



Versterk uw databeschermingsplan met een snelwerkende, robuustere oplossing voor cyberherstel

Op basis van ons
onderzoek kan
Dell Technologies
PowerProtect Cyber
Recovery fysieke
isolatie bieden
voor back-upkluizen
en dieper scannen
op ransomware



Fysieke air gap- isolatie voor back-upkluizen

Maak een fysieke
barrière die data niet
kan doorkruisen



Dieper scannen op ransomware

CyberSense kijkt
naar bestands- en
databasecontent, niet
alleen naar metadata



Scan 2x meer afwijkende workloads

Zoek op meer
plaatsen naar malware
met één tool

De gemiddelde kosten van een ransomware-aanval stegen in 2 jaar met bijna 20 procent naar \$ 5,23 miljoen.¹ Efficiënte oplossingen voor cyberherstel kunnen helpen deze potentiële kosten te verminderen of zelfs te voorkomen door organisaties in staat te stellen snel te herstellen van incidenten, dataverlies te verminderen, downtime te minimaliseren en, tijdens dit proces, hun merkintegriteit te behouden. Oplossingen moeten bekende goede data na de aanval lokaliseren en herstellen, zodat de organisatie kritieke data en systemen kan redden en tegelijkertijd bedrijfsrisico's en downtime kan minimaliseren.

Dell PowerProtect Cyber Recovery (Cyber Recovery) is zo'n oplossing. Het helpt organisaties hun data en apps te beschermen tegen ransomware, destructieve cyberaanvallen en onverwachte gebeurtenissen. Voor dit rapport hebben we gebruikgemaakt van openbaar beschikbare gegevens om de fundamentele gegevensbeschermingsfuncties van Cyber Recovery en een concurrerende oplossing, Rubrik Security Cloud (RSC), te vergelijken. We hebben specifiek gekeken naar functies die klanten van cyberhersteloplossingen mogelijk belangrijk vinden, waaronder de herstelkluis, onveranderlijkheid, workloadsupport, scantechnologie, herstelbaarheid en isolatie.

In tegenstelling tot RSC maakt Cyber Recovery gebruik van een aanpak met meerdere kopieën. Dit houdt in dat nadat back-ups zijn gemaakt, deze back-ups (of normaal gesproken een geselecteerde subset) worden gekopieerd naar geïsoleerde storage voor beveiliging en analyse. Cyber Recovery bestaat uit vele componenten, waaronder één of meer storagekluizen, die zowel op locatie als in de cloud geïmplementeerd kunnen worden op een PowerProtect Data Domain-apparaat of in de cloud via softwaregedefinieerde Dell APEX Protection Storage for Public Cloud. Ter vergelijking: RSC biedt geen lokale kluisopties. Cyber Recovery bevat ook CyberSense, een volledig geautomatiseerde en geïntegreerde intelligente engine voor beveiligingsanalytics die automatisch data, bestanden, databases en afbeeldingen in de kluis scant op tekenen van beschadiging door een ransomware-aanval. De CyberSense-oplossing kan twee keer meer afwijkende workloads scannen dan de Rubrik-oplossing, waardoor de ML (machine learning) van CyberSense de impact van malware of andere bedreigingsactiviteiten in meer data kan detecteren. Hieronder zetten we uiteen wat PowerProtect Cyber Recovery anders maakt en waarom het voordeliger kan zijn voor uw organisatie.

Productoverzicht

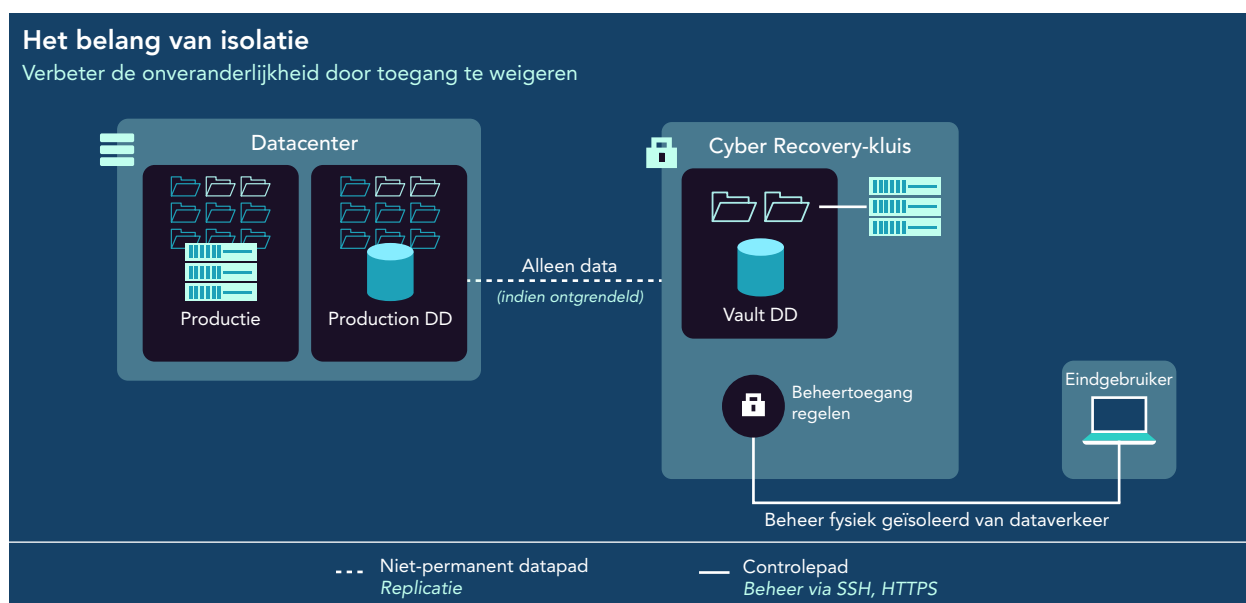
Overzicht van Dell PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery bestaat uit een storageapparaat dat productiedata bevat en een doelopslagapparaat in de kluis voor replicatie. Het bevat ook Cyber Recovery-software, die synchronisatie coördineert, meerdere datakopieën beheert op het PowerProtect Data Domain-systeem (PPDD) in de Cyber Recovery-kluis, toezicht houdt op het herstelproces en toezicht houdt op het analyseproces met CyberSense.

De oplossing draagt unieke data over van de productie-PPDD MTree naar de kluistegenhanger via MTree-replicatie en maakt onveranderlijkheid van data* mogelijk voor een bepaalde duur. De kluis is voorzien van een server die de Cyber Recovery-software bevat en een component waarmee de oplossing back-uptoepassingen en -data herstelt. Een Cyber Recovery-kluis bevat gewoonlijk veel van deze componenten. De kluis bevat ook een analyse-/indexeringshost die is uitgerust met software voor data-analyse, die directe integratie biedt tussen de Cyber Recovery-software en CyberSense.

*De producten van Dell zijn ontworpen om de inspanningen van klanten te ondersteunen om hun kritieke data te beveiligen. Net als bij elk elektronisch product kunnen er zich beveiligingslekken voordoen in databeschermings-, storage- en andere infrastructuurproducten. Het is belangrijk dat klanten beveiligingsupdates installeren zodra deze door Dell beschikbaar worden gesteld.

Figuur 1 bevat een overzicht van de Dell Cyber Recovery-oplossing.

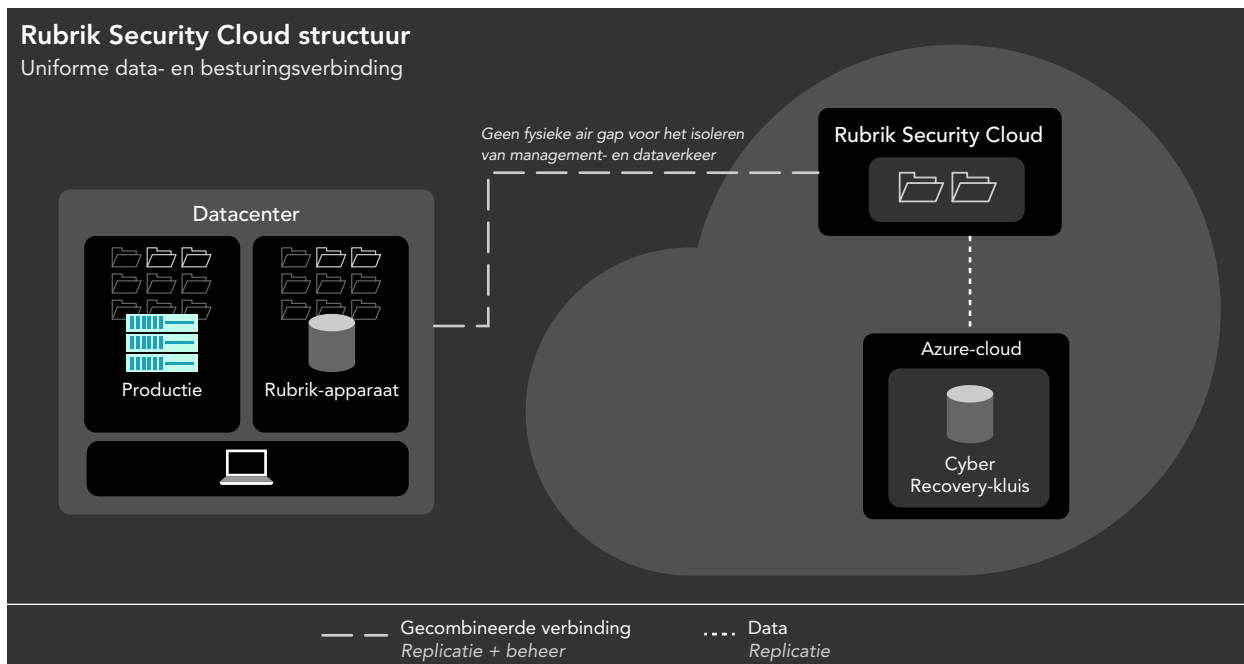


Afbeelding 1: Hoogwaardige data- en controlepadarchitectuur van de Cyber Recovery-kluis. Bron: Principled Technologies.

