技術検証

Cybersecurity with Veritas

(ベリタスによるサイバーセキュリティ)

ベリタスのランサムウェア対策

著者: Craig Ledo (IT 検証アナリスト)

2022 年 9 月

この ESG 技術検証はベリタスが委託したものであり、TechTarget 社の使用許諾を受けて配布されています。

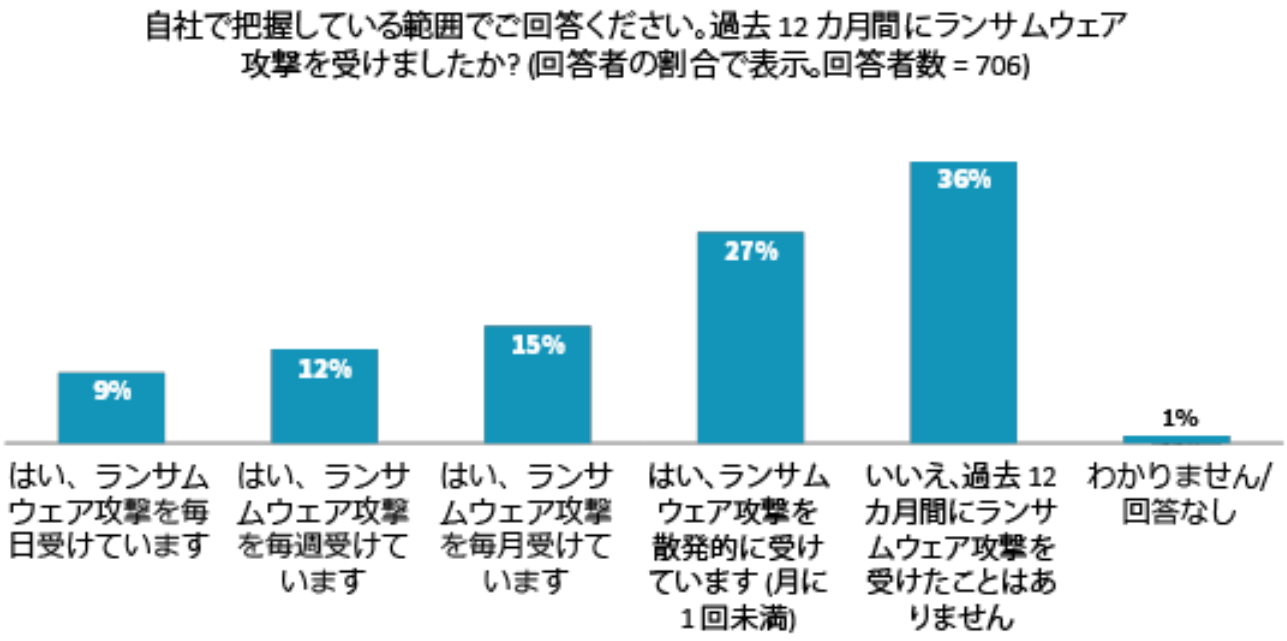
はじめに

この ESG 技術検証レポートは、データの保護、脅威の検出、大規模なリカバリなどを実現するベリタスのサイバーセキュリティソリューションを詳細に評価したものです。具体的には、ベリタスのサイバーセキュリティソリューションポートフォリオ全体を対象に、12 のテストシナリオを検証しました。

背景

ランサムウェア攻撃は、ビジネスリーダーや IT リーダーにとって常に最優先の課題となっていますが、これには理由があります。企業の生命線であるデータへのアクセスが危険にさらされるからです。今も続くランサムウェア攻撃は、ダウンタイム、生産性、デバイスコストやネットワークのコスト、機会の損失、身代金の支払い、ブランドの価値といった点で、企業に莫大なコストを発生させてしまいます。多くの企業は、データのエントリポイントの保護に年間数百万ドルを費やしながらも、データ保護を強化することの戦略的価値については依然として過小評価しています。ESG の調査によれば、過去 1 年間にこのようなプロービング攻撃を月に 1 回以上受けたと回答した人の割合は 36% で、そのうちの 9% は毎日、12% は毎週攻撃を受けています (図 1 を参照)。[1]

図 1. ランサムウェア攻撃は繰り返し行われるのが普通です



出典: ESG (TechTareget 社の子会社)

[1]出典: ESG 調査レポート、『2022 Technology Spending Intentions Survey (2022 年版テクノロジ支出予定調査)』、2021 年 11 月

また、回答者の 27% が、頻度は少ないながらも、ランサムウェア攻撃を経験しています。一度攻撃を受けた企業は再び標的にされる可能性があるため、企業にとっては、強力でプロアクティブな防御手段を講じてランサムウェア攻撃を阻止することがきわめて重要となります。

さらに、データ需要とデータ損失リスクが高まる中、エンドユーザーが期待するスムーズなエクスペリエンスを提供しながら、IT サービスの安全性、回復力、リカバリ能力を確保するには、高度で多層的な回復力戦略が必要になります。たとえば、ソフトウェアとハードウェアの両面から強化され、改ざん/消去不可能なストレージをサポートするソリューションなら、包括的で多層的なサイバーセキュリティ戦略を実現するのに役立ちます。

ベリタスのサイバーセキュリティソリューションの概要

ベリタスは、多層型の統合プラットフォームを採用し、プロアクティブな保護、脅威検出、およびバックアップとリカバリをシームレスに統合しています。具体的には、ゼロトラストセキュリティモデルを提供することで、企業がより優れたアクセス制御を実装し、侵害を封じ込め、資産を保護し、損害の可能性を軽減できるようにしています。

保護:

- 重要なデータと IT インフラを、予期せぬ未知の脅威から確実に保護します。そのために、環境全体をバックアップする包括的な保護機能をインテリジェントに適用し、自動管理によって適切に拡張します。
- バックアップインフラとバックアップデータを利用することで、企業はバックアップとリカバリのインフラを、回復力の確保に欠かせないコンポーネントに進化させることができます。
- Veritas NetBackup は、エッジからコア、クラウドまでをサポートし、800 種を超えるデータソース、1,400 社以上のストレージプロバイダ、60 社以上のクラウドプロバイダに対応しているため、最も要求の厳しい大規模な環境でも保護できます。
- ベリタスのインテリジェントポリシーは、自動化のレベルを高め、管理者に優れた効率性をもたらします。
- バックアップファイルを安全に保管し、悪質な侵入者による操作を阻止するために、データの整合性を保護するエアギャップソリューションを提供しています。
- 内部管理の安全なコンプライアンスクロックにより、改ざんも消去も不可能なバックアップイメージを実現します。

検出:

