Erkennen von Anomalien für Cloud-Daten

Ein leistungsstarkes Tool zur Überwachung von Cloud-Daten und Benutzeraktivitäten.

Die Anomalieerkennung ist ein leistungsstarkes Frühwarnsystem, das ungewöhnliche Aktivitäten oder ungewöhnliche Verhaltensweisen Ihrer Cloud-Daten und Benutzeraktivitäten verfolgt und Sie diesbezüglich warnt. Im Wesentlichen hilft sie dabei, Probleme zu erkennen, bevor sie auftreten. Das Erkennen dieser Anomalien ist heute eine ausschlaggebende Praxis für die Datensicherheit, da Anomalien Indikatoren für eine Kompromittierung, ein Hardware- oder Softwareproblem, veränderte Kundenanforderungen oder eine Reihe von Herausforderungen sein können, die sofortige Aufmerksamkeit erfordern. Sie funktioniert durch Anwendung eines Prozesses, bei dem ungewöhnliche Punkte oder Muster in einem Datensatz lokalisiert werden. Alles, was von einer festgelegten Basis (innerhalb einer vordefinierten Toleranz) abweicht, wird als Anomalie betrachtet. Mit einem Satz von Parametern und intelligenten Indikatoren wird vor Anomalien gewarnt, die sofortige Aufmerksamkeit erfordern. Sie sind auch über ein Dashboard abrufbar, das in Echtzeit mit Aktivitätsüberwachung aktualisiert wird. Beispiele für Anomalien sind ungewöhnliche Dateischreibaktivitäten, die auf eine Infiltration hindeuten (aber auch bekannte Ransomware-Dateierweiterungen werden erkannt), Dateizugriffsmuster, Datenverkehrspfade oder sogar ein ungewöhnlicher Anstieg der Aktivität im Vergleich zu typischen Mustern. Unmittelbar über etwas Außergewöhnliches benachrichtigt zu werden, bietet einen wertvollen Vorteil, um schnell zu handeln oder Abhilfe zu schaffen. Es zahlt sich aus, bei jedem auftretenden Problem den Überblick zu behalten oder ein Risiko zu mindern und es schnell zu isolieren, um Zerstörungen, Ausfallzeiten oder andere Probleme im Zusammenhang mit einem Verstoß zu verhindern.

Die Bedeutung eines Datenwächters

Angesichts der explodierenden Menge und Verbreitung von Cloud-Daten steigt der Bedarf an Anomalieerkennung als eine Art Wachturm über all Ihre Cloud-Daten, insbesondere in Zeiten von Cyberbedrohungen und Ransomware. In der Vergangenheit haben sich Cyberkriminelle auf verschiedenen kreativen Wegen Zugang zu Systemen und Daten verschafft. Sie gelangen in ein System, beginnen mit der Verschlüsselung und laden möglichst viel herunter, bevor sie sich aus dem Staub machen. In diesem Szenario würde Sie die Anomalieerkennung auf das Problem aufmerksam machen und Ihnen helfen, Maßnahmen zu ergreifen.

Die Cloud war 2022 der Ransomware-Angriffsvektor Nummer eins für Cyberkriminelle[1]. Mittlerweile setzen sie oft auf eine langfristige Strategie und schauen sich Tricks aus dem Handbuch der organisierten Kriminalität ab. Sie haben die Kunst der Ausspähung perfektioniert. Eine Praxis, die oft als ruhende Ransomware oder Sleeper-Ransomware bezeichnet wird, kommt in der digitalen Welt immer häufiger vor. Dies bedeutet, dass Kriminelle, sobald sie Zugang erhalten, erst einmal im Verborgenen bleiben. Warum? Weil ihre oberste Priorität darin besteht, Ihre Cloud-Umgebungen zu beobachten, zu lernen und sich darin zu bewegen, um Ihre Schwachstellen zu finden und auszunutzen – und dabei auf den optimalen Zeitpunkt zum Zuschlagen zu warten. In dieser Situation bietet die rechtzeitige Erkennung eine hervorragende Möglichkeit, schnell auf Probleme aufmerksam zu werden und zu handeln, um verheerende Auswirkungen zu verhindern.

