SOPHOS
Cybersecurity made simple.

CLOUD READY

Intercept X for Server

クラウド型、オンプレミス型の環境を問わず、企業や組織の業務を支える重要なアプリケーションやデータは保護する必要があります。Intercept X for Server 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、ランサムウェア対策テクノロジー、アプリケーションのホワイトリスティング、敵対行為に対するアクティブな保護、および詳細な根本原因解析 (RCA) を活用して、包括的で多層防御のアプローチを提供します。

主な特長

- Microsoft Azure および Amazon Web Services でワークロードを検出、保護
- 悪質なエンドポイントからのリモート攻撃など、ランサムウェア攻撃からサーバーを保護
- サーバーロックダウンで、アプリケーションをホワイトリスト化
- 高度なハッキングテクニックおよびエクスプロイトをブロック
- 根本原因解析 (RCA) で、攻撃の原因解析や感染経路をチェック
- Synchronized Security は、脅威、セキュリティの状態、およびセキュリティ情報を複数のソフォス製品と共有
- Sophos Central で簡単に管理
- Windows および Linux システムの脅威対策

サーバーに特化した強力なセキュリティ対策

Intercept X for Server は、多様な種類の保護機能を活用して、ゼロデイ攻撃、エクスプロイト、およびハッカー攻撃を阻止します。このような対策は、サーバーに到達する前に攻撃をブロックし、実行を未然に検出 / ブロックするとともに、防御機能を迂回する攻撃に対しては徹底的なクリーンアップを実行します。基盤となり、定期的に更新される人工知能モデルは、悪質と思われるコードの疑わしい属性をサーバーで検出するように設計されています。さらに、サーバーロックダウンおよびクラウドワークロードの検出などのサーバー固有の機能によって、サーバーの構成を保護します。

Intercept X for Server は、Microsoft Azure および Amazon Web Services などのクラウドにあるワークロードを検出、保護します。Sophos Central に AWS および Azure を関連付けて、Intercept X for Server は保護されているサーバーの可視化を実現し、該当する情報を Sophos Central に表示して、管理をより簡単にします。

サーバーベースのランサムウェアの阻止

CryptoGuard はランサムウェア対策を提供します。ファイルシステムレベルで動作して、ファイルの不正な暗号化を、サーバーまたはサーバーに接続しているリモートエンドポイントで検出・ブロックします。同様に、WipeGuard は不正な暗号化からマスターブートレコードを保護します。
Sophos Intercept X for Server は、ワンクリックでサーバーをロックダウンします。アプリケーションをホワイトリスト化してサーバーを安全な状態で保持し、認証されていないアプリケーションの実行を阻止します。この機能は、自動的にシステムをスキャンし、既知の正規のアプリケーションのホワイトリストを作成するので、手動でルールを作成する必要はありません。そして、アプリケーションと、アプリケーションに関連付けられている DLL、データファイル、スクリプトなどのファイルとの接続をロックします。

攻撃のブロック：ハッカーによるサーバーアクセスを拒否

脆弱性が日々発見されるなか、ユーザーの業務に支障をきたすことがないように、サーバーに修正パッチを適用するのは簡単なことではありません。エクスプロイト攻撃は、深刻な被害をもたらす可能性があり、従来のサーバー保護テクノロジーでは検出できないことが頻繁にあります。Intercept X for Server は、エクスプロイト手法を使用して認証情報を収集しようとする、最も強力なハッカー攻撃でさえも阻止するように設計されています。身を隠したり、持続的に感染したりするエクスプロイトや、ネットワーク内を移動するエクスプロイトであっても、Intercept X は阻止するように設計されています。

根本原因解析 (RCA)

Intecept X for Server には、検出・対応のテクノロジーも含まれ、感染元や感染ルート、感染範囲のほか、感染時の対応策に関する情報が、管理者向けに視覚的に表示されます。これは、追加のエージェントや管理コンソールを必要とせずに Intercept X for Server によって提供されます。

Synchronized Security

Synchronized Security は、巧妙な攻撃に先手を打つ、ベスト・オブ・ブリードの製品群を統合したセキュリティシステムです。　直感的に操作できるセキュリティプラットフォームと、数々の受賞歴を誇るソフォスの製品群を統合し、複数の製品が相互連係することで、高度な脅威に対して抜群の効果を発揮します。

Sophos Central で簡単に管理

Sophos Central によるセキュリティ管理では、システムのセキュリティ対策を導入するにあたり、サーバーの構築や設置が一切不要となります。ソフォスが提供するクラウドベースの Sophos Central は、即時にアクセスできるだけでなく、管理サーバーの設定は一切不要です。Sophos Central は、セットアップが簡単な保護を提供するだけでなく、Sophos Intercept X、モバイル、ワイヤレス、メール、Web のセキュリティ対策など、他のソフォス製品もすべて単一の画面から一元管理することができます。

