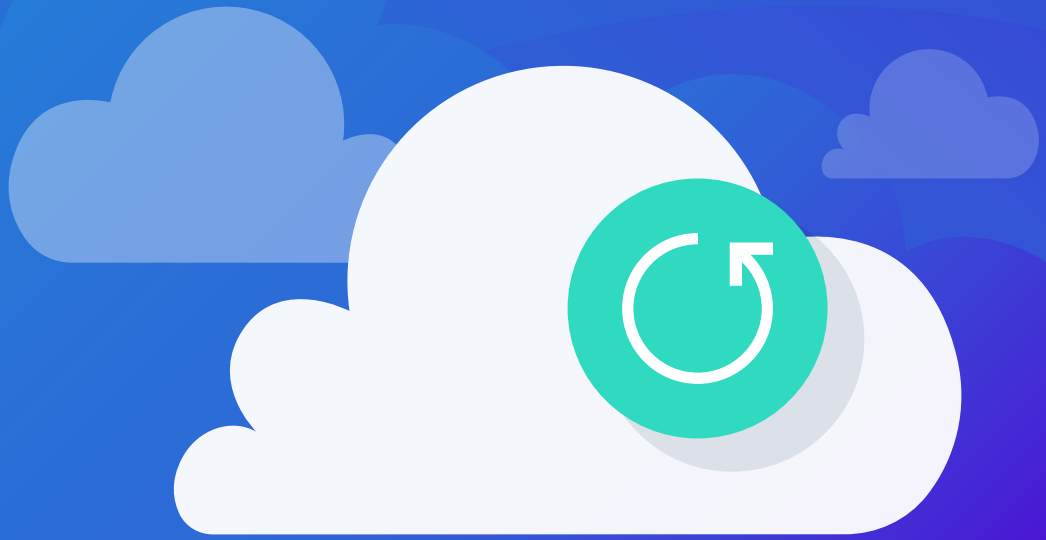
E-Book

datto

BCDR-Käuferleitfaden für MSPs



Einführung

Wenn der Server eines Kunden zusammenbricht oder bei einem Cyberangriff geschädigt wird, brauchen Managed Service Provider (MSPs) eine effektive BCDR-Lösung (Business Continuity und Disaster Recovery), um die Daten und den Betrieb schnell wiederherzustellen, ohne die Marge zu opfern. Dazu bedarf es einer branchenführenden Wiederherstellungstechnologie von einem Anbieter, der Sie rund um die Uhr unterstützt – egal, worum es geht. Kurz gesagt: Sie brauchen eine Lösung, auf die Sie sich verlassen können. Eine Lösung, die Ruhe schenkt – Ihnen und Ihren Kunden.

In diesem E-Book beschäftigen wir uns mit einigen weit verbreiteten Mythen und irrigen Annahmen rund um das Thema „BCDR" und geben Ihnen Tipps zu ein paar Punkten, auf die Sie achten sollten, wenn Sie auf der Suche nach einer BCDR-Lösung sind. Außerdem erfahren Sie, wie Datto Continuity dafür sorgt, dass BCDR für MSPs effizient und profitabel ausfällt.

Das könnte Sie auch interessieren:

Häufige Mythen und irrige Annahmen über BCDR

Ob Sie ein Neuling im Bereich der BCDR-Dienste sind oder Ihr derzeitiges Produkt ersetzen möchten – es ist immer wichtig, verbreitete Mythen als solche zu erkennen und das große Ganze zu betrachten. Letztendlich wird es Ihnen bei der Auswahl des richtigen Produkts für Ihr Managed Services-Angebot zugutekommen, diese irrigen Annahmen zu durchschauen.

