ソリューションの概説

Sophos Endpoint

セキュリティ侵害、ランサムウェア、データ流出を防止

Sophos Intercept X は、業界で最も洗練されたエンドポイントセキュリティソリューションであり、高度な攻撃に対して卓越した保護を実現するために複数のセキュリティレイヤを提供します。包括的な多層防御のアプローチを採用して、システムに影響を与える前に広範な脅威を阻止します。強力な EDR/XDR ツールを使用することで、IT チームやセキュリティチームは脅威の追跡、調査、対応を行うことができます。

ユースケース

1 | 予防第一のアプローチ

期待される結果: より多くの脅威を事前に阻止して、リスクを最小限に抑え、調査と対応の作業負荷を軽減します。

ソリューション: Intercept X は、単一のセキュリティ技術に依存するのではなく、すべてのエンドポイントを保護する包括的なアプローチを採用しています。Web、アプリケーション、周辺機器をコントロールにより、攻撃対象領域を縮小し、一般的な攻撃をブロックします。脅威が拡大する前に、AI、行動分析、ランサムウェア対策、エクスプロイト対策、その他の最先端テクノロジーが脅威を迅速に阻止します。

2 | 合理化された管理

期待される結果: 管理ではなく、脅威の防止、検出、対応に重点を置きます。

ソリューション: Sophos Central は、お客様がすべてのソフォス製品を管理し、脅威をハンティングして調査するクラウドベースの管理コンソールです。強力なデフォルトのポリシー設定により、お客様は追加のトレーニングや調査を行わなくても、推奨される保護設定をすぐに利用できます。Sophos Central 内のアカウントの状態のチェックは、セキュリティの問題を特定して対処するのに役立ちます。

3 | 適応型の防御機能

期待される結果: 攻撃の進化に応じて自動的に適応する防御を行います。

ソリューション: Intercept X は、ハンズオンキーボード攻撃を検出すると、「シールドアップ」のアプローチに従って、エンドポイントで追加の防御を自動的に有効にし、攻撃の進行を阻止します。適応型攻撃防御機能によって、リモート管理ツールのダウンロードなどの疑わしいアクティビティをブロックし、セキュリティチームが時間的な余裕をもって対応できるようにします。

4 | 検出と対応

期待される結果: 保護だけでは対処できない脅威を検出して対応します。

ソリューション: 強力な EDR/XDR 機能により、ソフォスや他社製品のセキュリティコントロール全体で疑わしいアクティビティを検出、調査、対応できます。たとえば、データ流出や悪意のあるコードを使用しないサイレントな攻撃者などが挙げられます。社内でセキュリティを管理する人材を持たないお客様は、エリート専門家チームによる 24時間年中無休体制の脅威の検出と対応を行う Sophos MDR を活用することができます。

Gartner

14回連続のレポートで、Magic Quadrant for Endpoint Protection Platforms でリーダーの評価

SE Labs

業界をリードする保護機能により、独立した第三者機関によるテストを実施

THE CHANNEL CO. CRN TECH INNOVATORS 2023

CRN Tech Innovators Awards で最優秀エンドポイントセキュリティ賞 (2023年 7月)

詳細を確認して試用
Sophos Intercept X:
sophos.com/endpoint

SOPHOS

2024-01-15 SB-JP (PC)