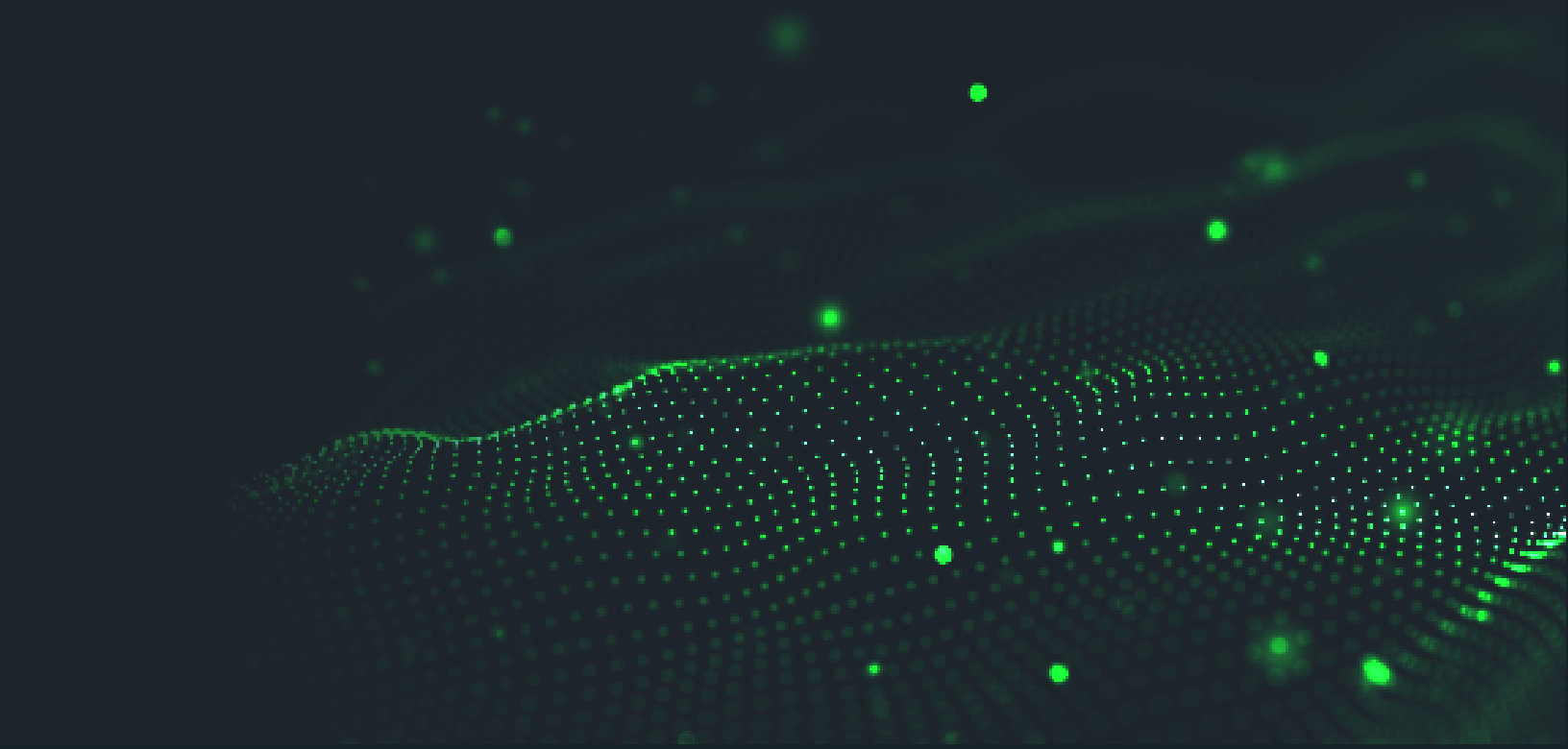
Die Argumente für eine moderne Plattform für Datensicherheit und -management

COHESITY



COHESITY

Inhaltsverzeichnis

COHESITY

Zusammenfassung

Das wichtigste Kapital eines Unternehmens sind heutzutage seine Daten – und das wissen auch die Führungskräfte. Sie wissen auch, dass Cyberangriffe, menschliches Versagen oder Naturkatastrophen jederzeit auftreten und erhebliche Auswirkungen haben können. Sie haben Datensicherungs- und wiederherstellungslösungen implementiert, um die Auswirkungen dieser Risiken zu mindern.