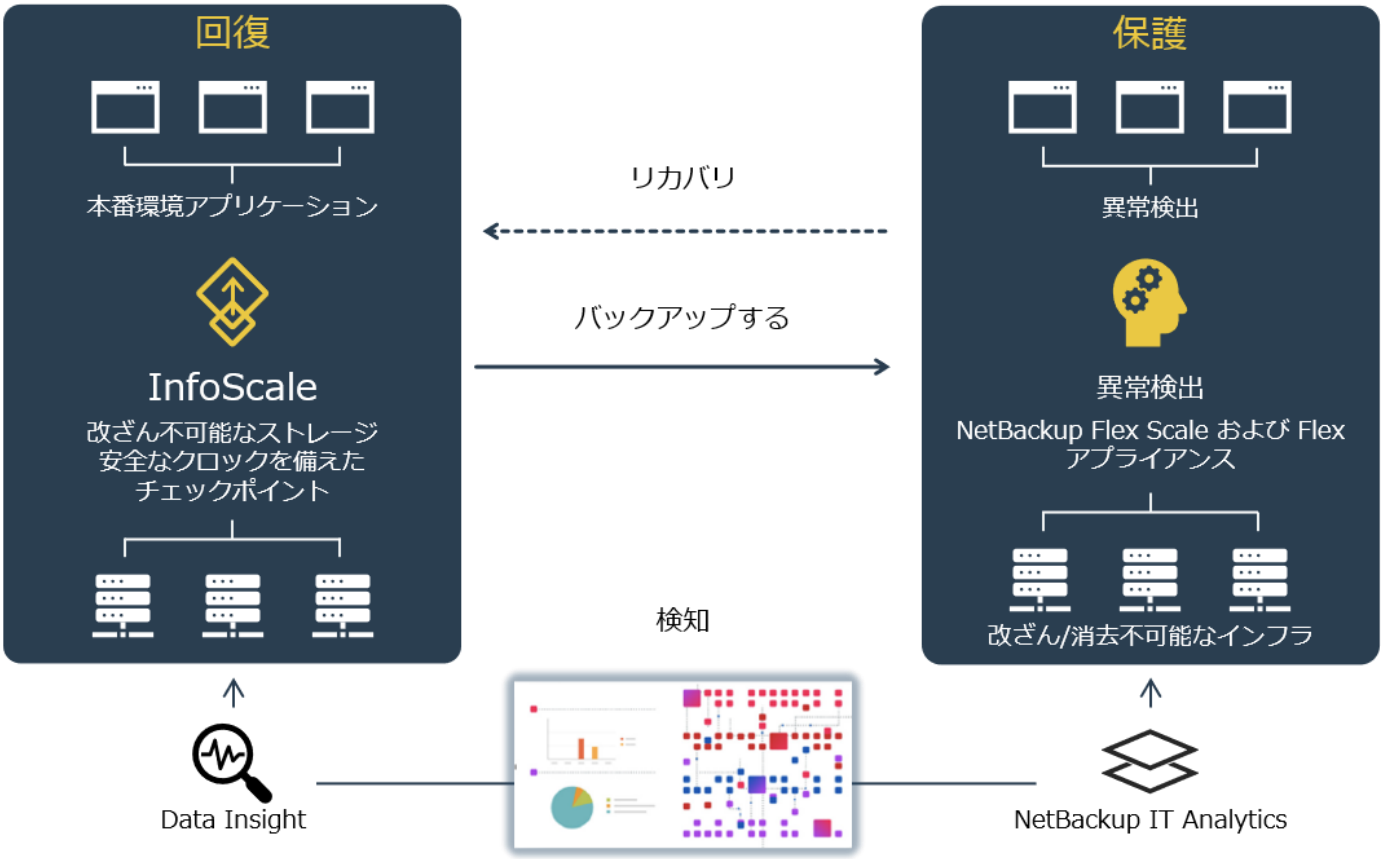
- ベリタスは、インフラを完全に把握できる機能を提供することで、企業の環境に存在するすべてのダークデータに光を当てます。
- また、環境内のあらゆるものを安全に保護し、企業がランサムウェアの脅威を克服できるようにします。
- さらにベリタスは、プライマリおよびバックアップデータに対して AI を活用した異常検出とマルウェア検出を可能にするほか、イベントトリガー式のマルウェアスキャンを実行し、サイバー犯罪者や悪質なコードが行動を起こす前に対処します。

回復:

- ベリタスのソリューションは、回復力の確保に欠かせないコンポーネントとして、リカバリに最適な環境を実現します。
- ベリタス製品に組み込まれたセキュリティソリューションにより、ランサムウェアのないクリーンなデータと環境をオンラインで復元できるようにします。
- 場合によっては、環境全体が影響を受け、データセンター全体をクラウドおよびオンデマンドでリカバリすることが必要になることがあります。
- その一方で、環境の一部のみが影響を受けることもあるため、データベースやファイルを個別にすばやく本番環境にリカバリできる柔軟なソリューションの導入が不可欠になります。
- サーバー全体が暗号化されている場合、そのサーバーを他の場所に迅速にリカバリしなければならないこともあります。
- また、多数のアプリケーションインスタンスを本番環境にリカバリするだけで済む場合もあります。
- ベリタスが提供するソリューションなら、リカバリのオーケストレーションや一括リカバリなど、大規模なリカバリが可能です。

ベリタスのソリューションは、データを常に利用可能な状態で保護し、アプリケーションの高可用性をサポートし、大規模なリカバリを実現します。ビジネスバリューの観点からランサムウェア攻撃に対する耐障害性に取り組むベリタスは、ランサムウェアからの保護、検出、リカバリの課題を解決することで、強固な回復戦略を可能にします (図 2 を参照)。

図 2. ベリタスのサイバーレジリエンスソリューションの概要



出典: ESG (TechTareget 社の子会社)

ESG Technical Validation (ESG 技術検証)

ESG は、データの保護、脅威の検出、大規模なリカバリなどを実現するベリタスのサイバーセキュリティソリューションを対象とする技術評価を実施しました。

データの保護

ベリタスでは、データ保護に役立つ以下のような幅広いセキュリティコントロールを提供しています。

- **個人情報およびアクセス管理**: ロールベースのアクセス、シングルサインオン、カスタマイズ可能な認証。
- **データの暗号化**: 送信中のデータと保管中のデータの両方を暗号化。
- **改ざん不可能なイメージ管理およびストレージ**: ストレージに依存しない柔軟なイメージ管理と WORM (Write Once, Read Many) ストレージへのイメージの保存。
- **ソリューションの強化**: NetBackup Flex および NetBackup Flex Scale が、ソフトウェアとハードウェアの両面から強化され、改ざん不可能なストレージをサポートする完全なセキュリティソリューションを提供。

ESG が検証した主要なデータ保護機能は以下のとおりです。

クラウドデータの改ざん防止機能

このソリューションは、サイバー犯罪の侵入や内部の脅威からデータを保護するために、データを変更できない期間を設定できるようにします。また、セキュリティを強化するため、NetBackup ストレージサービス経由でしか表示やアクセスができない安全なデータストアにバックアップストレージを配置し、ユーザーやファイルシステムサービスによるアクセスを阻止します。

