COHESITY

CLOUD-BACKUP:

Ein detaillierter Bewertungsleitfaden für **Backup as a Service** mit Checkliste

Steigern Sie die Flexibilität der Datennutzung, betriebliche Effizienz und Cyber-Resilienz

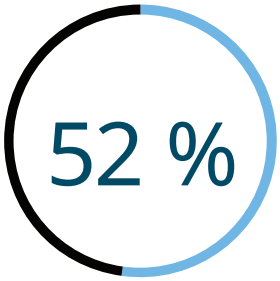
Inhaltsverzeichnis

Backup für das Cloud-Zeitalter

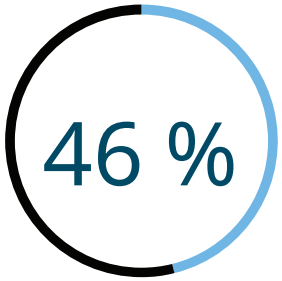
Die durch Cloud Computing angefeuerte IT-Modernisierung hat in den letzten Jahren die Innovation und das Wachstum erheblich beschleunigt. Doch nicht alle kritischen IT-Infrastrukturen wurden konsequent oder im gleichen Tempo auf die Cloud umgestellt. Dies führt zu Ineffizienzen und Cyber-Schwachstellen, die sich Unternehmen nicht leisten können.

Der oft übersehene Modernisierungsschritt hin zu einer Backup-Infrastruktur in der Cloud – über die Angebote von SaaS-Providern hinaus – kann Ihrem Unternehmen die gleiche Agilität bieten wie die Bereitstellung Ihrer modernen Apps in der Cloud. Backup as a Service (BaaS) ist eine grundlegende Geschäftskontinuitätslösung, die alte, vor der Cloud aufgebaute Backup-Silos bündelt. Gleichzeitig verbessert BaaS die Cloud-Erfahrung, den Betrieb und den Kostenaufwand. Mit BaaS können Sie nicht nur das Potenzial all Ihrer Daten für Geschäftseinblicke effektiver nutzen, sondern auch die Cyber-Resilienz Ihres Unternehmens sicherstellen.

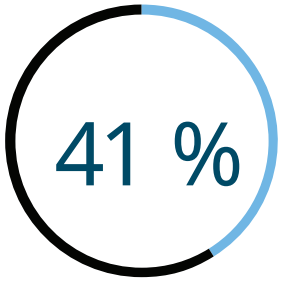
Die wichtigsten Vorteile von cloudbasierten Datensicherungsdiensten



Erhöhte Sicherheit



Verbesserte Wiederherstellbarkeit und Zuverlässigkeit von Backups



Geringere IT-Personalkosten

Quelle: Enterprise Strategy Group. „The Evolution of Data Protection Cloud Strategies“, 2021.

Ihr nächster Schritt auf dem Weg in die Cloud

Bei der Bewertung von BaaS-Angeboten sollten Sie die verfügbaren Funktionen kennen. Dazu gehören auch der Schutz Ihrer Daten und die Preisgestaltung für Ihr Unternehmen. Dieser Leitfaden enthält wichtige Bewertungskriterien und eine Checkliste, die Sie auf Ihrem Weg in die Cloud nutzen können.

Der Vergleich von Cloud-Backup-Lösungen beginnt mit der Frage, in welchem Umfang ein Angebot die folgenden wichtigen BaaS-Funktionen unterstützt:

1. Erweiterter Datenschutz und operative Handlungsfreiheit
2. Verstärkte Sicherheit und Ransomware-Bereitschaft
3. Mehr Flexibilität bei Verbrauch und Kosten sowie Nachhaltigkeit

Bewertung der aktuellen Herausforderungen

Bevor Sie ein Cloud-Backup-Angebot bewerten, sollten Sie zunächst klären, welche Unterschiede es zwischen einer Backup- und Recovery-Umgebung gibt, die von Ihrem Unternehmen lokal und selbst verwaltet oder von einem Backup-Anbieter gemanagt und in der Cloud gehostet wird. Tabelle 1 zeigt zehn häufige Probleme bei der Datensicherung und -wiederherstellung mit selbstverwalteten On-Premises-Lösungen.

