OpenText Core Endpoint Protection

有効性の高いリアルタイム保護によりあらゆる場所のユーザーを保護

利点

- 完全にリモートでエンドポイントを管理および制御
- 高度に自動化された低コスト運用
- 容易な導入
- ゼロデイ脅威に対する優れた効果
- マネージドサービスプロバイダーおよび中小企業向けに構築されたソリューション

あらゆる規模のビジネスが絶えず攻撃を受けています。攻撃の種類、量、速度が多様であるため、マルウェア、ランサムウェア、フィッシング、クリプトマイニング、およびユーザーやシステムを標的としたその他の有害な攻撃を阻止することがこれまで以上に重要になっています。

OpenText™ Core Endpoint Protection は、受賞歴のある直感的な管理コンソールを提供することで、これらの問題を解決します。40 を超えるサードパーティの統合、RESTful API、および完全に自動化されたエンドポイント検出、防止、修正により、OpenText は組織のサイバーレジリエンス戦略を補完する包括的エンドポイント保護を提供します。OpenText は、クラウドコンピューティングおよびリアルタイム機械学習の能力を利用して、各システムのエンドポイント防御を継続的に監視し、エンドユーザーまたはシステムが直面する固有の脅威に合わせて調整します。

プロアクティブ、予測型、多層アプローチをセキュリティに取り入れる

OpenText Core Endpoint Protection は、OpenText™ の BrightCloud™ Threat Intelligence プラットフォームを基盤としています。このプラットフォームは、人工知能と機械学習の優れた部分を組み合わせて、ビジネスが急速に変化する脅威状況に対処できるよう支援します。BrightCloud は 140 を超えるネットワーク、セキュリティ、テクノロジーベンダーから信頼されています。

このワールドクラスの脅威インテリジェンスを活用する OpenText のマルチシールド保護に含まれているリアルタイムの振る舞い、コアシステム、Web 脅威、識別情報、フィッシング、回避、およびオフラインシールドは、複雑な攻撃を検出および防止し、それらから保護します。特許取得済み OpenText Evasion Shield テクノロジーは、ファイルベース、ファイルレス、難読化された、または暗号化された回避スクリプト攻撃を検出、ブロック、および修正 (隔離) します。Script Shield を使用して PowerShell、JavaScript、VBScript で悪意のある振る舞いが実行されるのを防止します。

エンドポイントがオフラインの場合でも感染を監視、ジャーナリング、封じ込める

脅威を検出して阻止する機会が 1 つしかない従来のアプローチとは異なり、次世代 OpenText 保護は次の 3 つのステージで機能します。

1. マルウェアがシステムに侵入するのを予測的に防止します。次に、マルウェアおよび未知のファイルが悪意のある振る舞いを示した場合に、それらが実行されるのを防ぐように機能します。
2. OpenText 保護は、以前の未知のファイル (潜在的な感染など) が実行された場合に、ファイルのアクティビティを適切に分類できるまで、それらを監視してジャーナリングします。
3. ファイルが脅威とみなされると、ローカルドライブに加えられた変更は自動的に感染前の状態にロールバックされます。

この複数ステージ戦略は、現代の脅威に対してより効果的であるだけでなく、誤検出の可能性も減少させます。脅威防止はクラウドからリアルタイムで発生するため、更新すべき署名または定義はありません。OpenText エージェントの更新は自動的に実行されます。通常は 3 秒で完了し、ユーザーに完全に透過的に実行されます。

感染の警告と修正は自動的に実行され、コンテンツ、タイミング、および循環に関する定期的なレポートがスケジュールされます。当社のクラウドベース管理コンソールにより、OpenText エージェントがインストールされているデバイスを可視化して制御できます。複数のサイトと場所を管理し、強力なリモートエージェントコマンドを活用できます。当社のクラウド駆動型アプローチの主な利点は、マルウェアを検出して分析するための負荷の高い処理がクラウド内で実行されることです。

直感的で自動化されたサイバーセキュリティでレジリエンスを促進

OpenText ソリューションは、ビジネスのサイバーレジリエンスを維持するのに役立ちます。OpenText ソリューションは、迅速な検出、レスポンス、およびデータリカバリによって脅威の防止、保護をサポートします。また、組織が変化する規制に適応して、それらを準拠するのにも役立ちます。

OpenText Core Endpoint Protection は、最新の攻撃が猛烈な勢いで増加し進化する状況に対して、高度な保護を提供します。エンドポイントセキュリティが自動化されていることで、ビジネスのデジタル適合性を保証するために専任の IT セキュリティリソースまたはエキスパートが不要になります。つまり、感染およびセキュリティ関連インシデントが減少し、修正ケースおよび生産性低下も減少します。

高度なポリシーでセキュリティ担当者をサポート

OpenText は、企業のサイバーセキュリティ体制を大幅に強化するために不可欠なツールを提供します。当社のツールは、実用的なインサイトと柔軟なレスポンスオプションでセキュリティ担当者を保護し、サポートします。以下は、当社の最新の機能です。

- **バイス分離：**脅威が発生した場合、その脅威がネットワーク全体に広がるのを防ぐことが重要です。当社のデバイス分離機能により、影響を受けるデバイスを迅速に分離し、重要な通信を維持しながらマルウェアの進行を停止することができます。この機能は、迅速な脅威封じ込めと調査にとって重要であり、ネットワークの整合性を保護します。
- **プロセスツリーの可視化：**脅威の「方法」と「場所」を理解することは、効果的なサイバーセキュリティにとって非常に重要です。プロセスツリーの可視化により、セキュリティ担当者はシステムに関するフォレンジックレベルのインサイトを得ることができます。この機能を使用して、プロセスの起源と経路を追跡し、潜在的脅威を可視化できます。

セキュリティツールキットに対する軽量かつ強力な機能強化は、サイバー保険の要件を満たすために役立つ重要な要素です。それらは、不必要な複雑さを課したり、運用を遅くしたりすることなく保護するソリューションを提供するという、OpenText の取り組みを示すものです。

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームは、包括的なセキュリティポートフォリオでサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。