VERITAS

Le guide complet des ransomwares avec Veritas

Livre Blanc | Janvier 2023

VERITAS ALTA™

Sommaire

Synthèse

Aujourd'hui, la cybersécurité et la menace des attaques par ransomware constituent des préoccupations majeures pour tous les secteurs d'activité dans le monde. Selon le 2022 SonicWall Cyber Threat Report, il y a eu 19 attaques par seconde, soit 623,3 millions d'attaques dans le monde. Il est désormais clair que le ransomware est le type de cybercriminalité qui connaît la croissance la plus rapide. Le ransomware en tant que service (RaaS) est devenu un modèle commercial organisé et lucratif, et les attaquants ne cessent de mettre au point des techniques créatives pour déjouer les mesures de sécurité les plus vigilantes. Les vieilles techniques comme le phishing sont toujours d'actualité, mais de nouvelles méthodes sophistiquées impliquant l'ingénierie sociale, ciblant les appareils et l'infrastructure de l'internet des objets (IoT), ainsi que les vulnérabilités logicielles, gagnent en popularité. C'est pourquoi il est essentiel que les équipes informatiques comprennent qu'elles ne peuvent pas parvenir à une véritable résilience face aux ransomwares par la seule sécurité des terminaux. Elles ont, en fait, besoin d'une stratégie multicouche.

De nombreuses organisations considèrent la sauvegarde et la récupération de leurs données comme l'ultime ligne de défense contre les attaques de ransomware. Chez Veritas, nous recommandons de donner la priorité à une stratégie de sauvegarde sécurisée et à l'optimisation de la restauration en tant qu'élément significatif et fiable d'une stratégie de cybersécurité complète et multicouche. Lorsque vous êtes attaqué, vous ne perdez pas seulement vos données — c'est toute votre activité qui s'arrête.

Les solutions Veritas ont été développées en mettant l'accent sur la résilience et la sécurité, afin que nous puissions fournir à nos clients des solutions fiables qui garantissent le bon fonctionnement de leur entreprise avec un minimum d'impact. Nos solutions protègent les systèmes informatiques et préservent l'intégrité des données grâce à une large gamme de contrôles de sécurité confiance zéro, à une prise en charge de la charge de travail et à des options de stockage immuables et indélébiles à la pointe de l'industrie, afin de répondre à des besoins variés. Nos solutions offrent une visibilité complète de l'ensemble de votre environnement, y compris les charges de travail physiques, virtuelles et dans le cloud, du stockage au calcul, et même à travers d'autres fournisseurs et services de sauvegarde, garantissant ainsi qu'aucun système ne passe entre les mailles du filet. Nos outils vous permettent de détecter en temps quasi réel, grâce à l'intelligence artificielle (IA), les activités ou comportements anormaux associés aux données et à l'activité des utilisateurs dans l'ensemble de votre environnement. Notre analyse automatisée et à la demande des logiciels malveillants fournit également des messages d'avertissement clairs, et assure une vérification ponctuelle des zones à risque connues, ainsi que la récupération des données propres. En matière de récupération, la marque Veritas est synonyme de résilience depuis des décennies. Les solutions Veritas fiables intègrent une technologie éprouvée, ce qui vous permet de récupérer rapidement grâce à des options flexibles, automatisées et orchestrées, qui permettent à votre entreprise de reprendre ses activités en quelques minutes.

Introduction

Ce document est centré sur les solutions Veritas qui constituent la plateforme de résilience aux ransomwares la plus complète, la plus conforme et la plus sécurisée du secteur. Nos solutions vous apportent une tranquillité d'esprit inappréciable, réduisent les risques et vous garantissent la protection, la détection et la récupération de vos données, ainsi que la résilience face à la menace en constante mutation des ransomwares.

Ce document s'adresse à un public professionnel et technique, et notamment aux clients, aux partenaires et aux autres personnes qui souhaitent en savoir plus sur la manière dont nos solutions contribuent à la protection contre les attaques malveillantes et à la reprise après une telle attaque.

Ce livre blanc vous aidera :

- à apprendre à protéger vos systèmes informatiques et à préserver l'intégrité des données ;
- à comprendre comment les solutions Veritas vous aident à surveiller et à atténuer les menaces et les vulnérabilités ;
- à explorer les options pour une restauration rapide et complète de l'ensemble des systèmes, et à élaborer un plan pour optimiser votre environnement en vue d'une reprise.

Il est important de noter qu'en matière de résilience aux ransomwares, il n'existe pas de solution unique, et que le présent document n'a pas vocation à être exhaustif. Veritas vous donne la possibilité de choisir parmi une variété de solutions qui répondent le mieux aux besoins de récupération spécifiques de chaque application. Vous devez mettre en œuvre une stratégie globale à plusieurs niveaux, structurée autour de la méthodologie du National Institute of Standards and Technology (NIST) : identifier, protéger, détecter, répondre et récupérer. En plus des éléments présentés dans ce livre blanc, nous vous recommandons de conserver les mesures de sécurité traditionnelles comme élément principal de la stratégie défensive de votre organisation, de veiller à ajouter des pare-feu, des filtres de courrier électronique et de spam, ainsi que des logiciels anti-malware et de protection des points, et d'introduire des stratégies de réseau segmenté et des programmes de formation pour les employés.

Les entreprises doivent élaborer, répéter et évaluer régulièrement leur stratégie afin d'évoluer pour tenir compte de la sophistication croissante des menaces et des technologies employées. Les répétitions régulières et la validation sont essentielles à la réussite, car elles permettent de vérifier que la stratégie fonctionne effectivement en situation de crise. De plus, il est toujours conseillé de faire appel à une agence tierce pour auditer votre stratégie, vérifier votre travail et vous aider à identifier les faiblesses.

Examinons les meilleures pratiques recommandées pour l'écosystème de sauvegarde d'une entreprise (voir figure 1).

Figure 1. Meilleures pratiques recommandées pour l'écosystème de sauvegarde d'une organisation.

Bonnes pratiques

Bien que les ransomwares puissent causer de graves dommages à votre entreprise et à votre réputation, ils ne sont pas invincibles. En fait, leur solidité est fonction du maillon le plus faible de votre organisation. La bonne nouvelle, réside dans le fait qu'il existe des mesures claires que votre organisation peut prendre pour éviter de devenir une cible de la cybercriminalité, et pour réduire le risque qu'une attaque ne mette votre activité en péril.

Le NIST a développé un cadre de cybersécurité recommandé qui aide les organisations à mettre en place une méthodologie complète et structurée autour de cinq fonctions clés : l'identification, la protection, la détection, la réponse et la reprise. Veritas s'aligne sur cette approche et recommande de mettre en œuvre ses solutions dans le cadre plus large élaboré par le NIST.

En ce qui concerne l'écosystème de sauvegarde d'une entreprise, Veritas recommande de conserver à l'esprit les meilleures pratiques clés présentées dans la figure 1.

Gestion des versions et invite aux mises à jour du système

- Réduire l'exposition aux vulnérabilités se tenant à jour des correctifs de sécurité et des versions comportant des mises à jour de sécurité.
- Surveiller les alertes techniques de Veritas en visitant le site Veritas Support ou Veritas Services and Operations Readiness Tools (SORT).

Modèle et politiques de confiance zéro

- Acquérir un état d'esprit dans lequel aucun appareil ou utilisateur n'est fiable par défaut, même s'il se trouve à l'intérieur du réseau de l'entreprise.
- Au lieu d'exiger un simple mot de passe (même s'il est long et compliqué), utilisez la gestion des identités et des accès en mettant en place un contrôle d'accès basé sur les rôles (RBAC) et une authentification à deux facteurs (ou une authentification multifactorielle, MFA) pour limiter l'accès aux seules fonctionnalités requises pour chaque personne, et empêcher la prise de contrôle d'un compte à l'aide d'un seul jeu d'informations d'authentification.
- Toujours exiger des utilisateurs qu'ils se connectent avec leurs propres informations d'identification.
- Ne jamais utiliser les mots de passe d'usine. Modifier les identifiants et mots de passe génériques intégrés, y compris les comptes « admin », « maintenance », « sysadmin » et « nbasecadmin » de l'hôte.
- Limiter ou verrouiller l'accès aux sauvegardes, qui constituent une méthode d'entrée courante pour les ransomwares, et une autre paire de ports Ethernet 10/25 Gb pour la circulation de protection des données orientée vers le client.