Die in den letzten Jahrzehnten eingesetzten Prozesse und Produkte sind jedoch nicht für die aktuellen und zukünftigen Anforderungen der Unternehmen ausgelegt. Viele dieser Lösungen wurden für eine bestimmte Aufgabe entwickelt. Das führt zu einer fragmentierten Behandlung der Daten, sodass sich nicht nur das Risiko erhöht, sondern gleichzeitig auch die Kosten und die Komplexität zunehmen. Außerdem erfordern moderne Bedrohungen einen integrierten Ansatz, bei dem Datensicherheit und -management nahtlos miteinander verbunden sind. Ältere Tools behandeln diese beiden Bereiche als getrennte Welten.

Aufgrund dieser Einschränkungen sind viele Unternehmen dabei, ihre bestehenden Datensicherheits- und -managementstrategien neu zu bewerten. Nach sorgfältiger Recherche und Abwägung von ROI, TCO und dem Risikoprofil ihres derzeitigen Datenbestands wechseln sie zu modernen Plattformen, die mehr Schutz, schnellere Wiederherstellungszeiten sowie bessere Skalierbarkeit und Erweiterbarkeit bieten.

Wenn Sie also beschließen, dass es an der Zeit ist, sich eine moderne Lösung näher anzusehen, stellt sich als Erstes folgende Frage: „Wo fange ich am besten an?“ Darauf werden wir uns hier konzentrieren.

Versuchen Sie zunächst, das Geschäftsszenario für ein neueres Tool zu verstehen. Oder sind Sie vielleicht dafür verantwortlich, selbst ein Szenario für ein neues Tool zu erstellen? Wir werden untersuchen, warum Unternehmen bei ihren alten Anbietern bleiben, und erörtern, welche Auswirkungen das Festhalten an aktuellen Lösungen hat und welchen Mehrwert eine neuere Lösung bringen kann.

„Unsere langjährige Lösung war nicht mehr auf der Höhe der Zeit. Das Beheben periodisch auftretender Störungen dauerte einfach zu lange. Wenn eine virtuelle Maschine ausfiel, musste unser Entwicklungsteam sie aus den gesicherten Daten wiederherstellen, was Tage dauerte.“

Luis Suarez, Chief Information Officer, H.I.G. Capital

COHESITY

Vorherrschende Ansichten bezüglich moderner Datensicherheits- und -managementangebote

Wie jede Veränderung kann auch die Umstellung auf eine moderne Datensicherheits- und -managementlösung schwierig sein, vor allem wenn Sie oder Ihr Unternehmen Bedenken wegen des Übergangs haben. Überlegen Sie zunächst, welche Kriterien für Sie wichtig sind (wie z. B. Compliance oder Kosten), und wägen Sie Ihre Optionen entsprechend ab. Sie könnten feststellen, dass Ihr Status quo nicht die beste Option ist. Lesen Sie weiter, um zu verstehen, warum so viele Unternehmen einen neuen Ansatz in Betracht ziehen.

$ Kosten

Bei der Umstellung auf eine neue Lösung können Vorlaufkosten für neue Hardware, Softwarelizenzen und Personalschulung anfallen. Diese Investitionen könnten überwältigend erscheinen, besonders wenn Sie mit Ihrer bestehenden Lösung zufrieden sind.

