SOPHOS

Intercept X

世界トップクラスのエンドポイント保護製品

Sophos Intercept X は、ディープラーニングによるマルウェアの検出、エクスプロイト対策、ランサムウェア対策などを組み合わせて活用することにより、多種多様な攻撃をブロックします。

主な特長

- マルウェア検出エンジン - ディープラーニングを活用して最高位の検出率を実現
- エクスプロイト防止 - ソフトウェアの脆弱性を悪用する攻撃をブロック
- 敵対行為に対するアクティブな抑止 - マシン上に悪意のあるプログラムが常駐するのを阻止
- 根本原因解析 - マルウェアが加えた変更や感染経路が一目瞭然
- ランサムウェアに特化した保護テクノロジー
- EDR (Endpoint Detection and Response) - IT 管理者とセキュリティアナリストに強力な IT セキュリティ運用の予防策と脅威ハンティングを提供

Sophos Intercept X は、1つの主要機能に依存することなく、エンドポイント保護への包括的な多層防御のアプローチを採用しています。主要かつ基本的な技術と最新の技術を組み合わせて、「プラスのカ」を発揮しています。

最新の技術には、ディープラーニングによるマルウェア検出、エクスプロイト対策、およびランサムウェア対策の機能などがあります。基本的な技術には、シグネチャベースのマルウェア検出、動作解析、Malicious Traffic Detection (MTD)、デバイスコントロール、アプリケーションコントロール、Web フィルタリング、データ流出防止などがあります。

ディープラーニングによるマルウェア検出

Intercept X に組み込まれた人工知能は、高度な機械学習システムであるディープラーニング ニューラル ネットワークで、マルウェア定義ファイルに依存せずに、既知および未知のマルウェアを検出します。

第三者のテスト機関によっても評価されているように、Intercept X はディープラーニングを活用した業界トップクラスのマルウェア検出エンジンです。ディープラーニングによって、 Intercept X は他のエンドポイントセキュリティツールでは検出できなかったマルウェアを検出できます。

エクスプロイトを阻止し、攻撃をブロック

ソフトウェアのセキュリティ上の欠陥である脆弱性は日々発見され、ベンダーによって継続的にパッチが提供される必要があります。一方、新しい攻撃手法の出現はそれほど頻繁ではなく、新たに見つかる脆弱性には、同じ攻撃手法が繰り返し利用されます。エクスプロイト対策は、マルウェアの拡散や、認証情報の窃取、検出の摺り抜けなどに使用されるエクスプロイトやテクニックをブロックし、攻撃を阻止します。これによって、ネットワークで、回避型のハッカーやゼロデイ攻撃を回避できます。

実績のあるランサムウェア対策

Intercept X は、動作解析を活用して、未知のランサムウェアやブートレコード攻撃するランサムウェアを阻止することが可能で、業界で最も高度なランサムウェア対策テクノロジーを誇っています。信頼されていたファイルやプロセスが侵害されたりハイジャックされた場合でも、CryptoGuard がユーザーやヘルプデスク担当者の操作なしで攻撃を停止させ、ファイルの復元を行います。CryptoGuard はファイルシステムレベルでバックグラウンド動作し、リモートコンピュータやローカルプロセスを監視して文書やその他のファイルを変更する動きを検知します。

EDR (エンドポイント検出/対応)

Sophos Intercept X Advanced は、IT 管理者およびセキュリティアナリストが IT 運用と脅威ハンティングのユースケースを解決するために設計された最初の EDR ソリューションです。これを使用することで、エンドポイントで過去に何が起こったのか、今何が起きているのかについて質問できます。 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 セキュリティの衛生状態を維持します。問題を検出した際には、リモートで的確な対応します。

簡単な管理と導入

Sophos Central によるセキュリティ管理は、エンドポイントへのセキュリティ対策の導入の際、サーバーの構築や設置が一切不要です。また、あらかじめ用意されたデフォルトのポリシー群と推奨設定が用意されているため、導入後すぐに効果的なセキュリティ対策を展開することができます。

Managed Threat Response (MTR)

ソフォスの専門家チームが実施する脅威ハンティング、検出、対応を年中無休で提供するフルマネージド型サービスです (ご注意、現時点では英語による対応となります)。Intercept X Advanced with EDR に搭載されている高度な EDR 機能を活用して、ソフォスのアナリストは、潜在的な脅威に対応し、感染の痕跡を検索し、そして、いつ、どこで、誰により、何が、なぜ、どのように発生したのかの詳細を提供します。

システム要件

Sophos Intercept X は Windows 7 以降の 32ビット版および 64ビット版に対応しています。他社製のエンドポイント製品やウイルス対策製品とも共存でき、ディープラーニングによるマルウェア対策や、エクスプロイト対策、ランサムウェア対策、根本原因解析、Sophos Clean などの機能をアドオン的に導入することができます。

	機能	
エクスプロイト防止	データ実行防止 (DEP : Data Execution Prevention)	✓
	必須 ASLR	✓
	Bottom-up ASLR	✓
	Null ページ (Null デリファレンス対策)	✓
	ヒープスプレーアロケーション	✓
	ダイナミックヒープスプレー	✓
	スタックピボット	✓
	スタック実行 (MemProt)	✓
	スタックベースの ROP 抑止 (Caller)	✓
	分岐ベースの ROP 抑止 (ハードウェア拡張)	✓
	SEHOP (Structured Exception Handler Overwrite)	✓
	IAF (Import Address Table Filtering)	✓
	ライブラリ読み込み	✓
	Reflective DLL Injection (反射型 DLL インジェクション攻撃)	✓
	シェルコード	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall	✓
	コード書き換え	✓
	DLL ハイジャック	✓
	Squiblydoo Applocker Bypass	✓
	APC プロテクション (Double Pulsar / AtomBombing)	✓
	プロセスの権限昇格	✓
敵対行為に対するアクティブな抑止	認証情報盗難防止	✓
	コードケイブ抑止	✓
	MITB 攻撃対策 (セーフブラウジング)	✓
	Malicious Traffic Detection (MTD)	✓
	Meterpreter Shell Detection (Meterpreter シェル検出)	✓

	機能	
ランサムウェア対策	ランサムウェアからのファイル保護 (CryptoGuard)	✓
	ファイルの自動修復 (CryptoGuard)	✓
	ディスクとブートレコードの保護 (WipeGuard)	✓
アプリケーションロックダウン	Web ブラウジング (HTA を含む)	✓
	Web ブラウザのプラグイン	✓
	Java	✓
	メディアアプリケーション	✓
	Office アプリケーション	✓
ディープラーニング	ディープラーニングによるマルウェア検出	✓
	ディープラーニングによる業務外アプリケーションのブロック	✓
	誤検知削減	✓
	Live Protection	✓
レスポンス・調査・クリーンアップ	根本原因分析	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
導入形態	単体エージェントとして実行	✓
	既存の他社製ウイルス対策製品との共存	✓
	既存の Sophos Endpoint のエージェントのコンポーネントとして実行	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* CryptoGuard、MTD (Malicious Traffic Detection)、Synchronized Security Heartbeat、根本原因解析などが利用できます

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: sales@sophos.co.jp

2020-05-11 DS (PS)

SOPHOS