FAST LTA

Whitepaper

Immutable storage

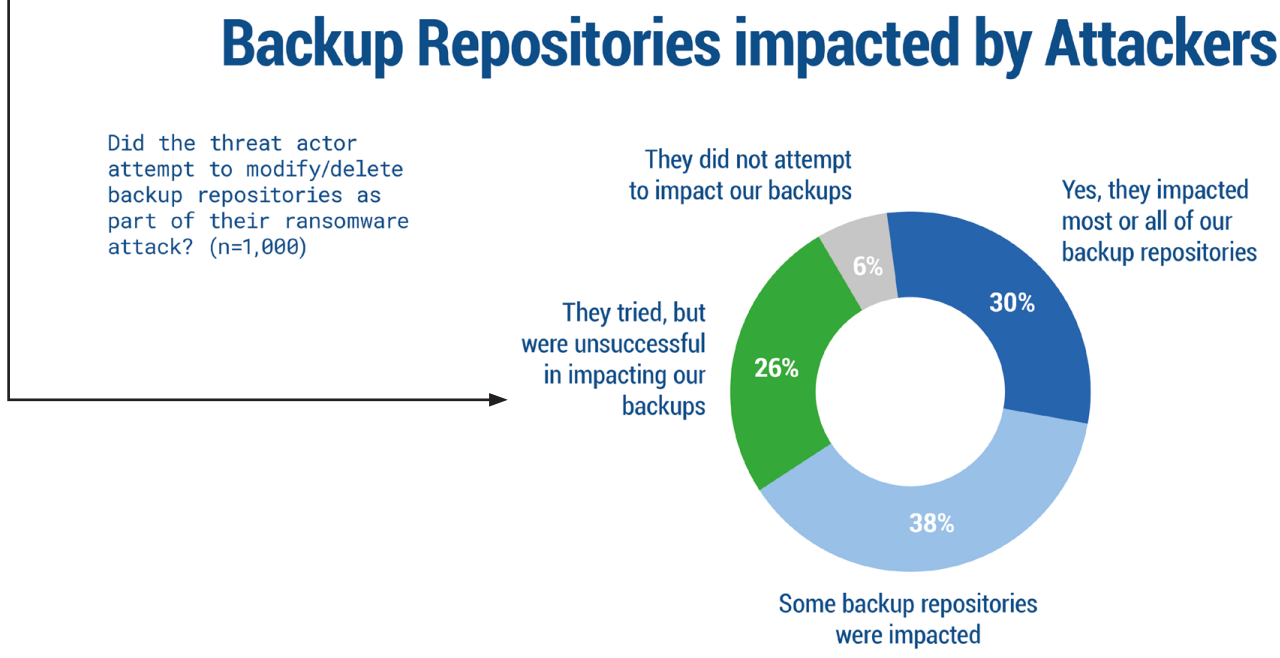
Moderne cyberaanvallen vragen om krachtiger beveiliging van data en back-ups. Dat is de reden waarom immutable storage (onwijzigbare opslag) momenteel in zwang is. Immutability is echter geen nieuw fenomeen. Wie zich de cassettebandjes van vroeger herinnert, weet nog dat het mogelijk was om het overschrijven van geluidsopnamen te verhinderen door een lipje aan de bovenkant van het cassettebandje te verwijderen. Het nieuwe aan immutability is de toepassing hiervan op het gebied van object stores. Daarbij worden objecten voor een bepaalde duur tegen overschrijven beveiligd met techniek die object locking wordt genoemd. Automatische snapshots, WORM-beveiliging en air gapping zijn andere methoden die het mogelijk maken om gegevens in onwijzigbare vorm op te slaan om ze te beschermen tegen onbevoegde of onopzettelijke verwijdering en knoeipogingen. Hoe gaat dit nu precies in zijn werk?

Cassettebandjes boden een mechanisch immutability-mechanisme: na de verwijdering van een lipje aan de bovenzijde was overschrijven niet langer mogelijk.

