

Intercept X

卓越したエンドポイント保護

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
- ▶ Intercept X はお客様の既存のウイルス対策システムを強化します。Intercept X Advanced は、最新の技術と基本的なアプローチを組み合わせて、お客様の既存のエンドポイントセキュリティを置き換えます。

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、「プラスの力」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せん。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

動作解析を活用して、未知のランサムウェアやファイル暗号化だけでなく、ブートレコード攻撃するランサムウェアも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。

根本原因分析

マルウェアを検出し、隔離や駆除を行えば、ひとまず当面の問題は解決できますが、それだけでは、マルウェアを駆除する前に加えられた変更や感染経路は判明しません。根本原因解析 (RCA) では、感染を引き起こしたすべてのイベントを表示できます。マルウェアがアクセスしたファイルやプロセス、レジストリキーを把握でき、高度なシステムクリーンアップ機能を有効にして感染前の状態に戻すこともできます。

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定が一切不要です。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。

	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)	✓

Enterprise Console で Endpoint Protection を管理している場合は、Sophos Central に移行し、Intercept X のライセンスをご購入していただくか、Enterprise Console をお使いのまま Endpoint Exploit Prevention ライセンスをご購入いただくとご利用になれます。

ソフォス株式会社営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

© Copyright 2018.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos は、Sophos Ltd. の登録商標です。その他すべての製品および会社名は、それぞれの所有者に帰属する商標または登録商標です。

2018/08/06 DS-JA (MP)

保護対策のための 4つのステップ

1. sophos.com/intercept-x にアクセスし、製品の無償評価を開始します。
2. Sophos Central の管理者アカウントを作成します。
3. Intercept X エージェントをダウンロードおよびインストールします。
4. Sophos Central からセキュリティ機能を管理します。

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の導入することができます。Intercept X Advanced は、Intercept X にある最新の技術と、Sophos Endpoint Protection にある基本的な技術を組み合わせています。

	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	✓
ディープラーニング	Office アプリケーション	✓
	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	✓
レスポンス・クリーンアップ	誤検知削減	✓
	Live Protection	✓
	根本原因分析	✓
	Sophos Clean	✓
導入形態	Synchronized Security Heartbeat	✓
	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)

www.sophos.com/ja-jp/intercept-x