VERITAS

Contrôlez vos données dans le cloud

Un outil puissant pour surveiller vos données cloud et l'activité de vos utilisateurs.

La détection d'anomalies est un système de protection instantanée puissant, capable de détecter les activités inhabituelles ou les comportements étranges de vos données cloud ou de l'activité de vos utilisateurs et de tirer le signal d'alarme. En un mot, elle permet de détecter les problèmes avant qu'ils ne se produisent. La détection de ces anomalies constitue désormais une pratique essentielle pour la sécurité des données, car elles peuvent servir d'indicateurs d'une faille de sécurité, d'un problème de matériel ou de logiciel, d'une évolution de la demande des clients ou de tout autre problème nécessitant une attention immédiate. La détection consiste en un processus de recherche de points ou de modèles inhabituels dans un ensemble de données. Tout élément qui s'écarte d'une baseline établie (dans les limites de tolérance prédéfinies) est considéré comme une anomalie. Grâce à un ensemble établi de paramètres et d'indicateurs intelligents, les clients sont alertés en cas d'anomalie nécessitant une attention immédiate et peuvent facilement consulter un tableau de bord mis à jour en temps réel en fonction de la surveillance de l'activité. Parmi les exemples d'anomalies, on peut citer une activité inhabituelle d'écriture de fichiers qui pourrait indiquer une infiltration (mais qui pourrait aussi détecter des extensions de fichiers de ransomwares connus), des schémas d'accès aux fichiers, des chemins de trafic ou même un bond inhabituel de l'activité par rapport aux schémas habituels. Le fait d'être informé immédiatement de tout ce qui sort de l'ordinaire constitue un avantage précieux qui permet rapidement d'agir ou d'atténuer les effets de l'anomalie. Être informé de tout problème dès qu'il survient, atténuer un risque et l'isoler rapidement afin d'éviter toute destruction, tout arrêt ou tout autre problème lié à une faille de sécurité, voilà des avantages considérables pour une entreprise.

Les avantages de la surveillance des données

Avec l'explosion de la taille et de l'étendue des données cloud, la détection d'anomalies devient de plus en plus nécessaire pour surveiller toutes vos données cloud, en particulier face aux cybermenaces et aux ransomwares. Au fil du temps, les cybercriminels ont trouvé des moyens de plus en plus créatifs d'accéder aux systèmes et aux données. Ils s'introduisent dans un système, commencent à chiffrer les données et téléchargent tout ce qu'ils peuvent, pour ensuite s'échapper avant d'être détectés. Dans ce cas, la détection d'anomalies vous alerterait et vous aiderait à prendre les mesures nécessaires.

En 2022, le cloud représente le premier vecteur d'attaque de ransomware pour les cybercriminels[1]. Ils se servent souvent de stratégies à long terme, en s'inspirant des méthodes de la criminalité organisée. Ils ont perfectionné l'art de la cyber-reconnaissance. Une pratique souvent appelée « ransomware dormant » est désormais courante dans le monde numérique. Cela signifie qu'une fois qu'ils ont obtenu l'accès à vos systèmes, les cybercriminels se font discrets et restent masqués. Pourquoi ? Parce que leur priorité absolue est d'observer, d'apprendre et de se déplacer dans vos environnements cloud en essayant de trouver vos faiblesses et d'exploiter vos vulnérabilités, tout en attendant le meilleur moment pour frapper. Dans ce genre de situation, la possibilité de les détecter avant qu'ils ne puissent passer à l'action est un avantage stratégique qui vous permet de connaître les problèmes avant qu'ils ne surviennent et de prendre des mesures afin d'éviter des conséquences dévastatrices.

Les acteurs malveillants sont résolus à causer autant de dégâts que possible afin d'accroître leurs revenus et de maximiser leurs efforts. Comme pour toute entreprise qui se respecte, l'objectif principal est d'optimiser le retour sur investissement. Certains rapports suggèrent que les ransomwares peuvent rester dormants pendant jusqu'à 18 mois. Les acteurs malveillants sont conscients qu'une destruction optimale dépend de multiples facteurs, tels que le moment et la portée de l'attaque. Ils veulent que vous n'ayez pas d'autre choix que de payer leur rançon. L'époque où une faille et une attaque se produisaient au même moment est bien révolue. Cette complexité accrue signifie que les cybercriminels peuvent souvent connaître vos systèmes mieux que vous, ce qui augmente considérablement le risque qu'ils lancent une série d'événements conçus pour perturber et paralyser des systèmes critiques afin d'obtenir des paiements plus importants.