Kriminelle sind hochmotiviert, möglichst viel Zerstörung anzurichten, um größeren Profit zu machen, und maximieren daher ihre Bemühungen – wie bei jedem Unternehmen dreht sich alles um den ROI. Einige Berichte melden, dass Ransomware bis zu 18 Monate inaktiv bleiben kann. Kriminelle wissen, dass eine optimale Zerstörung von mehreren Faktoren wie Timing und Umfang abhängt. Sie zielen darauf ab, Ihnen keine andere Wahl zu lassen, als das geforderte Lösegeld zu bezahlen. Die alten Zeiten, in denen ein Verstoß und ein Angriff gleichzeitig stattfanden, sind längst vorbei. Diese zusätzliche Komplexität bedeutet, dass sie Ihre Systeme oft besser kennen als Sie selbst. Daher steigt die Wahrscheinlichkeit drastisch an, dass sie eine Reihe von Ereignissen starten, die darauf abzielen, kritische Systeme zu stören und zu deaktivieren, um danach größere Summen zu verlangen.

Cloud-übergreifende Datentransparenz

Bevor ein Unternehmen eine erfolgreiche Anomalieerkennung implementieren kann, ist es wichtig, zunächst einen Schritt zurückzutreten. Sie müssen unbedingt wissen, wo sich alle Ihre Daten befinden, und sicherstellen, dass in Ihrer Umgebung keine Dark Data lauern. Laut einer Studie von Veritas[2] sind 35 Prozent der Daten immer noch unstrukturiert. Das ist eine erschreckend hohe Zahl. Wir empfehlen Ihnen, sich sofort an die Arbeit zu machen und herauszufinden, welche Daten Sie haben und wo sie sich befinden.

Veritas-Lösungen bieten einen umfassenden Überblick über alle Ihre Daten in allen Umgebungen - Cloud, physisch und virtuell. Sie haben auch einen Überblick über Ihren Speicher, die Rechenkapazität, alle wichtigen Datenschutzlösungen und produktübergreifende Berichterstellung, wodurch sichergestellt wird, dass kein System durchs Raster fällt. Dies ist besonders wichtig in der heutigen Bedrohungslandschaft, da Cyberkriminelle hoffen, dass Sie keine genaue Bestandsaufnahme aller Ihrer Anwendungen und Daten führen oder dass es Bereiche gibt, in denen Sie nur begrenzte Sicherheit und/oder Kontrolle über Ihre Daten haben.

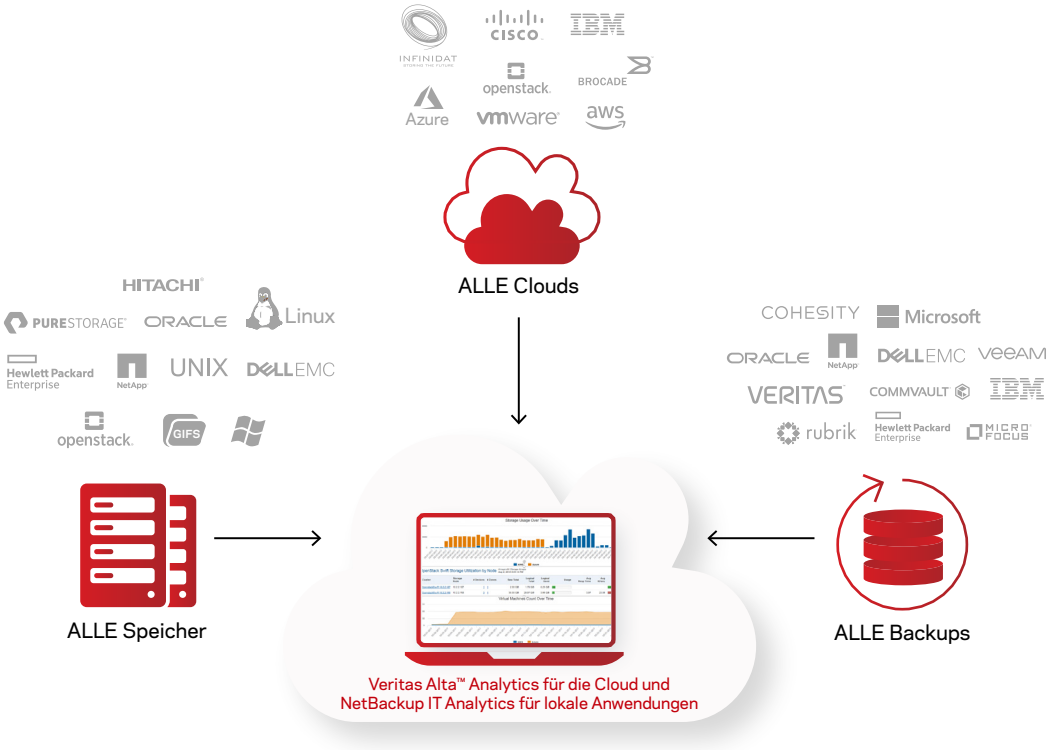


Abbildung 1: Einheitliche IT-Infrastruktur für alle Ihre Daten, unabhängig von ihrem Speicherort