Zehn häufige Probleme bei der Datensicherung und -wiederherstellung mit selbstverwalteten On-Premises-Lösungen

1. Silo-Infrastrukturen (z. B. separate Server, eigene Speicherziele usw.) sind kostspielig in der Anschaffung, was die Investitionsausgaben erhöht
2. Mangelnder Schutz von modernen, cloudnativen und SaaS-Anwendungen, was einen Wettbewerbsnachteil für das Unternehmen bedeutet
3. Komplexes Management mit mehreren fragmentierten Bedienoberflächen für verschiedene Datenquellen zur Konfiguration von Backup-Workflows, was die IT-Abteilung zusätzlich frustriert
4. Separate Cloud-Gateways, die für die Migration von Daten vor Ort und in verschiedene Public Clouds benötigt werden, was zu Komplexität führt
5. Forklift-Upgrades und disruptive Updates, die geplante Ausfallzeiten erfordern
6. Langsame Wiederherstellungen, die die RTOs verfehlen und/oder nur Restores zum letzten Sicherungszeitpunkt zulassen, was sich negativ auf die RPOs auswirkt
7. Variable und/oder feste Blockdeduplizierung mit Komprimierung, was die Kosten erhöht
8. Fehlende Funktionen zum Schutz vor Ransomware, was das Risiko für das Unternehmen erhöht
9. Nicht gewährleistete Wiederverwendung von Daten aufgrund von Fragmentierung, wodurch Einblicke verloren gehen
10. Langsame Einführung moderner Funktionen, was Innovationen blockiert

Tabelle 1: Bewertung von selbstverwalteten On-Premises-Datensicherungs- und -wiederherstellungsumgebungen

Das digitale Geschäft schreitet schnell voran. Durch Cloud-Backups können Sie nicht nur mithalten, sondern Ihren Weg in die Cloud und Ihre digitale Transformation beschleunigen.

1 Erweiterter Datenschutz und operative Handlungsfreiheit

Die geschäftlichen und behördlichen Anforderungen an die unterschiedlichen Informationsarten, die Ihr Unternehmen schützen muss, und deren Aufbewahrungsfristen ändern sich. Sie wünschen sich sicher eine umfassende Cloud-Backup-Lösung, die sich bei Bedarf schnell anpassen lässt. Wie können Sie sonst ohne eine einheitliche Methode zur Unterstützung von Aufbewahrungsrichtlinien und Service Level Agreements für alle Ihre cloudnativen, SaaS- und On-Premises-Anwendungen dafür sorgen, dass alle Ihre Daten geschützt sind und Ihr ohnehin schon überlastetes internes IT-Personal nicht noch weiter überfordert wird?

Ein Cloud-Backup kann für Ihr Unternehmen viel wertvoller sein als eine Versicherungspolice. Für den erweiterten Schutz von Datenquellen mit operativer Handlungsfreiheit sollten Sie ein BaaS mit den folgenden fünf wichtigen Betriebsfunktionen wählen:

Umfassende Unterstützung von Datenquellen

Backups sollten einfach sein. Trotzdem ist es heute schwierig, alle aufgabenkritischen Daten in Anwendungen über Ihre gesamte Umgebung hinweg zu sichern. Unterschiedliche Cloud-Plattformen, Services und APIs mit voneinander abweichenden Richtlinien, SLAs und Aufbewahrungsfristen sind wesentliche Hinderungsgründe. Dies führt zu Komplexität. Zur optimalen Vereinfachung ist eine zentrale BaaS-Lösung erforderlich, die ein breites Spektrum an Workloads in verschiedenen Umgebungen und Clouds unterstützt. Die Lösung muss Cloud-Workloads wie Amazon EC2 und RDS sowie SaaS-Anwendungen wie M365 mit einem zentralen, einheitlichen Service konsolidieren und schützen, der weit über die von Cloud-Anbietern bereitgestellten Schutzmechanismen hinausgeht.