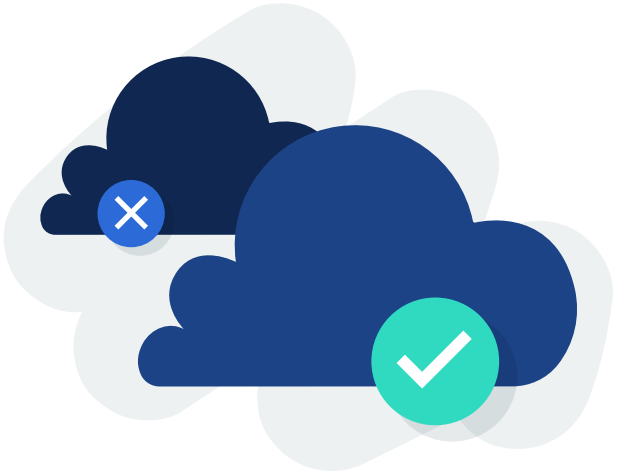
Mythos Nr. 1: **Ein Backup ist gut genug**

Ein Backup ist zweifellos ein wichtiger Teil der Business Continuity und Disaster Recovery. Steht es aber allein, bleibt ein Unternehmen anfällig für kostenintensive Ausfallzeiten. Warum? Weil die Wiederherstellung großer Datensätze (wie etwa der Inhalte eines kompletten Servers) zeitraubend sein kann. Ganz zu schweigen von der Zeit, derer es bedarf, um neue Hardware zu beschaffen, wenn die primären Systeme nicht mehr betriebsbereit sein sollten. In dieser Zeit muss die Produktivität zwangsweise auf Eis gelegt werden, was auch den Umsatz ausbremst.

Aus diesem Grund benötigen Unternehmen eine Lösung, die neben dem Backup auch schnelle Wiederherstellungen ermöglicht. Für viele Organisationen lautet die Antwort auf dieses Problem: BCDR. BCDR-Lösungen arbeiten mit Backups, Snapshots, Virtualisierung und der Cloud, um Daten zu schützen und dafür zu sorgen, dass Wiederherstellungen schnell über die Bühne gehen.

Mythos Nr. 2: **Anbieter von reinen Software-Lösungen sind günstiger**

Es ist verständlich, wie es zu diesem Mythos kommt, denn reine Softwareprodukte haben im Vergleich zu Komplettlösungen einfach geringere Vorlaufkosten. Das liegt zum großen Teil daran, dass Sie sie mit jeder Hardware (wie etwa günstigen, gebräuchlichen x86-Servern) und öffentlichen Clouds betreiben können. Wenn Sie sich jedoch die vollständigen Anschaffungs- und Betriebskosten (TCO) ansehen, können reine Softwareprodukte langfristig teurer werden als Komplettlösungen.



Ja, alle Cloud-Anbieter liefern eine in hohem Grade zugriffsfähige Server- und Speicherinfrastruktur. Aber das bedeutet nicht, dass sie alle in gleichem Maße auf BCDR ausgelegt sind.

Denn bei Komplettlösungen steht die Benutzerfreundlichkeit im Vordergrund. Sie arbeiten mit nur einem einzigen Anbieter (und einer monatlichen Gebühr) für die Hardware, die Software und die Cloud. Der technische Support ist geradlinig und zielgerichtet – egal, wo das Problem liegt. Und die Hardware ist größentechnisch auf den Bedarf des Kunden zugeschnitten, was manuelle Arbeiten, Konfigurationsfehler und die jeweils damit verbundenen Kosten reduziert. All-in-one-Lösungen können sogar Hardwareaustausch und Kapazitätserweiterungen umfassen, sodass die Skalierbarkeit, die über die Nutzugsdauer nötig sein kann, vereinfacht wird. Und zu guter Letzt bleiben Sie auch noch von überraschenden Kosten für die Cloud verschont.

Mythos Nr. 3: **Alle Clouds sind gleich**

Ja, alle Cloud-Anbieter liefern eine in hohem Grade zugriffsfähige Server- und Speicherinfrastruktur. Aber das bedeutet nicht, dass sie alle in gleichem Maße auf BCDR ausgelegt sind. Die Kosten sind bei öffentlichen Clouds ganz zweifellos am besten. Es stimmt, Sie zahlen nur für das, was Sie nutzen. Aber das bedeutet, dass die Kosten genau dann hoch auflaufen, wenn der Zeitpunkt am denkbar schlechtesten ist – wenn Sie nämlich eine virtuelle Maschine (VM) für Wiederherstellungen erstellen und nutzen. Darüber hinaus erheben Cloud-Anbieter Ausgabegebühren für Daten, die aus der Cloud entnommen werden. Insofern kann es teuer werden, wenn Sie einen großen Datensatz aus der Cloud herunterladen (wie Sie es beispielsweise tun müssen, um einen Server wiederherzustellen). Außerdem sind bei einigen Clouds Staffelungen für Rechnerleistung, Speicherung und Sicherheit vorgesehen, was die Komplexität erhöht.

