Enterprise Strategy Group | Getting to the bigger truth.™

Validation technique

Cybersécurité avec Veritas

Protection contre les ransomwares Veritas

Par Craig Ledo, IT Validation Analyst

Septembre 2022

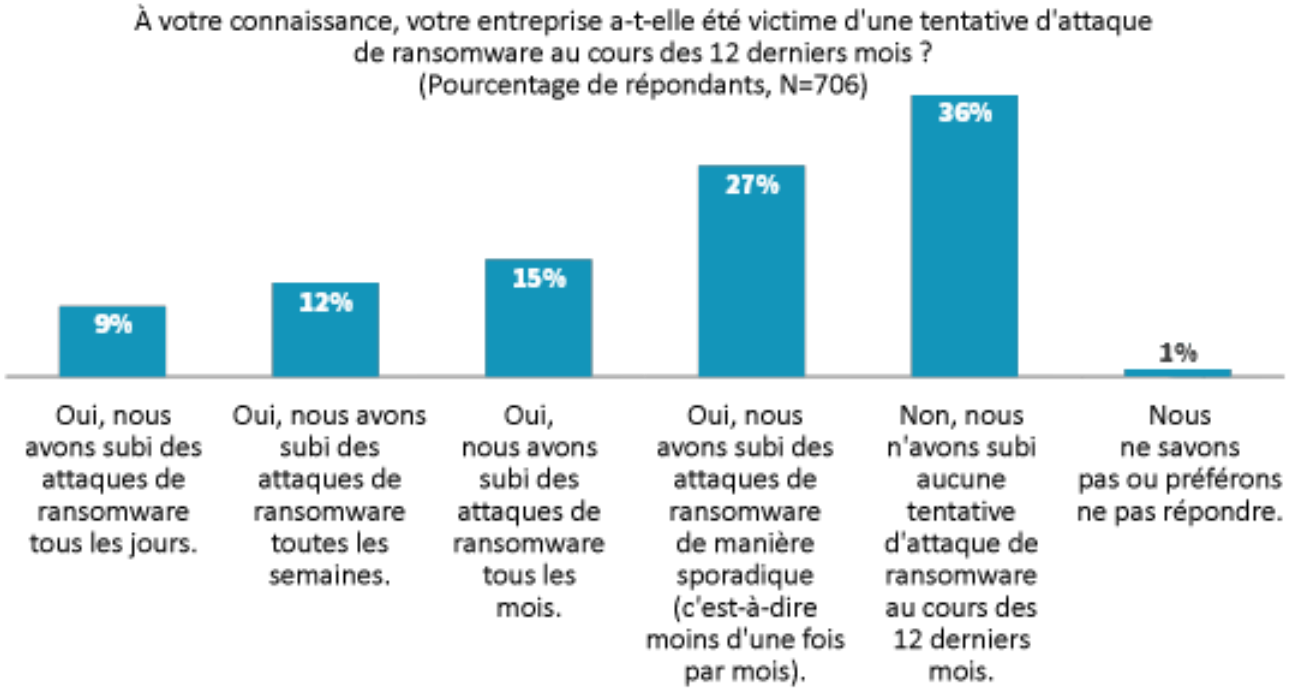
Introduction

Cette validation technique d'ESG documente l'évaluation détaillée de la solution Veritas pour la cybersécurité, notamment la protection des données, la détection des menaces et la restauration à grande échelle. Plus précisément, cette évaluation a consisté à valider 12 scénarios de test dans l'ensemble du portefeuille de solutions de cybersécurité de Veritas.

Contexte

Les attaques de ransomware continuent d'être une priorité pour les chefs d'entreprise et les responsables informatiques, et pour de bonnes raisons. Elles compromettent l'accès aux données de l'entreprise. Les attaques continues de ransomwares ont entraîné des coûts considérables pour les entreprises, notamment en raison des temps d'arrêt, des baisses de productivité, des coûts pour les appareils et pour les réseaux, des opportunités perdues, des rançons payées, des pertes de valeur de la marque, etc. Malgré les millions de dollars dépensés chaque année pour protéger les points d'entrée des données, de nombreuses entreprises sous-estiment toujours la valeur stratégique de la protection des données. D'après l'étude d'ESG, les entreprises de 36 % des personnes interrogées ont subi de telles attaques au moins une fois par mois au cours des 12 derniers mois. 9 % ont été ciblées quotidiennement et 12 % ont été attaquées chaque semaine (voir Figure 1).[1]

Figure 1 : Les attaques récurrentes de ransomware sont courantes



Source : ESG, une division de TechTarget, Inc.

27 % des personnes interrogées ont également subi des attaques de ransomware de manière plus sporadique. Il est donc essentiel que les entreprises mettent en œuvre des mesures proactives et défensives solides contre les attaques de ransomware afin de les empêcher d'atteindre leur but, d'autant plus que les victimes risquent d'être à nouveau ciblées par ces criminels.

[1] Source : Étude ESG, *Enquête sur les intentions de dépenses technologiques en 2022*, novembre 2021.

En outre, les demandes deviennent excessives et le risque de perte de données augmente. Une stratégie de résilience avancée à plusieurs niveaux est donc nécessaire pour garantir la sécurité, la résilience et la restauration des services informatiques, tout en offrant une expérience fluide à l'utilisateur final. Par exemple, les solutions qui ont été renforcées d'un point de vue logiciel et matériel et qui prennent en charge le stockage immuable (qui ne peut pas être modifié) et indélébile (qui ne peut pas être supprimé) contribuent à fournir une stratégie de cybersécurité complète à plusieurs niveaux.

Présentation de la solution de cybersécurité de Veritas

Veritas offre une approche unifiée et multiniveau sous forme de plate-forme qui intègre en toute transparence la protection proactive, la détection, la sauvegarde et la restauration. Plus précisément, Veritas fournit aux entreprises un modèle de sécurité « zéro confiance », qui leur permet de mettre en œuvre un meilleur contrôle d'accès, de contenir les fuites, de protéger les actifs et de limiter les dommages potentiels.

Protection :

- Assure la protection des données critiques et de l'infrastructure informatique contre l'inconnu et les imprévus en veillant à ce que toutes les parties de l'environnement soient sauvegardées avec une protection universelle appliquée intelligemment et gérée automatiquement pour s'adapter correctement.
- L'infrastructure de sauvegarde et les données sauvegardées permettent aux entreprises d'élever l'infrastructure de sauvegarde et de restauration au rang de composante essentielle du succès de la résilience.
- Veritas NetBackup offre une prise en charge de la périphérie jusqu'au cœur, en passant par le cloud, avec plus de 800 sources de données, plus de 1 400 fournisseurs de stockage et plus de 60 fournisseurs de cloud, de sorte que les environnements les plus exigeants et les plus variés peuvent être protégés.
- Les politiques intelligentes de Veritas apportent des niveaux d'automatisation accrus qui permettent aux administrateurs de gagner en efficacité.
- Veritas fournit une solution isolée physiquement pour protéger l'intégrité des données, afin de garantir que les fichiers de sauvegarde restent en sécurité et ne sont pas modifiés par des personnes malveillantes.
- Les images de sauvegarde sont immuables et indélébiles grâce à un horloge de conformité sécurisée gérée en interne.

