

Achtergrondartikel

# Schijfgebaseerde back-ups: een kerncomponent van moderne gegevensbescherming



De Silent Brick is een transporteerbare gegevensdrager voor het Silent Brick systeem, die 12 harde schijven bevat

Diverse technologieën voor gegevensbescherming zijn al herhaaldelijk doodverklaard. Naast de eeuwige kandidaat hiervoor, tape, zou ook de harde schijf geen lang leven zijn beschoren. Flash-opslag zou alles vervangen en schijfgebaseerde back-ups behoorden voorgoed tot het

verleden. De realiteit ziet er echter heel anders uit. Schijfgebaseerde back-ups winnen juist aan relevantie. Ze leveren een veel sterkere bijdrage aan het reduceren van de kosten en overhead van flash-opslag en 'last line of defense'-technologieën.

## Nieuwe complexiteit rond gegevensbescherming

Als gevolg van de toenemende gevaren rond ransomware en andere cyberbedreigingen is de focus verschoven van klassieke back-ups naar oplossingen voor databescherming die voorzien in snel en betrouwbaar gegevensherstel. In plaats van traditionele back-ups voor uiterste noodgevallen zijn nu de Recovery Time Objective (RTO) en Recovery Point Objective (RPO) bepalend voor het gegevensherstel. Voor het optimaliseren van deze parameters moet de back-upstrategie zowel aan het meest nabije als verafgelegen uiteinde van de storage-keten worden uitgebreid met aanvullende technologieën. En daarmee neemt de opslagcomplexiteit verder toe<sup>1</sup>. Naast klassieke schijfgebaseerde back-ups zorgen flash-gebaseerde back-ups ervoor dat moderne technologieën zoals continuous data protection (CDP), forever incrementals en InstantRecovery® aan een lagere RTO kunnen bijdragen. Vanwege de almaar groeiende datavolumes en hoge overhead die gepaard gaat met het herstel van gegevens uit incrementele back-ups zijn flash-gebaseerde storage-systemen hiervoor onmisbaar. Ook back-ups

naar (virtuele) tape maken onverwachts een opmars, zij het onder een nieuwe naam: air gapping. Fysiek uit het opslagsysteem verwijderbare gegevensdragers worden gezien als geheim wapen tegen de gevolgen van ransomware-aanvallen. Dat komt omdat zij voor de volle honderd procent tegen manipulatie door onbevoegden zijn beschermd. Voor de kostenefficiënte opslag van grote datavolumes (zoals bij archiefopslag) moet gebruik worden gemaakt van online opslagsystemen waarbinnen back-ups tegen onbevoegde wijzigingen worden beschermd volgens het principe van immutability.





Air gapping wordt in één adem genoemd met tape. Silent Bricks vertegenwoordigen echter moderne, op schijven of SSD's gebaseerde gegevensdragers die eveneens voor offline gebruik inzetbaar zijn.

## Vertrouw niet louter op air gapping en immutability

Er zijn diverse technieken die het mogelijk maken om gegevens tegen onbevoegde toegang en manipulatie te beschermen. De bekendste hiervan is air gapping, dat vaak in één adem wordt genoemd met tape, maar ook prima kan worden gerealiseerd met transporteerbare gegevensdragers zoals de Silent Brick. Om te waarborgen dat air gapping werkelijk volledige bescherming biedt moeten deze gegevensdragers van het opslagsysteem worden losgekoppeld of daaruit worden verwijderd. Het opnieuw toevoegen daarvan aan het opslagsysteem mag alleen handmatig gebeuren. Er bestaat namelijk bij geautomatiseerde toegang

principeel de kans dat deze door kwaadwillende personen wordt misbruikt. Met het oog op de voortdurend groeiende datavolumes en de komst van zero admin-benaderingen die voorzien in beheer zonder menselijke tussenkomst is het echter wenselijk om het aantal handmatige ingrepen zoveel mogelijk terug te dringen. En dat weersprekt het basisbeginsel om regelmatig air-gapped back-ups te maken. Bij tape-archieven komt er nog een extra nadeel kijken: er is alleen maar lineaire toegang tot data mogelijk. Het herstel van afzonderlijke bestanden is praktisch gezien geen haalbare kaart.

