INFINIDAT

ソリューション概要

InfiniSafe® Cyber Detection

サイバー攻撃により、企業の被害は年間8兆ドルに及ぶであろうと予想されています。[1]39秒に1回、新しいWeb攻撃が発生しています。[2] 企業が受ける被害として、データの破損や破壊、生産性損失、知的財産の盗難、個人情報や財務データの盗難、横領などがあります。攻撃を受けるとその後のビジネスの混乱や、信用と評判の失墜を招くだけでなく、フォレンジック調査やハッキングされたデータとシステムの検出・復元を行う必要があります。ほとんどのセキュリティおよびITチームは、サイバー攻撃を受けるのは時間の問題だと感じています。対策は万全ですか？

InfiniSafeテクノロジーは、InfiniBox®およびInfiniBox™ SSAプラットフォームによる多層サイバースタックを提供して、ストレージのサイバーレジリエンス環境を構築します。

InfiniSafe Cyber Detectionの登場で、セキュリティおよびITチームは、ランサムウェアやマルウェアの攻撃を最大99.5%の精度で検出することが可能になりました。また、InfiniBoxやInfiniBox SSAプラットフォーム上の、有効かつクリーンなコピーからほぼリアルタイムでデータをリカバリすることができ、Infinidatのサイバーレジリエンスおよび対応能力が向上しました。

InfiniSafe Cyber Detectionは、InfiniSafeのサイバースタックの主要な4層を囲むようにデータ検知の層を追加し、InfiniSafeのサイバーインシデント検知力を深化させます。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してその整合性を検証することで、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、機械学習によって、サイバー攻撃の可能性を示す悪意のある変更を特定します。

攻撃を検知すると、侵害されたデータや侵害の性質を診断するフォレンジックレポートを提供するため、侵害されたデータのソースについて重要なインサイトを得ることができます。InfiniSafeテクノロジーの機能を活用して、有効であることが分かっているデータのコピーを特定できるため、通常業務に復帰できます。

InfiniSafe Cyber Detectionは、メタデータだけでなくファイルやデータのコンテンツも検査する、全コンテンツベースの分析200種類以上を組み合わせて使用します。強力な機械学習アルゴリズムによって、データの破損に使われた攻撃の種類が99.5%の精度で特定され、誤検知が多発しません。これにより、本当に懸念される領域に集中して問題にすばやく対処でき、企業のビジネスクリティカルなインフラとコンテンツの保護に役立ちます。

「組織の**79%**が、**ランサムウェア対策**を、経営陣や取締役会から見た組織全体の**ビジネス上の優先事項**の1つであるとしています」

Enterprise Strategy Group Research Report、「The Long Road Ahead to Ransomware Preparedness」、2022年6月

検知

分析と機会学習による検知

フォレンジック

攻撃の影響を診断し、特定するための
フォレンジックレポート

リカバリ

リカバリを効率化するため、
有効であることが分かっているファイルの
最新バージョンを基にレポート

データの破損が確認された場合、InfiniSafe Cyber Detectionには、攻撃を受けた資産の診断と特定、リカバリにも役立つフォレンジックツールが用意されています。InfiniSafe Cyber Detectionは影響を受けたファイルについてレポートを作成します。セキュリティおよびソフトウェアチームはフォレンジックの結果を調べ、必要に応じて、ツールを使って問題を解決できます。その後、侵害されたデータを、有効であることが分かっている最新のバージョンと置き換えて、最小限のダウンタイムで通常業務に復帰できます。InfiniSafe Cyber Detectionは、中核となるInfiniSafeテクノロジーのアドオンオプションで、サブスクリプション方式でライセンスが提供されます。InfiniSafe Cyber Detectionは、InfiniSafeサイバースタックのデータレジリエンシーに焦点を当て、攻撃後の対策を考えた製品です。総合的なサイバーセキュリティ戦略を構成する、ランサムウェアおよびマルウェア対策のベストプラクティスや、従来のサーバ上で運用する脅威管理製品、アプリケーション、ネットワークなどに代わるものではありません。