Die Lösungen von Veritas bringen nicht nur Licht in die dunklen Bereiche Ihrer Umgebung, sondern bieten auch umfassende Einblicke, Warnungen und Berichte für On-Premises, Cloud, Datenschutz und Speicherung. Sie erhalten die nötigen Einblicke, um angesichts eines Cyberangriffs fundierte Entscheidungen treffen zu können, mit Berichtsoptionen, die Ihnen helfen, Einblick in Ihre Backup-Umgebung zu gewinnen:

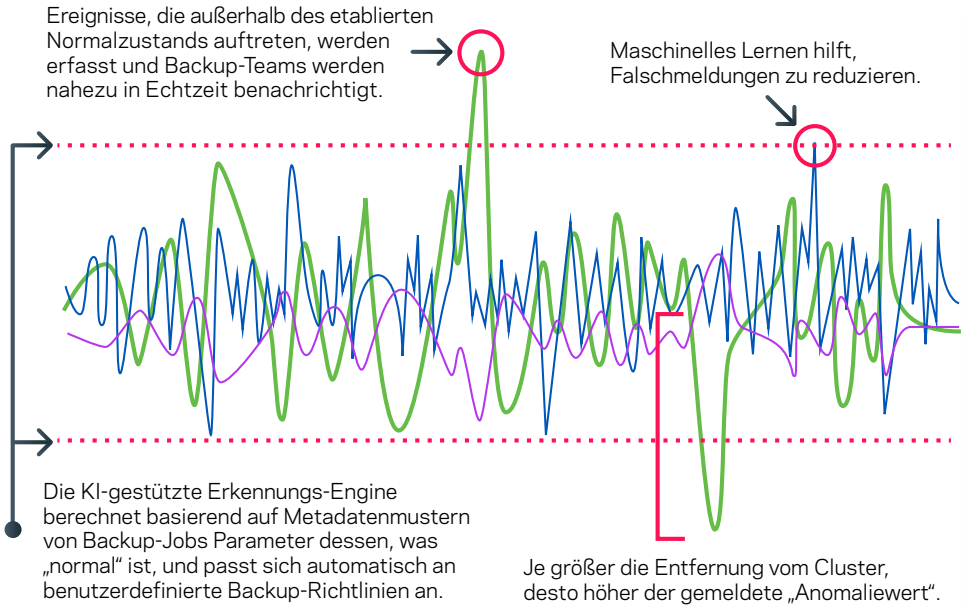
- Sehen Sie alle Hosts oder virtuellen Computer (VMs) in Ihrer Infrastruktur und vergleichen Sie sie mit den VMs, die von Veritas Alta™ Data Protection für Clouds und von NetBackup für On-Prem geschützt werden
- Kennzeichnen Sie Hosts, die in den Backups fehlen oder keine aktuellen Backups haben, als potenzielle Risiken
- Erkennen Sie potenziell von Ransomware betroffene Dateien zusammen mit ihrer Größe und ihrem Speicherort in der Umgebung
- Greifen Sie auf interaktive Diagramme zu, die eine historische Ansicht der generierten Risiken bieten

KI-übergreifende Erkennung von Anomalien in der Cloud

Sobald Datentransparenz vorhanden ist, besteht der nächste Schritt darin, eine KI-gestützte Anomalieerkennung zu implementieren. Veritas Alta™ Data Protection für die Cloud und NetBackup für lokale Speicher erkennen anomale Daten und Benutzeraktivitäten in Ihrer gesamten Umgebung und warnen Sie nahezu in Echtzeit vor verdächtigen Anomalien. Die Technologie wurde entwickelt, um eine enorme Menge an Daten zu analysieren, die Überwachung und Berichterstattung zu automatisieren und umsetzbare Einblicke in alle Vorgänge in der Umgebung zu liefern.