Bei manchen BCDR-Komplettlösungen sind die Kosten für die Cloud bereits in der monatlichen Gebühr inbegriffen. Das kommt den MSPs zugute, denn so bleiben die OPEX-Kosten kalkulierbar. Es vereinfacht die Aufgabe, den Kunden die BCDR-Dienstleistungen in Rechnung zu stellen, und gewährleistet, dass die Margen für die Dienstleistungen konsistent bleiben. Einige Komplettlösungen bieten außerdem zusätzliche Sicherheitsfunktionen, wie eine für jeden Schritt anstehende Zwei-Faktor-Authentisierung und gesicherte Cloud-Anwendungen. Bei anderen ist möglicherweise sichergestellt, dass Daten nicht verändert werden können, und sie verfügen über automatisierte Speicherfähigkeiten, die Unternehmen helfen, den Sicherheitszielen und Compliance-Vorgaben zu entsprechen.

Mythos Nr. 4: **Das Risiko ist bei allen BCDR-Lösungen gleich hoch**

Das ist schlicht nicht wahr. Welches Risiko Sie tragen, wenn Sie BCDR-Dienste erbringen, kann in hohem Maße davon abhängen, für welche Lösung und welchen Anbieter Sie sich entscheiden. Vergleichen wir doch noch einmal die Komplettlösungen mit den reinen Softwareprodukten.

Bei reinen Softwareprodukten verlassen Sie sich in Bezug auf die Hardware, die Software und die Cloud auf verschiedene Anbieter. Das kann mehrere verschiedene Fehlerquellen und das Abwälzen der Schuld von einem Anbieter auf den nächsten nach sich ziehen, wodurch mehr Zeit benötigt wird, um ein Problem zu lösen. Schlimmer noch: Wenn ein Anbieter eine Änderung vornimmt, kann sich das auf die gesamte Lösung auswirken. So besteht beispielsweise die Möglichkeit, dass ein Software-Update von einem kleinen Knick in der Leistung bis hin zu einem teuren Hardware-Upgrade nahezu alles nach sich ziehen kann.

Bei Komplettlösungen genießen die MSPs den Rückhalt und Support eines einzigen Anbieters, der sich um die Software, die Hardware und die Cloud kümmert. Und das wiederum senkt die Risiken für den MSP.

Das könnte Sie auch interessieren:

Beurteilung von BCDR- und DRaaS-Lösungen

Ihnen ist mittlerweile vermutlich bewusst, dass die Frage, ob Sie die BCDR-Komplettlösung mit Cloud-DRaaS eines einzelnen Anbieters wählen oder aus den Angeboten mehrerer Anbieter Ihr eigenes System zusammenstellen, zu den wichtigsten Entscheidungen des ganzen Prozesses gehört. Auch der Ort, an dem die Rechnerarbeiten stattfinden und die Speicherressourcen beheimatet sind, muss gut überlegt sein. Denn dabei kann es sich um eine selbst gehostete Cloud, eine öffentliche Cloud oder die Cloud eines BCDR-Anbieters handeln. Ungeachtet des Ansatzes, den Sie wählen, brauchen Sie aber in jedem Fall ein umfassendes Toolkit, um Ihren Kunden BCDR-Dienste bieten zu können. Dazu gehört Folgendes:

Software

Die BCDR-Software wird dazu verwendet, die Backup- und Wiederherstellungsprozesse zu automatisieren und zu verwalten. Nach einem ersten vollen Server-Backup macht die BCDR-Software immer wieder Folge-Snapshots, um „Wiederherstellungspunkte“