Lees voor meer informatie over de belangrijkste componenten van de Dell PowerProtect Cyber Recovery-oplossing de Dell PowerProtect Cyber Recovery Solution Guide.

Overzicht van Rubrik Security Cloud

Rubrik beschrijft Rubrik Security Cloud als een Software-as-a-Service-platform (SaaS) waarmee klanten "[hun] data veilig kunnen houden, datarisico's kunnen controleren en snel [hun] data kunnen herstellen, waar deze zich ook bevindt, in de hele onderneming, in de cloud en in SaaS-apps".⁴ Rubrik stelt dat het de oplossing heeft gebouwd op een "veilige microservicearchitectuur met behulp van services en infrastructuur met hoge beschikbaarheid die worden uitgevoerd via Google Cloud Platform (GCP)".⁵ Figuur 2 toont de algemene structuur van Rubrik Security Cloud.



Afbeelding 2: De algemene structuur van Rubrik Security Cloud. Bron: Principled Technologies.

Ondersteuning voor functies

Herstelkluis

Kluizen zijn de speciale storage die versleutelde kopieën van back-ups bevat die de oplossing in uw productieomgeving maakt. De kluizen maken geen deel uit van de back-upoplossingen voor productie. In plaats daarvan fungeert elke kluis als een geïsoleerde 'back-up naar de back-uplocatie' van waaruit klanten gevalideerde back-ups kunnen herstellen.

Dell biedt verschillende kluisopties, waaronder op locatie, op een externe colocatie of binnen een public cloud. De kluis op locatie gebruikt een operationele air-gapped PPDD die zich in uw datacenter bevindt, mogelijk zelfs binnen hetzelfde rack als uw back-upoplossing. Een air-gapped oplossing is meestal fysiek geïsoleerd van de productieomgeving. Een externe kluis op een colocatie vereist speciale netwerkverbindingen met een fysieke kluis, zoals een kluis op locatie, maar de kluis bevindt zich geografisch gescheiden in een extern datacenter. Dell biedt ook kluizen binnen de public cloud, in samenwerking met cloudserviceproviders Amazon Web Services (AWS), Microsoft Azure en Google Cloud. Public cloud-kluizen kunnen configuratieflexibiliteit bieden om aan de behoeften van klanten te voldoen.^{6, 7, 8}

Rubrik Cyber Recovery is een onderdeel van de Rubrik Security Cloud. De herstelkluis wordt geleverd via een Software-as-a-Service-model en maakt alleen gebruik van storage op Microsoft Azure. Veel van de openbaar beschikbare documenten die we in ons onderzoek vonden, koppelen de Rubrik Cyber Recovery-kluis aan de Rubrik Cloud Vault, de back-uplaag, die onveranderlijkheid biedt.^{9, 10} Deze kluis vereist geen extra hardware en kan worden gebruikt door elke versie van het Rubrik Cloud Data Management-platform (CDM) vanaf versie 6.02.

Onveranderlijkheid

Onveranderlijkheid verwijst naar de toestand van geen verandering of permanentheid. Met onveranderlijke back-ups en back-upkopieën kunnen beheerders permanente bestanden maken die gebruikers of systemen niet kunnen wijzigen of verwijderen totdat er een bepaalde tijd is verstreken. Dan verdwijnen de bestanden: de oplossing verwijdert ze automatisch. Oplossingen voeren dit proces meestal uit via beleidsregels of definities die bepalen hoe het systeem bestanden behandelt.¹¹

De onveranderlijkheid van Dell PowerProtect Cyber Recovery is afhankelijk van retentievergrendelingen, via de Retention Lock-functie, om verwijdering of wijziging (voor een bepaalde periode) of gedwongen vroegtijdig verloop van back-upkopieën te voorkomen. (De PPDD is een bestandssysteem waaraan alleen bestanden kunnen worden toegevoegd, ongeacht of de organisatie Retention Lock heeft ingeschakeld of niet.¹²) Dell klanten beheren back-ups met PPDD MTrees. Dit zijn door de gebruiker gedefinieerde logische partities met onafhankelijke retentie-instellingen die ze toewijzen als bestemming voor back-uptoepassingen.¹³ Klanten kunnen kiezen uit twee soorten retentievergrendelingen: beheer en naleving. Vergrendelingen voor naleving zijn de strengste en veiligste van de twee. Klanten schakelen retentievergrendelingen in per MTree, wat betekent dat de definitie voor retentievergrendeling voor een bepaalde MTree geldt voor alle bestanden in die MTree. Ze stellen de tijdsduur voor retentie in per bestand. Zodra klanten een retentievergrendeling voor naleving hebben gedefinieerd, kan geen enkele gebruiker of geen enkel systeem deze verwijderen. Een beheerder kan een retentievergrendeling voor beheer, de minder strikte optie, terugzetten.¹⁴

De onveranderlijkheid van de Rubrik-oplossing gebruikt ook retentievergrendelingen om verwijdering of gedwongen vroegtijdig verloop van back-upkopieën te voorkomen. Net als PowerProtect Cyber Recovery voegt de Rubrik-oplossing

De Rubrik-oplossing schakelt standaard geen retentievergrendelingen in en klanten moeten ofwel een ticket openen naar Rubrik Support of een tweepuntsregel inschakelen om retentievergrendelingen toe te staan.

nieuwe data toe aan het bestandssysteem in plaats van bestaande data te overschrijven. De oplossing maakt vingerafdrukken van inkomende data en slaat deze op bij de data. **De Rubrik-oplossing schakelt retentievergrendelingen standaard niet in** en klanten moeten een ticket openen bij Rubrik-support of een tweepersoonsregel inschakelen om retentievergrendelingen toe te staan. (Vóór Rubrik Cloud Data Management versie 7.0.1 moesten klanten contact opnemen met Rubrik-support om retentievergrendelingen in te schakelen. Uit de Rubrik-documentatie is niet duidelijk of klanten hiervoor nog steeds contact kunnen opnemen met support of niet.) Zodra klanten retentievergrendelingen hebben ingeschakeld, voorkomen die dat gebruikers of systemen data buiten de opgegeven parameters verwijderen. Rubrik-retentievergrendelingen vereisen een externe Network Time Protocol-server (NTP) voor tijdsynchronisatie, wat een kans kan bieden voor kwaadwillenden om de referentie-NTP-bron te manipuleren en daardoor retentievergrendelingen voortijdig te laten verlopen.¹⁵

Licenties en abonnementen

Dell PowerProtect Cyber Recovery is een gelicentieerde oplossing. Tijdens de installatie installeert Dell standaard een proeflicentie voor 90 dagen. Na 90 dagen moeten klanten een nieuwe licentie aanschaffen om het product te kunnen blijven gebruiken. Dell biedt zowel standaardlicenties (permanent) als licenties op abonnementsbasis.

Rubrik integreert Rubrik Cyber Recovery in Rubrik Security Cloud (RSC). Klanten moeten een abonnement hebben op Rubrik Enterprise Edition om Rubrik Cyber Recovery te kunnen gebruiken. De abonnementstermijn bedraagt drie jaar.^{16, 17} In het geval van een RSC-storing vereisen SAP HANA- en Db2-workloads dat tools van derden worden gebruikt om data te herstellen. Dit kan extra abonnementskosten met zich meebrengen.¹⁸

Beheertoegang

Het beheer van het Dell PowerProtect Cyber Recovery-systeem is lokaal voor de topologie die klanten kiezen voor de implementatie. Omdat de oplossing het herstel vanuit de kluis start, melden beheerders zich aan bij de beheergebruikersinterface vanaf de locatie waar de kluis zich bevindt. Kluizen op locatie bieden beheerders lokale toegang zonder dat ze internettoegang nodig hebben, wat ernstig beschadigd kan zijn na een cyberaanval door denial of service-

aanvallen of door de data te beveiligen door de internetverbinding te verbreken, zoals aanbevolen door het National Institute of Standards and Technology (NIST). Door middel van kluizen op colocatie is fysieke toegang tot het apparaat mogelijk vanaf een externe locatie en kunnen verbindingen buiten het openbare internet worden gebruikt. Cloudgebaseerde kluizen vereisen internettoegang voor herstel, waardoor herstel op locatie kan worden vertraagd totdat de cyberaanval is beëindigd en de normale netwerkverbinding wordt hersteld.