Mit einer modernen BaaS-Lösung beseitigen Sie alte Backup-Silos und implementieren einen umfassenden, einheitlichen Schutz der Enterprise-Klasse für eine breites Spektrum an Datenquellen. Dazu zählen beispielsweise:

- Cloudnative Apps
- SaaS-Workloads und -Apps
- Selbstentwickelte Cloud-Apps
- Virtuelle und physische Server
- Herkömmliche und containerisierte Anwendungen
- Relationale und verteilte Datenbanken
- Dateien und unstrukturierte Daten

Vorteile der Übertragung von nicht geschützten unstrukturierten Datenkopien in die Cloud

41 % mehr Sicherheit im Vergleich zu On-Premises-Ressourcen

38 % bessere Verfügbarkeit im Vergleich zu On-Premises-Ressourcen

37 % flexiblere Skalierbarkeit

36 % bessere Unterstützung einer höheren Endbenutzer-Anzahl

35 % schnellere Bereitstellung oder Wertschöpfung bei neuen Projekten

Quelle: Enterprise Strategy Group. „From Data Backup to Data Intelligence“, 2022.

Einheitliches Management

Unternehmen, die vor der Zeit des Cloud Computing gegründet wurden, werden wahrscheinlich die Datensicherung und -wiederherstellung einiger Workloads selbst verwalten. Gleichzeitig werden sie cloudbasierte Angebote wie M365, Salesforce und Workday vollständig nutzen. Unabhängig davon, wo sich Ihre Daten befinden oder wie sie bereitgestellt werden, muss Ihr Unternehmen sie gleichermaßen schützen – ohne dabei Verwaltungssilos zu erzeugen. Die richtige BaaS-Lösung vereint das Management von Datensicherung und -wiederherstellung in einer zentralen Bedienoberfläche. Selbst wenn Sie die Verwaltungsoberflächen Ihrer SaaS-Apps wie M365 oder SFDC verwenden möchten, haben Sie über eine zentrale Konsole vollständigen Einblick in diese Anwendungen sowie in alle selbstverwalteten On-Premises-Apps und Workloads. Vergewissern Sie sich, dass alle BaaS-Lösungen, die Sie in Erwägung ziehen, Backup-Daten über Hybrid- und Multicloud-Systeme hinweg vollständig vereinheitlichen. Außerdem sollten Sie Daten über eine zentrale Oberfläche schnell und global suchen und ortsunabhängig wiederherstellen können.

Einfacher Betrieb

Cloud-Anbieter nutzen ein Modell der geteilten Verantwortung. Die Anbieter garantieren die Betriebsbereitschaft der Infrastruktur und Sie sind für den Schutz der Daten Ihres Unternehmens verantwortlich. Obwohl Microsoft 365 (M365) in der Cloud auf Microsoft Azure läuft, hat beispielsweise jede der M365-Produktivitäts-Apps sowie Teams und SharePoint eine eigene begrenzte Schutzrichtlinie. Hinzu kommt, dass sich der Kampf um Talente verschärft. IT-Experten, die einen Großteil ihrer Zeit mit Routineaufgaben wie der Verwaltung von Schutzmaßnahmen durch Workload- und Cloud-Anbieter verbringen, werden sich daher nach neuen Möglichkeiten umsehen, die mehr positiven Einfluss auf das Unternehmen ermöglichen. Eine BaaS-Lösung auf Unternehmensebene entlastet Ihr IT-Personal. Sie erstellt routinemäßig Hunderte von Richtlinien und führt diese aus, sodass Ihre Experten mehr Zeit haben, sich auf Innovationen zu konzentrieren. Sie sichert Ihre Daten, bietet Ihnen Transparenz und vereinfacht den Schutz Ihrer Daten über mehrere Cloud-Dienste und On-Premises-Apps hinweg.