Bedenken Sie dabei aber Folgendes:
Das Festhalten an einer veralteten Lösung könnte Sie auf lange Sicht sogar mehr kosten. Warum? Die Lizenzierung und Wartung können kostspielig sein. Eine von Deloitte durchgeführte Umfrage ergab, dass IT-Abteilungen im Durchschnitt über 55 % ihres Technologiebudgets für die Aufrechterhaltung des Geschäftsbetriebs und nur 19 % für die Entwicklung innovativer Lösungen aufwenden. Da das Datenvolumen wächst, kann es auch teuer werden, Speicherplatz hinzuzufügen.

Sicherheit

Was ist sicherer: die moderne Option oder Ihre veralteten Lösungen? Viele Unternehmen sind der Meinung, dass ihnen herkömmliche Lösungen mehr Kontrolle über ihre vertraulichen Daten ermöglichen und sie weniger anfällig für Cyberangriffe sind.

Bedenken Sie dabei aber Folgendes:
Veraltete Lösungen haben ihre eigenen Sicherheitsschwachstellen. Sie sind einem erhöhten Risiko von Datenverlusten durch physische Manipulationen, Naturkatastrophen oder veraltete Schutzfunktionen ausgesetzt, was die Kundenbeziehungen beeinträchtigen und hohe Kosten verursachen kann. IBM berichtete, dass sich die durchschnittlichen weltweiten Kosten einer Datenschutzverletzung im Jahr 2023 auf 4,45 Millionen US-Dollar belaufen, was einem Anstieg von 15 % in den letzten drei Jahren entspricht.

COHESITY

Datenmigration

Kurz gesagt: ein schmerzhaftes Unterfangen. Die Migration von Daten kann zeitaufwändig und kostspielig sein und bei einem Wechsel zu einer anderen Lösung eine ganze Reihe neuer Herausforderungen mit sich bringen.

Bedenken Sie dabei aber Folgendes: Wenn Sie bei Ihrer derzeitigen Lösung bleiben, könnten Sie sich den Wert einer neuen Lösung entgehen lassen. Datenmigration kann zu größerer Effizienz, höherer Datensicherheit und besserer Datenqualität führen, und die meisten modernen Lösungen bieten Funktionen, die den Migrationsprozess erleichtern.

Compliance

In stark regulierten Branchen kann es Bedenken geben, ob eine neue Datensicherheitsplattform die regulatorischen Anforderungen erfüllen wird. Unternehmen ziehen es vielleicht vor, bei bestehenden Lösungen zu bleiben, die sich in Bezug auf die Compliance-Einhaltung bewährt haben, anstatt die vermeintlichen Risiken beim Einführen einer neuen Plattform einzugehen.

Bedenken Sie dabei aber Folgendes: Moderne Lösungen sind eigentlich ausgesprochen sicher und bieten integrierte Sicherheitsfunktionen wie Verschlüsselung, Zugriffsverwaltung und einen erweiterten Bedrohungsschutz, was die Einhaltung gesetzlicher Vorschriften wie der DSGVO und dem HIPAA erleichtern. Bei veralteten Lösungen kann es schwierig sein, den Zugriff auf die darin enthaltenen Daten zu beschränken. Sie wurden außerdem auch für die heutige Bedrohungslandschaft entwickelt, sodass viele Hersteller zusätzliche Funktionen und Fähigkeiten zusammengestellt haben, um auf dem neuesten Stand zu bleiben, was zu erhöhter Komplexität führt und das Risiko erhöht.

Einführung

Veränderungen können schwierig sein, insbesondere in großen Unternehmen mit eingefahrenen Kulturen und Arbeitsweisen. Es ist möglich, dass es Widerstände gegen die Einführung neuer Technologien gibt, weil man mit dem Status quo zufrieden ist oder es schwierig sein könnte, etwas Neues zu lernen.

Bedenken Sie dabei aber Folgendes: Die Benutzeroberflächen der meisten neueren Lösungen basieren auf bewährten Methoden und sind so konzipiert, dass sie sowohl benutzerfreundlich als auch einfach einzuführen sind. Viele von ihnen sind als SaaS-Lösungen verfügbar, d. h. Ihr Unternehmen muss sich nicht um die Verwaltung der Anwendung oder die Durchführung von Upgrades und Sicherheitspatches kümmern.