Ondertussen wordt het principe van immutability ook voor externe servers in de cloud als een mogelijk alternatief voor air gapping beschouwd. In het geval van een succesvolle ransomware-aanval levert dit echter problemen op. Want in dat geval is de eerste en voornaamste maatregel om de interne IT-systemen volledig los te koppelen van het internet. De toegang is dan pas weer mogelijk als de interne systemen volledig zijn opgeschoond en de IT-afdeling zich ervan heeft verzekerd dat er geen nieuwe problemen kunnen ontstaan wanneer gegevens uit de back-ups in de cloud worden hersteld. Hoewel storage-as-a-service als een kostenefficiënte oplossing wordt aangemerkt, kan het herstellen van grote datavolumes een hoop tijd in beslag nemen en vaak ook behoorlijk in de papieren lopen. In het geval van online archieven wordt het leeuwendeel van de kosten meestal gemaakt door het opvragen van data. En hoe sneller de gegevens beschikbaar moeten worden gesteld, hoe hoger de kosten. Bovendien blijven er aan softwarematige beveiligingsmechanismen zoals immutability risico's kleven. Elke beveiligingsmaatregel die door gebruikers met speciale rechten ongedaan kan worden gemaakt is in beginsel niet honderd procent veilig.



Het concept van immutability is afkomstig uit de programmeerwereld, waarin 'immutable data' onveranderlijke waarden vertegenwoordigen. Een van de belangrijkste voordelen van deze permanente waarden is de mogelijkheid om daarnaar te verwijzen in plaats van er kopieën of nieuwe instances van te maken, aangezien ze nooit kunnen worden gewijzigd. Op het gebied van gegevensopslag wordt immutability vaak gelijkgesteld aan object lock, een softwarefunctie van het S3-protocol die het mogelijk maakt om gegevensobjecten tijdelijk te vergrendelen, zodat ze niet kunnen worden gewijzigd of verwijderd. Een object lock-procedure omvat verschillende stadia waarvan sommige stappen alleen kunnen worden herroepen op basis van het vier-ogenprincipe. Meer informatie over het vergrendelen van objecten is te vinden in een blog van Backblaze op <https://www.backblaze.com/blog/five-ways-to-use-object-lock-immutability/>



De Silent Cube (links) en Silent Cube DS (rechts) zijn speciale systemen voor de revisiebestendige opslag van archieven die gegevens op basis van hardwarematige WORM-beveiliging beschermen.

Een hardwarematig vergrendeld archief met write once, read many (WORM)-functionaliteit archief is daarentegen wél volkomen veilig. De scheiding tussen operationele data en archiefgegevens moet evenwel vóór het back-upproces worden aangebracht. Het terugdringen van de hoeveelheid gegevens waarvan een back-up moet worden gemaakt, het verkorten van de back-uptijden en het uiterst veilige ontwerp van een dergelijk archief tillen de beveiliging naar nieuwe hoogten uit. Bij onwijzigbare opslag moet wel rekening worden gehouden met de eisen van de GDPR. Zo moet het mogelijk blijven voor het inwilligen van verzoeken van gebruikers om hun persoonsgegevens te laten wissen.