Visibilité sur les données entre les clouds

Avant de mettre en œuvre une détection d'anomalies efficace, il est important de prendre du recul pour vous assurer de connaître l'emplacement de toutes vos données et que votre environnement ne contienne pas de données obscures. Selon l'étude Veritas sur le retard dans l'élimination des vulnérabilités[2], 35 % des données sont toujours obscures. C'est un chiffre alarmant. Nous vous recommandons de commencer immédiatement un processus de découverte et de localisation de vos données.

Les solutions Veritas offrent un aperçu de toutes vos données sur l'ensemble de vos fournisseurs de cloud et de vos environnements physiques et virtuels. Vous obtenez également une vue d'ensemble de votre stockage, de votre capacité de calcul, de toutes vos principales solutions de protection des données ainsi que des fonctions de création de rapports croisés, afin de vous assurer qu'aucun système ne passe entre les mailles du filet. Ceci est particulièrement important dans le contexte actuel des menaces, car les cybercriminels espèrent que vous ne tenez pas un inventaire précis de toutes vos applications et données, ou que la sécurité et/ou la surveillance de vos données est limitée sur certains de vos systèmes.

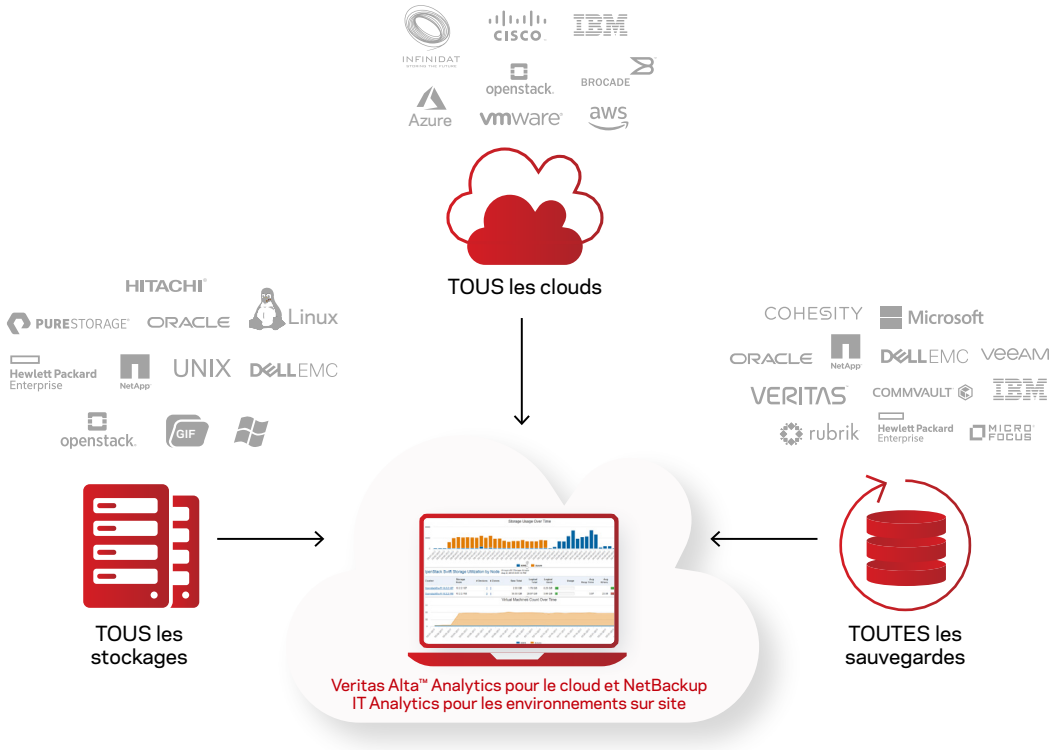


Figure 1 : Une infrastructure informatique unifiée pour toutes vos données, où qu'elles se trouvent

En plus d'éclairer les zones d'ombre de votre environnement, les solutions Veritas fournissent des informations complètes, des alertes et des rapports sur les systèmes sur site ou dans le cloud la protection des données et le stockage. Vous disposez alors des informations nécessaires pour prendre des décisions éclairées face à une cyberattaque grâce à des options de création de rapports qui vous aident à gagner en visibilité sur votre environnement de sauvegarde. Votre entreprise peut ainsi :

