Verbeter de cybertolerantie en bescherm data tegen cyberransomware-bedreigingen met behulp van een geïsoleerde kluis, op AI gebaseerde ML-analysesoftware en meer

Met Dell Technologies PowerProtect Cyber Recovery met CyberSense

Naarmate de frequentie van cyberdreigingen voortdurend toeneemt en aanvalsmethoden evolueren, moeten databeschermingsplannen een aanpak hanteren die alle IT-componenten beveiligt en analyseert, van het meest oppervlakkige tot het diepste bereik. Dell PowerProtect Cyber Recovery kan helpen de meest kritieke en gevoelige data te beschermen en tegelijkertijd te zorgen voor correct herstel bij een cyberaanval of een andere verstorende gebeurtenis.

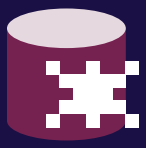
Dell PowerProtect Cyber Recovery is een oplossing voor databeheer, -bescherming en -herstel die organisaties helpt hun data en applicaties te beschermen tegen ransomware, destructieve cyberaanvallen en onverwachte gebeurtenissen. De oplossing maakt gebruik van een multi-copy aanpak, wat betekent dat na het maken van back-ups deze naar geïsoleerde storage worden gekopieerd voor beveiliging en analyse. PowerProtect Cyber Recovery bestaat uit vele componenten, waaronder één of meer storagekluizen, die mogelijk zowel on-premises als in de cloud geïmplementeerd kunnen worden in een PowerProtect DD (voorheen bekend als Data Domain) apparaat of in de cloud via softwarematige Dell APEX Protection Storage for Public Cloud (voorheen bekend als DD Virtual Edition). In beide gevallen is de kluis operationeel 'air-gapped', d.w.z. geïsoleerd van de productieomgeving. Mogelijk fysiek 'air-gapped' in het geval van de on-premises omgeving en logisch 'air-gapped' in het geval van de APEX-omgeving. Dit maakt het uiterst moeilijk voor kwaadwillenden of onbevoegde gebruikers om zich aan te melden en back-upkopieën te compromitteren.

PowerProtect Cyber Recovery bevat ook CyberSense, een volledig geautomatiseerde en geïntegreerde intelligente engine voor beveiligingsanalyse die automatisch data, bestanden, databases en images in de kluis scant op tekenen van beschadiging door een ransomware-aanval. CyberSense biedt volledige contentanalyse; gebruikt observaties uit bestanden als input voor zijn kunstmatige intelligentie (AI)-gebaseerde machine learning (ML)-model; en detecteert schadelijke activiteiten, waaronder massale verwijderingen, encryptie en andere verdachte wijzigingen in de kerninfrastructuur (waaronder Active Directory en DNS), gebruikersbestanden en kritieke productiedatabases die kunnen duiden op ransomware of een destructieve aanval. Wanneer CyberSense corruptiepatronen detecteert, genereert het een waarschuwing in het PowerProtect Cyber Recovery-dashboard dat aanvullende informatie geeft over de schaal en impact van de aanval.[1]

PowerProtect Cyber Recovery helpt organisaties cyberaanvallen te beperken, de veerkracht van data te verbeteren met meerdere kopieën van databack-ups vanaf verschillende locaties, downtime te verminderen en bedrijfscontinuïteit te behouden. Dit rapport gebruikt openbaar beschikbare data om belangrijke functies en functionaliteit voor databescherming te belichten en presenteert onze bevindingen uit een concurrerende analyse van CyberSense.

Bescherm gevoelige data

Versleutel actieve data tijdens back-upreplicatie naar fysiek en logisch geïsoleerde kluizen



Detecteer beschadiging van SQL Server-pagina

CyberSense vond een infectie waar een concurrerende oplossing niet in slaagde

Identificeer onbeschadigde back-upkopieën

CyberSense heeft de meest recente niet-geïnfecteerde back-upkopie voor herstel geïdentificeerd

Beveiliging

Dell PowerProtect Cyber Recovery biedt verschillende beveiligingsfuncties om kritieke data te beschermen tegen ransomware en andere geavanceerde bedreigingen, te voorkomen dat onbevoegde gebruikers toegang krijgen tot gevoelige informatie en om herstel snel te laten verlopen, zodat organisaties hun normale activiteiten kunnen hervatten.

