VERITAS

Jetzt handeln, um die Zukunft zu sichern

IM SPITZENFELD MIT DABEI SEIN

Datenschutz und -wiederherstellung ist kein Rennen, sondern eine Fahrt auf einem oft kurvenreichen Weg.

Die Bedrohungen für Ihre Daten nehmen zu und ändern sich. Cyberkriminelle entwickeln neue Angriffsmethoden, um sich Zugriff auf die Lebensadern Ihres Unternehmens verschaffen.

Der Datenschutz ist nicht mehr einfach nur eine Randnotiz, vielmehr ist er zu einem bedeutsamen Aspekt der Unternehmenskultur mit zahlreichen beweglichen Teilen geworden. Die Vielfalt und der Standort der Workloads sowie die Kritikalität jeder Anwendung und ihrer Daten sind wichtige Komponenten bei der Beurteilung des erforderlichen Schutzniveaus und der Art und Weise, wie Sie mit der Wiederherstellung umgehen.

Faktoren wie Hochverfügbarkeit, Governance und Compliance spielen alle eine Rolle und wirken sich auf Zielsetzungen wie Wiederherstellungszeit (RTO) und Wiederherstellungspunkt (RPO) aus.

Schatten-IT und Tech-Schulden erleben ein starkes Wachstum. Teams erzeugen massive Datenmengen und lassen geschäftskritische Daten ungewollt angreifbar werden. Unternehmen fehlt der vollständige Überblick über das Wesentliche, was es schwierig macht, Prioritäten zu setzen, um Risiken zu mindern.

Indem Sie vorausschauend planen und umsichtig handeln, können Sie Ihre Führung halten und sind gegen Herausforderungen auf dem Weg gut gerüstet.

Die eigenen Daten kennen

Wie können Sie etwas schützen, von dem Sie gar nichts wissen?

Zahlreiche Apps und Plattformen versprechen Effizienzsteigerungen und effektivere Daten. Ihre Teams beginnen, diese Tools in Silos zu nutzen; sie speisen Kundeninformationen und Unternehmensdaten in Plattformen ein, die sich immer häufiger in der Cloud befinden. Das Ergebnis? Ein unkontrollierter Wildwuchs von Daten und ein Multi-Cloud-Abdeckungsproblem.

Cyberkriminelle können diese Daten infiltrieren, da sie vom Unternehmen nicht ordnungsgemäß abgedeckt werden. Verdächtiges Verhalten kann unbemerkt bleiben, weil das IT-Team die Daten nicht auf dem Radar hat und möglicherweise von ihrer Existenz gar nichts weiß. Erst wenn eine Katastrophe eintritt, erfahren Sie, dass wichtige Informationen nicht ordnungsgemäß gesichert waren.

Kritische Informationen, von denen es keine Backups gibt, können dann auch nicht wiederhergestellt werden und sind für immer verloren.

Datenwildwuchs ist eine Herausforderung im Governance-Bereich, die neben einer verbesserten Transparenz der Unternehmensinfrastruktur mehr Struktur und Mitarbeiterschulung erfordert.

Um gegen Katastrophen besser gewappnet zu sein, stellen Sie Daten in einen Kontext und schätzen Sie Risiken bei komplexen Verfahren ein, um sinnvolle Entscheidungen bezüglich Backup- und Recovery-Strategien von Edge, Core und Cloud zu treffen.

Grundlegende Fragen:

- Was für Daten haben Sie und wo sind sie untergebracht?
- Wie lässt sich die Sichtbarkeit unserer Daten erhöhen?

Veritas-Lösungen

Die Veritas Datensicherheitslösungen bieten Datenschutz nach Maß. Die KI-gesteuerte Anomalieerkennung hilft dabei, enorme Datenmengen zu durchforsten, die Überwachung und Berichterstellung zu automatisieren und bei potenziellen Angriffen Frühwarnungen auszugeben.

Veritas Analytics-Lösungen helfen dabei, Server und Speicher mit all Ihren Backup-Anbietern abzugleichen, um sicherzustellen, dass nichts durchs Raster fällt und angreifbar bleibt. Es können sämtliche Systeme, einschließlich Produkte von Drittanbietern, gescannt und überwacht werden, um blinde Flecken zu beseitigen.

