

検出

NetBackupの検出機能で実現する
ランサムウェア対策、確実な復旧
および運用の効率化

勝野 雅巳

ベリタステクノロジーズ合同会社
データ保護ソリューション推進担当



ゼロトラストの考え方に基づく多層アプローチによるデータ保護

1



保護

- ✓ 統合バックアップに最適
- ✓ バックアップ基盤の防御、侵入防止
- ✓ バックアップデータの確実な保護

2



検出

- ✓ バックアップ元データの異常検出
- ✓ バックアップデータ上のマルウェア検出
- ✓ インフラ・バックアップ状況の可視化

3



回復

- ✓ 復旧に向けた事前確認
- ✓ 高速&柔軟な復旧の選択肢
- ✓ 復旧のオーケストレーションと自動化

ゼロトラストの考え方に基づく多層アプローチによるデータ保護

1 保護

- ✓ **統合バックアップに最適**
 - 業界で最も広いワークロードをサポート
 - 他社製品から群を抜く高パフォーマンス
 - シンプルな構成
- ✓ **バックアップ基盤の防御、侵入防止**
 - セキュアなバックアップ専用アプライアンス
 - アクセス管理（RBAC／多要素認証）
 - 限定された通信／プロセスのみ許可
- ✓ **バックアップデータの確実な保護**
 - 暗号化（データ転送／保管時）
 - 改ざん防止／削除防止（WORM）
（クラウドストレージ、Flex Appliance、3rdパーティ）
 - 遠隔地複製（レプリケーション、クラウド、テープ）

2 検出

- ✓ **バックアップ元データの異常検出**
 - AIベースでのバックアップ元データの異常を検出
 - バックアップデータの大幅な変更を検出することで異常な疑わしいデータを特定
- ✓ **バックアップデータ上のマルウェア検出**
 - 復旧前にスキャンし安全性を確認
 - 3rdパーティのスキャンツールと連携
 - バックアップデータを対象としたスキャン
- ✓ **インフラ・バックアップ状況の可視化**
 - バックアップの監視とリカバリーの準備
 - 仮想/クラウド環境の保護対象の自動検出（Intelligent Group）
 - 重要なシステムが保護されていることの確認

今回はこちらをご紹介します

3 回復

- ✓ **復旧に向けた事前確認**
 - 本番環境に影響なく復旧テスト
- ✓ **高速&柔軟な復旧の選択肢**
 - ファイル/アイテム単位リストア
 - VMインスタントロールバック（増分リストア）
 - バックアップデータからの即時起動（Instant Access）
 - クラウドインスタンスへの変換
 - マルチテナンシー／セルフサービス
 - 継続的データ保護（CDP）からの高速復旧
- ✓ **復旧のオーケストレーションと自動化**
 - 大規模な自動リカバリ
 - レプリケーションとオーケストレーション

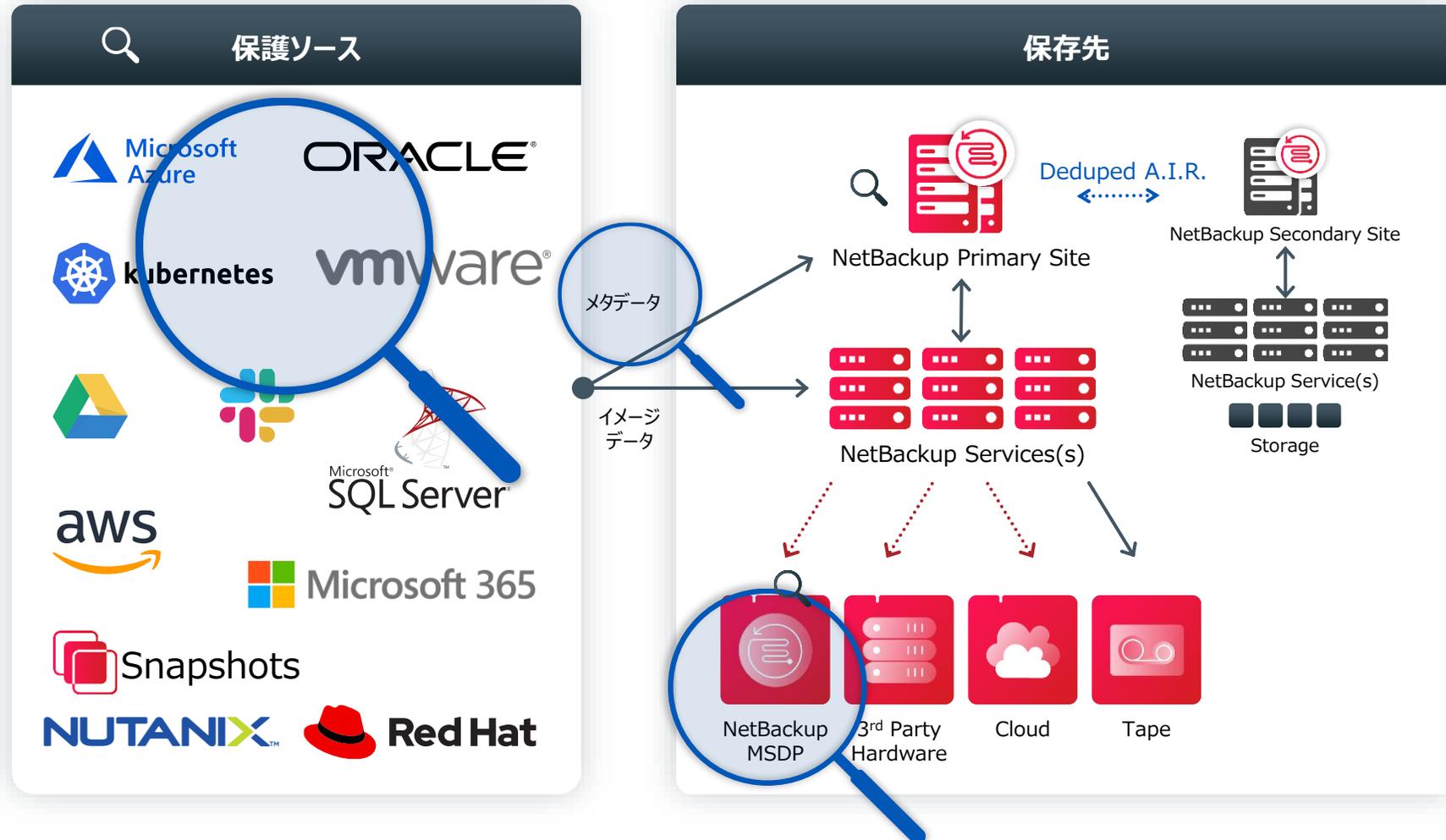


注意

製品の計画に関する将来的な記述は、仮のものです。
将来のリリース日は、確定したものではなく、変更されることがあります。

今後の製品のリリースや予定されている機能修正について、
ベリタスは継続的な評価を行っており、実装されるかどうかは確定していません。
したがって、購入の意思決定の判断材料にすべきではありません。

