WatchGuard MDR

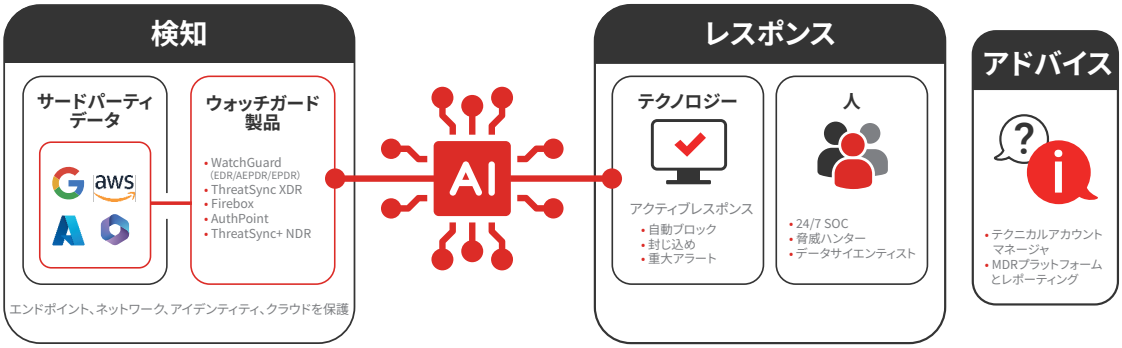
組織のセキュリティ対策全般に対応する24/7の脅威検知／レスポンス

WatchGuard MDRは24/7のセキュリティマネージドサービスを提供しており、アラートのみならず対策を施します。ノイズをカットして重大インシデントにフォーカスし、ラップトップ、サーバ、ユーザーアイデンティティ、ネットワーク、クラウドを横断して、脅威への迅速なレスポンスを実現します。

WatchGuard MDRを利用することにより、ビジネスに影響を及ぼさずにセキュリティ態勢を維持することが可能となり、常時監視するとともに優れた保護機能を提供します。リスクが伴うログイン、不審なメール、ネットワークに潜む脅威など、素早く検知し、被害を受ける前に自動的に阻止することができます。

WatchGuard MDRの特長

- エンドポイント、アイデンティティ、ネットワーク、クラウドを横断して24/7で脅威を検知
- ノイズをカットし、重大なアラートのみ発信
- 自動レスポンスを基本に、重要度に応じてエスカレーション
- 根本原因を特定することでリスクを削減し、問題を解決
- 脅威をリアルタイムで可視化し、レポートを作成



主な機能

セキュリティ環境全般に渡る単一ビュー
エンドポイント、ファイアウォール、アイデンティティ、ネットワーク、クラウドを横断して一元的に脅威活動を可視化し、時間の節約と複雑性の排除を可能にします。

24/7の監視とレスポンス
SOCのグローバルチームが常時対応し、優れた人材と強力な自動化機能により、脅威を検知・阻止し、重大事にはライブサポートを利用することができます。3つの拠点に冗長性を備えたセキュリティオペレーションが分散配置されており、24時間365日で対応します。

AI/ML活用した優れた検知能力
AIと機械学習により、リアルタイムで膨大な数のシグナルをスキャンし、人が見逃す可能性があるパターンを探り当て、新たな脅威への対策を学習します。全てのインシデントから学習することで日々進化し、より迅速な検知・レスポンスを可能にします。

プロアクティブな脅威ハンティング
自動化ツールが見逃す可能性のある脅威もウォッチガードのアナリストが発見し、巧妙化する攻撃にも対応します。

迅速に対応する自動化システム
手動による作業、ノイズのフィルタリング、重大事のエスカレーションを自動化し、脅威が拡散する前に迅速に封じ込めます。

脅威に対する正確なレスポンス
脅威の封じ込め、エンドポイントの隔離、不正なファイルのブロック、そしてセキュリティ対象の環境全般における活動の調査を迅速に行います。