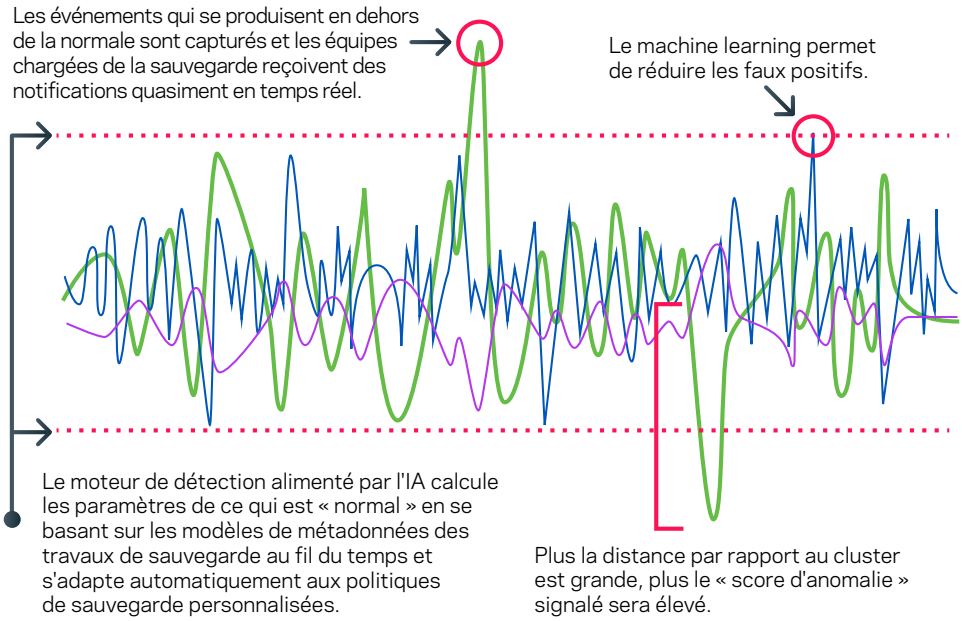
- Découvrir tous les hôtes ou les ordinateurs virtuels de votre infrastructure et les comparer avec les VM protégées par Veritas Alta™ Data Protection pour le cloud et NetBackup sur site
- Signaler les hôtes qui ne sont pas présents dans les sauvegardes ou ne présentent pas de sauvegarde récente comme représentant un risque potentiel
- Détecter les fichiers potentiellement infectés par un ransomware, ainsi que leur taille et leur emplacement dans l'environnement
- Accéder à des graphiques interactifs qui fournissent une vue historique des risques générés

Détection des anomalies basée sur l'IA entre les clouds

Une fois que la visibilité de vos données est en place, l'étape suivante consiste à mettre en œuvre une détection d'anomalies alimentée par l'IA. Veritas Alta™ Data Protection, pour le cloud, et NetBackup, pour les environnement sur site, détectent les données anormales et l'activité des utilisateurs sur l'ensemble de votre environnement et vous alertent en cas d'anomalies suspectes, pratiquement en temps réel. 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.

Pour visualiser la détection d'anomalies, il est utile d'imaginer un test polygraphique. Lorsque vous passez un test polygraphique, l'examinateur commence par un test préalable, au cours duquel il vous pose une série de questions afin d'établir les paramètres qui constitueront une baseline normale. Lorsque vous mentez, les indicateurs physiologiques que sont la pression artérielle**, le pouls, la respiration et la conductivité de la peau** fluctueront, comme on peut s'y attendre, en dehors des paramètres normaux établis. De même, Veritas Alta™ Data Protection, pour le cloud, et NetBackup, pour les environnements sur site, exploitent un moteur de détection alimenté par l'IA pour calculer les paramètres de conditions normales en fonction des modèles de métadonnées des travaux de sauvegarde au fil du temps. Ils sont automatiquement ajustés pour les politiques de sauvegarde personnalisées.

Les événements anormaux sont capturés et les notifications sont envoyées quasiment en temps réel. Les anomalies observées se voient attribuer une note basée sur leur gravité, qui est calculée en fonction de la distance observée par rapport au cluster. Plus la distance est grande, plus la note est élevée. Les administrateurs peuvent ainsi identifier les informations exploitables et réduire les faux positifs.