RPO/RTO

Das Wiederherstellungspunktziel (RPO) und das Wiederherstellungszeitziel (RTO) sind ebenfalls wichtige Aspekte. Diese Metriken beziehen sich jeweils auf den Wiederherstellungszeitpunkt und darauf, wie schnell Sie eine Wiederherstellung durchführen können. In Bezug auf BCDR ergeben sich RPO und RTO aus der Frequenz der Backups, der geschützten Datenmenge, den Fähigkeiten der Software, der Leistung der Hardware und/oder der Cloud und dem Cloud-Anbieter, für den Sie sich entscheiden.

oder Server-Images eines bestimmten Zeitpunkts zu generieren. Diese Wiederherstellungspunkte dienen dazu, die Daten eines primären Servers so wiederherzustellen, wie sie in einem bestimmten Moment aussahen (also vor dem Ausfall). Sie können auch erstellt oder „virtualisiert" werden, um Servertätigkeiten auf einem sekundären Gerät oder in der Cloud wiederherzustellen. Diesen Prozess nennt man „Failover".

Funktionen einer guten BCDR-Software:

- Lokales Backup und Backup in der Cloud
- Lokales Failover und Failover in der Cloud
- Wiederherstellungsfunktionen für eine Vielzahl von Wiederherstellungsszenarien*

**Die Bandbreite der Wiederherstellungsszenarien kann von der Wiederherstellung einiger weniger verloren gegangener Dateien bis hin zu einem kompletten Serverausfall reichen. Halten Sie also nach Lösungen Ausschau, die auf Ihre spezifischen Bedürfnisse eingehen. Neben dem VM-Failover sollte eine BCDR-Lösung auch Funktionen wie die Wiederherstellung von Dateien und Ordnern, eine Ransomware-Erkennung mit Rollback, Export von Server-Images und Bare Metal Recovery bieten.*

Cloud

Wie wir bereits erwähnt haben, beinhalten die BCDR-Lösungen von heute auch eine Komponente für Backups und Wiederherstellungen über eine Cloud. Sollten sowohl die primäre als auch die BCDR-Hardware ausfallen, kann ein Server-Image als VM in der Cloud erstellt werden.

Je nachdem, welchen Ansatz Sie wählen, gibt es folgende Möglichkeit für Clouds:

- Öffentliche Cloud (selbst erstelltes System)
- Selbst gehostete Cloud (selbst erstelltes System)
- Cloud eines BCDR-Anbieters (Komplettlösung)

Die Cloud dient im Rahmen der BCDR zwei Zwecken. Zunächst einmal ist sie ein ausgelagerter Speicherort für tertiäre Backup-Images des Servers, die für Wiederherstellungen genutzt werden können. Zweitens kann in der Cloud ein VM erstellt werden, um während eines Failovers die Funktionen des primären Servers zu übernehmen.

Sollten sowohl die primäre als auch die BCDR-Hardware ausfallen, kann ein Server-Image als VM in der Cloud erstellt werden.

Kosten und verborgene Gebühren für Clouds

Ob Sie eine Komplettlösung oder eine selbst zusammengestellte Lösung mit Nutzung einer öffentlichen Cloud wählen, hat Auswirkungen auf die Kosten. Werfen wir doch einmal einen genaueren Blick auf die Optionen:

Cloud-Komplettlösung von einem Anbieter	**Öffentliche Cloud**
Einfache, kalkulierbare monatliche Gebühr für Speicherung in der Cloud und Rechnerarbeiten	Kosten für Rechnerarbeiten in der Cloud laufen während einer Disaster Recovery hoch auf
Kalkulierbare Rechnerleistung in der Cloud während Disaster Recovery-Arbeiten	Cloud-Anbieter gibt möglicherweise keine Leistungsgarantien/Mindestwerte (oder die Kosten könnten steigen, um dem Leistungsbedarf gerecht zu werden)
Keine zusätzlichen Kosten für Wiederherstellungen auf dem primären Server	Cloud-Anbieter erheben Ausgabegebühren für Daten, die aus der Cloud entnommen werden
Physisches Wiederherstellungsgerät wird über Nacht versandt (wichtig für die Wiederherstellung großer Datensätze)	Wiederherstellung auf primärem Server ist von Geschwindigkeit des Internet abhängig
Spezialisierter technischer Support während Disaster Recovery-Tätigkeiten, einschließlich Failover und Failback	MSP muss DR-Tätigkeiten, einschließlich möglicherweise komplexer Failbacks, ohne Hilfe durchführen
Reiche Sicherheitsfunktionen, einschließlich Administrationszugriff und unveränderlicher Backup-Snapshots, die nicht von Ransomware angegriffen werden können	Ein „gemeinsames Modell", bei dem die Bürde der Datensicherheit beim Dateneigentümer liegt und nicht beim Anbieter der Cloud. Ein Beispiel ist das AWS-Modell der gemeinsamen Verantwortung