Stockage immuable et indélébile

L'un des meilleurs moyens de protéger vos données contre les ransomwares consiste à mettre en place un stockage immuable (qui ne peut être modifié) et indélébile (qui ne peut être supprimé) avec une horloge de conformité gérée en interne.

Chiffrement des données

- Mettre en œuvre un chiffrement en transit pour protéger vos données de toute compromission sur le réseau.
- Mettre en œuvre un chiffrement au repos pour empêcher les ransomwares ou les acteurs malveillants de voler vos données et de menacer de les rendre publiques, ou de se livrer à d'autres actes de malveillance.

Configuration et segmentation de réseau

- Suivre les guides en matière mise en œuvre de la sécurité.
- Durcir votre environnement en activant des pare-feu qui limitent l'accès aux ports et aux processus.
- Mettre à jour la politique de sauvegarde par défaut du catalogue primaire.
- Mettre en place une politique de sauvegarde pour le serveur de gestion des clés NetBackup (KMS).

Déploiement et stratégie de sauvegarde 3-2-1

- Adopter l'approche « 3-2-1 » recommandée par l'Agence américaine pour la cybersécurité et la sécurité des infrastructures (CISA) : conserver trois copies des données sur deux types de supports différents, dont une hors site. Nous recommandons d'aller plus loin dans cette approche en élaborant une stratégie 3-2-1-1, en conservant au moins une copie sur un support immuable et indélébile (voir figure 2).
- Utilisez la technologie Auto Image Replication (AIR) pour répliquer vers les domaines cibles.

Figure 2. Conservez trois copies des données sur deux types de stockage, avec une copie hors site et une autre sur un support immuable.

Visibilité complète des terminaux

La plupart des entreprises manquent cruellement de visibilité sur les terminaux clients distants. Il est désormais courant que des acteurs malveillants échappent à la sécurité de première ligne et restent là, en sommeil, suffisamment longtemps pour repérer les faiblesses et repérer le bon moment pour attaquer. Il est essentiel de mettre en œuvre des outils qui offrent une visibilité complète sur l'ensemble de votre environnement, détectent les anomalies, recherchent les activités malveillantes sur votre réseau et vous alertent, afin que les ransomwares n'aient nulle part où se cacher. Cette approche vous aidera à atténuer les menaces et les vulnérabilités avant que les acteurs malintentionnés n'aient la possibilité d'agir.

Optimiser pour une récupération rapide

La plupart des auteurs de ransomwares espèrent deux choses : dispose de suffisamment de temps pour que l'attaque se propage et de l'argent (de votre part) pour la faire cesser. Par le passé, la reprise pouvait prendre des semaines, voire des mois, lorsqu'il s'agissait d'un processus manuel, à forte intensité de main-d'œuvre, qui s'étendait à plusieurs parties prenantes au sein d'une organisation. Désormais, la reprise peut être orchestrée et automatisée grâce à des options souples et alternatives — comme la mise en place rapide d'un data center chez un fournisseur de cloud public — qui peuvent raccourcir les temps d'arrêt et offrir des solutions de rechange au paiement d'une rançon. Avec les bons systèmes en place, les délais de reprise de votre organisation peuvent être ramenés à quelques secondes, si nécessaire.

Répétitions fréquentes et assidues

Une fois votre stratégie en place, il est essentiel de la tester et de la répéter régulièrement. Non seulement cette pratique contribuera à raccourcir les délais de réponse aux menaces et à minimiser l'impact d'une attaque, mais la visibilité accrue vous aidera à identifier les problèmes, ainsi qu'à les résoudre et à améliorer la performance. Votre plan de résilience ne vaut que ce que vaut votre test le plus récent, c'est pourquoi il est avantageux de répéter et de réviser constamment votre stratégie de résilience.

Sensibiliser les collaborateurs

Il est bien connu que les employés sont souvent la porte d'entrée d'une attaque. Les attaques modernes par phishing et ingénierie sociale sont aujourd'hui si avancées qu'il n'est pas rare qu'elles abusent même des professionnels de la sécurité.

Il s'agit de former les collaborateurs à l'identification des tactiques d'hameçonnage et d'ingénierie sociale, à la création de mots de passe forts, à la navigation en toute sécurité, à l'utilisation du MFA et à l'emploi en toutes circonstances de VPN sécurisés, et jamais des réseaux Wi-Fi publics. Veillez également à ce que tous les collaborateurs de l'entreprise sachent ce qu'il convient de faire et qui alerter lorsqu'ils sont victimes d'un incident.

Notre stratégie : protection, détection, reprise

Veritas permet à ses clients de se protéger des attaques, de détecter celles-ci et de reprendre après celles-ci, grâce à un large éventail de caractéristiques et de fonctionnalités qu'ils peuvent personnaliser pour répondre à leurs besoins et à leurs exigences propres. Examinons le détail des trois piliers stratégiques de la stratégie de résilience aux ransomwares de Veritas.

Protection

La première étape de la résilience face aux ransomwares consiste à s'assurer que votre actif critique et le plus important — les données — et votre infrastructure informatique sont protégés contre l'inconnu et l'inattendu. Assurez-vous que toutes les parties de votre environnement (physique et virtuel, cloud et conteneurs) sont sauvegardées grâce à une protection universelle, appliquée intelligemment et gérée automatiquement, pour évoluer correctement. Votre infrastructure de sauvegarde et vos données sauvegardées deviennent alors la dernière ligne de défense contre une attaque et, en fin de compte, la clé du rétablissement de votre organisation. Veritas offre la prise en charge la plus large, de la périphérie au cœur et au cloud, avec plus de 800 sources de données, plus de 1 400 systèmes de stockage et plus de 60 fournisseurs de cloud, de sorte que votre environnement est protégé en permanence, et toujours récupérable.

Les administrateurs de cloud, de bases de données et de machines virtuelles (VM) gagnent beaucoup de temps grâce aux politiques intelligentes qui détectent et protègent automatiquement une application ou des instances de calcul avec le niveau de protection approprié.

Veritas met l'accent sur la protection de l'intégrité des données afin de garantir que les fichiers de sauvegarde demeureront en sécurité, et hors d'atteinte d'attaquants animés de mauvaises intentions. Pour préserver l'intégrité des données, nous proposons un large éventail de contrôles de sécurité qui contribuent à la protection des données.

Gestion d'identité et d'accès

- **Accès basé sur les rôles** — Contrôles d'accès que vous pouvez adapter aux besoins spécifiques des personnes, en spécifiant qui peut accéder aux données, et en définissant les actions qu'ils peuvent ou ne peuvent pas effectuer (voir figure 3).
- **Signature unique** — Prise en charge d'Active Directory et de LDAP, ainsi que de SAML 2.0. Les organisations peuvent utiliser leur fournisseur d'authentification pour réaliser une authentification à deux facteurs.
- **Authentification personnalisable** — Les appliances NetBackup Flex prennent en charge une force d'authentification configurable.

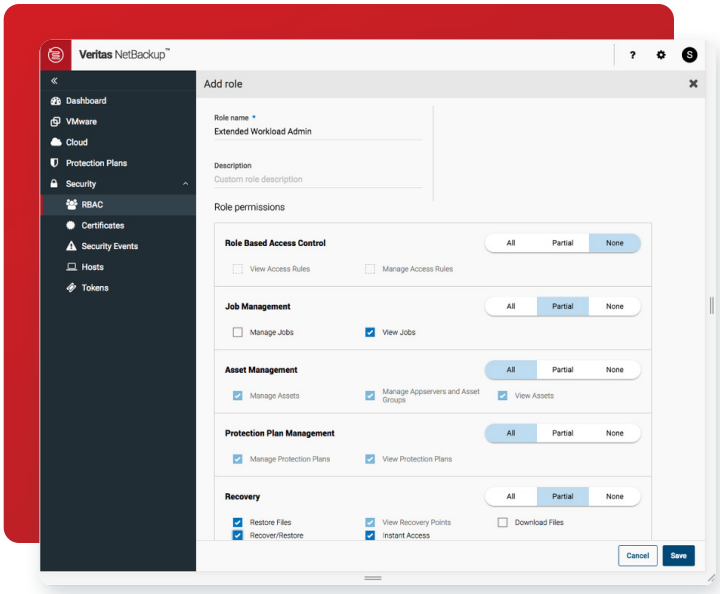


Figure 3. Le tableau de bord des autorisations d'accès dans NetBackup.