De kenmerken en functionaliteiten van PowerProtect Dd-toepassingen kunnen cruciaal zijn voor de beveiliging, integriteit en herstel die PowerProtect Cyber Recovery-oplossingen leveren. Het gaat om functies zoals:

1. **Onveranderlijkheid**
   Onveranderlijke data kunnen niet worden gewijzigd of verwijderd, alleen worden geschreven. DD-systemen kunnen onveranderlijke back-ups schrijven op zowel productiesystemen als in de Cyber Vault. Dat betekent dat als een kwaadwillende op een of andere manier toegang krijgt tot het back-upsysteem, deze de bestaande beschermde kopieën niet kan wijzigen, verwijderen of aantasten.[2] Elke back-up die het DD-systeem maakt in de productieomgeving is onmiddellijk onveranderlijk en beschikbaar voor IT om naar de kluis te kopiëren voor extra beveiliging. In het volgende gedeelte van dit rapport wordt meer aandacht besteed aan onveranderlijkheid.

2. **Retention Lock**
   De DD Retention Lock-functie maakt data onveranderlijk voor een vooraf bepaalde periode. Zodra de oplossing data onder een retentievergrendeling plaatst, kan geen enkele gebruiker of systeem de data wijzigen of, verwijderen totdat de vergrendelingsperiode is verstreken.[3]

   Retention Lock heeft governance- en nalevingsmodi. De nalevingsmodus kan klanten in staat stellen te voldoen aan veel wettelijke normen. Een onafhankelijke externe partij heeft verklaard dat DD Retention Lock voldoet aan de storagevereisten die zijn gespecificeerd in SEC-regels 17a-4(f)(2) en 240.18a-6(e)(2) en FINRA-regel 4511(c).[4] Deze voorziening kan ook helpen om de inspanningen van een organisatie te ondersteunen om te voldoen aan FDA 21 CFR Part11, Sarbanes-Oxley Act, IRS 98025 en 97-22, ISO Standard 15489-1 en MoREQ2010.[5]

   Omdat aanvallers kunnen proberen Retention Lock te omzeilen door de klok van een systeem te wijzigen, waardoor de oplossing bestanden eerder dan verwacht verwijdert, heeft DD een interne beveiligingsklok. Het systeem vergelijkt regelmatig de tijden van de beveiliging en de systeemklokken. Als er in één kalenderjaar een totale afwijking van twee weken tussen de twee is, schakelt het systeem automatisch het DDFS (DD File System) uit om toegang tot data te voorkomen.[6]

3. **Versleuteling van actieve data met DDBoost**
   Actieve data kunnen een aanzienlijk beveiligingsrisico vormen. DDBoost beperkt de hoeveelheid actieve data door de back-upserver of applicatieclient in staat te stellen om alleen unieke datasegmenten, in plaats van alle data, over het netwerk naar het DD-toepassing te verzenden. Bovendien kunnen organisaties het DDBoost-protocol gebruiken met of zonder certificaten voor verificatie en versleuteling van data. Certificaten bieden een veiliger datatransport. Met versleuteling voor actieve data kunnen applicaties actieve back-up versleutelen of data herstellen via LAN vanaf het systeem. De client kan Transport Layer Services (TLS) gebruiken om de sessie tussen de client en het systeem te versleutelen.[7]

4. **DD Operating System (DD OS)-beveiliging**
   DD-beveiligingsfuncties gelden ook voor het besturingssysteem. DD OS implementeert aangepaste toegangscontroles en beperkingen op de Bash-shell voor beveiligingsdoeleinden. Met de beperkte Bash-shellmodus kunnen gebruikers alleen een reeks vooraf gedefinieerde opdrachten uitvoeren die nodig zijn voor hun rollen en taken. DD OS verbetert de data-integriteit door ongedefinieerde opdrachten te blokkeren die ongeautoriseerde of onbedoelde wijzigingen aan het systeem aanbrengen.[8]

