ソリューション概要

InfiniSafe® Automated Cyber Protection: 脅威の縮小

脅威ウィンドウを縮小してサイバー攻撃を回避または防止することが、これまでになく重要になっています。1つのソリューションですべての脆弱性に対処できるわけではありませんが、企業の重要なデータ資産を保護するために柔軟性の高い機能やオプションのセットを持つことは非常に重要です。**忘れてはいけないのは、問題がサイバー攻撃を「受けるかどうか」ではなく、「いつサイバー攻撃を受けるか」だということです。**

準備

現時点では、ほとんどの組織が採用しているデータ保護の方法は、削除可能なスナップショットを含む従来のバックアップ/リカバリです。改竄防止スナップショットのスケジュール設定を使用して従来の方法を拡張すると、データ保護が段階的に進行します。残念ながら、スケジュールされたイベントでは大きなギャップが生じ、データが脆弱になります。これらのポイント間のタイムギャップは通常、目標復旧ポイント(RPO)によって決まります。RPOは、企業が一定期間内に失ってもかまわないデータ量を示す指標です。改竄防止スナップショットが1日に4回作成される場合、RPOは最大6時間になります。今日では、その時間内に侵害されたデータ量でも、ビジネスが壊滅的な被害を受ける可能性があります。

その結果、起こりうる攻撃からデータを保護するために、より積極的なプロセスが必要になります。セキュリティ監視チームのデータ保護のスピードは、高速化するサイバー攻撃に対応するのに十分とは言えません。InfiniSafe Automated Cyber Protectionは、この課題に対応するソリューションです。多くの企業のセキュリティオペレーションセンターで実施しているリアルタイム監視と計算速度をあらゆるアラートレベルで活用することで、セキュリティチームはInfinidatストレージ環境にすばやく改竄防止スナップショットを自動作成するトリガーを定義し、データ破損、データ削除、データ暗号化などによるダメージのリスクを軽減します。

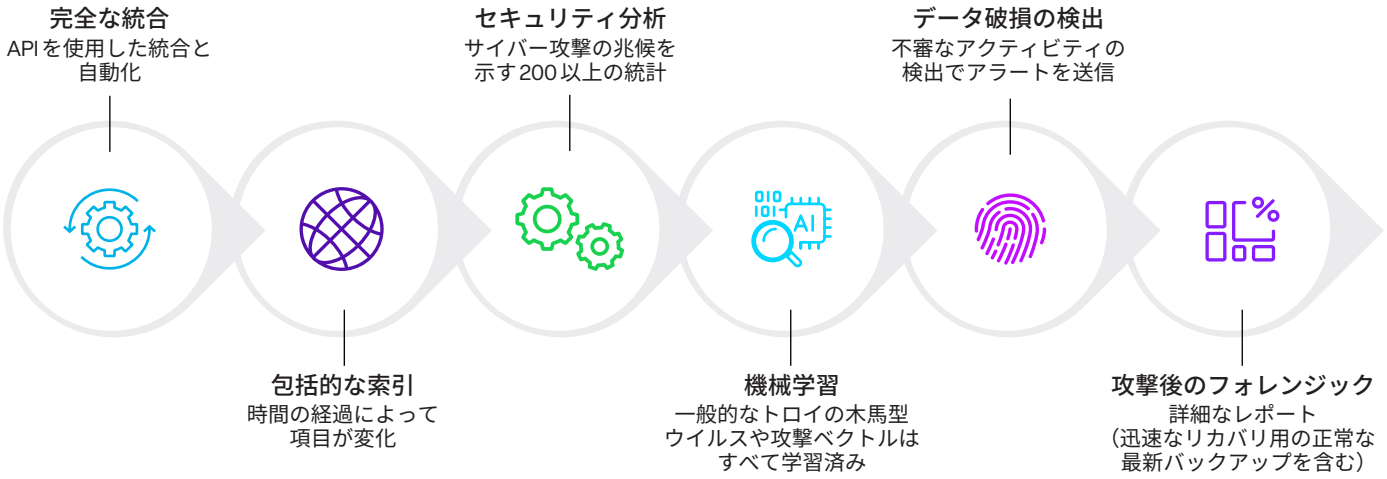
あらゆる攻撃は、情報を取得して優位に立つことを目的としています。データの暗号化やバックアップの破壊、情報の窃取によって攻撃者が優位に立ち、私たちに対して脅迫する手段を持つ可能性が高くなります。

「時は金なり」と言いますが、ことサイバーインシデントに関しては、時間を無駄にすることは莫大な損害につながります。大規模なサイバーイベントが起これば、企業は混乱に陥ります。データ状態の正常性を確認するまでの時間が短ければ短いほど、優位性を多少なりとも取り戻すまでの時間も短くなります。サイバー攻撃に対処しやすくするための仕組みを整えていても、攻撃者は私たちを混乱させ、不意を突いてくることがあります。そのため、それぞれのソリューションを組み合わせて体系的なプロセスを事前に構築しておく必要があります。