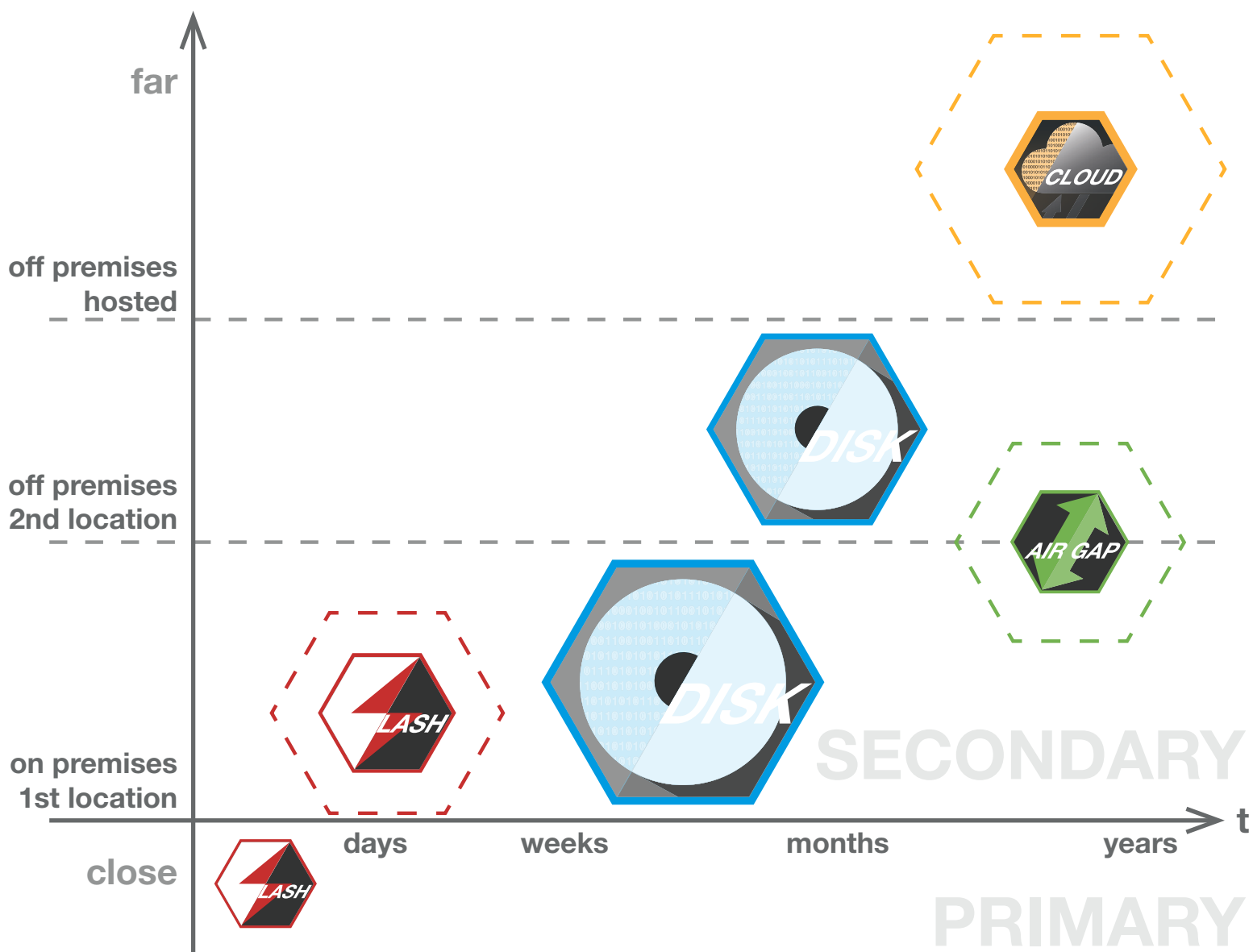
Deze technieken worden niet voor niets als 'last line of defense' aangemerkt, oftewel als laatste mogelijkheid voor het herstellen van verwijderde of ontoegankelijke data. Omdat downtime van IT-systemen bij succesvolle ransomware-aanvallen de grootste kostenpost vertegenwoordigt<sup>2</sup>, helpen deze beperkt toegankelijke archieven nauwelijks om de gevolgen van dergelijke aanvallen te verzachten. Ze zouden in de praktijk alleen als laatste redmiddel moeten worden gezien als alle andere data verloren is gegaan.