Het beheer van Rubrik Cyber Recovery vereist toegang tot Rubrik Security Cloud, waarvoor internettoegang nodig is. Zoals eerder genoemd kan dit type verbinding herstel op locatie vertragen totdat de netwerkfunctionaliteit na een cyberaanval weer normaal is.

Omdat klanten toegang moeten hebben tot RSC om Rubrik Cyber Recovery-functies te kunnen gebruiken, zorgt RSC voor storing. Als die service niet beschikbaar zou zijn, zou dit het herstel vanuit de kluis voor de getroffen klant belemmeren. Rubrik kan 10 workloads herstellen tijdens een RSC-serviceonderbreking, maar twee databaseworkloads vereisen tools van derden en hulp van Rubrik-support om ze te herstellen.^{19,20} Bovendien krijgen gecompromitteerde beheerdersaccounts of kwaadwillenden met toegang tot het RSC-platform toegang tot de hele omgeving in plaats van één kluis.

Krijg extra hulp bij Managed Detection and Response van Dell

Sommige organisaties willen misschien liever geholpen worden bij hun cyberbeveiliging. Dell biedt deze klanten Managed Detection and Response (MDR), een volledig beheerde service die bedreigingen en risico's controleert en detecteert en samenwerkt met klanten om deze risico's te beperken. Volgens Dell biedt de service het volgende:²¹

- Vertrouwde ondersteuning, inclusief deskundig advies voor het implementeren en configureren van de platforms voor beveiligingsanalytics van Managed Detection and Response (XDR) die Dell ondersteunt
- Threat Response en beveiligingsconfiguratie, inclusief tot 40 uur servicegerelateerde beveiligingsconfiguratie per kwartaal
- 24/7 detectie en onderzoek, inclusief proactieve opsporing van bedreigingen die specifiek zijn voor de omgeving van elke klant om nieuwe bedreigingen of variaties van bekende bedreigingen te ontdekken die beveiligingssystemen omzeilen
- Starten van reacties op cyberincidenten, inclusief 40 uur hulp per jaar bij incidentrespons op afstand waardoor onderzoeksactiviteiten snel kunnen worden gestart

In combinatie met APEX Cyber Recovery Services kunnen klanten met MDR kiezen uit vele opties om bedreigingen en risico's te controleren, te detecteren en te beperken. De beschikbaarheid van opties kan een uitgebreide dekking omvatten of een hybride aanpak zijn die past bij de behoeften van uw organisatie.

Ga voor meer informatie over MDR naar <https://www.dell.com/nl-nl/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm>.

Naadloos

Instellen

De installatie van Dell PowerProtect Cyber Recovery bestaat uit software-installatie op een Linux-systeem of het maken van een VMware® vSphere®-apparaat vanuit een Open Virtualization Format-sjabloon (OVF). Voor de software-installatie zijn 14 stappen nodig,²² terwijl de implementatie van het alternatieve vSphere-apparaat 8 stappen en 5 minuten kost.²³ Na de installatie hebben beheerders toegang tot de oplossing via webbrowsers vanuit de geïsoleerde omgeving.

Klanten moeten CyberSense afzonderlijk implementeren. Dit is een volledig geautomatiseerde en geïntegreerde engine voor intelligente beveiligingsanalytics.²⁴ De instructies voor het installeren van CyberSense in Dell PowerProtect Cyber Recovery zijn niet openbaar beschikbaar.²⁵

Dell heeft meerdere statistieken die gebruikers kunnen aanpassen, waaronder doel van vernietigingsdetectie (DDO), doel van de beoordeling van de vernietiging (DAO), Cyber Recovery-punt (CRP), Cyber Recovery-tijd (CRT), Cyber Recovery-synchronisatie-interval, en Cyber Recovery-gegevenskopie-aantal. Dell raadt ook aan om data te karakteriseren die moeten worden beschermd. Deze data kan essentieel zijn voor de missie, essentieel voor het bedrijf, afhankelijk van kerninfrastructuurservices of andere toepassingen, of algemeen zijn, zoals binaire app-bestanden, opstartimages en back-upcatalogi. De reeks opties geeft klanten volledige controle over hun back-upomgeving en de mogelijkheid om de classificatie van hun data aan te passen. Dell Consulting Services kunnen ook meer hulp en suggesties bieden.²⁶

De Rubrik-configuratie bestaat ook uit meerdere stappen. Voordat er een cluster wordt gemaakt, moet Rubrik-supportservices Rubrik CDM installeren en configureren. Daarna downloadt en installeert een beheerder de meest recente of gewenste versie van CDM (15 stappen).²⁷ Vervolgens kan de beheerder een Rubrik-cluster instellen via de gebruikersinterface of de CLI. U kunt het cluster instellen via de gebruikersinterface of de CLI. Beide bestaan uit 24 stappen.^{28, 29} De beheerder kan de Rubrik-clusters online registreren (12 stappen)³⁰ of offline registreren (18 stappen).³¹ Daarna schakelt de beheerder meervoudige verificatie (MFA) in, wat uit 13 stappen bestaat.³² Ten slotte voegt de beheerder het initiële account (6 stappen) en eventuele andere accounts toe.³³ Figuur 3 toont het maximale aantal mogelijke stappen om elke oplossing voor cyberherstel in te stellen.

Rubrik-klanten kunnen geen andere statistieken afstemmen, wat de flexibiliteit kan verminderen om aan hun behoeften te voldoen. Eén recensent schreef: "Het grootste deel van de gebruikersinterface is vrij eenvoudig, maar in sommige gebieden mis ik een beschrijving van waarvoor de optie wordt gebruikt, of de optie ontbreekt helemaal. Hoewel tunables de gebruikerservaring eenvoudig maken, zijn veel ervan niet aanwezig en moet er een Support Tunnel geopend zijn voor een supportmedewerker om een wijziging in de omgeving van de klant door te voeren."³⁴

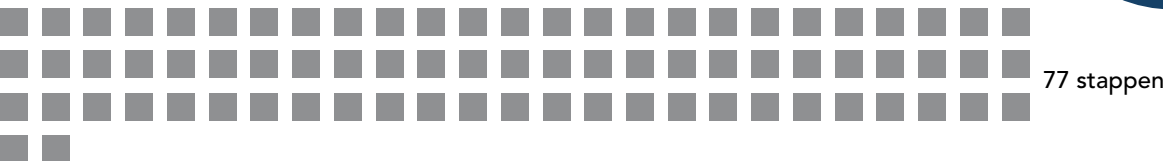
Maximaal mogelijke installatiestappen voor elke oplossing

Minder is beter

Dell PowerProtect Cyber Recovery



Rubrik Security Cloud



Tot 63
minder stappen

Afbeelding 3: Het maximale aantal mogelijke stappen voor het instellen van Dell PowerProtect Cyber Recovery en Rubrik Security Cloud. Minder is beter. Bron: Principled Technologies.

Onderhoud

We hebben gemerkt dat de gebruikersinterfaces van Dell en Rubrik na de installatie vergelijkbaar zijn voor het uitvoeren van dagelijkse onderhoudswerkzaamheden. Na de configuratie kunnen klanten Dell PowerProtect Cyber Recovery instellen om het volgende te doen:^{35, 36}

- Automatisch Cyber Recovery-taakrapporten genereren volgens een schema en als reactie op een handmatig verzoek van de gebruiker
 - Een gebruiker of schema maakt taken als die een beleid, hersteloperatie, systeemback-up of schoonmaakoperatie start
- Automatisch controleren van de status van de kluis, storagecapaciteit, Cyber Recovery-acties, waarschuwingen wanneer kopiëren/synchroniseren mislukt of als de Cyber Recovery-kluis niet actief is, en Cyber Recovery-taken
- Automatisch en continu scannen op aanvallen en daarna CyberSense-waarschuwingen weergeven, in volgorde van ernst, met het aantal bestanden, hosts, getroffen beleidsregels, specifieke gedetecteerde bedreiging, het tijdstip van de aanval (zodat u een schone back-up kunt vinden) en een lijst met beschadigde bestanden die u kunt gebruiken om de aanval te analyseren

Op dezelfde manier kunnen klanten Rubrik configureren om het volgende te doen:³⁷

- Rubrik Security Cloud automatisch alle gebeurtenissen van alle verbonden Rubrik-clusters laten volgen, controleren en te tonen. Het biedt drie soorten gebeurtenissen:³⁸
 - Kritiek: Gebeurtenissen die aandacht vereisen, zoals mislukte back-up, archivering of replicatie
 - Waarschuwing: Een back-up, archief of herstel is voltooid
 - Informatief: Alleen informatie
- Automatisch en continu snapshots scannen op nieuwe en bestaande indicatoren van aanvallen met behulp van Threat Monitor, wat het tijdstip aangeeft waarop de oplossing voor het laatst een snapshot heeft gemaakt, de tijdlijn van de gebeurtenis, de detectietijd, het aantal gewijzigde bestanden, het aantal verdachte bestanden, de clusternaam en het objecttype en -naam

