SOPHOS

E ブック

EDR、XDR、MDR

これらの違いを正しく把握し、自社に最適なものを選びましょう。

目次

EDR、XDR、MDR

これらの違いを正しく把握し、自社に最適なものを選びましょう。

IT、セキュリティ部門のリーダーは、限られた人数や予算を圧迫することなく、サイバーレジリエンスを強化するというプレッシャーに直面しています。脅威が増加し、攻撃がさらに高度化する中で、検知と対応機能に賢く投資することが不可欠になっています。

事業をグローバルかつ大規模に展開している場合でも、小規模なチームを管理している場合でも、セキュリティ戦略を組織のリスクプロファイルと実際の運用に適合させることが重要です。多くのリーダーは、検知と対応に最適なアプローチを選択する際、自社でソリューションを管理するか、信頼できるパートナーと連携して運用するかを決定しなければならない場面に直面します。EDR (Endpoint Detection and Response)、XDR (Extended Detection and Response)、MDR (Managed Detection and Response) にはそれぞれ独自の利点がありますが、組織に最も価値をもたらす製品を特定することが最も重要な課題です。EDR と XDR は、チームがより迅速に脅威を検知、調査、対応するのに役立つツールです。MDR は、通常は XDR やその他のテクノロジーを使用して、専門のアナリストによる 24 時間 365 日体制の監視と対応を提供するサービスです。

これらのアプローチの違いを理解し、どのように相互に補完し合うかを理解することが、現在の保護対策を強化し、未来を見据えてレジリエンスを高める戦略を構築する第一歩となります。

検知と対応が重要な理由

強力なエンドポイント保護は、依然として重要な防衛線です。しかし、高度なサイバー攻撃者は 正規のユーザーの認証情報を悪用し、信頼できるユーザーになりすまし、組織が利用している IT ツールを悪用して防御を回避します。単一の予防ツールでは、このような攻撃を悪意があると認識できない可能性があり、それが攻撃が成功する理由となっています。

EDR、XDR、MDR などの検知と対応機能は、この重大な弱点を解消します。これらの製品は、予防策をすり抜けた脅威が重大なインシデントにエスカレートする前に、特定して無効化します。

EDR とは?

EDR (Endpoint Detection and Response) は、継続的に組織を保護するエンドポイントセキュリティ戦略の一部です。EDR は、チームがノートパソコン、デスクトップ、サーバーなどのエンドポイントデバイス上の脅威やセキュリティインシデントを監視、検知、対応するのに役立ちます。

EDR の主なメリット：

ファイル実行、プロセスの動作、ラテラルムーブメントなどのエンドポイントにおけるアクティビティをリアルタイムで可視化することで、脅威が拡散する前に迅速に発見して阻止します。

行動指標を識別して回避型の脅威を検知し、従来の予防ツールでは見逃されがちな攻撃を特定するのに役立ちます。

脅威の影響を受けたエンドポイントの隔離や悪意のあるプロセスの強制終了などの対応を自動化し、滞留時間を短縮して攻撃の進行を防ぎます。

Sophos EDR が、オフィス、ネットワーク、クラウドのエンドポイントとサーバーを高度な人間主導の攻撃からどのように組織を保護するのかをご確認ください。

XDR とは？

XDR (Extended Detection and Response) は、エンドポイントやサーバーだけではなく、セキュリティエコシステム全体にわたってデータを統合して、脅威を包括的に可視化します。可視化の対象には、ファイアウォール、メール、クラウドインフラストラクチャ、アイデンティティシステム、バックアップおよびリカバリソリューション、生産性ツール、エンドポイント、サーバーなどが含まれます。XDR は、攻撃が疑われるアクティビティを効果的に相関し、サイロ化したツールでは見逃してしまう恐れのある複数の手法を組み合わせた高度な攻撃を特定するのに役立ちます。

EDR はエンドポイントを深く掘り下げて可視化・分析します。一方、XDR は可視性を高め、すべてのシステムにわたって脅威の全体像を描き出します。攻撃の全体像を把握し、見逃してしまうことの多い複数の手法を用いた多段階型の脅威の検知を容易にします。

XDR の主なメリット：

複数の攻撃方法にわたってシグナルを相関し、攻撃パターンを明らかにし、高精度のアラートを優先順位を付けて提供します。 これによりノイズが低減され、複数のシステムをまたいで段階的に進行する複雑な脅威を明確に特定します。

調査ワークフローを合理化することで、チームは迅速かつ自信を持って脅威に対応できるようになります。アナリストは、攻撃がどのように展開したか、また、再発を防ぐにはどうすればよいかを明確に把握できます。

分析と修復を加速する AI 搭載ツールが調査と対応のワークフローを支援し、迅速かつ確実なインシデント解決を実現します。

Sophos XDR を使用して、エコシステム全体にわたって攻撃が疑われるアクティビティを検知、調査、対応する方法をご覧ください。

MDR とは?