検知

InfiniSafe Cyber Detectionでは、保護する全てのデータを対象にした全コンテンツ分析を実行します。この深度で状態を把握することで、データの整合性が保たれていることや、サイバー犯罪者によるデータ分析ツールの回避、痕跡の消去、データの破損がないことに確信が持てるのです。

Infinidatのニューラルキャッシュ（Neural Cache）機械学習と同様に、InfiniSafe Cyber Detectionには強力な決定論的機械学習が組み込まれています。競合製品の20倍以上にもなる、200種類以上の分析と、観察するほどにインテリジェンスが高まるデータ観察を組み合わせています。この機械学習は、誤検出を最小限に抑えるため、異常な行動パターンを発見するだけでなく、ユーザーとランサムウェアのアクティビティを区別できるように、何千ものランサムウェア、マルウェア、トロイの木馬の感染データを基にトレーニングされています。

フォレンジック

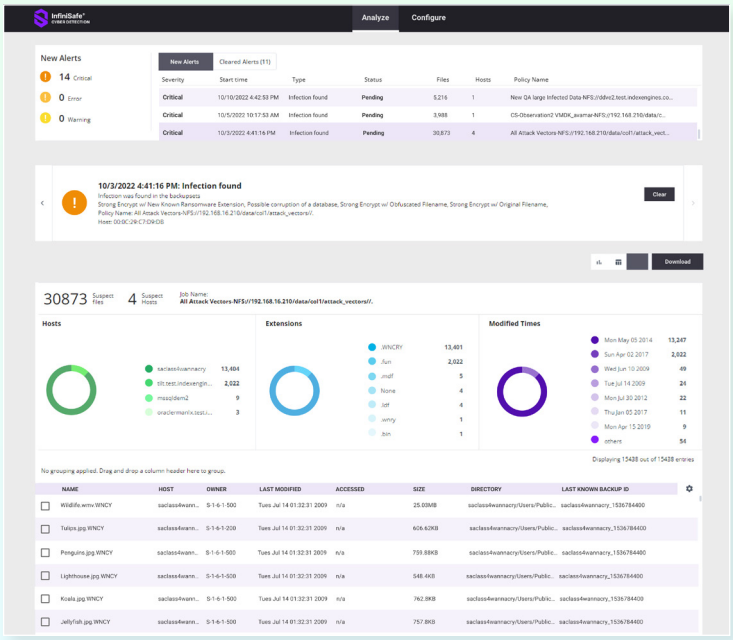
データが破損している場合、InfiniSafe Cyber Detectionは破損しているファイルのリストを生成します。破損しているファイルにはタグが付けられ、攻撃の影響を診断および特定し、スムーズなリカバリに必要な情報を提供するために、フォレンジックレポートが作成されます。