Versie: august 2022

Back-ups lopen groot risico

Alle nationale cybersecurity centra raden organisaties aan om gebruik te maken van back-ups om zich in te dekken tegen de gevolgen van cyberaanvallen met onder meer ransomware. Het is echter niet langer voldoende om die bescherming volledig te baseren op de beproefde back-upstrategie op basis van de 3-2-1-regel. Volgens een onderzoeksrapport van Veeam is ruim 90% van alle cyberaanvallen inmiddels op back-ups gericht. En bijna 70% van deze aanvallen is succesvol. Dat wil zeggen dat het cybercriminelen lukt om back-ups volledig of gedeeltelijk te versleutelen en daarmee onbruikbaar te maken. Nog geen kwart van deze aanvallen kon volledig worden voorkomen. Om met de woorden van Veeam te spreken: "**Daarom zijn air gapping en immutability zo belangrijk**."



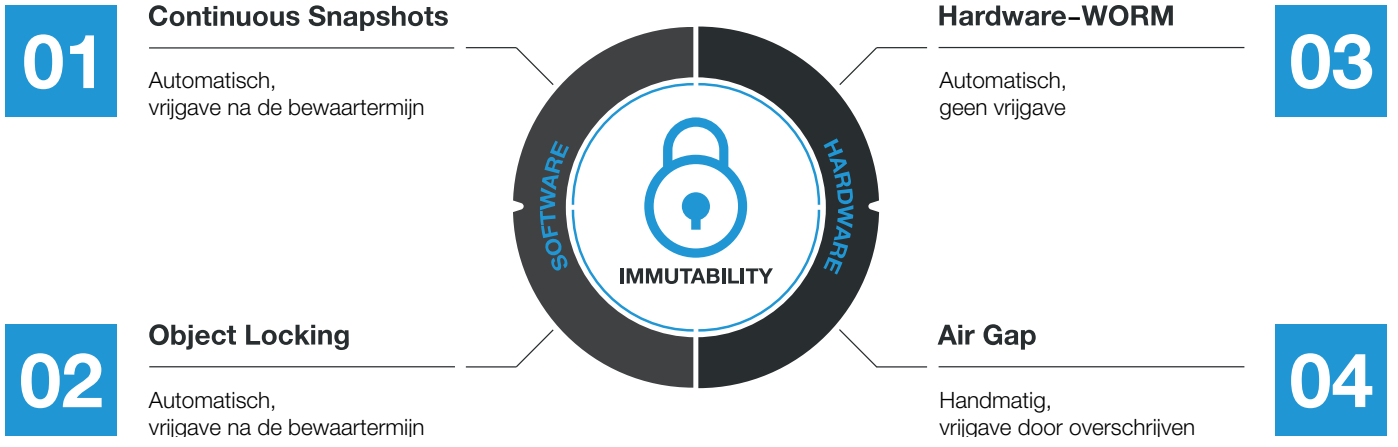
94% van alle cyberaanvallen was (mede) gericht op back-ups. 68% was ten minste gedeeltelijk succesvol.

Bron: Veeam

Immutability

Immutability betekent letterlijk onwijzigbaarheid. Zodra gegevens eenmaal zijn weggeschreven kunnen ze niet langer worden gewijzigd of gewist. Daarvoor hoeft echter geen gebruik te worden gemaakt van low-level schrijfbeveiliging, zoals in het geval van hardwarematige WORM-beveiliging. Immutability kan op diverse manieren worden gerealiseerd. En alle methoden hebben één ding met elkaar gemeen: **'immutable' data kan niet fysiek of door middel van programmeren door cybercriminelen worden gemanipuleerd of gewist, of is zelfs totaal onbereikbaar voor hen.**

Daarbij kunnen de volgende methoden worden onderscheiden. Elk daarvan kan effectief worden ingezet op verschillende punten in het proces voor databescherming, desgewenst in combinatie.



Automatische snapshots en S3 object locking:

Softwarematige WORM-beveiliging

WORM – Write Once Read Many, oftewel één keer schrijven, meerdere keren lezen, verwijst naar de bescherming van een object, bestand, map of gegevensdrager tegen verwijdering. Er zijn verschillende manieren om dit te realiseren. Een eenvoudige, maar niet echt veilige manier is om een bestand te beschermen met een read only-kenmerk. **Al naargelang hun toegangsrechten kunnen gebruikers deze beveiliging eenvoudig ongedaan maken**; voor gebruikers met beheerdersrechten is dat een fluitje van een cent. Daarmee is een read only-kenmerk op zichzelf ongeschikt als beschermingsmechanisme tegen cyberaanvallen. Desondanks maken alle softwarematige methoden voor WORM-beveiliging gebruik van een vergelijkbaar principe.