Zufrieden mit dem Status quo

Manche Unternehmen mögen sich mit dem begnügen, was für sie funktioniert. Einige Entscheidungsträger verstehen die Möglichkeiten und Vorteile moderner Datensicherheitslösungen nicht vollständig, sodass sie den Wert neuerer Angebote nicht erkennen.

Bedenken Sie dabei aber Folgendes: Was werden Sie brauchen, um die nächsten 10 Jahre zu überstehen? Wird Ihnen Ihre aktuelle Lösung noch ein weiteres Jahrzehnt dienen oder ziehen Sie das Neueste und Beste vor? Stellen Sie sich Fragen wie: Bietet die Lösung KI-Funktionen zur Entscheidungsfindung? Ist sie cloudnativ?

COHESITY

Kosten der Angst vor dem Wechsel

Wir alle wissen, dass es zu Überschwemmungen kommen kann und irgendwann der Strom ausfallen wird. Wahrscheinlich sind Sie auf solche Situationen vorbereitet. Doch was ist mit Ereignissen, die noch unvorhersehbarer sind, wie beispielsweise ein Cyberangriff? Da es nicht darum geht, ob es passiert, sondern wann es passiert, ist es wichtig, auch hierfür eine Strategie zu haben. Selbst wenn Sie bislang mit Ihrer aktuellen Lösung zufrieden sind, sind veraltete Lösungen nicht für die Anforderungen der heutigen Welt entwickelt worden. Bevor Sie sich also entscheiden, bei Ihrem derzeitigen Anbieter zu bleiben, sollten Sie bedenken, welche Auswirkungen diese Entscheidung auf Ihr Unternehmen haben könnte.

Datensilos Herkömmliche Systeme verwalten viele Unternehmensdatensilos und schränken die Fähigkeit eines Unternehmens ein, wachsende Datenmengen zu verarbeiten und zu skalieren. Dies kann die Erfüllung sich neu entwickelnder Geschäftsanforderungen behindern, Leistungsprobleme verursachen und die Produktivität verringern. Darüber hinaus führen Silos zu Ineffizienzen und treiben so die Betriebskosten in die Höhe. In einem IDC-Bericht wurde beispielsweise festgestellt, dass Unternehmen durch die Einführung einer modernen Lösung über 720.000 US-Dollar an Personalzeit pro Jahr einsparen konnten, da 7,2 Vollzeitstellen für das Management ihrer IT-Infrastruktur wegfielen.

Größere Angriffsfläche Heutzutage speichern Unternehmen Daten in verschiedenen Umgebungen (z. B. Cloud, SaaS, On-Premises), was die Angriffsfläche vergrößert und Sicherheitsmaßnahmen erschwert. Jede Umgebung kann einen anderen Ansatz für die Datensicherung erfordern, und es kann zu Unstimmigkeiten im Sicherheitsniveau in diesen Umgebungen kommen.

Überholte Sicherheitsstrategie Da veraltete Lösungen nicht für das heutige Bedrohungsumfeld entwickelt wurden, sind sie anfälliger für bekannte Schwachstellen und Sicherheitslücken. Cyberkriminelle können diese ausnutzen, um unbefugten Zugriff auf Systeme zu erhalten, vertrauliche Daten zu stehlen oder den Geschäftsbetrieb zu stören. Aus diesem Grund zahlen Unternehmen immer noch Lösegeld. Laut Compliance Week soll Change Healthcare, eine Tochtergesellschaft von UnitedHealth, Anfang 2024 22 Millionen Dollar gezahlt haben, um ihre Daten nach einem Ransomware-Angriff zurückzubekommen.

