OpenText Core EDR

複雑さのないオールインワンのエンドポイントセキュリティ

メリット

- SIEM と SOAR が組み込まれた統合プラットフォーム
- 事前設定されたポリシーによる迅速な導入
- 組み込まれた使いやすさにより、セキュリティ管理を効率化
- 継続的に更新される脅威検知とインテリジェンス

セキュリティチームはアラートに埋もれた状態になっており、高価な SIEM および SOAR アドオンを必要とする断片化されたエンドポイント検知および対応 (EDR) ツールをなんとか使いこなしています。その結果、システムが多くなりすぎ、複雑化しすぎて、十分に効果的な検知が行われなくなっています。

このような環境において効果を表すのが、OpenText™ Core EDR です。この製品はシンプルさとスピードを重視して設計されており、従来の EDR プラットフォームのような複雑さを排除して、一元化された効果的な脅威検知および対応を実現します。組み込みの SIEM および SOAR 機能がプラットフォームの一部として含まれているため、完全に機能させるだけのために高価なアドオンをつなぎ合わせる必要はありません。

統合プラットフォームによる完全な保護 (Day 1)

OpenText Core EDR は、エンドポイント保護、検知、対応、SIEM、SOAR、脆弱性評価などのすべてを、単一の統合プラットフォームで提供します。事前に構築されたポリシーと設定が担当者の運用の取り組みをサポートする一方、管理の一元化と自動化により、セキュリティチームが通常直面する手作業によるオーバーヘッドが削減されます。

つながりのない複数のツールをなんとか使いこなすのではなく、1 つのコントロールセットで、重要なエンドポイント保護とフルスペクトラム脅威検知を 1 か所から管理できます。つまり、導入の迅速化、ワークフローの効率化、環境全体での一貫した保護を、Day 1 から実現できます。

効率性を重視した設計

直感的なインターフェイス、事前設定されたポリシー、自動化されたワークフローを備えた OpenText Core EDR は、迅速な導入と日常業務の簡素化を実現するために構築されています。チームの規模に関係なく、手作業によるオーバーヘッドを削減し、セキュリティの成果を迅速に得ることができます。

グローバルなインテリジェンスに裏打ちされた実証済みの脅威検知

OpenText Core EDR は、脅威に先んじるために継続的に進化しています。検知のロジックは、一元化された検知エンジニアリング、実際のパートナーからのフィードバック、および OpenText のグローバル脅威インテリジェンスチームを通じて更新されます。

業界の調査によると、現在、サイバー保険プロバイダーの 65% が EDR ソリューションの導入を組織に求めています [1]。

1. Cyber Insurance Industry Statistics 2025: Growth, Trends, and Data

機能	目的
軽量エージェント	パフォーマンスへの影響を最小限に抑えた、非侵入型の迅速な導入。
事前設定されたポリシー	即座に脅威の検知を開始できる、すぐに使用可能な保護の提供。
継続モニタリング	エンドポイントのアクティビティをリアルタイムで可視化し、脅威を早期に特定して阻止。
隔離と封じ込め	感染したデバイスを分離し、疑わしいファイルを隔離し、悪意のあるファイルに関連するプロセスを終了させる。
SOAR による自動対応	組み込みのプレイブックと対応アクションにより、脅威を封じ込め、滞留時間を短縮。
統合された SIEM	エンドポイント、ID、ネットワークイベントを関連付けて、環境全体にわたって脅威を明確化。
脅威ハンティング	過去のエンドポイントイベントデータを Lucene ベースのログクエリを使用して検索し、統合された脅威インテリジェンスとともに検証することが可能。
脆弱性評価	CVE や CIS のガイドラインなどの標準に基づいて脆弱性を検出することで、パッチ未適用のソフトウェアやさらされた状態のままのエンドポイントから生じるリスクを特定。
コンプライアンスのサポート	脅威検知、インシデント対応、ロギング、エンドポイントレベルでのリスク緩和を有効にすることで、NIS2、NIST 800-53/171、CIS コントロール、HIPAA、PCI-DSS、ISO 27001 への準拠をサポート。
サードパーティの統合	syslog およびカスタム API の広範な統合セットを提供。
一元管理	単一のクラウドネイティブのコンソールから、オンプレミス、リモート、クラウドのすべてのエンドポイントを管理。
レポーティング	エージェントのステータス、指標、サインインログ、IOC、脆弱性、ポリシーの変更など、DOCX 追跡型の詳細なレポートを提供。
広範なシステムサポート	Windows、Linux、macOS、iOS、Android、および主要なサーバー環境にまたがる包括的なカバレッジ：デバイスや OS に関係なく、一貫したエンドポイントの保護と検知を保証

次の製品も利用可能：OpenText Core MDR

24 時間 365 日対応でエキスパートによる環境の監視が必要ですか？ OpenText™ Core MDR では、ランサムウェア、マルウェア、フィッシングなどの脅威を検出して封じ込めるため、継続的なモニタリングとエキスパートのサポートが提供されます。そのため、チームは独力で対応を行う必要がなくなります。

OpenText Core EDR の詳細はこちら ›

OpenText Core Endpoint Protection の詳細はこちら ›

OpenText Core MDR の詳細はこちら ›

実際のユースケースの概要

ランサムウェアの動きを阻止

OpenText Core EDR には、迅速に対応するためのツールが用意されています。プレイブックを使用すると、感染したデバイスの隔離、悪意のあるファイルに関連するプロセスの強制終了、エンドポイントの分離などの封じ込めのアクションが可能になり、被害を抑え、拡散の前にリテラルムーブメントを阻止することができます。

コンプライアンスと監査対応を強化

OpenText Core EDR では、NIS2、NIST 800-53/171、HIPAA、PCI-DSS、ISO 27001 などのコンプライアンスフレームワークがサポートされており、組織が厳しい規制要件を満たすのに役立ちます。ロギング、インシデント対応、エンドポイントレベルでのリスク緩和が組み込まれており、セキュリティチームは監査を簡素化し、継続的なコンプライアンスを実証し、規制上のエクスポージャーを減らすことができます。

エンドポイントのセキュリティ運用を簡素化

断片化されたツールやつながりのない複数のワークフローを、エンドポイント保護、検知、対応、SIEM、SOAR、脆弱性評価をまとめて提供する統合プラットフォームと取り替えてください。すべてを 1 か所で管理できるため、チームはより効率的に運用を行い、自信を持って対応することができます。

opentext™