検出個所の概要



= 不変(WORM)ストレージ

= 検出

-----> = 重複排除

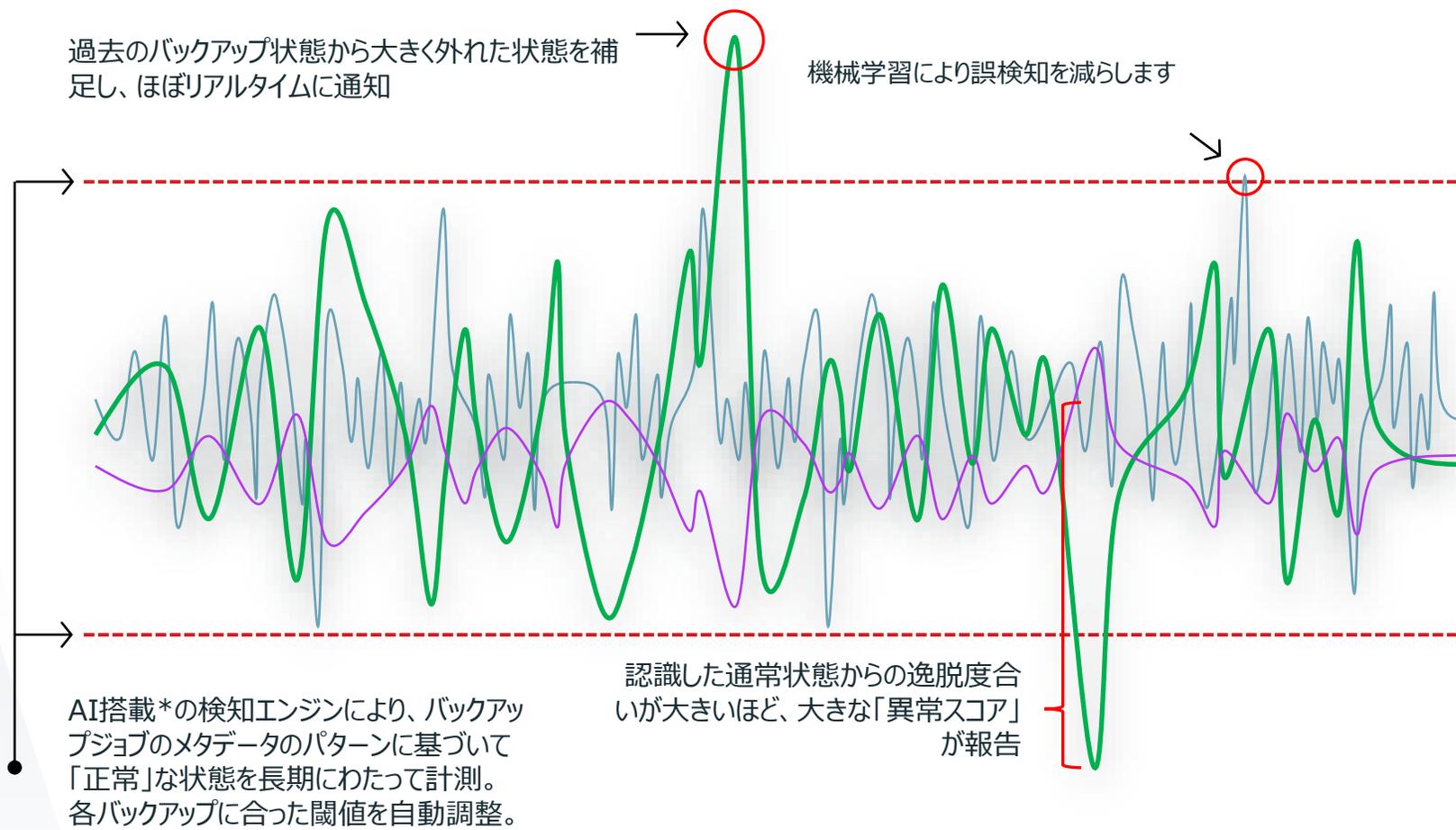
Agenda

1. バックアップ元データの異常検出
2. バックアップデータ上のマルウェア検出
3. インフラ・バックアップ状況の検出・可視化
 - 3-1. バックアップ状況の可視化
 - 3-2. 保護対象の自動検出&保護
4. まとめ

Agenda

1. バックアップ元データの異常検出
2. バックアップデータ上のマルウェア検出
3. インフラ・バックアップ状況の検出・可視化
 - 3-1. バックアップ状況の可視化
 - 3-2. 保護対象の自動検出&保護
4. まとめ

バックアップ元データの異常検出とは



NetBackupに搭載したAIアルゴリズムで異常検出

- 過去の実績から正常パターンを解析
- 自動モニタリング&レポーティング
- 5つの基準に基づいたレポート
- 攻撃に対する早期対応を促す

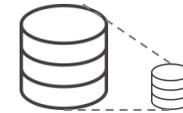
* 機械学習モデルは、nbdeployutilの出力を利用しています。
AIはDBSCANアルゴリズムによって実現されています。

異常検出チェック項目

- NetBackupによる**バックアップデータの異常を検出**
- AI／機械学習により、バックアップ時の異常な偏差（統計的なズレ）を検出



✓ バックアップ・データ・サイズ



✓ バックアップ・データの重複排除率



✓ データ転送サイズ



✓ バックアップ・ジョブの所要時間



✓ バックアップ対象ファイルの数

異常検出例

異常検出数は「4」

Veritas NetBackup™

異常検出

検索...

ジョブ ID	クライアント名	ポリシー形式	数	スコア	概略
153	kiji-media	Standard	4	12.95	Anomaly i...

ジョブ 153 に異常が検出されました。

Schedule name	Summary	Policy name
user	Anomaly image size, Backup files count, Data transferred, Deduplication ratio	userbk

Client name	Anomaly feedback	Count
kiji-media	誤検知として報告	4

Jobid	Score	Anomaly ID
153	12.95	153_1624431730

Policy type	Anomaly deduplication ratio	Anomaly backup files count
Standard	0% (Usual: 89% - 97.6%)	1 (Usual: 2 - 1101)

Anomaly image size	Anomaly data transferred
200.03 MB (Usual: 0.03 MB - 1.21 MB)	200.03 MB (Usual: 0.03 MB - 1.09 MB)

イメージサイズが異常
通常：0.03MB～1.21MB
今回：200.03MB

Anomaly image size
200.03 MB (Usual: 0.03 MB - 1.21 MB)

Storage name
stu-msdp-master

Anomaly data transferred
200.03 MB (Usual: 0.03 MB - 1.09 MB)