Moteur de détection d'anomalies alimenté par l'AI dans Veritas Alta™ Data Protection pour le cloud et NetBackup pour les environnements sur site

- Exploitez un volume immense de données
- Automatisez la surveillance et les rapports
- Obtenez des informations exploitables
- Produisez des rapports basés sur plusieurs critères
- Mettez en place un système d'alerte précoce en cas d'attaque

Figure 2 : Comprendre la détection d'anomalies

Globalement, le moteur de détection d'anomalies alimenté par l'IA vous aide à exploiter d'énormes quantités de données, à automatiser la surveillance et la création de rapports, à obtenir des informations exploitables, à créer des rapports basés sur plusieurs critères et, plus important encore, à mettre en place un système d'alerte précoce en cas d'attaque. Les administrateurs sont en mesure de consulter les données et de formuler des recommandations associées aux anomalies à tout moment, en surveillant tous les appareils et en établissant des alertes précoces en cas d'attaque, afin de rester au fait 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. Elle permet d'exploiter de grandes quantités de données et de fournir des informations exploitables pour faire face aux événements liés aux ransomwares, ainsi qu'à de simples changements dans l'environnement dont un administrateur doit être conscient. Ces solutions peuvent vous aider à reconnaître les signes précurseurs d'une attaque, ou le fait qu'elle est déjà en cours, et vous permet ainsi de prendre des mesures immédiates afin d'en limiter l'impact.

Cet outil est également intelligent et capable d'identifier les faux-positifs potentiels en comparant les sauvegardes historiques et la nouvelle sauvegarde. Il identifie les anomalies telles que les modifications de la durée des tâches, les modifications de la taille des images et/ou les modifications de la politique de configuration. Le moteur d'IA surveille les fichiers ou les groupes de fichiers et comprend quand les caractères du fichier changent (jusqu'au niveau des métadonnées), qu'il s'agisse d'un disque en bloc ou d'un stockage d'objets dans le cloud, le tout sans post-traitement. Seule Veritas est capable d'analyser et de surveiller tous les systèmes et de couvrir toutes les plates-formes cloud, y compris les produits de sauvegarde tiers, le tout de manière indépendante. Notre moteur d'intelligence artificielle/de machine learning (IA/ML) peut être exécuté sur n'importe quel serveur. Ce niveau de couverture permet d'éliminer les angles morts.

Détection des logiciels malveillants

Veritas peut vous aider à détecter plusieurs types de logiciels malveillants, notamment le chiffrement et l'exfiltration, à l'aide des analyses automatisées et à la demande. La fonction de détection automatisée des logiciels malveillants supprime les dépendances humaines et permet à la technologie IA/ML d'intervenir et de rechercher des logiciels malveillants. La détection IA/ML de logiciels malveillants est automatiquement déclenchée par un score d'anomalie élevé. La détection inclut les données non structurées, Windows, Linux et VMware. 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.