強化された侵入防止機能

Linux オペレーティングシステム、管理アクセス、アプリケーションバイナリ、構成設定など、NetBackup アプライアンスのすべてのスタックでセキュリティが強化されています。STIG ガイドラインへの準拠や強制アクセス制御の実装など、独自のセキュリティポリシーの適用もその 1 つです。また、プロセスとリソースへのアクセスを制限し、ユーザーやシステムの重要なアクションの監査証跡を維持する侵入検知防止サービスも提供されています。

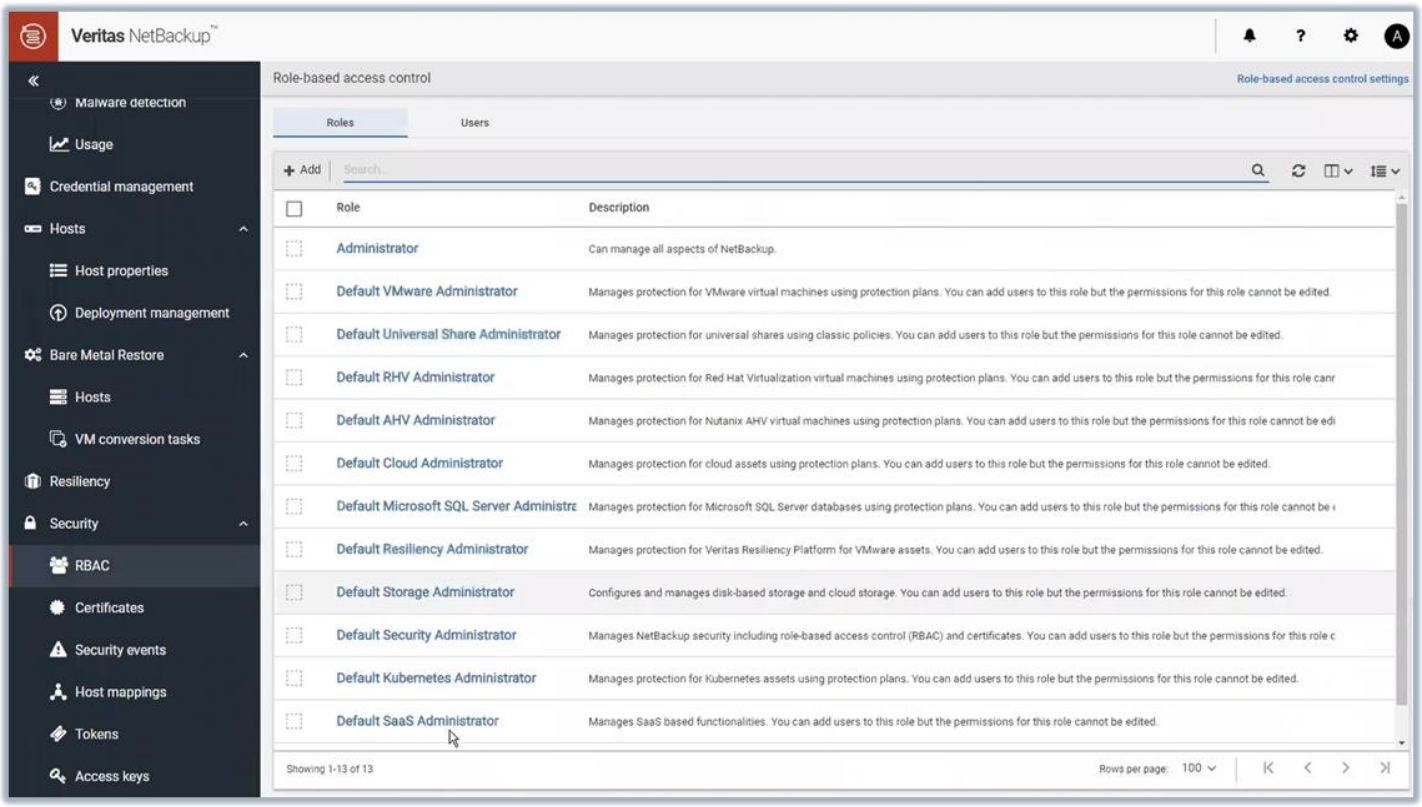
改ざん防止ハードウェア

改ざん不可能なストレージをホストするアプライアンスをより高度なセキュリティレベルに移行し、データとインフラの両方を保護できます。管理者が OS や内部コンポーネントに変更を加えることが不可能になり、すべてのエンドポイントが不正アクセスから保護されます。また、すべてのサービスへのアクセスが保護され、認証を求められるようになります。

アクセス制御の保護

このソリューションでは、ロールベースのアクセス制御 (RBAC) テンプレートが提供されます (図 3 を参照)。これにより、管理者はユーザーまたはユーザーグループに適切なアクセスや権限を簡単に提供できるようになります。また、各テンプレートの詳細な権限 (NetBackup の管理、保護、セキュリティ、ストレージなど) を確認できます。ユーザーまたはグループのアクセスや権限をカスタマイズすることも可能です。管理者はこのカスタムロールに基づいて、ワークロードの割り当て (ユーザーが管理できるワークロードアセットの選択など)、保護プランの割り当て (ユーザーが管理できる保護プランの選択など)、資格情報の割り当て (ユーザーが管理できる資格情報の選択など) を行うこともできます。