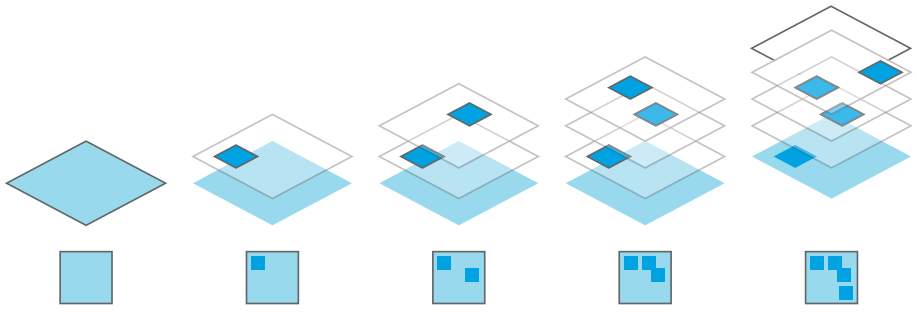
Om werkelijke bescherming te bieden zijn er twee aanpassingen van deze soft-WORM-functionaliteit nodig. De eerste maatregel is om objecten die onwijzigbaar moeten worden gemaakt (zoals bij automatische snapshots of een object lock) **automatisch af te scheiden van de systeemlogica**, zodat ze niet door de gebruikers of beheerders van het systeem kunnen worden gewist. De tweede maatregel is om een **retention period (bewaartermijn)** in te stellen. Na deze termijn kan de beveiliging handmatig worden opgeheven of automatisch worden verwijderd.

01

Continuous Snapshots

Automatisch,
vrijgave na de bewaartermijn

Continuous Snapshots functioneren als een tijdmachine. Met elke (in dit voorbeeld dagelijkse) snapshot worden de wijzigingen ten opzichte van de voorgaande snapshot opgeslagen. Indien nodig kan elke toestand die in de snapshot is opgeslagen, worden hersteld.



Het belangrijkste verschil tussen **automatische snapshots** met een retention period en object locking met een retention period is het tijdstip waarop de beveiliging wordt geactiveerd. Automatische snapshots worden beheerd door het storage-systeem. **Er worden nieuwe snapshots van de opslagtoestand gemaakt** zodra er wijzigingen (inclusief verwijderingen) plaatsvinden. Elke snapshot vraagt uiteraard om aanvullende opslagcapaciteit. Automatische snapshots maken het mogelijk om als het ware in de tijd terug te gaan en voor een bepaalde periode elke wijziging van de gegevens tot in detail ongedaan te maken. Hoe “dichterbij” een te beschermen dataset bij het tijdstip van de aanmaak en het gebruik van gegevens ligt, hoe nuttiger zijn snapshots, omdat de gegevens in kwestie op dat moment nog vaak werden gewijzigd en (opzettelijk) gewist.

Verder weg liggende beschermde datasets hebben betrekking op gegevens die zelden of nooit meer worden gewijzigd en absoluut niet meer gewist mogen worden. Voor deze datasets wordt vaak gebruikgemaakt van **object stores** die van nature veel minder opslagruimte vereisen. Na de eerste kopie worden er immers alleen nog maar wijzigingen (incrementals) opgeslagen. Object stores bieden daarnaast het voordeel dat ze relatief goedkoper en in wezen onbeperkt schaalbaar zijn.