データ転送量が異常
通常：0.03MB～1.09MB
今回：200.03MB

重複排除率が異常
通常：89%～97.6%
今回：0%

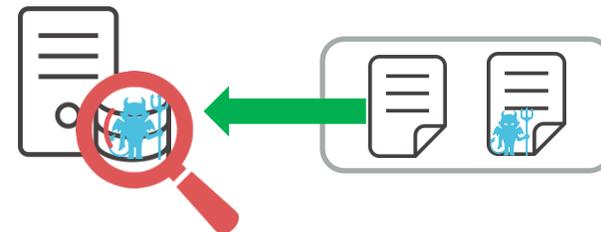
ファイル数が異常
通常：2～1100
今回：1

バックアップ元データからの異常検知の必要性

- セキュリティソフトのチェックをかいくぐるランサムウェア
 - 第三者視点のバックアップから被害の可能性を検出
- NetBackupはあらゆるデータを保護できる
 - 業務サーバ全体のチェックが統合的に可能

異常に気付かず、
バックアップ保持期限を過ぎると、
正常なデータが無くなってしまう

データの異常を検出することで、
ランサムウェア被害の可能性を確認復
旧することができる

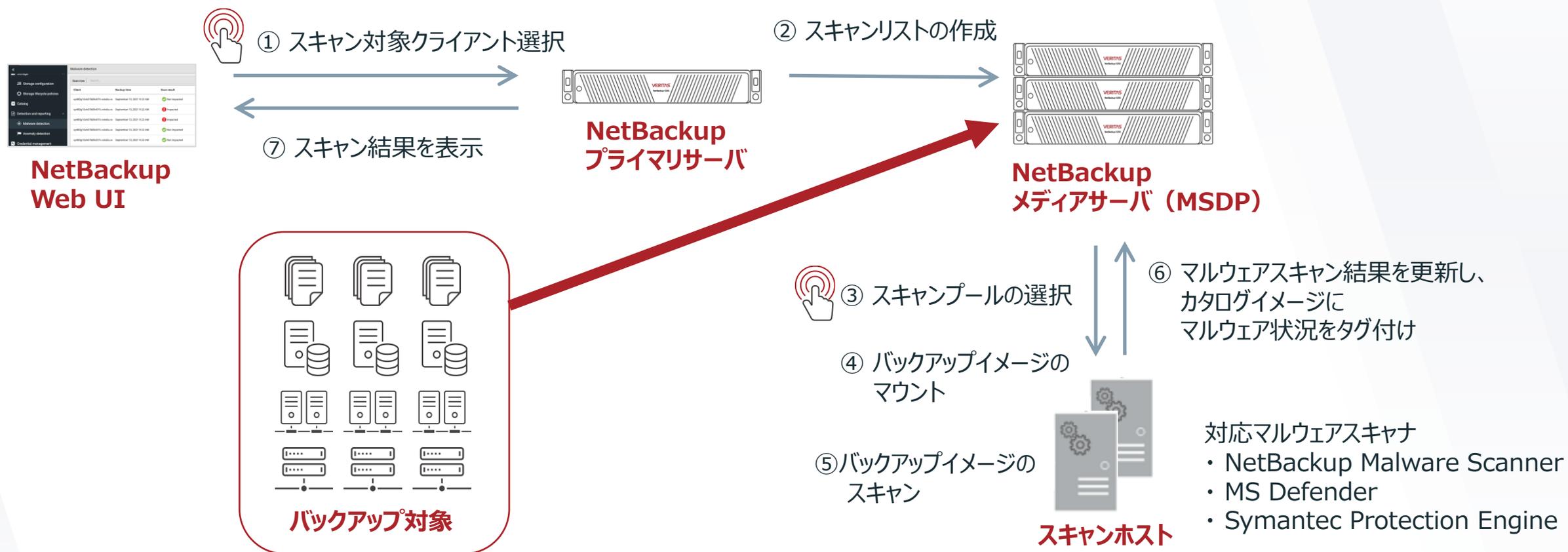


Agenda

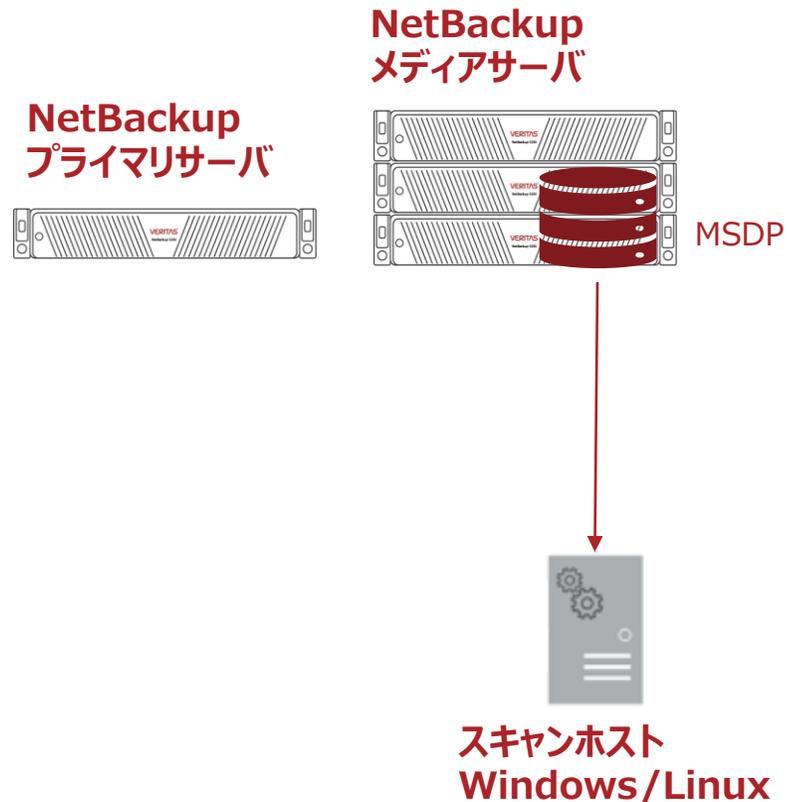
1. バックアップ元データの異常検出
2. バックアップデータ上のマルウェア検出
3. インフラ・バックアップ状況の検出・可視化
 - 3-1. バックアップ状況の可視化
 - 3-2. 保護対象の自動検出&保護
4. まとめ

NetBackupによるバックアップデータ上のマルウェア検出フロー

※NetBackup次期バージョンにて対応予定



マルウェア検出の構成



- Instant AccessがサポートされるMSDPメディアサーバを構成
- マルウェア検出を行うスキャンホストを用意（WindowsまたはRHEL）
- スキャンホストにマルウェアスキャナを導入
 - NetBackup Malware Scanner: ベリタスより提供
 - Microsoft Defender Antivirus: お客様ご手配
 - Symantec Protection Engine: お客様ご手配
- スキャンプールの構成
 - スキャンホスト
 - マウントタイプ(CIFS/NFS)
 - クレデンシャル