Chiffrement des données

- **En transit** — Assurez-vous que vos données sont envoyées à des environnements authentifiés et qu'elles sont protégées pendant le transit. Cette solution exploite les certificats TLS 1.2 de Veritas ou ceux fournis par le client, avec une prise en charge des clés de 2048 bits et plus pour garantir le cryptage des données pendant le transit.
- **Au repos** — Si les attaquants parviennent à accéder à vos données, le fait de les crypter les protège contre toute exploitation. Veritas propose une cryptographie AES 256 bits, FIPS 140-2 avec notre propre gestion des clés, tout en vous permettant de tirer parti de votre gestion des clés préférée à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Gestion et stockage d'images immuables/indélébiles

- Gestion d'images flexible indépendamment du type de stockage
  - Des options flexibles, y compris BYO, Appliance, Cloud et Software as a Service (SaaS) immuables permettent de sécuriser vos données et de les rendre conformes, indépendamment de leur localisation.
  - L'API OpenStorage Technology (OST) vous permet de gérer des images de sauvegarde immuables avec Veritas ou des solutions de stockage tierces.
  - Prend en charge la réplication primaire, secondaire (duplication) et inter-domaines (avec AIR), ce qui vous offre des options de configuration illimitées pour tous les niveaux de stockage de sauvegarde.
  - Utilise le stockage immuable dans le cloud avec Amazon Web Services (AWS) S3 Object Lock pour garantir que vos données dans le cloud sont sécurisées et ne peuvent pas être compromises. Pour en savoir plus sur le stockage immuable dans le cloud de NetBackup, consultez la fiche technique Object Lock support for AWS4.
  - Le déploiement de NetBackup Flex Appliance permet un stockage à la fois immuable et indélébile.
- Images stockées en mémoire WORM (write once, read many)
  - NetBackup Flex inclut un serveur de stockage WORM offrant une solution MSDP sécurisée et basée sur des conteneurs.
  - NetBackup Flex offre des modes de verrouillage Entreprise et Conformité, ce qui vous permet de choisir le niveau d'immutabilité approprié (voir figure 4).
  - Le mode conformité permet un stockage immuable, dans lequel aucun utilisateur — y compris l'utilisateur racine — ne peut supprimer des données pendant une période de rétention prédéfinie.

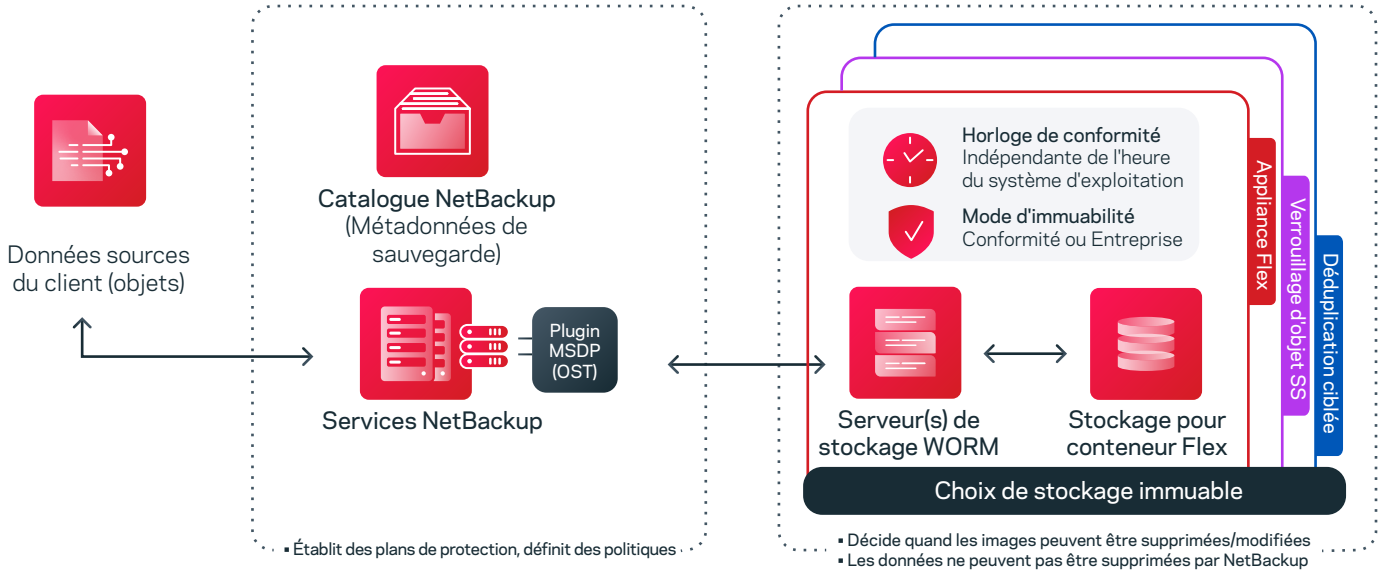


Figure 4. Vue d'ensemble des options de stockage immuable dans NetBackup.

  - Le mode Entreprise empêche la suppression des données pendant une période de conservation prédéfinie, mais seuls les utilisateurs disposant d'autorisations spéciales peuvent modifier les paramètres de conservation ou supprimer les données à l'aide d'une double autorisation. Deux personnes dont les niveaux RBAC sont différents doivent être d'accord pour modifier la durée de conservation, ou pour changer ou supprimer des données.
  - NetBackup Flex Appliance a fait l'objet d'une évaluation de l'immutabilité par Cohasset Associates, un évaluateur de contrôles d'immutabilité reconnu par l'industrie, en particulier par rapport à la règle 17a-4(f) de la SEC, à la règle 4511(c) de la FINRA et aux principes de la Commodity Futures Trading Commission (CFTC) dans la réglementation 17 CFR § 1 31(c)-(d).
  - Pour prendre connaissance de l'évaluation de NetBackup par Cohasset Associates, consultez Veritas.com.

Durcissement de solution

NetBackup Flex Appliance et NetBackup Flex Scale ont été renforcés, tant du point de vue des logiciels que du matériel, pour offrir une solution sécurisée complète prenant en charge le stockage immuable et indélébile. La solution comporte un serveur de stockage WORM sécurisé et des fonctions de sécurité du matériel.

- Tout au long du cycle de développement, Veritas analyse le code de NetBackup Flex et de NetBackup Flex, pour déceler d'éventuelles vulnérabilités, à l'aide d'outils de détection tiers reconnus et performants :
  - analyse statique du code ;
  - contrôles de vulnérabilité lors de l'exécution ;
  - tests de pénétration.
- NetBackup Flex et Flex Scale sont dotés d'un large éventail de fonctions de sécurité, dont les suivantes :
  - le renforcement de la sécurité du système d'exploitation, y compris le système SELinux (Security-Enhanced Linux) ;
  - le système de détection d'intrusion (IDS)/système de protection contre les intrusions (IPS) ;
  - une authentification robuste basée sur les rôles ;
  - un stockage verrouillé ;
  - un système de fichiers Veritas sécurisé, robuste et renforcé.

Pour plus d'informations, consultez le livre blanc Veritas Flex Appliances with NetBackup Security pour prendre en charge le déploiement sécurisé, ainsi que le livre blanc Veritas Flex Appliances with NetBackup.

Détection

Les acteurs malveillants recherchent vos maillons les plus faibles, les zones d'ombres où la sécurité et/ou la surveillance de votre environnement peuvent être limitées. Veritas propose des solutions qui permettent de connaître l'intégralité de l'infrastructure, de mettre en lumière toutes les données obscures de votre environnement, ainsi que de veiller à ce que vous sachiez ce qu'il contient, et à ce que ce contenu soit sûr, sécurisé et capable de résister au danger que représente les ransomwares. Veritas propose également une détection des anomalies et des programmes malveillants qui permet d'agir avant que les cybercriminels ou de tels programmes n'aient la possibilité de le faire.