Eine gute Möglichkeit, die Anomalieerkennung zu visualisieren, besteht darin, sie sich als Lügendetektortest vorzustellen. Bei einem solchen Test beginnt der Prüfer mit einer Voruntersuchung, bei der er eine Reihe von Fragen stellt, um die Parameter des Normalen abzustecken. Wenn Sie lügen, **schwanken die physiologischen Indikatoren für** Blutdruck, Puls, Atmung und Hautleitfähigkeit erwartungsgemäß außerhalb dieser Parameter. In ähnlicher Weise nutzen Veritas Alta™ Data Protection und NetBackup eine KI-gestützte Erkennungs-Engine, um auf der Grundlage von Backup-Job-Metadatenmustern im Laufe der Zeit zu ermitteln, was für die Umgebung normal ist, und sich automatisch an benutzerdefinierte Backup-Richtlinien anpassen.

Ereignisse, die außerhalb des etablierten Normalzustands auftreten, werden erfasst, und Benachrichtigungen erfolgen nahezu in Echtzeit. Erkannten Anomalien wird basierend auf dem Schweregrad eine Punktzahl zugewiesen, die anhand der beobachteten Entfernung vom Cluster berechnet wird. Je größer die Entfernung, desto höher die Punktzahl. Dies soll Administratoren dabei helfen, zu erkennen, welche Erkenntnisse umsetzbar sind, und Fehlalarme zu reduzieren.



KI-gestützte Engine zur Anomalieerkennung in Veritas Alta™ Data Protection für die Cloud und NetBackup für On-Prem-Anwendungen

- Analyse enormer Datenmengen
- Automatisierte Überwachung und Berichterstattung
- Verwertbare Erkenntnisse
- Bericht basierend auf mehreren Kriterien
- Frühwarnung vor einem Angriff

Abbildung 2: Verständnis der Anomalieerkennung.

Insgesamt hilft Ihnen die KI-gestützte Anomalie-Erkennungs-Engine dabei, enorme Datenmengen zu durchsuchen, die Überwachung und Berichterstattung zu automatisieren, umsetzbare Erkenntnisse zu gewinnen, Berichte auf der Grundlage mehrerer Kriterien zu erstellen und, was noch wichtiger ist, eine Frühwarnung bei Angriffen zu erhalten. Administratoren können jederzeit Daten anzeigen und Empfehlungen zu Anomalien geben, indem sie alle Geräte überwachen, um bei auftretenden Problemen auf dem Laufenden zu bleiben. Beispielsweise lässt sich die KI-gestützte Anomalieerkennung von Veritas nahtlos in den primären Server integrieren und ermöglicht es ihm, anomale Formen von Beobachtungen zu erkennen – wobei diejenigen, die nicht in den Cluster fallen, als Anomalien oder Ausreißer betrachtet werden. Mit dieser Funktion kann ein Administrator Anomalien erkennen und einen Drilldown durchführen, um Bedenken zu identifizieren. Es bietet die Möglichkeit, große Datenmengen zu durchsuchen und umsetzbare Informationen bereitzustellen, um Ransomware-Ereignisse sowie einfache Änderungen in der Umgebung zu beheben, die ein Administrator kennen sollte. Diese Lösungen können dabei helfen, Anzeichen dafür zu erkennen, dass ein Angriff im Gange ist oder möglicherweise kurz bevorsteht, sodass Sie sofort Maßnahmen ergreifen und die Auswirkungen begrenzen können.

Das Tool ist auch intelligent und verfügt über die Fähigkeit, potenzielle Fehlalarme zu identifizieren, indem es historische Backups mit dem neuen Backup vergleicht und Anomalien wie signifikante Änderungen in der Auftragsdauer, Variationen der Image-Größe und/oder Änderungen der Richtlinienkonfiguration erkennt. Die KI-Engine überwacht Dateien oder Dateigruppen und sieht, wenn sich Dateizeichen ändern (bis auf die Metadatenebene), unabhängig davon, ob sie sich auf einer Blockfestplatte oder im Objektspeicher in der Cloud befinden – alles ohne Nachbearbeitung. Nur Veritas kann alle Systeme scannen und überwachen, ist Anbieter-agnostisch und kann alle Cloud-Plattformen einschließlich Backup-Produkte von Drittanbietern abdecken. Unsere Engine für künstliche Intelligenz/maschinelles Lernen (AI/ML) ist mit jedem Server kompatibel. Dieser Abdeckungsgrad stellt sicher, dass blinde Flecken verschwinden.