# De sleutelrol die schijfgebaseerde back-ups vervullen

Schijfgebaseerde back-ups hebben al decennia hun waarde bewezen als middel om gegevens snel te beschermen en opnieuw op te vragen. Maar vanwege de sterk toegenomen datavolumes is conventionele RAID-opslag niet langer toereikend. Deze biedt onvoldoende schaalbaarheid. En door het gebruik van grote aantallen schijven die uit dezelfde productiebatch afkomstig zijn, bestaat ook het gevaar van gecorreleerde storingen, ook wel epidemische uitval genoemd. Moderne disk arrays moeten vrijwel onbeperkt kunnen worden opgeschaald zonder de noodzaak van configuratiewijzigingen (scale up). Daarbij moet het van meet af aan mogelijk zijn om gebruik te maken van verschillende standaard gegevensdragers om gecorreleerde storingen te voorkomen.

Het reduceren van de hoeveelheid gegevens in de arbeidsintensieve laatste instance (air gapping/online archief) is alleen mogelijk als er bij schijfgebaseerde back-ups ingrijpende maatregelen worden getroffen om bescherming te bieden tegen storingen en cyberaanvallen. Er is namelijk sprake van een groeiende kans op gerichte cyberaanvallen waarbij hackers eerst de IT-omgeving verkennen om in een later stadium (vaak pas na maanden) back-ups onklaar te maken alvorens tot een aanval over te gaan<sup>3</sup>. Als zij daarin slagen, zal er een beroep moeten worden gedaan op de last line of defense. En dat zal ten koste gaan van de actualiteit van de data en de snelheid van het herstelproces.

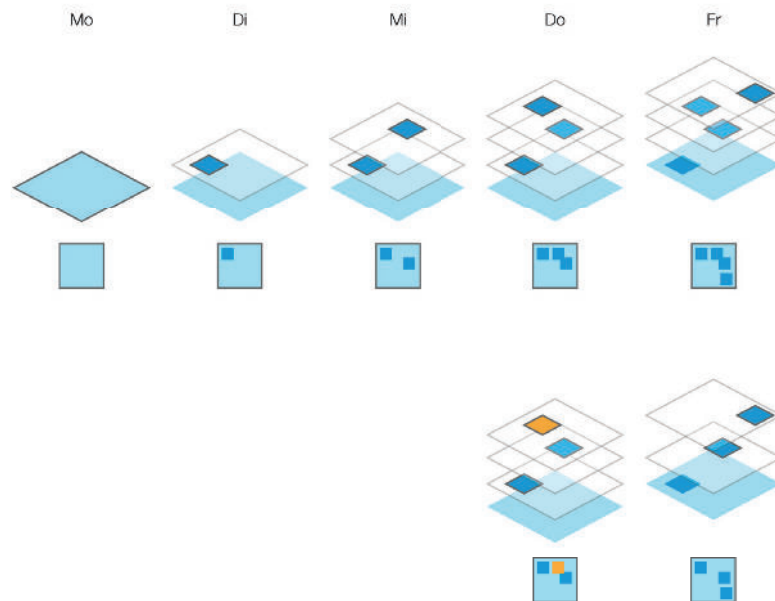
Om dit te voorkomen kunnen er verschillende maatregelen worden genomen voor het beschermen van schijfgebaseerde back-ups.



Schijfgebaseerde back-ups vormen een kerncomponent van gegevensbescherming. Met behoud van dezelfde mate van beveiliging kan voor een reductie worden gezorgd van kostbare flash-opslag en arbeidsintensieve air gapping-technieken.

# 1. De toegang bemoeilijken

Netwerkbeheerders en managers hebben maar al te vaak toegang tot back-upservers. Meestal is dit te wijten aan de integratie met standaardauthenticatie op basis van Active Directory (AD). Dit is de meest voorkomende kwetsbaarheid in de beveiliging. NAS-systemen die voor de opslag van back-ups worden gebruikt mogen niet direct als stations worden toegewezen. Ze mogen alleen toegankelijk zijn via beveiligde UNC-paden. De toegang tot alle back-upsystemen mag niet via Active Directory verlopen, maar moet op basis van multi-factorauthenticatie worden beschermd. Het valt sterk aan te raden om een zero trust-strategie toe te passen om aanvallen door insiders of via gekaapte accounts te voorkomen. De root-toegang tot bedrijfskritische servers en NAS-systemen moet volledig worden geblokkeerd of zoveel mogelijk worden bemoeilijkt dan wel beveiligd.