Bei einer Komplettlösung hingegen ist das Schreiben Ihrer eigenen Rechnungen eine geradlinige Angelegenheit, denn Sie haben eine einfache Pauschalgebühr, in der die Kosten für die Speicherung in der Cloud, die Rechnerarbeiten und die Wiederherstellung enthalten sind.

Wie Sie sehen können, schwanken die Kosten für eine Cloud ganz erheblich – je nachdem, für welchen Ansatz Sie sich entscheiden. Für einen MSP ist diese Überlegung auch im Hinblick auf die Rechnungen bedeutsam, die er selbst stellen wird. Wenn Sie sich beispielsweise für die Nutzung einer öffentlichen Cloud entscheiden, nehmen Sie die (geschätzten) Kosten für eine Wiederherstellung dann in die monatliche Gebühr auf, die Sie von Ihren Kunden verlangen? Oder stellen Sie die Kosten für eine Wiederherstellung separat in Rechnung? Ersteres schafft ein besseres Kundenerlebnis, aber es birgt auch Risiken: Was geschieht, wenn Sie die Kosten unterschätzt haben? Die zweite Option mindert die Risiken für den MSP, kann aber dazu führen, dass die Kunden unzufrieden werden, wenn hohe Kosten auflaufen.

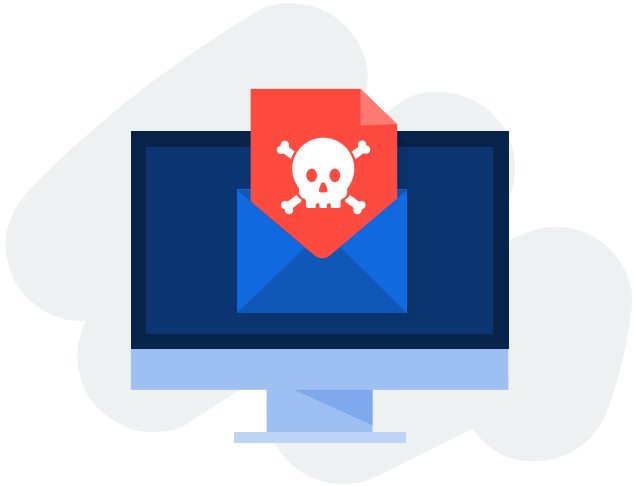
Bei einer Komplettlösung hingegen ist das Schreiben Ihrer eigenen Rechnungen eine geradlinige Angelegenheit, denn Sie haben eine einfache Pauschalgebühr, in der die Kosten für die Speicherung in der Cloud, die Rechnerarbeiten und die Wiederherstellung enthalten sind. So profitieren Sie von einem unkomplizierten Kundenerlebnis und kalkulierbaren Margen für die Dienstleistungen, die Sie erbringen.

Hardware

Die BCDR-Hardware dient einer Reihe von Zwecken. Zunächst einmal ist sie die Grundlage für die Arbeit der BCDR-Software. Zum Zweiten agiert sie als Speicherort für Backup-Images des Servers, die für Wiederherstellungen genutzt werden können. Zum Dritten überträgt sie die Server-Images an die Cloud, um eine Disaster Recovery zu ermöglichen. Und schließlich übernimmt sie bei einem lokalen Failover die Rolle des primären Servers, sodass die Betriebstätigkeit weiterlaufen kann, während der ausgefallene primäre Server wiederhergestellt wird.