Hohe Zuverlässigkeit und Leistung – keine disruptiven Upgrades

In der schnelllebigen digitalen Geschäftswelt von heute erwarten die IT-Abteilungen und Teams der Geschäftsbereiche flexible, verfügbare, skalierbare und zuverlässige Backups. Eine moderne BaaS-Lösung kann Ihnen helfen, SLAs einzuhalten und Geschäftsergebnisse zu beschleunigen. Sie stellt zeitgerecht die benötigten Daten bereit und wehrt gleichzeitig Ransomware-Angriffe ab. Ein Cloud-Backup sorgt für einen unterbrechungsfreien Betrieb – es ist immer verfügbar, wird vor Ort aktualisiert und ist sofort einsatzbereit.

Geringer bis gar kein Platzbedarf im Rechenzentrum

Veraltete Backup-Infrastrukturen bestehen in der Regel aus einem Flickenteppich von Produkten. Ihre Daten sind dadurch anfälliger für Cyberangriffe. Cloud-Backups von unterschiedlichen SaaS-Anbietern bieten zahlreiche Angriffspunkte, über die Ransomware eindringen kann. Ein zentrales, konsolidiertes BaaS-Angebot mit wenig bis gar keiner On-Premises-Hardware verstärkt Ihren Schutz. Es reduziert den Platzbedarf Ihres Rechenzentrums und damit Ihre Angriffsfläche.

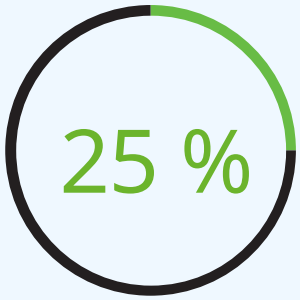
Was Sie die Anbieter fragen sollten: erweiterte Datensicherung und operative Handlungsfreiheit

- Wie groß ist die Toleranz Ihres Unternehmens (Unternehmens- und Anwendungsbesitzer) für Ausfallzeiten aufgrund von Aktualisierungen und Upgrades, die Backups betreffen?
- Wie soll Ihre nächste Lösung all die verschiedenen Datenquellen sichern, die Ihrem Unternehmen zur Verfügung stehen?
- Wie viel Zeit verbringen Ihre Mitarbeiter mit dem Management von Backups für SaaS-, cloudnative und On-Premises-Apps und -Daten?
- Welche Prozesse sind verfügbar, um Ihnen zu helfen, sich schnell an veränderte gesetzliche oder geschäftliche Anforderungen an den Datenschutz und die Datenspeicherung anzupassen?
- Welche Änderungen in Ihrer IT-Umgebung ziehen Sie in Betracht, um das Risikoprofil Ihrer On-Premises-Infrastruktur und der Cybersicherheit zu reduzieren?

2 Verstärkte Sicherheit und Ransomware-Bereitschaft

Unternehmensdaten sind ein gefährdetes Gut und Cyberkriminelle werden immer reicher. Laut Cybersecurity Ventures wird es bis zum Jahr 2031 alle 2 Sekunden zu einem Ransomware-Angriff kommen und die betroffenen Unternehmen jährlich 265 Milliarden US-Dollar kosten. Ihr Unternehmen muss daher nicht nur die IT-Flexibilität verbessern, sondern auch die Sicherheitslage verstärken und die Daten besser gegen Ransomware schützen.

BaaS kann Ihrem Unternehmen dabei helfen, die Zahlung von Lösegeld zu verweigern. Doch nicht alle BaaS-Angebote bieten die gleichen Fähigkeiten zur Abwehr von Ransomware. Achten Sie darauf, dass Sie in eine BaaS-Lösung investieren, die über wichtige Anti-Ransomware-Funktionen verfügt. Dazu gehören:



der Unternehmen gaben an, dass böswillige Löschungen die Hauptursache für SaaS-Datenverluste sind.