5. **Op rollen gebaseerde toegangscontrole (RBAC) en DD-bestandssysteem (DDFS)-beveiliging**
   DD-systemen gebruiken verschillende maatregelen om bestanden en data binnen het bestandssysteem te beschermen. Ten eerste bieden DD-systemen RBAC, waarmee beheerders rollen met specifieke bevoegdheden kunnen definiëren en gebruikers aan deze rollen kunnen toewijzen. Alleen geautoriseerde gebruikers met de juiste bevoegdheden hebben toegang tot het apparaat en de bijbehorende data. Dit zorgt ervoor dat gebruikers alleen toegang hebben tot de functies en data die ze nodig hebben om hun taken uit te voeren, waardoor het risico op onbevoegde toegang of onbedoelde blootstelling van data wordt verminderd.

   DDFS maakt ook gebruik van hashing voor data-integriteitsverificatie. Hashing zet een bepaalde sleutel of tekenreeks om in een andere waarde. Het apparaat slaat unieke datablokken op in logische storagecontainers en het bestandssysteem hasht zowel de datablokken als de containers. Wanneer het systeem data ophaalt, wordt de hash-waarde van de data opnieuw berekend om overeen te komen met de opgeslagen hash-waarde in DDFS, wat ervoor zorgt dat er niets met de data is geknoeid of beschadigd.[9]

6. **Autorisatie met dubbele rol**
   Wanneer een organisatie de DD Retention Lock-nalevingsmodus inschakelt, biedt het DD-systeem extra beheerbeveiliging in de vorm van dubbele aanmelding. Dit betekent dat zowel de systeembeheerder als een tweede geautoriseerde gebruiker (bijv. de beveiligingsfunctionaris) zich samen moeten aanmelden. Het mechanisme voor dubbele aanmelding van de DD Retention Lock-nalevingsmodus fungeert als bescherming tegen acties die de integriteit van vergrendelde bestanden kunnen aantasten voordat de bewaarperiode is verlopen.[10]

7. **Data Invulnerability Architecture**
   Het DD-besturingssysteem biedt end-to-end verificatie, foutvermijding en -beheersing, continue foutdetectie en -herstel en herstelbaarheid van het bestandssysteem om te beschermen tegen problemen met data-integriteit die worden veroorzaakt door hardware- en softwarestoringen. Wanneer het DD-systeem schrijfaanvragen van back-upsoftware ontvangt, analyseert het eerst een datasegment op redundantie door de vingerafdruk voor het datasegment te berekenen en deze te vergelijken met bestaande vingerafdrukken die in het systeem zijn opgeslagen. Het slaat alleen unieke datasegmenten en hun vingerafdrukken op schijf op. DD leest vervolgens voortdurend data terug van de schijf, berekent de vingerafdruk die wordt teruggelezen en zorgt ervoor dat deze overeenkomt met de vingerafdruk op de schijf. Het DD-systeem voert een zelfherstelproces uit om beschadigde data te reconstrueren en data naar de juiste status te herstellen als het systeem tijdens dit proces beschadiging detecteert (d.w.z. als wat het terugleest niet overeenkomt met wat er is geschreven). Bovendien helpt het zelfherstelproces het systeem te beschermen tegen andere wijzigingen die van invloed kunnen zijn op de integriteit van het platform.

Onveranderlijkheid*

Het onveranderlijk maken van back-ups zorgt ervoor dat een organisatie deze back-ups kan vertrouwen voor herstel. Operationeel gezien helpt onveranderlijkheid de authenticiteit en betrouwbaarheid van data te behouden.

*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.

