VERITAS

L'avenir de la protection des données, dès maintenant

CONSERVEZ UNE LONGUEUR D'AVANCE SUR LES CYBER-RISQUES

La protection des données et leur récupération est une tâche continue.

Les menaces qui pèsent sur vos données se multiplient et évoluent. Les acteurs malveillants développent continuellement de nouvelles techniques d'attaque pour accéder à l'élément vital de vos opérations.

La protection des données est passée d'un poste de dépense à un aspect évolutif de la culture d'entreprise, avec de nombreux éléments mobiles. La variété et l'emplacement des charges de travail ainsi que la criticité de chaque application et de ses données sont des éléments essentiels pour évaluer les niveaux de protection dont vous avez besoin et la manière dont vous gérez la récupération.

Les facteurs tels que la haute disponibilité, la gouvernance et la conformité jouent tous un rôle et affectent les objectifs de temps de récupération (RTO) et de point de récupération (RPO).

Le Shadow IT et la dette technologique ont explosé. Les équipes créent des volumes de données écrasants et laissent par erreur des données critiques exposées aux risques. Les organisations n'ont pas une visibilité totale des éléments essentiel, ce qui rend difficile l'établissement de priorités pour atténuer les risques.

En faisant preuve d'anticipation et d'attention, vous pouvez garder une longueur d'avance et rester prêt à relever les défis potentiels qui se présenteront à vous.

Identifier les données dont vous disposez

Est-ce possible de protéger de manière adéquate les données dont nous n'avons pas conscience ?

Un grand nombre d'applications et de plates-formes promettent d'améliorer l'efficacité et de fournir des données plus performantes. Vos employés commencent à utiliser ces outils de façon isolée, en saisissant des informations sur les clients et des données sur l'entreprise dans des plates-formes qui sont probablement situées dans le cloud. Résultat : les données se multiplient et la couverture cloud devient un problème.

Des acteurs malveillants peuvent infiltrer ces données parce qu'elles ne sont pas correctement protégées par l'entreprise. Un comportement suspect peut passer inaperçu parce que l'équipe informatique n'est pas consciente qu'elle devrait le surveiller, ou même qu'il existe. En cas de sinistre, vous risquez d'apprendre que des informations essentielles n'ont pas été sauvegardées correctement.

Pire encore, elles ne sont pas récupérables.

La prolifération des données est un problème de gouvernance qui nécessite davantage de structure et de formation des employés, ainsi qu'une meilleure visibilité de l'infrastructure de l'entreprise.

Pour obtenir de meilleurs résultats, il faut mettre les données en contexte et évaluer les risques liés aux procédures complexes afin de décider de la manière d'exécuter les stratégies de sauvegarde et de restauration de la périphérie, au cœur et au cloud.

Questions clés :

- Quelles sont les données dont vous disposez et où se trouvent-elles ?
- Comment améliorer la visibilité de nos données ?

Solutions Veritas

Les solutions Veritas Data Protection offrent une protection des données à grande échelle. Le moteur de détection des anomalies alimenté par l'IA permet d'exploiter d'énormes quantités de données, d'automatiser la surveillance et la création de rapports, d'identifier des informations exploitables et de lancer des alertes précoces en cas d'attaques potentielles.

Les solutions Veritas Analytics aident à recouper les serveurs et le stockage avec tous vos fournisseurs de sauvegarde pour assurer que rien ne passe à travers les mailles du filet et ne reste vulnérable. Elles permettent d'analyser et de surveiller tous les systèmes, y compris les produits tiers, afin d'éliminer les zones d'ombre.

Veritas Data Insight peut vous aider à découvrir le potentiel de la création de rapports tout en permettant la détection des données potentiellement dangereuses, la révocation de l'accès aux données sensibles et la collaboration avec les propriétaires des données pour une meilleure prise de décision et le respect des normes de conformité. Mettez en évidence les risques, découvrez les données obscures et enregistrez l'activité des utilisateurs pour de nombreuses activités afin de découvrir des modèles d'activité et d'identifier et de détecter les anomalies.

