

e-boek

datto

BCDR Buyer's Guide voor MSP's



Inleiding

Wanneer de server van een klant uitvalt of wordt gecompromitteerd door een cyberaanval, hebben managed service providers (MSP's) een effectieve oplossing voor bedrijfscontinuïteit en rampenherstel (BCDR) nodig om gegevens en activiteiten snel te herstellen, zonder dat dit ten koste gaat van de marge. Dat betekent toonaangevende hersteltechnologie van een leverancier die er is om u 24x7x365 te ondersteunen, wat er ook gebeurt. Simpel gezegd heeft u een oplossing nodig waarop u kunt vertrouwen. Een die zorgt voor gemoedsrust – voor u en voor uw klanten.

In dit e-book ontkrachten we veelvoorkomende mythen en misvattingen over BCDR-oplossingen en geven we tips over waar u op moet letten bij de keuze van een BCDR-oplossing. U leert ook hoe Datto Continuity BCDR efficiënt en winstgevend maakt voor MSP's.

Mogelijk bent u ook geïnteresseerd in:

Recovery Time
& Downtime
Cost Calculator

LEARN MORE



Veelvoorkomende mythen en misvattingen over BCDR

Of BCDR-diensten nu nieuw voor zien of dat u uw huidige product vervangt, het is belangrijk om verder te kijken dan de gangbare mythen en het grotere geheel te zien. Inzicht in deze misvattingen kan u helpen het juiste product voor uw MSP-praktijk te selecteren.

Mythe 1: Back-up is goed genoeg

Back-up is uiteraard een cruciaal onderdeel van bedrijfscontinuïteit en rampenherstel. Met back-up alleen blijven bedrijven echter kwetsbaar voor kostbare uitvaltijd. Waarom? Omdat het herstellen van grote datasets (zoals de inhoud van een complete server) tijdrovend kan zijn. Om nog maar te zwijgen over de tijd die het kost om nieuwe hardware aan te schaffen als de primaire systemen onbruikbaar worden. Intussen komt de productiviteit tot stilstand en stopt de inkomstenstroom.

Daarom hebben bedrijven een oplossing nodig die naast het maken van back-ups ook snel herstel mogelijk maakt. Voor veel organisaties betekent dat vandaag de dag BCDR. BCDR-oplossingen maken gebruik van back-up, snapshots, virtualisatie en de cloud om gegevens te beschermen en snel herstel mogelijk te maken.

Mythe 2: BCDR-leveranciers met alleen software zijn minder duur

Het is begrijpelijk waarom deze mythe bestaat, want producten die alleen software omvatten, hebben lagere initiële kosten in vergelijking met alles-in-een-oplossingen. Dat komt voor een groot deel omdat u ze kunt inzetten op elke hardware (bijv. goedkope, gangbare x86-servers) en publieke cloud. Als u echter kijkt naar de totale eigendomskosten (TCO), dan kunnen producten met alleen software op de lange termijn duurder zijn dan alles-in-een-oplossingen.

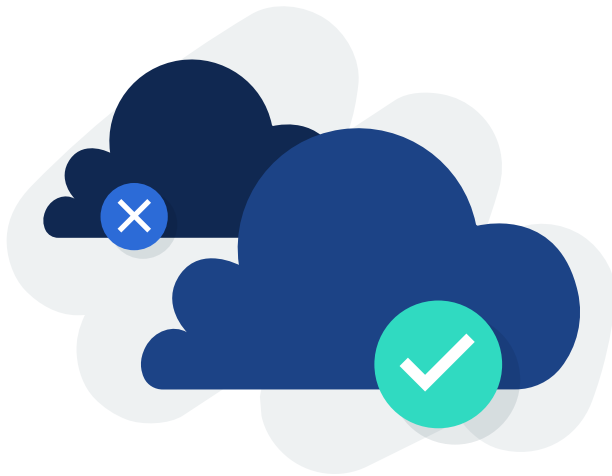
Met alles-in-een-oplossingen krijgt gebruiksgemak prioriteit. U krijgt één leverancier (en een maandelijks tarief) voor hardware, software en cloud. De technische ondersteuning

is ongecompliceerd, ongeacht waar het probleem zit. Ook heeft hardware de juiste maat voor klantimplementaties, waardoor handmatige arbeid, configuratiefouten en de bijbehorende kosten van elk worden verminderd. Alles-in-een-oplossingen kunnen zelfs hardwarevervanging en capaciteitsuitbreidingen omvatten, hetgeen de schaalbaarheid in de loop van de tijd vergemakkelijkt. Tot slot zijn er geen onverwachte cloudkosten, die u hieronder vindt.