Sensibilisation à l'infrastructure de sauvegarde et de stockage

En matière de ransomware, chaque seconde compte. Veritas Alta™ Analytics pour le cloud et NetBackup IT Analytics pour les installations sur site peuvent aider votre entreprise à appréhender l'ampleur et la profondeur d'une attaque de ransomware, afin de pouvoir procéder à une récupération stratégique. Grâce aux informations environnementales corrélées de NetBackup IT Analytics — sur site, dans le cloud, de protection des données et de stockage — les alertes et les rapports sont complets et faciles à mettre en place. Vous disposerez, grâce à ces options de rapports analytiques, des informations nécessaires pour prendre des décisions éclairées face à une attaque, qui vous aideront à obtenir une visibilité sur votre environnement de sauvegarde, ce qui permettra à votre organisation de :

- découvrir tous les hôtes ou toutes les machines virtuelles de votre infrastructure, et de les comparer avec les machines virtuelles protégées par NetBackup ;
- signaler les hôtes qui ne figurent pas dans les sauvegardes ou qui n'ont pas de sauvegardes récentes comme présentant un risque potentiel ;
- détecter les fichiers potentiellement infectés par un ransomware, ainsi que leur taille et leur emplacement dans l'environnement ;
- utiliser des graphiques interactifs qui donnent une vue historique des risques générés.

NetBackup Analytics permet de surveiller les sauvegardes de bout en bout :

- analyse des mesures d'atténuation (voir figure 5) ;
- sources avec échecs consécutifs ;
- sources sans sauvegarde récente ;
- défaillances des sauvegardes par application.

NetBackup Analytics identifie les faux positifs potentiels en comparant les sauvegardes historiques avec la nouvelle sauvegarde, et en identifiant les anomalies telles que les changements significatifs dans les durées de travail, les variations de taille d'image et/ou les changements de configuration de la politique.

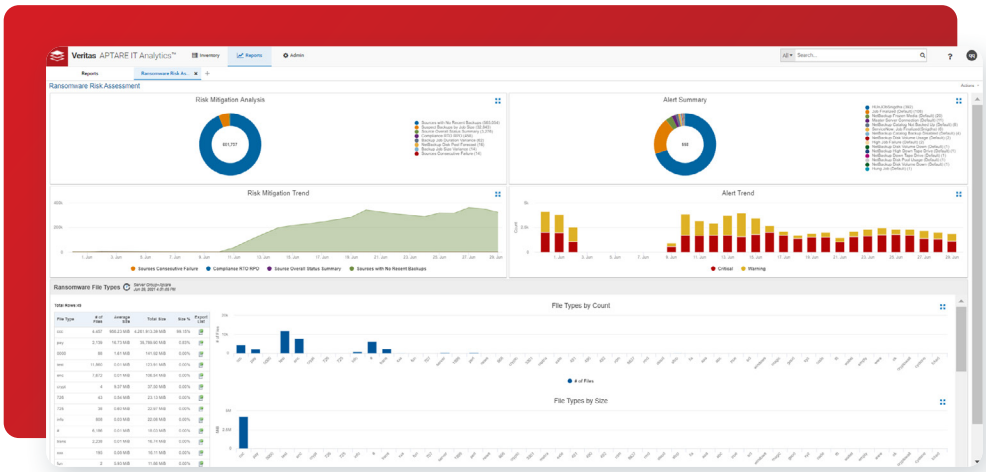


Figure 5. Le tableau de bord d'évaluation des risques de ransomware dans NetBackup IT Analytics.

Pour en savoir plus, consultez Augmenter la résilience face aux ransomwares : Obtenez une connaissance complète de l'infrastructure avec NetBackup IT Analytics.

Détection des anomalies

Veritas détecte les données étranges et l'activité des utilisateurs dans l'ensemble de votre environnement, et vous alerte, en cas d'anomalie suspecte, en temps quasi réel grâce à la détection d'anomalies alimentée par l'IA avec Veritas Alta™ Data Protection pour le cloud et NetBackup pour l'environnement sur site. Cette technologie est conçue pour exploiter une énorme quantité de données, automatiser la surveillance et la création de rapports et fournir des informations exploitables sur ce qui se passe dans votre environnement. Les alertes peuvent porter sur des éléments tels qu'une activité inhabituelle d'écriture de fichiers, qui pourrait être indicatrice d'une infiltration, mais aussi concerner la détection d'extensions de fichiers de ransomwares connus, de schémas d'accès aux fichiers, de schémas de trafic, de téléchargements de codes, de demandes d'accès, d'augmentations de la capacité de stockage, de chemins de trafic externes, ou même d'une augmentation inattendue de l'activité par rapport aux schémas habituels des individus.

Cette fonction garantit que vos données sont toujours récupérables et vous permet de prendre des mesures immédiates en cas de ransomware, en isolant les sauvegardes qui contiennent des logiciels malveillants et en limitant leur impact. Les solutions Veritas permettent aux administrateurs de visualiser les données et de formuler à tout moment des recommandations associées aux anomalies, en surveillant tous vos appareils et en créant des alertes précoces en cas d'attaque, afin que vous puissiez maîtriser des problèmes dès qu'ils surviennent. Par exemple, la détection d'anomalies pilotée par l'IA de Veritas s'intègre parfaitement au serveur principal, ce qui lui permet de détecter les formes d'observation anormales, en considérant comme des anomalies ou des cas particuliers celles qui n'entrent pas dans le cadre du cluster. Cette fonctionnalité permet à un administrateur de détecter les anomalies et de les analyser pour identifier les problèmes posés. Il permet d'exploiter de grandes quantités de données et de fournir des informations exploitables pour faire face à des événements liés à des ransomwares, ou simplement à des changements dans l'environnement dont un administrateur doit avoir connaissance (voir figure 6).

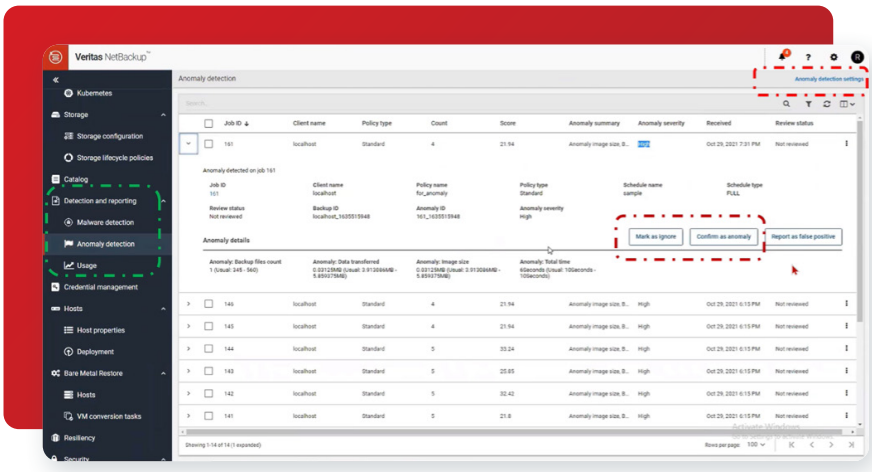


Figure 6. Utilisez NetBackup pour détecter les anomalies et prendre les mesures qui s'imposent.

Pour en savoir plus sur les capacités de détection des anomalies, consultez le document technique Veritas Anomaly Detection.

Détection du stockage primaire

Veritas s'intéresse non seulement aux données de sauvegarde secondaires avec NetBackup, mais aussi au stockage primaire — là où réside l'application — avec Veritas Alta™ Data Insight pour le cloud, et NetBackup Data Insight pour les installations sur site. Data Insight complète les outils de détection de sécurité existants en fournissant une détection des comportements anormaux, des modèles de requête personnalisés spécifiques aux ransomwares et une identification des extensions de fichiers utiles à la détection des ransomwares. Data Insight comprend un système de surveillance et d'alerte en temps quasi réel, basé sur des règles, qui permet de détecter tout comportement malveillant ou anormal dans les comptes d'utilisateurs. Pour ce faire, il analyse les systèmes de données non structurées qu'il surveille et collecte des audits de toutes les activités des utilisateurs effectuées sur tous les fichiers — lecture, écriture, création, suppression et renommage —, tout en procédant à des comptages de sécurité et de fichiers pour chaque utilisateur (voir figure 7).