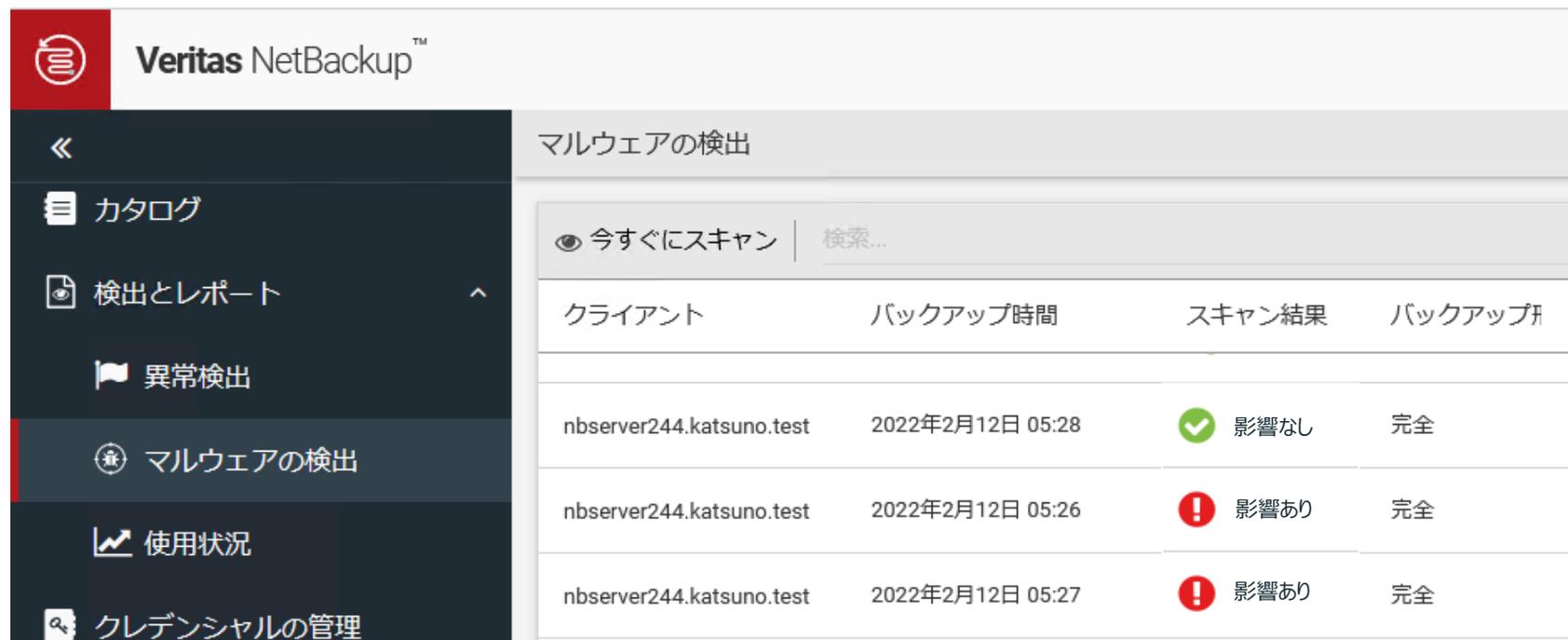
なぜバックアップデータのマルウェア検出が必要か？

- バックアップの動作から異常が検出された場合
 - 単純に変更が多かったのか、マルウェア被害が発生しているのか、確認が必要
 - 複数サーバが疑わしい場合、すべてのサーバの確認が必要
- 重要業務サーバに過去のバックアップから必要ファイルをリストア
 - そのバックアップデータをリストアしてマルウェアが発動することはないか不安



複数サーバのバックアップデータを
一括マルウェア・スキャン

マルウェア検知例



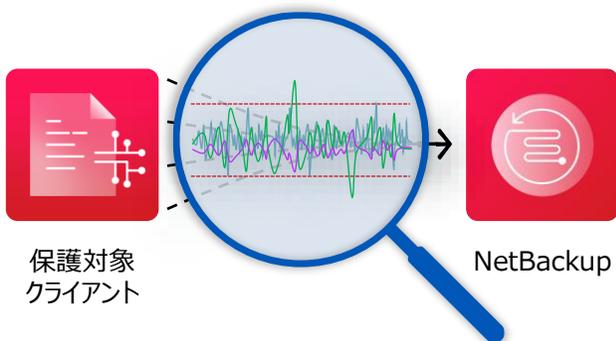
The screenshot shows the Veritas NetBackup™ interface. On the left is a dark sidebar with navigation options: カタログ, 検出とレポート, 異常検出, マルウェアの検出 (highlighted), 使用状況, and クレデンシャルの管理. The main area is titled 'マルウェアの検出' and contains a search bar with '今すぐにスキャン' and '検索...'. Below is a table with columns: クライアント, バックアップ時間, スキャン結果, and バックアップ#. The table lists three scan results for client 'nbserver244.katsuno.test' on 2022年2月12日.

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#
nbserver244.katsuno.test	2022年2月12日 05:28	🟢 影響なし	完全
nbserver244.katsuno.test	2022年2月12日 05:26	🔴 影響あり	完全
nbserver244.katsuno.test	2022年2月12日 05:27	🔴 影響あり	完全

- 保持しているバックアップ・イメージごとにスキャン状況を表示
- キーワード検索（フィルタリング）可能
- 「影響あり」イメージ内の感染ファイル名確認可能
- バックアップイメージの期限切れ操作可能

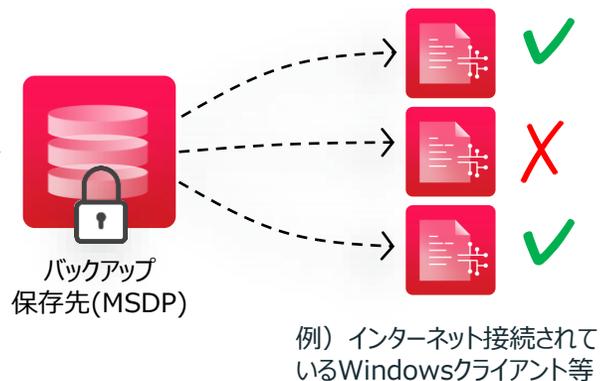
異常検出とマルウェア検出の関係

バックアップ中の動作



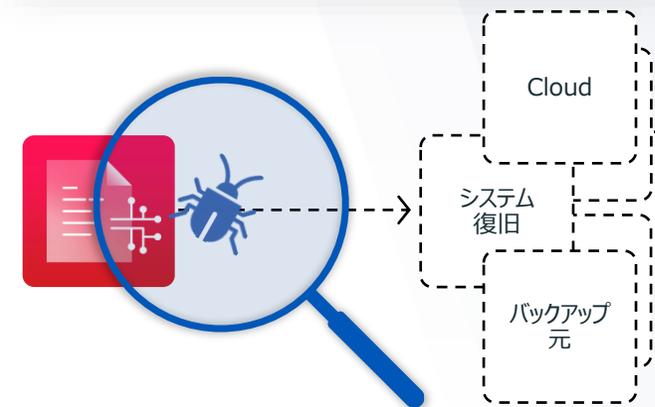
普段との保護状況の違いを
異常検出

バックアップ完了後



リスクの高いまたは疑わしい
バックアップデータの
マルウェア手動検出

リストア前



リストア前に感染していないこと
を確認

異常検出スコアが高い場合、マルウェア検出が自動起動

Agenda

1. バックアップ元データの異常検出
2. バックアップデータ上のマルウェア検出
3. インフラ・バックアップ状況の検出・可視化
 - 3-1. バックアップ状況の可視化
 - 3-2. 保護対象の自動検出&保護
4. まとめ

