DELL Technologies

ソリューション概要

CyberSense® for Dell PowerProtect Cyber Recovery

AI搭載の分析、フォレンジック ツールでサイバー攻撃をよりスマートに検出、診断し、復旧

CyberSenseのメリット

CyberSense®はDell PowerProtect Cyber Recoveryヴォールト ソリューションと完全に統合されています。

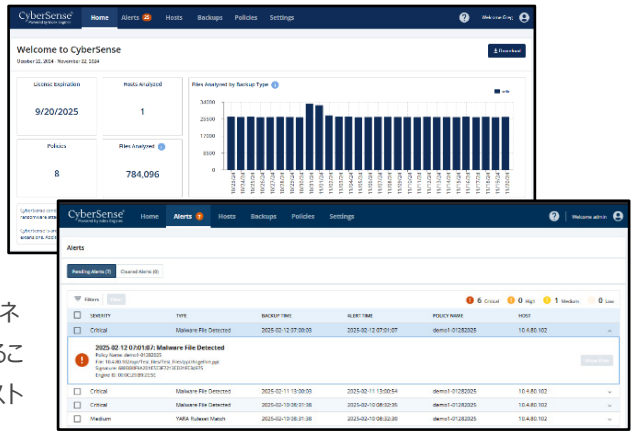
- バックアップ データの定期的なスキャンを自動化して、データの整合性を検証し、不審な振る舞いが検出された場合にアラートを送信します。
- Dell Avamar、NetWorker、Commvault、NetBackup、PowerProtect Data Managerからバックアップ イメージ内のコンテンツを直接スキャンするため、データをリハイドレートする必要はありません。
- データのスキャンごとに詳細なフルコンテンツ分析を行い、高度なランサムウェア攻撃も検出します。
- YARAルールとマルウェア シグネチャーのカスタム アラートにより、ランサムウェアや内部の攻撃者からの既知の動作を検出します。
- 攻撃後のフォレンジック レポートにより、攻撃の深度と範囲に関する詳細なインサイトを獲得し、破損前の最後の正常なバックアップ セットのリストを提供することで、よりスマートで迅速なリカバリーを促進します。

***CyberSense*は、他のデータ分析アプローチとは一線を画しており、バックアップ データの整合性が確保されていて攻撃発生後に迅速に復旧できるというワンランク上の安心感をもたらします。**

サイバー攻撃の頻度が増加し続け、サイバー犯罪者のレジリエンスが高まるにつれて、従来のセキュリティ ツールでは、サイバー攻撃からデータを保護することができなくなっています。

CyberSense®は攻撃後のデータ破損を99.99%の精度で検出*し、インテリジェントかつ迅速なリストアを促進します。世界中の何千もの組織の復旧の第一線として機能するCyberSenseは、コア インフラストラクチャやデータベース、重要なドキュメントなどのデータ資産の整合性を確保し、データに悪意のある破損がないという安心感をもたらします。

CyberSenseは、Cyber Recoveryヴォールト内でのデータのバックアップをスキャンし、データの経年変化を監視します。次に、機械学習とAIを活用して、ランサムウェア攻撃を示す破損の兆候を検出します。データは200以上のコンテンツベースの分析情報と比較され、99.99%の信頼度*で破損を特定するため、ビジネスクリティカルなインフラストラクチャとコンテンツの保護に役立ちます。CyberSenseは、巧妙な攻撃の結果として発生する、コア インフラストラクチャ（Active Directory、DNSなど）やファイル リポジトリー、ファイル システム、重要なデータベースにおける大量の削除や暗号化、その他の疑わしい変更を検出します。



