ソリューション概要

Lenovo
INFINIDAT

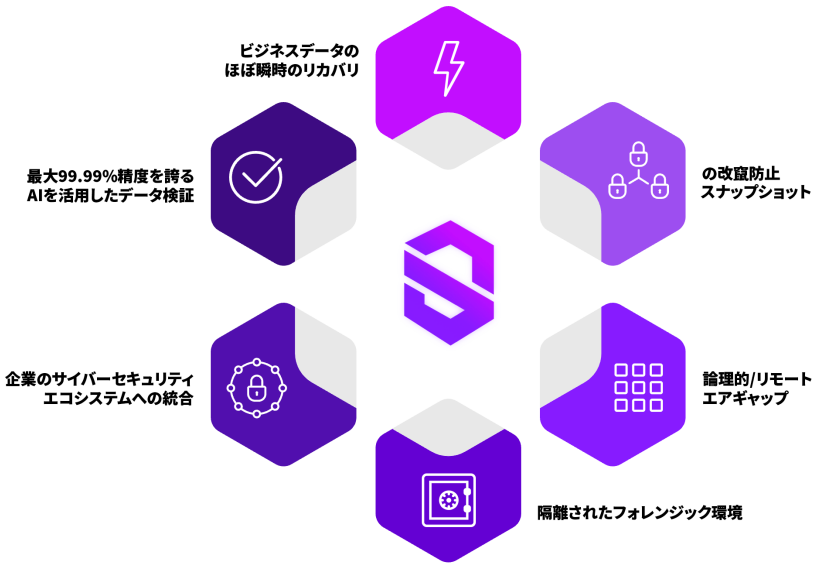
InfiniSafe® Cyber Detection

サイバー攻撃による企業の被害は、年間９兆5,000億米ドルに及ぶであろうと予想されています。[1] 39秒に1回、新たな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？

Infinidatは次世代のデータ保護とリカバリ戦略として、サイバーフォーカス、リカバリファーストを掲げています。InfiniVerse®プラットフォームのサイバーレジリエンスサービスは、InfiniSafeポートフォリオを使用し、広範なサイバーストレージ機能を直接サポートして、エンドツーエンドの完全な保護、防御、検知、確実なリカバリを提供します。セキュアバイデザインのInfiniSafeは、核となるサイバースタックであるInfiniSafe Automated Cyber Protection（ACP）とInfiniSafe Cyber Detectionで構成されています。

InfiniSafe Cyber Detectionにより、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99.99%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の核となるサイバースタックレジリエンスおよび対応能力が向上しました。Infinidatのサイバーセキュリティサービスを活用することで、攻撃者に先んじた対策が可能です。

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、VMwareデータ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。



InfiniSafe ACPは、セキュリティオペレーションに直接統合されます。攻撃を検知すると、自動的に改竄防止スナップショットを実行し、InfiniSafe Cyber Detectionに提示します。InfiniSafe Cyber Detectionではディープスキャンを実行し、侵害されたデータや侵害の性質を診断する広範な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。

調査対象の**ITおよびサイバーセキュリティ専門家の65%**が
組織に対する3大脅威の1つはランサムウェアであると考えています

ESG Report: 2023 Ransomware Preparedness

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

InfiniSafe Cyber Detectionのトレーニングは、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対象として、全コンテンツベースの分析200種類以上を組み合わせて継続的に行われます。機械学習アルゴリズムが強力であるため、従業員は次々と生まれる新種の攻撃を逐一把握する必要はありません。きめ細やかなスキャンで、既知と未知の攻撃、部分暗号化を特定します。疑わしいアクティビティの有無を常に把握でき、既知の攻撃では破損に使われた攻撃の種類が特定され、未知の攻撃ではどのような攻撃を受けたかなどを、99.99%の精度で特定できます。誤検知が多発することはなく、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。このように広範な自動化とオーケストレーション、InfiniSafe ACPとのセキュリティ統合に加え、さらに広範なエンドツーエンドのソリューションでストレージのサイバーレジリエンスを確立できます。

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。

InfiniBoxプラットフォーム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

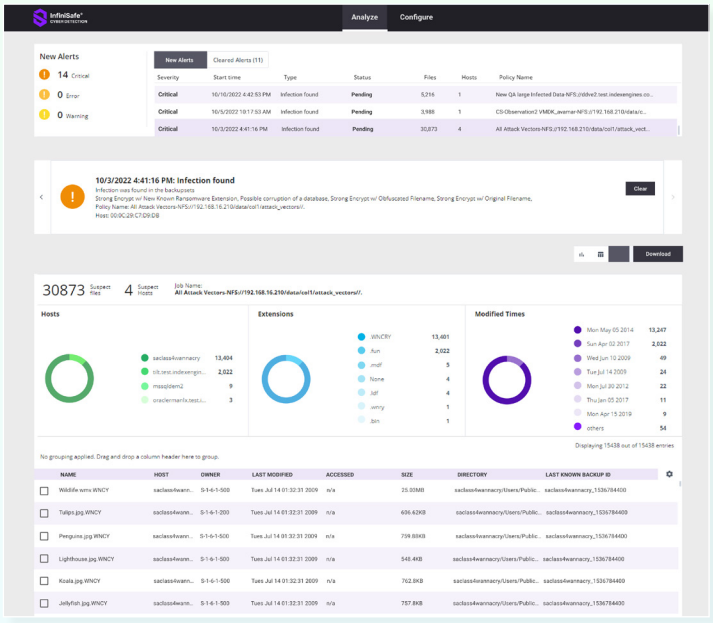
データが破損している場合、InfiniSafe Cyber Detectionは破損しているファイルのリストを生成します。破損しているファイルにはタグが付けられ、攻撃の影響を診断および特定し、スムーズなリカバリに必要な情報を提供するために、フォレンジックレポートが作成されます。