Détection :

- Veritas propose des solutions qui offrent une visibilité totale sur l'infrastructure, afin de mettre en lumière toutes les données obscures dans l'environnement d'une entreprise.
- En outre, Veritas fait en sorte que les entreprises sachent que tout ce qui se trouve dans l'environnement est sécurisé et en mesure de surmonter la menace des ransomwares.
- Veritas propose également une détection des anomalies et des logiciels malveillants alimentée par l'IA pour les données principales et les données de sauvegarde, ainsi qu'une analyse de détection des logiciels malveillants déclenchée par des événements, qui permet d'agir avant les cybercriminels ou le code malveillant.

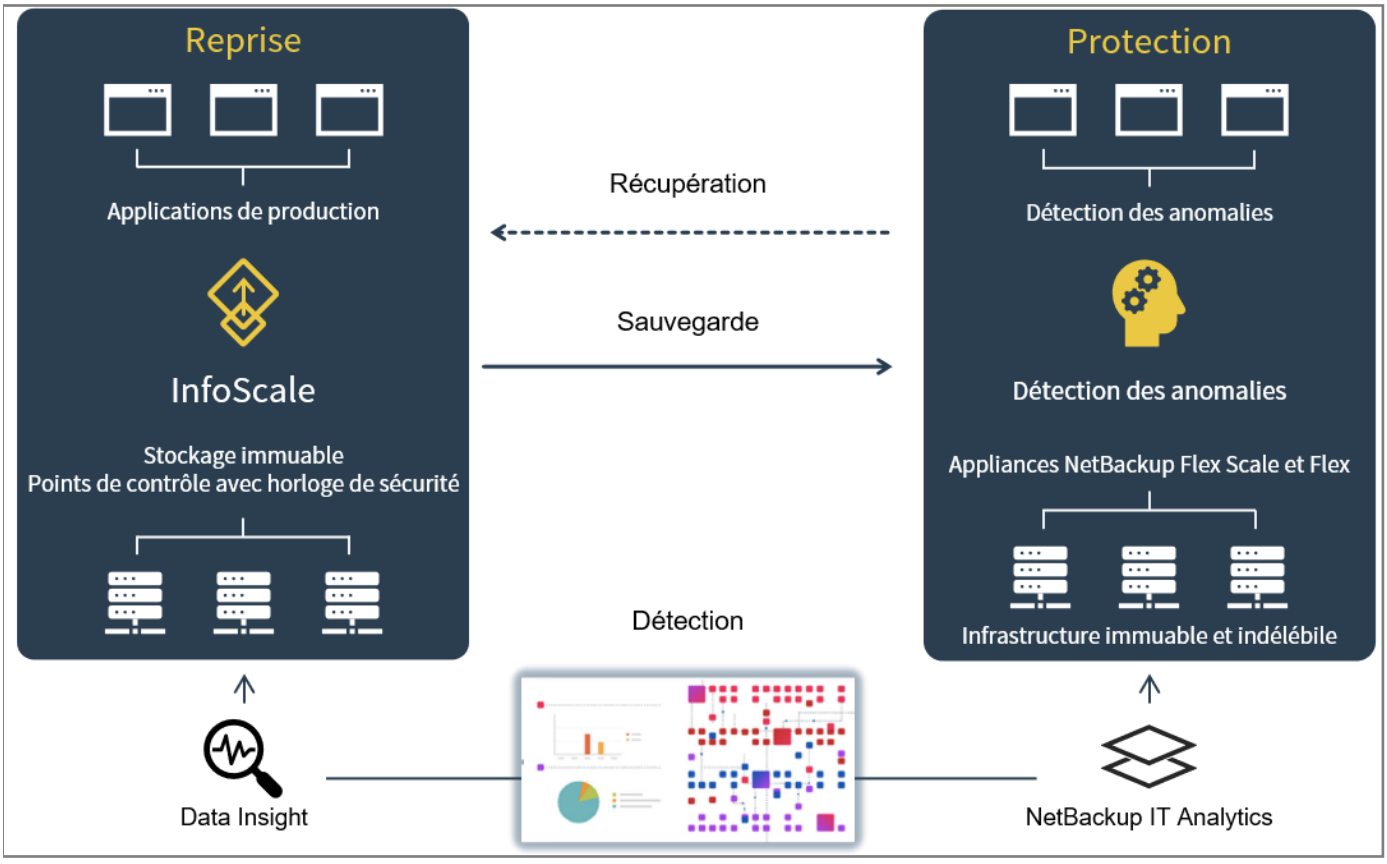
Restauration :

- Avec les solutions Veritas comme élément essentiel du succès de la résilience, les environnements sont optimisés pour la restauration.
- Veritas dispose de solutions de sécurité intégrées pour garantir la remise en ligne de données et d'environnements propres et exempts de ransomware.

- Parfois, tout est affecté, de sorte que les entreprises doivent récupérer un datacenter complet dans le cloud et à la demande.
- Il est également possible qu'une partie de l'environnement seulement soit affectée. Il est donc essentiel de disposer de solutions qui offrent la flexibilité nécessaire pour récupérer rapidement des bases de données et des fichiers individuels en production.
- Dans le cas où des serveurs entiers sont chiffrés, les entreprises peuvent avoir besoin de récupérer rapidement ces serveurs ailleurs.
- Les entreprises peuvent simplement avoir besoin de remettre en production un grand nombre d'instances d'applications.
- Veritas fournit des solutions de restauration à toutes les échelles, y compris la restauration orchestrée et la récupération en masse.

Les solutions Veritas garantissent que les données sont toujours disponibles et protégées, contribuent à la haute disponibilité des applications et assurent une restauration à toutes les échelles. Veritas aborde la résilience contre les ransomwares à travers le prisme de la valeur commerciale. Elle fournit une stratégie de résilience robuste en offrant la protection, la détection et la restauration contre les ransomwares (voir Figure 2).

Figure 2 : Présentation de la solution de cyber-résilience de Veritas



Source : ESG, une division de TechTarget, Inc.

Validation technique ESG

ESG a effectué une validation technique de la solution de cybersécurité de Veritas, y compris la protection des données, la détection des menaces et la restauration à grande échelle.

Protection des données

Veritas propose un large éventail de contrôles de sécurité pour contribuer à la protection des données, notamment :

- **Gestion des identités et des accès :** accès basé sur les rôles, authentification unique et authentification personnalisable.
- **Chiffrement des données :** en transit et au repos.
- **Gestion et stockage des images immuables :** gestion des images flexible et indépendante du stockage et stockage des images WORM (non réinscriptible).
- **Renforcement de la solution :** NetBackup Flex et NetBackup Flex Scale ont été renforcés d'un point de vue logiciel et matériel pour offrir une solution sécurisée complète prenant en charge le stockage immuable.

Plus précisément, ESG a validé les capacités clés suivantes en matière de protection des données.