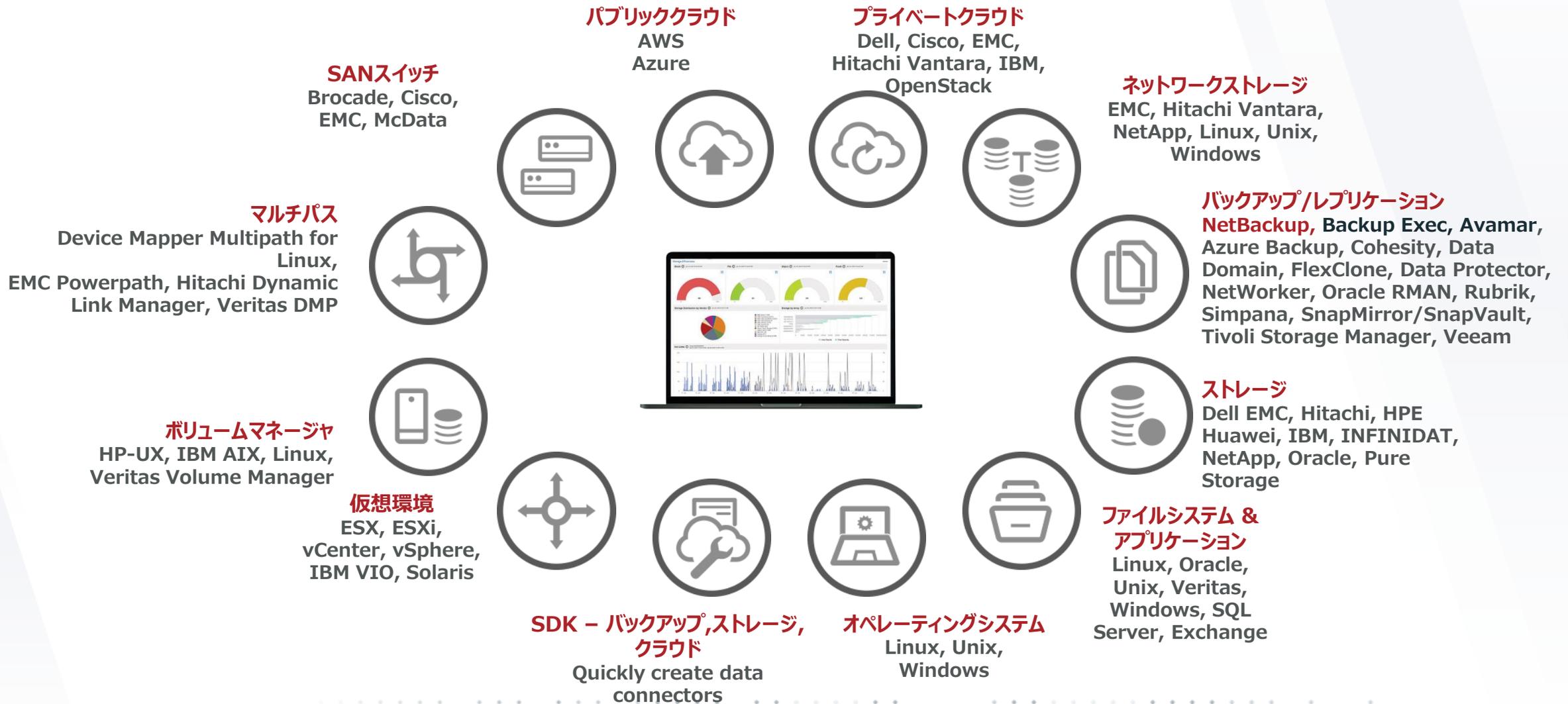
NetBackup IT Analytics とは？

バックアップ、ストレージ、クラウド向けのベンダーに依存しない IT分析プラットフォーム



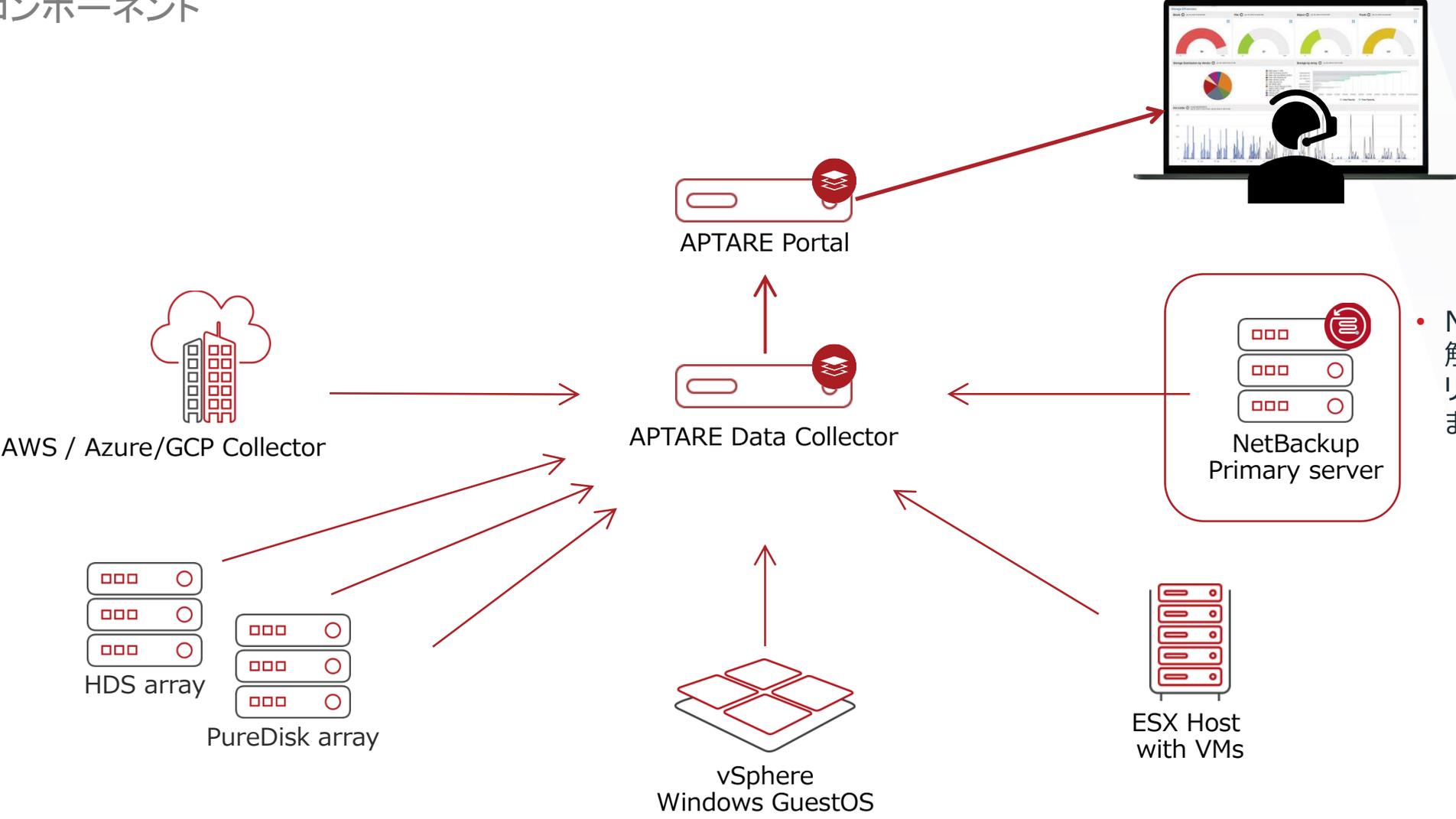
NetBackup IT Analyticsの守備範囲

検出・解析可能なITインフラ例



NetBackup IT Analytics

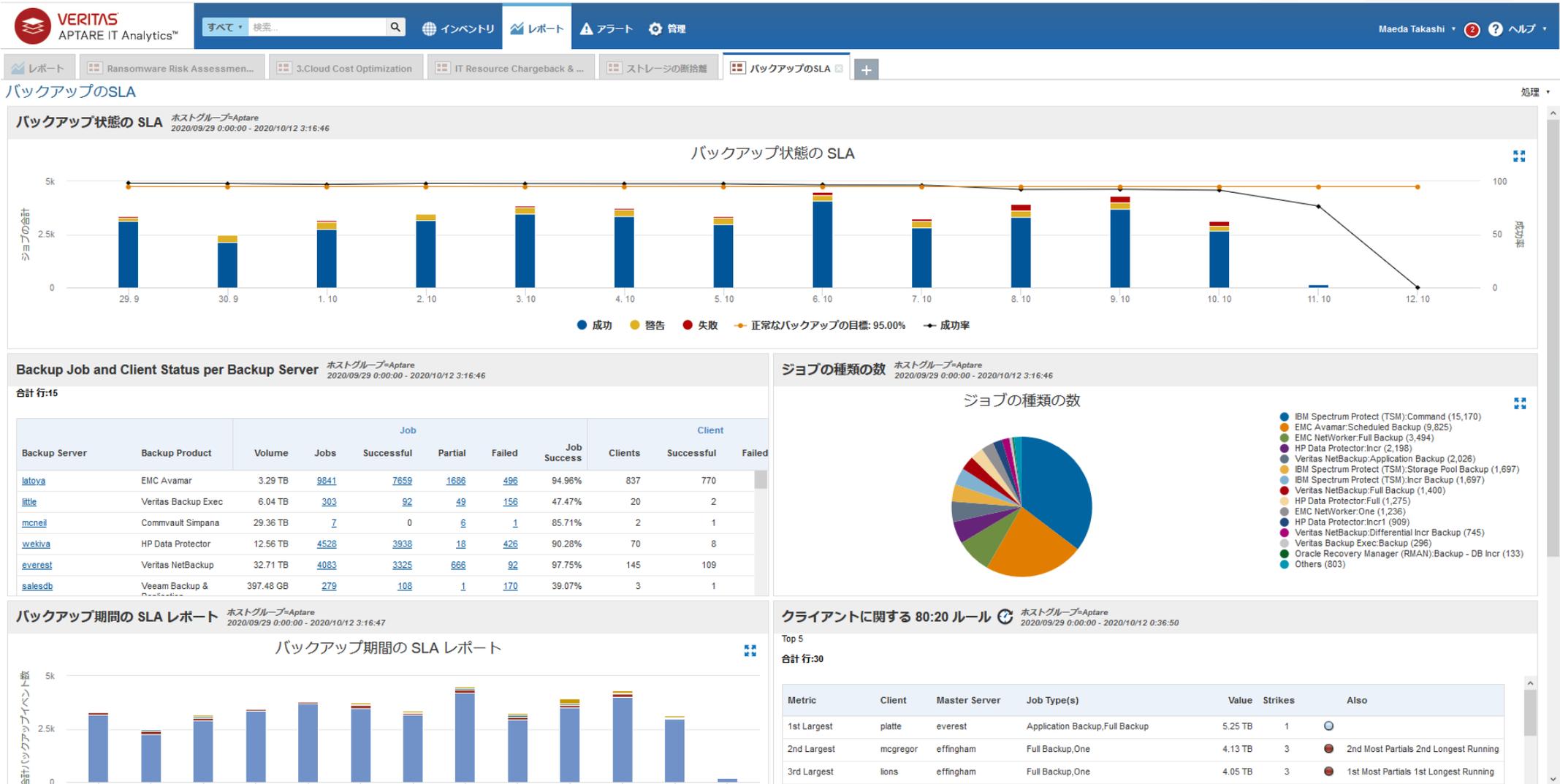
コンポーネント



- NetBackupの情報収集 & 解析はNetBackupサブスクリプションライセンスに含まれます。

