DATASHEET

WatchGuard MDR

ウォッチガードのSOCの専門知識でパートナーを支援

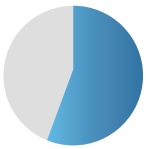
MDRの卓越した機能を活用

脅威が深刻化するにつれ、企業は複雑なセキュリティ上の課題とサイバーセキュリティの専門家不足に悩まされています。さらに、限られたリソースと時間により、サイバーセキュリティの効果的な管理が実現できていません。企業は、こうした問題に対処するために、マネージドセキュリティプロバイダー（MSP）にサイバーセキュリティ業務をアウトソーシングするようになってきています。

しかし、セキュリティオペレーションセンター（SOC）は、熟練したスタッフと多額の投資を必要とするため、MSPがマネージドディテクション&レスポンス（MDR：マネージド型検知／レスポンスサービス）を提供するには課題が残ります。パートナーが抱えるこのような問題は、WatchGuard MDRを活用することで克服することができます。ウォッチガードの包括的な検知／レスポンスサービスをポートフォリオに組み込むことで、パートナーは自社でSOCを構築する負荷がなくなり、顧客の要求に応えることができ、サイバーセキュリティのスキルと予算のギャップを埋めることが可能になります。

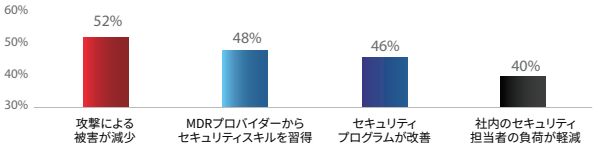
増加するMDRに対する要望

50%
2025年までにMDRサービスを利用する予定の組織の割合[1]



57%
MSPの方が自社の仕組みより優れていると考える組織の割合[2]

MDRが中堅規模組織にもたらしたメリット[2]



ウォッチガードのサイバーエキスパートと連携して最高レベルのMDRを実現

サイバーセキュリティのエキスパートで構成されるウォッチガードの熟練チームが、24時間365日のセキュリティ監視、脅威ハンティング、攻撃の防止、検知、封じ込めにより、お客様のエンドポイントの安全を守ります。

サイバー攻撃の可能性がある場合、チームは封じ込めと修復のプロセスを通じてパートナーを指導し、脅威を直ちに阻止して修復します。パートナーの利便性と攻撃発生時のレスポンス時間を最小限に抑えるため、封じ込めをウォッチガードに委任することもできます。ウォッチガードで自動的に攻撃者を検知し、追跡してブロックするため、パートナーは攻撃の分析および修復に注力することができます。

さらに、サービスのオンボーディングの一環として、ウォッチガードのチームがエンドポイントの攻撃対象領域を評価し、セキュリティ態勢を強化することで、サイバー脅威に対するレジリエンシー（回復力）全般を即座に向上させます。

WatchGuard MDR では、自動的に配信されるサービス活動およびセキュリティヘルスステータスの定期レポートによりパートナーをサポートすることで、予防サービスや攻撃対象領域の削減サービスの提供を支援します。

ウォッチガードのSOC専門家チームは、エンドポイントの監視と365日のテレメトリ（遠隔測定）を通じて、業界先端の信頼性の高いセキュリティ機械学習／AI、および24時間体制で運用される最新の脅威インテリジェンスにより、実用的なセキュリティ分析を実現します。

WATCHGUARD MDRの特長

WatchGuard MDRでは、以下の特長により、プロアクティブなサイバーセキュリティの威力を発揮し、熟練したセキュリティの専門家によって顧客を保護します。

- パートナー向けの包括的なMDRサービス
- サービスのオンボーディングでエンドポイントの攻撃対象領域を最小化
- エンドポイントの活動を継続的に監視
- クラウド上で365日のテレメトリ
- 24時間365日のプロアクティブなハンティング、振舞い検知、調査
- メールや電話で必要な連絡先にインシデントを即時に通知
- MITRE ATT&CKフレームワークを活用した攻撃の詳細レポート
- エンドポイントでフィルタリングされた自動封じ込め向けのカスタマイズされたプレイブック
- 軽減と修復のガイドライン
- 攻撃対象領域の継続的な評価
- エンドポイントのヘルスステータスに関する週次レポート
- リスクステータス、活動監視、検知、レスポンスに関する月次レポート

[1]「マネージド型検知／レスポンスサービス市場ガイド」ガートナー社（2021年10月25日） [2]「セキュリティチームがMDRプロバイダーに求めるものとは」（2023年5月）

メリット

WatchGuard MDRを活用することにより、MSPは最新のSOCを構築・管理する負担がなくなり、トップクラスのサイバーセキュリティ機能をシームレスに提供することができます。また、ウォッチガードの専門知識を生かしてMSPのビジネスを支援するとともに、包括的な脅威のハンティング、検知、レスポンスをMSPの顧客に提供することで、サイバー攻撃のリスクを大幅に低減し、顧客の貴重な資産を保護します。

WatchGuard MDRは時代を先取りしたサービスであり、セキュリティ運用を変革することで比類ない顧客価値を提供し、進化し続ける今日のサイバー脅威に対する強靭な防御体制を構築することができます。