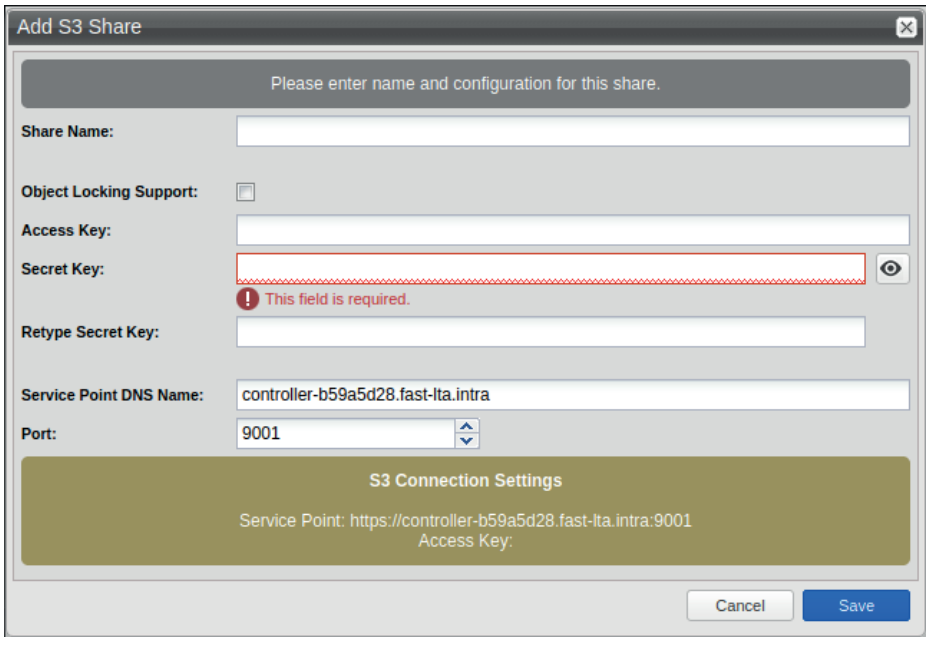
Het object locking-mechanisme wordt door de back-upsoftware beheerd en biedt directe bescherming voor de weggeschreven objecten. Het is simpelweg niet mogelijk om deze gegevens gedurende de bewaartermijn te wijzigen of verwijderen. Na het verstrijken van deze termijn zorgt de back-upsoftware er automatisch voor dat de desbetreffende objecten, waarvan de object lock is opgeheven, direct worden verwijderd. **Op die manier komt er opnieuw opslagruimte vrij.**

Beide methoden bieden een hoge mate van bescherming tegen de meeste cyberaanvallen en knoeipogingen. Deze WORM-beveiliging is echter gebaseerd op software en daardoor principieel kwetsbaar. Er zijn mensen verantwoordelijk voor de bescherming van toegangsrechten en accounts, waarmee fouten en beveiligingslekken niet zijn uitgesloten. Het verdient de aanbeveling om op elk punt gebruik te maken van twee-factorauthenticatie (2FA) of **multi-factorauthenticatie (MFA)** om onbevoegde toegang te voorkomen.

02

Object Locking

Automatisch,
vrijgave na de bewaartermijn



De software van de Silent Bricks biedt vanaf versie 2.45 ondersteuning voor object locking voor S3-shares. Dat betekent dat buckets kunnen worden beschermd op basis van een retention period en immutability met behulp van back-upsoftware, zoals Veeam.

Hardwarematige WORM-beveiliging

Hardwarematige beveiliging gaat veel verder. Hierbij bepaalt de firmware van de hardware welke gedeeltes binnen de gegevensdrager toegankelijk zijn voor schrijfbewerkingen en welke gedeeltes alleen nog maar kunnen worden gelezen. Bij de Silent Cube en de Silent Brick WORM wordt dit gebaseerd op basis van het 'waterpeil'. Als er gegevens naar de verbonden gegevensdrager worden weggeschreven, stijgt daarmee het waterpeil. Onder deze markering voert de hardware alleen nog leesbewerkingen uit. **Deze functionaliteit in de firmware sluit manipulatie uit.** Het betekent echter wel dat gegevensdragers steeds voller raken, omdat afzonderlijke gegevens nooit meer kunnen worden gewist. Een reset of reductie van het waterpeil is simpelweg niet in de opdrachtenreeks van de hardware beschikbaar. In dit geval is er inderdaad sprake van maximale beveiliging. Daarom wordt hardwarematige WORM-beveiliging meestal ingezet voor gegevens die niet of nog maar heel zelden worden gewijzigd. Dan valt bijvoorbeeld te denken aan archiefdata.