Veritas Data Insight kann Ihnen helfen, das Potenzial der Berichterstellung zu entdecken und gleichzeitig gefährliche Daten zu erkennen, den Zugriff auf sensible Daten zu widerrufen und mit Dateneigentümern zusammenzuarbeiten, um eine bessere Entscheidungsfindung und Einhaltung von Compliance-Standards zu erreichen. Identifizieren Sie Risiken, ermitteln Sie „Dark Data“ und zeichnen Sie Benutzeraktivitäten auf, um Aktivitätsmuster aufzudecken und Anomalien zu erkennen und zu identifizieren.

Cyberkriminelle fernhalten

Cyberkriminelle wissen, dass die Schwachstellen in Ihrem Netzwerk die Menschen sind.

Tatsächlich gehen die meisten Cyberattacken und Datenverletzungen auf menschliche Handlungen und Unterlassungen oder auf mangelnde Aufmerksamkeit zurück. Genau deshalb ist Phishing so wirksam!

Wie verhindern Sie einen Angriff? Vorkehrungen wie Identitäts- und Zugriffsverwaltung und Verschlüsselung sind wichtige Schutzmaßnahmen. Zur Verringerung der Wahrscheinlichkeit eines erfolgreichen Angriffs können Sie eine mehrstufige Authentifizierung und eine rollenbasierte Zugriffskontrolle einrichten. Das Verschlüsseln von Daten im Ruhezustand und während der Übertragung verringert die Nutzbarkeit Ihrer Daten und trägt zum Schutz gegen Datenexfiltration (nicht autorisierte Datentransfers) bei. Dinge wie Smartcard-Authentifizierung, Single-Sign-On und privilegierte Zugriffsverwaltung tragen dazu bei, das „Least Privilege"-Prinzip (PoLP) von Zero Trust zu stärken.

Mehrschichtige Präventions- und Schutzstrategien verwenden verschiedene Lösungen, die auf mehreren Ebenen implementiert sind. Sie können (und sollten) zur zusätzlichen Authentifizierung digitale Zertifikate für Geräte ausstellen. Verwenden Sie als eine weitere Schutzmaßnahme eine doppelte Autorisierung für den Zugriff auf Backups.

Die Verwaltung des sicheren Zugriffs und der Schutz Ihrer Daten vor Fehlkonfigurationen ist extrem wichtig. Die Identifikation und das Verständnis von Ressourcen, Aktionen und Identitäten in Ihrer Umgebung sind entscheidend, um Benutzerrechte zu verwalten und entsprechende Berechtigungen durchzusetzen – ob lokal oder in der Cloud. Das Verfolgen und Überwachen von Angriffsversuchen und von Änderungen im Lauf der Zeit hilft Ihnen, Ihre Sicherheitslage zu stärken und zeitnah Verbesserungen vorzunehmen.

Grundlegende Fragen:

- Was unternehmen wir derzeit, um Phishing und Malware zu unterbinden?
- Gibt es Möglichkeiten, wie wir unsere aktuellen Schutzmaßnahmen verbessern können?

Veritas-Lösungen

Die Veritas Datensicherheitslösungen sind anbieterunabhängig und bauen auf den Grundlagen von Zero Trust auf. Sie helfen, Ihr Netzwerk zu sichern, Daten während der Übertragung und im Ruhezustand mit AES-256-Bit-Verschlüsselung zu schützen, die FIPS 140-2-Zertifizierung zu erfüllen, den Benutzerzugriff zu beschränken und rollenbasierte Zugriffskontrolle und Multi-Faktor-Authentifizierung zu ermöglichen.

Veritas Data Insight bietet Einblick in Produktionsdaten nahezu in Echtzeit, um Ransomware anhand von anomalem Benutzerverhalten und bekannten Ransomware-Erweiterungen zu identifizieren.
Es kann auch stark exponierte Daten erkennen und dann Angriffsflächen entsprechend eingrenzen und verkleinern.

Veritas Analytics Solutions bietet ein einziges, einheitliches Dashboard mit geschäftsrelevanten Insights und Informationen, um Ransomware, ungeschützte Systeme und Backup-Anomalien zu identifizieren. Anhand dieser Daten können Sie den Speicherplatz optimieren, Kosten senken und den Überblick über Compliance- und gesetzliche Anforderungen behalten.