MSPメリット
WatchGuard MDR

- マネージドサービスポートフォリオの拡大により、競争優位を確保
- 最新SOCを自社で構築する必要がなく、投資が不要
- 経験豊富なサイバーエキスパートが支援
- 常時サポート体制により負荷を軽減
- 巧妙化する脅威に対して24時間365日のハンティング、脅威検知／レスポンス
- 柔軟な封じ込めルールにより、レスポンスをカスタマイズ
- マネージドサービスを含む顧客のセキュリティスタックを集約

顧客メリット
MSP経由のMDR

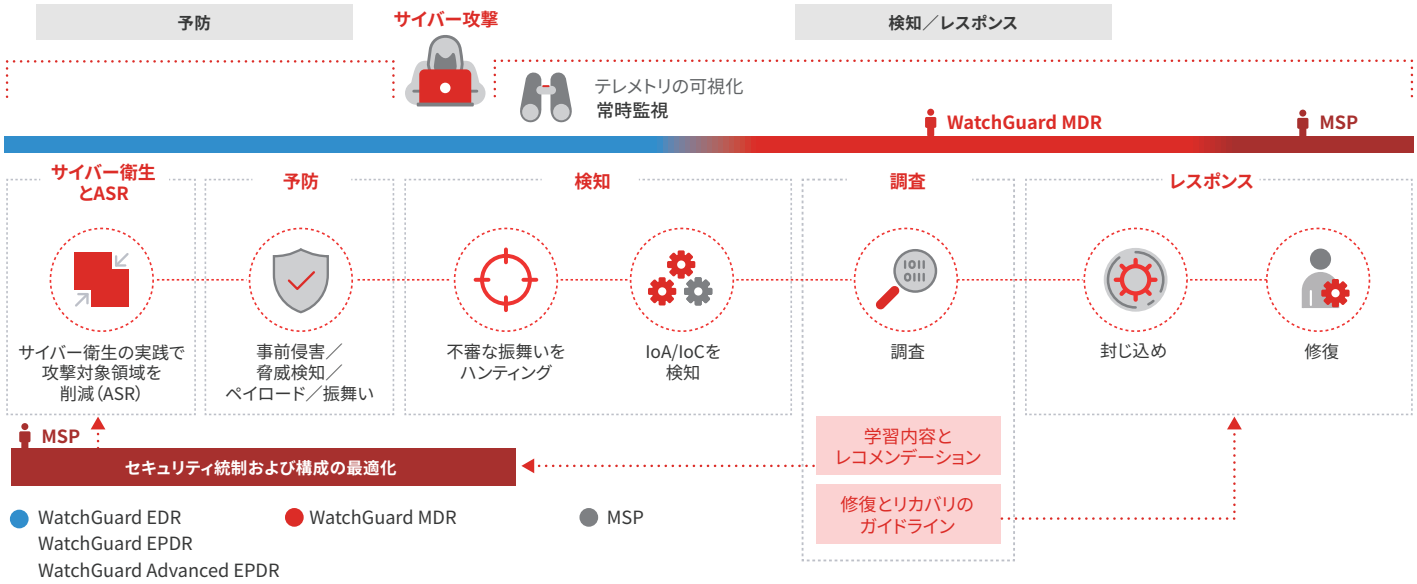
- 脅威をリアルタイムで抑止するプロアクティブなアプローチ
- 24時間365日の監視、検知、レスポンスによる迅速な被害対策
- サイバーセキュリティの専門家の豊富な知識と経験を活用
- 常時変化する脅威情勢に対する柔軟な拡張性
- 導入オプションとビジネスの成長に柔軟に対応
- 脅威と攻撃対象領域の可視化によるセキュリティの向上
- コンプライアンスや規制要件を遵守

効率的な予防、ハンティング、検知、レスポンス

顧客のサイバーセキュリティ態勢を強化するには、予防と攻撃対象領域の縮小、そしてプロアクティブな検知とレスポンスの組み合わせを優先することが極めて重要です。こうしたセキュリティ戦略はすべて相互に関連しています。予防の取り組みは、インシデントと関連コストを最小限に抑えることを目的とし、検知とレスポンスは、予防対策をすり抜けた脅威に対処し、検知とレスポンスにかかる時間を最小限に抑えることで、全体的なセキュリティコストを削減します。

WatchGuard MDRは、WatchGuard EDR、EPDR、Advanced EPDRとそのマネージドサービスを利用することで、自動化された脅威の防御、検知、レスポンスを最大化させることができます。また、ゼロトラストアプリケーションサービスは、マルウェア攻撃対象領域を自律的に最小化し、セキュリティ態勢を強化するとともに、スケーラブルな検知とレスポンスを可能にします。熟練したサイバーセキュリティアナリストは、脅威ハンティングサービスを活用してIoA（攻撃パターン）や僅かな兆候を調査し、複雑なサイバー攻撃を発見します。また、継続的なセキュリティヘルスチェックでは、構成や攻撃対象の露出を評価します。さらにウォッチガードのサイバーセキュリティアナリストは、エンドポイントの攻撃対象領域の最小化、セキュリティ統制の強化、そして設定の微調整に関するガイドラインを提供し、タイムリーなパッチの適用を推奨します。

攻撃対象領域の縮小、予防、および効果的な検知とレスポンス戦略を組み合わせることで、WatchGuard EDR、EPDR、Advanced EPDRとWatchGuard MDRは、MSPに堅牢なサイバーセキュリティフレームワークを提供することができます。



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