柔軟なレスポンスオプション
レスポンスは自身で行うか、ウォッチガードで対応するか、あるいは共同で対処するか選択することができます。

リアルタイムで可視化
MDRポータルではセキュリティ対象の環境全般をライブで可視化し、アラート、アクション、保護状況の指標を一元的に把握することができます。

低ノイズと重要シグナル
重大なアラートのみ受信し、誤検知（フォールスポジティブ）は1ヵ月に1件未満の精度を実現することで、担当者の負荷を軽減します。

エキスパートガイダンス
テクニカルアカウントマネージャが継続してセキュリティガイダンスを提供し、SOC活動、トレンド情報、および保護態勢の改善といった面で支援します。エキスパートが常時サポートすることで、MSPはクライアントに優れた成果をもたらすことができます。

ウォッチガードの競争優位性

実績豊富なセキュリティリーダー
ウォッチガードはサイバーセキュリティ分野で25年以上の経験を持ち、シンプル、スケーラブル、そして利用しやすいエンタープライズクラスのプロテクション機能の提供において実績があります。今日、世界25万組織に対して、1,000万以上のエンドポイントの保護を支援しています。

真に統合されたセキュリティ
一般的なMDRプロバイダーのようにエンドポイントの監視のみを行うか、クラウドサポートを後付けで提供するのではなく、エンドポイント、アイデンティティ、ファイアウォール、ネットワーク検知の統合型ソリューションを提供しています。

パートナーを考慮した設計
MSPや小規模組織向けに、予めエンタープライズクラスのツールが利用できるように設計されており、顧客にニーズに沿ったサービスデリバリを可能にします。

アラートのストレスを解消
一部のベンダーでは、1日あたり15件以上の誤検知（フォールスポジティブ）が発生しますが、ウォッチガードの場合、月平均1件未満であり、不要な通知が減ることで迅速なレスポンスが可能になります。

迅速に保護態勢を確立
迅速なオンボーディング、プリビルトの統合ソリューション、強力なパートナーサポートにより、大きな負荷もなく素早く稼働開始することができます。

最新の環境向けに構築
Microsoft 365、Azure、AWS、およびGoogle Workspaceのネイティブサポートにより、ハイブリッド環境やクラウド環境を即座に保護することができます。

実績豊富なテクノロジーと信頼性の置けるチーム
ウォッチガードのSOCはセキュリティの深い専門知識と強力なAIを組み合わせることで、脅威を迅速に検知・阻止します。MDRプラットフォームはMITREなどの業界の第三者機関によってテスト・評価されており、長年に渡り、世界中の企業に信頼性の高い高性能の保護機能を提供しています。

全ての攻撃対象領域を保護

エンドポイント保護
エンドポイントは、ランサムウェア、フィッシング、ファイルレス攻撃の主要な標的となっています。Total MDRは、WatchGuard EDR/EPDR/AEPDRを活用し、資格情報の窃取や権限のエスカレーションといった不正な振舞いを検知します。その後、侵害されたデバイスを隔離し、悪意のあるプロセスを停止し、マルウェアが水平方向に拡散したり、権限をエスカレーションさせたりする前に、ライブでアナリストがレスポンスします。

アイデンティティ保護
Total MDRはWatchGuard AuthPointと連携し、ログイン異常、ログイン失敗の急増、不正アカウントの作成など、不審な活動を検知／レスポンスします。侵害されたアカウントをリアルタイムで無効化することで、攻撃者がユーザーを偽装したり、クラウドプラットフォームに検知されずにアクセスしたりするのを阻止します。

ネットワーク保護
水平方向の移動、ポートスキャン、C2トラフィックなどといった、エンドポイントをバイパスする攻撃は、FireboxとThreatSync+ NDRによって検知されます。Total MDRは即座にレスポンスし、悪意のあるIPアドレスのブロック、ポートの閉鎖、またはデータ漏洩の阻止により、内部システムをステルス型の脅威から保護します。

クラウド保護
Total MDRは、Microsoft 365およびその他のクラウドプラットフォームにおいて、不審なサインイン、権限の変更、メールボックスへのアクセスなど、セキュリティ侵害の兆候を監視します。Microsoft 365に対しては、API連携を通じてアクセス権限の無効化、資格情報のリセット、脅威の封じ込めを実行し、メール詐欺やデータロスが発生する前に防止します。