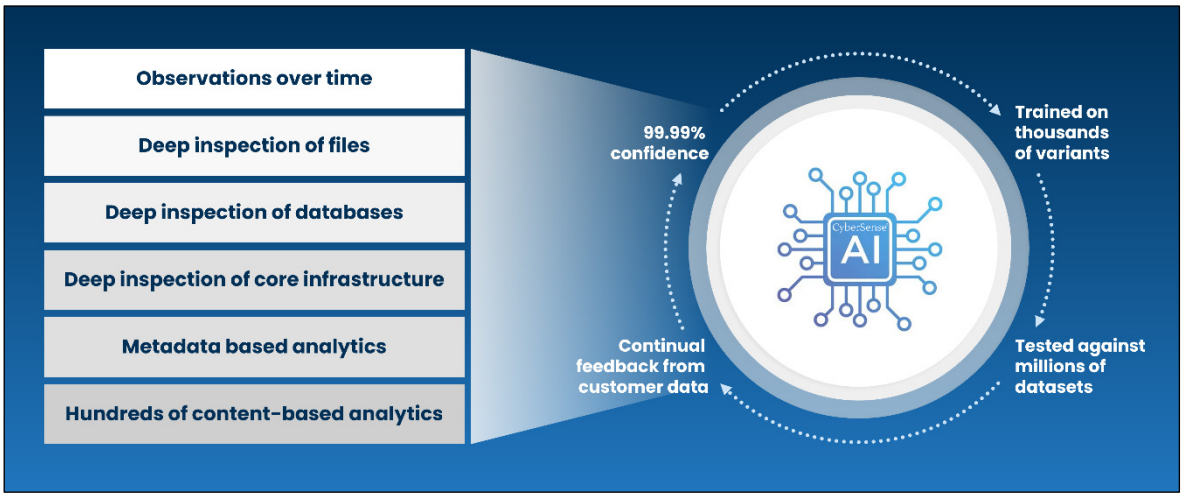
不審な振る舞いが発生すると、CyberSenseは、サイバー攻撃の影響範囲を診断するための攻撃後のフォレンジック レポートを作成します。データの破損が検出されると、破損前の最後の正常なバックアップ データセットのリストが提供されるので、迅速かつ的を絞ったリカバリーを行い、ビジネスの中断とデータ ロスを最小限に抑えることができるため、サイバー リカバリーのコストが抑えられます。

Cyber Recoveryのワークフロー

CyberSenseはDell PowerProtect Cyber Recoveryとシームレスに統合されており、ファイルとデータベースをアクティブにモニタリングして、データの整合性を分析することでランサムウェアによる破損を検出します。データがCyber Recoveryヴォールトに複製され、保存ロックが適用されると、CyberSenseはバックアップ データの包括的なスキャンを自動的に開始し、ファイル、データベース、コア インフラストラクチャのポイントインタイムの観測記録を作成します。CyberSenseはファイルの経時的な変化を綿密に追跡し、巧妙なサイバー脅威によるデータ破損も効果的に発見します。

フル コンテンツ分析

CyberSenseは、すべての保護対象データに対してフルコンテンツのインデックス作成と分析を行う市場で唯一の製品です。CyberSenseの詳細なAI分析はデータ全体にわたって実行され、データの整合性があるか、ランサムウェアによってデータが破損しているかについて99.99%の精度*で確率的な判断が生成されます。CyberSenseが他のソリューションと大きく異なるのはこの点です。一般的なソリューションは、データのハイレベル ビューを取得し、メタデータに基づいて破損の明らかな兆候を探す分析を利用します。メタデータレベルの破損（例：ファイル拡張子が「.encrypted」に変更される、ファイル サイズが大幅に変化している）を検出するのは難しくありません。しかし、このような種類の攻撃は、現代的なサイバー犯罪者による巧妙な攻撃では用いられません。



CyberSenseは、メタデータのみのソリューションにとどまらず、フルコンテンツ分析を使用してデータの破損を検出します。ファイルやデータベースを監査し、ファイルの全体的または部分的な破損など、攻撃を示す変更がないかどうかを確認します。従来の分析では、このような脅威を見逃すことがあり、誤った信頼性につながる恐れがあります。カスタム警告しきい値は、ファイルの変更、追加されたファイル、または削除されたファイルに基づいて設定できます。また、バックアップ中のマルウェアの前方および後方検出のために、カスタムのYARAルールやマルウェア シグネチャーを実装することもできます。

サポートされているデータ タイプ

CyberSenseは、幅広いデータ タイプからの分析を生成できます。例えば、DNSやLDAP、Active Directoryなどのコア インフラストラクチャ、ドキュメントや契約書、知的財産などの非構造化ファイル、OracleやDB2、SQL、PostgreSQL、Epic Cachéなどのデータベースに対応しています。

サマリー

CyberSenseはDell PowerProtect Cyber Recoveryと完全に統合されており、ヴォールト データを分析し、侵害や破損の兆候となる挙動を検出します。CyberSenseを導入すると、発生しているサイバー攻撃の影響範囲をプロアクティブに把握し、迅速な診断と復旧のための計画を円滑に実施できるため、ビジネスの中断とそれに伴う多額の損失を軽減できます。

Dell PowerProtect Cyber Recoveryの詳細はこちら	デル・テクノロジーズのエキスパートに問い合わせる	CyberSenseの詳細はこちら	#PowerProtectで会話に参加

・Index Enginesの委託によるESGのレポート、『Index EnginesのCyberSenseはランサムウェアによる破損の検出で99.99%の有効性を立証』に基づきます。 2024年6月