Continuous Snapshots zorgen er in het Silent Brick System voor dat alle wijzigingen - ook ongewenste verwijderingen - ongedaan kunnen worden gemaakt.

## **2. Automatische, voor onbevoegden**

### **ontoegankelijke snapshots**

Het back-upstelsysteem moet met regelmatige intervallen automatisch snapshots maken die pas na het verstrijken van de ingestelde bewaartermijn kunnen worden gewist. Het mag niet mogelijk zijn om die bewaartermijn te wijzigen via standaardaccounts. Dit moet met multi-factorauthenticatie worden beveiligd. De regelmaat van snapshots en de bewaartermijn moeten zodanig worden geconfigureerd dat ze optimale beveiliging bieden in combinatie met acceptabele overhead. Omdat cybercriminelen zich vaak wekenlang binnen IT-systemen ophouden valt het sterk aan te raden om voor een lange bewaartermijn te kiezen.

## **3. Georedundantie**

Om bescherming te bieden tegen de uitval van complete installaties of locaties moeten back-ups indien mogelijk naar een tweede locatie worden gerepliceerd, en het liefst op basis van in het opslagsysteem geïntegreerde functies die niet via het reguliere netwerk toegankelijk zijn (zie hierboven). De opslag op de secundaire locatie mag niet vanuit het hoofdnetwerk toegankelijk zijn, tenzij dit voor replicatiedoeleinden nodig is.

## **4. Testen, testen en nog eens testen**

Zowel de inspectie van back-ups onder de quarantaineomstandigheden waarvan sprake is na een succesvolle cyberaanval als de herstelprocedures moeten regelmatig worden geverifieerd en gedocumenteerd. Het is ook belangrijk om single points of failure te identificeren die het gegevensherstel in de weg zouden kunnen zitten. Dan valt onder meer te denken aan een storing van switches of routers. Voor dergelijke componenten moeten simulaties van downtime-scenario's worden uitgevoerd en moeten de configuraties worden aangepast.

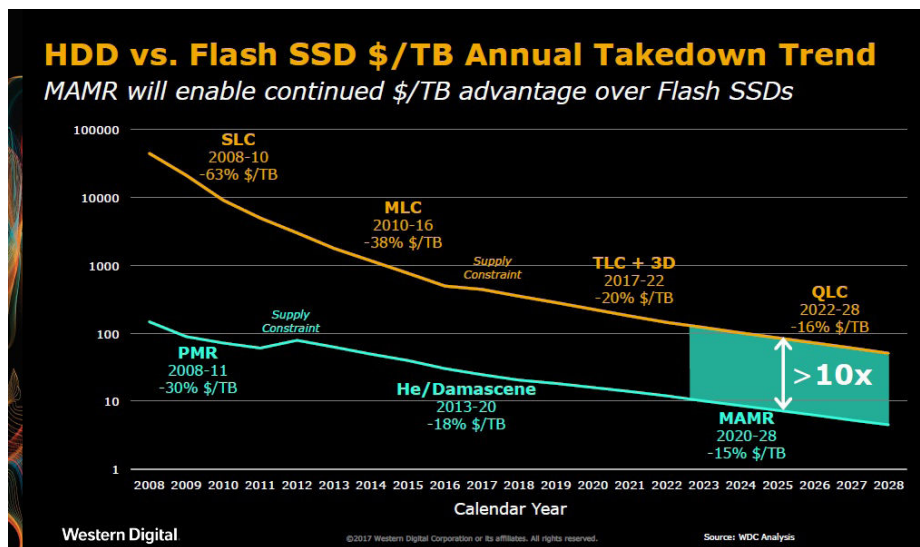
Omdat het voor het optimaliseren van de RTO (een zo snel mogelijk herstel) nodig is om back-ups daar te maken waar de gegevens aanwezig zijn resp. weer nodig zijn, moet deze centrale back-upomgeving on premises, oftewel op locatie worden ingericht.