Mythe 3: Alle clouds zijn hetzelfde

Ja, alle cloudbaanbieders bieden zeer beschikbare server- en opslaginfrastructuur aan. Dat betekent echter niet dat ze ook voor BCDR zijn gemaakt. De kosten van publieke cloud zijn in het beste geval onvoorspelbaar. Ja, u betaalt alleen voor wat u gebruikt, maar dat betekent dat de kosten pieken op het slechtst mogelijke moment – wanneer u een virtuele machine (VM) voor herstel gebruikt. Daarnaast brengen cloudbaanbieders egresskosten in rekening voor het verplaatsen van gegevens uit de cloud. Het downloaden van een grote dataset uit de cloud (bijv. om een server te herstellen) kan dus ook kostbaar zijn. Tot slot hebben sommige clouds verschillende niveaus voor rekencapaciteit, opslag en beveiliging, wat de complexiteit kan vergroten.

Bij sommige alles-in-een BCDR-oplossingen zijn de cloudkosten opgenomen in één maandelijks tarief. Dit kan een voordeel zijn voor MSP's, omdat het de kosten van OPEX voorspelbaar houdt. Het maakt het factureren van klanten voor BCDR-diensten eenvoudig en zorgt ervoor dat marges op diensten consistent blijven. Sommige aanbieders van alles-in-een-oplossingen bieden extra beveiligingsmaatregelen zoals tweeledige verificatie bij elke stap en geharde cloudapparaten. Andere bieden mogelijk onveranderlijkheid van gegevens en geautomatiseerde retentiemogelijkheden die organisaties helpen om te voldoen aan beveiligingsdoelstellingen en complianceregelgeving.



Ja, alle cloudbaanbieders bieden zeer beschikbare server- en opslaginfrastructuur aan. Dat betekent echter niet dat ze ook voor BCDR zijn gemaakt.

Mogelijk bent u ook geïnteresseerd in:



Mythe 4: Alle BCDR-oplossingen brengen hetzelfde risico met zich mee

Dit is gewoon niet waar. De hoeveelheid risico die u op zich neemt bij het leveren van BCDR-diensten kan sterk variëren, afhankelijk van de oplossing en de leverancier die u kiest. Nogmaals, laten we alles-in-een-oplossingen vergelijken met producten die alleen software omvatten.

Met producten die uitsluitend uit software bestaan, vertrouwt u op meerdere leveranciers voor hardware, software en cloud. Dit kan resulteren in meerdere zwakke punten en potentieel vingerwijzen door leveranciers, waardoor het langer duurt om problemen op te lossen. Wat nog erger is, als één leverancier een wijziging doorvoert, kan dit invloed hebben op de gehele oplossing. Een software-update kan bijvoorbeeld leiden tot alles van een kleine afname van de prestaties tot een dure hardware-upgrade.

Met alles-in-een-oplossingen krijgen MSP's ondersteuning van één enkele leverancier voor software, hardware en cloud. Dat betekent minder risico voor MSP's.

Evaluatie van BCDR- en DRaaS-oplossingen

Zoals u waarschijnlijk al heeft begrepen, is een van de grootste beslissingen of u kiest voor een alles-in-een BCDR-oplossing van één leverancier met cloud-DRaaS, of dat u uw eigen oplossing bouwt met behulp van producten van meerdere leveranciers. U moet ook overwegen waar de offsite reken- en opslagmiddelen zich zullen bevinden. Dat kan een zelf-gehoste cloud zijn, een publieke cloud of de cloud van een BCDR-leverancier. Ongeacht de aanpak hebben MSP's een complete toolkit nodig om BCDR te leveren aan klanten. Deze omvat:

Software

BCDR-software wordt gebruikt voor het automatiseren en beheren van back-up- en herstelprocessen. Na een eerste volledige serverback-up maakt BCDR-software