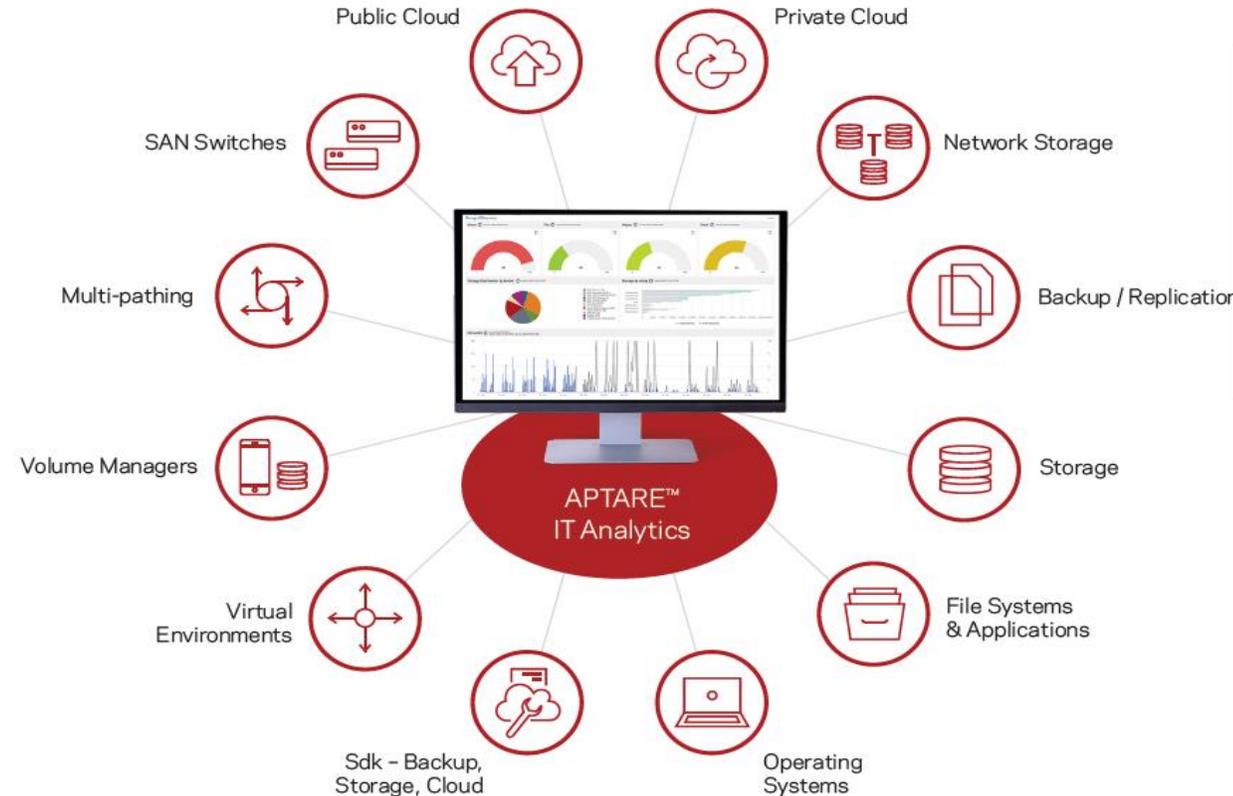
APTARE IT Analytics

ダッシュボード: データ保護のSLA分析



NetBackup IT Analyticsのデータ保護に関する効果

ハイブリッドクラウド環境をダッシュボードで把握



IT Analytics の効果

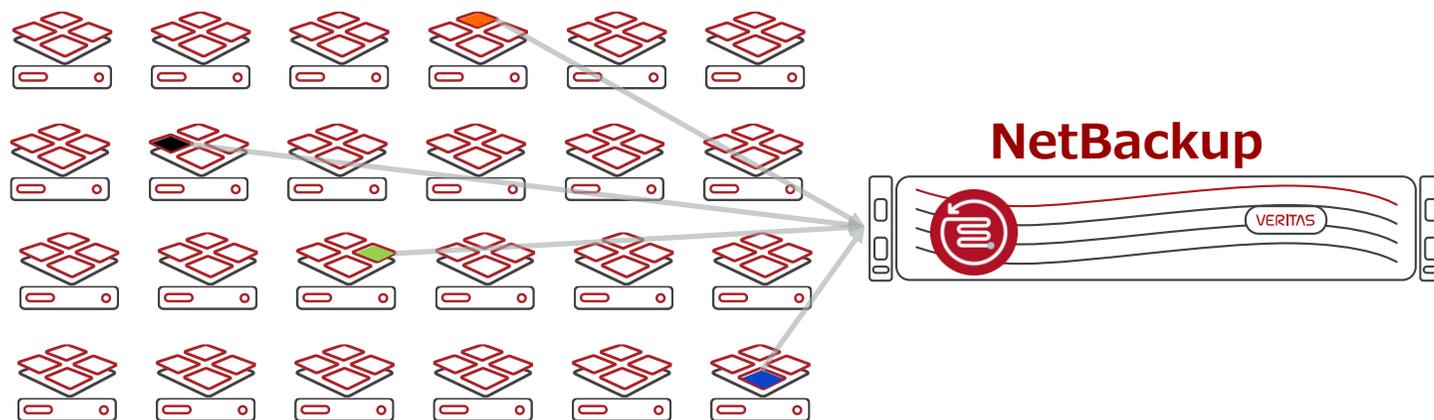
- 保護されていない資産がどこにあるかを表示しリスクを軽減化
- バックアップ状況を可視化し、失敗原因を分析➡成功率の向上
- ストレージ、クラウドテクノロジーを可視化
- プロアクティブに問題を特定

Agenda

1. バックアップ元データの異常検出
2. バックアップデータ上のマルウェア検出
3. インフラ・バックアップ状況の検出・可視化
 - 3-1. バックアップ状況の可視化
 - 3-2. 保護対象の自動検出&保護
4. まとめ

仮想マシンの自動検出&保護

VMインテリジェントグループ



- バックアップの取りこぼしが無い
 - ✓ タグや属性で自動検出
 - ✓ VM所有者とバックアップチーム間の調整を容易に
- VM保護の複雑さを解消
 - ✓ VM毎のバックアップ設定が不要
 - ✓ 主要なHyper visorで一貫した保護復旧操作
- インテリジェントVMグループを簡単に作成
 - ✓ タグや属性で条件指定
 - ✓ 保護プラン（保護サイクル・保持期間）にグループを登録
 - ✓ プレビュー、検証、カスタマイズ
 - ✓ RBAC適用で、特定のユーザが特定条件のVMを保護・復旧