図 3. アクセス制御の保護

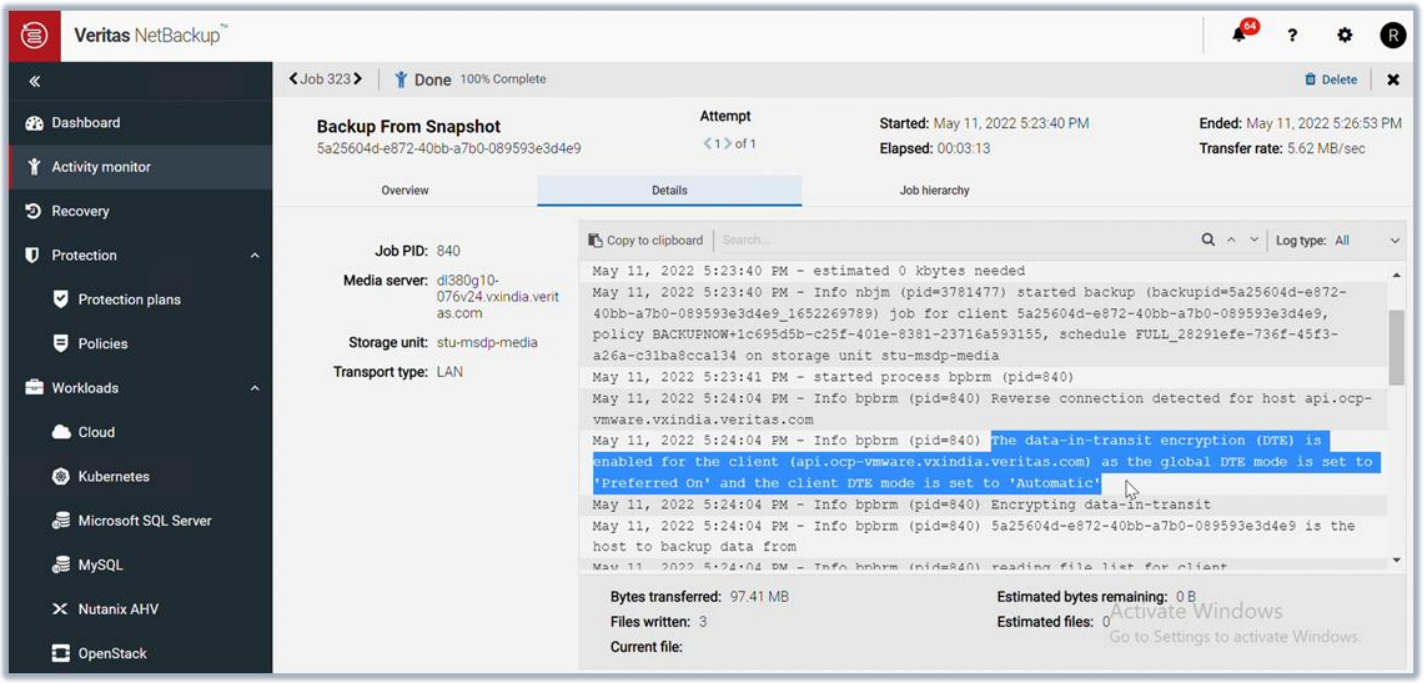


出典: ESG (TechTareget 社の子会社)

最新インフラの保護

このソリューションは、ビッグデータ、ハイパーコンバージド、オープンソースの MySQL/NoSQL データベースといった最新インフラ向けの次世代データ保護テクノロジを提供します。NetBackup を使用すれば、ワークロードがマルチクラウド、仮想、物理、最新インフラのどこにあっても、そのワークロードを 1 つのコンソールから保護できるようになります。図 4 は、スナップショットからのバックアップを示したものです。バックアップでクライアントに対して送信中のデータ暗号化（DTE）が有効になっているのは、グローバル DTE モードが［Preferred On］に、クライアント DTE モードが［Automatic］に設定されているためです。バックアップイメージの DTE モードが［On］に設定されているため、ユーザーは必要に応じて、DTE が有効化されているこのバックアップからリストアを実行できます。

図 4. 最新インフラの保護



出典: ESG (TechTareget 社の子会社)

なぜ重要か

ランサムウェア攻撃が進化し、巧妙化する中、企業がサービスのダウンタイムやデータ損失を回避するには、急速に変化する脅威ベクトルに簡単に適応できることが重要です。ベリタスの高度なデータ保護アプライアンスとセキュアアプライアンスは、統合された異常検出、マルウェアスキャン、ゼロトラストアーキテクチャ、改ざんも消去も不可能なストレージなど、ランサムウェアを阻止するさまざまな機能を備えています。

脅威の検出

ベリタスでは、脅威の検出に役立つ以下のような幅広いセキュリティコントロールを提供しています。

- **バックアップおよびストレージインフラの把握**: NetBackup IT Analytics は、緩和分析、連続失敗のソース、最近のバックアップがないソース、アプリケーション別のバックアップの失敗など、エンドツーエンドのバックアップを監視します。
- **異常検出**: NetBackup は、AI を活用した異常検出によって環境全体から異常なデータを検出し、不審な異常に関するアラートをほぼリアルタイムで送信します。
- **プライマリストレージの検出**: ベリタスでは、NetBackup でセカンダリバックアップデータに、Veritas Data Insight でプライマリストレージデータに対応しています。後者は既存のセキュリティ検出ツールを補完するものとして、ユーザーやデータの異常なふるまいをほぼリアルタイムで検出するほか、ランサムウェア専用のカスタムクエリーテンプレートや、ランサムウェアの検出に役立つファイル拡張子識別機能を提供します。
- **マルウェアの検出**: ベリタスでは、保護されたバックアップに対して自動スキャンとオンデマンドスキャンの両方を実行します。自動マルウェアスキャン機能は、人による操作をなくし、人工知能/機械学習 (AI/ML) テクノロジを使って迅速にマルウェアをスキャンします。