RPO/RTO

Recovery point objective (RPO) en recovery time objective (RTO) zijn belangrijke dingen om te overwegen. Deze maatstaven verwijzen respectievelijk naar een tijdstip waarnaar u kunt herstellen en hoe snel u een herstel kunt uitvoeren. Als het gaat om BCDR, RPO en RTO worden deze gedicteerd door de frequentie van back-ups, de hoeveelheid gegevens worden beschermd, de softwaremogelijkheden, de hardware- en/of cloudprestaties en de cloudbaanbieder die u kiest.



incrementele snapshots om herstelpunten of point-in-time serverimages te creëren. Herstelpunten worden gebruikt om primaire servergegevens te herstellen naar een specifiek punt in de tijd (d.w.z. voordat het mis ging). Ze kunnen ook worden gemount of "gevirtualiseerd" om serveractiviteiten te herstellen op een secundair apparaat of in de cloud. Dit proces staat bekend als failover.

De juiste BCDR-software maakt het volgende mogelijk:

- Lokale en cloudback-up
- Lokale en cloudfailover
- Herstelmogelijkheden die voldoen aan verschillende herstelscenario's*

**Herstelscenario's kunnen variëren van het herstellen van enkele verloren gegane bestanden tot een complete serverstoring. Zoek dus naar oplossingen die tegemoetkomen aan specifieke herstelbehoeften. Naast VM-failover moet een BCDR-oplossing mogelijkheden bieden zoals het herstellen van bestanden en mappen, het detecteren en terugdraaien van ransomware, het exporteren van serverimages en bare metal herstel.*

Cloud

Zoals hierboven genoemd, bevatten hedendaagse BCDR-oplossingen ook een cloudbackup- en herstelcomponent. In het geval dat zowel de primaire als de BCDR-hardware onbruikbaar wordt, kan een serverimage als VM in de cloud worden gemount.

Afhankelijk van de benadering die u kiest, kan de cloud het volgende zijn:

- Publieke cloud (u bouwt uw eigen oplossing)
- Zelf-gehoste cloud (u bouwt uw eigen oplossing)
- Cloud van BCDR-aanbieder (alles-in-een)

De cloud dient twee doelen voor BCDR. Ten eerste is het de offsite opslag voor tertiaire serverback-upimages die worden gebruikt voor herstel. Ten tweede kan een VM in de cloud worden gemount om de primaire serveractiviteiten over te nemen tijdens failover.

Cloudkosten en verborgen kosten

Het kiezen van een alles-in-een-oplossing of het bouwen van uw eigen oplossing met behulp van een publieke cloud heeft impact op de kosten, dus laten we elke oplossing eens bekijken:



In het geval dat zowel de primaire als de BCDR-hardware onbruikbaar wordt, kan een serverimage als VM in de cloud worden gemount.

Cloud van alles-in-een-leverancier	Publieke cloud
Eén voorspel maandelijks tarief voor cloudopslag en rekencapaciteit	De kosten van cloudreken capaciteit pieken tijdens rampenherstel
Voorspelbare cloudrekenprestaties tijdens rampenherstel	De cloudaanbieder biedt mogelijk geen prestatiegaranties/minima (of de kosten kunnen stijgen om aan de prestatiebehoeften te voldoen)
Geen extra kosten voor herstel naar de primaire server	De cloudaanbieder brengt egresskosten in rekening voor het verplaatsen van gegevens uit de cloud
Fysiek herstelapparaat dat binnen een dag wordt verzonden (belangrijk voor herstel van grote datasets)	Herstel naar de primaire server vindt plaats op internetsnelheid
Toegewijde technische ondersteuning tijdens rampenherstel, inclusief failover en failback	De MSP moet DR uitvoeren, inclusief potentieel complexe failback, zonder assistentie
Rijke beveiligingsfuncties waaronder beheertoegang en onveranderlijke back-upsnapshots die niet door ransomware kunnen worden geïnfecteerd	Een "gedeeld model" waarbij de verantwoordelijkheid voor gegevensbeveiliging bij de eigenaar van de gegevens ligt, niet bij de cloudaanbieder. Een voorbeeld is het AWS Shared Responsibility Model



Daarentegen maken alles-in-een-oplossingen het factureren eenvoudig, met één vast bedrag dat de kosten voor cloudopslag, rekencapaciteit en herstel omvat.