Ondersteuning voor afwijkende workloads

Zowel Rubrik Security Cloud Data Threat Analytics als CyberSense scannen meerdere workloadtypen, maar volgens de bronnen die we hebben gevonden, ondersteunt CyberSense drie keer zoveel workloads voor detectie van afwijkingen. Onder andere de volgende typen workloads worden gescand:

- VM's
- Kerninfrastructuur
- Gebruikersbestanden die documenten, contracten en intellectueel eigendom kunnen bevatten
- databases;
- Back-ups gemaakt door andere clients

Als we het aantal ondersteunde workloads tellen dat we in openbaar beschikbare data hebben gevonden, zien we dat CyberSense 21 workloads voor detectie van afwijkingen ondersteunt en Rubrik 7. Daarom ondersteunt CyberSense volgens openbaar beschikbare data die door beide worden gedeeld drie keer zoveel workloads dan Rubrik Security Cloud Data Threat Analytics. Hoe meer data een oplossing voor cyberherstel kan scannen, hoe groter de kans dat deze hardnekkige malware of andere beschadigingen kan vinden.



Als we het aantal ondersteunde workloads tellen dat we in openbaar beschikbare data hebben gevonden, zien we dat CyberSense 21 workloads voor afwijkingdetectie ondersteunt en Rubrik 7.

Ondersteuning voor VM-workloads

VM-workloads verwijzen naar de toepassingen, services of taken die VM's uitvoeren op een fysieke hostserver of in een cloudomgeving. Omdat deze workloads kunnen variëren in functie en op vele andere manieren waardoor ze vaker kunnen worden blootgesteld aan malware, is het scannen van VM's essentieel. Rubrik Security Cloud Data Threat Analytics, dat "detectie van afwijkingen, bedreigingsbewaking, bedreigingsopsporing en dataherstelservices op beschermde resources bevat"³⁹, ondersteunt het scannen van de volgende VM-workloads:⁴⁰

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense ondersteunt het scannen van de volgende VM-workloads:^{41 42, , 43}

- VMware
- Hyper-V, met Dell Avamar of Dell NetWorker back-ups
- Amazon Web Services (AWS)

VMware beweert dat "maar liefst 80 procent van de gevirtualiseerde workloads op VMware-technologie draait".⁴⁴

In het eerste kwartaal van 2024 bestuurd Amazon Web Services (AWS), de populairste leverancier in de markt voor cloudinfrastructuurservices, 31 procent van de hele markt. Microsoft Azure neemt de tweede plaats in met een marktaandeel van 25 procent.⁴⁵

Kerninfrastructuur

De kerninfrastructuur is de basiscomponenten en -services die de werking van een technologieomgeving mogelijk maken. Het detecteren van malware op dit niveau kan helpen de ernst van een aanval te verminderen, omdat de functionaliteit van de kerninfrastructuur van invloed kan zijn op veel systemen en gebruikers. In de Rubrik Security Cloud-documentatie staat nergens of het scannen van een kerninfrastructuur wordt ondersteund.⁴⁶

CyberSense ondersteunt daarentegen het scannen van de volgende kerninfrastructuur:⁴⁷

- Active Directory
- DNS
- LDAP

Gebruikersbestanden die documenten, contracten en intellectueel eigendom kunnen bevatten

Rubrik Security Cloud Data Threat Analytics ondersteunt het scannen van de volgende gebruikersbestanden:⁴⁸

- NAS-bestandssets en datasets
- Windows-volumegroepen
- Linux en Windows

CyberSense kan Linux- en Windows-gebruikersbestanden scannen.⁴⁹

databases;

Apps kunnen verschillende soorten databases gebruiken om veel verschillende redenen. Het detecteren van de aanwezigheid van malware in verschillende databases kan dus cruciaal zijn voor een snelle reactie. Rubrik Security Cloud Data Threat Analytics kan een back-up maken van databases, maar we hebben geen openbare documentatie gevonden waarin staat dat ze die databaseback-ups kunnen scannen.

CyberSense ondersteunt het scannen van de volgende databases met scans op paginaniveau:⁵⁰

- SQL
- PostgreSQL
- Oracle®
- Epic® Caché
- SAP HANA
- MariaDB/MySQL
- Db2



Databases scannen

CyberSense 7 en
RSC Data Threat Analytics 0

Back-ups gemaakt door andere clients

Sommige organisaties hebben mogelijk databack-ups van meerdere leveranciers om te zorgen voor redundantie, om te voldoen aan regelgeving of om een andere belangrijke reden. In de Rubrik Security Cloud-documentatie staat niet of ze back-ups kunnen scannen die door andere back-upclients zijn gemaakt.⁵¹

CyberSense heeft een duidelijk voordeel in deze categorie en ondersteunt het scannen van back-ups die zijn gemaakt door de volgende back-upclients:^{52 53, , 54}

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Omruilings-
- Avamar
- Commvault

Scantechnologie

Rubrik Security Cloud bevat veel tools om te scannen en te helpen met scannen, in Data Threat Analytics:

- Rubrik Anomaly Detection toont verdachte bestanden, wijzigingen in snapshots⁵⁵ en afwijkingsdetails als afwijkingsincidenten die klanten kunnen bestuderen en gebruiken bij het onderzoeken van momentopnamen.⁵⁶ De software biedt ook herstelopties.⁵⁷
- Rubrik VM Encryption Detection detecteert aanvallen op VMware vSphere-virtuele schijf-bestanden.⁵⁸
- Rubrik Threat Monitoring toont informatie over gedetecteerde bedreigingen en overeenkomsten.⁵⁹
- Rubrik Threat Hunt is een door de gebruiker gestarte scan voor indicatoren van inbreuk.⁶⁰
- Rubrik Quarantine isoleert objecten die naar voren komen bij het zoeken naar bedreigingen.⁶¹

Rubrik RSC heeft ook Rubrik Backup Service Connectors voor elk Rubrik-cluster.

Rubrik-klanten moeten de juiste tool voor hun taak selecteren, mogelijk scans handmatig starten of meerdere tools gebruiken om een taak uit te voeren. Dell heeft daarentegen één scanoptie, CyberSense, die klanten misschien makkelijker vinden om te beheren.

CyberSense-scans gaan dieper dan het scannen 'aan de oppervlakte' van Rubrik RSC Data Threat Analytics. CyberSense voert volledige contentscans van bestanden en scans van databases op paginaniveau uit en kan gedeeltelijke versleuteling van bestanden detecteren.⁶² De tool gebruikt een machine learning-database (ML) die is getraind door Index Engines op duizenden databedreigingen. De database bevat meer dan 200 analysepunten om databeschadiging te detecteren.⁶³ In tegenstelling tot Rubrik Threat Monitoring en Threat Hunt vertrouwt CyberSense niet op malwarehandtekeningen die worden verkregen van externe organisaties die bedreigingen herkennen. In plaats daarvan ontdekt het zelf nieuwe bedreigingen.⁶⁴ **CyberSense vertrouwt ook niet op willekeurige drempels van acceptabele bestandswijzigingen of entropieniveaus tussen momentopnamen die kunnen leiden tot fout negatieven** en traint de ML niet op een basislijn van eerder klantgedrag.^{65, 66, 67}

De Rubrik-afwijkingsdetectiesoftware vertrouwt uitsluitend op metadata om te bepalen of een momentopname beschadigd is voordat er een contentanalyse wordt uitgevoerd. In vergelijking met de doorlopende ML van CyberSense ontdekt de Rubrik-software beschadiging pas nadat de handtekeningen zijn verkregen. Rubrik-afwijkingsdetectie moet een gedragsmodel maken om de normale basislijn van een klant te bepalen. Dit kan verschillende back-ups lang duren. Het Rubrik-gedragsmodel vereist ten minste twee back-ups om een basislijn te maken van typische wijzigingen in een bestandssysteem wanneer er geen aanvallen zijn. Het is echter mogelijk dat één set wijzigingsstatistieken niet voldoende is om vast te stellen wat typisch is.

CyberSense vertrouwt ook niet op willekeurige drempels van acceptabele bestandswijzigingen of entropieniveaus tussen snapshots die kunnen leiden tot foutnegatieven....