Hoe het werkt

DD-systemen bieden onveranderlijkheid in de manier waarop ze data opslaan met behulp van MTrees. MTrees zijn logische partities van het bestandssysteem. Wanneer een applicatie data naar een MTree schrijft, gebruikt het DD-systeem een functie genaamd Fast Copy om een point-in-time-kopie van de oorspronkelijke MTree naar een nieuwe MTree te maken. Binnen de nieuwe MTree past DD Retention Lock toe om ervoor te zorgen dat een gebruiker of proces de nieuwe MTree niet kan verwijderen gedurende de duur die is gedefinieerd door de retentieperiode. De nieuwe MTree is een onveranderlijke kopie van data en is onafhankelijk van de oorspronkelijke MTree.[11]

PowerProtect Cyber Recovery-oplossingen gebruiken ook MTree-replicatie om onveranderlijke datakopieën te kopiëren van een productie-DD naar een andere DD in de kluis via het DDBoost-protocol.[12] Bij de eerste synchronisatie tussen de twee DD's kopieert de oplossing alle data naar de kluis-DD. Bij elke volgende synchronisatie worden alleen nieuwe en gewijzigde datasegmenten gekopieerd. CyberSense, dat we later in dit rapport bespreken, scant alle onveranderlijke kopieën in de kluis op mogelijke beschadiging.

Benaderingen van onveranderlijkheid

De noodzaak om onveranderlijke back-ups te verwijderen is zeldzaam, maar het scenario komt voor. Organisaties kunnen te maken krijgen met capaciteitsproblemen en de daaruit voortvloeiende kosten nadat ze onveranderlijke back-ups hebben verzameld die ze niet kunnen verwijderen. Het opslaan van back-ups kan een grote hoeveelheid capaciteit vereisen, wat op zijn beurt doorlopende operationele, beheer- en bewakingskosten vereist naast de initiële hardware-investering. Het periodiek verwijderen van onveranderlijke back-ups kan helpen deze problemen op te lossen.

Zoals we al hebben opgemerkt, biedt Dell PowerProtect Cyber Recovery onveranderlijkheid door gebruik te maken van Retention Lock en andere tools. Retention Lock biedt enige flexibiliteit omdat de twee modi, naleving en governance, kleine wijzigingen bieden in de manier waarop klanten onveranderlijkheid kunnen implementeren. Onveranderlijkheid betekent dat gebruikers of kwaadwillenden geen back-ups kunnen verwijderen, maar in bepaalde gevallen, zoals problemen met de storagecapaciteit, kunnen klanten met PowerProtect Cyber Recovery deze verwijderen met de Retention Lock – Governance-modus.

Hoe presteren vergelijkbare oplossingen van andere bedrijven in vergelijking met PowerProtect Cyber Recovery? We hebben naar openbaar beschikbare informatie gekeken voor Cohesity Cyber Recovery, Veeam, Rubrik en Veritas NetBackup. Behalve Cohesity Cyber Recovery kunnen de oplossingen zowel on-premise als off-site geïmplementeerd worden (Cohesity is een cloud-gebaseerde oplossing die ondersteund wordt door AWS). Documentatie voor de vier oplossingen beweren onveranderlijkheid te bieden, maar opvallend genoeg verschillen Rubrik en NetBackup op een aantal punten van PowerProtect Cyber Recovery.

Voor Rubrik kunnen beheerders back-ups verwijderen, maar niet vanaf de clientzijde en alleen met bepaalde besturingselementen. Bovendien zijn alle schrijfacties "out-of-place", wat betekent dat nieuwe schrijfacties nooit eerder geschreven data beïnvloeden.[13]

Ondanks het bieden van onveranderlijkheid kunnen beheerders of kwaadwillenden de vergrendeling op back-ups in een storage die geschikt is voor NetBackup WORM verwijderen. Vervolgens kunnen ze de image verwijderen met de opdracht bpexpdate.[14]

Isolatie

Data-isolatie verwijst naar de scheiding van en beperkte toegang tot data die worden gecreëerd door barrières of grenzen om onbevoegde toegang te voorkomen. Isolatie maakt gebruik van tijdelijke netwerkverbindingen in plaats van permanente verbindingen.

Dankzij data-isolatie blijven kritieke data los van een geïnfecteerd netwerk, om te voorkomen dat kwaadwillenden configuraties kunnen wijzigen, data kunnen verwijderen, beleid kunnen wijzigen of het netwerkverkeer kunnen bespieden op zoek naar gebruikersreferenties. Isolatie helpt ook het aanvalsoppervlak te verminderen, waardoor kwaadwillenden minder kansen krijgen om toegang en controle te krijgen. Bovendien kunnen organisaties de toegang beperken tot alleen geautoriseerd personeel, wat helpt voorkomen dat onbevoegde gebruikers data overschrijven.