Empêcher l'accès aux données

Les cybercriminels savent que les employés sont les points faibles de votre réseau.

La plupart des cyberattaques et des violations de données sont le résultat d'une interaction humaine et d'un manque d'attention. C'est pourquoi le phishing est si efficace.

Comment prévenir les attaques de ransomware ? Des éléments tels que la gestion de l'identité et de l'accès et le chiffrement sont des mesures de protection essentielles. Vous pouvez réduire les chances de réussite d'une attaque en mettant en place une authentification multifactorielle et un contrôle d'accès basé sur les rôles. Le chiffrement des données au repos et en mouvement réduit la possibilité d'utiliser vos données et contribue à les protéger contre l'exfiltration. Des éléments tels que l'authentification par carte à puce, l'authentification unique et la gestion des accès privilégiés contribuent à renforcer le principe du moindre privilège de la confiance zéro.

Les stratégies de prévention et de protection à plusieurs niveaux font appel à des solutions multiples mises en œuvre à chaque niveau. Vous pouvez (et devez) fournir des certificats numériques aux appareils pour une authentification plus poussée. Utilisez la double autorisation comme un niveau supplémentaire de protection pour l'accès aux sauvegardes.

La gestion d'un accès sécurisé et la protection de vos données contre une mauvaise configuration sont de la plus haute importance. L'identification et la compréhension des ressources, des actions et des identités dans votre environnement sont essentielles pour gérer les privilèges et appliquer les autorisations appropriées, que vous soyez sur site ou dans le cloud. Le suivi et la surveillance des tentatives et de la progression des changements vous permettent d'améliorer votre posture de sécurité et d'effectuer des améliorations en temps réel.

Solutions Veritas

Les solutions Veritas Data Protection sont indépendantes des fournisseurs et reposent sur les fondements de la confiance zéro. Elles permettent de sécuriser votre réseau, de protéger les données en transit et au repos grâce au chiffrement AES 256 bits, de répondre à la certification FIPS 140-2, de limiter l'accès des utilisateurs et d'activer le contrôle d'accès basé sur les rôles et l'authentification multifactorielle.

Veritas Data Insight offre une visibilité en temps quasi réel des données de production pour aider à identifier les ransomwares en fonction du comportement anormal des utilisateurs et des extensions de ransomwares connues. La solution peut également découvrir les données surexposées afin de limiter et de réduire les surfaces d'attaque.

Les solutions Veritas Analytics offrent un tableau de bord unique et unifié avec des informations opérationnelles et des renseignements permettant d'identifier les ransomwares, les systèmes non protégés et les anomalies de sauvegarde. Utilisez-les pour optimiser le stockage, réduire les coûts et rester au fait des exigences de conformité et de réglementation.

Veritas Alta™ Classification élimine les obstacles qui vous empêchent d'assurer la sécurité et la conformité des données. Rassemblez les attributs des métadonnées et les analyses du comportement des utilisateurs pour obtenir des informations exploitables, identifiez la propriété des données, l'utilisation et les contrôles d'accès, et atténuez les risques liés à la confidentialité et à la sécurité des données.

Questions clés

- Que faisons-nous pour prévenir les violations dues au phishing et aux malwares ?
- Existe-t-il des moyens d'améliorer nos mesures de protection actuelles ?

Identifier les données critiques et vulnérables

Vos données ne sont pas statiques, votre stratégie et vos solutions ne doivent pas l'être non plus.

Veillez à mettre en œuvre des produits et des services évolutifs et prêts à s'adapter. La flexibilité est cruciale pour fournir des performances sous pression avec de multiples intégrations à travers de multiples clouds.

Il n'est pas logique de supposer qu'une entreprise achètera toutes les solutions d'un seul fournisseur sur une seule facture. Le développement des entreprises ne fonctionne pas de cette manière : il est désordonné et implique des combinaisons de logiciels et de technologies anciens avec des solutions plus récentes et plus sophistiquées.