MDR (Managed Detection and Response) は、AI と豊富な専門知識を有する人間のアナリストを組み合わせて、24 時間 365 日体制の監視、脅威ハンティング、インシデント対応を提供するサービスモデルです。これは、24 時間 365 日稼働の運用体制を持たない組織や、自社の SOC では対応できない領域があり、人員の課題、脅威の複雑化に直面している組織にとって特に価値があります。

MDR は、完全にアウトソーシングできるソリューションとして、また社内チームと共同で管理する拡張機能として利用でき、脅威の滞留時間を短縮し、ランサムウェアなどのインシデントが拡大する前に阻止するのに役立ちます。

MDR の主なメリット：

24 時間 365 日体制のサポート脅威は、自社のセキュリティチームが稼働している業務時間を選んで攻撃してくるわけではありません。ランサムウェア攻撃の 88% は通常の業務時間外に発生します。MDR は、すべての時間帯で脅威に対応します。

攻撃者の行動を深く理解し、確実に防御策を講じる専門のセキュリティアナリストのスキルを最大限に活かすことができます。これらのスペシャリストは日々インシデントを迅速に処理し、脅威を優先順位付けして封じ込めることで、ビジネスの円滑な運営を維持します。

アラート疲れと手動のトリアージからチームを解放します。MDR はノイズを排除するため、チームは誤検知されたアラートを追いかけるのではなく、戦略的な取り組みに注力できます。

最も重要な局面で迅速に解決へと導きます。ランサムウェアのような重大インシデントでは、MDR チームが社内のチームよりも早く脅威を検知し封じ込めることで、混乱を未然に防ぎ、リスクを大幅に軽減できます。

Sophos MDR が、どのようにオープンな AI 搭載プラットフォームと専門知識を有するアナリストを融合してチームを補完し、セキュリティ対策のあらゆる段階でお客様を包括的にサポートする仕組みをご覧ください。

EDR、XDR、MDR を検討するタイミング

ソリューション	課題と検討事項	最適解にならない可能性があるケース
EDR	• 強力なエンドポイントの検知と対応が必要。 • 予防的なエンドポイント保護ツールだけではなく、より包括的に防御を強化することを検討している。 • 将来的な XDR または MDR 統合をサポートできる多層防御を構築している。	• クラウド、アイデンティティ、ネットワーク、バックアップなど、環境全体にわたる広範な可視性が必要。 • アウトソーシングやスタッフの増員なしに、24 時間 365 日の検知と対応を可能にしたい。
XDR	• エンドポイント、ファイアウォール、ネットワーク、クラウド、アイデンティティ、バックアップ、生産性ツールなどにわたって、あらゆる主要な攻撃方法を統合的に把握する必要がある。 • 脅威の相関関係を迅速に把握し、アラート疲れを軽減したい。 • 既存および今後のセキュリティや IT への投資で、より大きな効果 (ROI) を得たい場合。	• エンドポイントとサーバーのみを監視している。 • 自社チームが対応できる範囲を超えた実践的なサポートが必要。 • XDR プラットフォームを管理するために必要な社内リソースがない。
MDR	• 専門家による 24 時間 365 日の脅威検知と対応が必要。 • アラート疲れ、人材不足、燃え尽き症候群を経験している。 • 自社チームに代わって脅威を調査し、無力化するプロアクティブなパートナーが必要。 • より有利な条件でサイバー保険を契約し、保険料を下げて補償範囲を拡大したいと考えている。	• すでに、十分な人員と能力を備えた成熟したセキュリティ運用を社内で実施しており、24 時間 365 日体制で堅牢なセキュリティ体制を構築している。 • 検知と対応業務の一部をアウトソーシングする準備ができていない。

決定する前の注意事項

検討する際には、EDR、XDR、MDR のどれが自社に適しているか、またどのパートナーが期待に応えられるかを判断する上で重要な要素がいくつかあります。

脅威インテリジェンスの重要性

検知と対応ソリューションの有効性は、ソリューションを支える脅威インテリジェンスの品質によって決まります。脅威を迅速に特定し阻止するには、広範かつ詳細で、最新の情報が不可欠です。検討しているベンダが脅威データのソースと範囲を明確に説明できることを確認してください。

単なる約束ではなく、実際に価値をもたらすサービス

優れたテクノロジーでも、迅速なサポートがなければ十分に機能しない可能性があります。自社でソリューションを管理する場合でも、マネージドサービスのパートナーを活用する場合でも、必要なときにサポートを確実に受けられることを確認してください。サポートが実際にどのように提供されるのかをベンダーに問い合わせてください。対応するのは誰か、どのくらいの迅速にサポートが提供されるのか、サポートの内容、インシデント発生時にどのような支援を受けることができるかなどを確認してください。

コストを慎重に見極める

どの選択肢が高コストになるかを、最初から決めつけるべきではありません。価格は、各ソリューションの実装方法とサポート方法によって大きく異なります。自社固有のニーズに注目し、現在の人員体制や既存の投資を考慮してください。その際、各テクノロジーのトレードオフや、社内リソースとアウトソーシングのコストを比較することが重要です。

検知と対応ソリューション、特に MDR は、サイバー保険のコストに影響を与える可能性があります。多くの保険会社は、24 時間 365 日体制の脅威監視と対応を実施している組織を高く評価しており、サイバー保険費用の引き下げや補償条件の改善を期待できます。

運用コストの削減、リスクの軽減、保険のメリットまでを考慮した包括的な ROI 分析により、各アプローチの実際のコストと価値を明らかにすることができます。

結論

153 万ドル

ランサムウェア攻撃からの復旧にかかる平均コスト。（身代金の支払いを除く）*

40%

ランサムウェアの被害を受けた組織のうち、サイバーセキュリティの専門知識の不足が攻撃の一因になったと回答した組織の割合。*

サイバーセキュリティでは間違った判断や手探りは許されない

適切な検知と対応戦略の選択は、単にテクノロジーの問題ではありません。人材を最大限に活用し、業務を保護、長期的に持続可能なレジリエントなサイバー防御を構築することが重要です。

* ソフォスランサムウェアの現状レポート 2025 年版

SOPHOS
DEFEAT CYBERATTACKS

ソフォスのソリューションとサービスの詳細

ソフォスは、現在だけでなく未来を見据え、脅威をより効果的に検知して対応できるようにセキュリティ対策を進化させます。

ソフォスの専門家にぜひご相談ください。お客様のビジネスに最適なソリューションを、共に見つけましょう。