Malware-Scan

Veritas hilft Ihnen bei der Erkennung verschiedener Arten von Malware, z. B. Verschlüsselung und Exfiltration, und bietet automatisierte und On-Demand-Scans. Die Funktion zum automatisierten Malware-Scannen beseitigt menschliche Abhängigkeiten und integriert KI/ML-Technologie in den Prozess. Der AI/ML-Malware-Scan wird automatisch durch einen hohen Anomalie-Score ausgelöst und umfasst unstrukturierte Daten, Windows, Linux und VMware. Diese Aufnahme ist von entscheidender Bedeutung, da Malware häufig über ein Hauptverzeichnis in Ihre Umgebung gelangt, weil dort meist große Mengen unstrukturierter Daten vorhanden sind.

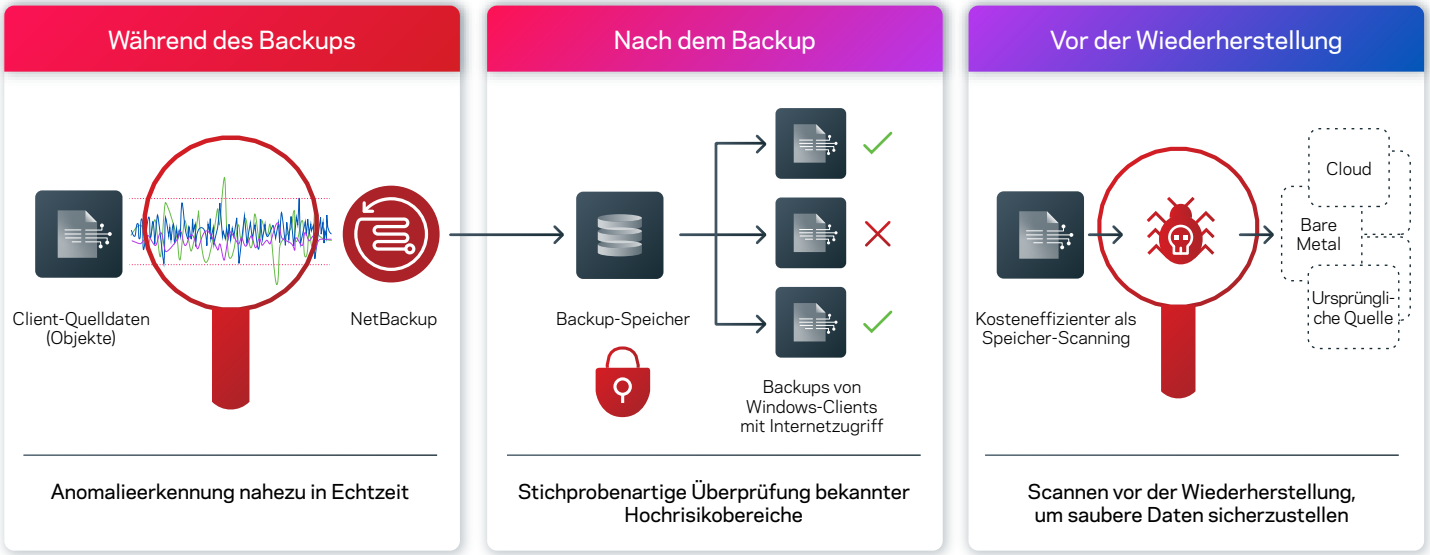


Abbildung 3: Überblick über Malware-Scans

Wenn eine Wiederherstellung erforderlich ist, können die Backup-Daten ebenfalls gescannt werden, um sicherzustellen, dass die neuesten Malware-Signaturen genutzt werden. Klare visuelle Darstellungen und Warnhinweise machen auf infizierte Backups aufmerksam und stellen sicher, dass alle wiederhergestellten Daten sauber und unbeeinträchtigt sind. Diese Vorgehensweise wird oft als Wiederherstellen der letzten als funktionierend bekannten Kopie bezeichnet.

Veritas – sicher von Grund auf

Veritas bietet all diese einheitliche Datentransparenz, Anomalieerkennung und Malware-Scans über Veritas Alta™ Analytics für die Cloud und NetBackup IT Analytics für On-Premises. Ein Beispiel-Dashboard ist unten abgebildet.