Naast de functies die we hebben opgemerkt, kan PowerProtect Cyber Recovery zowel fysieke als logische isolatie bieden, in de vorm van operationele air gaps, om data te beschermen. PowerProtect Cyber Recovery kan zowel een fysieke air gap gebruiken, waarbij de back-updata fysiek losgekoppeld zijn van het productienetwerk en opgeslagen zijn op een geïsoleerde locatie, als een logische air gap, die afhankelijk is van netwerktoegangscontroles om de logisch losgekoppelde back-upkopieën te scheiden van de productieomgeving. Beide typen air gaps zijn waardevol omdat een logische air gap alleen niet kan voorkomen dat een interne gebruiker met netwerktoegang tot de kluis toegang krijgt tot de data en deze in gevaar brengt.

Een fysiek geïsoleerde on-premise PowerProtect DD kan functioneren als de kluis, waarin gebruikers of systemen uit de productieomgeving geen toegang hebben tot de componenten en de kluis fysiek is losgekoppeld van het productienetwerk.[15] Door de toegang tot de herstelomgeving vanuit het productienetwerk te elimineren, kan een organisatie het aanvalsoppervlak verkleinen. Zoals opgemerkt, vereist toegang tot de geïsoleerde data afzonderlijke beveiligingsreferenties en meervoudige verificatie (MFA).[16]

Benaderingen van isolatie

Gartner stelt: "Geïsoleerde herstelomgevingen (IRE's) met onveranderlijke datakluizen (IDV's) bieden het hoogste niveau van beveiliging en herstel tegen bedreigingen van binnenuit, ransomware en andere vormen van hacking."[17] Ze merken ook op dat een "IRE met een IDV niet de traditionele back-upsystemen en herstel na noodgeval (DR) vervangt, maar aanvult door een tertiaire onveranderlijke back-upkopie te leveren in een IRE die is uitgerust met alle tools, processen en resources om getroffen systemen te herstellen."[18]

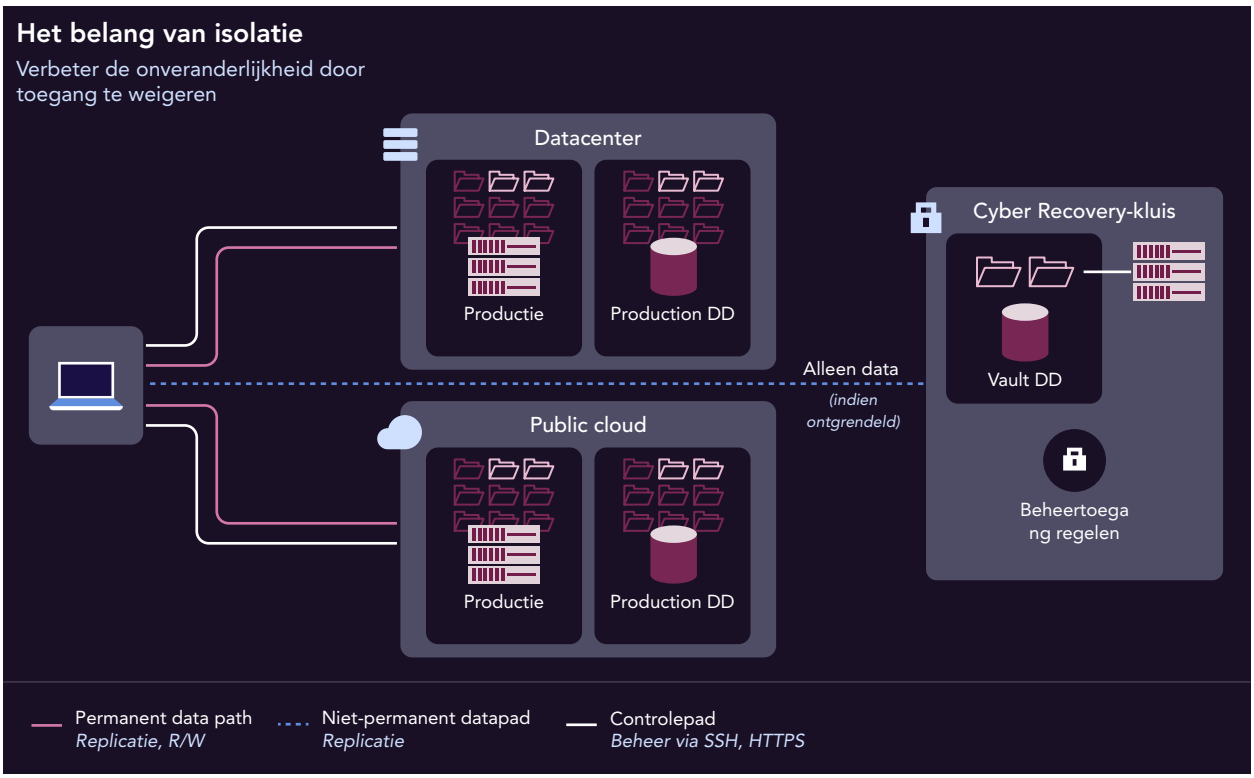
Tijdens het bekijken van openbaar beschikbare informatie over de oplossingen van Cohesity, Veeam, Rubrik en Veritas, ontdekten we dat elke oplossing ten minste een iets andere benadering van IRE heeft dan PowerProtect Cyber Recovery. Met de Dell oplossing kunnen klanten hun DD-kluizen fysiek of logisch isoleren van de productie om de controle en datalagen van de productie gescheiden te houden van de kluizen. Bovendien automatiseert PowerProtect Cyber Recovery air gaps, iets wat niet alle andere oplossingen doen.