Immuabilité des données cloud

La solution garantit que les données ne peuvent pas être modifiées pendant une durée déterminée pour les protéger contre les intrusions cybercriminelles et les menaces internes. Pour améliorer encore davantage la sécurité, le stockage de sauvegarde se fait sur un stockage de données sécurisé qui n'est visible et accessible que par le service de stockage NetBackup, ce qui empêche les utilisateurs et les services de systèmes de fichiers d'y accéder.

Impénétrabilité renforcée

L'ensemble de la pile d'appliances NetBackup a été renforcé en matière de sécurité, y compris le système d'exploitation Linux, l'accès à la gestion, les binaires d'application et les paramètres de configuration. Il comprend des politiques de sécurité propriétaires conformes aux directives STIG et applique un contrôle d'accès obligatoire. Il comprend également des services de détection et de protection contre les intrusions qui limitent l'accès aux processus et aux ressources et conservent une piste d'audit des actions importantes des utilisateurs et du système.

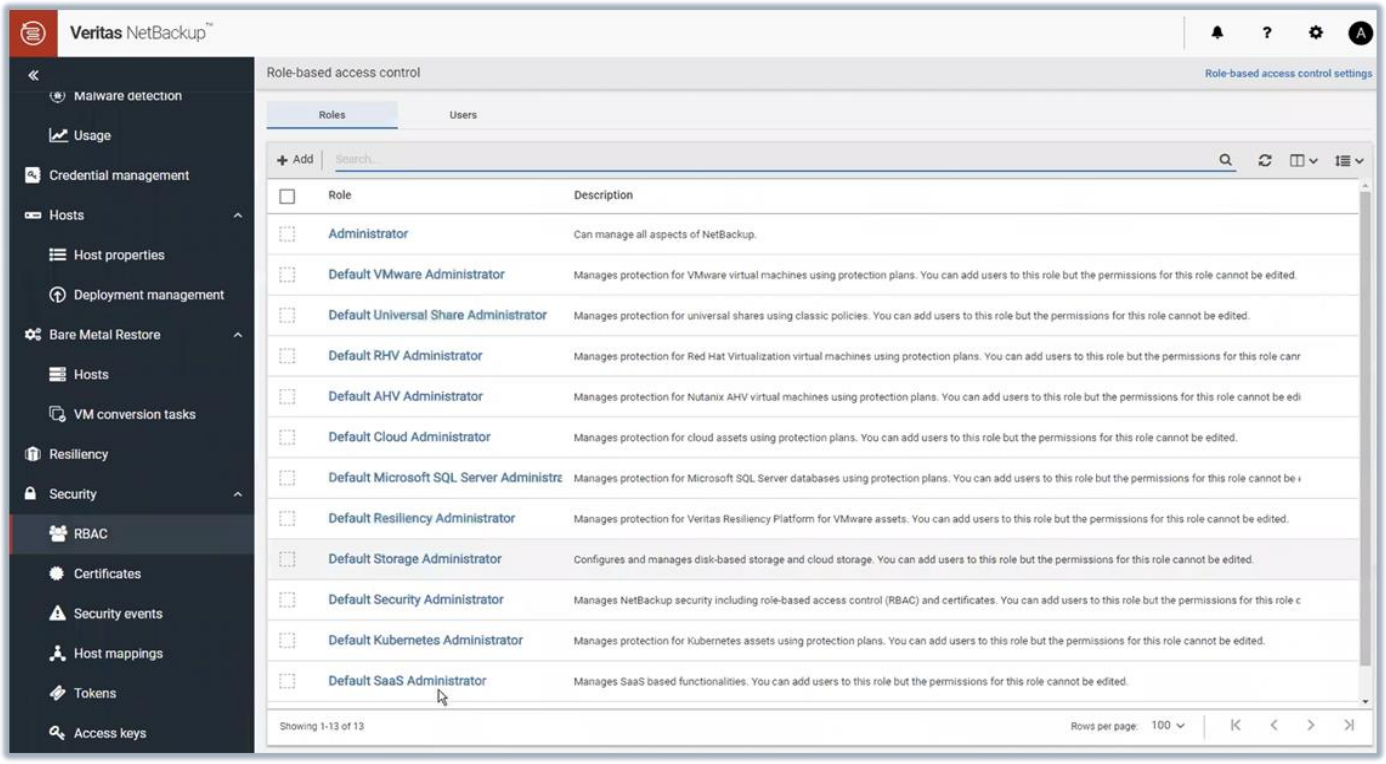
Matériel inviolable

Les appliances hébergeant un stockage immuable peuvent passer à un niveau de sécurité plus élevé pour protéger à la fois les données et l'infrastructure. Les administrateurs ne peuvent pas apporter de modifications au système d'exploitation et aux composants internes, tous les terminaux sont protégés contre les accès non autorisés et l'accès à tous les services est protégé et authentifié.

Contrôles d'accès sécurisés

La solution fournit des modèles de contrôle d'accès basé sur les rôles, comme illustré dans la Figure 3. Cela permet aux administrateurs de fournir facilement un accès ou des autorisations appropriés aux utilisateurs ou aux groupes d'utilisateurs. Les administrateurs peuvent également explorer chacun des modèles pour voir les autorisations détaillées (par exemple, gestion, protection, sécurité et stockage NetBackup). En outre, ils peuvent créer des accès ou des autorisations personnalisés pour les utilisateurs ou les groupes. En fonction du rôle personnalisé, les administrateurs peuvent également attribuer des charges de travail (par exemple, sélectionner les ressources de charge de travail que les utilisateurs peuvent gérer), des plans de protection (par exemple, sélectionner les plans de protection que les utilisateurs peuvent gérer) et des identifiants (par exemple, sélectionner les identifiants que les utilisateurs peuvent gérer).