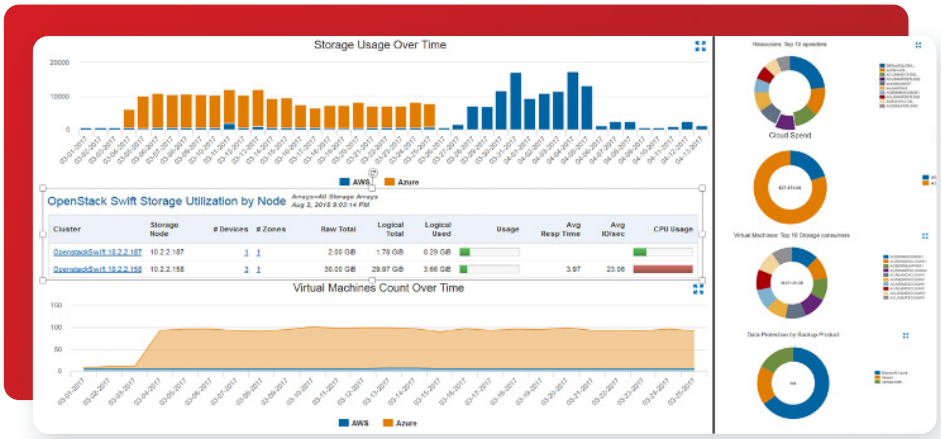


Abbildung 4: Ein Beispiel-Dashboard von NetBackup IT Analytics, das die Speichernutzung im Laufe der Zeit zeigt.

Merkmale von Veritas Analytics:

- **Umfassend**: Veritas Alta™ Analytics für die Cloud und NetBackup IT Analytics für On-Prem-Anwendungen ermöglichen die Identifizierung von Datenbeständen mit nur einer Konsole und bieten Unterstützung für alle gängigen Server, Speicher, Hypervisoren, Datenbanken und Anwendungsplattformen, die heute von Unternehmen verwendet werden.
- **Skalierbar**: Das zentralisierte Management bietet einen agentenlosen Daten-Collector, der ungefähr 30.000 eindeutige Datenpunkte aus allen Aspekten von lokalen und Cloud-Umgebungen sammelt, einschließlich Anwendungen, Cloud, Datenschutz, Hosts, Netzwerk, Speicher, Virtualisierung und unstrukturierte Daten.
- **Innovativ**: Proprietäre Algorithmen – gestützt von fünf Patenten für autonomes Design und Updates aus der Cloud – analysieren Datenpunkte und geben Empfehlungen ab, die die Leistung, Ausfallsicherheit und Nutzung verbessern. Die Analyse erfolgt maschinell, wird jedoch von menschlichen Richtlinien gesteuert und nutzt die Daten, um umsetzbare Lösungen zu präsentieren, die dazu beitragen, Effizienzmaßnahmen zu verbessern und Risiken zu minimieren, Ausfälle vorherzusagen und Audits und Compliance zu rationalisieren.
- **Bewährt**: Seit mehr als einem Jahrzehnt ist NetBackup IT Analytics und nun auch Veritas Alta™ Analytics für die Cloud branchenführend bei Skalierbarkeit und Zuverlässigkeit, führt Daten aus dem gesamten Unternehmen zusammen und analysiert sie.

Hauptmerkmale von Veritas Analytics:

- Eine integrierte Konsole bietet Einblick in:
  - lokale und Cloud-Backups, Computing und Speicher
  - Cloud- und On-Prem-Kapazität, -Kosten und -Nutzung
- Nutzungsorientierte Abrechnung:
  - nach beliebigen benutzerdefinierten Gruppen wie Anwendung, Abteilung und Kostenstelle
  - in allen Backups und Clouds, Computing-Anwendungen und Speichern
- Kapazitätsplanung:
  - Budget basierend auf Cloud-Kosten und Nutzungsraten
  - Medien-/Speicherplanung basierend auf der Verbrauchsnutzung

Maximieren Sie den geschäftlichen Nutzen der Cloud mit Veritas Alta™ Analytics für die Cloud und NetBackup IT Analytics für On-Premises