Volgens documentatie:

- Cohesity Cyber Recovery biedt slechts een dynamische automatische logische air gap voor hun AWS-gebaseerde FortKnox-kluis.[19]
- Veeam ondersteunt een logische air gap voor public en private cloud-providers via Veeam Cloud Connect, maar het is niet geautomatiseerd. Veeam biedt ook Veeam Hardened Repository, die fungeert als de on-premise kluis voor de oplossing en die organisaties kunnen configureren om een fysieke air gap te hebben.[20]
- Rubrik biedt geen automatische air gap voor Rubrik Cloud Vault, maar klanten kunnen een logische air gap toevoegen via een samenwerkingsverband met Microsoft.[21]
- NetBackup-klanten moeten handmatig een logische air gap inschakelen en kunnen een fysieke air gap creëren met een on- of off-premise oplossing.[22]

Hoe het werkt

Afbeelding 1 toont de netwerkpaden van de geïsoleerde Cyber Recovery-kluis. Houd er rekening mee dat de kluis geen beheer- of controlepad naar de productieomgeving heeft om het aanvalsvlak te verminderen.



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

De enige vereiste verbinding voor de Cyber Recovery-kluis is een datapad voor periodieke datasynchronisatie. Synchronisatie is wanneer de Cyber Recovery-oplossing data opneemt in korte, beleidsgestuurde intervallen voor replicatie.[23] In de PowerProtect Cyber Recovery handleiding met oplossingen staat dat "de architectuur van de Cyber Recovery-oplossing op basisniveau bestaat uit twee PowerProtect DD-systemen en de Cyber Recovery-beheerhost. In deze configuratie op basisniveau schakelt de Cyber Recovery-software, die op de beheerhost wordt uitgevoerd, de Ethernet-interface voor replicatie in en uit, samen met replicatiecontexten op het PowerProtect DD-systeem in de Cyber Recovery-kluis om de stroom van data van de productieomgeving naar de kluisomgeving te beheren."[24] Dell stelt extra manieren voor waarop organisaties datapaden kunnen beveiligen en isoleren. We hebben in onze tests waargenomen dat Cyber Recovery de kluis ontgrendelde en vergrendelde tijdens en na replicatie.