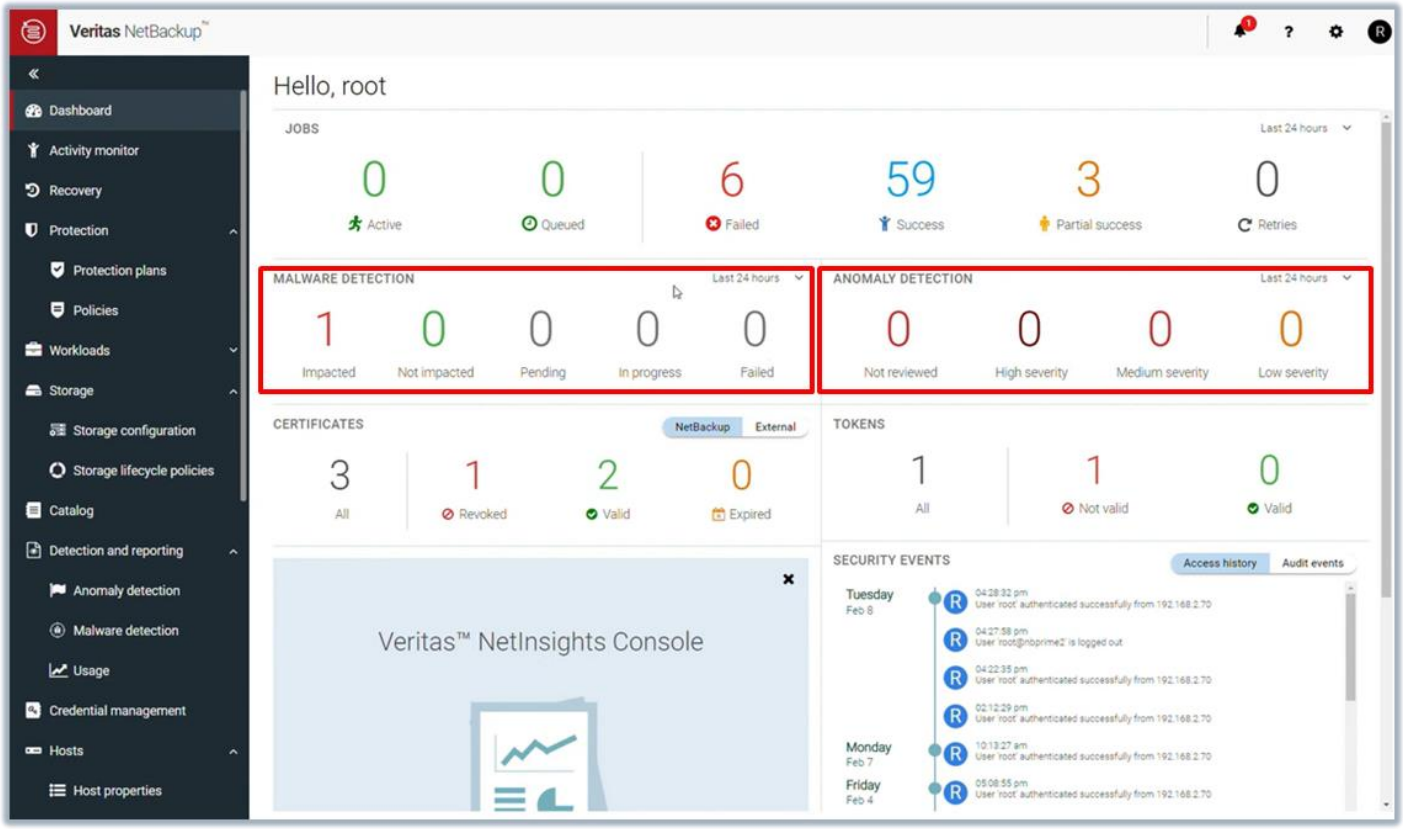
ESG が検証した主要な脅威検出機能は以下のとおりです。

マルウェアスキャンと異常検出の統合

異常検出ではマルウェア検出とは別にイメージのメタデータを追跡しますが、マルウェア検出では異常検出スコアを利用できます。図 5 に示すように、マルウェア検出イベントは「過去 24 時間」の状況に基づき、［Impacted］、［Not Impacted］、［Pending］、［In Progress］、［Failed］に分類されます。この期間は、「過去 48 時間」または「過去 72 時間」に設定することもできます。ユーザーは、分類 (［Imacted］など) ごとに詳細を確認できます。また、影響を受けたバックアップイメージごとに、すべてのコピーを期限切れにする、あるいは感染したファイルを確認するなどのアクションを実行できます。マルウェア検出ダッシュボードには、クライアント、バックアップ時間、スキャン結果、バックアップの種類、スキャン日、マルウェアアプリケーションスキャナ、影響を受けたファイルの数、スキャンホスト名、バックアップ ID などの情報が表示されます。マルウェアのスキャン時間は、イメージのサイズやファイルの数など、複数の要因によって変化します。

図 5 に示すように、異常検出イベントは「過去 24 時間」の状況に基づき、［Not Reviewed］、［High Severity］、［Medium Severity］、［Low Severity］に分類されます。この期間は、「過去 48 時間」、「過去 72 時間」、「過去 7 日間」に設定することもできます。また、レビュー状態 (［Not Reviewed］、［False Positive］、［Anomaly, Ignore］) と異常の重大度 (［High］、［Medium］、［Low］) で絞り込むこともできます。異常検出ダッシュボードには、ジョブ ID、クライアント名、ポリシー形式、数、スコア、異常の重大度、異常の概略、受信日、レビュー状態、ポリシー名、スケジュール名、スケジュール形式などの情報が表示されます。ユーザーは、検出された異常に対して、無視、異常として確認、誤検知として報告などのアクションを実行できます。

図 5. マルウェアスキャンと異常検出の統合



出典: ESG (TechTareget 社の子会社)

レポートとアラート

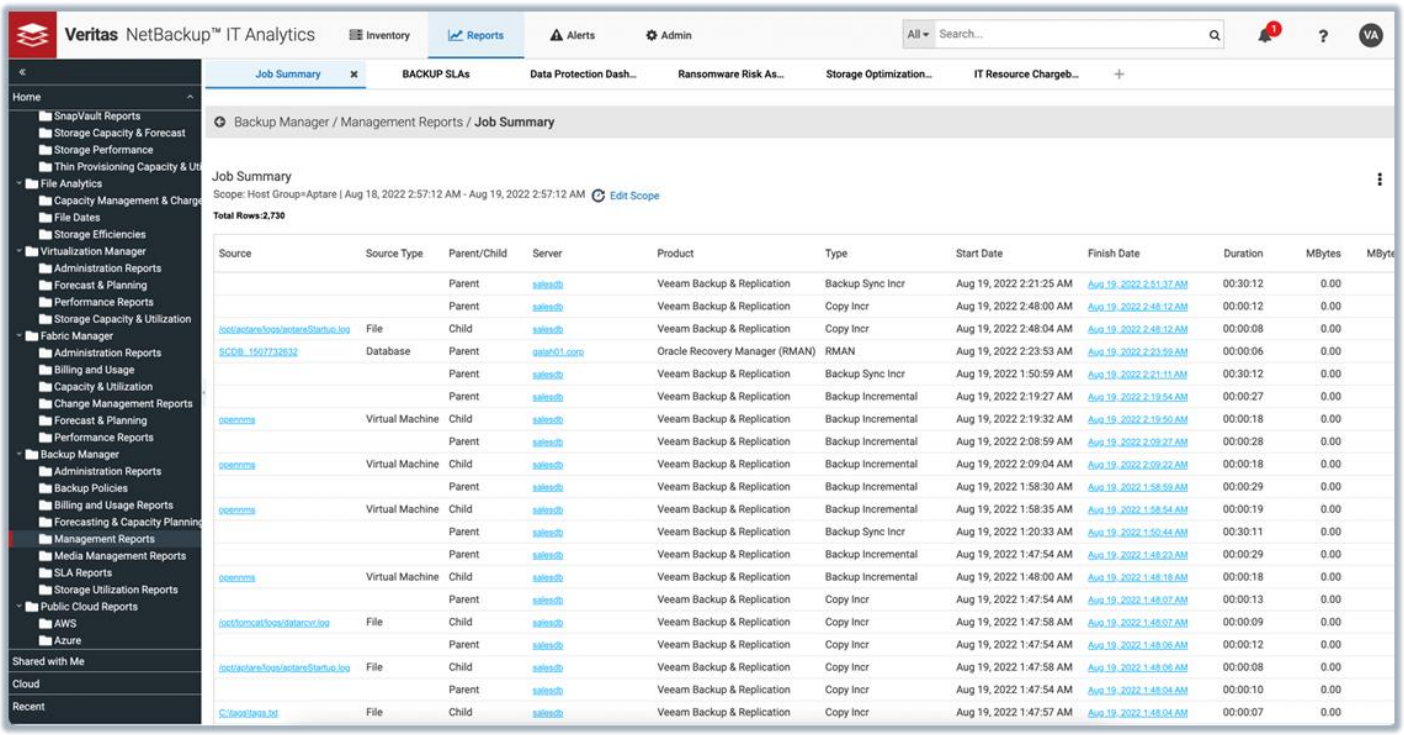
Veritas NetBackup IT Analytics には、すぐに使えるランサムウェアリスク評価ダッシュボードが用意されています。このダッシュボードでは、予測分析を通じてあらかじめ作成されたレポートを表示して、バックアップ環境内の潜在的なリスクを把握できます (図 6 を参照)。ユーザーはこの分析結果から、以下のような複数のデータポイントに関する包括的なレポートを作成し、バックアップ環境の最適化と保護を実現できます。