Classez les données par ordre de priorité et identifiez le niveau de conformité et de réglementation à respecter. Décidez comment gérer les sauvegardes et comment gérer l'échelle et la taille des sauvegardes qui influencent le temps de récupération. Comprenez comment la capacité de votre bande passante affecte votre sauvegarde et votre restauration afin de déterminer comment sauvegarder et restaurer le plus efficacement possible les workflows critiques.

Questions clés

- Quelles sont les données les plus importantes pour maintenir la visibilité sur vos données ?
- Comment prioriser nos sauvegardes de données ?

Solutions Veritas

Les solutions Veritas Data Protection sont indépendantes des fournisseurs et offrent un workflow de rétention et de protection solide, rentable et facile à déployer et à gérer. Simplifiez et organisez les environnements multicloud et cloud hybride au sein d'une plate-forme unique.

Veritas Alta™ Shared Storage est conçu pour alimenter vos applications critiques et fournir un stockage partagé de qualité professionnelle avec des performances et une résilience supérieures, tout en maintenant des coûts réduits. Il permet aux administrateurs d'applications et d'infrastructures de sécuriser les données sensibles. Il offre en outre des fonctions de chiffrement, d'écriture unique et de lecture universelle (Write Once Read Many ou WORM), d'instantanés cohérents et d'accélération des bases de données.

Veritas Alta™ SaaS Protection vous permet de conserver l'accès aux données stockées dans les comptes Microsoft 365 après le départ des employés sans avoir à maintenir, et à payer, la licence supplémentaire. Restaurez des dossiers, des boîtes aux lettres ou des sites avec une récupération granulaire et multi-niveaux vers un emplacement préféré, que ce soit dans le cloud ou sur site. Maximisez les performances et la flexibilité en faisant évoluer le stockage de sauvegarde jusqu'à des pétaoctets et des milliards d'objets. Effectuez des sauvegardes incrémentielles plus régulièrement pour minimiser le RPO et le RTO tout en mettant en œuvre une protection continue des données pour les récupérations sur les sites.

Rendre les données et les sauvegardes disponibles et efficaces

Vous avez sauvegardé vos données. Pourquoi est-il si difficile de les restaurer en cas d'incident ?

La migration de grandes quantités de données (comme le déplacement vers le stockage secondaire) prend beaucoup de temps et de ressources informatiques. Et cette action n'est pas unique. Si vous utilisez la règle de sauvegarde 3-2-1, vous effectuez le processus trois fois pour deux types de stockage différents, dont au moins un hors site pour une protection supplémentaire.

De nombreux éléments peuvent faire échouer une sauvegarde complète pendant la migration, d'où l'importance de la haute disponibilité et du basculement. C'est comme verser de l'eau d'un pichet dans un verre ; lorsqu'un verre déborde, un verre secondaire peut recueillir l'excédent. L'équilibrage de la charge distribue la charge de travail en évaluant quel système peut traiter votre demande. Vous pouvez regrouper plusieurs serveurs pour assurer une haute disponibilité et permettre le basculement. Si un serveur tombe en panne, un autre peut prendre sa place, sans aucune interruption.

Questions clés

- Où pouvons nous améliorer l'efficacité de nos sauvegardes ?
- Comment savoir si nos sauvegardes sont propres, exemptes de malwares et non corrompues ?

Solutions Veritas

Les solutions Veritas Data Protection prennent facilement en charge la stratégie de sauvegarde 3-2-1+1 et ajoutent un niveau de sécurité supplémentaire avec un système de prévention des intrusions intégré et un environnement de restauration isolé physiquement pour un stockage indélébile et un centre de sauvegarde des données intégré, isolé et immuable.