Bedrijfsgebeurtenissen kunnen meer of minder activiteiten of meer verdachte soorten activiteiten veroorzaken die niet plaatsvonden tussen de eerste en tweede Rubrik-momentopname. Hoe meer back-ups de Rubrik-oplossing analyseert, hoe nauwkeuriger het gedragsmodel kan worden getraind tot een basislijn.^{68, 69}

CyberSense voert alle analyses uit in de kluis. In de pijplijn voor gedragsanalyse van het bestandssysteem stuurt Rubrik metadata over wijzigingen in het bestandssysteem van de klant naar het cloudgebaseerde Polaris-platform om de gedragsanalyse uit te voeren, waardoor een aanvalsoppervlak wordt geopend.⁷⁰

Klanten kunnen Rubrik Threat Monitoring en Threat Hunt alleen gebruiken als onderdeel van de Rubrik Enterprise Edition.⁷¹ Klanten moeten Threat Hunt-scans uitvoeren met bevoegdheden voor op rollen gebaseerde toegangscontrole (RBAC) en de gebruikers moeten aangeven op welke specifieke indicatoren van inbreuk (IOC) ze willen zoeken.⁷² Dit is geen best practice in de branche.⁷³ Net als CyberSense ondersteunt Threat Hunt bestandssets van VMware, AHV, Hyper-V en NAS en servers van Linux en Windows.⁷⁴

In de volgende gedeelten vindt u meer informatie over hoe de Rubrik-oplossing bedreigingsdetectie biedt.

Metadata en bestandssysteemstatistieken

Het Rubrik Anomaly Detection ML-gedragsmodel registreert de wijzigingen in het bestandssysteem sinds de laatste momentopname als metadata, zoals het aantal bestanden dat is toegevoegd, verwijderd of verplaatst.⁷⁵ Vervolgens traint een ML-model op deze wijzigingen om een basislijn voor het gedragsmodel te maken voor het bestandssysteem. Rubrik markeert een momentopname als afwijkend als er te veel wijzigingen worden gedetecteerd. Nadat een momentopname is gemarkeerd door de gedragsanalyse, analyseert de oplossing de bestandsinhoud.⁷⁶ Het controleren van metadata kan een beveiligingslaag toevoegen, maar biedt mogelijk niet de benodigde bescherming die downtime door een gebeurtenis helpt voorkomen of verminderen.

CyberSense heeft geen basislijn nodig. Het controleert en analyseert wijzigingen in bestands- en databasecontent vanaf de eerste back-upkopieën.

CyberSense heeft daarentegen geen basislijn nodig.

Het controleert en analyseert wijzigingen in bestands- en databasecontent vanaf de eerste back-upkopieën. De CyberSense-aanpak biedt meer detailniveau, omdat de software zelfs stukjes van een bestand of afzonderlijke pagina's van een database analyseert. Vergelijkbaar met de Rubrik-oplossing nemen CyberSense-scans metadata-eigenschappen mee en voeren ze resultaten in de ML-engine in. In tegenstelling tot de Rubrik-oplossing is CyberSense niet beperkt tot het scannen van metadata en heeft Index Engines de ML-engine getraind op aanvallen die zijn gedocumenteerd door Index Engines, niet op handtekeningen of eerder klantgedrag.^{77, 78}

Drempels

Tijdens de gedragsanalyse bepaalt Rubrik-ML hoe waarschijnlijk het is dat er een afwijking is opgetreden in een bestandssysteem. Als de Rubrik-oplossing dit waarschijnlijk vindt, wordt er een inhoudsanalyse uitgevoerd. Dit kan een door gedragsmodellen bepaalde drempel voor 'afwijkend gedrag' zijn. De Rubrik-oplossing

kan bijvoorbeeld afwijkend gedrag markeren als er veel nieuwe of gewijzigde bestanden worden waargenomen, of een verhoogde willekeur of versleutelingsindicatoren.⁷⁹ Tijdens de inhoudsanalyse toont Rubrik Anomaly Detection wijzigingen in de bestandsinhoud en berekent het de kans op versleuteling door de entropie van het bestandssysteem te berekenen. De entropie van een bestandssysteem toont aan hoe waarschijnlijk het is dat een ransomware-aanval bestanden heeft versleuteld. Als de entropie een afwijkingsdrempel overschrijdt, waarschuwt de oplossing de gebruiker.^{80, 81} De effectiviteit bij het detecteren van databeschadiging is afhankelijk van de striktheid van de drempels. Als de drempels niet strikt genoeg zijn, kan dit foutnegatieven veroorzaken en dus een vals gevoel van veiligheid.⁸² Klanten moeten drempels correct instellen.

CyberSense controleert daarentegen op gedeeltelijke versleuteling van een bestand door bestandsinhoud te scannen en biedt daarbij een vertrouwenspercentage van 99,99 procent (volgens Dell en Index Engines) in de detectie van databeschadiging.⁸³

Handtekeningen en bestandsextensies

Rubrik Threat Monitoring en Threat Hunts scannen momentopnamen op IOC's. Als een van de meerdere informatiebronnen over bedreigingen die Rubrik controleert een nieuwe IOC ontdekt, pusht Threat Monitoring de bedreigingsfeed met Yet Another Ridiculous Acronym-regels (YARA) voor de identificatie van de nieuwe malware, ook wel bekend als de malwarehandtekening, naar alle Rubrik-clusters. De clusters beginnen dan met scannen.⁸⁴ Een recent WatchGuard-rapport geeft aan dat 57,8 procent van de malware handtekeningdetectie omzeilt. Geavanceerde malware, zoals BianLian, kan methoden gebruiken om handtekeningherkenning te omzeilen, en nieuwe malwarevarianten kunnen iets andere handtekeningen hebben dan de oorspronkelijke. Daarom is dreigingsinformatie misschien niet altijd up-to-date.⁸⁵

Ter vergelijking: CyberSense gebruikt meer dan 200 analytics en biedt een ML-model getraind op duizenden ransomware-varianten. Index Engines heeft bewezen dat de CyberSense-methode eerder ongeziene, geavanceerde varianten kan detecteren zonder handtekeningen te downloaden,⁸⁶ wat een ander voordeel is als u het internet niet wilt gebruiken tijdens een aanval.

Massale versleutelingsgebeurtenissen

De Rubrik-oplossing controleert op massale versleutelingsgebeurtenissen door de entropie van het hele bestandssysteem te berekenen.⁸⁷ CyberSense werkt veel gedetailleerder. Het scant niet alleen het bestandssysteem in het algemeen, of zelfs elk afzonderlijk bestand, maar scant in plaats daarvan delen van de interne inhoud van bestanden. Volgens Index Engines zal het berekenen van de entropie op een heel bestand in plaats van op stukjes ervan "alleen extreme versleuteling van het gehele bestand detecteren", oftewel massale versleutelingsgebeurtenissen.⁸⁸

Herstelbaarheid

Op basis van de documentatie beschouwen we herstel met Dell PowerProtect Cyber Recovery als een eenvoudiger, gestroomlijnder proces dan herstel met Rubrik. In dit gedeelte van het rapport, inclusief de subgedeelten, vergelijken we de herstelkenmerken van de twee oplossingen en hoe ze deze kenmerken implementeren.

In de Rubrik-documentatie staat welke van hun herstelfuncties werken voor welke VM-typen. Dit lijkt misschien een nuttig detailniveau, maar de vele bepalingen en variaties maken het herstelproces complex. Als Rubrik-kanten bijvoorbeeld data, bestanden en systemen moeten herstellen, moeten ze selecteren welke objecten in de snapshot ze in het herstelplan willen meenemen. Na het maken van een of meer herstelplannen biedt Rubrik diverse herstelopties, waaronder de volgende:^{89, 90, 91, 92, 93}

- Bestanden herstellen via downloaden of overschrijven en herstellen naar een aparte map, exporteren naar een andere host of exporteren naar een geclusterde service
- Bestanden herstellen voor VM's via downloaden of overschrijven en herstellen naar een aparte map of exporteren naar een andere virtuele machine
- Volledig snapshotherstel van een VM of snapshot van een schijf via het volgende:
 - Live Mount, waarmee een nieuwe VM wordt gemaakt van de snapshot
 - Mount Virtual Disks, waarmee nieuwe virtuele schijven worden gemaakt van de snapshot
 - Instant Recovery, waarbij de huidige VM wordt vervangen door een nieuwe VM die door de snapshot is gemaakt
 - Export, waarmee een nieuwe VM wordt gemaakt van de snapshot in een geselecteerde datastore
 - Batchherstel van VM's
- Cyberherstel in bulk voor herstelplannen via Live Mount en Export
- Rubrik Security Cloud Orchestrated Application-herstel voor VM-noodherstel naar een geïsoleerde sandbox, externe site of op locatie

Rubrik-batchherstel maakt het nog complexer. Tabel 1 toont de batchherstelfuncties die Rubrik biedt, afhankelijk van de hypervisor.⁹⁴

Tabel 1: Rubrik biedt batchherstelfuncties voor verschillende hypervisors. Bron: Rubrik.