Quelle: Enterprise Strategy Group. „The Evolution of Data Protection Cloud Strategies“, 2021.

Unveränderliche Snapshots

Ihre Daten sind in Cloud-Backups mit unveränderlichen Snapshots besser geschützt. So können sie von Ransomware weder verschlüsselt noch verändert oder gelöscht werden. Mit dem richtigen BaaS gewährleisten Sie, dass Ihre strukturierten und unstrukturierten Daten – von E-Mails über Audio- und Videodateien bis hin zu Bildern – gesichert werden und diese im Falle eines Ransomware-Angriffs wiederhergestellt werden können.

Anomalieerkennung und Warnungen

Laut der Studie „Cost of a Data Breach 2022“ dauerte es durchschnittlich 277 Tage, um eine Sicherheitsverletzung zu erkennen und einzudämmen. Eine so lange Zeitspanne ermöglicht es Cyberkriminellen, Ihre Daten nicht nur zu verschlüsseln, sondern auch zu exfiltrieren, um sie im Dark Web zu verkaufen. Deshalb ist eine leistungsstarke automatische Anomalieerkennung, die nahezu in Echtzeit erfolgt, eine wichtige Funktion eines BaaS-Angebots. Mit einem Cloud-Backup können Sie den normalen Systembetrieb kontinuierlich verfolgen, um Unregelmäßigkeiten und abnormales Benutzerverhalten schnell zu erkennen, die auf einen Ransomware-Angriff hindeuten. Zusammen mit Warnungen können diese Funktionen eine potenzielle Gefahr signalisieren und Abhilfemaßnahmen einleiten. Beides trägt dazu bei, den Zerstörungsradius eines Ransomware-Angriffs zu minimieren.

Strikte Zugriffskontrollen

Die Studie „Cost of a Data Breach 2022“ fand außerdem heraus, dass kompromittierte Anmeldedaten im Jahr 2022 der bevorzugte erste Angriffsvektor waren. Das bedeutet, dass Ihr Unternehmen die Identität und die Zugriffsrechte von Benutzern effektiver verwalten muss. Optimale BaaS-Angebote unterstützen eine granulare rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC), um zu verhindern, dass Unbefugte Ihre Daten gefährden. Ihre Lösung sollte darüber hinaus auch eine Multifaktor-Authentifizierung (MFA) beinhalten. Dabei handelt es sich um einen zweistufigen Prozess, bei dem Sie etwas „haben“ und etwas „wissen“ müssen, um sich zu authentifizieren und sich gegen Phishing und andere Passwort-Hacks zu wappnen.

Datenisolation

Vor der Cloud-Ära bestand die gängigste Methode zur Wiederherstellung von Unternehmensdaten darin, Daten, die auf Bändern in einer externen Einrichtung gespeichert waren, zum Standort zurückzubringen. Dieser Prozess ist allerdings nicht mehr mit der Erfüllung der Wiederherstellungs-SLAs vereinbar, die im heutigen Geschäftsleben verlangt werden.

Modernes BaaS isoliert Daten von Ihrer Produktionsumgebung, indem es Backup-Daten in die Cloud auslagert und sichert. So kann modernes BaaS zum Beispiel eine Isolierung für Services in AWS schaffen. Dazu verschiebt es die Daten in einen separaten Tenant. Wenn Sie also nach einem Ransomware-Angriff eine schnelle Wiederherstellung benötigen, können Sie diese bewerkstelligen, ohne Ihre Produktionsumgebung erneut zu infizieren.