Veritas InfoScale permet de réduire la surface d'attaque des données de production et d'isoler les données de production des E/S grâce aux instantanés et à la mise en miroir des données. La solution optimise également la récupération pour un RTO et un RPO faibles. Vous pouvez exécuter des analyses de malwares sur le volume isolé à l'aide de scripts automatisés pour vous assurer qu'il est exempt de malwares.

Veritas NetBackup Flex et Flex Scale appliquent un niveau de sécurité supplémentaire en éliminant les points de défaillance multiples dans le matériel. Ces solutions utilisent des composants de cluster pour rester disponibles.

Les solutions Veritas Analytics créent une base de référence des sauvegardes réussies connues pour comparer les sauvegardes futures et vous aider à repérer les anomalies. Vous pouvez également classer les sauvegardes par application pour visualiser la restaurabilité de toutes vos applications à partir d'un seul tableau de bord.

Veiller à ce que les sauvegardes soient immuables et isolées

Comment vous assurer que vos données de sauvegarde ne sont pas vulnérables au chiffrement malveillant ?

Même si votre entreprise fait preuve d'anticipation en matière de sauvegarde des données, elle n'est pas à l'abri du risque d'erreur humaine ou de défaillance du matériel. Le risque de suppression ou de modification accidentelle des données est élevé.

Les sauvegardes doivent être effectuées de manière à ce que les données ne puissent pas être modifiées. Les fichiers stockés dans un espace de stockage immuable peuvent vous éviter la corruption ou les cyberattaques.

Les sauvegardes immuables offrent le plus haut niveau de protection des données pour votre entreprise. La permanence des données fait partie intégrante du stockage immuable, garantissant que les fichiers ne sont pas modifiés par accident ou volontairement. Cela permet de créer un processus plus efficace dans le cadre de votre stratégie de cybersécurité et de reprise après incident et peut vous aider à éviter les pertes financières et les temps d'arrêt.

Le niveau de sécurité supplémentaire d'une solution isolée physiquement garantit que vos données de sauvegarde immuables sont isolées et non corrompues afin que vous puissiez procéder à une restauration propre des données.

Questions clés

- Comment protégeons-nous actuellement les sauvegardes contre la corruption ?
- Existe-t-il des normes de conformité qui exigent que vous disposiez d'une solution isolée physiquement pour vos données ?

Solutions Veritas

Veritas s'aligne sur les principes du NIST pour offrir une immuabilité, une visibilité, une récupération rapide et une indélébilité inégalées. Elle prend en charge plusieurs méthodes pour les solutions sur site et hors site, notamment les sauvegardes sur bande, le stockage d'objets verrouillés dans le cloud et le stockage efficace des données dans AWS S3 Object Lock.

Les solutions Veritas Data Protection bloquent de manière proactive les comportements d'accès aux ressources indésirables avant que le système d'exploitation ne puisse agir.

Veritas Flex vous permet d'implémenter un environnement de restauration isolé (IRE) avec un centre de sauvegarde des données immuable et de fournir une copie sécurisée des données de sauvegarde critiques à partir d'un environnement isolé et immuable. L'architecture IRE protège vos sauvegardes importantes et fournit un espace sûr que vous pouvez utiliser pour orchestrer une récupération propre ou simuler votre plan de récupération de cyber-résilience. L'espace virtuel agnostique de l'infrastructure Veritas offre un niveau supplémentaire de protection et d'isolement pour aider à répondre aux attaques malveillantes.

Décider d'un processus de reprise après incident

La solution de récupération idéale prend en charge toutes les charges de travail.