Systemwartung Lizenz- und Wartungsgebühren können Unternehmen Tausende von Dollar pro Jahr kosten. Darüber hinaus können Upgrades Zeit von höherwertigen Arbeiten abziehen, die Innovation, Produktdifferenzierung und Sicherheitsinitiativen vorantreiben. Hinzu kommt, dass es mit dem Aufkommen neuerer Lösungen immer schwieriger und kostspieliger wird, die für die Bedienung eines älteren Systems erforderlichen Fachkräfte zu finden.

COHESITY

Mitarbeiterproduktivität Im Laufe der Jahre haben Unternehmen ihr technisches Angebot um neue Produkte erweitert, um spezifische Anforderungen zu erfüllen. Tatsächlich verfügt ein durchschnittliches Unternehmen über mehr als 130 verschiedene Cybersicherheitstools, die alle mit einer getrennten Sicht auf die Daten arbeiten, die sie schützen. Dies senkt die Produktivität, da Benutzer ständig zwischen den Systemen wechseln müssen. Darüber hinaus kommt es zu Personalproblemen, da es schwieriger ist, Mitarbeiter zu finden, die mit älteren, komplexen Lösungen vertraut sind.

Reaktionszeiten Eine von Cohesity in Auftrag gegebene Studie ergab, dass 79 % der Befragten zwischen Juni und Dezember 2023 Opfer von Ransomware-Angriffen wurden und nur 7 % ihre Geschäftsprozesse innerhalb von 1–3 Tagen wiederherstellen konnten. Der Grund dafür ist, dass ältere Lösungen neuere Anwendungen nicht unterstützen oder nicht die erforderlichen Funktionen für deren Schutz bieten. Erschwerend kommt hinzu, dass die meisten Unternehmen den Großteil ihres Cybersicherheitsbudgets für den Schutz und die Erkennung und nur einen Bruchteil für die Reaktion und Wiederherstellung ausgeben. Wie aus diesen Daten hervorgeht, wird es jedoch in jedem Fall zu Angriffen kommen, sodass Investitionen in beide Bereiche für das Erreichen von RTOs/RPOs unerlässlich sind.

[2] https://www.cohesity.com/press/cohesity-research-reveals-most-companies-pay-millions-in-ransoms-breaking-their-do-not-pay-policies/

COHESITY

Die Vorteile einer modernen Plattform für Datensicherheit und -management

Bislang haben wir die Probleme betrachtet, die mit älteren Technologien verbunden sind, und erörtert, was eine moderne Lösung nicht ist. Wir haben jedoch noch keine Alternative aufgezeigt, und wir sind auch noch nicht darauf eingegangen, worauf Sie beim Modernisieren Ihrer Datensicherung- und wiederherstellung achten sollten. Im Allgemeinen empfehlen wir, auf die folgenden Merkmale zu achten.

Benutzerfreundlichkeit

Eine moderne Plattform für Datensicherheit und -management sollte überall ein konsistentes und nahtloses Erlebnis bieten: in der gesamten Infrastruktur (On-Premises, in der Cloud, am Edge) und bei allen Workloads. Außerdem sollte sie auf dem API-First-Ansatz basieren und eine einfache Integration mit anderen IT-Systemen unterstützen. Auf diese Weise können Daten problemlos von anderen Systemen und Tools aufgenommen, verarbeitet und analysiert werden, anstatt ein kompliziertes Netz von Lösungen zu schaffen. Durch die Zentralisierung aller Daten an einem Ort können Unternehmen Silos beseitigen und IT-Mitarbeiter in die Lage versetzt werden, große Datenbestände effizienter zu verwalten. Ein führender Versicherungsanbieter sparte beispielsweise jährlich 2 Millionen US-Dollar an Backup-Kosten und ermöglichte es seinem kleinen Team, mehr Daten mit weniger Aufwand zu verwalten.