Die Veritas Alta™ -Klassifizierung beseitigt Hürden, die Sie daran hindern, Datensicherheit und Compliance zu erreichen. Sammeln Sie Metadatenattribute und Forensik zum Benutzerverhalten, um umsetzbare Informationen zu erhalten. Identifizieren Sie Dateneigentum, Datennutzung und Zugriffskontrollen und reduzieren Sie Datenschutz- und Sicherheitsrisiken.

Kritische, anfällige Daten identifizieren

Ihre Daten sind nicht statisch, Ihre Strategie und Lösungen sollten es auch nicht sein.

Implementieren Sie nur Produkte und Services, die skalierbar und anpassungsfähig sind. Flexibilität ist entscheidend, um unter Druck hohe Leistung mit mehreren Integrationen über mehrere Clouds hinweg zu erbringen.

Es wäre sinnlos, davon auszugehen, dass ein Unternehmen alle seine Lösungen von einem einzigen Anbieter auf einer einzigen Rechnung kauft. Business Development funktioniert so nicht: Es ist chaotisch und beinhaltet Kombinationen aus schon lange in Gebrauch befindlicher, teilweise veralteter Software und Technologie mit neueren, ausgefeilteren Lösungen.

Priorisieren Sie die Daten und finden Sie heraus, welches Maß an Compliance und Vorschriften Sie erfüllen müssen. Entscheiden Sie, wie Sie Backups verwalten und mit der Skalierung und Größe der Backups umgehen, die letztlich die Wiederherstellungszeit beeinflussen. Verstehen Sie, wie sich Ihre Bandbreitenkapazität auf Ihre Backups und Wiederherstellung auswirkt: So können Sie entscheiden, wie Sie kritische Workflows am effizientesten sichern und wiederherstellen.

Grundlegende Fragen:

- Welche Daten sind die wichtigsten, damit wir weiter produktiv bleiben können?
- Wie priorisieren wir unsere Daten-Backups?

Veritas-Lösungen

Die Veritas-Datensicherheitslösungen sind anbieterunabhängig und bieten einen soliden Aufbewahrungs- und Schutz-Workflow, der kostengünstig und einfach bereitzustellen und zu verwalten ist. Vereinfachen und organisieren Sie Multi-Cloud- und Hybrid-Cloud-Umgebungen auf einer einzigen Plattform.

Veritas Alta™ Shared Storage wurde entwickelt, um Ihre geschäftskritischen Anwendungen zu unterstützen und gemeinsam genutzten Speicher der Enterprise-Klasse mit überragender Leistung und Ausfallsicherheit bereitzustellen und gleichzeitig die Kosten niedrig zu halten. Es ermöglicht Anwendungs- und Infrastrukturadministratoren, empfindliche Daten zu schützen. Und es bietet Verschlüsselung; Write-Once/Read-Any (WORM); konsistente Snapshots; und Datenbankbeschleunigung.

Mit Veritas Alta™ SaaS Protection können Sie nach dem Ausscheiden eines Mitarbeiters weiterhin Zugriff auf die in Microsoft 365-Konten gespeicherten Daten behalten, ohne die zusätzliche Lizenz aufrechterhalten und bezahlen zu müssen. Stellen Sie Ordner, Postfächer oder Sites mit granularer, mehrstufiger Wiederherstellung an einem bevorzugten Speicherort wieder her, egal ob in der Cloud oder lokal. Maximieren Sie Leistung und Flexibilität, indem Sie den Backup-Speicher auf Petabytes und Milliarden von Objekten skalieren. Führen Sie mit größerer Regelmäßigkeit inkrementelle Backups durch, um RPO- und RTO-Vorgaben zu minimieren und gleichzeitig eine kontinuierliche Datensicherung auch standortübergreifend zu implementieren.

Verfügbare, effiziente Daten und Backups

Sie haben Backups von Ihren Daten erstellt. Warum ist es dann im Katastrophenfall so schwierig, sie wiederherzustellen?

Das Migrieren großer Datenvolumen (z. B. das Verschieben auf einen sekundären Speicher) nimmt viel Zeit und Rechenressourcen in Anspruch. Und Sie tun das ja nicht nur ein Mal, sondern bei Befolgung der 3-2-1-Backup-Regel drei Mal und auf zwei verschiedenen Speichertypen, von denen sich mindestens einer aus Gründen zusätzlicher Sicherheit an einem entfernten Standort befindet.