Créez un processus qui incorpore une intégration facile, répond à vos RPO et RTO souhaités, prend en charge tous les types de stockage et offre un tableau de bord consolidé de tout ce qui est protégé. Lorsque vous définissez votre processus, tenez compte des facteurs suivants :

- Récupération orchestrée (avec un ordre de récupération déterminé)
- Déduplication intelligente
- Intégration des instantanés
- Hiérarchisation du stockage
- Réplication automatisée d'images, de catalogues et d'instantanés vers un stockage sur site et sur le cloud
- Prise en charge des conteneurs
- Informations sur les données et analyses
- Sécurité, conformité et flexibilité pour les entreprises sur site et dans le cloud
- Protection des données et des systèmes de sauvegarde par un chiffrement

Exploitez la puissance de la confiance zéro, de la sécurité des données multiniveau et de l'automatisation intelligente pour garantir la résilience des opérations commerciales. Débloquez l'intelligence multicloud et améliorez les cyberdéfenses tout en réduisant les coûts et en utilisant des solutions intégrées. Réduisez vos coûts et restez en conformité avec les réglementations en vigueur en consolidant la sauvegarde et la restauration des charges de travail basées sur le cloud, en automatisant la migration des charges de travail et en mettant en œuvre une reprise après incident facile avec une restauration en un seul clic, des scripts personnalisés et des simulations.

Solutions Veritas

Si seule une partie de vos fichiers a été compromise, vous avez le choix entre la récupération complète et la récupération granulaire des fichiers. Nous proposons également un retour en arrière instantané pour les machines virtuelles afin de récupérer et de restaurer simultanément des centaines de machines virtuelles en quelques minutes.

La résilience des données améliorée et Veritas Resiliency Platform vous permettent d'attribuer différentes priorités de restauration aux applications et de restaurer les applications multiniveaux dans un ordre correspondant à leur niveau d'importance pour l'entreprise. Les points de contrôle continus de la protection des données permettent une récupération à faible RPO.

Veritas NetBackup Flex et Flex Scale disposent d'un système d'exploitation renforcé, d'une architecture de confiance zéro et d'un stockage immuable et indélébile. L'IRE et le centre de sauvegarde de données immuables offrent une solution isolée physiquement, qui ne peut pas être découverte de l'extérieur. L'analyse des malwares et des anomalies garantit que vos données de sauvegarde sont propres et que vous pouvez les récupérer instantanément, quel que soit l'environnement, sur site ou dans le cloud.

Questions clés

- Combien de temps me faudra-t-il pour récupérer les données ?
- Quels sont les éléments prioritaires pour la récupération ?

Simuler votre stratégie de reprise après incident

Vos simulations ne sont pas qu'une question de restauration, il s'agit également d'éviter les temps d'arrêt.

Les cybercriminels espèrent que votre organisation, comme la plupart des autres, n'est pas optimisée pour la récupération. Ils veulent créer un maximum de dégâts et de temps d'arrêt pour s'assurer du paiement des rançons. Si votre récupération est prête à être effectuée, vous avez déjà une longueur d'avance. Une reprise rapide nécessite un plan d'intervention en matière de cybersécurité pour l'ensemble de votre environnement, qui prévoit des tests précoces et fréquents. Des simulations et des exercices réguliers de récupération permettent de limiter les temps d'arrêt et les perturbations et de réduire l'impact d'une attaque.

Avec l'augmentation de la demande de systèmes hybrides et multiclouds, vous devez être en mesure de gérer plusieurs cadres et de coordonner plusieurs clouds et systèmes de stockage. Les équipes sont chargées de gérer et d'adapter plusieurs serveurs et applications.

Tirez parti de l'automatisation pour gérer la complexité de vos environnements, identifier les menaces potentielles et gérer les simulations de manière proactive afin d'assurer une préparation continue et de minimiser les temps d'arrêt.

Questions clés

- Comment réduire les temps d'arrêt ?
- Comment accélérer la remédiation ?

Solutions Veritas

Veritas NetBackup Flex et Flex Scale maximisent le potentiel de la protection des données avec une architecture facilement extensible. Grâce à plusieurs niveaux d'immuabilité, au provisionnement automatisé et à l'équilibrage de charge, vous pouvez déployer une solution de protection des données complète et prête à l'emploi.

