PLATFORMPERSPECTIEF

Back-up Hoort In Het Securityplatform, Niet Ernaast

Back-up staat al decennia buiten de securitystack. De reden waarom dat zo is geregeld, geldt niet langer.

Voor de meeste lean IT-teams — en voor de MSP's die hen ondersteunen — heeft back-up altijd in een eigen silo gezeten: een aparte leverancier, een aparte console, een apart contract, en meestal maar één of twee mensen die weten hoe een restore werkelijk verloopt. Dat was logisch toen back-up vooral een verzekering was tegen kapotte schijven en verwijderde mappen. Het is veel minder logisch nu dataverlies meestal het gevolg is van een securityincident.

De aanleiding is vandaag vaker een gecompromitteerde identiteit, een kwaadaardige bijlage, ransomware in een SaaS-tenant, of precies het soort vergissing dat een DLP-beleid had moeten tegenhouden. Herstel is ongemerkt de laatste stap van incident response geworden, en wordt nog steeds uitgevoerd buiten de securitystack, door een tool die niets weet over het incident waarvan hij herstelt.

Dat is de gedachte achter de toevoeging van de geïntegreerde back-up en recovery van Keepit aan het Coro-platform, nu in early access en met algemene beschikbaarheid verwacht tegen het einde van 2026. De opslagarchitectuur blijft bewust onafhankelijk — air-gapped, immutable en leveranciersonafhankelijk, gescheiden van de productieomgeving en zonder externe subverwerkers — want juist die onafhankelijkheid maakt hem waardevol op het moment dat de productieomgeving zelf onder vuur ligt. Wat verandert, is waar het beheer plaatsvindt.

Back-up zit nu in hetzelfde platform, onder hetzelfde beleid, en maakt gebruik van dezelfde telemetrie die al endpoint, e-mail, cloud, netwerk, identiteit, databescherming en gebruikersbewustzijn dekt. Eén data-engine, één laag. Het praktische verschil blijkt uit de vragen die een incident vertragen: wat is geraakt, wanneer was de omgeving voor het laatst schoon, naar welk punt moet je terug. Dat zijn securityvragen, en ze zijn een stuk eenvoudiger te beantwoorden wanneer detectie en herstel niet twee losse administraties zijn. Hetzelfde geldt voor de bewijslast rond NIS2, DORA, AVG en HIPAA, die daarmee geen tweede rapportagetraject meer is.

Voor MSP's is er een commerciële variant van hetzelfde argument. Vendor sprawl is zelden fataal, maar het is wel waar marge ongemerkt verdwijnt — elke extra leverancier brengt zijn eigen integratie, eigen alerts, eigen leercurve, eigen contract en eigen supportpad mee. Eén daarvan wegnemen, en tegelijk een dienst toevoegen bij klanten die al op het platform zitten, doet meer met de P&L dan welke korting ook.

> In juli noemde Gartner in de Market Overview for Workspace Cybersecurity Platforms Coro als Example Vendor en beschreef dit platformmodel als steeds relevanter voor mid-market-organisaties en de MSP's die hen bedienen. Dat is minder interessant als onderscheiding dan als signaal: consolidatie van dit type is nu een categorie die de markt erkent, en niet langer een positioneringsclaim die een leverancier over zichzelf maakt.