Wir bei Veritas haben festgestellt, dass der Wechsel in die Cloud aus mehreren Gründen erfolgt: Kleinere Unternehmen profitieren davon, dass sie den Aufwand für die Wartung eines Rechenzentrums und/oder einer Disaster-Recovery-Site reduzieren; mittelständische Unternehmen schätzen die Möglichkeit der externen Datenspeicherung, die auf hochskalierbarer Hardware basiert und die Just-in-Time-Wiederherstellung aus der Cloud nutzt; und große Unternehmen identifizieren Workloads, die in der Lage sind, die Vorteile der Cloud-Verfügbarkeit und -Kosten zu nutzen und geben gleichzeitig teure Rechenzentrumsfläche für unternehmenskritische Workloads frei. Manchmal wird nur vorübergehend Speicherplatz für eine Workload benötigt. Anstatt ein neues Rack mit Festplatten in einem Rechenzentrum hochzufahren, kann dann Platz bei einem Cloud-Anbieter gemietet werden, sodass keine zusätzlichen Kosten für gekaufte Rechenzentrumshardware entstehen. Cloud-Abonnementmodelle eignen sich gut für solche Projekte und bieten skalierbare, einfach zu verwendende Modelle.

Beim aktuellen Megatrend, Daten in die Cloud zu verlagern, geht es darum, die geschäftlichen Kosten zu senken. Das Cloud-Modell lässt sich flexibel an Anforderungen anpassen, und ermöglicht es Unternehmen, einfach und schnell eine Festplatte hinzuzufügen, anstatt für Hardware und den dazugehörigen Einbau zu bezahlen. Die Cloud spart zudem Zeit und Geld, die mit dem Austausch oder Upgrade von Hardware und Software im Rechenzentrum verbunden sind. Stattdessen kümmert sich der Cloud-Service-Anbieter um all dies. Unabhängig davon, aus welchem Grund sich ein Unternehmen für den Wechsel in die Cloud entscheidet, können Veritas Alta™ Analytics bzw. NetBackup IT Analytics sicherstellen, dass das Erlebnis im Vergleich zu einer lokalen Umgebung konform und kostengünstig ist.

Veritas bietet Ihnen einen KI-gestützten Wächter, damit Sie die Kontrolle über Ihre wachsenden Cloud-Daten übernehmen können. Dank Veritas wissen Sie stets, wo sich alle Ihre Daten befinden und erhalten mit nur einer Konsole den vollständigen Überblick darüber, unabhängig vom Speicherort. Es lässt sich leicht skalieren, bietet gleichzeitig die beste Leistung seiner Klasse für Kapazitäten auf Petabyte-Ebene und ebnet den Weg zu IT-as-a-Service durch bequemen Self-Service-Betrieb. Veritas beseitigt Unsicherheiten mit umfassender Datensichtbarkeitstechnologie, intelligenter Anomalieerkennung und Malware-Scanning – alles bereitgestellt durch unsere Analyselösungen.

Denken Sie über Cloud-native Dienstprogramme und Einzelprodukte hinaus und entwickeln Sie eine einheitliche Strategie für das Datenmanagement, bei der Cybersicherheit und Datenschutz an erster Stelle stehen.

Mit Veritas übernehmen Sie die Kontrolle über die 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

Über Veritas

Veritas Technologies ist ein weltweit führender Anbieter von Datenschutz und Verfügbarkeit. Über 80.000 Kunden – darunter 95 Prozent der Fortune 100 – verlassen sich darauf, dass wir die IT-Komplexität abstrahieren und das Datenmanagement vereinfachen. Die Veritas Enterprise Data Services Platform automatisiert den Schutz und koordiniert die Wiederherstellung von Daten überall dort, wo sie sich befinden, stellt die Verfügbarkeit geschäftskritischer Anwendungen rund um die Uhr sicher und liefert Unternehmen die Einblicke, die sie benötigen, um die sich entwickelnden Datenvorschriften einzuhalten. Veritas Enterprise Data Services Platform ist bekannt für Zuverlässigkeit im großen Maßstab und ein Bereitstellungsmodell, das allen Anforderungen gerecht wird. Veritas Enterprise Data Services Platform unterstützt mehr als 800 verschiedene Datenquellen, über 100 verschiedene Betriebssysteme, mehr als 1.400 Speicherziele und mehr als 60 verschiedene Cloud-Plattformen. Erfahren Sie mehr unter www.veritas.com. Folgen Sie uns auf Twitter unter @veritastechllc.

VERITAS

Veritas (Deutschland) GmbH
Theatinerstr. 11, 8. Etage
80333 München
Tel.: 0800-724 40 75
veritas.com/de/de

Die weltweiten Kontaktinformationen finden Sie hier:
veritas.com/de/de/company/contact

V1627 12/22