VERITAS

クラウドデータの異常の検出

クラウドデータとユーザーアクティビティを監視するための強力なツール

異常検出とは、クラウドデータやユーザーアクティビティの通常とは異なるアクティビティや、不自然な動作を追跡して警告する強力な早期警告システムです。本来は、問題を事前に把握するためのものです。異常はセキュリティ違反、ハードウェアやソフトウェアの問題、お客様の需要の変化など、早急な対応が必要となる多くの課題の指標となり得るため、このような異常を検出することが、データセキュリティにとって重要な作業となっています。異常検出は、データセット内の異常なポイントやパターンを特定するプロセスを使用することによって機能します。事前定義の許容範囲内に確立された基準から逸脱するものは、すべて異常とみなされます。確立された一連のパラメータとインテリジェントな指標により、早急な対応が必要な異常についてアラートがお客様に送信され、アクティビティ監視によってリアルタイムに更新されるダッシュボードを簡単に表示できます。異常の例としては、侵入を示している可能性のある異常なファイル書き込み動作 (ただし既知のランサムウェアファイル拡張子を検出している可能性もあります)、ファイルアクセスパターン、トラフィックパス、さらには通常のパターンと比較して異常なアクティビティのジャンプなどがあります。通常とは異なる動作が直ちに通知されることは重要なアドバンテージであり、これによって対応や緩和策を迅速に実行できます。問題が発生した場合に適切に対応したり、リスクを軽減してそれを迅速に隔離し、破壊的事態、ダウンタイム、または侵害に関するその他の問題を防止したりできることには大きな価値があります。

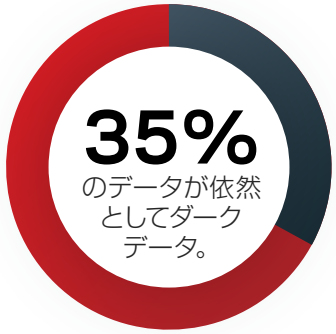
データ監視塔の力

クラウドデータが爆発的に増加し、無秩序に広がる中、特にサイバー脅威やランサムウェアに対抗するために、すべてのクラウドデータの監視塔として機能する異常検出の必要性が高まっています。サイバー犯罪者はさまざまな工夫を凝らしてシステムやデータにアクセスしています。システムに侵入し、暗号化を開始し、できるだけ多くをダウンロードし、あとは検出される前に逃げるだけです。このような場合は、異常検出が問題についての警告と対策に役立ちます。

2022 年、クラウドはサイバー犯罪者にとって最大の攻撃経路であり[1]、サイバー犯罪者は組織化された犯罪プレイブックの手法を採用し、長期的な戦略を多数実行しています。サイバー犯罪者はサイバー偵察の技術を完成させてしまいました。この手法は休眠状態のランサムウェアやスリーパーランサムウェアとも呼ばれ、デジタルの世界では今や当たり前のものになっています。つまり、犯罪者は一度アクセスしたら戦略的に身を潜め、表に出てこないということです。その理由は、サイバー犯罪者の最優先事項がクラウド環境を観察し、学習し、動き回ることで弱点を見つけ、脆弱性を悪用しようとすることだからです。彼らはその間、常に攻撃に最適なタイミングを計っています。このような状況において、サイバー犯罪者が行動を起こす前に問題を検出できれば、問題を事前に把握し、壊滅的な影響を防ぐための対策に最適な機会が得られます。

攻撃者は大金を稼ぎ、その労力の効率を最大限高めるためにできるだけ多く破壊しようとしています。あらゆるビジネスと同様に、重要なのは ROI です。ランサムウェアは最長で 18 カ月間休眠するという報告もあります。攻撃者は、最適な破壊がタイミングや範囲など複数の要因に左右されることを知っており、その標的を、身代金を支払う以外の選択肢がない状況に追い込もうとします。侵害と攻撃が同時に起こるというのは、すでに昔の話です。このような複雑さが増している背景として、システムについて、その所有者より攻撃者のほうが詳しく理解していることが多いことが挙げられます。そのため、重要なシステムを混乱させ、動作を停止するよう設計された一連のイベントが攻撃者によって開始され、より大きな身代金が奪われる可能性が急激に高まっています。