Zoals u kunt zien, variëren cloudkosten aanzienlijk, afhankelijk van de benadering die u kiest. Als MSP is dit een belangrijke overweging vanuit factureringsoogpunt. Als u bijvoorbeeld kiest voor een publieke cloud, bouwt u dan (geschatte) herstelkosten in uw maandelijkse tarieven voor klanten in? Of gaat u hen apart factureren voor herstelkosten? Het eerste zorgt voor een betere klantervaring, maar brengt risico met zich mee: wat gebeurt er als u de kosten onderschat? Het laatste beperkt het MSP-risico, maar kan leiden tot ontevreden klanten als de kosten oplopen.

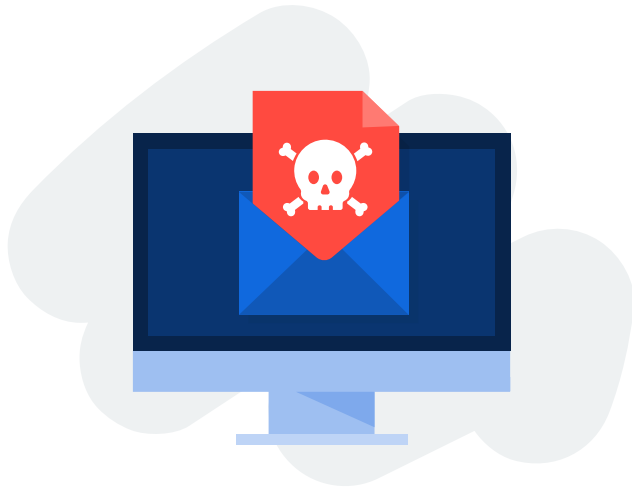
Daarentegen maken alles-in-een-oplossingen het factureren eenvoudig, met één vast bedrag dat de kosten voor cloudopslag, rekencapaciteit en herstel omvat. Dit zorgt voor een ongecompliceerde klantervaring en zorgt voor voorspelbare marges op geleverde diensten.

Hardware

BCDR-hardware dient een aantal doelen. Ten eerste voert deze de BCDR-software uit. Ten tweede levert deze de opslag voor serverback-upimages die worden gebruikt voor herstel. Ten derde stuurt deze serverimages naar de cloud voor rampenherstel. Tot slot neemt deze de primaire server over tijdens een lokale failover, waardoor de bedrijfsactiviteiten kunnen doorgaan terwijl de primaire server wordt hersteld.

Vandaag de dag wordt met BCDR-hardware gewoonlijk een secundaire server op locatie bedoeld met:

- Voldoende verwerkingskracht om de normale serveractiviteiten uit te voeren, en
- Voldoende opslagcapaciteit om herstelpunten gedurende een bepaalde periode (bijv. 90 dagen) te bewaren.



Bedreigingsactoren richten zich in ransomwareaanvallen steeds meer op back-ups om de mogelijkheid te elimineren om eenvoudig te herstellen zonder losgeld te betalen. MSP's hebben dus een BCDR-oplossing nodig die aan deze zorgen tegemoet komt.

BCDR-hardware kan een gangbare X86-server zijn of het kan een speciaal BCDR-apparaat zijn. Met oplossingen die alleen uit software bestaan, zet u uiteraard de software van de BCDR-leverancier in op een x86-server. Aan de andere kant kunnen alles-in-een-oplossingen worden geleverd met BCDR-software voorgeïnstalleerd op een apparaat of alleen als software.