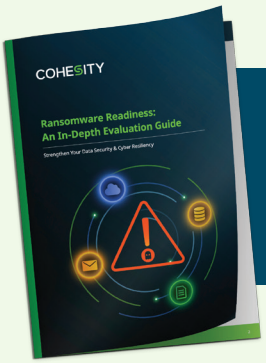
Schnelle, skalierbare Datenwiederherstellung

Angesichts der weiten Verbreitung von Ransomware und der Anzeichen, dass eine Verlangsamung der Malware-Entwicklung nicht in Sicht ist, muss Ihr Unternehmen dazu in der Lage sein, sich jederzeit schnell von einem Cyberangriff zu erholen. Dazu gehören Prozesse und Technologien, die es Ihnen ermöglichen, Ihre Daten zuverlässig und in großem Umfang wiederherzustellen.

Sie benötigen einen Cloud-Backup-Dienst, der alle Arten von Datenquellen – z. B. Hunderte von VMs, große Datenbanken oder große Mengen unstrukturierter Daten, M365-Produktivitätsdaten und vieles mehr – sofort, in großem Umfang, zu jedem Zeitpunkt und an jedem Ort wiederherstellen kann.

Was Sie die Anbieter fragen sollten: verstärkte Sicherheit und Ransomware-Bereitschaft

- Wie schützen Sie all Ihre verschiedenen Apps und Workloads vor Ransomware?
- Wie verhindern Sie zurzeit den unbefugten Zugriff auf Ihre Geschäftsdaten?
- Welche Pläne haben Sie für die skalierbare Datenwiederherstellung nach einer Ransomware-Attacke?



Ransomware-Bereitschaft: Ein ausführlicher Bewertungsleitfaden

Dieses Dokument kann Ihnen ebenfalls bei der Entscheidungsfindung helfen.

3 Mehr Flexibilität bei Verbrauch und Kosten sowie Nachhaltigkeit

Datensteuerung ist der neue Standard im Geschäftsleben. Unternehmen sind deshalb zunehmend bestrebt, die von ihnen gesammelten und gesicherten Daten zu nutzen, um neue Einblicke zu gewinnen und die Markteinführung von Produkten und Dienstleistungen zu beschleunigen. Doch die Daten, die Unternehmen steuern, wachsen exponentiell, sodass ihre Speicherung immer kostspieliger wird. Die Umstellung auf ein Service-Provider-Modell ist sowohl für das Unternehmen als auch für Ihre IT- und Beschaffungsteams eine Win-Win-Situation. Bei einem BaaS-Abonnement spart das Beschaffungsteam Zeit, da es nicht erst Verträge mit mehreren Anbietern von Backup-Hardware und Cloud-Lösungen abschließen muss. BaaS-Abonnements vereinfachen zudem Erneuerungen und deren vorhersehbare Preise verhindern unangenehme Budgetüberraschungen.

Wenn Sie BaaS zur Verbesserung Ihres Finanzmanagements und Ihrer Transparenz in Betracht ziehen, sollten Sie sich für einen Anbieter entscheiden, der Ihnen sowohl Vorhersehbarkeit als auch Auswahlmöglichkeiten bietet.