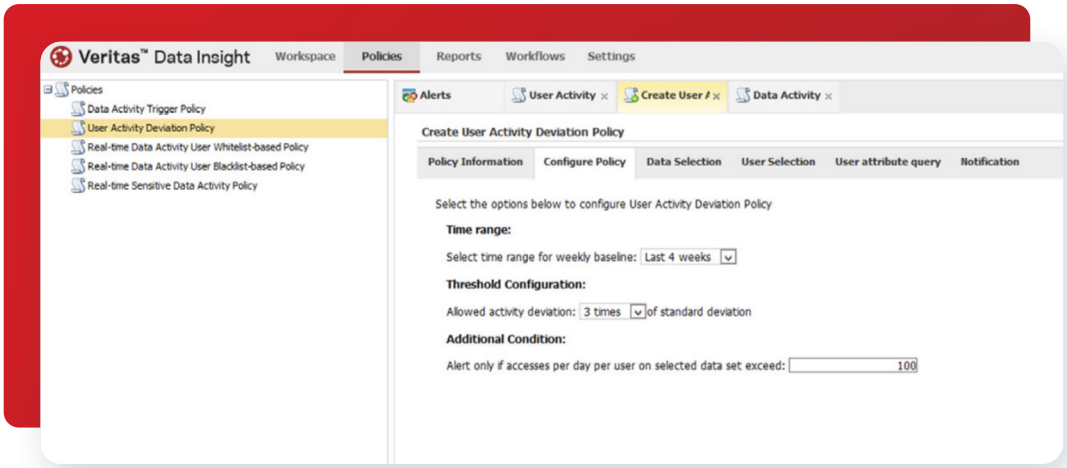


Figure 7. Configuration d'une politique de détection des activités des utilisateurs dans Data Insight.

Cette technologie compare les données historiques qu'elle a collectées et recherche les écarts types statistiques pour contribuer à la détection des comportements anormaux tout en identifiant les comptes susceptibles d'être compromis par un ransomware. Data Insight peut également détecter les comptes d'utilisateurs malveillants ou les activités spécifiques aux ransomwares, et identifier l'emplacement des fichiers de ransomwares potentiels.

Détection des logiciels malveillants

Veritas propose des analyses automatisées et à la demande pour les sauvegardes protégées. La fonction d'analyse automatisée des logiciels malveillants supprimera les dépendances humaines, et permettra à la technologie d'intelligence artificielle/apprentissage machine (IA/ML) d'intervenir et d'analyser les logiciels malveillants. La détection IA/ML de logiciels malveillants est automatiquement déclenchée par un score d'anomalie élevé. L'analyse porte sur les données non structurées, tant pour Windows que pour Linux. Cette inclusion est vitale, car les logiciels malveillants pénètrent souvent dans votre environnement par le biais d'un répertoire personnel. En effet, ce genre de répertoire contient généralement de vastes ensembles de données non structurées.

Lorsque la récupération est nécessaire, les données de sauvegarde sont analysées. Des visuels clairs et des messages d'avertissement signalent les sauvegardes infectées, garantissant que toutes les données restaurées sont propres et n'ont pas été touchées. Cette pratique est souvent appelée restauration de la dernière copie saine connue. (Voir figure 8.)

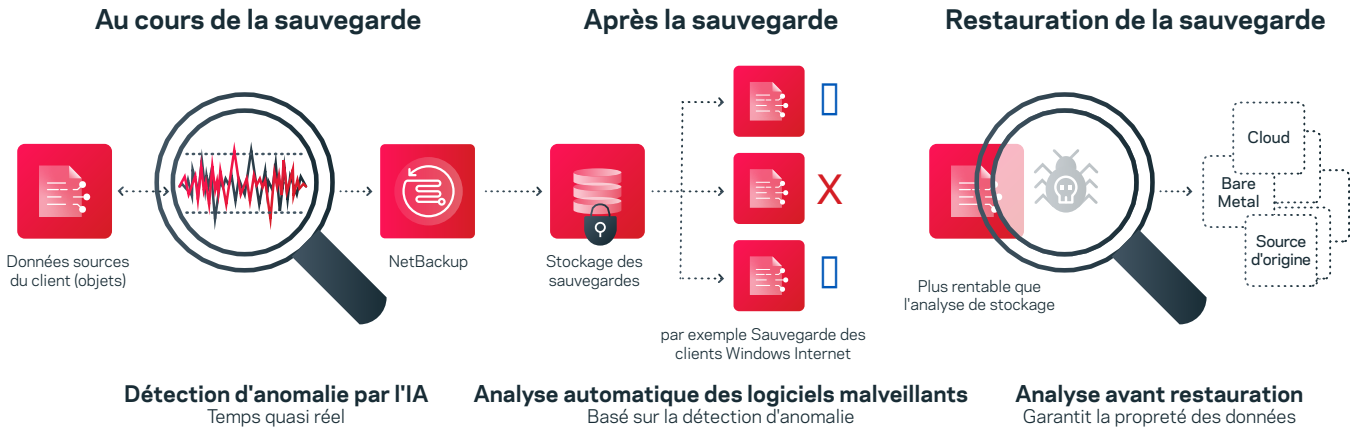


Figure 8. Vue d'ensemble de la détection des logiciels malveillants dans NetBackup.

Reprise

Chaque cyberattaque est unique. Dans le paysage actuel, fait de menaces en constante mutation, il est vital de mettre en place une stratégie optimisée qui va bien au-delà des points de restauration et des copies de sauvegarde uniques. La structuration d'une expérience de récupération optimisée et simplifiée vous aidera à reprendre vos activités en quelques minutes, au lieu de plusieurs heures ou jours, quelle que soit l'échelle.

Traditionnellement, les entreprises considèrent la sauvegarde et la restauration comme la dernière ligne de défense, mais avec les solutions Veritas, les environnements sont optimisés pour la restauration, et celle-ci devient un élément essentiel de la réussite de la résilience. Veritas propose une variété de solutions qui garantissent la résilience des opérations et des entreprises, en offrant la flexibilité et les choix nécessaires à une reprise rapide. Pourquoi cette flexibilité est-elle importante ? Parfois, tout est touché et vous pouvez avoir besoin de récupérer un centre de données entier dans le cloud et à la demande. D'un autre côté, il se peut qu'une partie seulement de votre environnement soit touchée. Il peut alors être crucial de mettre en place des solutions qui vous permettent de récupérer des bases de données et des fichiers individuels afin de rétablir rapidement la production. Lorsque des serveurs entiers sont cryptés, il est possible que vous deviez rapidement récupérer ces serveurs ailleurs. Ou peut-être avez-vous simplement besoin de récupérer un grand nombre de machines virtuelles pour les remettre en production.

Complexités liées à la reprise grandeur nature

Hétérogénéité

Mélange d'environnements informatiques dans les data centers, de la périphérie au cœur et au cloud. (physique, virtuel, cloud, hybride, bande)

Reprise flexible, hybride et rapide. Il n'est pas toujours possible de revenir à l'original ou de passer d'une reprise au niveau de l'objet à une reprise au niveau data center.

Répétitions de reprise rentables et n'entraînant pas de perturbation
Productivité accrue et réduction des arrêts.

Dépendances

Gestion d'infrastructures complexes, de réseaux, de stockage et d'équipes interfonctionnelles. (sur site, hybride, cloud)

Applications multi-composants à plusieurs niveaux. Reprendre avec des données propres, où que ce soit, vers n'importe où. (de la périphérie au cœur et au cloud)

Il peut s'agir d'un processus manuel long et laborieux. Lacunes en matière d'éducation et de compétences.

Figure 9. Les solutions Veritas répondent à la complexité de la récupération à l'échelle.

Veritas propose des solutions destinées à résoudre les problèmes complexes de récupération à l'échelle, qui sont illustrés dans la figure 9.