クラウド間のデータの可視化



企業が異常検出の実装を成功させるには、まず一歩引いて、自社のすべてのデータがどこにあるのかを把握し、環境内にダークデータが潜んでいないことを確認することが重要です。脆弱性との時間差に関するベリタスの調査[2]によれば、35% という驚異的な割合のデータが依然としてダークデータです。自社がどのようなデータを所有しており、それがどこに保存されているのかを把握するよう、すぐに作業に取りかかることをお勧めします。

ベリタスのソリューションなら、クラウドプロバイダ、物理環境、仮想環境のすべてにおいて、あらゆるデータを包括的に把握できます。また、ストレージ、コンピューティング能力、主要なすべてのデータ保護ソリューション、クロスレポーティングを確認できるため、システムが見落とされることもありません。これは、サイバー犯罪者がすべてのアプリケーションやデータの正確なインベントリが企業で保持されていないこと、あるいはデータのセキュリティや監視が制限されている領域があることを想定しているため、今日の脅威の状況においては特に重要です。

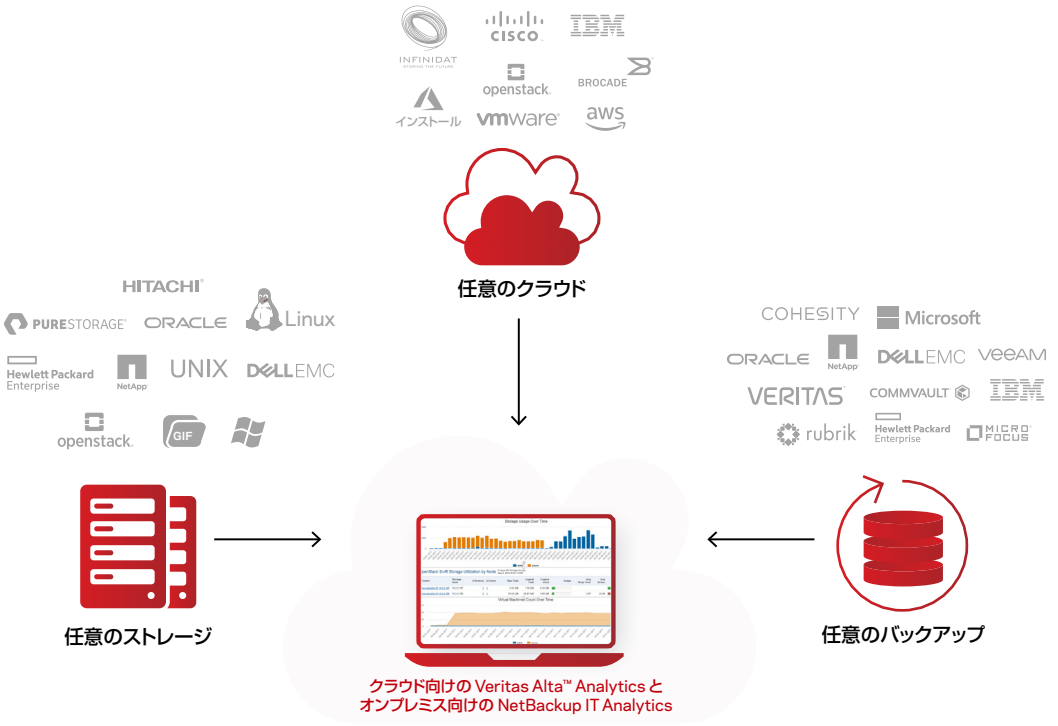


図 1: データの保存場所に関係なく、すべてのデータをまたいで統合された IT インフラ

ベリタスのソリューションは、環境のダークな領域に光を当てるだけでなく、オンプレミス、クラウド、データ保護、ストレージ全体で包括的なインサイト、アラート機能およびレポート機能を提供します。バックアップ環境を可視化するレポートオプションにより、サイバー攻撃に直面した場合でも、情報に基づく意思決定を実行するためのインサイトを得ることができます。これにより、企業は以下のことが可能になります。

- インフラ内のすべてのホストまたは仮想マシン (VM) を検出し、それらをクラウド向けの Veritas Alta™ Data Protection およびオンプレミス向けの NetBackup で保護された VM と比較する
- バックアップで欠落しているホスト、または最新のバックアップがないホストに潜在的なリスクとしてフラグを立てる
- ランサムウェアの影響を受ける可能性のあるファイルを、そのサイズと環境内における場所と共に検出する
- 発生したリスクの履歴を表示するインタラクティブなグラフにアクセスする