Bei der Migration eines kompletten Backups kann vieles schiefgehen, weshalb Hochverfügbarkeit und Failover extrem wichtig sind. Es ist, als würde man Wasser aus einem Krug in ein Glas gießen: Wenn dieses am Überlaufen ist, kann ein zweites Glas den Überschuss auffangen. Der Lastenausgleich entscheidet, welches System eine Anfrage übernehmen kann. Er verteilt also den Workload je nach Auslastung. Sie können mehrere Server zu einem Cluster zusammenfassen, um eine hohe Verfügbarkeit und Failover (Ausfallsicherheit) zu gewährleisten: Wenn einer der Server ausfällt, übernimmt ein anderer an seiner Stelle – ganz ohne Unterbrechung.

Grundlegende Fragen:

- Wo gibt es Möglichkeiten, unsere Backup-Effizienz zu verbessern?
- Wie können wir sicher sein, dass unsere Backups sauber, frei von Malware und unbeschädigt sind?

Veritas-Lösungen

Die Veritas-Datensicherheitslösungen decken die 3-2-1+1-Backup-Strategie problemlos ab und ergänzen diese durch eine zusätzliche Sicherheitsebene mit einem integrierten Intrusion-Prevention-System und einer isolierten Wiederherstellungsumgebung mit Air Gap. So haben Sie einen unlöschbaren Speicher, zusammen mit einem eingebauten, isolierten und unveränderlichen Datentresor (vault).

Veritas InfoScale trägt dazu bei, die Angriffsfläche für Produktionsdaten zu reduzieren und isoliert Produktionsdaten mit Snapshots und Datenspiegelung vom E/A. Es optimiert auch die Wiederherstellung für niedrige RTO- und RPO-Zielsetzungen. Mithilfe automatisierter Skripts können Sie Malware-Scans auf dem isolierten Datenträger ausführen, um sicherzustellen, dass er frei von Malware ist.

Veritas NetBackup Flex und Flex Scale bilden eine zusätzliche Sicherheitsebene, indem sie mehrere Fehlerquellen in der Hardware eliminieren. Sie nutzen Cluster-Komponenten, um kontinuierliche Verfügbarkeit zu gewährleisten.

Veritas Analytics-Lösungen erstellen anhand erfolgreicher Backups eine Vergleichsbasis für zukünftige Backups, um das Erkennen von Anomalien zu erleichtern. Sie können Backups auch nach Anwendung klassifizieren, um die Wiederherstellbarkeit aller Ihrer Apps über ein einziges Dashboard anzuzeigen.

Daten mit Air Gap und unveränderlichem Datenspeicher schützen

Wie schützen Sie Backup-Daten gegen bösartige Verschlüsselung?

Selbst wenn Ihr Unternehmen gewissenhaft Datensicherungen durchführt, besteht immer noch das Risiko menschlicher Fehler und Geräteausfälle. Das Risiko einer versehentlichen Löschung oder Änderung ist hoch.

Backups müssen gegen Veränderungen immun sein. Durch einen unveränderlichen Speicher lassen sich die unangenehmen Folgen von Datenkompromittierung und -angriffen vermeiden.

Unveränderliche Backups bieten das höchste Maß an Datenschutz für Ihr Unternehmen. Datenpermanenz ist ein wesentlicher Bestandteil der unveränderlichen Speicherung und gewährleistet ein absichtliches oder versehentliches Ändern von Daten. Dies sorgt für einen effizienteren und effektiveren Prozess innerhalb Ihrer Cybersicherheits- und Disaster-Recovery-Strategie und kann Ihnen dabei helfen, Ausfallzeiten und finanzielle Verluste zu vermeiden.

Die zusätzliche Ebene einer Air-Gap-Lösung stellt sicher, dass Ihre unveränderlichen Backup-Daten isoliert und unbeschädigt bleiben, sodass Sie sich auf eine saubere Wiederherstellung der Daten verlassen können.

Grundlegende Fragen:

- Wie schützen wir derzeit Backups vor Beschädigung?
- Gibt es Compliance-Standards, die einen Air Gap und eine Isolierung unserer Daten erfordern?