平均6分未満でレスポンス

「私たちは、導入と維持が容易なソリューションが必要です。複雑で重いツールは採用できません。これにより、戦略的なサポートに集中するための時間を確保できます。小さなチームでは管理が困難な複数のコンソールを操作する必要がなくなります。」

~ Julien Perret(ジュリアン・ペレット)氏、Eiffie

AIを活用した脅威ハンティングと自動化

Firebox、AuthPoint、ThreatSync+ NDR、WatchGuard EDR/EPDR/AEPDRのビルトインサポート

Microsoft 365、Azure、AWS CloudTrail、Google Workspaceをサポート

可視化、レスポンス、レポーティング用のシングルポータル

単独管理または共同管理の有効オプション

1カ月1件未満の誤検知

Total MDRで広範な保護を実現

攻撃者の活動	TOTAL MDRで阻止	保護対象
資格情報の窃取	AuthPoint：アカウントの乗っ取りをブロック	アイデンティティ
エクスプロイトとマルウェア	EDR：マルウェアを阻止してエンドポイントを隔離	保存データ
水平移動	NDR + Firebox：水平移動を検知・ブロック	転送データ
クラウドアクセス／データ漏えい	クラウド連携：アクセスを無効化し、資格情報をリセット	アプリケーション

適切なMDRサービスを提供

企業のセキュリティ環境は1つとして同じものはありません。すでにMicrosoft Defenderを使用している場合もありますし、ウォッチガードのフルスタックの保護機能を要する場合もあります。WatchGuard MDRは個々のお客様にとって適切な保護レベルを実現します。

	WatchGuard Core MDR	WatchGuard Core MDR for MS	WatchGuard Total MDR
パートナー／エンドユーザー向け：	WatchGuard Endpoint を使用	Microsoft Defender を使用	ウォッチガード エンドポイント、NDR、アイデンティティ、ファイアウォールを使用
24/7 SOC モニタリング	✓	✓	✓
AI/ML ベースの脅威検知	✓	✓	✓
自動脅威レスポンス／リアルタイムアラート	✓	✓	✓
根本原因分析	✓	✓	✓
脅威ハンター	✓	✓	✓
インシデントレスポンス			✓
ディフェンスポータル	✓	✓	✓
パートナーのテクニカルアカウントマネージャへのアクセス	✓	✓	✓
エンドポイントインテグレーション	WatchGuard EDR/EPDR/AEPDR	Microsoft Defender	WatchGuard EDR/EPDR/AEPDR
ネットワークインテグレーション			WatchGuard Firebox ThreatSync+ NDR
アイデンティティインテグレーション			WatchGuard Authpoint
Threat Sync + XDR			✓
Microsoft 365	✓	✓	✓
AWS CloudTrail カバレッジ			✓
Google Workspace			✓

WatchGuard Technologiesについて

WatchGuard® Technologies, Inc.は、統合型サイバーセキュリティにおけるグローバルリーダーです。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）は、マネージドサービスプロバイダー向けに独自に設計されており、世界トップクラスのセキュリティを提供することで、ビジネスのスケールとスピード、および運用効率の向上に貢献しています。17,000社を超えるセキュリティのリセラーやサービスプロバイダと提携しており、25万社以上の顧客を保護しています。ウォッチガードの実績豊富な製品とサービスは、ネットワークセキュリティとインテリジェンス、高度なエンドポイント保護、多要素認証、セキュアWi-Fiで構成されています。これらの製品では、包括的なセキュリティ、ナレッジの共有、明快さと制御、運用の整合性、自動化という、セキュリティプラットフォームに不可欠な5つの要素を提供しています。同社はワシントン州シアトルに本社を置き、北米、欧州、アジア太平洋地域、ラテンアメリカにオフィスを構えています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多彩なパートナーを通じて、国内で拡大する多様なセキュリティニーズに応えるソリューションを提供しています。詳細はhttps://www.watchguard.co.jpをご覧下さい。

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