Intercept X for Server および Central Server Protection の概要

Sophos Central で管理

	機能	Central Server Protection	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR
攻撃対象領域の削減	Web セキュリティ	✓	✓	✓
	ダウンロードレピュテーション	✓	✓	✓
	Web コントロール / カテゴリベースの URL ブロック	✓	✓	✓
	周辺機器コントロール	✓	✓	✓
	アプリケーションコントロール	✓	✓	✓
	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)		✓	✓
実行前防御	ディープラーニングによるマルウェア検出		✓	✓
	ファイルのマルウェア検索	✓	✓	✓
	Live Protection	✓	✓	✓
	実行前動作解析 (HIPS)	✓	✓	✓
	不要と思われるアプリケーション (PUA) のブロック	✓	✓	✓
	侵入防御システム (IPS、2020年に発売)	✓	✓	✓
脅威の実行を停止	データ流出防止 (DLP)	✓	✓	✓
	ランタイム動作解析 (HIPS)	✓	✓	✓
	Antimalware Scan Interface (AMSI)	✓	✓	✓
	Malicious Traffic Detection (MTD)	✓	✓	✓
	エクスプロイト対策 (詳細は 5 ページ)		✓	✓
	敵対行為に対するアクティブな抑止 (詳細は 5 ページ)		✓	✓
	ランサムウェアからのファイル保護 (CryptoGuard)		✓	✓
	ディスクとブートレコードの保護 (WipeGuard)		✓	✓
	MITB 攻撃から保護 (セーフブラウジング)		✓	✓
	アプリケーションロックダウンの機能拡張		✓	✓
検出	Live Discover (脅威ハンティングと IT セキュリティの運用の予防策に対する保護領域の SQL クエリ)			✓
	SQL クエリライブラリ (事前に作成され、自由にカスタマイズ可能なクエリ)			✓
	疑わしいイベントの検出と優先順位付け			✓
	高速アクセス、ディスク上のデータストレージ (最大 90 日間)			✓

機能は次のページに続きます

Intercept X for Server および Central Server Protection の概要

Sophos Central で管理

	機能	Central Server Protection	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR
調査	脅威ケース (根本原因分析)		✓	✓
	ディープラーニングによるマルウェア解析			✓
	SophosLabs の高度な脅威解析情報をオンデマンドで利用			✓
	フォレンジックデータのエクスポート			✓
修正	マルウェアの自動削除	✓	✓	✓
	Synchronized Security Heartbeat	✓	✓	✓
	Sophos Clean		✓	✓
	リモートターミナルアクセス (リモートで調査して対処)			✓
	オンデマンドのサーバー隔離			✓
	「クリーン&ブロック」をワンクリック			✓
可視性	クラウドワークロード保護 (Amazon Web Services、Microsoft Azure、Google Cloud Platform)*	✓	✓	✓
	AWS 地図、複数のリージョンの可視化	✓	✓	✓
	Synchronized Application Control (アプリケーションの可視性)	✓	✓	✓
	クラウドのセキュリティ状態を管理 (クラウドホスト、サーバーレス機能、S3 バケットなどの監視とセキュリティ保護)			✓
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	✓	✓	✓
	ファイル整合性の監視	✓	✓	✓

[1]パブリッククラウドのサポートについては、サポートデータベースの文章を参照ください: https://community.sophos.com/kb/en-us/132540

OS 機能の比較

SOPHOS

	機能	WINDOWS	LINUX*
攻撃対象領域の削減	Web セキュリティ	✓	
	ダウンロードレピュテーション	✓	
	Web コントロール / カテゴリベースの URL ブロック	✓	
	周辺機器コントロール	✓	
	アプリケーションコントロール	✓	
	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)	✓	
実行前防御	ディープラーニングによるマルウェア検出	✓	
	ファイルのマルウェア検索	✓	* 注記参照
	Live Protection	✓	* 注記参照
	実行前動作解析 (HIPS)	✓	
	不要と思われるアプリケーション (PUA) のブロック	✓	
	侵入防御システム (IPS、2020年に発売)	✓	
脅威の実行を停止	データ流出防止 (DLP)	✓	
	ランタイム動作解析 (HIPS)	✓	
	Antimalware Scan Interface (AMSI)	✓	
	Malicious Traffic Detection (MTD)	✓	* 注記参照
	エクスプロイト対策 (詳細は 5 ページ)	✓	
	敵対行為に対するアクティブな抑止 (詳細は 5 ページ)	✓	
	ランサムウェアからのファイル保護 (CryptoGuard)	✓	
	ディスクとブートレコードの保護 (WipeGuard)	✓	
	MITB 攻撃から保護 (セーフブラウジング)	✓	
	アプリケーションロックダウンの機能拡張	✓	
検出	Live Discover (脅威ハンティングと IT セキュリティの運用の予防策に対する保護領域の SQL クエリ)	✓	✓
	SQL クエリライブラリ (事前に作成され、自由にカスタマイズ可能なクエリ)	✓	✓
	疑わしいイベントの検出と優先順位付け	✓	
	高速アクセス、ディスク上のデータストレージ (最大 90 日間)	✓	✓