Veritas-Lösungen

Veritas orientiert sich an den NIST-Grundsätzen und bietet beispiellose Unveränderlichkeit, Sichtbarkeit, schnelle Wiederherstellung und Unlöschbarkeit.
Es unterstützt mehrere Methoden für Onsite- und Offsite-Lösungen, einschließlich bandbasierter Backups, cloudbasierter gesperrter Objektspeicherung und effizienter Datenspeicherung in AWS S3 Object Lock.

Die Veritas Datensicherheitslösungen blockieren proaktiv unerwünschte Verhaltensweisen beim Ressourcenzugriff, bevor das Betriebssystem darauf reagieren kann.

Mit Veritas Flex können Sie eine isolierte Wiederherstellungsumgebung (IRE) mit einem unveränderlichen Datentresor implementieren und eine sichere Kopie wichtiger Backup-Daten aus einer isolierten, unveränderlichen Umgebung bereitstellen.
Die IRE-Architektur schützt Ihre wichtigen Backups und bietet einen sicheren Bereich für die Orchestrierung einer sauberen Wiederherstellung oder zum Testen Ihres ausfallsicheren Wiederherstellungsplans.
Der infrastrukturunabhängige Virtual Air Gap von Veritas bietet eine zusätzliche Schutz- und Isolationsebene, um Angriffe abzuwehren.

Disaster Recovery-Verfahren festlegen

Die ideale Wiederherstellungslösung unterstützt jeden Workload.

Legen Sie einen Prozess fest, der eine einfache Integration beinhaltet, Ihre gewünschten Zielstellungen für RPO und RTO erfüllt, alle Speichermedien unterstützt und ein konsolidiertes Dashboard für alles bietet, was geschützt ist. Berücksichtigen Sie bei der Definition Ihres Prozesses unter anderem die folgenden Faktoren:

- Orchestrierte Wiederherstellung (Entscheidung zur Reihenfolge der Wiederherstellung)
- Intelligente Deduplizierung
- Snapshot-Integration
- Storage Tiering
- Automatisierte Replikation von Bildern, Katalogen und Snapshots auf lokale und Cloud-Speicher
- Containerunterstützung
- Data Insight und Analysen
- Sicherheit und Compliance sowohl für On-Premises als auch in der Cloud
- Verschlüsselung von Daten und Backup-Systemen

Nutzen Sie die Leistungsfähigkeit von Zero Trust, mehrschichtiger Datensicherheit und intelligenter Automatisierung, um sicherzustellen, dass der Geschäftsbetrieb robust und ausfallsicher ist. Profitieren Sie von Multi-Cloud-Intelligenz und verbessern Sie die Cyber-Abwehr, während Sie gleichzeitig Ihre Kosten reduzieren und integrierte Lösungen nutzen. Minimieren Sie Ihre Kosten und halten Sie sich an die sich ändernden Vorschriften, indem Sie Backups und Wiederherstellung für Cloud-basierte Workloads konsolidieren, die Workload-Migration automatisieren und eine problemlose Disaster Recovery mit Ein-Klick-Wiederherstellung, benutzerdefinierten Skripten und Proben implementieren.

Grundlegende Fragen:

- Wie lang brauche ich für eine Wiederherstellung?
- Was sind die Prioritäten bei der Wiederherstellung?

Veritas-Lösungen

Sie können zwischen Bare-Metal-Wiederherstellung und granularer Dateiwiederherstellung wählen, wenn nur ein Teil Ihrer Dateien kompromittiert wurde. Wir bieten auch ein sofortiges Rollback für VMs an, um Hunderte von VMs in wenigen Minuten wiederherzustellen und gleichzeitig ein Rollback durchzuführen.

Dank der verbesserten Datenausfallsicherheit und der Veritas Resiliency Platform können Sie unterschiedliche Wiederherstellungsprioritäten anwendungsübergreifend zuweisen und mehrschichtige Anwendungen in einer Reihenfolge wiederherstellen, die der Geschäftskritikalität entspricht. Kontinuierliche Datenschutzkontrollpunkte ermöglichen eine Wiederherstellung mit niedrigem RPO.