Figure 3 : Contrôles d'accès sécurisés

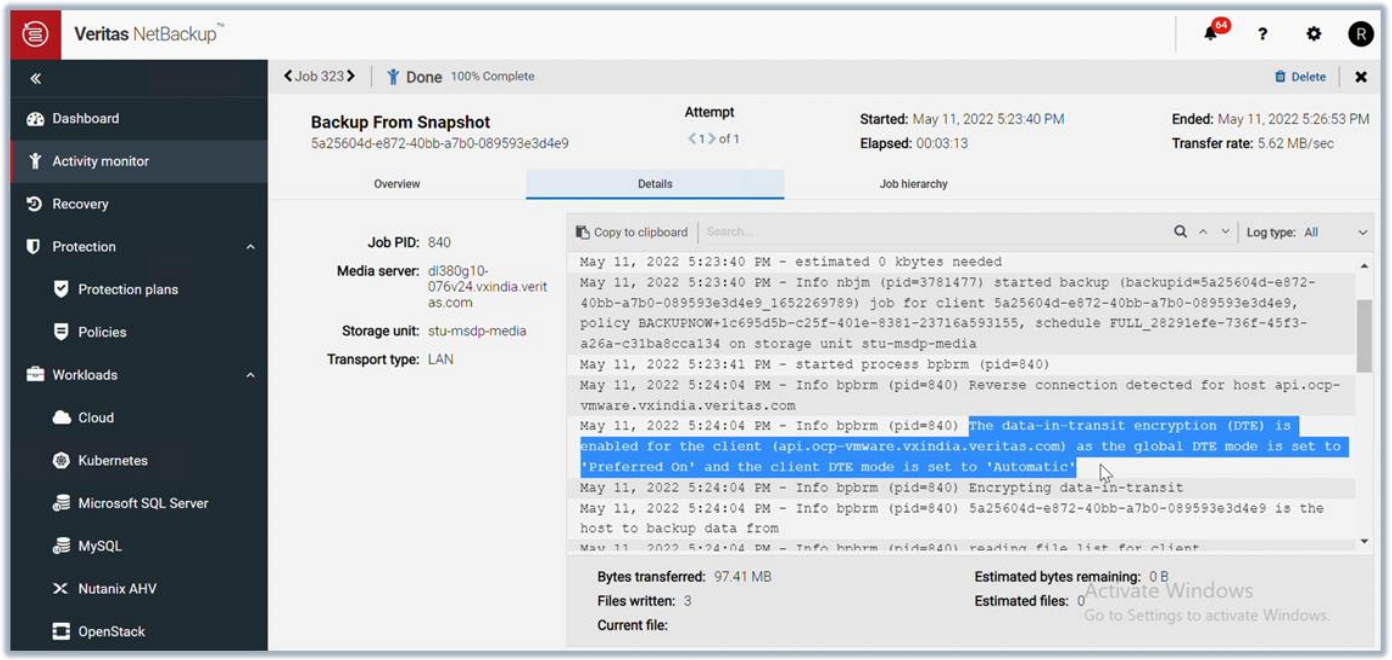


Source : ESG, une division de TechTarget, Inc.

Protection pour les infrastructures modernes

La solution offre des technologies de protection des données nouvelle génération pour les infrastructures modernes, notamment des bases de données Big Data, hyperconvergées ou open source MySQL/NoSQL. NetBackup permet aux entreprises de protéger leurs charges de travail multicloud, virtuelles, physiques et modernes, où qu'elles se trouvent, à partir d'une seule console. La Figure 4 présente une sauvegarde à partir d'un instantané. La sauvegarde a activé le chiffrement en transit des données (DTE) pour le client car le mode DTE global est défini sur « Preferred On » et le mode DTE client est défini sur « Automatic ». Les utilisateurs peuvent effectuer une restauration, si nécessaire, à partir de cette sauvegarde, le mode DTE étant activé, car le mode DTE de l'image de sauvegarde est « On ».

Figure 4 : Protection des infrastructures modernes



Source : ESG, une division de TechTarget, Inc.

Pourquoi est-ce important ?

À mesure que les attaques de ransomware évoluent et deviennent plus sophistiquées, il est important pour les entreprises de s'adapter facilement à l'évolution rapide des vecteurs de menaces pour éviter les temps d'arrêt de service et les pertes de données. La protection avancée des données et les appliances sécurisées de Veritas offrent plusieurs fonctionnalités pour lutter contre les ransomwares, telles que la détection intégrée des anomalies, l'analyse des logiciels malveillants, une architecture « zéro confiance » et un stockage immuable et indélébile.

Détection des menaces

Veritas propose un large éventail de contrôles de sécurité pour aider à détecter les menaces, notamment :

- Visibilité sur la sauvegarde et le stockage : NetBackup IT Analytics fournit une surveillance de la sauvegarde de bout en bout qui comprend l'analyse de la réduction des risques, les sources avec des échecs consécutifs, les sources sans sauvegarde récente et les échecs de sauvegarde par application.
- Détection des anomalies : NetBackup fournit une détection des anomalies alimentée par l'IA qui détecte les données inhabituelles dans l'ensemble de l'environnement et fournit des alertes sur les anomalies suspectes en temps quasi réel.
- Détection du stockage principal : Veritas traite les données de sauvegarde secondaire avec NetBackup et les données de stockage principal avec Veritas Data Insight, qui complète les outils de détection de sécurité existants en fournissant une détection des comportements anormaux dans le contexte de l'utilisateur et des données en temps quasi réel, des modèles de requête personnalisés spécifiques aux ransomwares et une identification des extensions de fichiers utile pour la détection des ransomwares.

- **Détection des logiciels malveillants :** Veritas fournit à la fois des analyses automatisées et à la demande pour les sauvegardes protégées. La fonction d'analyse automatisée de détection des logiciels malveillants supprime les dépendances humaines et permet à la technologie d'intelligence artificielle/apprentissage machine (IA/ML) d'intervenir et de rechercher les logiciels malveillants.

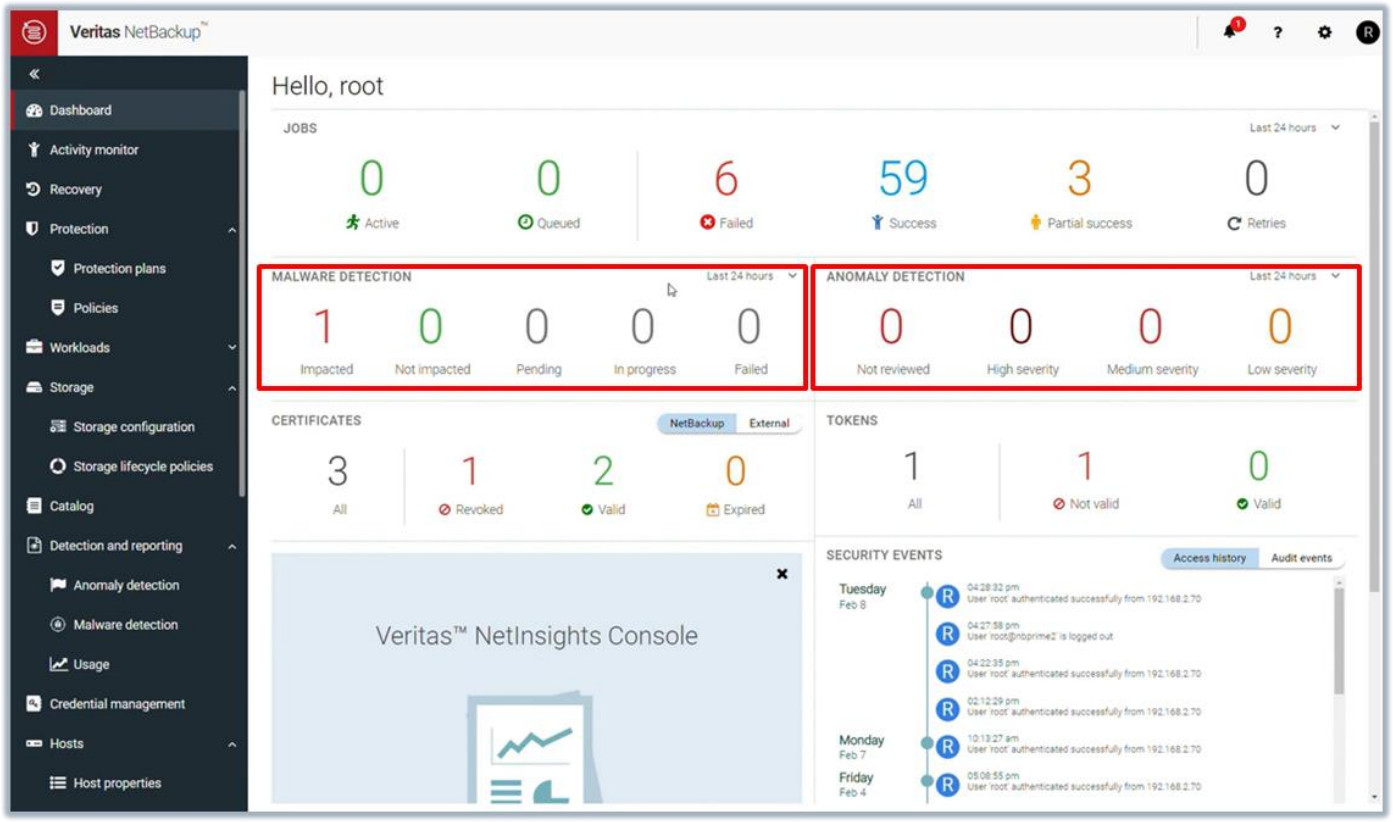
Plus précisément, ESG a validé les capacités clés suivantes en matière de détection des menaces.