AI を活用したクラウド間の異常検出

データを可視化できたら、次のステップは AI を活用した異常検出を実装することです。クラウド向けの Veritas Alta™ Data Protection とオンプレミス向けの NetBackup なら、環境全体で異常なデータとユーザーアクティビティを検出し、疑わしい異常をほぼリアルタイムで警告できます。このテクノロジは膨大な量のデータをマイニングし、監視とレポートを自動化し、環境内で何が起こっているかについて実用的なインサイトを提供するように設計されています。

異常検出をイメージするのなら、うそ発見器を想像してみてください。うそ発見器による検査では、まず検査官が、一連の質問によってプレスクリーニングを行い、正常の基準を構成するパラメータを確立します。嘘をつくと、**血圧、脈拍、呼吸、皮膚電気伝導度**などの生理的な指標は、予想通り、確立した正常のパラメータから外れて変動します。同様に、クラウド向けの Veritas Alta™ Data Protection とオンプレミス向けの NetBackup は、AI を活用した異常検出エンジンを利用してパラメータを計算します。このパラメータが、長期にわたるバックアップジョブのメタデータパターンに基づいて正常を構成し、カスタムのバックアップポリシーに合わせて自動的にこれを調整します。

確立した正常値から外れて発生したイベントはキャプチャされ、ほぼリアルタイムに通知されます。観測された異常には、クラスタからの観測距離をベースに算出された重大度に基づいてスコアが割り当てられます。距離が遠いほどスコアは大きくなります。これは、管理者がどのインサイトが実用的かを特定し、誤検知を減らせるように設計されています。