Veritas Resiliency Platform

Veritas Resiliency Platform résout ces problèmes de récupération en assurant une orchestration automatisée à l'échelle de l'ensemble de l'environnement hétérogène de votre entreprise, avec une expérience utilisateur cohérente et une visibilité des meilleures options de récupération en fonction des options disponibles, afin que vous puissiez atteindre vos objectifs de temps de récupération (RTO) et de point de récupération (RPO). (Voir figure 10)

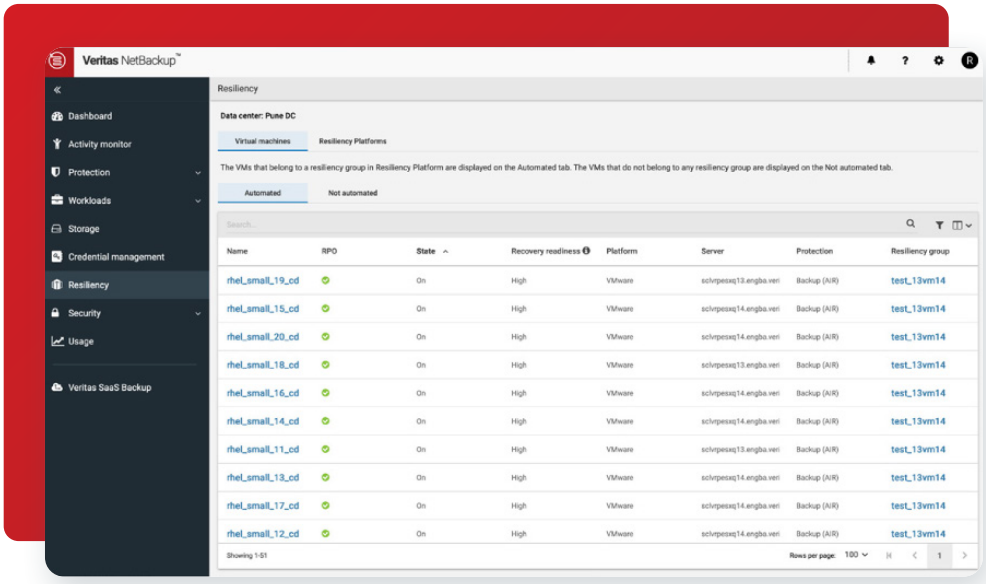


Figure 10. Le tableau de bord de la résilience dans l'interface web de NetBackup.

Pour atteindre le RTO le plus efficace, Veritas fournit des informations sur les opérations de récupération qui contribuent à la détermination de la meilleure méthode de récupération, en appréhendant vos RTO, vos charges de travail et vos applications dans l'ensemble de votre centre de données.

Veritas Resiliency Platform permet l'orchestration dans des environnements hétérogènes qui incluent la charge de travail et l'application ainsi que les données correspondantes à l'aide de la réplication automatisée, de la réplication basée sur le stockage ou du transfert de données intégré de NetBackup, ce qui vous permet de choisir le RTO et le RPO qui répondent aux exigences commerciales de votre application.

Plus précisément, la solution prend en charge l'automatisation en s'appuyant sur les Virtual Business Services (protection de la reprise après sinistre pour une application multi-niveaux), avec les plans de résilience et d'évacuation (le runbook), ce qui vous permet d'automatiser la reprise à l'échelle entre les centres de données ou vers les infrastructures cloud.

La solution permet également une validation répétée par bouton-poussoir dans les réseaux isolés. Dans les scénarios de récupération en relation avec un ransomware, les entreprises peuvent utiliser des scripts personnalisés pour intégrer des solutions tierces d'analyse antivirus dans le flux de travail, afin de vérifier l'absence de logiciels malveillants avant le retour à la production.

Du point de vue du RPO, NetBackup pour les installations sur site et Veritas Alta™ Data Protection pour la protection continue des données (CDP) dans le cloud offrent une résilience supplémentaire au moyen d'une récupération granulaire des machines virtuelles, avec un RPO proche de zéro. La CDP garantit la capacité de reprise des applications dans votre environnement hétérogène en utilisant des points de reprise granulaires dans la réplication des données en temps quasi réel de résilience (voir figure 11). Cette capacité permet de récupérer les données, en cas de logiciels malveillants ou de corruption, lorsqu'elles ont déjà été répliquées.

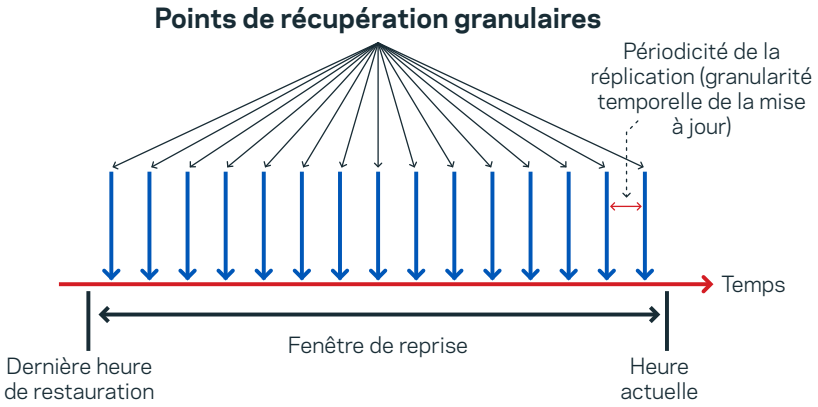
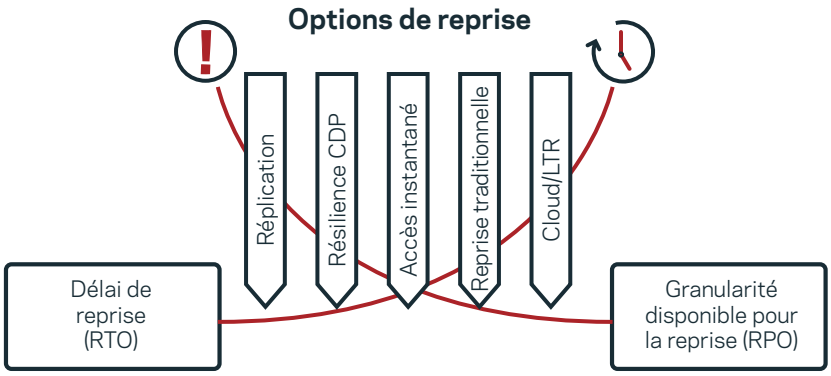


Figure 11. Une vue d'ensemble de la protection continue des données de NetBackup.

Pour en savoir plus sur Continuous Data Protection for VMware et les options de résilience avancées pour la protection des applications VMware, consultez les blogs correspondants.

Autres méthodes de reprise avec NetBackup

Veritas propose plusieurs autres méthodes de récupération en fonction de vos RTO et RPO, ce qui vous apporte la flexibilité requise pour choisir la méthode de récupération la mieux adaptée à votre organisation. La figure 12 illustre l'option de reprise optimale en fonction des RPO et des RTO.



Les objectifs RTO et RPO déterminent l'option optimale

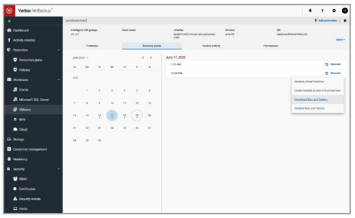
Figure 12. Choix d'une option de récupération optimale sur la base des RTO et RPO.

NetBackup Instant Rollback for VMware — assure une restauration rapide des machines virtuelles en utilisant le suivi des blocs de changement pour identifier les blocs uniques qui doivent être récupérés et en appliquant uniquement ces changements pour que votre machine virtuelle soit à nouveau saine — après un sinistre ou une attaque de ransomware — en quelques secondes, au lieu de minutes ou d'heures. Ce processus permet de récupérer sans effort 1 ou 100 machines, et d'assurer ainsi une récupération rapide en masse, quel que soit la localisation de votre infrastructure.

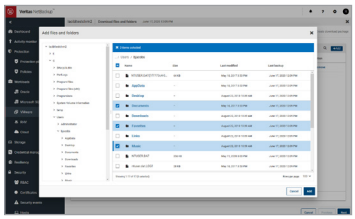
Pour plus d'informations sur Instant Rollback pour VMware, lisez ce blog.

Récupération de VM — Huit types de récupération sont disponibles pour une sauvegarde de machines virtuelles VMware : VM complète, VMDK individuelle, fichier et dossier, application complète, accès instantané, téléchargement de fichier, application GRT et conversion AMI. La prise en charge supplémentaire de vTPM garantit la sauvegarde et la restauration dans les environnements hautement sécurisés.

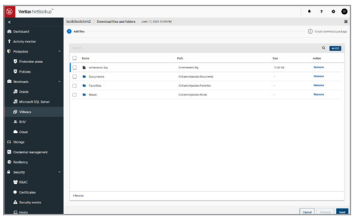
Instant Access for MSSQL and VMware— Avec Instant Access for VMware, vous pouvez récupérer n'importe quelle machine presque instantanément, sans attendre le transfert des données de la VM à partir de la sauvegarde (voir la figure 13). Vous pouvez également utiliser une sauvegarde pour tester ou récupérer des machines virtuelles directement à partir du stockage de sauvegarde. Ces machines virtuelles s'afficheront automatiquement comme des invités normaux dans l'infrastructure VMware. En outre, vous pouvez parcourir et récupérer des fichiers individuels directement dans l'interface Web de NetBackup. Pour les scénarios de récupération rapide, vous pouvez utiliser VMware Storage vMotion pour migrer la VM du stockage de sauvegarde vers la production en cours d'utilisation.