Analyse intégrée de détection des logiciels malveillants et détection des anomalies

La détection d'anomalies suit les métadonnées des images séparément de la détection des logiciels malveillants, mais cette dernière peut tirer parti des résultats de la détection des anomalies. Les événements de détection de logiciels malveillants sont triés selon les catégories suivantes : Affecté, Non affecté, En attente, En cours et Échec, en fonction des « 24 dernières heures », comme le montre la Figure 5. Le délai peut également être configuré sur les « 48 dernières heures » ou les « 72 dernières heures ». Les utilisateurs peuvent explorer chaque domaine (par exemple, Affecté) pour afficher plus de détails. Pour chaque image de sauvegarde affectée, les utilisateurs peuvent prendre des mesures, y compris l'expiration de toutes les copies ou l'affichage des fichiers infectés. Le tableau de bord de détection des logiciels malveillants fournit les informations suivantes : Client, Temps de sauvegarde, Résultat d'analyse, Type de sauvegarde, Date d'analyse, Scanner d'applications malveillantes, Nombre de fichiers affectés, Nom d'hôte d'analyse et ID de sauvegarde. Le temps d'analyse de détection des logiciels malveillants varie en fonction de plusieurs facteurs, notamment la taille de l'image et le nombre de fichiers.

Les événements de détection d'anomalies sont triés selon les catégories suivantes : Non examiné, Gravité élevée, Gravité moyenne et Gravité faible, en fonction des « 24 dernières heures », comme le montre la Figure 5. Le délai peut également être configuré sur les « 48 dernières heures », les « 72 dernières heures » ou les « 7 derniers jours ». Les utilisateurs peuvent également filtrer le statut d'examen (Non examiné, Faux positif, Anomalie, Ignoré) et la gravité des anomalies (Élevée, Moyenne, Faible). Le tableau de bord de détection des anomalies fournit les informations suivantes : ID de tâche, Nom du client, Type de politique, Nombre, Score, Gravité de l'anomalie, Résumé de l'anomalie, Reçu, Statut d'examen, Nom de la politique, Nom de la planification et Type de planification. Les utilisateurs peuvent prendre les mesures suivantes concernant les anomalies : Marquer comme ignoré, Confirmer comme anomalie et Signaler comme faux positif.

Figure 5 : Analyse intégrée de détection des logiciels malveillants et détection des anomalies



Source : ESG, une division de TechTarget, Inc.

Rapports et alertes

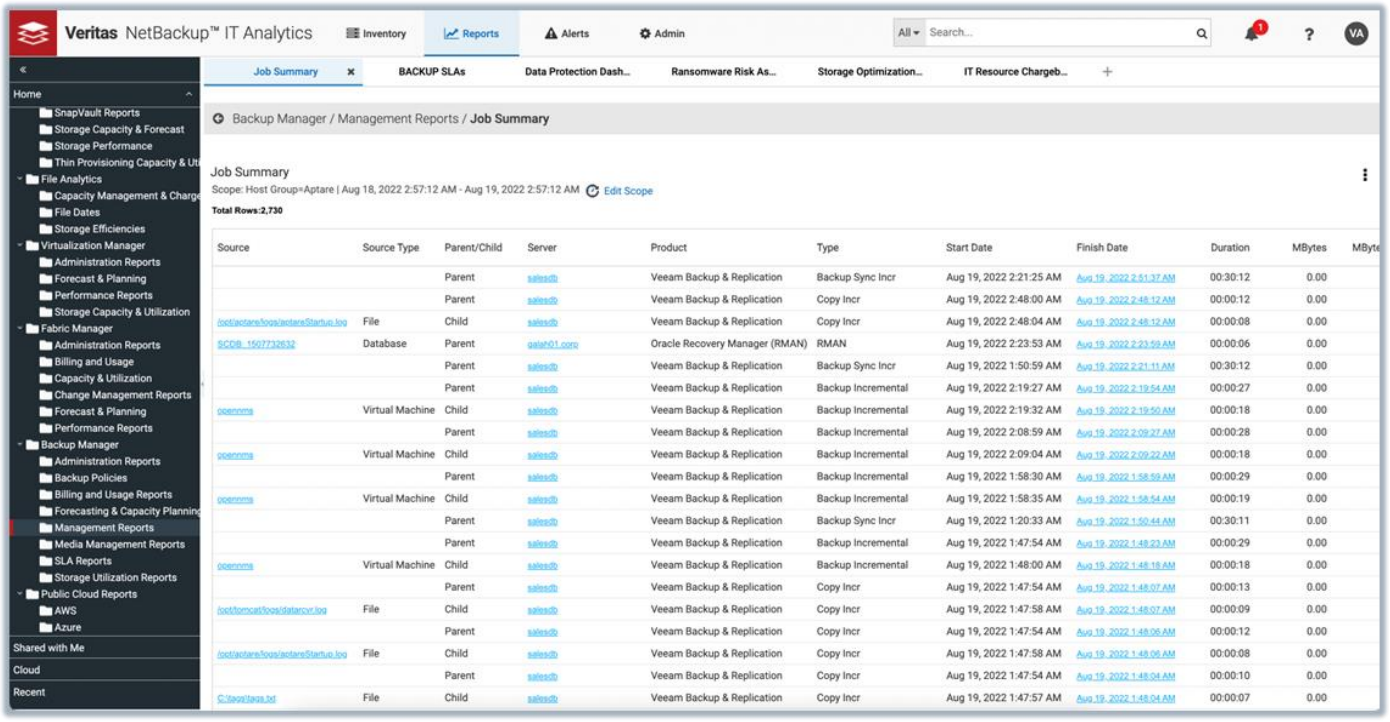
Veritas NetBackup IT Analytics fournit un tableau de bord d'évaluation des risques de ransomware prêt à l'emploi. Le tableau de bord offre aux utilisateurs une vue rapide des rapports prédéfinis qui utilisent l'analyse prédictive pour comprendre les risques potentiels au sein d'un environnement de sauvegarde (voir Figure 6). Les analyses aident les utilisateurs à s'assurer que l'environnement de sauvegarde est à la fois optimisé et sécurisé en fournissant des rapports complets sur plusieurs points de données, notamment :

- **Découverte :** les utilisateurs peuvent suivre toutes les modifications au sein de l'environnement de sauvegarde pour aider à détecter les ransomwares et à réagir rapidement. Plus de 850 extensions de ransomware connues sont prises en charge.
- **Visualisation des risques :** des graphiques intuitifs donnent aux utilisateurs une vue historique de tous les risques générés dans l'environnement, signalent les hôtes absents de la planification de sauvegarde et permettent de visualiser les applications dont les sauvegardes ont échoué.
- **Surveillance des sauvegardes :** les utilisateurs peuvent surveiller et identifier les modifications au sein de l'environnement de sauvegarde grâce à des graphiques récapitulatifs qui fournissent des informations exploitables. Les utilisateurs peuvent également atténuer les risques en identifiant les anomalies à l'aide d'une baseline de sauvegardes réussies connues.