Veritas NetBackup Flex und Flex Scale verfügen über ein „gehärtetes" Betriebssystem, eine Zero-Trust-Architektur sowie einen unveränderlichen und unlöschbaren Speicher. Das IRE und der unveränderliche Datentresor bieten eine isolierte Lösung mit Air Gap, die von außen nicht erkennbar ist. Malware- und Anomalie-Scans geben Ihnen die Gewissheit, dass Ihre Backup-Daten sauber sind. Das heißt, Sie können unabhängig von der Umgebung, vor Ort oder in der Cloud, eine sofortige Wiederherstellung vornehmen.

Ausfallsicherheit testen

Hier geht es nicht um die Wiederherstellung, sondern um das Verhindern von Ausfallzeit.

Cyberkriminelle gehen davon aus, dass Ihr Unternehmen, genau wie die meisten, nicht für die Wiederherstellung optimiert ist. Sie sind auf maximalen Schaden und Ausfallzeiten aus, um Sie zu einer Lösegeldzahlung zu zwingen. Wenn Sie für eine Wiederherstellung gerüstet sind, dann sind Sie bereits einen großen Schritt voraus. Um eine schnelle Wiederherstellung zu erreichen, müssen Sie über einen Cybersicherheits-Reaktionsplan für Ihre gesamte Umgebung verfügen, der frühzeitige und regelmäßige Tests umfasst. Regelmäßiges Üben und Trainieren Ihres Wiederherstellungsverfahrens trägt dazu bei, Ausfallzeiten und Störungen zu begrenzen und die Auswirkungen eines Angriffs zu verringern.

In dem Maße, wie die Nachfrage nach Hybrid- und Multi-Cloud-Systemen steigt, müssen Sie in der Lage sein, mehrere Frameworks zu verwalten sowie mehrere Clouds und Speichersysteme zu koordinieren. Die Teams sind verantwortlich dafür, mehrere Server und Anwendungen zu verwalten und zu skalieren.

Nutzen Sie die Automatisierung, um die Komplexität Ihrer Umgebungen zu verwalten, potenzielle Bedrohungen zu identifizieren und Tests proaktiv zu verwalten, um eine kontinuierliche Bereitschaft sicherzustellen und Ausfallzeiten zu minimieren.

Grundlegende Fragen:

- Wie reduziere ich Ausfallzeiten?
- Wie beschleunige ich die Behebung?

Veritas-Lösungen

Veritas NetBackup Flex und Flex Scale maximieren das Potenzial der Datensicherung mit einer leicht erweiterbaren Architektur. Mit mehreren Ebenen der Unveränderlichkeit, der automatisierten Bereitstellung und des Lastenausgleichs können Sie eine komplette, schlüsselfertige Datenschutzlösung bereitstellen.

Veritas InfoScale und Veritas Alta™ Application Resiliency prüfen nicht nur, ob Ihr Setup funktioniert, sondern auch, ob es gut genug funktioniert. Es handelt sich um eine umfassende Infrastrukturlösung, die darauf ausgelegt ist, die Verfügbarkeit und Disaster Recovery durch enge Integration mit kritischen Geschäftsanwendungen zu maximieren, um maximale Betriebszeit und Failover zu gewährleisten. Als allumfassende Plattform bietet es die Flexibilität, die Schutzniveaus je nach Branchenbedarf anzupassen, mit Funktionen wie:

- Datenintegritäts-Compliance
- Automatisierte Runbooks für mehrschichtige Anwendungen zur Reduzierung des manuellen Aufwands
- Mobilität, die es ermöglicht, Workloads mühelos zwischen Plattformen zu verschieben
- Nahtlose Integration mit traditionellen Systemen und Umgebungen

Backups und Wiederherstellung optimieren

Vereinfachen der Verwaltung des Datenschutzes im gesamten Unternehmen.

Datenorchestrierung ist die Antwort, um Engpässe zu identifizieren und die Prozesse zu identifizieren, die am meisten Zeit verschlingen. Orchestrierung kann durch die Automatisierung von Prozessen wie Serverbereitstellung, Datenbankverwaltung und Anwendungen Zeit sparen. Verwenden Sie sie für Aufgaben wie das Aufspüren von Schwachstellen und die Suche nach Protokollen oder auch als Hilfe beim Vernetzen von Sicherheitstools und beim Integrieren von Systemen, um so die Teams zu entlasten.

Die Wahl der richtigen Lösung kann die Datenverwaltung erleichtern, bringt jedoch gewisse Herausforderungen mit sich.