Skalierbarkeit

Moderne Datenplattformen müssen hochgradig skalierbar sein, um die großen Datenmengen zu bewältigen, die von modernen Anwendungen und Geräten erzeugt werden. Ferner müssen sie den wachsenden Datenmengen und Benutzerzahlen standhalten. Dies ermöglicht eine nahtlose Erweiterung der Kapazität und Leistung, wenn sich die Anforderungen des Unternehmens weiterentwickeln. Die Plattform sollte außerdem in der Lage sein, Daten aus einem breiten Spektrum von Quellen (VMs, Unternehmensdatenbanken, NAS, SaaS, Cloud-Datenquellen) zu verarbeiten, einschließlich strukturierter und unstrukturierter Daten.

Vorher und nachher: Die Geschichte von Hyatt

Für Hyatt, ein weltweit führendes Unternehmen im Gastgewerbe, war das Management mehrerer veralteter IT-Produkte weltweit nicht mehr tragbar, insbesondere da die Datenmenge an einigen Standorten um bis zu 20 % anstieg. Um die Effizienz zu steigern, wechselte das IT-Team zu einer modernen Lösung, die eine qualitativ hochwertige Datenreplikation und flexible Entwicklungs-/Testfunktionen zwischen den Rechenzentrumsstandorten gewährleistet.

Dadurch konnte Hyatt die Zeit für die Datenreplikation von Tagen auf Minuten reduzieren und den Kapazitätsbedarf um 40 % verringern.

Fallstudie lesen

COHESITY

Verlässliche Sicherheit

Eine moderne Plattform basiert auf Zero-Trust-Prinzipien, einschließlich rollenbasierter Zugriffskontrollen (RBAC), MFA, Unveränderlichkeit und Datenverschlüsselung im Ruhezustand und während der Übertragung. Dadurch wird gewährleistet, dass vertrauliche Daten gesichert und vor unbefugtem Zugriff und Cyberangriffen geschützt sind. Sie unterstützt außerdem die Identifizierung vertraulicher Daten, das Daten-Vaulting, die Erkennung von Angriffen sowie die Bündelung der Reaktionsfähigkeit auf Cybervorfälle. Schließlich sollte die von Ihnen gewählte Lösung idealerweise mit anderen etablierten und neuen Sicherheitstools integriert werden können, um die Sicherheitslage Ihres Unternehmens zu verbessern.

Schnelle Wiederherstellung

Im Falle eines Cyberangriffs oder einer ungeplanten Störung ermöglicht eine moderne Plattform die schnelle, vorhersehbare Wiederherstellung aufgabenkritischer Datenbanken. Unternehmen können dies mit inkrementellen Backups und Snapshots erreichen, die an einem separaten Ort gespeichert werden, wo sie nicht verändert werden können. Dies ist besonders wichtig für die Einhaltung der Compliance. Eine moderne Plattform ermöglicht außerdem eine sofortige Recovery und bietet granulare Wiederherstellungsoptionen, damit Unternehmen bestimmte Dateien, Datenbanken oder Anwendungen schnell wiederherstellen können, ohne dass ein Restore des gesamten Backups erforderlich wäre. Mithilfe dieser Funktionen haben Fortune-500-Unternehmen ihre Wiederherstellungszeiten auf ein Zehntel reduziert.

Datengesteuerte Lösungen

Jede moderne Datenmanagementplattform sollte eine Reihe von Datenanalytik- und Visualisierungstools unterstützen, wie z. B. SQL-basierte Analytik, maschinelles Lernen und die Verarbeitung natürlicher Sprache (NLP), damit Unternehmen Erkenntnisse und Wert aus ihren Daten schöpfen können. Sie sollte auch KI-Funktionen bieten, die nicht überall erhältlich sind, aber Unternehmen in die Lage versetzen, schneller Erkenntnisse zu gewinnen.

Vorher und nachher: Pearl River Community College

In den letzten Jahren sind Bildungseinrichtungen zu beliebten Zielen für Identitätsdiebstahl und Ransomware-Angriffe geworden. Zum Schutz der Daten der Studierenden und zur Aufrechterhaltung eines reibungslosen Betriebs im Katastrophenfall wechselte das Pearl River Community College zu einer modernen Datensicherheits- und -managementlösung, die Zugriffskontrollen, einschließlich MFA, unveränderliche Backups, Quorum und Cyber-Vaulting-Funktionen bietet.