- **発見** – バックアップ環境内のすべての変更を追跡してランサムウェアを検出し、迅速に対処できます (850 を超える既知のランサムウェア拡張子に対応)。
- **リスクの可視化** – 直感的なグラフを使用して、環境内で発生したすべてのリスクの履歴を確認したり、バックアップスケジュールに含まれていないホストにフラグを付けたり、バックアップが失敗したアプリケーションを可視化したりできます。
- **バックアップの監視** – 実用的なインサイトを提供するサマリーグラフを使用して、バックアップ環境内の変更を監視および特定できます。また、成功した既知のバックアップのベースラインを使用して異常を特定し、リスクを軽減できます。

NetBackup IT Analytics では、既知のランサムウェア拡張子を使ってファイルを検出できるだけでなく、この情報をわかりやすく整理し、計画を迅速に実行することができます。ユーザーは、ホストによって検出されたランサムウェアファイル、ランサムウェアファイルが最も多い場所、ランサムウェア拡張子のタイプ、およびファイルの所有者別に情報を整理できます。

さらに NetBackup IT Analytics は、潜在的な誤検知を特定するために、正常なバックアップを調査します。具体的には、バックアップ履歴を新しいバックアップと比較して、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します。これにより、ユーザーは重要な IT サービスを確実に保護できるようになります。

図 6. レポートとアラート



出典: ESG (TechTareget 社の子会社)

なぜ重要か

前述のとおり、ランサムウェア攻撃は進化し、巧妙化しています。そのため、ベリタスはプライマリデータとバックアップデータの両方でマルウェアの侵入を特定するのに役立つ異常検出とカスタマイズされたインサイトを通じて、アプリケーションとデータの全体的な状態をリアルタイムで可視化します。

大規模なリカバリ

ベリタスでは、大規模なリカバリに役立つ以下のような幅広い機能を提供しています。

- **NetBackup Resiliency**: 一貫したユーザーエクスペリエンスを提供し、利用できる最適なリカバリオプションを提示することで、企業のヘテロジニアス環境全体で自動オーケストレーションを実現します。
- **NetBackup Instant Rollback for VMware**: Reverse Change Block Tracking を使用してリカバリが必要な一意のブロックを特定し、その部分の変更のみを適用して VM をわずか数秒で健全な状態にロールバックするという、高速な VM リカバリを実現します。

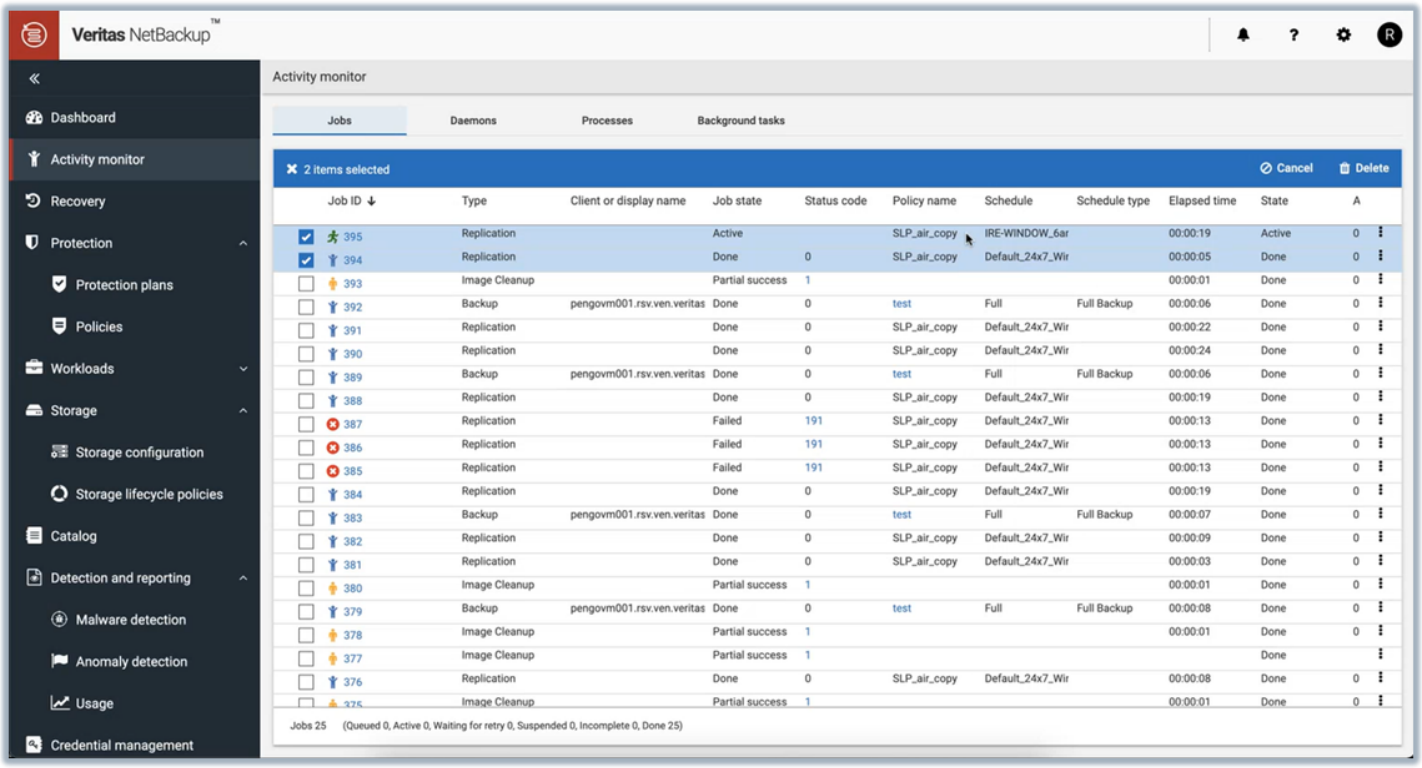
- **VM リカバリ**: VMware VM の 1 つのバックアップに対して、8 種類のリカバリ (VM 全体、個々の VMDK、ファイルとフォルダ、アプリケーション全体、インスタントアクセス、ファイルのダウンロード、アプリケーション GRT、AMI 変換) が可能です。
- **MSSQL および VMware のインスタントアクセス**: VM のデータがバックアップから転送されるまで待つ必要がほとんどない迅速なマシンリカバリが可能です (1,600 台の VM など)。また、バックアップストレージから直接 VM をテストまたはリカバリできます。
- **NetBackup CloudPoint**: クラウドベンダーに依存しない方法でクラウドネーティブのスナップショットテクノロジを使用して、ハイブリッドおよびマルチクラウドインフラを簡単に保護できます。
- **Universal Share と保護ポイント**: NetBackup サーバー上にセキュリティの高い共有として重複排除バックアップストレージをプロビジョニングすることで、エージェントもバックアップ API も存在しないデータベースやその他のワークロードを保護できます。
- **NetBackup Universal Shares for Oracle**: Oracle データベース管理者が NetBackup アプライアンスのストレージから直接データベースを起動できるようにします。
- **長期保存アーカイブ**: この手法により、オブジェクトストレージとプライベート/パブリッククラウドの併用など、データの重複排除と圧縮機能を備えたコスト効率と耐久性の高いソリューションを実現します。従来のリカバリ手法には、別のサイトや場所またはクラウドを対象とした、特定ファイルの個別リストア、完全サーバー/アプリケーションリストア、ディザスタリカバリ (DR) リストアなどがあります。Veritas Resiliency Platform を使用すれば、ボタン 1 つで従来のリカバリを自動化および統合し、DR プロセスを合理化できます。
- **ベアメタルリストア**: サーバーのリカバリプロセスを自動化することで、手動によるオペレーティングシステムの再インストールやハードウェアの構成を不要にします。企業は、1 回の操作で OS およびアプリケーションデータをリストアし、システムをゼロから短時間で再構築できます。