Een andere vorm van hardwarematige WORM-beveiliging is een fysieke blokkering. Dit valt te vergelijken met **het verwijderen van het lipje van een cassettebandje** of het verplaatsen van het vergrendelingsschuifje van een SD-geheugenkaart. Dit soort fysieke blokkeringen is echter alleen beschikbaar op verwijderbare opslagmedia zoals tape die om een handmatige omgang vragen en waar de blokkering tevens eenvoudig ongedaan kan worden gemaakt. Ze kunnen daarom alleen als een **beschermingsmechanisme tegen onopzettelijke verwijdering** worden gezien. Want als een cybercrimineel fysieke toegang heeft tot verwijderbare opslagmedia, kan die de schrijfbeveiliging in een handomdraai ongedaan maken.

Hardware-WORM

Automatisch,
geen vrijgave

03

Er zijn ook Silent Bricks met hardwarematige WORM-beveiliging verkrijgbaar (links: Silent Brick DS WORM, rechts: Silent Brick WORM). De mobiele datacontainers Silent Brick en Silent Brick WORM zijn tevens volledig geschikt voor air gapping.

Air gapping

Over verwijderbare media gesproken: een andere vorm van fysieke WORM-beveiliging is air gapping, **dus het fysiek scheiden van het opslagmedium en het storage-systeem**. Dit is onder meer mogelijk met tape of **Silent Bricks**. Wat niet langer met een systeem is verbonden, is per definitie beschermd, maar kan dan natuurlijk ook niet meer worden uitgelezen. Voor de leesbewerking moet het opslagmedium opnieuw in het systeem worden aangebracht, en daarmee zijn er opnieuw lees- en schrijfbewerkingen mogelijk.

Overigens worden er soms heel rekkelijke definities van de term air gapping gebruikt. Zo rekent Veeam ook het **onderbrengen van back-ups** in een afzonderlijk datacenter (een secundaire locatie) of bij een cloud provider als air gapping, ongeacht of en hoe de gegevens daar benaderbaar zijn voor cybercriminelen. Om deze back-ups effectief tegen manipulatie of verwijdering te beschermen worden gegevens binnen object stores met behulp van object locking beveiligd, waarmee er weer sprake is van een gesloten kring.