Opties voor het maken van VM's				
	Live Mount	Live Mount met optionele migratie	Exporteren	Direct herstel
vSphere-VM's	Beschikbaar, gebruikt het Rubrik-cluster als datastore	Niet beschikbaar	Beschikbaar, gebruikt de datastore van de herstelde hypervisor	Beschikbaar, gebruikt het Rubrik-cluster als datastore
AHV-VM's	Beschikbaar, gebruikt het Rubrik-cluster als datastore	Beschikbaar, gebruikt het Rubrik-cluster als datastore en gebruikt de Nutanix-container voor alle daaropvolgende schrijfbewerkingen	Beschikbaar, gebruikt de Nutanix-container als datastore	Niet beschikbaar
Virtuele machines van Hyper-V	Beschikbaar, gebruikt het Rubrik-cluster als datastore	Niet beschikbaar	Beschikbaar, gebruikt de datastore van de herstelde hypervisor	Beschikbaar, vervangt de huidige VM door een nieuwe vanuit de snapshot. Gebruikt het Rubrik-cluster als datastore.

Voor de Rubrik-oplossing bevindt de herstelde datastore zich meestal in het Rubrik-cluster, niet in de productieomgeving, wat problemen kan veroorzaken. Deze problemen worden in het volgende gedeelte behandeld, “[Rubrik limitations](#)”. PowerProtect kan daarentegen herstelde data in herstel- of productieomgevingen plaatsen om sneller, soepeler herstel te bieden dat downtime tot een minimum kan beperken.

Tabel 2 toont aanvullende informatie van Rubrik over herstel van vSphere-VM's.⁹⁵ Zoals de tabel laat zien, bevinden de meeste vSphere-hersteldatastores zich in het Rubrik-cluster.

Tabel 2: Herstelfuncties die Rubrik biedt voor vSphere-VM's. Bron: Rubrik.

Herstelfuncties die Rubrik biedt voor vSphere				
Actie	Datastore	Stroomtoestand	Netwerk-	Bron VM
Bestanden herstellen	Niet van toepassing	Niet van toepassing	Niet van toepassing	Geen invloed
Live mount	Lokaal Rubrik-cluster	Aan of uit	Niet verbonden	Geen invloed
Mount Virtual Disks	Lokaal Rubrik-cluster	Aan	Niet verbonden	Geen invloed
Direct herstel	Lokaal Rubrik-cluster	Aan	Verbonden (optioneel)	Uitgeschakeld en hernoemd
Exporteren	Datastore van hypervisor	Off (Uit)	Niet verbonden	Geen invloed
Herstel op locatie	Datastore van hypervisor	Aan	Hetzelfde als de bron-VM	Herstel op locatie overschrijft de virtueleschijfbestanden van de bron-VM door de virtueleschijfdata uit de snapshot, zonder de eigenschappen van de VM te wijzigen

De Rubrik-oplossing implementeert niet bulkherstel op grote schaal en de opties voor bulkherstel zijn beperkt en complex. Zoals in het gedeelte “Dell PowerProtect Data Manager offers the equivalent of Rubrik “mass restore”” van dit rapport verder wordt uitgelegd, is Dell PowerProtect gestroomlijnd en eenvoudiger.

De minder goede kant van massaherstel

Rubrik adverteert met massaherstel en definieert dit als het snel herstellen van bedrijfsactiviteiten door apps, bestanden of gebruikers op schaal te herstellen.⁹⁶ Ze bieden veel opties voor bulkherstel. Maar de Rubrik-oplossing slaat de herstelde data meestal in het Rubrik-cluster op en niet in de productieomgeving.⁹⁷ Workloads zijn afhankelijk van de beschikbaarheid van het Rubrik-systeem totdat de oplossing de migratie voltooit. Het lokale Rubrik-cluster is tier 3-storage. Klanten moeten dus een extra migratie naar hun productieomgeving uitvoeren om terug te keren naar de geplande prestatieniveaus. Door dit storingspunt en de verminderde prestaties terwijl het systeem de migratie voltooit, kunnen we het herstel niet als voltooid beschouwen totdat de Rubrik-oplossing de workloads naar de productieomgeving heeft hersteld.

Dell PowerProtect biedt ook bulkherstel door gebruikers in staat te stellen meerdere VM's voor herstel te selecteren in de herstel-UI.

Dell PowerProtect Data Manager biedt het equivalent van 'massaherstel' van Rubrik

Vergeleken met de Rubrik-oplossing biedt de oplossing van Dell ook meerdere vergelijkbare herstelopties voor vSphere-VM's. Dell PowerProtect kan VM-data plaatsen in herstel- of productieomgevingen. De meeste Rubrik-opties plaatsen data alleen in het Rubrik-cluster. Tabel 3 toont de herstelopties van Dell.^{98, 99, 100, 101}

Tabel 3: Herstelopties van Dell. Bron: Principled Technologies.

Herstelopties van Dell	
Type	Over de functie
Herstel op bestandsniveau	Herstelt alleen geïnfecteerde bestanden op locatie of door rollback
Live VM	Herstelt een VM naar het cluster met een latere migratie naar productieomgeving
Herstel naar nieuw	Herstelt naar de oorspronkelijke omgeving of een nieuwe omgeving (bijv. een cleanroom of herstelinfrastructuur), gebruikers kunnen meerdere VM's tegelijk selecteren voor bulkherstel of herstel op schaal
Toegang/ Live VM	Maakt een geïsoleerde kopie van productiedata
Integratie van herstel	Stelt beheerders in staat herstel te plannen of beschikbaar te maken op aanvraag, geeft prioriteit aan automatisch herstel van VM's naar productie- of herstelomgeving

Beperkingen van Rubrik

De Rubrik-oplossing plaatst snapshots die zijn geïnfecteerd met malware in quarantaine voor toekomstige analyse. Maar de Rubrik-oplossing plaatst snapshots niet standaard in quarantaine. Klanten kunnen dan forensische analyses van de in quarantaine geplaatste bestanden zelf downloaden en uitvoeren, handmatig of met tools van derden, waardoor ze mogelijk worden blootgesteld aan malware.^{102, 103}

CyberSense voert zijn analyse uit zonder dat de gebruiker zijn eigen forensische analyse hoeft uit te voeren, en de software automatiseert het maken van herstelpunten.

CyberSense analyseert standaard bestanden en databases. Gebruikers hoeven snapshots niet handmatig in quarantaine te plaatsen. **CyberSense voert de analyse uit zonder dat de gebruiker zelf een forensische analyse hoeft uit te voeren, en de software automatiseert het maken van herstelpunten.**¹⁰⁴

Rubrik-RSC in de RSC-only-beheermodus is een storingspunt voor veel functies. Het meest zorgwekkend is dat een aanval een RSC-serviceonderbreking kan veroorzaken die de internetverbinding of de verbinding tussen de gebruikerslocatie en de RSC beïnvloedt. Na zo'n aanval biedt de oplossing een beperkte reeks functies aan gebruikers, die beschikbaar zijn via de Rubrik CDM UI- of API-gebaseerde automatisering, maar alleen als de gebruikers voorafgaand aan de aanval een RSC-serviceaccount hebben gemaakt.^{105, 106} Een organisatie kan de volgende workloads en data herstellen

zonder de RSC: MongoDB, Microsoft Exchange, bestanden, Hyper-V-snapshots, Live Mount vanuit beheerde volumes, NAS-hostbestanden, Oracle, SQL Server, VCD en VMware.¹⁰⁷ Voor het herstellen van SAP HANA zonder de RSC zijn tools van derden vereist, zoals Studio en Cockpit Cross, en Rubrik-support via de supporttunnel. Voor het herstellen van IBM Db2 zonder de RSC zijn ook IBM-tools van derden en Rubrik-support via de supporttunnel vereist.¹⁰⁸

Air gap/isolatie

NIST definieert een air gap als "een interface tussen twee systemen waarbij (a) ze niet fysiek zijn verbonden en (b) een eventuele logische verbinding niet is geautomatiseerd (d.w.z. dat data alleen handmatig via de interface worden overgedragen, onder menselijke controle)".¹⁰⁹

Air gaps kunnen helpen bij het beheersen van de datastroom van een bron naar een doel en kunnen een belangrijk onderdeel zijn van een strategie voor bescherming tegen ransomware en cyberherstel. Als een aanval of gebeurtenis uw productieback-upsystemen in gevaar brengt, kan de mogelijkheid om verkeer van uw productiesystemen naar beschermde back-ups in uw cyberherstelkluisen te voorkomen, een extra beveiligingslaag bieden.

Fysieke isolatie

Misschien hebt u het voorbeeld van een fysiek geïsoleerde oplossing gezien in de film Mission Impossible, waarbij de hoofdpersoon voorbij alle andere beveiligingsfuncties van het gebouw moest komen om toegang te krijgen tot gevoelige data op een computersysteem dat niet was aangesloten op een extern netwerk. Fysieke isolatie kan ook normaal losgekoppelde segmenten van speciale fysieke netwerken gebruiken om back-upkopieën van uw productiesystemen naar de kluis te transporteren. Als deze operationele air gaps zijn losgekoppeld, vormen ze een fysieke barrière die data niet automatisch kan passeren, waardoor de toegang voor kwaadwillenden moeilijker wordt.