Heute handelt es sich bei BCDR-Hardware üblicherweise um einen sekundären, vor Ort befindlichen Server mit:

- reichlich Verarbeitungsleistung, um normale Servertätigkeiten zu übernehmen, und
- genügend Speicherkapazität, um Wiederherstellungspunkte für einen bestimmten Zeitraum aufzubewahren (beispielsweise 90 Tage).



Angreifer zielen mit ihrer Ransomware immer öfter auf Backups ab, um ihren Opfern die Chance zu nehmen, ohne die Zahlung des Lösegelds problemlos eine Wiederherstellung durchzuführen. Deshalb brauchen MSPs eine BCDR-Lösung, die auf diese Nöte eingeht.

Die BCDR-Hardware kann ein gebräuchlicher x86-Server oder ein spezielles BCDR-Gerät sein. Bei reinen Softwarelösungen werden Sie die Software des BCDR-Anbieters wohl vermutlich auf einem x86-Server laufen lassen. Komplettlösungen hingegen werden möglicherweise als reine Software versandt oder sind so ausgefertigt, dass die BCDR-Software bereits auf einem Gerät vorinstalliert ist.

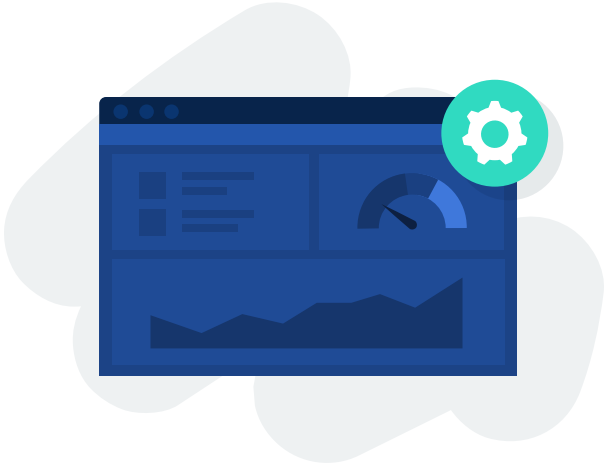
Der Einsatz eines speziellen BCDR-Geräts kann für den MSP sehr nützlich sein. Denn in diesem Fall sind die Software und die Hardware aufeinander abgestimmt und der Anbieter kann das Gerät so konfigurieren und größentechnisch anpassen, dass es dem individuellen Bedarf des Kunden entspricht. Sollten Sie die Komplettlösung wünschen, Ihre Hardware jedoch selbst auswählen wollen, ist dies natürlich auch möglich – suchen Sie einfach nach BCDR-Anbietern, die einen flexiblen Einsatz unterstützen.

Wenn Unternehmen die Lasten einiger oder aller primärer Server in die Cloud verlegen, kann es sein, dass sich die lokale BCDR-Hardware ändern muss oder ganz überflüssig wird. Allerdings geht aus unserer jährlichen „State of the MSP"-Umfrage hervor, dass die Akzeptanz der Cloud steigt, die lokale Hardware aber derzeit immer noch die Norm ist.

Sicherheit und Compliance

Viele MSPs betreuen Kunden in Branchen mit erheblichen Sicherheits- und Compliance-Anforderungen. Darüber hinaus zielen Angreifer mit ihrer Ransomware immer öfter auf Backups ab, um ihren Opfern die Chance zu nehmen, ohne die Zahlung des Lösegelds problemlos eine Wiederherstellung durchzuführen. Deshalb brauchen MSPs eine BCDR-Lösung, die auf diese Nöte eingeht. Eine Ransomware-Erkennung und die Möglichkeit eines auf einen bestimmten Zeitpunkt ausgerichteten Rollbacks sind ein Muss. Und auch die Unveränderlichkeit von Daten sollte man nicht außer Acht lassen.