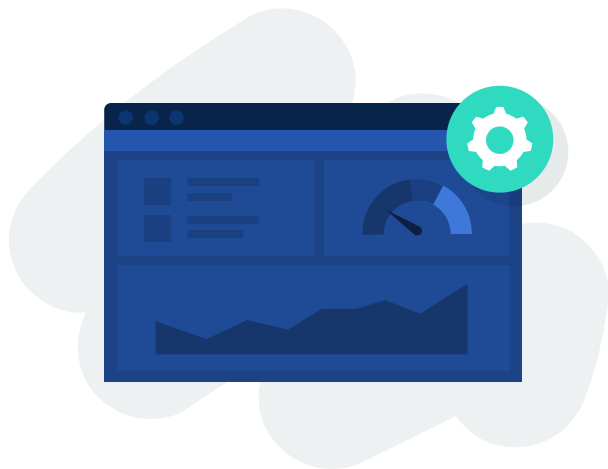
Het inzetten van een speciaal BCDR-apparaat kan een voordeel zijn voor MSP's. Software en hardware kunnen worden geoptimaliseerd om samen te werken en de leverancier kan het apparaat configureren en aanpassen aan de specifieke behoeften van de klant. Als u echter de ervaring van een alles-in-een-leverancier wilt, maar liever uw eigen hardware kiest, dan is dat ook een optie zoek – naar BCDR-leveranciers die een flexibele inzetbaarheid mogelijk maken.

Als bedrijven sommige of alle werklusten van de primaire server naar de cloud verplaatsen, kunnen lokale BCDR-hardwarebehoeften veranderen of overbodig worden. Echter, hoewel onze jaarlijkse State of the MSP-enquête aangeeft dat de cloudadoptie toeneemt, is lokale hardware vooralsnog de norm.

Beveiliging en compliance

Veel MSP's bedienen klanten in sectoren waar de eisen met betrekking tot beveiliging en compliance aanzienlijk zijn. Bovendien richten bedreigingsactoren zich in ransomwareaanvallen steeds meer op back-ups om de mogelijkheid te elimineren om eenvoudig te herstellen zonder losgeld te betalen. MSP's hebben dus een BCDR-oplossing nodig die aan deze zorgen tegemoet komt. Mogelijkheden voor ransomwaredetectie en point-in-time rollback zijn een must. De onveranderlijkheid van gegevens is een andere belangrijke overweging.

Onveranderlijkheid van gegevens betekent dat gegevens worden opgeslagen op een manier die niet kan worden gewijzigd door externe handelingen. Dat zorgt ervoor dat back-ups niet kunnen worden beschadigd door ransomware of worden verwijderd in



Zoek naar producten die integreren met essentiële tools waarop u vertrouwt, zoals RMM-software (Remote Monitoring and Management) en PSA-software (Professional Services Automation).

een andere aanvalsvorm. Het kan sommige organisaties ook helpen om te voldoen aan specifieke compliancienormen waarvoor gegevens moeten worden gearchiveerd. Zoek naar BCDR-oplossingen die onveranderlijkheid van gegevens bieden, gegevens opslaan in overeenstemming met de rapportagenormen van Service Organization Control (SOC 1 / SSAE 16 en SOC 2 Type II) en overal verplichte tweeledige verificatie hebben.

Oplossingen die geautomatiseerd, beleidsmatig retentiebeheer mogelijk maken om aan compliancienormen te voldoen kunnen de noodzaak voor handmatig ingrijpen beperken; ze stroomlijnen het management en zorgen ervoor dat klantgegevens voor de juiste duur worden opgeslagen in de cloud.

Gebruiksgemak / beheer

Gebruiksgemak is van kritiek belang voor MSP's. Met een grotere efficiëntie kunnen de marges op de geleverde diensten worden vergroot. Daarom moet het vinden van een product dat gemakkelijk is in te zetten en beheren als iets van wezenlijk belang worden gezien. Zoek naar BCDR-producten die specifiek voor MSP's zijn ontworpen. Dat kan betekenen: gestroomlijnd inwerken, beheer van meerdere huurders, een scala aan inzetmogelijkheden, end-to-end beveiliging en een flexibel retentiebeleid.

Zoek naar producten die integreren met essentiële tools waarop u vertrouwt, zoals RMM-software (Remote Monitoring and Management) en PSA-software (Professional Services Automation). Integraties kunnen uw vermogen om BCDR-diensten efficiënt te leveren vergroten door het aantal stappen te verminderen dat nodig is om gemeenschappelijke taken uit te voeren.

Zoals we al eerder hebben besproken, kunt u overwegen of u kiest voor een alles-in-een-oplossing die door één leverancier wordt ondersteund of dat u uw eigen oplossing bouwt. Softwarematige BCDR-producten zijn niet noodzakelijkerwijs moeilijker te beheren, maar het oplossen van problemen kan moeilijker zijn als u met meerdere leveranciers te maken heeft.