機能は次のページに続きます

OS 機能の比較

SOPHOS

	機能	WINDOWS	LINUX*
調査	脅威ケース (根本原因分析)	✓	
	ディープラーニングによるマルウェア解析	✓	
	SophosLabs の高度な脅威解析情報をオンデマンドで利用	✓	
	フォレンジックデータのエクスポート	✓	
修正	マルウェアの自動削除	✓	
	Synchronized Security Heartbeat	✓	* 注記参照
	Sophos Clean	✓	
	Live Response (さらなる調査と対応のためのリモートターミナルアクセス)	✓	✓
	オンデマンドのサーバー隔離	✓	
	「クリーン&ブロック」をワンクリック	✓	
可視性	クラウドワークロード保護 (Amazon Web Services、Microsoft Azure、Google Cloud Platform)	✓	
	AWS 地図、複数のリージョンの可視化	✓	
	Synchronized Application Control (アプリケーションの可視性)	✓	
	クラウドのセキュリティ状態を管理 (クラウドホスト、サーバーレス機能、S3 バケットなどの監視とセキュリティ保護)	✓	✓
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	✓	
	ファイル整合性の監視	✓	

* Linux には 2 つの導入オプションがあります。1) Intercept X Advanced for Server with EDR の導入では、表に記載されている機能にアクセスできます。2) Sophos Anti-Virus for Linux の導入には、次のものが含まれます。マルウェア対策、Live Protection、悪意のあるトラフィックの検出 (MTD)、および Synchronized Security。2 つの導入オプションは混在できないことをご留意ください。

Sophos Intercept X の機能

Intercept X に含まれる機能の詳細

SOPHOS

	機能	
エクスプロイト防止	データ実行防止 (DEP：Data Execution Prevention)	✓
	アドレス空間配置のランダム化の強制	✓
	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	✓
	ダイナミックシェルコード対策	✓
	EFS Guard	✓
	CTF Guard	✓
	ApiSetGuard	✓
敵対行為に対するアクティブな抑止	認証情報盗難防止	✓
	Code Cave 抑止	✓
	MITB 攻撃から保護 (セーフブラウジング)	✓
	Malicious Traffic Detection	✓
	Meterpreter Shell Detection (Meterpreter シェル検出)	✓

	機能	
ランサムウェアの対策	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プロテクション	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不要と思われるアプリケーション (PUA) のブロック	✓
	誤検知削減	✓
対応 調査 クリーンアップ	脅威ケース (根本原因分析)	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓

Managed Threat Response (MTR)

SOPHOS

Sophos Managed Threat Response (MTR) は、脅威ハンティング、検出、対応機能を年中無休でソフォスの専門家チームより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。)MTR をご利用のお客様には、Intercept X Advanced for Server with EDR も提供されます。

Sophos MTR：Standard

年中無休のリード主導の脅威ハンティング

確認された悪意のあるアーティファクトやアクティビティ (強力なシグナル) を自動的にブロックまたは終了し、脅威ハンターの負担を軽減し、手がかりをもとにリード主導の脅威ハントを実行できます。このタイプの脅威ハントでは、以前は検出できなかった新しい攻撃の指標 (IoA) と感染の痕跡 (IoC) を発見するための因果的および隣接するイベント (弱い信号) のアグリゲーションと調査が行われます。

セキュリティ状態のチェック

Intercept X Advanced with EDR から始めて、動作状況と推奨される構成の改善を積極的に調査することで、最高のパフォーマンスで Sophos Central 製品を稼働させ続けます。

アクティビティレポート

ケースアクティビティの概要により、優先順位付けとコミュニケーションが可能になり、各レポート期間内でどのような脅威が検出され、どのような対応が実行されたかを把握できます。

攻撃を検出

成功する攻撃のほとんどでは、監視ツールで正当と思わせるプロセスを実行します。ソフォスは独自の調査手法を使用して、正当な動作と攻撃者が使用するTTP (戦術、技術、攻撃手順) との違いを判断します。

Sophos MTR：Advanced すべての Standard 機能に加えて、以下の機能となります。

年中無休のリードレス (手掛かりなし) の脅威ハンティング

データサイエンス、脅威インテリジェンス、および経験豊富な脅威ハンターの直感を適用して、企業プロファイル、価値の高い資産、リスクの高いユーザーを組み合わせ、攻撃者の行動を予測し、新しい攻撃の指標 (IoA) を特定します。

テレメトリーの強化

エンドポイントを超えて拡大される他の Sophos Central 製品からのテレメトリで脅威調査を補完し、持続的攻撃の全体像を提供します。

プロアクティブな対策改善

セキュリティ対策をプロアクティブに改善し、全体的なセキュリティ機能を低下させる構成とアーキテクチャの弱点に対処するために、規範的なガイダンスを使用して防御を強化します。

専用の脅威対応リード

インシデントが確認されると、専用の脅威対応リードが提供され、アクティブな脅威が無力化されるまで直接オンプレミスリソース (社内チームまたは社外パートナー) と連携して取り組みます。

直接連絡サポート

セキュリティ オペレーション センター (SOC) へ直接連絡できます。MTR 運営部門は世界 26か国にわたり年中無休態勢でサポートします。

アセットの検出

OSのバージョン、アプリケーション、脆弱性をカバーするアセット情報から、マネージドアセットとアンマネージドアセットの識別までをカバーし、影響の評価中、脅威ハント実施中、プロアクティブな対策改善の推奨事項の一環として、分析情報を提供します。