重大度別のアラート

破損の疑いについての追加の詳細情報

攻撃の詳細を掘り下げられる、
カスタマイズ可能な動的チャート

破損したファイルの
ダウンロード可能なリスト

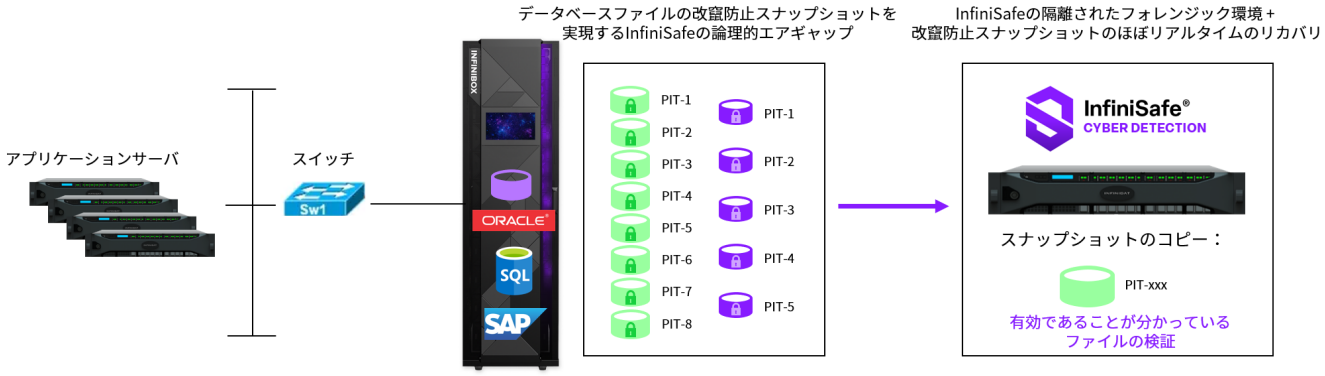


攻撃後ダッシュボード：改善されたユーザーエクスペリエンス、さらに深いデータの理解、直感的な攻撃後ワークフロー。

リカバリ

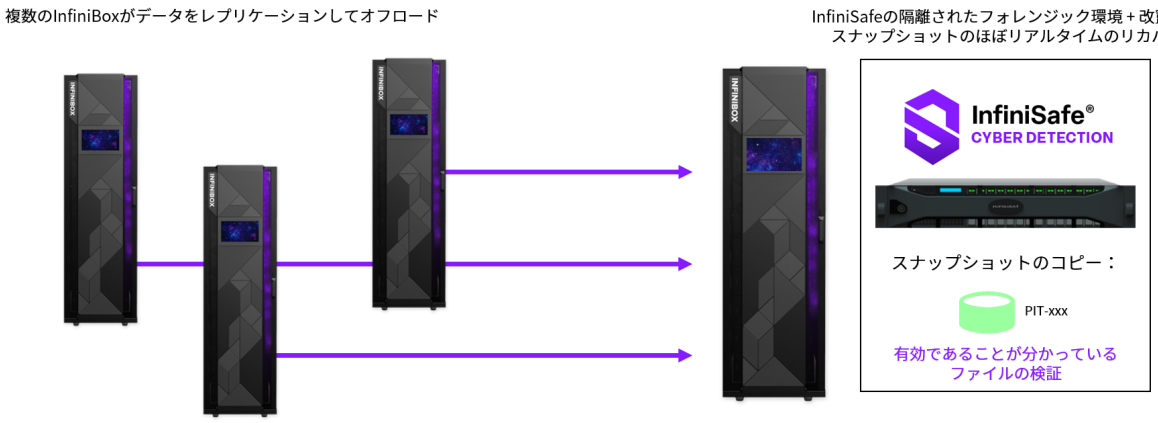
InfiniSafe Cyber Detection は、ファイルまたはバックアップの最新の有効なコピーが InfiniBox または InfiniBox SSA 上にある場合、そのバックアップコピーを基にレポートを作成します。破損したデータのある場所、そのデータの最新の有効なバージョンがある場所、データが含まれるスナップショットまたはバックアップセットを特定し、リカバリプロセスを効率化します。

ユースケース：ブロック、ファイル、データベースのサイバー攻撃の検知



ミッションクリティカルなデータベースアプリケーションに InfiniBox または InfiniBox SSA を使用している場合、InfiniSafe サイバースタックテクノロジーと Cyber Detection を併用すると、頻繁に作成される改竄防止スナップショットを基にそれらのアプリケーションの整合性を検証し、さらに、機械学習によって、サイバー攻撃を示す変更を特定できます。InfiniSafe Cyber Detection は、有効であることが分かっているデータのコピーを基に問題を判定し、レポートを作成して、InfiniSafe によるほぼリアルタイムのリカバリを促します。

Cyber Detection Array



複数の InfiniBox または InfiniBox SSA を使用している企業は、隔離されたフォレンジック環境で、Infinidat のネイティブのレプリケーションツールを使用して、指定した Cyber Detection Array にデータをレプリケーションできます。Cyber Detection Array が、全てのデータファイルをスキャンし、破損しているファイルにタグを付け、フォレンジックレポートを作成します。この構成が、企業にサイバー攻撃を検知するインテリジェンスを提供します。

悪意のあるランサムウェアやマルウェアのインシデントによって、エネルギーパイプラインから学校、病院まで、重要なサービスやビジネスに障害が発生し続けています。ランサムウェアやマルウェアの攻撃による経済的損失の総額も増える一方です。効果的なサイバー攻撃検知戦略を実施することで、企業の被害を緩和し、速やかなリカバリを確実なものにできます。

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

jp_sales@infinidat.com

INFINIDAT

