OpenText Core Endpoint Detection and Response により MSP のセキュリティを強化

OpenText Core Endpoint Protection を搭載した MSP 専用の
SMB のセキュリティ保護

利点

- 500 を超える MSP テクノロジースタックとのシームレスな統合により、迅速な導入と価値実現までの時間を短縮
- 追加コストなしで SIEM と SOAR を含めることで、ログの取り込み、脅威のトリアージ、検索、コンプライアンスレポーティング、ワークフローを使用した自動脅威対策が可能
- 堅牢で一貫性のあるセキュリティ体制を確保しながら、運用を簡素化

MSP は、クライアントのエンドポイントセキュリティを管理する際に、多くの課題に直面しています。限られたリソース、高度なサイバー脅威、ツールのスプロール、エンドポイントの可視性の制限、圧倒的な量の脅威は、インシデント対応の非効率化と運用リスクの増大につながります。

エンドポイント保護を含む OpenText™ Core Endpoint Detection and Response (EDR) は、感染したエンドポイントで脅威を検知、調査、修正するために、エンドポイントアクティビティの完全な可視性を提供します。これは、MSP がこのような課題に対処することを目的として構築されています。

OpenText Core Endpoint Detection and Response が重要な理由

OpenText Core Endpoint Detection and Response は、エンドポイント保護を含めることで、MSP のサイバーセキュリティを再定義し、階層化された強力なサイバーセキュリティ戦略を作成します。この包括的なソリューションは、スケーラビリティと柔軟性を備えているため、ハードウェア要件や設備投資へのコミットメントは必要ありません。OpenText Core Endpoint Detection and Response は、統合された SIEM と SOAR を含む最先端のプラットフォームにより、自動化を活用してエンドポイントの不審な振る舞いを検知、調査、対応し、感染したエンドポイントを分離して隔離し、組織への財政的および風評的な損失を防止します。

主な機能とユースケース

- **無理のない導入：**EDR と EPP の両方に対応した、軽量で非侵入型の単一エージェントです。既存の OpenText Core Endpoint Protection をご利用中のお客様は、再導入やスクリプト変更なしで OpenText Endpoint Detection and Response にアップグレードできます。
- **統合 PSA：**統合されたプロフェッショナルサービスの自動化により、チケット発行と脆弱性管理を合理化します。
- **強化された EDR：**リアルタイムの脅威検知と対応により、完全なエンドポイント保護を実現します。
- **SIEM および SOAR を追加コストなしで提供：**ワークフローによって、脅威の検知、対応、修正を自動化します。
- **高度な EPP：**プロアクティブな監視とリアルタイムのグローバルな脅威インテリジェンスによるメリットを享受できます。
- **コンプライアンス：**NIST、PCI、SOC 2 などの業界標準に準拠します。

リソース

OpenText Endpoint Protection とビジネス向けウィルス対策ソフトウェア | Webroot ›

包括的な検知および対応プラットフォーム

OpenText Core Endpoint Detection and Response は、影響の少ない単一のエージェントを使用して、脅威の検知、調査、対応をエンドポイント保護と同じプラットフォーム上で結合します。このプラットフォームは既存のツールとシームレスに統合され、堅牢で一貫性のあるセキュリティ体制を確保しながら、運用を簡素化します。脅威はエンドポイント保護をバイパスして、エンドポイントに感染することがあります。EDR ソリューションは、ワークフローを使用して、感染したエンドポイントを自動的に分離し、隔離することができます。

OpenText Endpoint Detection and Response と OpenText Core Endpoint Protection (EPP) の組み合わせが、MSP に価値をもたらす理由は以下のとおりです：

- **包括的な保護の提供：**OpenText EPP は、マルウェアやランサムウェアのような既知および未知の脅威の防止に重点を置き、OpenText EDR は高度な脅威とゼロデイ脅威の検知、調査、対応を行います。
- **脅威の可視性を向上：**この組み合わせによって、エンドポイントアクティビティを包括的に把握できるようになり、監視を改善し、不審な振る舞いの特定が迅速化します。
- **インシデント対応の合理化：**リアルタイムの検知と対応に、キュレーションされた脅威インテリジェンスと OpenText EPP の予防措置を組み合わせることで、インシデントに対する MTTD と MTTR を短縮します。
- **調査と学習の改善：**OpenText EDR はすべてのエンドポイントアクティビティを記録することでインシデントの分析をサポートし、OpenText EPP は学んだ教訓を予防措置の強化に生かすことができます。
- **管理の簡素化：**統合ソリューションは MSP のセキュリティ運用を合理化し、Endpoint Security Management (ESM) のための単一プラットフォームを提供します。
- **コスト効率に優れたセキュリティで収益性を向上：**OpenText の EPP と EDR を活用することで、複数のベンダーソリューションとのコストのかかる複雑な統合を回避することができます。

OpenText Core Endpoint Detection and Response は、既存のインフラストラクチャと統合する単一の検知および対応プラットフォームにエンドポイント保護を含めることで、スケーラブルで柔軟性がある費用対効果の高いエンドポイント保護ソリューションを MSP に提供します。このソリューションは、脅威のトリアージとワークフローを使用した自動応答のための SIEM と SOAR を追加コストなしで導入することで、運用上の負担とインシデント対応時間を削減し、ビジネスに包括的なエンドポイントセキュリティを提供します。OpenText Core Endpoint Protection は、長期的な使用契約や隠れたコストがないため、エンドポイントセキュリティの体制強化を検討している MSP にとって理想的なソリューションです。

詳細の確認やデモの予約については、OpenText アカウント担当者にお問合せいただくか、cybersecurity.opentext.com をご確認ください。

opentext™