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

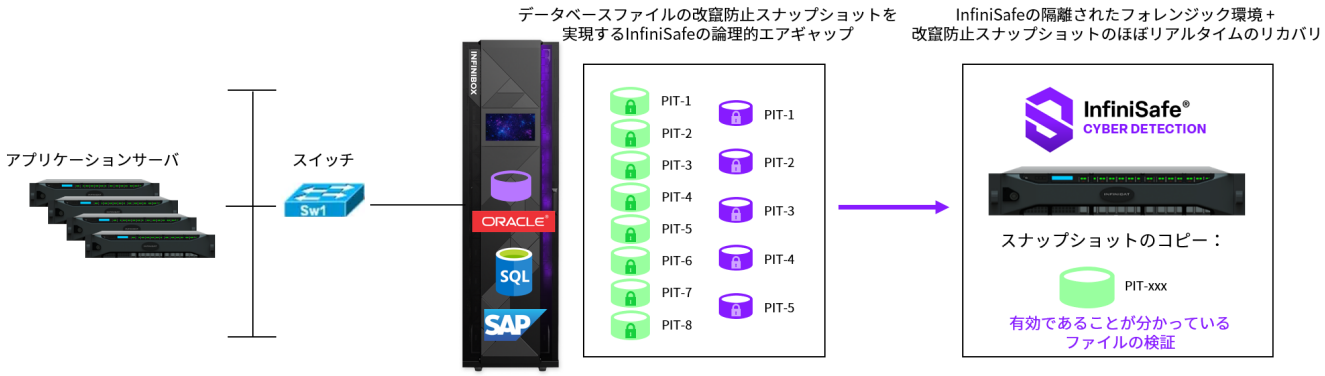


攻撃後ダッシュボード：改善されたユーザーエクスペリエンス、さらに深いデータの理解、直感的な攻撃後ワークフロー。

リカバリ

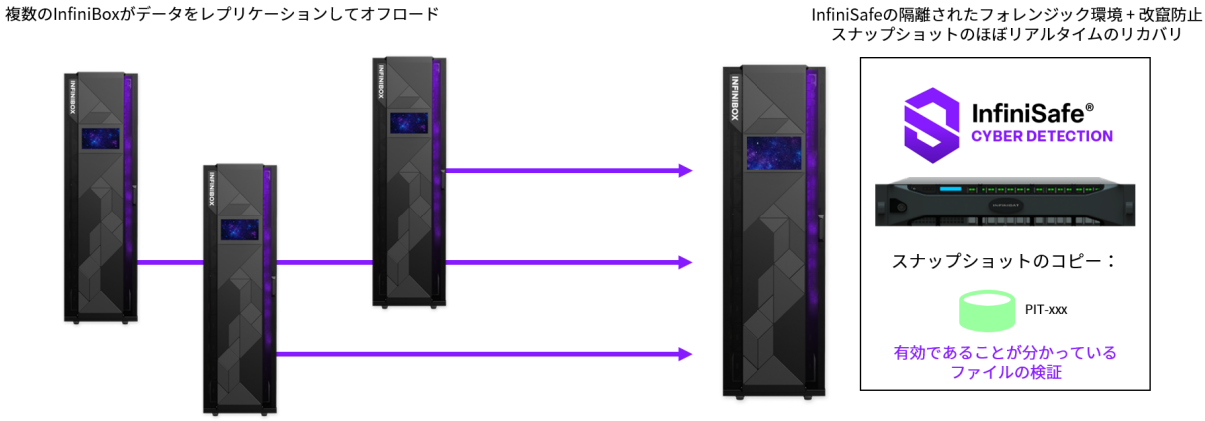
InfiniSafe Cyber Detectionは、ファイルまたはバックアップの最新の有効なコピーがInfiniBoxまたはInfiniBox SSA上にある場合、そのバックアップコピーを基にレポートを作成します。破損したデータのある場所、そのデータの最新の有効なバージョンがある場所、データが含まれるスナップショットまたはバックアップセットを特定し、リカバリプロセスを効率化します。

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。効果的な次世代のデータ保護とリカバリ戦略を実施して、企業の被害を緩和し、速やかなリカバリを確実なものにしましょう。

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

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

jp_sales@infinidat.com

 | © 2026 Infinidat, a Lenovo company

Lenovo
INFINIDAT