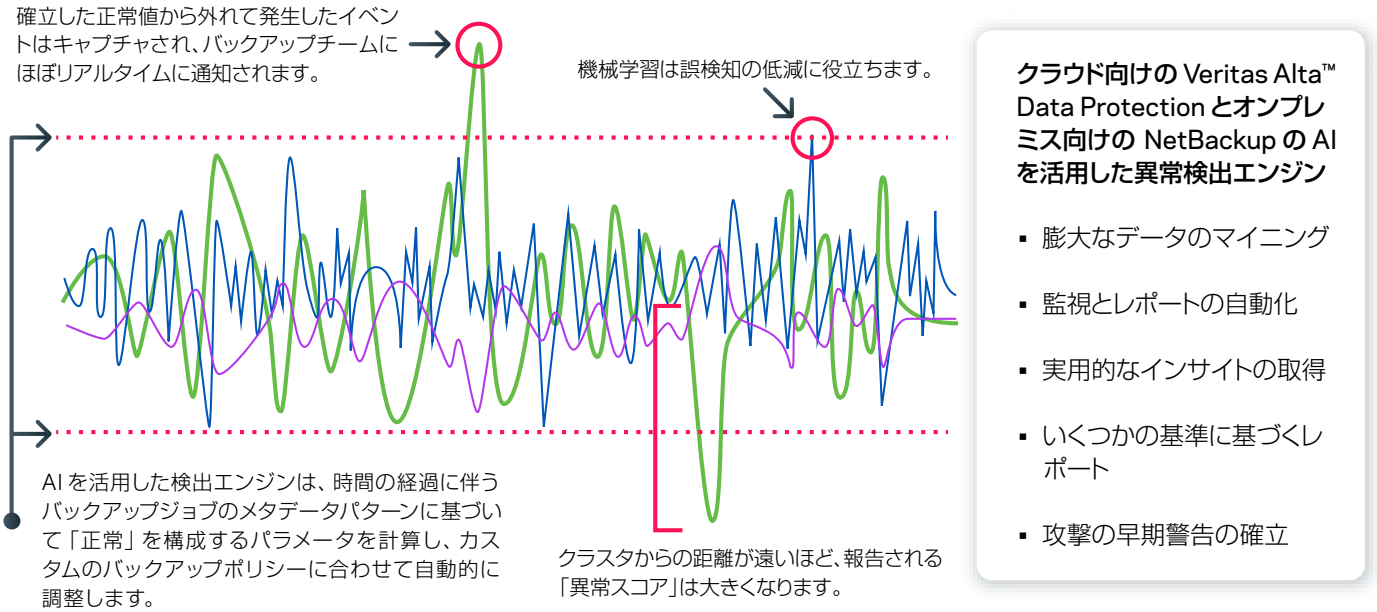


図 2: 異常検出を理解する

全体として、AI を活用した異常検出エンジンは、膨大なデータのマイニング、監視とレポートの自動化、実用的なインサイトの取得、いくつかの基準に基づくレポート、そしてさらに重要なこととして、攻撃の早期警告の確立に役立ちます。管理者は、すべてのデバイスを監視し、攻撃の早期警告を確立することで、いつでもデータを確認し、異常に関する推奨事項を提供して、問題が発生した場合にはすぐに対処できます。たとえば、ベリタスの AI を活用した異常検出なら、プライマリサーバーにシームレスに統合され、クラスタに分類されないものを異常または外れ値とみなして、異常な形式の観測値を検出できます。この機能では、管理者は異常を確認し、それを掘り下げることで懸念事項を特定できます。これによって大量のデータをマイニングし、ランサムウェアイベントに対処するための実用的なインテリジェンスと共に、管理者が注意すべき環境内の単純な変化を提供することができます。これらのソリューションは、攻撃が進行中、または始まろうとしている可能性があることを示すインジケーターを認識するのに役立ち、すぐに対処して影響を抑えることができます。

また、このツールは、新しいバックアップをバックアップの履歴と比較して、ジョブの所要時間の大幅な変化、イメージサイズの変化、ポリシー構成の変化などの異常を識別することで、潜在的な誤検知を特定する機能を備えたインテリジェントなものです。AI エンジンは、ファイルがブロックディスクにあるかクラウド内のオブジェクトストレージにあるかに関係なく、そのファイルやファイルのグループを監視し、ファイル特性がいつ (メタデータレベルまで) 変化するかを理解します。すべてのシステムをスキャンして監視でき、非依存型で、サードパーティのバックアップ製品を含むすべてのクラウドプラットフォームをカバーできるのはベリタスだけです。ベリタスの人工知能/機械学習 (AI/ML) エンジンは、あらゆるサーバー上で実行できます。これほど幅広い機能を備えているからこそ、盲点を確実になくすことができるのです。

マルウェアスキャン

ベリタスは、自動スキャンやオンデマンドスキャンによって、暗号化や転送など、複数の種類のマルウェアを検出できます。自動マルウェアスキャン機能は、人による操作をなくし、AI/ML テクノロジを活用したマルウェアのスキャンを可能にします。AI/ML マルウェアスキャンは、異常スコアが高い場合に自動的に実行されます。スキャンには、非構造化データ、Windows、Linux、VMware が含まれます。マルウェアは、非構造化データが大量に存在するホームディレクトリ内の環境に侵入することが多いため、これらが含まれていることが非常に重要です。