Voor de fysieke implementatie van de kluis raadt Dell aan "de Cyber Recovery-kluisapparatuur te installeren in een speciale ruimte met fysieke toegangscontroles. Deze beveiligde ruimte moet een lijst met beperkte toegang hebben met een sleutel of toegang voor twee personen. Videobewaking van de toegangspunten tot de ruimte en van de apparatuur moet aanwezig zijn. Voor de beste beveiliging moet de Cyber Recovery-software alleen toegankelijk zijn via fysieke toegang tot de Cyber Recovery-beheerserver en een bijbehorend toetsenbord en muis."[25]

Met de scheiding van de beheer- en controlepaden onderscheiden de fysieke en logische isolatieopties van Cyber Recovery zich van andere oplossingen. Sommige oplossingen bieden toegang tot hun kluisdata vanuit een productieomgeving-interface. Dit plaatst de kluisdata op hetzelfde aanvalsoppervlak als de productiedata, waardoor kwaadwillenden mogelijk toegang hebben tot back-upkopieën met behulp van gecompromitteerde inloggegevens.

CyberSense

Om uw data goed te beschermen, is een uitgebreide strategie nodig die beveiliging op elk niveau biedt. Ondanks alle zelfherstellende, beveiligings-, onveranderlijke en isolatiefuncties van een Dell PowerProtect Cyber Recovery oplossing, kunnen minder voor de hand liggende aanvallen nog dieper in een bedrijfsinfrastructuur duiken, zoals op het niveau van databack-ups, die mogelijk niet worden gedetecteerd totdat productiedata of een hele gebruikersgroep in gevaar zijn gekomen. Dell PowerProtect Cyber Recovery oplossingen bieden een laatste verdedigingslinie tegen cyberaanvallen en een efficiënte aanpak om herstel via CyberSense te versnellen. CyberSense is een analytics-engine die AI-gebaseerde ML-analysealgoritmen gebruikt om de integriteit van back-ups in de kluis en de gebruikersinhoud van de bestanden in de back-ups te scannen en te valideren.

CyberSense wordt binnen de kluis uitgevoerd, afgezonderd van de productieomgeving. Het controleert bestanden, VM-images en databases in de kluis om te bepalen of er een aanval is opgetreden door de integriteit van de data te analyseren. Zodra de Cyber Recovery-oplossing back-upkopieën naar de kluis repliceert en de Retention Lock-functie toepast, scant CyberSense automatisch de kopieën, waardoor point-in-time-observaties van bestanden, databases en de core-infrastructuur worden gemaakt. De analytics-engine scant de volledige inhoud van bestanden en elke databasepagina, niet alleen metadata. Waar andere oplossingen zoeken naar wijzigingen in datadrempels of metadata, zoekt CyberSense in de inhoud van bestanden om de data-integriteit te valideren. Met deze observaties kan CyberSense bijhouden hoe bestanden en databases in de loop van de tijd veranderen en veel geavanceerde typen verborgen aanvallen ontdekken. CyberSense genereert vervolgens analytics die patronen van corruptie detecteren die kunnen wijzen op activiteiten van kwaadwillenden, waaronder versleuteling; verwijderen, maken of verduisteren van bestanden en meer.[26] Andere oplossingen verplaatsen analyse naar de cloud, waardoor het aanvalsoppervlak mogelijk wordt vergroot, terwijl organisaties ervoor kunnen kiezen om CyberSense on-premise uit te voeren of in een van de vele cloudopties die Cyber Recovery ondersteunt.

CyberSense combineert meer dan 200 analytics met data-observaties die in de loop van de tijd nuttiger worden naarmate de observaties toenemen. Het ML-algoritme gebruikt informatie over duizenden malware-infecties om ongebruikelijke gedragspatronen te vinden en gebruikersactiviteiten te onderscheiden van ransomware, terwijl fout-positieve en negatieve meldingen worden geminimaliseerd. Het algoritme krijgt via doorlopend onderzoek nieuwe informatie over dingen, zoals aanvalsvarianten. Bovendien ontvangt het ML-algoritme updates op basis van echte data van bestaande CyberSense-klanten.[27]

Daarnaast ondersteunt CyberSense het indexeren van data in veelvoorkomende schijfback-upindelingen van Dell, IBM, CommVault en Veritas.[28] Door back-upindelingen van andere leveranciers te ondersteunen, toont Dell zich bereid om klanten te ondersteunen waar zij zich bevinden op het gebied van databack-ups.