En plus de détecter les fichiers avec des extensions de ransomware connues, NetBackup IT Analytics permet aux utilisateurs d'organiser ces informations de manière significative afin que les utilisateurs puissent exécuter un plan d'action rapide. Les utilisateurs peuvent organiser les fichiers de ransomware détectés par hôte, emplacement avec le plus grand nombre de fichiers de ransomware, type d'extension de ransomware et propriétaire de fichiers.

NetBackup IT Analytics examine également les sauvegardes réussies pour identifier les faux positifs potentiels en comparant les sauvegardes historiques aux nouvelles sauvegardes et en identifiant les anomalies, telles que les modifications importantes de la durée des tâches, les modifications de la taille des images et/ou de la politique de configuration. Les utilisateurs ont ainsi l'assurance que les services informatiques essentiels sont protégés.

Figure 6 : Rapports et alertes



Source : ESG, une division de TechTarget, Inc.

Pourquoi est-ce important ?

Comme indiqué précédemment, les attaques de ransomware ont évolué pour devenir plus sophistiquées. Veritas offre une visibilité globale en temps réel sur l'état des applications et des données grâce à une détection des anomalies et à des informations personnalisées qui permettent d'identifier les infiltrations de logiciels malveillants dans les données principales et les données de sauvegarde.

Restauration à l'échelle

Veritas offre un large éventail de fonctionnalités pour favoriser la restauration à l'échelle, notamment :

- NetBackup Resiliency : fournit une orchestration automatisée dans l'ensemble de l'environnement hétérogène d'une entreprise, avec une expérience utilisateur cohérente et une visibilité sur les meilleures options de restauration en fonction des options disponibles.

- **Restauration instantanée de NetBackup pour VMware :** permet de restaurer des machines virtuelles à grande vitesse en utilisant le suivi des blocs de modification inversé pour identifier quels blocs uniques doivent être restaurés et appliquer uniquement ces modifications pour rétablir des machines virtuelles saines en quelques secondes.

- **VM Recovery :** fournit huit types de restauration pour une sauvegarde des machines virtuelles VMware, y compris la machine virtuelle complète, le VMDK individuel, le fichier et le dossier, l'application complète, l'accès instantané, le téléchargement de fichier, le GRT d'application et la conversion AMI.

- **Accès instantané pour MSSQL et VMware :** permet une restauration quasi instantanée des machines (par exemple, 1 600 machines virtuelles) sans attendre le transfert des données de la machine virtuelle à partir de la sauvegarde. Offre également la possibilité de tester ou de restaurer des machines virtuelles directement à partir du stockage de sauvegarde.

- **NetBackup CloudPoint :** utilise la technologie d'instantané conçue pour le cloud d'une manière indépendante des fournisseurs de cloud, ce qui permet de protéger facilement les infrastructures hybrides et multicloud.

- **Universal Share et Protection Points :** permet aux entreprises de provisionner un stockage protégé par déduplication sur le serveur NetBackup en tant que partages sécurisés, protégeant ainsi les bases de données ou autres charges de travail sans agent ni API de sauvegarde.

- **NetBackup Universal Shares for Oracle :** permet aux administrateurs de bases de données Oracle de démarrer des bases de données directement à partir du stockage d'une appliance NetBackup.

- **Archivage de conservation à long terme :** offre une solution rentable et durable qui intègre la déduplication et la compression des données, notamment l'utilisation d'un stockage d'objet et des clouds privés ou publics avec cette méthode. La restauration traditionnelle inclut la restauration granulaire d'un fichier spécifique, la restauration complète de serveur/d'application et la restauration de reprise après incident vers un autre emplacement sur site ou dans le cloud. Grâce à Veritas Resiliency Platform, les entreprises peuvent automatiser et orchestrer la restauration traditionnelle en appuyant sur un bouton, ce qui rationalise le processus de reprise après incident.

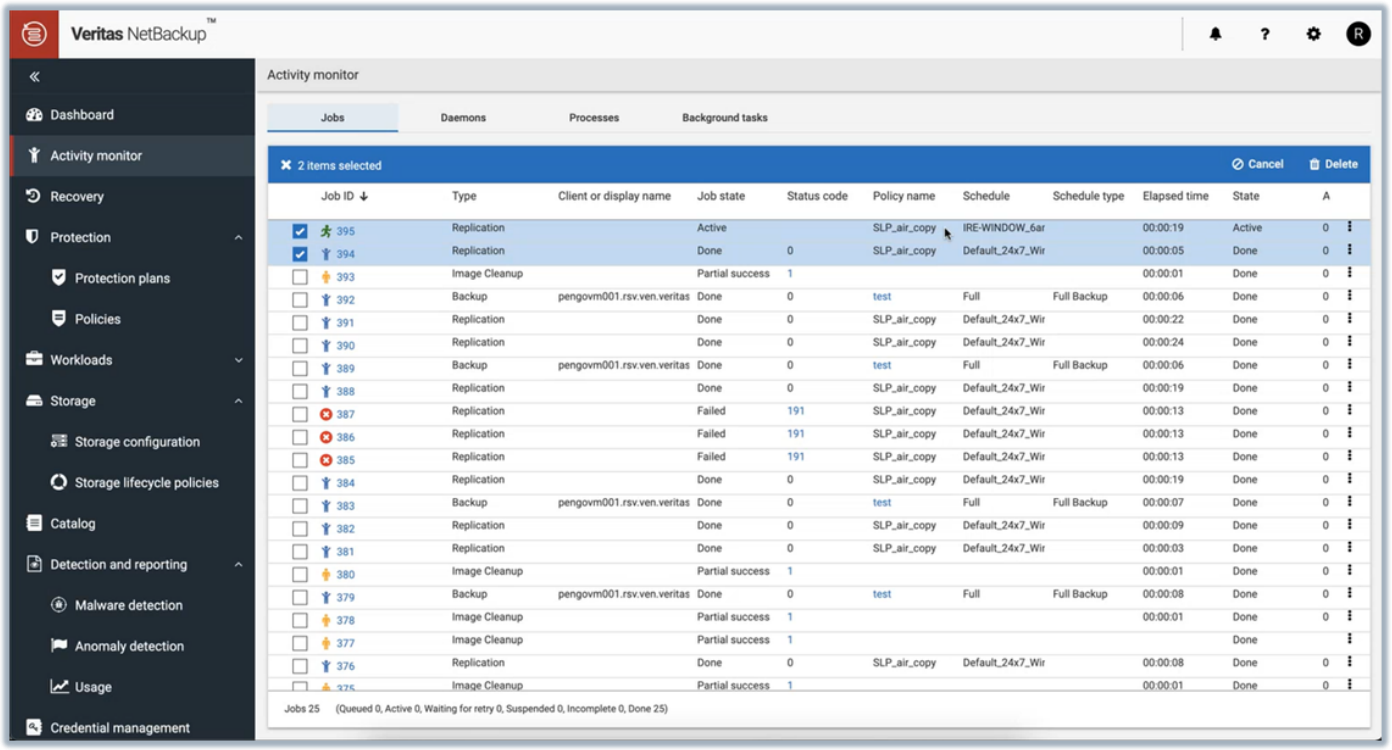
- **Bare Metal Restore :** automatise le processus de restauration de serveur, rendant inutile la réinstallation des systèmes d'exploitation ou la configuration manuelle du matériel. Permet aux entreprises de reconstruire rapidement des systèmes à partir de zéro, en restaurant le système d'exploitation et les données des applications en une seule opération.