Air Gap

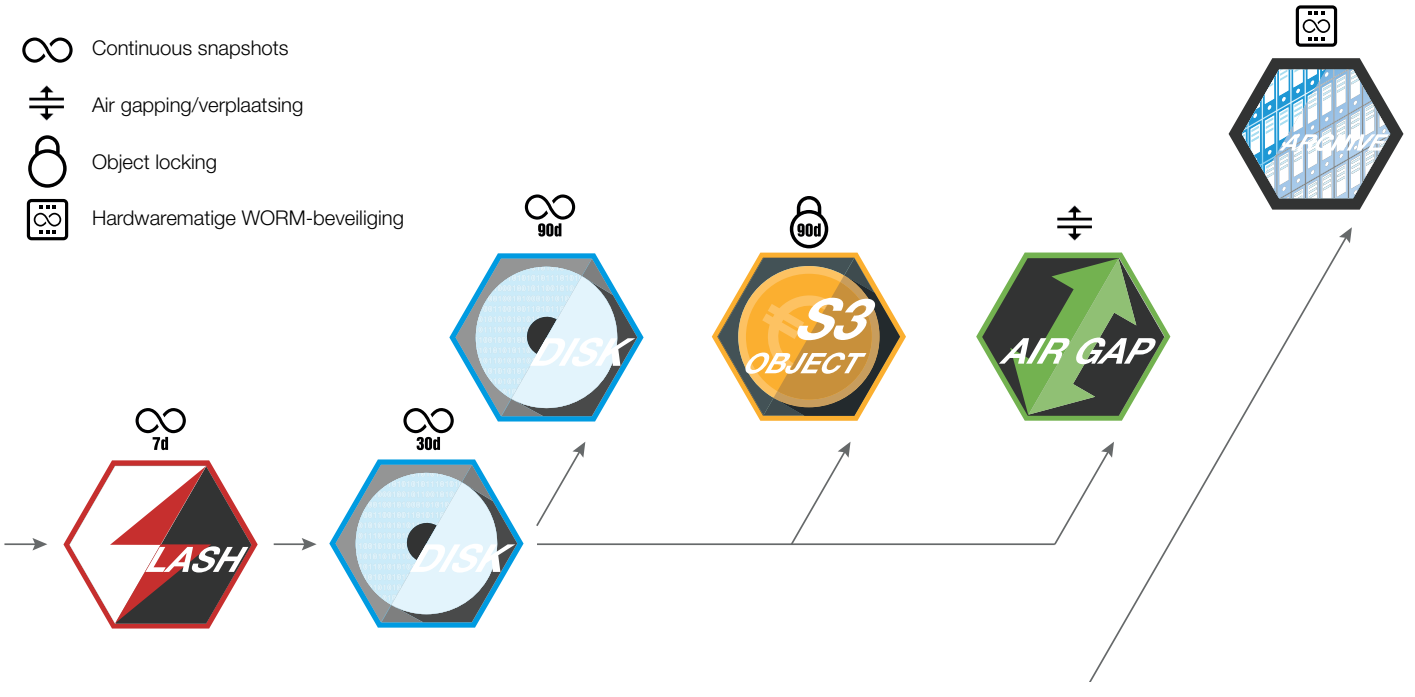
Handmatig,
vrijgave door overschrijven

04

Wat heb je nu precies nodig?

Vanzelfsprekend luidt het antwoord op die vraag: **dat hangt ervan af**. Zoals zo vaak het geval is bestaat er geen technologie die elk toepassingsscenario kan ondersteunen. Als gegevens langdurig en honderd procent veilig moeten worden opgeslagen, bijvoorbeeld in het kader van archivering volgens de eisen van de wet- en regelgeving, kun je niet om hardwarematige WORM-beveiliging heen. Maar in het geval van back-ups en gegevensherstel is het vaak niet praktisch haalbaar om gegevens 'voor altijd' te bewaren en de benodigde opslagcapaciteit zo buitenproportioneel te laten groeien. Daarom wordt voor dergelijke toepassingen gebruikgemaakt van softwarematige WORM-beveiliging of immutability.

Al naargelang het gebruikte systeem en de koppeling kan gebruik worden gemaakt van allerhande technologieën, van air gapping tot S3 object locking. Als fysieke air gapping niet wenselijk is of vanwege de datavolumes geen haalbare kaart is, is het mogelijk om data op te slaan in lokale of externe object stores. Die moeten dan wel immutable worden gemaakt met behulp van object locking.



Multi-immutable storage:

Het Silent Brick System

Het Silent Brick System beschermt gegevens op diverse manieren tegen manipulatie en onopzettelijke verwijdering.

In het file system (SecureNAS) zorgen continuous snapshots ervoor dat er in het geval van wijzigingen automatisch nieuwe snapshotversies worden gemaakt. Dit werkt net zoals bij een tijdmachine: in noodgevallen is het mogelijk om tot 90 dagen oude versies te herstellen.

Als het Silent Brick System wordt ingezet als met S3 compatibele object store kunnen gegevens worden beschermd met behulp van object locking en retention.

Silent Bricks bieden een bruto opslagcapaciteit tot 24 TB en zijn als transporteerbaar fysiek opslagmedium inzetbaar voor air gapping, ongeacht de koppeling waarvoor wordt gekozen.

De Silent Brick WORM wordt ingezet voor de opslag van alle gegevens die in geen geval verloren mogen gaan of mogen worden gewist. Deze worden beschermd op basis van hardwarematige WORM-beveiliging.

De afzonderlijke technologieën kunnen al naargelang de toepassing, het gewenste beveiligingsniveau en de specifieke eisen in combinatie worden gebruikt. Daarmee worden gegevens tijdens elke stap in de opslagketen effectief beschermd tegen manipulatie en onopzettelijke verwijdering.

Het Silent Brick System biedt daarmee de meest uitgebreide bescherming op basis van immutability van alle systemen voor secundaire gegevensopslag.

Silent Brick Controller met twee Silent Bricks en een Silent Brick WORM daaronder een Silent Brick DS WORM

Silent Brick (offline)

PROUDLY MADE IN EUROPE

COMEX

FAST LTA

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.de | **www.fast-lta.com**