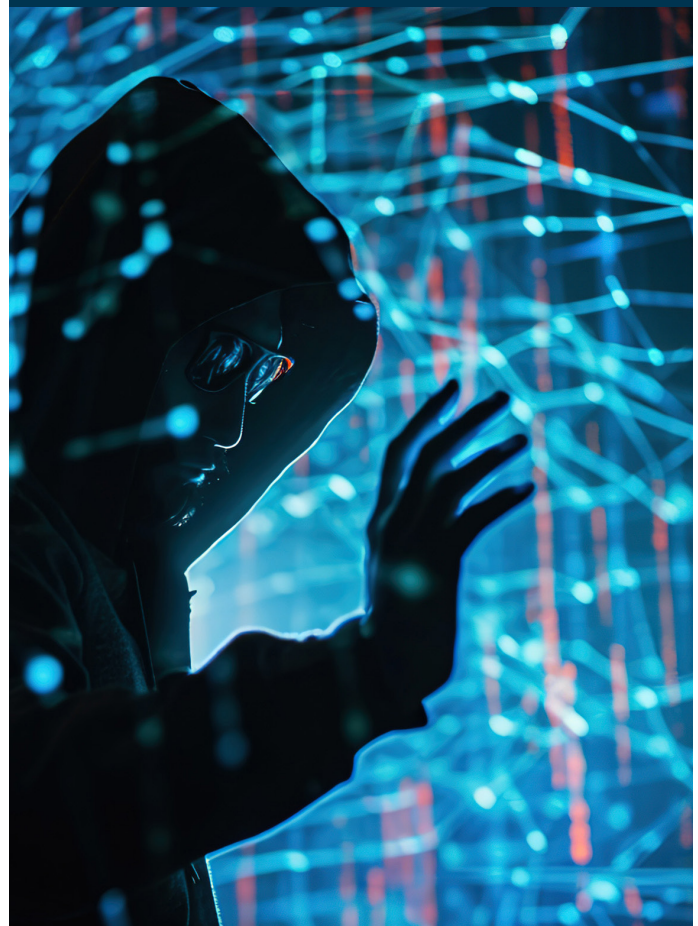
Organisaties kunnen Dell PowerProtect Cyber Recovery fysiek isoleren om een operationele air gap-strategie mogelijk te maken. De oplossing gebruikt een speciale fysieke verbinding en voert datareplicatie uit als een pull-bewerking vanuit de kluis in plaats van een push-bewerking vanuit de back-upoplossing. Tijdens kopiëren/replicatie activeert de oplossing de verbinding en worden de data versleuteld en gemigreerd via de speciale lijn.¹¹⁰ Nadat de replicatie is voltooid, schakelt de oplossing de verbinding opnieuw uit vanaf de kluiszijde. De oplossing maakt kluis kopieën onveranderlijk met beleid voor retentievergrendeling, zodat zelfs als een gebruiker of systeem toegang heeft, deze de kluis kopieën niet kan wijzigen of verwijderen. Beheerverkeer doorloopt het replicatiepad niet, dus **zelfs als kwaadwillenden controle krijgen over uw lokale back-upoplossing, start en verbreekt de kluis het replicatiepad en gebruikt het eenrichtingspulls met alleen gegevens vanuit de gegevensbron, waardoor directe toegang tot de kluis wordt beperkt.**¹¹¹

Logische isolatie

Logische isolatie daarentegen gebruikt systemen die zich misschien op hetzelfde fysieke netwerk bevinden, maar zorgt voor logische netwerkscheiding en -controle om ervoor te zorgen dat systemen geen data naar elkaar kunnen sturen. De oplossing gebruikt extra beveiligingsimplementaties, zoals versleuteling en hashing, samen met RBAC en meervoudige verificatie, om ervoor te zorgen dat een onbevoegd systeem of onbevoegde gebruiker de data in een ander systeem niet kan lezen.

Rubrik beschrijft de functie voor cyberherstel als het gebruik van een logische air gap-strategie.^{112, 113} Veel van de beschikbare openbare uitspraken van Rubrik roepen twijfels op over de noodzaak van air gaps. In een Rubrik-presentatie met de titel "Rubrik Security – Air Gap and Immutability" wordt beweerd dat hun systeemeigen oplossing air gap heeft, omdat er geen manier is om de back-ups te openen of te bewerken zodra de oplossing ze heeft gemaakt, zelfs al blijft het Rubrik-apparaat verbonden met het fysieke netwerk.¹¹⁴ Een geverifieerde kwaadwillende kan echter nog steeds toegang krijgen tot de GUI van het apparaat, wat gevolgen kan hebben voor het herstel. Om dit te beperken, gebruikt Rubrik retentievergrendelingen die voorkomen dat back-ups verlopen, waardoor ze onveranderlijk zijn. Na inschakeling voorkomen retentievergrendelingen ook dat een Rubrik-cluster wordt teruggezet naar fabrieksinstellingen en wordt gewist. Volgens de Rubrik CDM Security Guide schakelt de oplossing wereldwijd standaard retentievergrendelingen in het cluster uit en moeten klanten contact opnemen met Rubrik-support om ze in te schakelen.¹¹⁵ Openbaar beschikbare bronnen geven niet aan of Rubrik-support ook retentievergrendelingen kan uitschakelen, waardoor een geautoriseerde kwaadwillende nog steeds de beveiligingslagen zou kunnen omzeilen.

Beheerverkeer doorloopt het replicatiepad niet, dus zelfs als kwaadwillenden controle krijgen over uw lokale backupoplossing, start en verbreekt de kluis het replicatiepad en gebruik het eenrichtingspulls met alleen gegevens vanuit de gegevensbron, waardoor directe toegang tot de kluis wordt beperkt.





Conclusie

Organisaties moeten actief rekening houden met tal van aanvalsmogelijkheden op hun datacenters. Een goed plan voor databescherming beschermt alle data, met name de data die essentieel is voor de bedrijfsactiviteiten. We hebben de openbaar beschikbare informatie voor Dell PowerProtect Cyber Recovery en Rubrik Secure Cloud bekeken om te zien hoe beide oplossingen databeheer, bescherming en herstel aanpakken.

PowerProtect Cyber Recovery isoleert fysiek back-upkopieën van kritieke data in een kluis en zorgt voor herstelbaarheid in het geval van een cyberaanval. De oplossing gebruikt een operationele air gap-strategie met fysieke isolatie, iets wat Rubrik Secure Cloud niet kan bieden. Deze oplossing gebruikt namelijk logische isolatie.

Cyber Recovery gebruikt ML-gebaseerde analyses in CyberSense om de integriteit van data in de kluis te beoordelen en schone back-updata te identificeren voor herstel. Rubrik Secure Cloud biedt daarentegen een ML-getrainde analysetool die naar afwijkingen zoekt in plaats van diepe scans op bestanden uit te voeren.

Bovendien biedt de Cyber Recovery-oplossing meerdere herstelopties, waarbij gebruik wordt gemaakt van schone data uit de kluis om een efficiënte en naadloze terugkeer naar de bedrijfsvoering mogelijk te maken. In veel gevallen kan PowerProtect Cyber Recovery functies en voordelen bieden die Rubrik Secure Cloud niet heeft, waardoor dit mogelijk een veiligere oplossing is die dieper kan analyseren, om downtime te minimaliseren en herstel te versnellen.

1. Anastasia Dergacheva and Jesse R. Taylor, "Study Finds Average Cost of Data Breaches Continued to Rise in 2023", geraadpleegd op 25 juli 2024, <https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023>.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", geraadpleegd op 18 april 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf>.
3. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
4. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", geraadpleegd op 18 april 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf>.
5. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", geraadpleegd op 18 april 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf>.
6. Rob Emsley, "Public Cloud Vault to Secure, Isolate and Recover Data", geraadpleegd op 20 maart 2024, <https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/>.

7. Brian White, "Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure", geraadpleegd op 20 maart 2024, <https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/>.
8. Dell, "Cyber Recovery on Google Cloud Platform", geraadpleegd op 20 maart 2024, <https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/>.
9. Chris Mellor, "Up to \$5m compensation if Rubrik Cloud Vault recovery busted", geraadpleegd op 20 maart 2024, <https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/>.
10. Kristina Avrionova, "Frequently Asked Questions about Rubrik Cloud Vault", geraadpleegd op 20 maart 2024, <https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault>.
11. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", geraadpleegd op 22 maart 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf>.
12. Dell, "Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability", geraadpleegd op 7 juni 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invol-arch-wp.pdf>.
13. Dell, "Consolidate Governance and Compliance Archive Data", geraadpleegd op 4 april 2024, <https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/>.
14. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", geraadpleegd op 24 maart 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf>.
15. Rubrik, "Retention-locked SLA Domain attributes", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, "Rubrik Cyber Recovery", geraadpleegd op 20 maart 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf>.
17. Rubrik, "Rubrik Licensing: Subscribe to Simplicity", geraadpleegd op 20 maart 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf>.
18. Rubrik, "Workloads require third-party tools for recovery", geraadpleegd op 6 mei 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, "Recoverable workloads during RSC service disruption", geraadpleegd op 6 mei 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, "Workloads require third-party tools for recovery".
21. Dell, "Strengthen your security posture with Managed Detection and Response", geraadpleegd op 2 april 2024, <https://www.delltechnologies.com/asset/nl-nl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf>.
22. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide", geraadpleegd op 20 maart 2024, https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide".
24. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide".
25. Dell, "Installing CyberSense in Dell PowerProtect Cyber Recovery", geraadpleegd op 20 maart 2024, <https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/>.
26. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
27. Rubrik, "Downloading and installing Rubrik CDM", geraadpleegd op 20 maart 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, "Setting up a Rubrik cluster using the UI", geraadpleegd op 20 maart 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, "Setting up a Rubrik cluster using the CLI", geraadpleegd op 20 maart 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, "Registering Rubrik clusters using the online method", geraadpleegd op 20 maart 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, "Registering Rubrik clusters using the offline method", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, "Enabling MFA", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, "Adding the initial account", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.