Darunter versteht man, dass die Daten auf eine Art und Weise gespeichert werden, die die Möglichkeit einer Änderung durch externe Aktivitäten ausschließt. So wird gewährleistet, dass Backups nicht durch Ransomware zerstört oder im Rahmen eines anderen Angriffs gelöscht werden. Eine solche Funktion kann den Unternehmen auch dabei helfen, spezifischen Compliance-Standards in Bezug auf die Archivierung von Daten zu



Achten Sie auf Produkte, die jene kritischen Tools integrieren, auf die Sie vertrauen, wie etwa eine Remote Monitoring & Management-Software (RMM) und Professional Services Automation (PSA).

entsprechen. Halten Sie nach BCDR-Lösungen Ausschau, die auf die Unveränderlichkeit von Daten achten, die Daten in Übereinstimmung mit den Berichtsstandards der Service Organization Control (SOC 1 / SSAE 16 und SOC 2 Typ II) speichern und überall obligatorisch eine Zwei-Faktor-Authentisierung verlangen.

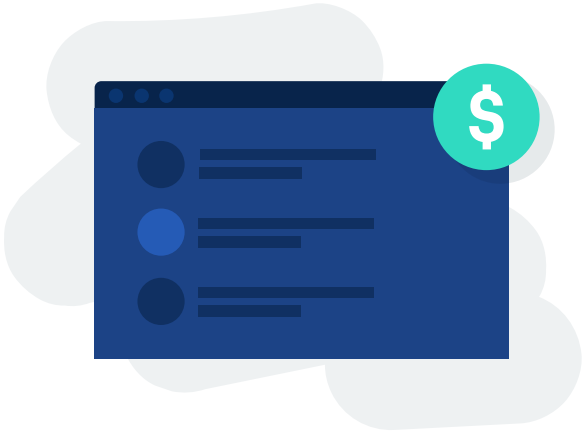
Lösungen, die ein automatisiertes, auf Richtlinien basierendes Aufbewahrungsmanagement ermöglichen, um Compliance-Standards zu erfüllen, können den Bedarf an manuellen Eingriffen verringern. Sie optimieren das Management und stellen sicher, dass Kundendaten für eine angemessene Zeitdauer in der Cloud gespeichert werden.

Benutzerfreundlichkeit/Verwaltung

Die Benutzerfreundlichkeit ist für MSPs von entscheidender Bedeutung. Durch die Steigerung der Effizienz können die Margen bei den erbrachten Dienstleistungen erhöht werden. Daher sollte es als unerlässlich angesehen werden, ein Produkt zu finden, das einfach bereitzustellen und zu verwalten ist. Suchen Sie nach BCDR-Produkten, die speziell für MSPs entwickelt wurden. Das könnte eine optimierte Eingliederung, Multi-Tenant-Management, verschiedene Einsatzmöglichkeiten, End-to-End-Sicherheit und flexible Aufbewahrungsrichtlinien beinhalten.

Achten Sie auf Produkte, die jene kritischen Tools integrieren, auf die Sie vertrauen, wie etwa eine Remote Monitoring & Management-Software (RMM) und Professional Services Automation (PSA). Integrationen können dafür sorgen, dass Sie bei der Erbringung Ihrer BCDR-Dienstleistungen effizienter werden, indem Sie weniger Schritte brauchen, um häufige Aufgaben zu erledigen.

Außerdem müssen Sie sich überlegen, ob Sie eine Komplettlösung haben möchten, bei der Sie die Rückendeckung eines einzigen Anbieters haben, oder ob Sie Ihr System lieber selbst zusammenstellen. Reine BCDR-Softwareprodukte sind nicht per se komplizierter zu verwalten, aber der Umgang mit mehreren verschiedenen Anbietern kann mögliche Fehlerbehebungen erschweren.



Lösungen, die die Effizienz verbessern, sorgen auch für eine höhere Marge und mehr Gewinn, denn sie erfordern weniger manuelle Intervention, wenn es um den Einsatz und die Verwaltung geht.

Profitabilität

Keine Diskussion über Produktbewertung ist für MSPs vollständig, ohne die Rentabilität zu berücksichtigen. Suchen Sie nach Produkten mit den erforderlichen Eigenschaften und Funktionen zu einem Preis, mit dem Sie Margen für Ihre Services aufbauen können. Wenn Sie die Lösungen beurteilen, müssen Sie sich die gesamten Anschaffungs- und Betriebskosten ansehen, nicht nur die Kosten für Software und Hardware. Wir sind auf diesen Punkt bereits zu einem früheren Zeitpunkt eingegangen.

