Managed Threat Detection

ソフォス製品以外の既存のエンドポイント保護を、24時間 365日体制の監視と検出を提供するフルマネージド型サービスで補完

既存の保護を使用

セキュリティプログラムを 24時間 365日体制で効果的に管理する適切なツール、人材、プロセスを社内に持っている組織はほんとどありません。多くの組織は、自動化されたエンドポイント保護に依存していますが、攻撃者がそれを回避した場合はどうなるのでしょうか？ 手遅れになる前に、それに気づくことができるでしょうか？

Sophos Managed Threat Detection は、24時間 365日体制の脅威監視と検出を提供して、既存のエンドポイント保護を回避した疑わしいアクティビティを検出します。 このサービスは、ソフォス製品以外の既存のエンドポイント保護と並行して動作するように設計されており、組織は、ソフォスの脅威専門家による監視を継続しながら、現在のエンドポイント保護を引き続き使用できます。

検出

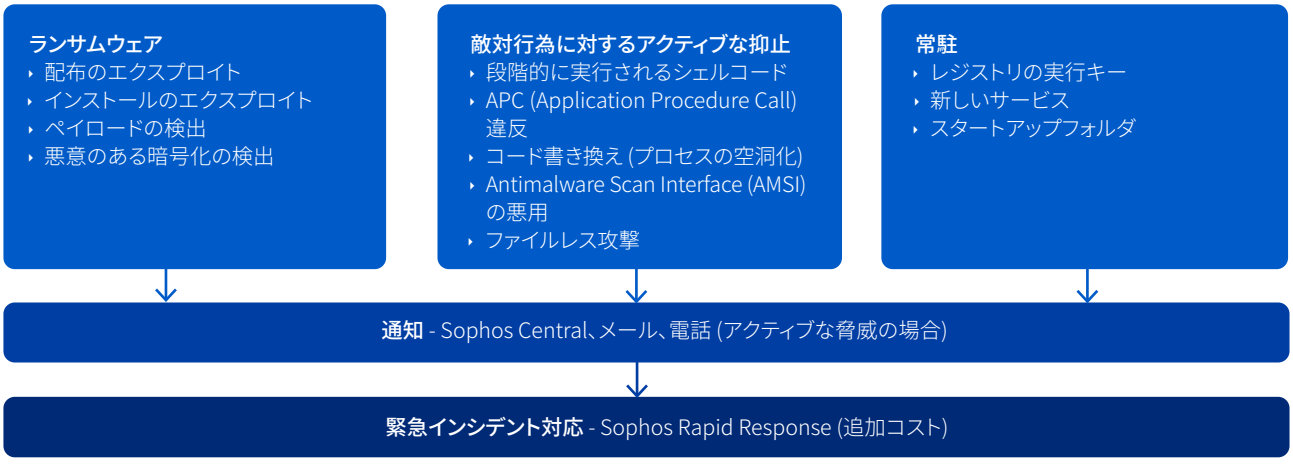
Managed Threat Detection は、「通知」脅威レスポンスモードで使用できます。お客様は、危険度の高い脅威がエンドポイント保護ソリューションを回避した場合、警告を受信します。脅威には、ランサムウェア攻撃の前によく見られる、さまざまな動作のアクティビティが含まれます。

検出イベントの例は次のとおりです。

- CobaltStrike Beacon や Metasploit Meterpreter などでよく検出される、段階的に実行されるシェルコード
- $PS を実行する新しいスケジュールタスク。一般的に、マルウェアや攻撃者によって、永続化に使用される場所 (レジストリの実行キー、サービス、Windows スタートアップ項目など) でのアクティビティを含みます。
- 他の保護製品が見逃す可能性のあるランサムウェアや動作のアクティビティ

主な特長

- 疑わしいアクティビティの 24時間 365日体制の監視と検出
- サードパーティのエンドポイント保護製品と並行して動作するように設計
- 「通知」脅威レスポンスモード
- 危険度の高い脅威の検出すべては、アナリストが検証
- 修正の推奨事項を含む通知
- 追加サービスの Sophos Rapid Response で、インシデント対応を提供



SOPHOS

通知とレスポンス

セキュリティ運用プログラムを実行する際は、明確なコミュニケーションが非常に重要です。このため、Managed Threat Detection サービスは、週次および月次のレポート、メール通知、Sophos Central のダッシュボードなど、頻繁に情報を提供します。

お客様には、ケースの最新ステータスを含むメール通知が送信されます。これには、対処が必要な場合やケースが解決された場合などの警告があります。すべてのケースはアナリストによって検証され、通知にはケースの概要、影響を受けたデバイスのリスト、および修復の推奨事項が含まれます。

さらに、脅威の最新情報、ソフォスの対応、保護を維持するためにお客様ができることなどを説明した、最新の業界ニュースをお客様に通知するブロードキャストメールも配信されます。

お客様の環境でアクティブな脅威が検出された場合は、ソフォスの担当者が電話で連絡します。これによって、重要な情報を速やかに通知することができます。お客様は、Managed Threat Detection の承認済み担当者の連絡先と設定を、Sophos Central ダッシュボードでいつでも更新できます。また、ダッシュボードには、関連するすべての Managed Threat Detection アクティビティの概要が表示され、お客様は必要なときにいつでもどこでも最新の情報を入手できます。

脅威に対応するためにインシデント対応のサポートが必要な場合は、Sophos Rapid Response チームを追加サービスとしてご利用いただけます。Sophos Rapid Response は、アクティブな脅威を調査して無効化するための迅速な緊急支援を提供します。セキュリティ制御を回避しようとしている (または侵害に成功した) 感染や侵害、不正アクセスのいずれであっても、ソフォスは経験を活かして阻止することができます。Rapid Response インシデント対応チームは、Managed Threat Detection エージェントが提供するテレメトリやデータレコーダーに即座にアクセスできるので、ソフォスのお客様は、迅速な対応サービスが提供されます。

	Managed Threat Response (MTR) Standard	Managed Threat Response (MTR) Advanced	Managed Threat Detection
サードパーティのエンドポイント保護製品との互換性	✗	✗	✓
24時間 365日体制の監視	✓	✓	✓
攻撃の検出	✓	✓	✓
レポート、ダッシュボード	✓	✓	✓
脅威通知	✓	✓	✓
Sophos Firewall MTR Connector	✗	✓	✓
Sophos Cloud Optix MTR Connector	✗	✓	✗
複数の OS に対応	✓	✓	✗ (Win10/2012r2 以降のみ)
アナリスト主導のリードレス脅威ハンティング	✗	✓	✗
ソフォスエンドポイントのセキュリティ状態のチェック	✓	✓	✗
リアルタイム保護	✓	✓	✗
封じ込めと無効化	✓	✓	✗
電話による連絡	✗ (アクティブな脅威のみ)	✓	✗ (アクティブな脅威のみ)

ソフォス株式会社
営業部
Email: sales@sophos.co.jp

21-07-13 DS-JA (MP)