Sophos MDR for Microsoft Defender

Microsoft 環境向けの専門家による脅威対応

Sophos Managed Detection and Response (MDR) for Microsoft Defender は、Microsoft Security アラートを 24時間 365日体制で監視、調査、対応を行う高度なスキルを持つ専門家でチームを強化します。

貴社の Microsoft Security 製品への投資を最大限に活用

多くの組織が Microsoft Security スイートに投資していますが、Microsoft のマルチ製品の技術スタックを効果的に使用して、毎日何百ものセキュリティアラートを検出、調査、対応するための十分な専門知識が社内にない可能性があります。

- サイバーセキュリティの専門家不足は世界的に 340万人に達しています[1]。
- セキュリティチームの 71% は、ツールによって生成されるノイズの中から、どのセキュリティアラートを調査するかを判断するのが難しいと感じています[2]。
- セキュリティ運用チームを専門とする組織の脅威対応時間の中央値は 16時間であり、攻撃者がネットワーク内で活動するのにかなりの時間が残されています[3]。

Sophos MDR for Microsoft Defender は、Microsoft 環境で利用できる最も堅牢な脅威検出、ハンティング、対応機能を提供します。ソフォスのアナリストは、Microsoft Security アラートを 24時間年中無休で監視、調査、対応し、アナリスト主導の対応アクションを即時に実行して、発見した脅威を阻止します。平均脅威対応時間は 38分と業界をリードしており、業界のベンチマークよりも 96% 高速です。

Microsoft Defender 以外の脅威の検出と阻止

Sophos MDR for Microsoft Defender を使用する Microsoft Security の専門家が、次の Microsoft 製品のセキュリティデータを使用して脅威を検出、調査、対応します。

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Microsoft 365 セキュリティ & コンプライアンスセンター
- Microsoft Sentinel
- Office 365 Management Activity

さらに、当社独自の検出、業界トップレベルの脅威インテリジェンス、アナリスト主導の脅威ハンティングにより、多層防御が追加され、Microsoft Security ツールだけでは不可能なより多くの脅威を特定して阻止します。

また、組織は、Microsoft 以外のセキュリティツールやソフォスのソリューション、または Palo Alto Networks、Fortinet、Check Point、AWS、Google、Okta、Darktrace などの他のベンダーのテレメトリソースを統合して、完全な可視性と保護を実現することもできます。