ESG が検証した主要な大規模リカバリ機能は以下のとおりです。

分離型リカバリ環境

Veritas NetBackup の分離型リカバリ環境を使用すると、多層型の複雑な環境に含まれている可能性がある数千台の VM のリカバリ計画を実行したり、分離された環境で同様のリカバリのリハーサルを実行したりできます (図 7 を参照)。これにより、あらかじめ組み込まれた改ざん防止機能や消去防止機能をサポートしたり、第三者製ハードウェア、クラウドベースのロックされたオブジェクトストレージ、SaaS のワークロードバックアップで改ざんを不可能にしたりすることができます。また、重複排除されたデータを AWS S3 オブジェクトロックに直接送信し、効率的に保存することができます。

図 7. 分離型リカバリ環境

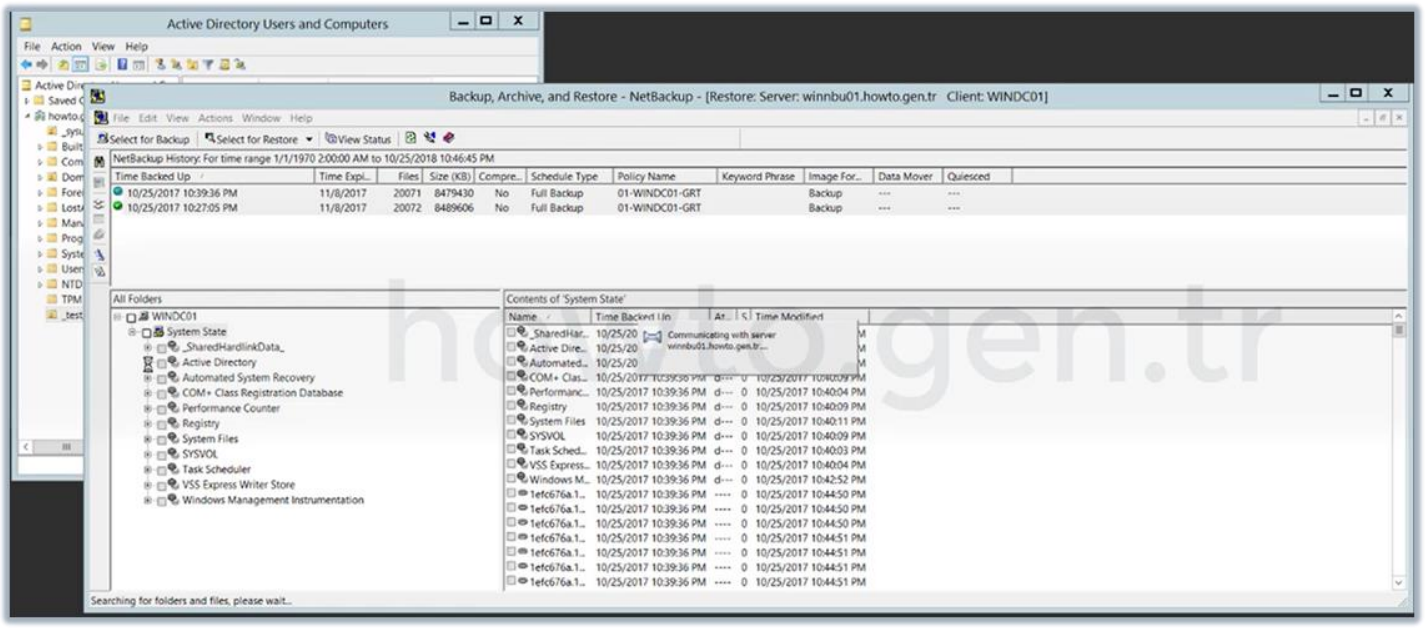


出典: ESG (TechTareget 社の子会社)

削除された Active Directory のリカバリ

Veritas NetBackup ソリューションには、Active Directory のバックアップを参照し、削除された Active Directory をリカバリできる機能が用意されています (図 8 を参照)。ユーザーは、Active Directory の適切なバックアップを開始するだけです。また、要求した操作が正常に完了するまで、リストアの進行状況を確認することもできます。

図 8. 削除された Active Directory のリカバリ

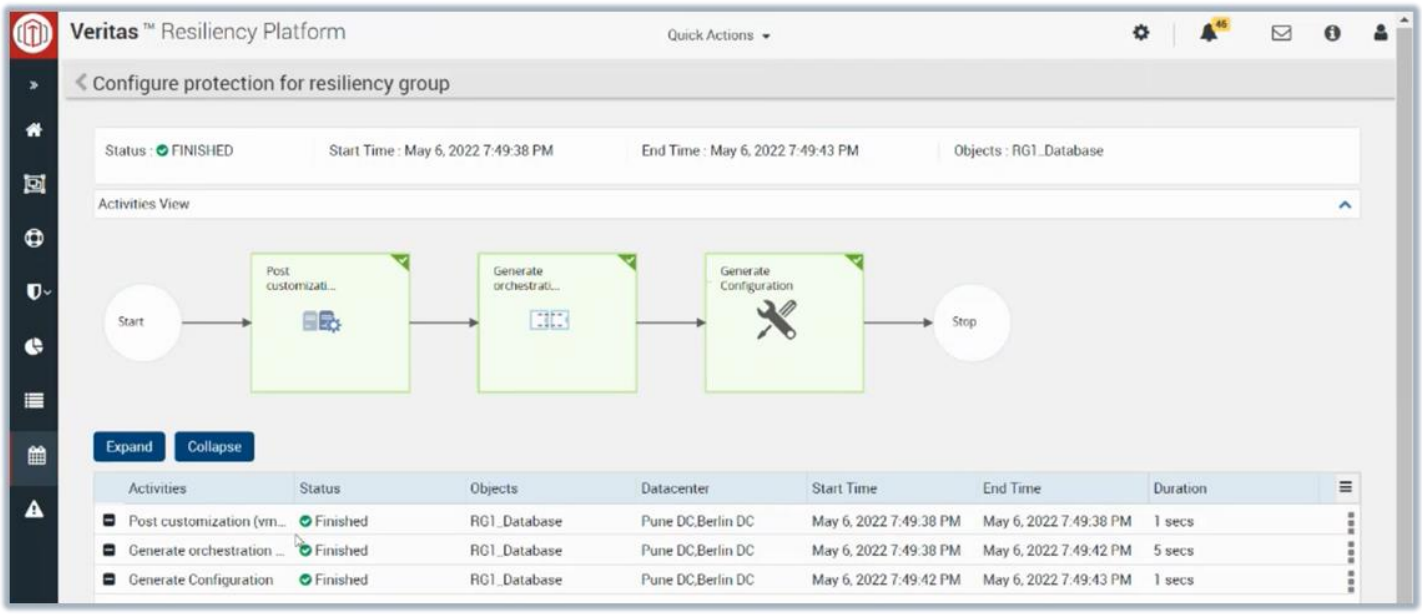


出典: ESG (TechTareget 社の子会社)