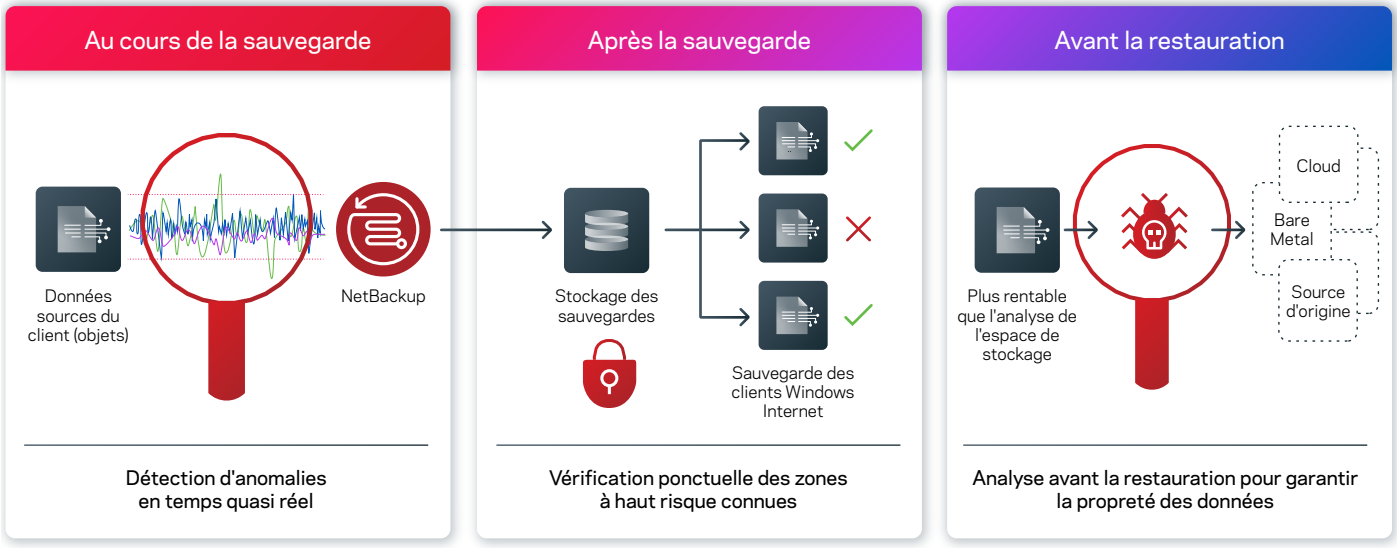


Figure 3 : Aperçu de la détection des logiciels malveillants

De plus, lorsqu'une restauration est nécessaire, les données de sauvegarde peuvent être analysées, ce qui permet d'exploiter les dernières signatures des logiciels malveillants. 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 ».

La sécurité est au cœur de Veritas

Veritas offre la visibilité unifiée des données, la détection d'anomalies et la détection des logiciels malveillants grâce à Veritas Alta™ Analytics pour le cloud et NetBackup IT Analytics pour les environnements sur site. Vous trouverez ci-dessous l'illustration d'un tableau de bord.

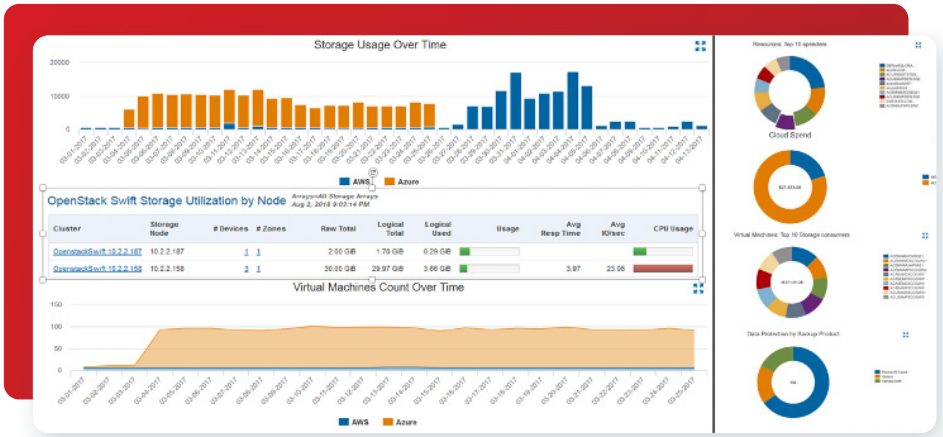


Figure 4 : Exemple de tableau de bord NetBackup IT Analytics montrant l'utilisation du stockage au fil du temps.

Caractéristiques de la solution Veritas Analytics :

- **Complète** : solution unique permettant d'identifier des ressources en données à partir d'une console intégrée, Veritas Alta™ Analytics, pour le cloud, et NetBackup IT Analytics, pour les environnements sur site, assurent la prise en charge de tous les serveurs, systèmes de stockage, hyperviseurs, bases de données et plates-formes applicatives que les entreprises actuelles utilisent le plus.
- **Évolutive** : la gestion centralisée fournit un collecteur de données sans agent qui rassemble environ 30 000 points de données uniques provenant de tous les aspects des environnements sur site et dans le cloud y compris les applications, le cloud, la protection des données, les hôtes, le réseau, le stockage, la virtualisation et les données non structurées.
- **Innovante** : des algorithmes propriétaires, optimisés par cinq brevets de conception autonome et des mises à jour à partir du cloud, analysent les points de données et formulent des recommandations qui améliorent les performances, la résilience et l'utilisation des systèmes. L'analyse est dirigée par la machine, mais régie par des politiques humaines. Les données sont utilisées pour présenter des solutions exploitables afin d'améliorer les mesures d'efficacité et de minimiser les risques, de prévoir les défaillances et de rationaliser les audits et la conformité.
- **Éprouvée** : depuis plus d'une décennie, NetBackup IT Analytics, qui inclut désormais Veritas Alta™ Analytics pour le cloud, domine le secteur grâce à une évolutivité et une fiabilité éprouvées par les clients, en rassemblant et en analysant les données associées à l'ensemble d'une entreprise.

