Sophos Workload Protection ライセンスガイド

SOPHOS
Cybersecurity delivered.

Intercept X for Server、XDR、Cloud Native Security、および MTR 概要

Sophos Central で管理

機能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
管理						
複数のポリシー		✓	✓	✓	✓	✓
アップデート制御		✓	✓	✓	✓	✓
攻撃対象領域の削減						
アプリケーションコントロール		✓	✓	✓	✓	✓
周辺機器コントロール		✓	✓	✓	✓	✓
Web コントロール / カテゴリベースの URL ブロック		✓	✓	✓	✓	✓
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)		✓	✓	✓	✓	✓
ダウンロードレピュテーション	✓	✓	✓	✓	✓	✓
Web セキュリティ	✓	✓	✓	✓	✓	✓
デバイスで実行される前						
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)	✓	✓	✓	✓	✓	✓
脅威の実行を停止						
データ流出防止		✓	✓	✓	✓	✓
ランタイム動作解析 (HIPS)	✓	✓	✓	✓	✓	✓
Antimalware Scan Interface (AMSI)	✓	✓	✓	✓	✓	✓

機能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
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 (事前作成され、カスタマイズ可能なクエリ)			✔	✔	✔	✔
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)			✔	✔	✔	✔
製品間のデータソース (ファイアウォール、メールなど)			✔	✔	✔	✔
検出の優先リスト			✔	✔	✔	✔
Sophos Data Lake (クラウドデータストレージ)			30 日間	30 日間	30日間	30 日間
定期的なクエリ			✔	✔	✔	✔
コンテナランタイムの可視性と検出			✔	✔	✔	✔
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			✔	✔	✔	✔
AI ガイドによる調査			✔	✔	✔	✔

機能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
修復						
マルウェアの自動削除	✓	✓	✓	✓	✓	✓
Synchronized Security Heartbeat	✓	✓	✓	✓	✓	✓
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			✓	✓	✓	✓
コンテナランタイムの可視性と検出			✓	✓	✓	✓
制御						
Synchronized Application Control (アプリケーションの可視性)	✓	✓	✓	✓	✓	✓
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			✓	✓	✓	✓
クラウド環境						
クラウド環境の監視: AWS、Azure、GCP、Kubernetes、IaC および Docker Hub レジストリ		プロバイダごとに 1つ	プロバイダごとに 1つ	無制限	プロバイダごとに 1つ	プロバイダごとに 1つ
セキュリティの監視 (CSPM ベストプラクティスルール)		毎日スキャン	毎日スキャン	スケジュールスキャン、毎日スキャン、オンデマンドスキャン	毎日スキャン	毎日スキャン
アセットインベントリ		✓	✓	✓	✓	✓
高度な検索機能		✓	✓	✓	✓	✓
AI による異常検知		✓	✓	✓	✓	✓
SophosLabs Intelix 悪質なトラフィック警告		✓	✓	✓	✓	✓
メール警告		✓	✓	✓	✓	✓
AWS ネイティブサービスの統合 (Amazon GuardDuty、AWS Security Hub、Amazon Inspector など)		✓	✓	✓	✓	✓
Azure ネイティブサービスの統合 (Azure Sentinel および Azure Advisor)		✓	✓	✓	✓	✓
Cloud Workload Protection: Sophos Intercept X Server エージェント検出		✓	✓	✓	✓	✓
Cloud Workload Protection: Sophos Intercept X Server のエージェント自動削除		✓	✓	✓	✓	✓

機能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
コンプライアンスポリシーとレポート		CIS Benchmarks	CIS Benchmarks	CIS Benchmarks、ISO 27001、EBU R 143、FEDRAMP FIEC、GDPR、HIPAA、PCI DSS、SOC2、ソフォス ベスト プラクティス	CIS Benchmarks	CIS Benchmarks
カスタムポリシー				✔		
ネットワークの可視化		✔	✔	✔	✔	✔
IAM の視覚化		✔	✔	✔	✔	✔
消費の監視		✔	✔	✔	✔	✔
警告管理の統合（Jira、ServiceNow、Slack、Teams、PagerDuty、Amazon SNS）		✔	✔	✔	✔	✔
SIEM 統合（Splunk、Azure Sentinel）		✔	✔	✔	✔	✔
Rest API		✔	✔	✔	✔	✔
Infrastructure-as-Code のテンプレートスキャン		✔	✔	✔	✔	✔
環境アクセス制御		✔	✔	✔	✔	✔
コンテナイメージのスキャン（ECR、ACR、Docker Hub、API）		✔	✔	✔	✔	✔
マネージドサービス						
24時間365日のリード主導型脅威ハンティング					✔	✔
セキュリティ状態チェック					✔	✔
データ保管					✔	✔
アクティビティレポート					✔	✔
攻撃を検出					✔	✔
脅威の無効化と修復					✔	✔
24時間365日のリードレス型脅威ハンティング						✔
脅威対応チームのリード						✔
直接連絡サポート						✔
プロアクティブなセキュリティポスチャの管理						✔
ランサムウェアからのファイル保護 (CryptoGuard)						✔

OS 機能の比較

機能	Windows	Linux*
管理		
複数のポリシー	✔	✔
アップデート制御	✔	✔
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)	✔	
デバイスで実行される前		
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)	✔	
脅威の実行を停止		
データ流出防止	✔	
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	✔	

機能	Windows	Linux*
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 (事前作成され、カスタマイズ可能なクエリ)	✔	✔
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)	✔	✔
製品間のデータソース (ファイアウォール、メールなど)	✔	✔
検出の優先リスト	✔	✔
Sophos Data Lake (クラウドデータストレージ)	✔	✔
定期的なクエリ	✔	✔
コンテナランタイムの可視性と検出		✔
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	✔	
AI ガイドによる調査	✔	✔
修復		
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	✔	
制御		
Synchronized Application Control (アプリケーションの可視性)	✔	
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	✔	

機能	Windows	Linux*
ファイル整合性の監視	✔	
マネージドサービス		
24時間365日のリード主導型脅威ハンティング	✔	✔
セキュリティ状態チェック	✔	✔
データ保管	✔	✔
アクティビティレポート	✔	✔
攻撃を検出	✔	✔
脅威の無効化と修復	✔	✔
24時間365日のリードレス型脅威ハンティング	✔	✔
脅威対応チームのリード	✔	✔
直接連絡サポート	✔	✔
プロアクティブなセキュリティポスチャの改善	✔	✔

* Linux には 2 つの導入オプションがあります。1) Sophos Protection for Linux 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。

ソフォス保護の概要

Intercept X および Cloud Native Security に含まれるワークロード保護機能の詳細

特徴	
エクスプロイト対策	
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	✔

特徴	
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)	✔
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 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	✔
レスポンス・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 MTR (Managed Threat Response) は、脅威ハンティング、検出、対応機能を24時間365日で、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。
MTR をご利用のお客様には、Intercept X Advanced for Server with XDR も提供されます。

Sophos MTR：Standard

24時間365日のリード主導型 (手掛かりあり) 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、手がかりを基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
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、Intercept X Advanced for Server with XDR をはじめとする Sophos Central 製品を最高のパフォーマンスで稼働させ続けます。

アクティビティレポート
ケースアクティビティの概要を基にして、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。

攻撃の検出
成功した攻撃の多くは、監視ツールからは正規のプロセスに見えるプロセスの実行に依存しています。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、以下の機能が追加されます。

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。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

© Copyright 2022.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。その他記載されている会社名、製品名は、各社の登録商標または商標です。

22-07-25 JA (DD)

SOPHOS