。

## ゼロトラストモデル：多層防御

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つの技術にのみ依存しているわけではなく、複数の技術を組み合わせることで攻撃から組織を守っています。多彩な技術が連携することにより、エンドポイントに対する侵害リスクを最小限に止めます。

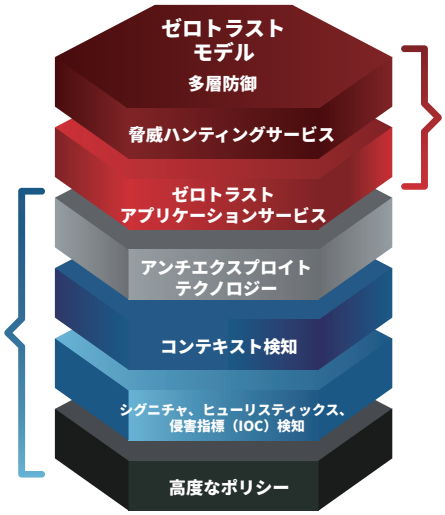
### エンドポイントレイヤー：

**レイヤー1：高度なセキュリティポリシー**
一般攻撃手法の実行を検知または防御

**レイヤー2：シグニチャファイル、ヒューリスティックテクノロジー、STIX IOC検索エンジン**
ハッシュ値、ファイル名、パス、C2ドメイン、IP、YARAルールによって最近公開された攻撃のハンティングをサポート

**レイヤー3：コンテキスト検知**
PowerShell、WMI、Webブラウザ、およびJavaやAdobeといったその他の一般的な攻撃対象アプリケーションなど、OSツールを用いて非マルウェア型攻撃を検知

**レイヤー4：アンチエクスプロイトテクノロジー**
脆弱性を標的とするファイルレス攻撃を検知




### クラウドネイティブレイヤー

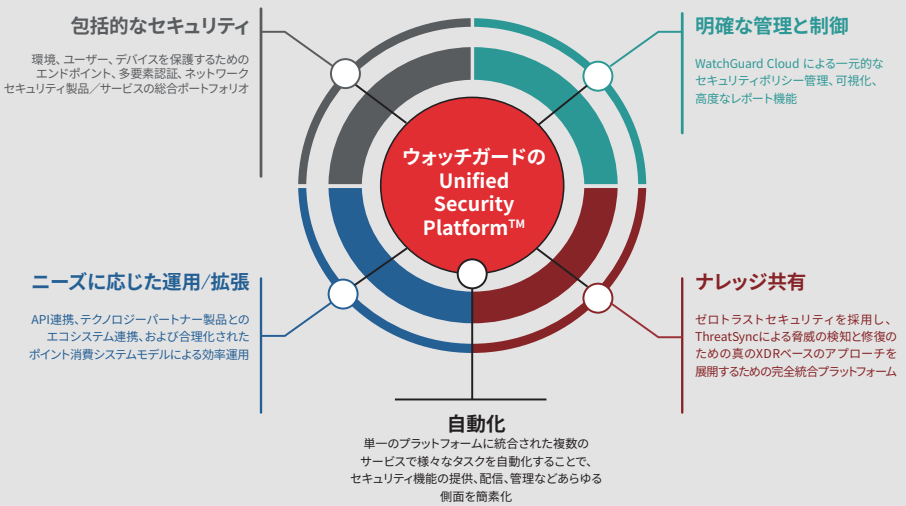
**レイヤー5：ゼロトラストアプリケーションサービス** 実行前にプロセスを100%分類し、信頼できると認定されるまで実行を拒否

**レイヤー6：脅威ハンティングサービス**
侵害されたエンドポイント、早期ステージの攻撃、不審な活動、および攻撃指標（IOA）の検知を実現します。非決定論的な攻撃指標（IOA）は、クラウドベースのコンソールで関連イベントとともにコンテキスト化されるため、セキュリティアナリストは潜在的な攻撃の試みを調査することが可能

## 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（統合型セキュリティプラットフォーム）アーキテクチャは
シングルプラットフォームで最先端のセキュリティを提供します。

### スケーラブルなシングルプラットフォームで最先端のセキュリティを実現します。




**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　FAX：03-5797-7207　https://www.watchguard.co.jp　Email: jpnsales@watchguard.com