Veritas InfoScale et Veritas Alta™ Application Resiliency ne se contentent pas de vérifier si votre installation fonctionne, mais également si elle fonctionne suffisamment bien. Il s'agit d'une solution d'infrastructure complète conçue pour maximiser la disponibilité et la reprise après incident grâce à une intégration étroite avec les applications professionnelles critiques afin de garantir un temps de fonctionnement maximum et un basculement. Plate-forme globale, elle permet de personnaliser les niveaux de protection en fonction de la demande du secteur, grâce à des fonctionnalités telles que :

- Respect de l'intégrité des données
- Runbooks automatisés pour les applications multi-niveaux afin de réduire les efforts manuels
- Mobilité qui permet aux charges de travail de passer d'une plate-forme à l'autre sans effort
- Intégration transparente avec les systèmes et environnements traditionnels

Optimiser votre sauvegarde et restauration

Facilitez la gestion de la protection des données dans l'ensemble de l'entreprise.

L'orchestration des données permet d'identifier les goulots d'étranglement et de comprendre où se situent les processus qui prennent le plus de temps. L'orchestration permet de gagner du temps en automatisant des processus tels que l'approvisionnement en serveurs, la gestion des bases de données et les applications. Utilisez-la pour effectuer des tâches telles que l'analyse des vulnérabilités, la recherche de journaux et même la connexion d'outils de sécurité et l'intégration de systèmes, afin que les équipes ne soient pas submergées par les tâches.

Le choix de la bonne solution peut faciliter la gestion des données, mais constitue un défi permanent.

L'accès aux bonnes analyses permet d'avoir une visibilité sur les éléments essentiels de votre environnement. En creusant davantage, vous pouvez également identifier ce qui est sous-utilisé, mal configuré ou non indexé, ce qui aide le service informatique à résoudre les problèmes et à identifier les ressources à réaffecter pour réaliser des économies.

Découvrez des informations exploitables pour améliorer votre utilisation, vos performances et votre résilience tout en prévoyant les défaillances et en identifiant des recommandations proactives pour atténuer les risques liés aux contrat de niveau de service (SLA).

L'automatisation intelligente peut vous aider à éliminer les inefficacités des processus manuels et à débloquer des possibilités infinies.

Mettre en œuvre et déployer une sauvegarde et une restauration agiles et sécurisées pour une protection et une optimisation complètes des données.

Rationalisez les ressources, réduisez les coûts et surveillez l'ensemble de votre réseau, de la périphérie au cœur et au cloud, à l'aide d'une console unique et complète.

Solutions Veritas

Veritas Data Insight vous permet d'analyser l'activité et de fournir une analyse approfondie de l'utilisation et de l'activité collaborative. La solution permet de classer les utilisateurs et de mieux comprendre les modèles d'activité, d'identifier les données dupliquées, obsolètes ou orphelines et d'exploiter les scores de risque pour évaluer les menaces potentielles et donner la priorité aux données à haut risque. Créez des pistes d'audit détaillées et tirez parti de l'analyse intégrée des fichiers, de la prévention des pertes de données et de l'archivage avec les solutions de conformité de Veritas.

Les solutions Veritas Analytics permettent d'identifier rapidement les applications et les services à risque. Récupérez plus rapidement en ayant la possibilité de surveiller et d'optimiser les sauvegardes dans tous les environnements et de localiser efficacement les hôtes affectés par emplacement, environnement ou application.

Questions clés

- Vos données sont-elles optimisées pour une récupération rapide ?
- Comprenez-vous vos contrats de niveau de service ?

Pour une cybersécurité à toute épreuve. En savoir plus >

À propos de Veritas

Veritas Technologies est un leader dans la gestion des données multi-cloud. Plus de 80 000 entreprises, dont 91 % des entreprises faisant partie du classement Fortune 100, font confiance à Veritas pour les aider à assurer la protection, la restauration 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/fr/fr. Suivez-nous sur X : @veritastechllc.

VERITAS

veritas.com/fr/fr/

Pour obtenir nos coordonnées dans le monde entier, rendez-vous sur : veritas.com/fr/fr/company/contact

V1812 06/23