Plus précisément, ESG a validé les capacités clés de restauration à grande échelle suivantes.

Environnement de restauration isolé

L'environnement de restauration isolé Veritas NetBackup permet d'établir des plans de restauration pour des milliers de machines virtuelles qui peuvent faire partie d'environnements complexes à plusieurs niveaux et d'exécuter des répétitions de ces mêmes machines dans un environnement isolé (voir Figure 7). Cette fonctionnalité peut fournir une prise en charge de l'immuabilité et de l'indélébilité intégrées, une immuabilité matérielle tierce, une immuabilité du stockage d'objet verrouillé dans le cloud et une immuabilité pour les sauvegardes de charges de travail SaaS. En outre, NetBackup peut envoyer directement et stocker efficacement des données dédupliquées sur AWS S3 Object Lock.

Figure 7 : Environnement de restauration isolé

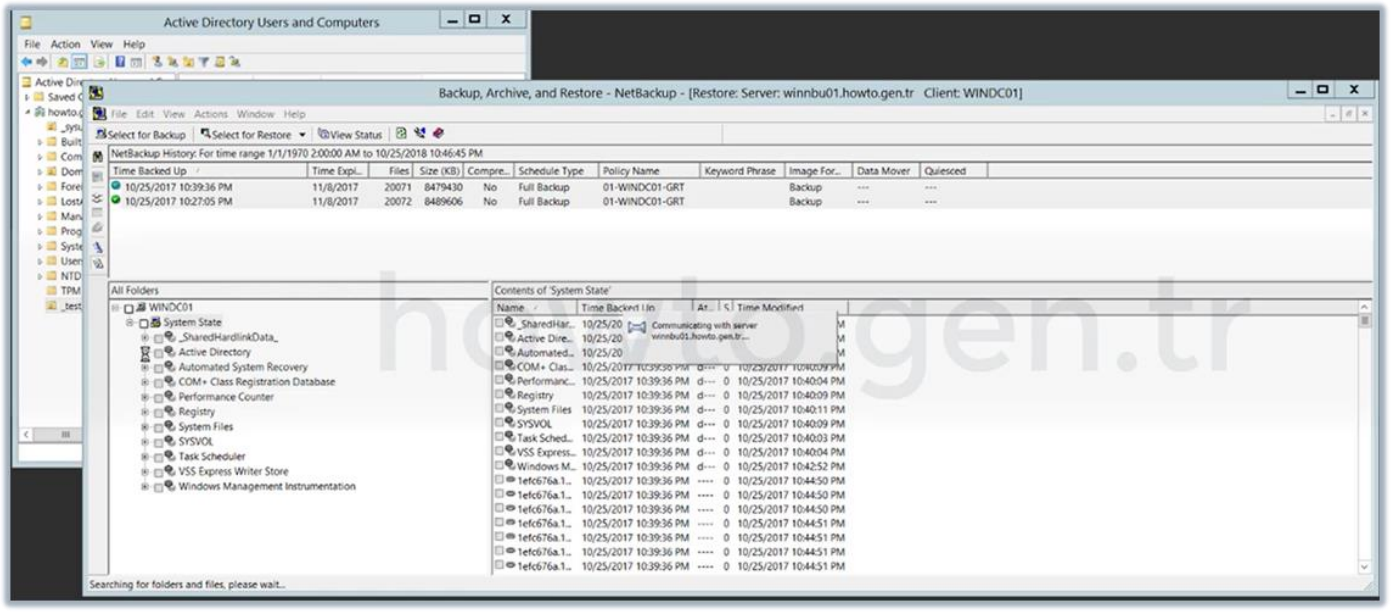


Source : ESG, une division de TechTarget, Inc.

Restauration de répertoire Active Directory perdu

La solution Veritas NetBackup permet de récupérer un répertoire Active Directory perdu en parcourant les sauvegardes Active Directory (voir Figure 8). Ensuite, l'utilisateur lance simplement la sauvegarde Active Directory appropriée. L'utilisateur peut également visualiser la progression de la restauration jusqu'à ce qu'elle indique que l'opération demandée a été effectuée.