34. TrustRadius, "Learning Rubrik by putting the pieces together Brik by Brik", geraadpleegd op 21 maart 2024, <https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04>.
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
36. Index Engines, "CyberSense®: How it Works", geraadpleegd op 21 maart 2024, <https://www.indexengines.com/how-it-works>.
37. Rubrik, "Anomaly event details", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, "Events page", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, "RSC Data Threat Analytics", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, "RSC Data Threat Analytics".
41. Dell Technologies, "Dell PowerProtect Cyber Recovery: Reference Architecture", geraadpleegd op 6 mei 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf>.
42. Dell Technologies, "Dell EMC Avamar for Hyper-V", geraadpleegd op 16 mei 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf>.
43. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V", geraadpleegd op 16 mei 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf>.
44. VMware, "Accelerate IT. Innovate with your cloud.", geraadpleegd op 9 mei 2024, <https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf>.
45. Statista, "Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024", geraadpleegd op 17 juli 2024, <https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/>.
46. Rubrik, "RSC Data Threat Analytics".
47. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery", geraadpleegd op 27 juni 2024, <https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf>.
48. Rubrik, "RSC Data Threat Analytics".
49. Index Engines, "CyberSense® Support Matrix", geraadpleegd op 21 maart 2024, <https://www.indexengines.com/csmatrix>.
50. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery".
51. Rubrik, "Keep Your Databases Running in the Face of Any Threat".
52. Index Engines, "CyberSense® Support Matrix".
53. Dell Technologies, "Dell EMC Avamar for Hyper-V".
54. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V".
55. Rubrik, "Anomaly incidents", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, "Data Threat Analytics events", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, "Viewing Anomaly Detection", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, "VM Encryption Detection", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, "Viewing the Threat Monitoring page", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, "Initiating a threat hunt", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, "Quarantining matched files or objects", geraadpleegd op 2 april 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, "CyberSense® for PowerProtect Cyber Recovery".
63. Dell, "CyberSense® for PowerProtect Cyber Recovery".
64. Index Engines, "The Power of CyberSense's Machine Learning", geraadpleegd op 2 april 2024, <https://go.indexengines.com/csmachinelearning>.
65. Index Engines, "The Power of CyberSense's Machine Learning".
66. Index Engines, "The Power of CyberSense's Machine Learning".
67. Dell, "CyberSense® for PowerProtect Cyber Recovery".
68. Rubrik, "Anomaly Detection behavioral model", geraadpleegd op 20 mei 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, "Training ML Models", geraadpleegd op 2 april 2024, <https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html>.
70. Rubrik, "Defense in Depth with Polaris Radar", geraadpleegd op 21 maart 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf>.

71. Rubrik, "Data Threat Analytics dashboard", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, "Initiating a threat hunt", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, "What Is A Malware File Signature (And How Does It Work)?", geraadpleegd op 4 april 2024, <https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/>.
74. Rubrik, "Threat hunts", geraadpleegd op 21 maart 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, "Anomaly Detection features", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, "Behavioral model".
77. Index Engines, "The Power of CyberSense's Machine Learning".
78. Dell, "CyberSense® for PowerProtect Cyber Recovery".
79. Rubrik, "Behavioral model".
80. Rubrik, "Anomaly Detection features".
81. Rubrik, "Behavioral model".
82. Dell, "CyberSense® for PowerProtect Cyber Recovery".
83. Morningstar, "Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery", geraadpleegd op 17 juli 2024, <https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery>.
84. Rubrik, "Threat Monitoring", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, "The Power of CyberSense's Machine Learning".
86. Index Engines, "The Power of CyberSense's Machine Learning".
87. Rubrik, "Anomaly Detection features", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, "The Power of CyberSense's Machine Learning".
89. Rubrik, "Investigating and recovering anomalous files for filesets", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, "Investigating and recovering anomalous files for virtual machines", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, "Full snapshot recovery of a virtual machine", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, "Recovery of a batch of virtual machines", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, "Performing bulk recovery for Recovery Plans", geraadpleegd op 22 maart 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, "Recovery of a batch of virtual machines", geraadpleegd op 4 april 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, "Recovery of virtual machines", geraadpleegd op 16 april 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. De herstelde datastore bevindt zich meestal in het Rubrik-cluster, niet in de productieomgeving.
97. Rubrik, "Recovery of a batch of virtual machines", geraadpleegd op 16 april 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, "Restore plan", geraadpleegd op 16 april 2024, <https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/>.
99. Dell, "PowerProtect Data Manager overview", geraadpleegd op 16 april 2024, <https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/>.
100. Dell, "PowerProtect Data Manager 19.9 Administration and User Guide", geraadpleegd op 16 april 2024, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, "Recovery Orchestration with PowerProtect Data Manager Overview", geraadpleegd op 16 april 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, "Quarantine files or objects", geraadpleegd op 24 maart 2024, <https://docs.rubrik.com/en-us/saas/saas/quarantine.html>.
103. Rubrik, "Downloading quarantined files for forensic analysis", geraadpleegd op 24 maart 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, "The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery", geraadpleegd op 16 april 2024, <https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf>.

105. Rubrik, "Workload recovery during an RSC service disruption", geraadpleegd op 16 april 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.
106. Rubrik, "Rubrik CDM APIs and service account workflows", geraadpleegd op 16 april 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.
107. Rubrik, "Recoverable workloads during RSC service disruption", geraadpleegd op 16 april 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
108. Rubrik, "Workloads require third-party tools for recovery", geraadpleegd op 16 april 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
109. NIST, "Computer Security Resource Center Glossary: air gap", geraadpleegd op 29 juli 2024, https://csrc.nist.gov/glossary/term/air_gap.
110. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
111. Dell, "Dell PowerProtect Cyber Recovery: Reference Architecture".
112. Adam Eckerle, "Debunking the Myths about Air Gaps", geraadpleegd op 14 maart 2024, <https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps>.
113. Rubrik, "Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value", geraadpleegd op 14 maart 2024, <https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf>.
114. Brian Williams, "Rubrik Air Gap and Immutability", geraadpleegd op 14 maart 2024, <https://vimeo.com/561870246>.
115. Rubrik, "Retention locks in the Rubrik cluster", geraadpleegd op 18 maart 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

► Bekijk de oorspronkelijke, Engelse versie van dit rapport op

Dit project is uitgevoerd in opdracht van Dell Technologies.



Facts matter.®

Principled Technologies is een geregistreerd handelsmerk van Principled Technologies, Inc. Alle andere productnamen zijn de handelsmerken van hun respectieve eigenaren.

NIET-AANSPRAKELIJKHEIDSVERKLARING; BEPERKING VAN AANSPRAKELIJKHEID:

Principled Technologies, Inc. heeft redelijke inspanningen geleverd om zorg te dragen voor de nauwkeurigheid en geldigheid van de tests. Principled Technologies, Inc. biedt evenwel geen uitdrukkelijke dan wel geïmpliceerde garanties met betrekking tot de testresultaten en -analyses en de nauwkeurigheid, volledigheid of kwaliteit daarvan, met inbegrip van geïmpliceerde garanties voor de geschiktheid voor een bepaald doel. Alle personen of rechtspersonen die vertrouwen op de resultaten van deze tests, doen dit op hun eigen risico en aanvaarden dat Principled Technologies, Inc., haar werknemers en haar onderaannemers niet aansprakelijk zijn voor claims met betrekking tot verlies of schade naar aanleiding van vermeende fouten of gebreken in testprocedures of -resultaten.

Principled Technologies, Inc. zal in geen geval aansprakelijk zijn voor gevolg-, indirecte, speciale of incidentele of schade met betrekking tot de tests, zelfs als Principled Technologies, Inc. is gewezen op de mogelijkheid van dergelijke schade. De aansprakelijkheid van Principled Technologies, Inc. is in elke situatie beperkt tot het bedrag dat is betaald in verband met de tests door Principled Technologies, Inc. De klant beschikt alleen over de verhaalsmogelijkheden die hier worden vermeld.