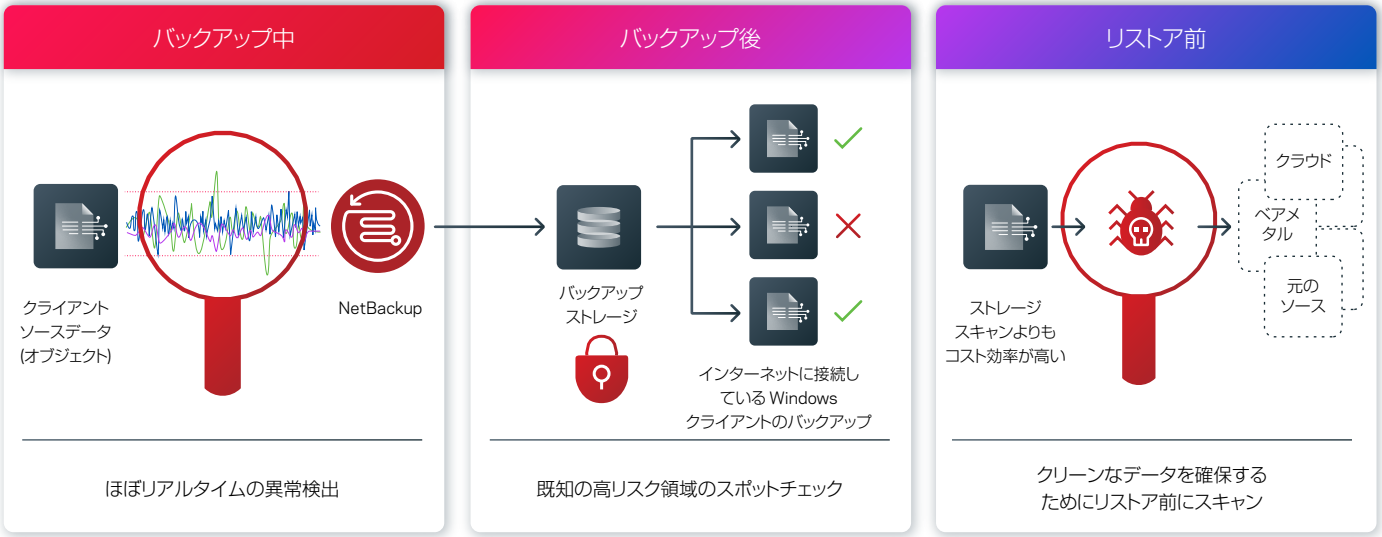


図 3: マルウェアスキャンの概要

また、リカバリが必要な場合には、バックアップデータをスキャンして、最新のマルウェアシグネチャが利用されていることを確認できます。また、明快なビジュアルと警告プロンプトによって、感染したバックアップを認識し、リストアされたすべてのデータがクリーンで影響を受けていないことを確認できます。この手法は、しばしば、最新の正常なコピーへのリストアと呼ばれます。

ベリタスのセキュリティによる設計

ベリタスは、クラウド向けの Veritas Alta™ Analytics とオンプレミス向けの NetBackup IT Analytics を通じて、この統合されたデータの可視化、異常検出、マルウェアスキャンのすべてを実現します。以下は、ダッシュボードのサンプルです。

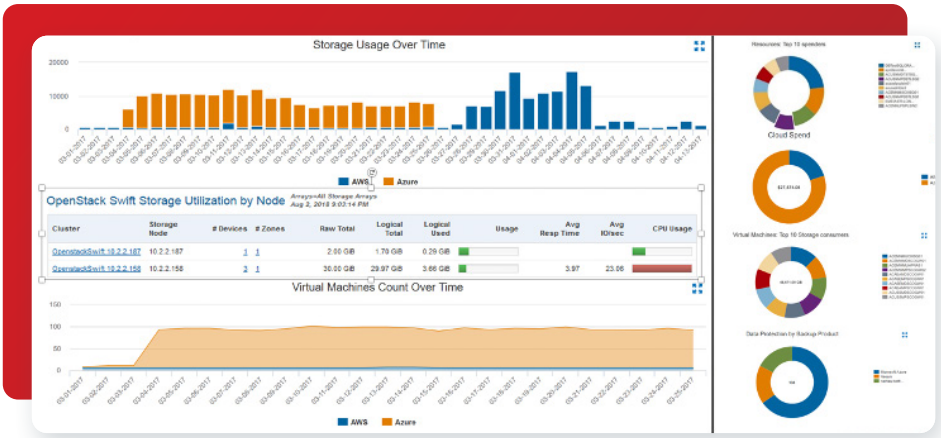


図 4.時間経過に伴うストレージ使用状況を示した NetBackup IT Analytics ダッシュボードのサンプル。

Veritas Analytics の特徴:

- **総合的**—クラウド向けの Veritas Alta™ Analytics とオンプレミス向けの NetBackup IT Analytics は、統合コンソールからデータ資産を特定できる単一ソリューションとして、今日の企業で使用されるあらゆる一般的なサーバー、ストレージ、ハイパーバイザ、データベース、アプリケーションプラットフォームをサポートします。
- **拡張性**—一元管理により、アプリケーション、クラウド、データ保護、ホスト、ネットワーク、ストレージ、仮想化、非構造化データなど、オンプレミスおよびクラウド環境のあらゆる側面から約 30,000 の独自のデータポイントを収集するエージェントレスのデータコレクタを提供します。
- **革新的**—自律設計のための 5 つの特許とクラウドからの更新による独自のアルゴリズムにより、データポイントを分析し、パフォーマンス、耐障害性、使用率を改善する推奨事項を作成します。分析は機械が主導しますが、人間のポリシーによって管理されます。データによって実用的なソリューションが提供され、効率測定を改善し、リスクを最小限に抑え、障害を予測し、監査とコンプライアンスを合理化するために役立てられます。
- **実証済み**—10 年以上にわたり、NetBackup IT Analytics (現在はクラウド向けの Veritas Alta™ Analytics を含む) は、お客様に認められた拡張性と信頼性によって業界をリードし、組織全体のデータをまとめて分析してきました。

Veritas Analytics の主な機能:

- **以下に関するインサイトを提供する統合コンソール。**
  - ローカルおよびクラウドのバックアップ、コンピューティング、ストレージ
  - クラウドとオンプレミスの容量、コスト、使用状況
- **チャージバック**:
  - アプリケーション、部門、コストセンターなどのユーザー定義グループごと
  - バックアップおよびクラウド、コンピューティング、ストレージ全体の使用状況
- **キャパシティ計画**:
  - クラウドのコストと使用率に基づく予算
  - 消費量に基づくメディア/ストレージ計画

クラウド向けの Veritas Alta™ Analytics とオンプレミス向けの NetBackup IT Analytics でクラウドビジネスの価値を最大化する

ベリタスでは、企業がクラウドへと移行している理由にはいくつかあることを確認しています。小規模企業には、データセンターやディザスタリカバリサイトのメンテナンスにかかる負担を削減できるというメリットがあります。中規模企業では、拡張性に優れたハードウェア上に構築されたアクセス可能なオフサイトデータストレージにより、ジャストインタイムのクラウドリカバリを活用しています。大企業は、クラウドの可用性とコストを活用できるワークロードを特定しながら、ミッションクリティカルなワークロードのために高価なデータセンターのスペースを解放しています。企業では、ワークロード用に一時的なスペースが必要になることがあります。データセンターで新しいディスクラックを設置する代わりに、クラウドプロバイダのスペースを活用すれば、データセンターのハードウェア購入にかかる追加コストを回避できます。クラウドのサブスクリプションモデルはこのようなプロジェクトに適しており、拡張性のあるシンプルで使いやすいモデルを提供しています。

データをクラウドに移行するという現在の大きなトレンドは、企業のコスト削減を中心に展開しています。クラウドモデルでは、ハードウェアおよびそれに付随するラックやスタックを調達するのに比べて、すばやく簡単にサーバーにディスクを追加でき、要件に関して俊敏に対応できます。また、クラウドを利用することで、データセンターのハードウェアやソフトウェアを置き換えたりアップグレードしたりするためのコストと時間も回避できます。代わりに、これらの要件はクラウドサービスプロバイダによって満たされるため、企業自身には見えません。企業がクラウドへの移行を決断する理由に関係なく、クラウド向けの Veritas Alta™ Analytics とオンプレミス向けの NetBackup IT Analytics なら、オンプレミス環境と比較して、コンプライアンスに準拠したコスト効率の高いエクスペリエンスを確保できます。

ベリタスが提供する AI を活用した監視塔を活用すれば、お客様は拡大するクラウドデータを管理できるようになります。ベリタスを利用すれば、どこに保存されているのかに関係なく、すべてのエンタープライズデータの場所を確実に一元的に把握できます。ペタバイトレベルの容量に対してクラス最高のパフォーマンスを提供しながら簡単に拡張でき、便利なセルフサービス操作によって IT-as-a-Service (サービスとしての IT) への道を切り開くことができます。ベリタスは、完全なデータ可視化テクノロジ、インテリジェントな異常検出、マルウェアスキャンなどのあらゆる機能を分析ソリューションを通じて提供することによって、不確実性を解消しています。

クラウドネイティブなユーティリティや単体製品の先を考え、サイバーセキュリティとデータ保護を最優先とした統合戦略を設計してみましょう。

ベリタスは、クラウドの制御を実現します。

1. https://www.esg-global.com/ransomware
2. https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

ベリタスについて

Veritas Technologies は、マルチクラウドデータ管理のリーダーです。データの保護、リカバリ能力、コンプライアンスを確保するために、Fortune Global 100 の 95% を含む、先進企業 80,000 社以上が、ベリタスのソリューションを導入しています。ベリタスは、ランサムウェアのようなサイバー攻撃がもたらす脅威に対してお客様が必要とする回復力を提供し、大規模な環境でも信頼できると評価をいただいております。単一の統合されたアプローチを通じ、800 以上のデータソース、100 以上のオペレーティングシステム、1,400 以上のストレージターゲット、60 以上のクラウドをサポートしており、ベリタスの実行能力に匹敵するベンダーは他にありません。Cloud Scale Technology により、ベリタスは運用にかかる煩雑さや業務量を削減しつつ優れた価値を提供する、自律型データ管理の戦略を提供しています。ベリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

VERITAS

〒107-0052 東京都港区
赤坂 1-11-44
赤坂インターシティ 4 階
www.veritas.com/ja/jp

各国オフィスとお問い合わせ先については、弊社の Web サイトを参照してください。
veritas.com/ja/jp/company/contact

V1627 12/22