Lösungen, die die Effizienz verbessern, sorgen auch für eine höhere Marge und mehr Gewinn, denn sie erfordern weniger manuelle Intervention, wenn es um den Einsatz und die Verwaltung geht. Halten Sie nach Lösungen Ausschau, die speziell auf MSPs zugeschnitten sind und eine effiziente, zuverlässige Technologie, Multi-Tenant-Management und die Integration mit all den anderen Tools bieten, auf die Sie bauen.

Eine solche Lösung kann Ihnen die Möglichkeit eröffnen, Ihre Kunden noch besser zu unterstützen und Ihrem Unternehmen zum Wachstum zu verhelfen. Sie müssen keine Zeit mehr mit Konfiguration, fortlaufender Verwaltung und Fehlerbehebung verschwenden. Dies spart den Technikern Zeit und reduziert die OpEx-Ausgaben – was die Margen erhöht und den Umsatz steigert.

Das könnte Sie auch interessieren:

Datto Continuity (BCDR)

Datto Continuity ist eine BCDR-Komplettlösung, die umfassende Backup- und Speichermöglichkeiten für physische und virtuelle Server bietet. Ob als physisches Gerät, auf einer virtuellen Maschine installierte Software oder Image auf Ihrer eigenen Hardware – mit Datto Continuity genießen Sie lokale Backups, Backups in der Cloud, Wiederherstellungen und Failover für einen monatlichen Pauschalpreis. Ganz ohne versteckte Kosten oder nicht kalkulierbare Ausgaben für die Cloud.

Da müssen sich MSPs keine Sorgen mehr machen, dass sie oder ihre Kunden angegriffen werden könnten. Mit der unveränderlichen Datto Cloud, AES-256-Verschlüsselung bei der Übertragung und optional auch bei der Speicherung, Cloud Deletion Defense zum Schutz der Backups, gesicherten Geräten und durchgehender Zwei-Faktor-Authentisierung gewährleistet diese Lösung eine ganzheitliche Sicherheit.

Die patentierte Inverse Chain-Technologie macht Backups widerstandfähig gegenüber Ransomware und sorgt dafür, dass alle Backups automatisch gescannt werden, um sicherzustellen, dass die Server-Images vollständig, frei von Ransomware und bootbar sind. Datto Continuity schützt vor dauerhaftem Datenverlust und ermöglicht es MSPs, mit granularen, zeitpunktgenauen Backups die Daten von Kunden nach einem Ransomware-Angriff problemlos wiederherzustellen.

Wie Sie wissen, geht es bei der Bereitstellung profitabler Managed Services darum, die Effizienz zu steigern und die Rendite der Services zu maximieren. Mit einer einzigen Ansicht erhalten Sie einen vollständigen Überblick über Kunden-Backups und können so die Effizienz weiter steigern.

Das könnte Sie auch interessieren:

Datto SIRIS Datenblatt →

Datto Cloud Datenblatt →

DEMO ANFORDERN

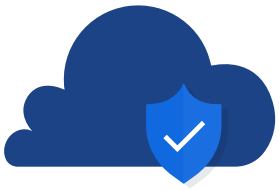
Datto Continuity bietet:

- Inverse Chain: patentierter Schutz der Backups vor Ransomware
- Sofortige Wiederherstellung
- Erstklassige Cloud
- Durchgängige Sicherheit
- Unbegrenzte Skalierbarkeit
- Unbegrenzte Aufbewahrung
- 24/7/365 Support mit Sitz in den USA
- Unbegrenzte Backup-Agents
- Unbegrenzte Speicherung in der Cloud
- Pauschalpreis
- Flexible Einsatzmöglichkeiten
- Sicheres Multi-Tenant-Cloudmanagement

Datto Continuity in Zahlen:

Milliarden von Backups

Zehntausende von Wiederherstellungen



Exabyte-skalierte Cloud

Werfen Sie noch heute einen Blick auf datto.com **und erfahren Sie mehr über Datto Continuity.**