# Kan dat niet met flash-opslag

## worden geregeld?

Flash-opslag is snel, maar ook kostbaar, en nog altijd een stuk duurder dan schijfgebaseerde opslag. Flash is inmiddels uitgegroeid tot de norm als het om primaire opslag gaat. In gevallen waarin sprake is van beperkte capaciteit weegt het snelheidsvoordeel zwaarder dan de hoge kosten.

Dit ziet er echter heel anders uit als er sprake is van de hierboven beschreven beveiligingsmaatregelen. Als die ook worden toegepast op de primaire opslag (het flash-systeem), vallen de kosten ettelijke malen hoger uit dan die voor schijfgebaseerde opslag. Als gevolg van de langere opslagtermijn en de daarvoor benodigde capaciteit staan de kosten niet langer in verhouding tot het realiseerbare snelheidsvoordeel. In plaats van afzonderlijke flash-opslag aan te schaffen voor de primaire back-up bestemming en daarmee de opslagcomplexiteit verder te vergroten is het eventueel mogelijk om een gedeelte van de reeds aanwezige primaire opslagcapaciteit toe te wijzen. Als de oplossing voor secundaire opslag op flexibele wijze met schijven en flash-opslag kan worden ingericht, kan dit ook direct in de omgeving voor de opslag van back-ups gebeuren, mits die daarop is ingericht. Het ligt voor de hand dat er met het oog op de kosten van flash-opslag voor een zo klein mogelijk gedeelte wordt gekozen. Er is een nauwgezette analyse van de RTO-strategie nodig om de juiste omvang van de flash-opslag te bepalen. In tegenstelling tot schijfgebaseerde back-ups is er bij flash-systemen meestal geen sprake van speciale maatregelen voor beveiliging tegen manipulatie of verwijdering (snapshots). Er mag echter niet worden afgestapt van redundante bescherming tegen de uitval van afzonderlijke gegevensdragers en de mogelijkheid van probleemloze capaciteitsuitbreiding.



Bij veel kostenprognoses wordt niet bedacht dat ook de harddisktechnologie steeds verder ontwikkelt. De fabrikant Western Digital is overtuigd dat flash-storage ook in de toekomst ongeveer 10x duurder zal zijn dan harde schijven.

## Samenvatting: investeer in een veilige oplossing voor schijfgebaseerde back-ups

Flash-opslag is onmisbaar als primaire storage instance en dient voor het realiseren van de beoogde RTO. Air gapping en online archieven kunnen in het uiterste noodgeval worden gebruikt als last line of defense, maar zijn vaak moeilijk toegankelijk en vertragen daarmee het herstelproces.

Schijfgebaseerde back-ups vertegenwoordigen het beste compromis tussen de opslagkosten, opslagprestaties en beveiliging. Hoe veiliger en uitgebreider de centrale omgeving voor schijfgebaseerde back-ups, hoe minder flash-opslag en air gapping of online storage er nodig is. Dit draagt bij aan een reductie van de kosten en handmatige overhead zonder nadelige gevolgen voor de RTO en RPO. Omdat cyberaanvallen hun pijlen tegenwoordig speciaal op de back-upinfrastructuur richten moeten schijfgebaseerde back-ups niet alleen tegen de uitval van gegevensdragers worden beschermd, maar ook tegen deze gerichte aanvallen. Dat is onder meer mogelijk op basis van zero trust, continuous snapshots en georedundantie.

Het Silent Brick System is een integrale storage-oplossing voor gegevensbescherming. Het combineert flashgeheugen, air gapping en S3 compatibele object storage. Maar ook bij dit systeem ligt de primaire focus op schijfgebaseerde back-ups, die met meervoudige redundantie, continuus snapshots en replicatie effectieve bescherming bieden tegen manipulatie en gegevensverlies.