Der Zugriff auf die richtigen Analysen bietet Einblick in die wesentlichen Elemente Ihrer Umgebung. Wenn Sie tiefer schürfen, können Sie erkennen, was nicht ausgelastet, falsch konfiguriert oder nicht indiziert ist. Dies hilft der IT, Probleme anzugehen und Ressourcen zu identifizieren, die für andere Zwecke eingesetzt werden können, um Kosteneinsparungen zu erzielen.

Entdecken Sie umsetzbare Erkenntnisse, um Ihre Auslastung, Leistung und Ausfallsicherheit zu verbessern, während Sie Ausfälle vorhersagen und proaktive Empfehlungen zur Minderung von Risiken für Service Level Agreements (SLAs) identifizieren.

Intelligente Automatisierung kann dabei helfen, die Ineffizienzen manueller Prozesse auszuräumen und unendlich viele Möglichkeiten zu erschließen.

Implementieren Sie agile, zuverlässige Backups und Wiederherstellung für eine vollständige Datensicherung und -optimierung.

Optimieren Sie Ressourcen, senken Sie Kosten und überwachen Sie Ihr gesamtes Netzwerk vom Edge über den Core bis zur Cloud über eine umfassende Konsolenansicht.

Veritas-Lösungen

Mit Veritas Data Insight können Sie Aktivitäten analysieren und eine detaillierte Analyse der Nutzung und kollaborativen Aktivitäten bereitstellen. Es kann dabei helfen, Benutzer zu klassifizieren und Aktivitätsmuster besser zu verstehen. Identifizieren Sie Daten, die dupliziert, veraltet oder verwaist sind; und nutzen Sie Risikobewertungen, um potenzielle Bedrohungen zu bewerten und Hochrisikodaten zu priorisieren. Erstellen Sie detaillierte Prüfprotokolle und nutzen Sie integrierte Dateianalyse, Datenverlustprävention und Archivierung mit den Compliance-Lösungen von Veritas.

Veritas Analytics-Lösungen helfen dabei, gefährdete Anwendungen und Dienste zeitnah zu identifizieren. Schnellere Wiederherstellung durch die Möglichkeit, Backups in allen Umgebungen zu überwachen und zu optimieren und betroffene Hosts effizient nach Standort, Umgebung oder Anwendung zu lokalisieren.

Grundlegende Fragen:

- Sind unsere Daten für eine schnelle Wiederherstellung optimiert?
- Verstehen wir unsere SLAs?

DIE EIGENEN DATEN KENNEN | DATEN GEGEN BEDROHUNGEN SCHÜTZEN | KRITISCHE, ANFÄLLIGE DATEN IDENTIFIZIEREN | VERFÜGBARE, EFFIZIENTE DATEN UND BACKUPS | UNVERÄNDERLICHE, LÜCKENLOSE BACKUPS | DISASTER RECOVERY-VERFAHREN FESTLEGEN | DISASTER RECOVERY-STRATEGIE TESTEN | **BACKUPS UND WIEDERHERSTELLUNG OPTIMIEREN**

Schließen Sie Lücken in der Cybersicherheits-Strategie. Weitere Informationen >

Über Veritas

Veritas Technologies ist ein weltweit führender Anbieter im Bereich Multicloud-Datenmanagement. Über 80.000 Kunden – darunter 95 Prozent der Fortune 100 – vertrauen darauf, mit Lösungen von Veritas den Schutz, die Wiederherstellbarkeit und Compliance ihrer Daten zu gewährleisten. Veritas steht für skalierte, zuverlässige Produkte, welche die Widerstandsfähigkeit bieten, die seine Kunden im Fall von Cyberangriffen wie Ransomware benötigen. Kein anderer Anbieter erreicht Veritas' Leistungsfähigkeit mit Unterstützung für mehr als 800 Datenquellen, über 100 Betriebssystemen, über 1.400 Speicherzielen und über 60 Clouds im Rahmen eines einzigen, einheitlichen Ansatzes. Mithilfe der Cloud Scale Technology setzt Veritas heute seine Strategie für autonomes Datenmanagement um, die den betrieblichen Aufwand reduziert und gleichzeitig einen größeren Mehrwert bietet. Weitere Informationen finden Sie unter veritas.com/de/de und 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

V1811 04/23