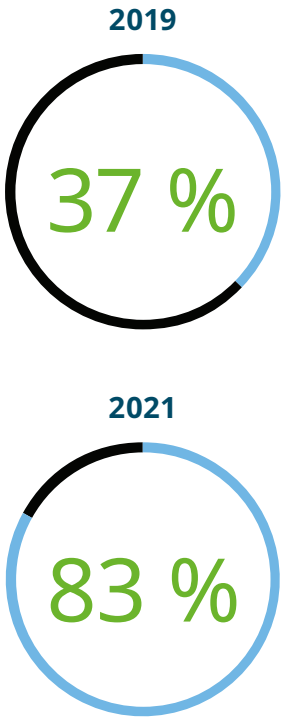
Einfache Übernahme

Flexibilität ist einer der wichtigsten Faktoren für Unternehmen, die BaaS in Erwägung ziehen. Vergewissern Sie sich, dass Ihr gewähltes BaaS-Angebot überschaubare Bindungsfristen bietet (z. B. ein Jahr) und Sie nur für die Kapazität zahlen, die Sie benötigen. Achten Sie auch darauf, dass die Abrechnung einfach zu verstehen ist. Sie sollte transparent und granular sein, um eine möglichst präzise Kostenvorhersage zu gewährleisten. Im Gegensatz zu selbstverwalteten Angeboten, die nur eine Option zulassen, bieten moderne BaaS-Lösungen mit mehreren Lizenzierungsoptionen höchstmögliche Flexibilität, darunter Frontend-, Backend- oder benutzerbasierte Lizenzen. Ein BaaS-Angebot sollte eine einfache Implementierung ermöglichen: registrieren – Konto einrichten –Datenquellen verbinden – automatische Workload-Erkennung. Sie sollten in der Lage sein, aufgabenkritische Daten und Anwendungen innerhalb von Minuten zu sichern.

Übertragbarkeit von Lizenzen

Unternehmensleiter investieren in die IT, um geschäftliche Erfolge zu erzielen. Technologien sollten nicht dazu führen, dass Sie beim Implementieren ihre Verfahrensweise oder den ausgewählten Standort ändern müssen. Wenn Ihr Unternehmen ein Backup benötigt, das Workloads und Apps sowohl vor Ort als auch in der Cloud unterstützt, sollten Sie sich nach einem BaaS-Anbieter umsehen, der die Übertragbarkeit von Lizenzen zwischen verschiedenen Nutzungsmodellen zulässt.

Wir senden unstrukturierte Datenkopien an Public-Cloud-Infrastrukturdienste für nicht schutzrelevante Zwecke (z. B. Entwicklung/Test, Analysen).



Quelle: Enterprise Strategy Group. „From Data Backup to Data Intelligence“, 2022.

Unterstützung für die Anforderungen der Datenhoheit

In einer kürzlich durchgeführten ESG-Umfrage äußerten sich die Unternehmen zunehmend besorgt über die Einhaltung von Vorschriften und Fragen der Datensouveränität bzw. des Standorts. Wenn Ihre Unternehmensleitung voll und ganz auf die Cloud setzt, können BaaS-Angebote Ihnen helfen, die Anforderungen an die Datensicherheit zu erfüllen. Die optimale BaaS-Lösung wird in Private Clouds von Rechenzentren und in führenden Public Clouds bereitgestellt, die Ihre Daten in Übereinstimmung mit nationalen und lokalen Vorschriften nach Regionen auf der ganzen Welt aufteilen können.

Transparente Pay As You Grow-Preise – keine versteckten Kosten

In wirtschaftlich unsicheren Zeiten kann es wichtig sein, Geld für Innovationen zu sparen. BaaS ermöglicht Ihrem Unternehmen, von Investitionsausgaben zu einem besser vorhersehbaren Betriebskostenmodell überzugehen. Gleichzeitig entfallen mit der richtigen BaaS-Lösung die Bereitstellungs- und versteckten Cloud-Kosten, wie z. B. die Gebühren für den Dateneingang und -ausgang. Suchen Sie nach einem Angebot, mit dem Sie Ihre Backup-Daten sicher und effizient in der Cloud sichern und konsolidieren können. Darüber hinaus sollten Sie Ihre Daten besser nutzen können, um mehr Einblicke zu gewinnen und Ihr Risiko zu senken.

Nachhaltigkeitsvorteile

Ihre Marke wird heute nicht nur danach bewertet, wie gut Sie sich um Ihre Kunden und Mitarbeiter kümmern, sondern auch danach, wie sehr Sie sich für den Schutz unseres Planeten einsetzen. Ein Cloud-Backup verringert den Bedarf an Hardware in Ihrem Rechenzentrum, was Ihren Energieverbrauch senkt – ein wichtiges Ziel von Unternehmensinitiativen im Bereich Umwelt, Soziales und Unternehmensführung (Environment, Social and Governance, ESG). Wählen Sie deshalb ein BaaS-Angebot, das mit Ihren ESG-Zielen übereinstimmt.