Intercept X for Server とその他の Server Protection ライセンスの主な特長

			Sophos Central (クラウド管理)		SEC (オンプレミス管理)	
			Central Intercept X Advanced for Server (SVRCIXA)	**Central Server Protection** (SVRC)	**Server Protection for Virtualization, Windows, and Linux** (SVRWLV)	**Server Protection Enterprise (SAVSVR)**
Sophos Server Protection Agent						
プラットフォーム		Windows Server	✓	✓	✓	✓
		Linux[1]	✓	✓	✓	✓
		UNIX[3]				✓
		パブリッククラウド (Microsoft Azure、Amazon AWS)	✓	✓		
防御	攻撃対象領域の削減	アプリケーションのホワイトリスト化 [サーバーロックダウン]	✓			
		Web セキュリティ	✓	✓	✓	✓
		Windows ファイアウォールの制御	✓	✓		
		ダウンロードレピュテーション	✓	✓	✓	✓
		Web コントロール (URL によるブロック)	✓	✓	✓	✓
		周辺機器コントロール (USB など)	✓	✓	✓	✓
		アプリケーションコントロール	✓	✓	✓	✓
	実行前防御	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	✓			
		ファイルのマルウェア検索	✓	✓	✓	✓
		Live Protection	✓	✓	✓	✓
		実行前動作解析 [HIPS]	✓	✓	✓	✓
		VM のオフボード型検索 (ESXi、Hyper-V 環境)[2]	✓	✓	✓	✓
		業務上不要と思われるアプリケーション (PUA) の検出	✓	✓	✓	✓
		データ流出防止 (DLP)	✓	✓	✓	✓

1 Windows ではすべての機能が利用可能。Linux では一部利用できない機能もあります。
2 超軽量型エージェントを装備した Sophos for Virtual Environments の機能の詳細は、3ページを参照してください。
3 Sophos Anti-Virus for UNIX は、スタンドアロン版 (管理機能なし) での提供。オンデマンドスキャンとスケジュールスキャンのみ。

			Sophos Central (クラウド管理)		SEC (オンプレミス管理)	
			Central Intercept X Advanced for Server (SVRCIXA)	**Central Server Protection** (SVRC)	**Server Protection for Virtualization, Windows, and Linux** (SVRWLV)	**Server Protection Enterprise (SAVSVR)**
検出	脅威の実行を停止	ハッキングに対する防御 / 敵対行為に対するアクティブな抑止	✓			
		ランサムウェアからのファイル保護 [CryptoGuard]： サーバーに接続しているエンドポイントからのサーバーに対する攻撃も検出	✓		アドオン機能[4]	✓
		ディスクとブートレコードの保護 [WipeGuard]	✓			
		Malicious Traffic Detection (MTD)	✓	✓		
対応	調査して削除	Sophos Clean：マルウェアの自動削除	✓			
		マルウェアの削除		✓	✓	✓
		根本原因解析 (RCA)	✓			
管理	制御	サーバー専用ポリシーの管理	✓	✓	✓	✓
		アップデートキャッシュとメッセージリレー	✓	✓		
		検索から除外する項目を自動検出	✓	✓		
		Synchronized Application Control[5]	✓	✓		
	可視化	Azure のワークロードの検出と保護	✓	✓		
		AWS のワークロードの検出と保護	✓	✓		
		AWS 地図、複数のリージョンの可視化	✓	✓		
		Synchronized Security と Security Heartbeat™ (強化された脅威対策、感染先検出、自動隔離)[5]	✓	✓		
		Windows リモートデスクトップサービス (ユーザーの可視化)	✓	✓		
	SOPHOS CENTRAL	クラウドベースの管理：専用のオンプレミス型サーバーのインストール、維持は不要。エンドポイント、モバイルデバイス、メール、ワイヤレスデバイスと併せて、単一のコンソールからサーバーのセキュリティを管理	✓	✓		
		多要素認証	✓	✓		
		ロールベースの管理	✓	✓	✓	✓

4 Sophos Enterprise Console の管理下にある Windows Server 環境で CryptoGuard をご利用いただく場合は、Endpoint Exploit Prevention (EXP) ライセンスの追加購入が必要です。
5 Sophos XG Firewall と併用した場合。

Azure

aws partner network
Advanced Technology Partner
Security Competency
Public Sector Partner
Marketplace Seller

無償評価版

無償評価版の登録 (30日間)
sophos.com/ja-jp/server

ソフォス株式会社営業部
Email：sales@sophos.co.jp

2018/06/28 DS-JA (MP)

SOPHOS