多層型リカバリのオーケストレーション

Veritas NetBackup Resiliency の Virtual Business Service では、多層型アプリケーションのリカバリを単一の統合されたエンティティとして管理できます。Virtual Business Service なら、複数のシステムにまたがって動作する多層型の複雑なアプリケーションのリカバリを完全に自動化できます。そのため、ランサムウェア攻撃が発生しても、簡単かつ迅速にリカバリを実行して、アプリケーションのダウンタイムを最小限に抑えることができます。具体的には、Veritas Resiliency Platform が、仮想化やプライベートクラウド (VMware vCenter の追加など)、NetBackup プライマリサーバー、ネットワーク (ネットワークペアリングなど)、物理サーバー、データベースなどを構成するといった方法で、多層型リカバリのオーケストレーションを実現します。Resiliency Group の保護設定の完了については、図 9 を参照してください。

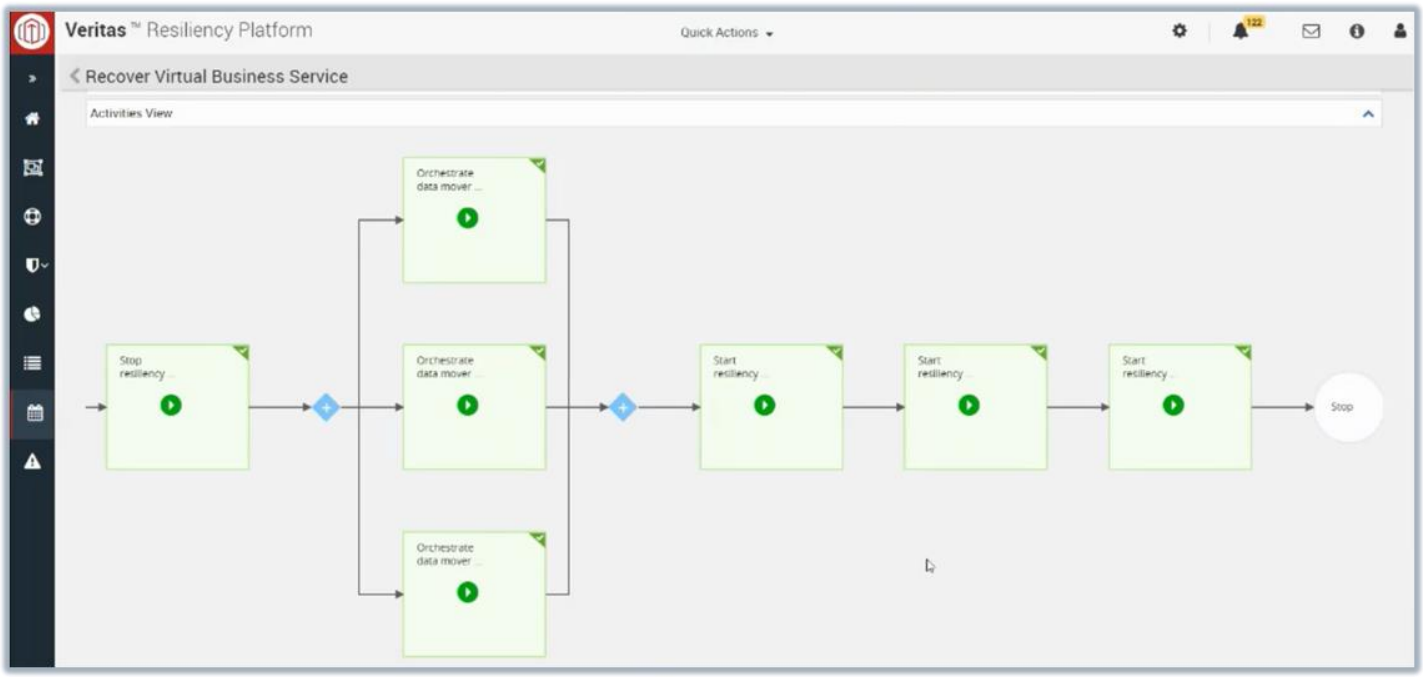
図 9. 多層型リカバリの設定



出典: ESG (TechTareget 社の子会社)

Resiliency Group の保護設定が完了したら、多層型の Virtual Business Service を設定する必要があります。これにより、Virtual Business Service の多層型リカバリのオーケストレーションが可能になります (図 10 を参照)。

図 10. 多層型リカバリのオーケストレーション



出典: ESG (TechTareget 社の子会社)

なぜ重要か

増加するランサムウェア攻撃に対処するには、ランサムウェア攻撃からの回復力とリカバリに関する包括的な戦略を策定することが重要になります。ベリタスは、プライマリデータ用の高度なストレージ機能と迅速なリカバリ機能を提供することで、ストレージの回復力、改ざん防止機能、データ分離機能を統合し、データの安全性と整合性、およびアプリケーションの可用性を確保します。

総合的な結論

ランサムウェアと悪意のある内部関係者が深刻な脅威となっています。オペレーティングシステムの新たな脆弱性が絶えず発見されており、既知のマルウェアおよびランサムウェアの亜種も定期的に開発されています。ランサムウェアは大きなビジネスであり、攻撃者にとっては、それが企業のインフラに侵入し、その企業の業務を停止させる方法を革新し続ける動機になります。

ESG は、データの保護、脅威の検出、大規模なリカバリなどを実現するベリタスのサイバーセキュリティソリューションを対象に、12 のテストシナリオを検証しました。多層的で包括的なサイバーセキュリティ戦略は、マルウェアの侵入によるダウンタイムやデータ損失に対する最善の防御策です。こうした戦略の策定は複雑な取り組みになりますが、ベリタスはこれを理解した上で、包括的なサイバーセキュリティ戦略の一環として IT サービスを保護する企業に役立つ基盤を提供しています。ベリタスのサイバーセキュリティ戦略は、IT サービスが常に高い可用性と回復力を備え、ランサムウェアから確実に保護されるようにするためのツールと機能を提供するというものです。

© 2022 TechTarget, Inc. All Rights Reserved.