Was Sie die Anbieter fragen sollten: mehr Flexibilität bei Verbrauch und Kosten sowie Nachhaltigkeit

- Wie haben sich Ihre Investitionen in die Datensicherung in den letzten Jahren verändert?
- Auf welche Weise hat Ihr Unternehmen die IT optimiert, um in Zeiten wirtschaftlicher Unsicherheit Innovationen zu fördern?
- Welche ESG-Ziele verfolgt Ihr Unternehmen?

Checkliste: BaaS-Angebote

Gehen Sie mit BaaS den nächsten Schritt zur cloudgesteuerten IT-Modernisierung. Dadurch können Sie Ihre Ziele in puncto Sicherung für alle Ihre Datenquellen vorantreiben, Handlungsspielraum gewinnen, Ihre Umgebung besser gegen Ransomware schützen und Ihre Kosten optimieren. Die folgende Checkliste mit den wichtigsten Funktionen soll Ihnen bei der Bewertung von BaaS-Angeboten helfen, die optimale Lösung für Ihr Unternehmen zu finden.

Funktionen		Anbieter 1	Anbieter 2	Anbieter 3
Erweiterte Datenquellensicherung und operative Handlungsfreiheit	Umfassende Unterstützung von Datenquellen	☐	☐	☐
	Einheitliches Management	☐	☐	☐
	Einfacher Betrieb	☐	☐	☐
	Hohe Zuverlässigkeit und Leistung – keine disruptiven Upgrades	☐	☐	☐
	Geringer bis gar kein Platzbedarf im Rechenzentrum	☐	☐	☐
Verstärkte Sicherheit und Ransomware-Bereitschaft	Unveränderliche Snapshots	☐	☐	☐
	Anomalieerkennung und Warnungen	☐	☐	☐
	Strikte Zugriffskontrollen	☐	☐	☐
	Datenisolation	☐	☐	☐
	Schnelle, skalierbare Datenwiederherstellung	☐	☐	☐
Mehr Flexibilität bei Verbrauch und Kosten sowie Nachhaltigkeit	Einfache Übernahme	☐	☐	☐
	Übertragbarkeit von Lizenzen	☐	☐	☐
	Unterstützung für die Anforderungen der Datenhoheit	☐	☐	☐
	Transparente Pay As You Grow-Preise – keine versteckten Kosten	☐	☐	☐
	Nachhaltigkeitsvorteile	☐	☐	☐

„Backup as a Service von Cohesity ermöglicht uns, unsere wertvollen Benutzerdaten zu sichern, ohne dass wir im Voraus eine große Menge an zusätzlicher Speicherinfrastruktur kaufen müssen. Da wir keine Hardware kaufen mussten, waren wir mit dem BaaS-Angebot von Cohesity innerhalb einer Stunde startklar.“

Jake Parham
IT Manager, St. Johns County Sheriff’s Office

Lassen Sie BaaS für sich arbeiten

Erweitern und beschleunigen Sie Ihre IT-Modernisierung, indem Sie BaaS einführen. Mit einem einfacheren, effizienteren und sichereren Unternehmensschutz für die Vielzahl von Datenquellen, auf die Ihr Unternehmen heutzutage angewiesen ist, wird Ihr Unternehmen agiler. Erfüllen Sie Business-SLAs und Compliance-Anforderungen. Ersparen Sie sich Zeit und Kopfzerbrechen beim IT-Datenmanagement. Erreichen Sie Ihre ESG-Ziele. Mit dem richtigen BaaS-Angebot ist all dies möglich.

Erfahren Sie mehr über BaaS von Cohesity.

COHESITY