Figure 8 : Restauration de répertoire Active Directory perdu

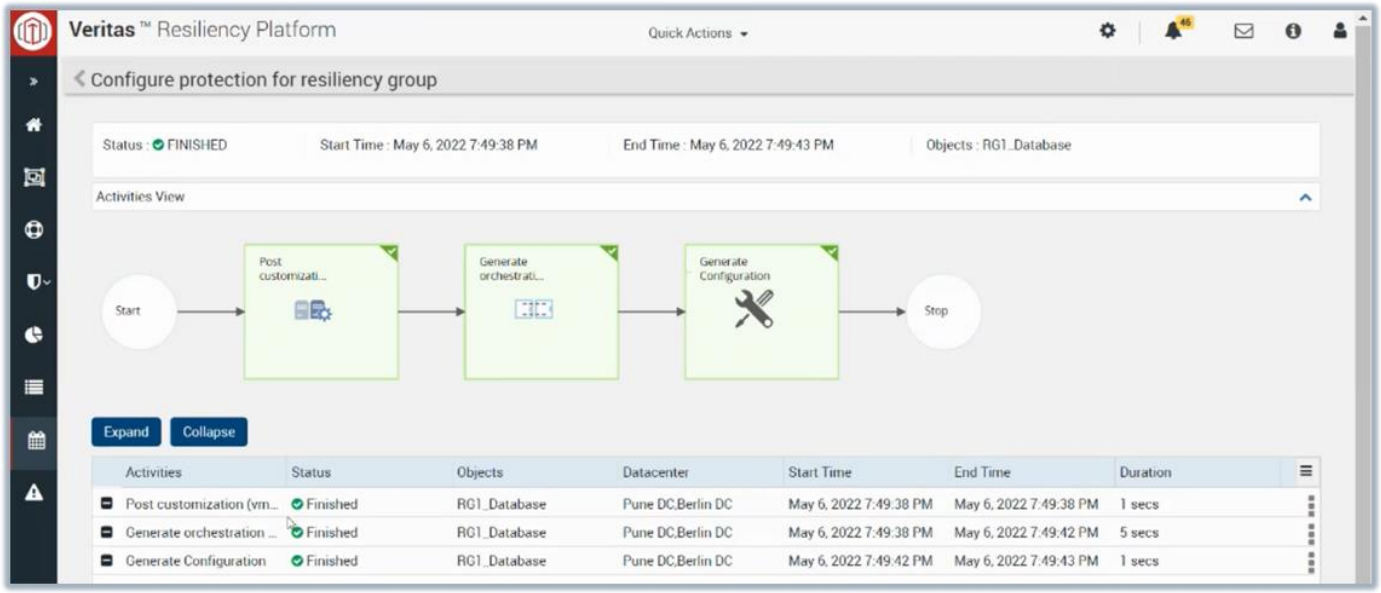


Source : ESG, une division de TechTarget, Inc.

Orchestration de restauration à plusieurs niveaux

Les services VBS (Virtual Business Services) de Veritas NetBackup Resiliency permettent aux utilisateurs de gérer la restauration des applications à plusieurs niveaux en tant qu'entité consolidée unique. Grâce aux services VBS, les utilisateurs peuvent automatiser complètement la restauration d'une application complexe à plusieurs niveaux, qui s'étend sur plusieurs systèmes. En cas d'attaque de ransomware, cela permet une récupération plus facile et plus rapide et un temps d'arrêt minimal des applications. Plus précisément, Veritas Resiliency Platform fournit une orchestration de la reprise à plusieurs niveaux, par exemple, en configurant la virtualisation et les clouds privés (par exemple, en ajoutant VMware vCenter), les serveurs principaux NetBackup, les réseaux (par exemple, par l'association de réseaux), les serveurs physiques, les bases de données, etc. Voir la Figure 9 pour la configuration de protection du groupe de résilience terminée.

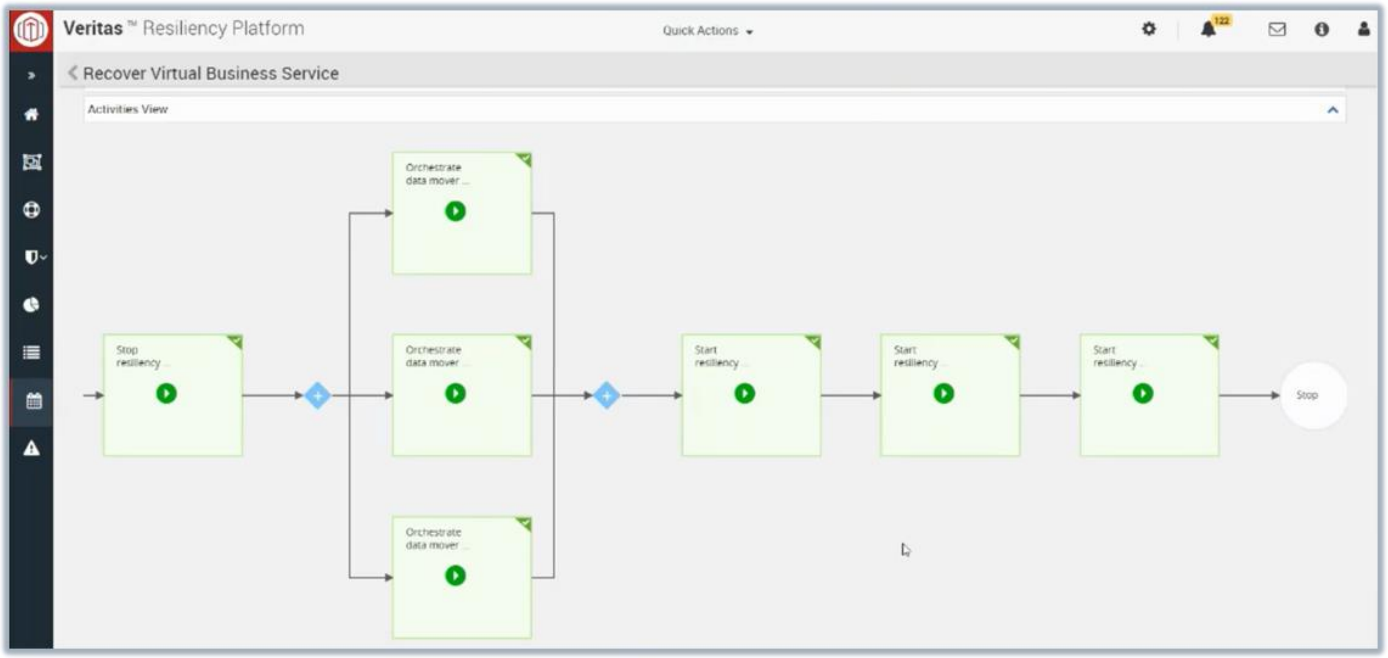
Figure 9 : Configuration de la restauration à plusieurs niveaux



Source : ESG, une division de TechTarget, Inc.

Une fois la configuration de protection du groupe de résilience terminée, l'utilisateur doit configurer le service VBS à plusieurs niveaux. Ensuite, l'utilisateur peut orchestrer la restauration à plusieurs niveaux du service VBS (voir Figure 10).

Figure 10 : Orchestration de restauration à plusieurs niveaux



Source : ESG, une division de TechTarget, Inc.

Pourquoi est-ce important ?

Face à l'augmentation des attaques de ransomware, il est important que les entreprises disposent d'une stratégie complète de résilience contre les ransomwares et de restauration. Veritas offre des capacités avancées de stockage et de restauration rapide pour les données principales avec des fonctionnalités intégrées de résilience, d'immuabilité et d'isolation des données qui garantissent la disponibilité des applications, ainsi que la sécurité et l'intégrité des données.

The Bigger Truth

Les ransomwares et les acteurs internes malveillants constituent de grandes menaces. On découvre constamment de nouvelles vulnérabilités dans les systèmes d'exploitation, et des variantes des malwares et ransomwares connus sont développées sans arrêt. Les ransomwares rapportent beaucoup, ce qui signifie que les pirates sont motivés pour innover et créer de nouvelles façons de pénétrer l'infrastructure d'une entreprise et l'immobiliser.

ESG a validé 12 scénarios de test de la solution Veritas pour la cybersécurité, y compris la protection des données, la détection des menaces et la restauration à l'échelle. Les stratégies de cybersécurité globales, complètes et à plusieurs niveaux constituent toujours la meilleure défense contre les temps d'arrêt et les pertes de données dues à l'infiltration de logiciels malveillants. Veritas comprend que cela peut être un défi complexe et a fourni une base pour aider les entreprises à protéger les services informatiques dans le cadre d'une stratégie globale de cybersécurité. La stratégie de cybersécurité de Veritas fournit aux entreprises les outils, les fonctionnalités et la confiance nécessaires pour garantir la haute disponibilité, la résilience et la protection des services informatiques contre les ransomwares.