 VMware

 Nutanix AHV

 RHV

VMware自動検出設定例

増殖・移動するVMを**逃さず**自動バックアップ

Veritas NetBackup™

インテリジェント VM グループの追加

名前 *

Test-VM-Group

説明

説明を入力してください

仮想マシンの選択

VMware サーバー *

vcsa-67.katsuno.test

すべての VM を含める

instanceUid

networkName

powerState

tagName

次の値を含む

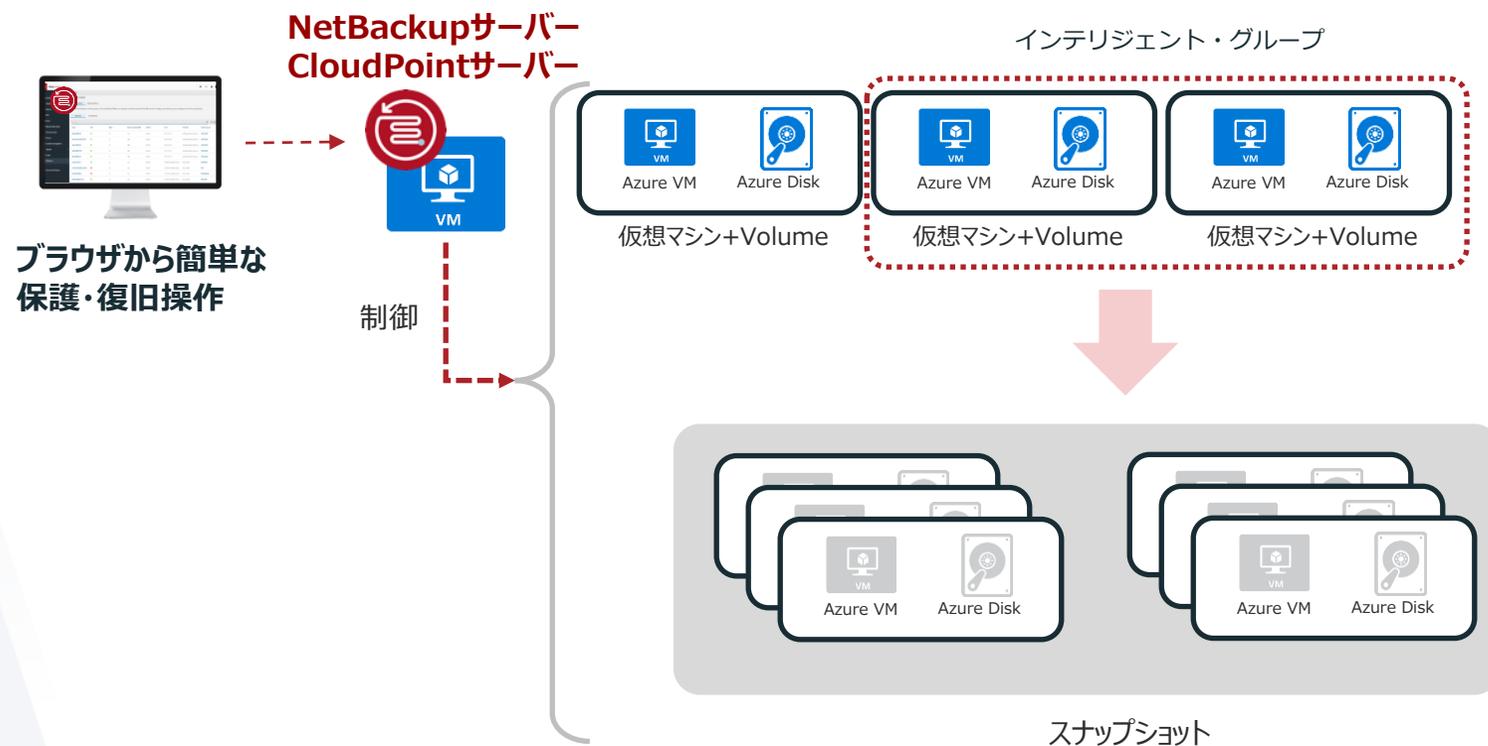
test

- 事前に設定のポリシーに従い、新しく作られたまたは移動したVMを**自動的に検出し確実にバックアップ**
- 大量VMも一括でバックアップ設定

例) tagNameにtestという文字列を含むすべてのVMをバックアップ

クラウドインスタンスの自動検出&保護

クラウド・インテリジェント・グループ



- バックアップの取りこぼしが無い
 - ✓ タグや属性で自動検出
 - ✓ アプリの所有者とバックアップチーム間の調整を容易に
- クラウドデータ保護の複雑さを解消
 - ✓ VM毎のバックアップ設定が不要
 - ✓ すべての主要なクラウドで一貫した保護復旧操作
- クラウドインテリジェントグループを簡単に作成
 - ✓ タグや属性で条件指定
 - ✓ 保護プラン（保護サイクル・保持期間）にグループを登録
 - ✓ プレビュー、検証、カスタマイズ
 - ✓ RBAC適用で、特定のユーザが特定条件の資産を保護・復旧

Azure Stack

Microsoft Azure

aws

Google Cloud

条件によるグループ設定で大量インスタンスも一括保護

増殖・移動するインスタンスを逃さず自動バックアップ

Veritas NetBackup™

ダッシュボード
アクティビティモニター
リカバリ
保護
保護計画
ポリシー
作業負荷
Oracle
Microsoft SQL Server
VMware
RHV
クラウド
Nutanix AHV
OpenStack
Kubernetes
ストレージ

Add intelligent group

Name *
demo-group

Description
this is for demo

Select assets

Provider *
Amazon AWS

Account ID *
veritas-cloudpoint (165323042987)
Account ID corresponds to Subscription ID for Azure, Account ID for AWS, and Project ID for GCP.

Location *
us-east-2
Location corresponds to Region for Azure, Region for AWS and Zones in GCP.

Asset type
 Virtual machine Application
 Include all assets of the selected type

AND OR

displayName Starts with cloudpoint

tagName Ends with dnd

Preview VMs

Search...

Name

- cloudpoint-demo-viveksatpute-21-04-08-dnd
- cloudpoint-swapnilgaikwad-21-04-07-171507-dnd
- cloudpoint-DONOT_STOP_vivek-rhel83-ipv6-dualstack-dnd
- cloudpoint-santoshvispute-21-04-05-120705-dnd
- cloudpoint-swapnilgaikwad-21-04-06-135506-dnd
- cloudpoint-reenarawat-21-04-06-132214-dnd
- cloudpoint-reenarawat-21-04-06-dnd
- cloudpoint-vishaljoshi-new_dnd
- cloudpoint-viveksatpute-rhel78-dnd

Showing 1-9

Close

Preview

+ Condition + Sub-query

Cancel Add and Protect Add

Agenda

1. バックアップ元データの異常検出
2. バックアップデータ上のマルウェア検出
3. インフラ・バックアップ状況の検出・可視化
 - 3-1. バックアップ状況の可視化
 - 3-2. 保護対象の自動検出&保護
4. まとめ

まとめ

- バックアップ状況から業務サーバのランサムウェア被害の可能性を**検出**
 - 手遅れになる前に初動確認を促す
- バックアップデータからマルウェアを**検出**
 - 感染が疑われるホストのバックアップデータをスキャン・チェック
 - 重要な業務システムへのリストア実行前にスキャン・チェック
- IT環境全体の状況を**検出**、可視化、分析、最適化
 - 保護されるべき業務の保護漏れ確認
 - バックアップが失敗せずに稼働していることの確認
- 保護対象を自動**検出**
 - 抜け漏れのない確実な保護

Veritasの検出技術で確実・安全な保護復旧を！

Veritas Solution Day 2022

VERITAS™

ありがとうございました

Copyright © 2022 Veritas Technologies, LLC. All rights reserved.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.