Oplossingen die de efficiëntie verbeteren, verhogen ook de marge en de omzet, omdat ze minder handmatige tussenkomst vereisen om te implementeren en beheren.

Winstgevendheid

Geen enkele discussie over productevaluatie voor MSP's is compleet zonder aan winstgevendheid te denken. Ga op zoek naar producten die de eigenschappen en functionaliteit hebben die u nodig heeft, voor een prijs die u in staat stelt de marges op uw diensten te vergroten. Bij het evalueren van oplossingen is het essentieel om de totale eigendomskosten in aanmerking te nemen in plaats van alleen de software- en hardwarekosten, zoals we hierboven uiteen hebben gezet.

Oplossingen die de efficiëntie verbeteren, verhogen ook de marge en de omzet, omdat ze minder handmatige tussenkomst vereisen om te implementeren en beheren. Zoek naar oplossingen die speciaal voor MSP's zijn ontworpen en die een combinatie zijn van efficiënte, betrouwbare technologie, beheer van meerdere huurders en integratie met andere tools waarop u vertrouwt.

Dit type oplossing kan u in staat stellen om meer klanten te ondersteunen en uw bedrijf te laten groeien. U hoeft geen tijd te verspillen aan lastige configuraties, doorlopend beheer en het oplossen van problemen. Dit bespaart technici tijd en verlaagt de OPEX-kosten, waardoor de marges en de inkomsten toenemen.

Mogelijk bent u ook geïnteresseerd in:



Datto Continuity (BCDR)

Datto Continuity is een complete BCDR-oplossing die uitgebreide back-up- en herstelmogelijkheden biedt voor fysieke en virtuele servers. Ingezet als een fysiek apparaat, als software geïnstalleerd op een virtuele machine, of als image op uw eigen hardware biedt Datto Continuity back-up, herstel en failover, zowel lokaal als in de cloud, tegen een vast maandelijks bedrag. Er zijn geen verborgen kosten of onvoorspelbare cloudkosten.

MSP's hoeven zich geen zorgen dat zij of hun klanten worden aangevallen. De oplossing biedt end-to-end beveiliging met de onwrikbare Datto Cloud, AES 256-encryptie tijdens bedrijf en optioneel in rust, Cloud Deletion Defense om back-ups te beschermen, geharde apparaten en overal tweeledige verificatie.

Gepatenteerde Inverse Chain-technologie betekent dat back-ups bestand zijn tegen ransomware en dat alle back-ups automatisch worden gescand om te controleren of de serverimages volledig, vrij van ransomware en opstartbaar zijn. Datto Continuity beschermt tegen permanent gegevensverlies en stelt MSP's in staat om de gegevens van klanten eenvoudig te herstellen na een aanval met ransomware met behulp van granulaire point-in-time back-ups.

Zoals u weet, draait het bij winstgevende managed services volledig om hogere efficiëntie en maximalisering van rendement op dienstverlening. Met één enkel deelvenster krijgt u een compleet overzicht in back-ups van klanten wat opnieuw de efficiëntie verhoogt.

Mogelijk bent u ook geïnteresseerd in:



Datto SIRIS-gegevensblad →



Datto Cloud-gegevensblad →

DEMO AANVRAGEN

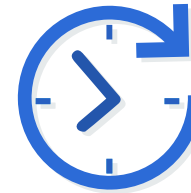
Datto Continuity biedt:

- Inverse Chain: gepatenteerde back-ups bestand tegen ransomware
- Onmiddellijk herstel
- Cloud van wereldklasse
- End-to-end beveiliging
- Oneindige schaalbaarheid
- Oneindige retentie
- 24/7/365 ondersteuning in de VS
- Onbeperkt aantal back-upagenten
- Onbeperkte cloudopslag
- Vaste prijs
- Flexibele inzetbaarheid
- Veilig cloudbeheer voor meerdere huurders

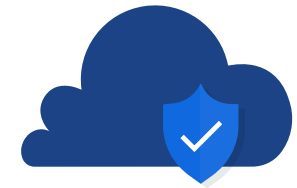
Datto Continuity in cijfers:



Miljarden back-ups



Tienduizenden herstelacties



Cloud op exabyteschaal

Bezoek vandaag nog datto.com voor meer informatie over Datto Continuity.