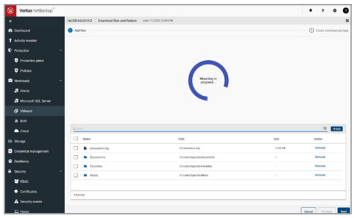
Parcourez les points de récupération disponibles pour une machine virtuelle VMware protégée



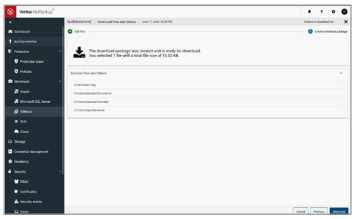
Sélectionnez les fichiers ou dossiers à récupérer



Vérifiez la liste des fichiers ou dossiers à télécharger



NetBackup Instant Access monte l'image de sauvegarde pour extraire les fichiers dans un paquet.



Les fichiers ou les dossiers comprimés sont disponibles pour le téléchargement

Figure 13. Utilisation de VMware Instant Access pour sauvegarder les machines virtuelles de votre infrastructure.

Pour une configuration complète et des détails, consultez le Veritas NetBackup for VMware Administrator's Guide.

Instant Access for MSSQL offre une disponibilité instantanée des bases de données et une récupération granulaire des éléments de la base de données à l'aide d'un stockage de sauvegarde (voir figure 14). Les fonctionnalités en libre-service permettent aux administrateurs de bases de données de provisionner rapidement les bases de données MSSQL pour leurs besoins de développement/test. Lorsque certaines copies de données sont touchées par un ransomware, NetBackup vous offre la possibilité de récupérer à partir de n'importe quelle copie de sauvegarde disponible à l'aide de notre interface et de nos API (voir figure 15).

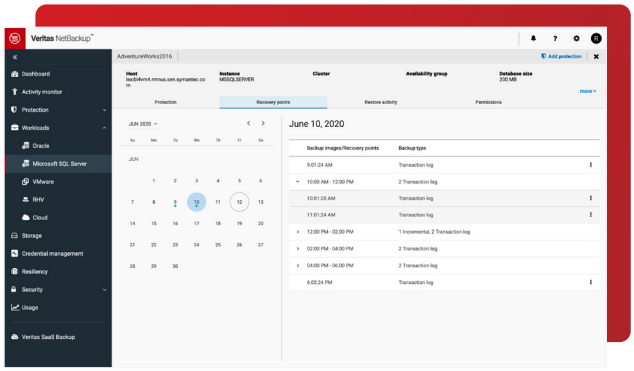


Figure 14. NetBackup fournit des options granulaires de restauration ponctuelle pour MSSQL.

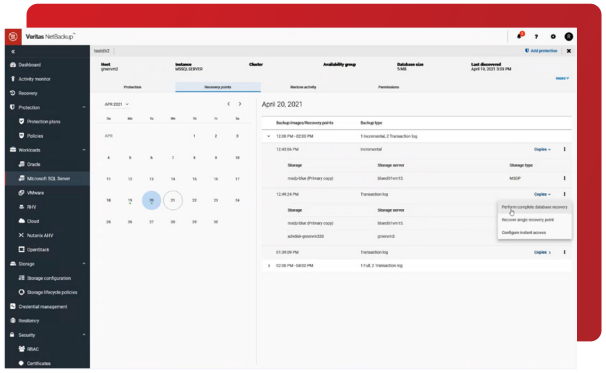


Figure 15. Récupération des bases de données à partir de n'importe quelle copie d'une sauvegarde MSSQL.

NetBackup Snapshot Manager — Utilisation de la technologie des conteneurs et des fournisseurs de services cloud Indépendamment de la plate-forme de stockage, NetBackup Snapshot Manager utilise une technologie d'instantané cloud-native, indépendamment des fournisseurs cloud, qui permet une protection facile des infrastructures hybrides et multi-cloud. En outre, Snapshot Manager propose des fonctions qui vont au-delà des fonctions de base dans un cloud public, en permettant des instantanés tenant compte des applications, la restauration d'un seul fichier et la migration d'instantanés multirégionaux. La prise en charge de comptes multiples par Snapshot Manager permet de stocker en toute sécurité des sauvegardes dans un compte différent, ce qui réduit l'impact en cas de compromission d'un compte.

Universal Share et Points de protection — La fonctionnalité MSDP, Universal Share vous permet de provisionner un stockage renforcé par déduplication sur serveur NetBackup sous forme de partages sécurisés, et de protéger ainsi les bases de données ou d'autres charges de travail lorsqu'il n'existe pas d'agent ou d'API de sauvegarde. Vous pouvez utiliser Universal Share comme stockage en réseau (NAS) pour conserver des données par compression et déduplication. Avec une prise en charge complète de l'API et une gestion centralisée des partages et des points de protection dans l'interface Web NetBackup, ainsi que la prise en charge des quotas d'utilisateurs et l'intégration d'Active Directory, les appliances NetBackup HA offrent une gestion améliorée des points de protection pour les partages universels qui vous permettent de créer une copie ponctuelle des données sur le partage, de générer instantanément une image de sauvegarde, puis de l'utiliser comme n'importe quelle autre sauvegarde.

Pour en savoir plus, voir la section Partage universel dans le Guide de l'administrateur de Veritas NetBackup.

NetBackup Universal Shares for Oracle — Tirant parti des fonctionnalités d'Oracle, la dernière version de 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.

Pour en savoir plus, consultez le Veritas NetBackup™ for Oracle Administrator's Guide.

Archive de conservation à long terme — Si vous devez conserver des données pendant une longue période, cette option offre une solution rentable et durable qui comprend la déduplication et la compression des données. Cette méthode permet également d'utiliser le stockage d'objets et les clouds privés ou publics. Pour les cas d'utilisation du cloud privé, l'appliance Veritas Access de notre plate-forme Enterprise Data Services Platform permet une rétention à long terme (LTR). Lorsque vous choisissez une méthode de récupération, gardez à l'esprit que les solutions LTR sont rentables et optimales pour les systèmes de santé et les autres organisations qui ont besoin de conserver leurs données pendant longtemps. Pour les organisations qui préfèrent continuer à utiliser les technologies sur bande, nous disposons de la solution sur bande la plus complète, qui offre un moyen fiable et étanche de récupération des données suite à un ransomware.

Restauration traditionnelle — Cette méthode comprend la restauration granulaire d'un fichier spécifique, la restauration complète d'un serveur/d'une application et la restauration après sinistre (DR) vers un autre site ou le cloud. Grâce à Veritas Resiliency Platform, vous pouvez automatiser et orchestrer la restauration traditionnelle d'un simple « clic », ce qui rationalise le processus de reprise après sinistre.

Bare Metal Restore — Si la récupération d'un ransomware nécessite d'exploiter le matériel touché, la restauration bare metal (BMR) peut constituer une solution précieuse lorsque les ressources sont limitées. La BMR automatise le processus de restauration du serveur, rendant inutile la réinstallation des systèmes d'exploitation ou la configuration manuelle du matériel. Lorsque les systèmes sont corrompus et doivent être complètement écrasés, la BMR vous permet de reconstruire rapidement les systèmes à partir de zéro, en restaurant le système d'exploitation et les données d'application en une seule opération.

Différenciation concurrentielle

Nos solutions Veritas garantissent que vos données sont toujours disponibles et protégées, contribuent à la disponibilité élevée des applications et assurent une récupération éprouvée à grande échelle, tout en maintenant la continuité de l'activité en cas d'attaque sur les données et l'infrastructure. Nos concurrents traditionnels, qu'il s'agisse de géants du stockage primaire ou de fournisseurs de solutions évolutives, n'abordent pas la résilience aux ransomwares de manière aussi complète que Veritas. À l'inverse de ses concurrents, Veritas aborde la résilience face aux ransomwares sous l'angle de la valeur commerciale, en proposant une stratégie de résilience solide qui prend en charge la protection contre les ransomwares, leur détection et la récupération après une attaque.

Voici quelques questions clés à se poser lors de la sélection d'un fournisseur de protection des données :

- La solution apporte-t-elle une résilience contre les ransomwares au cœur du système, à la périphérie et dans le cloud ?
- Offre-t-il un stockage immuable, qu'il soit déployé sous forme de BYO, d'appliance, de cloud ou de SaaS ?
- La solution prend-elle en charge la règle de copie de sauvegarde 3-2-1-1 dans tous les scénarios ?