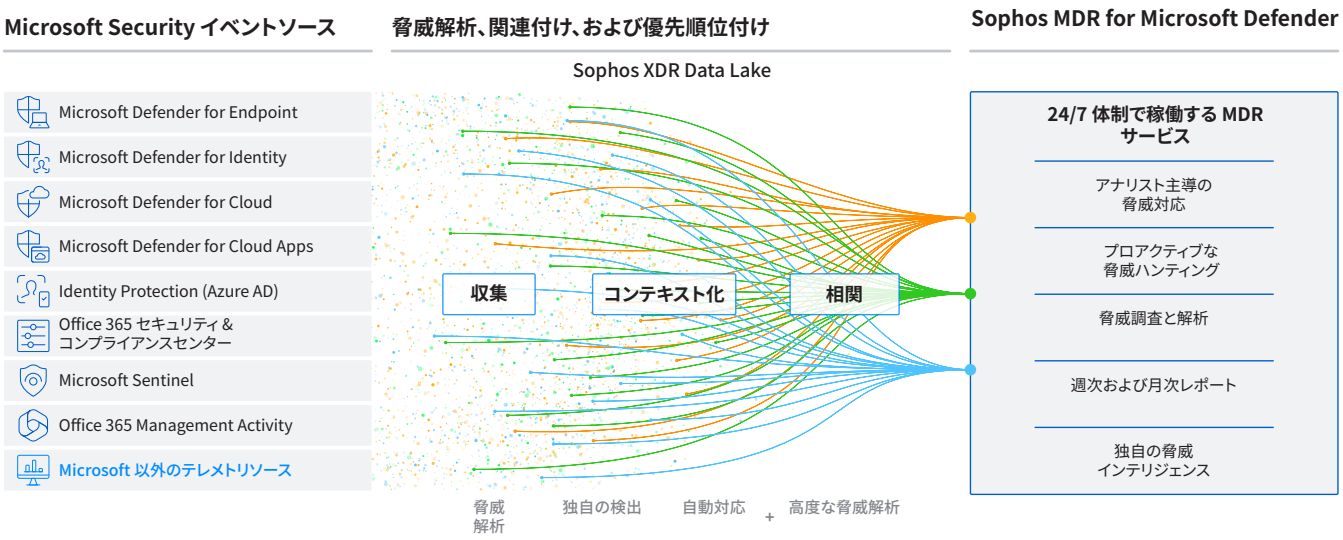
主な特長

- Sophos MDR アナリストが、Microsoft Security アラートを 24時間年中無休で監視、調査、対応し、発見した脅威を阻止するために迅速に対応
- サービス機能は、Microsoft Defender for Endpoint や Microsoft Sentinel を超えて、Microsoft Security プラットフォーム全体をカバー
- アクティブな脅威が特定されると、Sophos MDR 運用チームがお客様に代わって広範な脅威対応アクションを実行
- ソフォス独自の検出、脅威インテリジェンス、アナリスト主導の脅威ハンティングにより、多層防御が追加
- Microsoft 以外のツールとテレメトリソースを統合して、ネットワーク、ユーザー、顧客を標的とした攻撃を阻止

1 2022 Cybersecurity Workforce Study, (ISC)2
2 サイバーセキュリティの現状 2023年版：サイバー攻撃者が防御側のビジネスに及ぼす影響、ソフォス
3 Gartner Cybersecurity Business Value Benchmark database, 2022

SOPHOS

Sophos MDR for Microsoft Defender：主なサービス機能



24時間年中無休の脅威監視

Microsoft Security の専門家は、データが侵害されたり、業務が中断されたりする前に、脅威を検出して阻止します。ソフォスは、世界 6か所のセキュリティ オペレーション センター (SOC) に支えられ、24時間体制で対応しています。

人間主導の脅威対応

Sophos MDR チームは、お客様に代わって、攻撃者を阻止、封じ込め、排除するための一連の対応策を広範囲にわたって実行します。脅威対応アクションには、次のものがあります。

- Sophos Central を使用しているホストの隔離
- ホストベースのファイアウォール IP ブロックの適用
- プロセスの終了
- ユーザーセッションの強制ログオフ
- ユーザーアカウントの無効化
- 悪意のあるアーティファクトの削除
- Sophos Central でブロックされたアイテムへの悪意のあるハッシュの追加

プロアクティブ、アナリスト主導の脅威ハンティング

高度な訓練を受けたアナリストが実行するプロアクティブな脅威ハンティングにより、脅威を発見して迅速に排除し、展開されたツールセットから検出を回避した攻撃者の動作を特定します。

Microsoft 以外のセキュリティツールとの互換性

Sophos MDR は、Microsoft 以外のセキュリティツールとテレメトリソースを統合して、環境全体の攻撃を検出して阻止することができます。

週次および月次レポート

Sophos Central では、リアルタイムの警告、レポート、管理オプションを簡単に利用できます。また、週次および月次のレポートからは、セキュリティ調査、サイバー脅威、組織のセキュリティ体制に関する洞察を得ることができます。

月次の脅威インテリジェンスブリーフィング

Sophos MDR チームが提供する「Sophos MDR ThreatCast」は、最新の脅威インテリジェンスとセキュリティのベストプラクティスに関する洞察を提供する月次ブリーフィングです。

独自の検出

ソフォスのプラットフォームに組み込まれた当社独自の検出、高度な脅威分析、業界トップレベルの脅威インテリジェンスにより多層防御が追加され、Microsoft Security ツールだけでは不可能なより多くの脅威を特定できます。

詳細はこちら

sophos.com/microsoft-defender

ソフォス株式会社営業部
Email: sales@sophos.co.jp

23-07-10 DS-JP (DD)