Server Workload Protection

Linux 保護

Intercept X Advanced for Server、Intercept X Advanced for Server with XDR および Intercept X Advanced for Server with MTR

クラウドまたはデータセンター、ホストおよびコンテナ。パフォーマンスへの影響が少ないソフォスのワークロード保護により、インフラの成長や進化に合わせて保護します。

最小限に抑えた検出と対応の時間

ホストとコンテナのワークロードを包括的に可視化し、マルウェア、エクスプロイト、および異常な動作が発生する前にそれを特定することができます。XDR（Extended Detection and Response）は、ホスト、コンテナ、エンドポイント 、ネットワークトラフィック、クラウドプロバイダーのネイティブセキュリティサービスへの詳細な情報を提供します。

クラウドネイティブの動作検知とエクスプロイトランタイム検出により、コンテナのエスケープ、カーネルのエクスプロイト、権限昇格の試みなどの脅威を特定します。合理化された脅威調査ワークフローにより、リスクの高いインシデントの検出に優先順位を付け、接続されたイベントを統合して効率を向上させ、時間を節約します。

セキュリティ運用の改善

Sophos Central 管理コンソールを介して提供される、または展開オプションを選択して既存の脅威対応ツールに統合された、すぐに使用可能なホストやコンテナのランタイムの可視性と脅威検出を使用して脅威と戦います。

Sophos Central の管理 – この軽量 Linux エージェントは、セキュリティチームに、振る舞い、エクスプロイト、マルウェアの脅威を 1ヵ所で調査および対応するために必要な重要な情報を提供します。Linux ホストを監視するこの展開オプションにより、チームはすべてのソフォスソリューションを単一画面で管理し、脅威ハンティング、修復、管理間をシームレスに移動できます。

API の統合 - Sophos Linux Sensor は、パフォーマンスに合わせて微調整された、柔軟性の高い展開オプションです。Linux Sensor は、API を使用して、ホスト環境またはコンテナ環境でのリッチランタイム脅威検出と既存の脅威対応ツールを統合します。より幅広い検出、カスタムルールセットを作成するための制御、ホストリソースの使用率を調整するための設定オプションを提供します。

スムーズなパフォーマンスを実現

Intercept X for Server による保護は、DevSecOps ワークフローに最適化されているため、カーネルモジュール、オーケストレーション、ベースライン、システムスキャンを必要とせず、巧妙な攻撃を発生と同時に特定できます。CPU、メモリ、データ収集の制限など、リソースの制限を最適化することで、ホストの過負荷によるダウンタイムや安定性の問題によるコストのかかるダウンタイムをさらに回避できます。アプリケーションのパフォーマンスと稼働時間を最適化します。

主な特長

- クラウド、オンプレミス、および仮想 Linux ワークロードとコンテナの安全を確保
- 最小限に抑えた脅威の検出と対応時間
- パフォーマンスが重要なミッションクリティカルなワークロード向けに最適化
- 拡張した XDR (Extended Detection and Response) を使用して、エンドポイント、ネットワーク、メール、クラウド、M365、モバイルデータを活用
- クラウドセキュリティポスチャ管理により、幅広いクラウド環境を理解し、セキュリティを確保
- フルマネージドサービスとして提供される24時間年中無休のセキュリティを提供

SOPHOS

クラウドセキュリティチェックリストの自動化

広範なパブリッククラウド環境全体をカバーする統合されたクラウドセキュリティポスチャ管理で、可視性やツールを維持するためそれらを使用して、ベストプラクティスの基準に満たすようにお客様のクラウド環境を設計します。

- AWS、Microsoft Azure、GCP（Google Cloud Platform）にわたり、未承認のアクティビティ、ホストやコンテナイメージの脆弱性、構成ミスを積極的に特定
- ソフォスのホスト保護と Sophos Firewall 展開の詳細なインベントリと可視化により、クラウドリソースを継続的に検出
- セキュリティのベストプラクティス標準を自動的にオーバーレイして、ポスチャのギャップを検出し、クイックウィンと重要な問題を特定
- ユーザー IAM ロールの動作におけるリスクの高い異常を検出し、異常なアクセスパターン、場所、悪意のある動作をすばやく特定して、侵害を防止

チームを強化するパートナーシップ

Sophos Managed Threat Response の SOC アナリストは、お客様のチームと連携して、24時間年中無休で環境を監視し、効率を高めるために必要な Linux の専門知識を活用して、お客様に代わって脅威を積極的に探し、修復します。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、いつ、どこで、なぜ、どのようにして何が発生したかなど、イベントに関する詳細な分析を提供する必要があります。

技術仕様

最新情報に関しては、Linux のシステム要件を参照してください。Windows の機能の詳細については、Windows データシートを参照してください。

特徴	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Linux 保護エージェント （マルウェアスキャン、エクスプロイト防止、ファイルスキャンなどを含む）	✔	✔	✔
Linux Sensor （Linux およびコンテナランタイムの脅威検出を、API を介して既存の脅威対応ツールと統合）		✔	✔
クラウドインフラストラクチャのセキュリティ （クラウドセキュリティポスチャを監視して、セキュリティおよびコンプライアンスのリスクを防止）	✔	✔	✔
XDR (Extended detection and response)		✔	✔
MTR (Managed threat response – 24時間年中無休の脅威ハンティングおよび対応サービス)			✔

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

22-05-24 DS-JA (MP)