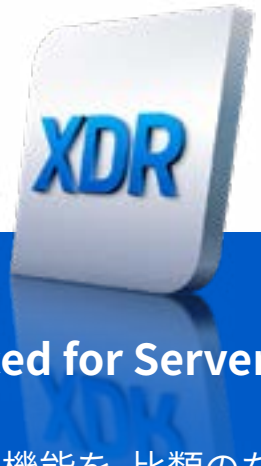
Sophos XDR



Intercept X Advanced with XDR、Intercept X Advanced for Server with XDR

Intercept X は、強力な XDR (Extended Detection and Response) 機能を、比類のないエンドポイント保護に統合します。脅威を探し出し、アクティブな敵対行為を検出、またはIT 運用を活用して IT セキュリティの予防状態を維持します。問題を検出した際には、リモートで的確な対応します。エンドポイント、サーバー、ファイアウォール、メールなどの豊富なデータソースでエンドポイントの可視性を拡張します。

IT 運用や脅威ハンティングに関する質問に回答

ビジネスに不可欠な質問への回答を迅速に得られます。IT 管理者とサイバーセキュリティの専門家の両者は、日常で IT 運用と脅威ハンティングタスクを実行している際に、真の付加価値を見出せるでしょう。

最適な保護から始める

Intercept X は、侵害が開始される前にそれを阻止します。つまり、保護が強化され、自動的に阻止されるべきインシデントの調査時間を短縮できます。また、詳細な脅威インテリジェンスにアクセスして、情報に基づいた迅速なアクションを実行するために必要な情報を提供します。

詳細を確認し、迅速に対応

さらに調査が必要なものを特定したら、Sophos Data Lake からピボットして、最大 90日間の履歴データに加えて、直接デバイスから詳細をライブで取得できます。問題が確認されたら、デバイスにリモートでアクセスし、アプリケーションのアンインストールや再起動などの必要な操作を実行します。

製品間における可視性

Sophos XDR は、エンドポイントやサーバーを超えて、Sophos Firewall、Sophos Email、およびその他のデータソース* が Sophos Data Lake に重要なデータを送信できるようにすることで、組織の環境を非常に広範に把握できます。

デバイスがオフライン状態でも情報を把握

Sophos Data Lake は、XDR 機能の重要なコンポーネントであり、クラウドデータリポジトリです。エンドポイント、サーバー、ファイアウォール、、メールから重要な情報を保管、アクセスするできるだけでなく、デバイスがオフラインの場合でもデバイス情報を利用することができます。

数秒で開始

事前に作成された SQL クエリのライブラリから選択して、さまざまな IT およびセキュリティに関する質問を行えます。必要に応じて、カスタマイズしたり、独自に作成することができます。また、定期的に質問が共有されている Sophos Community を参照することもできます。

主な特長

- ビジネスの重要な IT 運用や脅威ハンティングに関する質問に回答
- IT 管理者とセキュリティアナリスト向けに設計
- 対象のデバイスに対して、リモートで修正措置を実行
- 組織の IT 環境の全体像を把握し、必要に応じて詳細に調査
- エンドポイント、サーバー、ファイアウォール、メールなどのデータソースを活用*
- すぐに使用可能で自由にカスタマイズできる SQL クエリ
- Windows、MacOS 、および Linux で利用可能

*Cloud Optix と Sophos Mobile は まもなく登場

SOPHOS

使用例

IT 運用

- デバイスの動作が遅い理由は？
- どのデバイスに既知の脆弱性、不明なサービス、または不正なブラウザ拡張機能があるか？
- 削除すべきプログラムが実行されていないか？
- 管理されていないゲストおよび IoT デバイスを特定
- オフィスのネットワーク接続が遅いのはなぜか？原因となっているアプリケーションはどれか？
- 紛失したデバイスや破壊されたデバイスでの異常なアクティビティを 30日間遡り確認する

脅威ハンティング

- 非標準ポートでネットワーク接続の確立を試みているのはどのプロセスか?
- ファイルまたはレジストリキーを最近変更したプロセスを表示
- MITRE ATT&CK フレームワークにマッピングされている検出された IOC を一覧表示
- デバイスをオンラインに戻すことなく調査を 30日間へ延長
- ファイアウォールから ATP や IPS 検出を使用して、疑わしいホストを調査
- メールヘッダー情報、SHA、その他の IoC を比較して、悪意のあるドメインへのトラフィックを特定

含まれる機能

	XDR (Extended Detection and Response)
製品間のデータソース	✓
製品間のクエリ	✓
エンドポイントとサーバーのクエリ	✓
Sophos Data Lake	✓
Data Lake の保持期間	30 日間
ディスク上のデータ保持期間	✓
SQL クエリライブラリ	✓
Intercept X の保護機能	✓

ライセンスの詳細については、Intercept X および Intercept X for Server のライセンスガイドを参照してください。

無償評価版

無償評価版の登録 (30日間)
sophos.com/intercept-x

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

21-07-08 DS-JA (PS)