Principales fonctionnalités de Veritas Analytics :

- Une console intégrée fournissant des informations sur les éléments suivants :
  - Sauvegarde, calcul et stockage locaux et dans le cloud
  - Capacité, coût et utilisation dans le cloud et sur site
- Ventilation des frais :
  - Par groupe défini par l'utilisateur, tel que l'application, le service et le centre de coûts
  - Utilisation de la sauvegarde, du cloud, du calcul et du stockage
- Planification de la capacité :
  - Budget basé sur les coûts du cloud et les taux d'utilisation
  - Planification des supports et du stockage basée sur la consommation

Optimisez la valeur commerciale du cloud avec Veritas Alta™ Analytics pour le cloud et NetBackup IT Analytics pour les environnements sur site

Chez Veritas, nous avons constaté que les entreprises choisissent le cloud pour plusieurs raisons : les petites entreprises bénéficient d'une réduction des coûts liés à l'entretien d'un data center et/ou d'un site de reprise après incident ; les entreprises de taille moyenne apprécient le stockage accessible de données hors site basé sur un matériel hautement évolutif et tirent parti de la restauration « just in time » dans le cloud ; les grandes entreprises, pour leur part, identifient les charges de travail capables de tirer parti de la disponibilité et du coût du cloud et réservent l'espace coûteux d'un data center aux charges de travail critiques. Il arrive qu'une entreprise ait besoin d'un espace temporaire pour exécuter une certaine charge de travail. Au lieu de mettre en place un nouveau rack de disques dans un data center, elle peut exploiter l'espace d'un fournisseur de services cloud pour éviter les coûts supplémentaires liés à l'achat de matériel pour le data center. Les modèles d'abonnement cloud sont idéaux pour ces projets, car ils offrent des modèles évolutifs et simples à utiliser.

La tendance de fond actuelle du transfert de données vers le cloud part du besoin des entreprises de réduire leurs coûts. Le modèle cloud est souple et permet aux entreprises d'ajouter un disque à un serveur facilement et rapidement, plutôt que d'investir dans du matériel et dans l'intégration qui l'accompagne. Le cloud permet également aux entreprises d'éviter les coûts et les délais liés au remplacement ou à la mise à niveau du matériel et des logiciels dans le data center. Ces exigences sont remplies par le fournisseur de services cloud et ne concernent pas l'entreprise elle-même. Quelle que soit la raison à l'origine de la décision d'une entreprise de passer au cloud, Veritas Alta™ Analytics, pour le cloud, et NetBackup IT Analytics, pour les environnement sur site, peuvent assurer une expérience conforme et rentable par rapport à un environnement sur site.

Veritas vous fournit une surveillance basée sur l'intelligence artificielle et vous permet de prendre le contrôle de vos données cloud et de leur expansion. Avec Veritas, vous pouvez être certain de l'emplacement de vos données, grâce à une interface unique pour toutes les données d'entreprise, où qu'elles se trouvent. Nos solutions évoluent facilement tout en fournissant des performances optimales en termes de capacités en pétaoctets, et ouvre la voie de l'informatique en tant que service grâce à un fonctionnement en libre-service pratique. Grâce à ses solutions analytiques, Veritas élimine les incertitudes à l'aide d'une technologie de visibilité complète des données, de la détection intelligente des anomalies et de la recherche de programmes malveillants.

Au-delà des utilitaires et des produits ponctuels cloud natifs, il convient d'élaborer une stratégie unifiée pour la gestion des données qui donne la priorité à la cybersécurité et à la protection des données.

Veritas vous permet de contrôler le cloud.

1. https://www.esg-global.com/ransomware
2. https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

À propos de Veritas

Veritas Technologies est un leader mondial de la protection et disponibilité des données. Plus de 80 000 clients, dont 95 % du classement Fortune 100, comptent sur nous pour faire abstraction de la complexité informatique et simplifier la gestion des données. La plate-forme Veritas Enterprise Data Services automatise la protection et orchestre la récupération des données partout où elles se trouvent, garantit la disponibilité des applications critiques, 24 h/24 et 7 j/7, et fournit aux entreprises les informations dont elles ont besoin pour se conformer à une réglementation en constante évolution. Réputée pour sa fiabilité à grande échelle et son modèle de déploiement adapté à tous les besoins, la plate-forme Veritas Enterprise Data Services prend en charge plus de 800 sources de données différentes, plus de 100 systèmes d'exploitation différents, plus de 1 400 cibles de stockage et plus de 60 plates-formes cloud différentes. Pour en savoir plus, rendez-vous sur www.veritas.com ou suivez-nous sur Twitter : @veritastechllc.

VERITAS

veritas.com/fr

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

V1627 12/22