Veritas peut faire tout cela, et plus encore :

- Offre de multiples options de déploiement, et la résilience contre les ransomwares demeure disponible pour tout scénario de déploiement d'entreprise.
- Adopte une approche de sécurité multicouche pour protéger les données de sauvegarde, en fermant les portes dérobées telles que les réinitialisations de clusters, les horloges externes ou le BIOS.
- Utilise un système d'exploitation renforcé pour réduire la surface d'attaque des ransomwares.

- Conçoit des solutions à partir des meilleures pratiques 3-2-1-1, en fournissant une norme de copie pour la prise en charge des bandes, le stockage immuable et l'isolement.
- Crée des appliances avec des déploiements conteneurisés renforcés, ce qui les rend encore plus difficiles à pénétrer que les facteurs de forme physiques ou VM traditionnels.
- Inclut la détection et la protection intégrées contre les intrusions dans des appliances qui évitent aux équipes informatiques et de sécurité d'avoir à intervenir.
- La détection ne se limite pas à la surveillance des sauvegardes, mais s'étend également à l'infrastructure et au modèle d'accès aux données primaires, ce qui permet de supprimer les ransomwares connus et de désactiver les comptes potentiellement infectés afin de minimiser l'impact des ransomwares.
- Permet de revenir uniquement sur les modifications apportées aux machines virtuelles à la suite d'une attaque de ransomware, ce qui rend la récupération efficace et rapide.

Chez Veritas, nous comprenons la nature vitale de la résilience. Prenons l'exemple de deux types de systèmes de sécurité qui surveillent une installation : l'un ne regarde que l'historique des images de sécurité pour identifier les intrusions, et l'autre regarde les flux en direct provenant de la surveillance, ainsi que les images historiques. Le système qui examine les flux en direct peut également désactiver l'accès à l'installation s'il détecte des signes d'intrusion. Selon vous, quel est le meilleur système ? Veritas permet de détecter les ransomwares en surveillant les systèmes de production. Cette surveillance va au-delà de la taille et des extensions pour couvrir les données et l'infrastructure. Elle peut détecter des écarts dans les schémas d'accès aux données et verrouiller les comptes susceptibles d'être utilisés pour exécuter un ransomware/malware. En analysant les changements dans les attributs de sauvegarde à l'aide de l'IA/ML, Veritas Alta™ Data Protection for cloud et NetBackup for on-premises peuvent alerter les organisations à propos d'éventuelles intrusions de ransomware.

Nous reconnaissons la nécessité de récupérer les données de la manière la plus efficace et la plus rapide possible. NetBackup offre des fonctionnalités telles que la restauration instantanée, qui permet d'annuler les dommages causés par le ransomware sans avoir besoin de restaurer et d'arrêter complètement les machines virtuelles. Veritas Alta™ Data Protection for cloud et NetBackup for on-premises permettent d'établir des plans de reprise pour des milliers de VM susceptibles de partie d'environnements complexes à plusieurs niveaux et d'exécuter des répétitions de ces mêmes environnements dans un environnement isolé. Les appliances NetBackup Flex et Flex Scale affichent certains des meilleurs chiffres de leur catégorie en matière d'accès instantané optimisé et de restauration des principales charges de travail. Veritas Alta™ SaaS Protection (anciennement connu sous le nom de Netbackup Saas Protection) a également prouvé son efficacité en matière de récupérations à l'échelle du pétaoctet. Tous ces éléments sont des points de recherche essentiels pour comparer l'exhaustivité de la résilience aux ransomwares de Veritas à celle de n'importe quel concurrent.

Conclusion

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. Même si les administrateurs des systèmes et des sauvegardes déploient des efforts considérables pour protéger les données de l'entreprise, les ransomwares et les initiés malveillants peuvent encore occasionnellement passer au travers et avoir un impact sur les données les plus critiques de l'entreprise. C'est pourquoi une stratégie globale, multicouche et complète est essentielle et constitue la meilleure défense.

Veritas a simplifié le processus pour vous. Nos solutions ont été développées avec la résilience en tête de liste, fournissant une plateforme unique et unifiée pour vous aider à protéger les systèmes informatiques et l'intégrité des données, à détecter par la surveillance et l'atténuation, ainsi qu'à récupérer rapidement grâce à l'automatisation et l'orchestration. Nos solutions réduisent la vulnérabilité, éliminent les îlots ou les surfaces d'attaque potentielles et sont faciles à adapter, à mettre à niveau et à entretenir. Aucune donnée n'est laissée sans protection, de la périphérie au cœur du système jusqu'au cloud. Bien que beaucoup considèrent la sauvegarde et la restauration comme la dernière ligne de défense contre les attaques de ransomware, nous recommandons de les considérer comme une partie significative et fiable de votre stratégie de cybersécurité complète et multicouche de protection, de détection et de restauration.

Pour en savoir plus sur nos solutions, consultez le site https://www.veritas.com/ransomware ou contactez-nous à l'adresse https://www.veritas.com/form/requestacall/requestacall.

Références

Gouvernement

- Le National Cybersecurity Center of Excellence (NCCoE), qui fait partie du National Institute of Standards and Technology (NIST), a publié un document spécial intitulé « Data Integrity, Recovering from Ransomware and Other Destructive Events » (Intégrité des données, récupération après un ransomware et d'autres événements destructeurs). Il s'agit d'un document complet en trois parties qui détaille les stratégies que les organisations doivent adopter pour se protéger contre les activités malveillantes, ainsi que les mesures de reprise à prendre après un événement de cybersécurité.
  Publication spéciale du NIST 1800-11 « Intégrité des données : Recovering from Ransomware and other Destructive Events » (page principale)
  - NIST SP 1800-11a : Résumé
  - NIST SP 1800-11b : Approche, architecture et caractéristiques de sécurité : ce que nous avons construit et pourquoi
  - NIST SP 1800-11c : How-To Guides : instructions pour construire la solution d'exemple
- Équipe d'intervention en cas d'urgence informatique aux États-Unis : « Options de sauvegarde des données »

Veritas

- « Menace d'initié 101 : détecter et protéger avec Veritas Data Insight »

Pour en savoir plus sur les modèles de rapport sur les ransomwares, consultez ces sections dans le Guide de l'utilisateur de Veritas Data Insight :

- À propos des rapports personnalisés de Data Insight
- A propos des modèles de requête DQL

- Appliance Veritas Flex avec NetBackup™ Security
- Appliance Veritas Flex avec NetBackup
- Guide de l'administrateur de Veritas Data Insight
- Guide de l'utilisateur de Veritas Data Insight
- Guide de l'administrateur de Veritas NetBackup, Volume I
- Guide de l'administrateur de l'appliance Veritas NetBackup
- Guide de l'appliance Veritas NetBackup Fibre Channel
- Guide de sécurité des appliances Veritas NetBackup
- Guide de l'administrateur cloud Veritas NetBackup
- Guide de déduplication Veritas NetBackup
- Guide de la sécurité et du chiffrement Veritas NetBackup
- Guide de l'administrateur de Veritas NetBackup for Oracle
- Veritas NetBackup for VMware Guide de l'administrateur

1 https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-

À propos de Veritas

Veritas Technologies est un leader dans la gestion des données multicloud. Plus de 80 000 entreprises, dont 95 % des entreprises du classement Fortune 100, font confiance à Veritas pour les aider à assurer la protection, la récupération et la conformité de leurs données. Veritas est réputée pour sa fiabilité à grande échelle, qui offre la résilience dont les clients ont besoin contre les interruptions qui pourraient survenir en cas de cyberattaque, par exemple de ransomware. Aucun autre fournisseur n'est en mesure d'égaler la capacité d'exécution de Veritas, avec la prise en charge de plus de 800 sources de données, de plus de 100 systèmes d'exploitation, de plus de 1 400 cibles de stockage et de plus de 60 plates-formes cloud, via une seule approche unifiée. Avec la technologie Cloud Scale, Veritas propose aujourd'hui sa stratégie de gestion autonome des données, qui réduit les coûts opérationnels tout en offrant une plus grande valeur ajoutée. En savoir plus sur www.veritas.com. Suivez-nous sur Twitter : @veritastechllc.

VERITAS

veritas.com/fr

Pour obtenir les coordonnées pour le monde entier, consultez la page : veritas.com/company/contact

V1726 01/23