„Ohne diese Funktionen wären unsere Versicherungsprämien viel höher, wenn wir überhaupt einen Vertrag bekommen würden," so Matt Logan, CIO.

Fallstudie lesen

COHESITY

Nächste Schritte

Die Umstellung auf eine moderne Datensicherheits- und -managementlösung mag entmutigend erscheinen, insbesondere wenn sich Ihre alte Lösung über Jahre hinweg als zuverlässig erwiesen hat. Angesichts der Zunahme und kontinuierlichen Änderungen der Angriffsarten ist der Status quo jedoch nicht mehr ausreichend. Aus diesem Grund bereiten sich führende Unternehmen auf die Zukunft vor, indem sie ihre Daten mit modernen Sicherheits- und Managementlösungen schützen.

Wir empfehlen folgende nächste Schritte:

1. **Bestimmen Sie, was Sie mit dem Wechsel zu einer neuen Lösung erreichen möchten.**
   - Legen Sie Ziele für RTOs und RPOs, Speicherung, Betriebskosten usw. fest.
2. **Skizzieren Sie die Anwendungsfälle, die Sie unterstützen möchten, und die wichtigsten Funktionen.**
3. **Bewerten Sie den ROI und die Gesamtbetriebskosten einer modernen Datenplattform für Ihre bestehende Lösung. Die wichtigsten Vergleichspunkte sollten sein:**
   - Effizienz der Datensicherung
   - Betriebliche Effizienz
   - Risiken und Compliance
4. **Entwickeln Sie einen Business Case. Um wichtige Beteiligte zu überzeugen, sollten Sie Folgendes beachten:**
   - Zeigen Sie, wie die neue Technologie mit den strategischen Zielen des Unternehmens in Einklang steht.
   - Definieren Sie klar die Probleme, die mit der modernen Lösung angegangen werden sollen.
   - Erklären Sie die neue Technologie und ihre Funktionsweise.
   - Beachten Sie die Kosten und Kriterien einer Cyberversicherung.
   - Quantifizieren Sie den Nutzen (ROI), wie beispielsweise die Kosteneinsparungen, Produktivitätssteigerungen und verbesserten Funktionen.
   - Skizzieren Sie die nächsten Schritte für die Bereitstellung der Lösung. Gehen Sie dabei auf potenzielle Risiken ein und zeigen Sie auf, wie Sie diese verringern werden.

Sobald Sie sich für eine Lösung entschieden haben und bereit sind, einen Anbieter auszuwählen, sollten Sie Ihre Daten, deren Speicherort und die Abhängigkeiten Ihres Teams bewerten. Sie müssen sich auch Gedanken über Data-Governance-Prozesse machen, um eine langfristige Pflege zu gewährleisten.

COHESITY

Über Cohesity

Cohesity ist ein Branchenführer für KI-gestützte Datensicherheits- und -managementlösungen. Unterstützt durch ein umfangreiches Ökosystem von Partnern vereinfacht Cohesity den Schutz, das Management und die Wertschöpfung Ihrer Daten – im Rechenzentrum, am Edge und in der Cloud. Cohesity unterstützt Unternehmen dabei, sich vor Cybersicherheitsbedrohungen mit umfassenden Data Security und Data Management-Funktionen zu schützen, einschließlich unveränderliche Backup-Snapshots, KI-basierte Bedrohungserkennung, Überwachung des Benutzerverhaltens sowie schnelle und skalierbare Wiederherstellung. Lösungen von Cohesity können als SaaS, selbst verwaltet oder über Cohesity-Partner bereitgestellt werden. Cohesity hat seinen Hauptsitz in San Jose, Kalifornien, und genießt das Vertrauen der weltweit größten Unternehmen.

COHESITY

www.cohesity.com

2000052-001-DE 7-2024