特定、オーケストレーション、行動

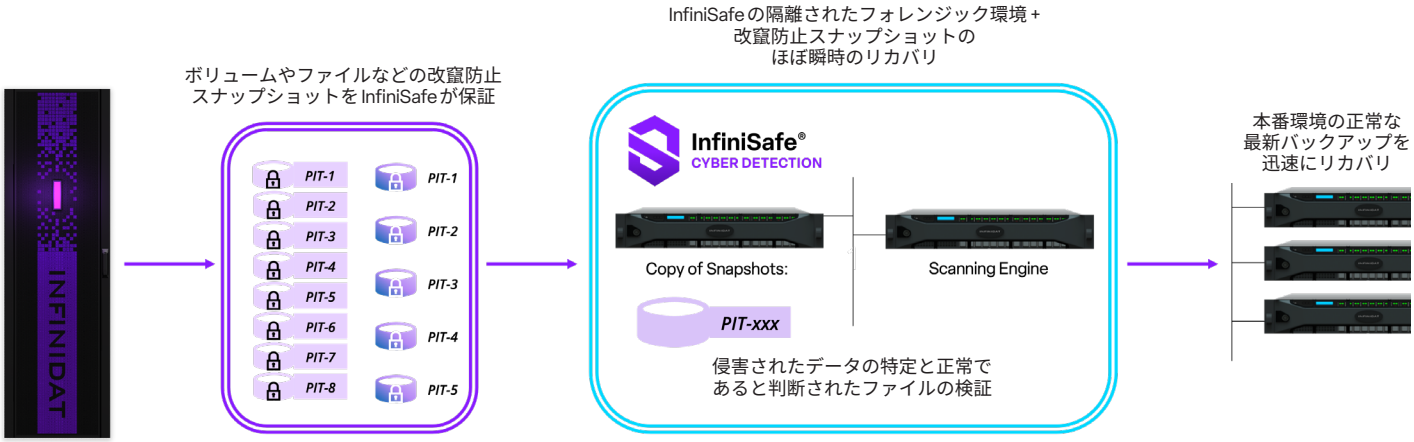
今日の企業の環境は複雑で多層的になっており、多数のツール、監視システム、プロセスで構成されています。多くの場合、その中心には専用のセキュリティオペレーションセンター（SOC）があります。SOC内には、SIEM（Security Information and Event Management）やSOAR（Security Orchestration and Response）と呼ばれた、インフラストラクチャセキュリティ向けに設計された多数のアプリケーションが含まれています。SIEMやSOAR環境は中央管理室として機能し、問題が検出されるとセキュリティに関連するほぼすべての情報を即時に収集します。次のステップは、人間の介入なしに瞬時に実行される、明確な定義で体系的なプロセスを構築することです。データ流出を防ぐには、ほぼ瞬時に実行することが重要で1秒未満のスピードが求められます。

Infinidatはこれらのステップをシンプルな手法で実現します。当社では長年にわたり、自社製品にInfiniSafe機能を搭載してきました。InfiniBoxファミリー向けInfiniSafeの強力なリファレンスアーキテクチャは、場所を問わずあらゆるイベントによってトリガーされるように容易に拡張および調整できます。つまり、企業のSIEM環境やSOAR環境によってもデータ保護機能がトリガーされるよう設定できます。これらのアプリケーション環境には、APIやCLIで拡張可能なインターフェースがあり、明確に定義されたInfiniSafeリファレンスアーキテクチャと結びつくことにより、完全に自動化された一連の機能を実現します。これらの機能をオーケストレーションして、プロアクティブにすばやく改竄防止スナップショットを作成し、最も重要なプライマリデータ資産を保護することができます。



データの検証と迅速なリカバリ

InfiniSafeには、影響を受けかねない内部のユーザーネットワークやシステムから隔離されたプライベートでクリーンなネットワークスペースである、隔離されたフォレンジック環境の作成を調整する機能もあります。必要な関連ツールやソフトウェアを使用してデータのテストや検証を行うために、運用環境とは別に専用のリソースのセットを用意する必要があります。InfiniSafeは、ボリュームやファイルシステムの改竄防止スナップショットを隔離されたフォレンジック環境に即座にアタッチし、利用可能なすべてのツールを使ってデータを検証できます。Infinidatの強力で洞察力に富んだツール群は、検証プロセスにも役立ちます。



InfiniSafe Cyber Detectionは、InfiniSafeの無償コンポーネントへのアドオンソリューションです。InfiniSafe Cyber Detectionは、強力なAIベースのスキャンエンジンにInfiniBoxとInfiniBox™ SSAの改竄防止スナップショットを提供することでブロック、ファイル、データベースストアのディープスキャンを実行します。このスキャンは、データの整合性を検証し、サイバー攻撃の結果発生した悪意のある変更をAIベースの機械学習によって特定するためのものです。さらに重要なのは、200を超えるデータポイントを使用してスキャンすることにより、侵害された可能性のあるデータを99.99%の精度で特定することです。サイバーイベントには迅速かつ正確に対処する必要がありますが、このレベルの精度と詳細さがあれば誤検知の可能性を最小限に抑えることができ、効果的に機能するようより詳細に定義したフォレンジックを追加できるようになります。InfiniSafe Cyber Detectionにこの機能を拡張するには、スキャン用に容量に応じたライセンスを購入する必要があります。

まとめ

準備が不十分だと、悪意ある人物の陽動に乗せられて、最も重要なデータ資産を悪用される可能性があります。スケジュールされたイベントだけに頼るのではなく、プロアクティブにデータを保護してその状態を把握することが、脅威ウィンドウを縮小し、優位性を奪還し、悪意ある人物によるデータの侵害や脅迫を防ぐために重要なポイントです。

jp_sales@infinidat.com

 | © 2026 Infinidat, a Lenovo company

Lenovo
INFINIDAT