We hebben de ML-gestuurde intelligente analysesoftware van twee kant-en-klare oplossingen voor enterprise databescherming en cyberherstel getest: CyberSense voor Dell PowerProtect Cyber Recovery op een Dell PowerStore™ 7000T en een vergelijkbaar functionerende tool van het databeheerplatform van een concurrent (“leverancier X”) voor een apparaat van vergelijkbare grootte.

Hoe we hebben getest

We hebben alle tests op afstand uitgevoerd en hadden volledige controle over en onbelemmerde toegang tot de testomgevingen. Zowel de Dell oplossing (inclusief CyberSense, de back-upapplicatie van PowerProtect Data Manager, APEX Protection Storage (voorheen DD Virtual Edition) en de PowerProtect Cyber Recovery-oplossing) als de oplossing van leverancier X bevinden zich in een offsite datacenter-lab.

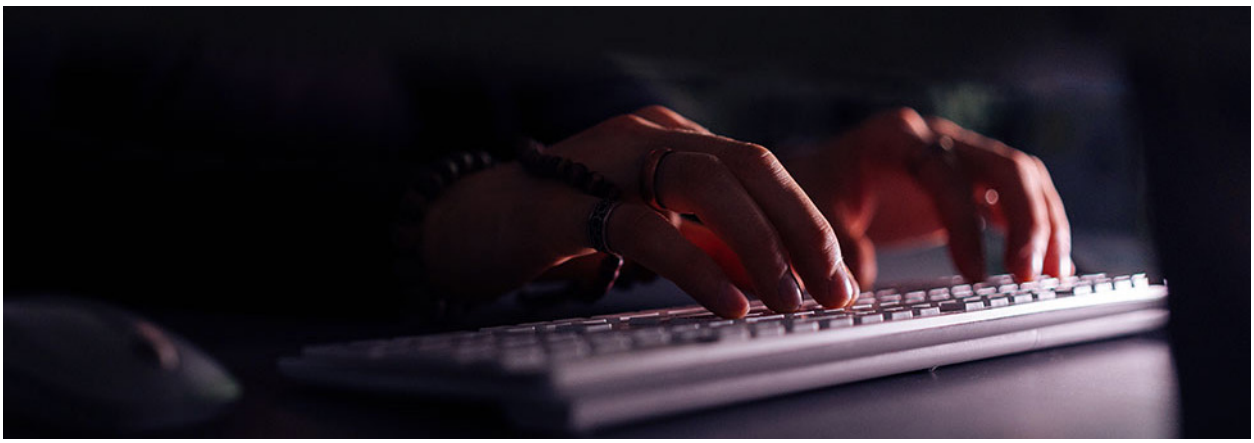
Op beide oplossingen hebben we drie scenario's voor schadelijke gebeurtenissen op basis van scripts uitgevoerd die gericht waren op back-ups:

Afbeelding 2: Onze testscenario's. Bron: Principled Technologies.

Voor beide oplossingen volgden de eerste twee scenario's dezelfde algemene procedure. Eerst hebben we een volledige back-up gemaakt van alle schone VM's op de Dell PowerProtect Data Manager en storage-apparaten van leverancier X, incrementele back-ups gemaakt voor scannen en gecontroleerd of de doeloplossing geen bedreiging heeft gedetecteerd. Dit gaf ons een uitgangssituatie van back-ups waarop we de aanvalsscripts konden uitvoeren.

Vervolgens hebben we het ransomware-simulatiescript uitgevoerd op vier VM's met verschillende besturingssystemen en applicatietypen, nieuwe incrementele back-ups gemaakt op het doelapparaat en gecontroleerd of de doelanalysesoftware de versleutelingsbedreiging heeft gedetecteerd.

Voor het derde scenario (infecteer een SQL Server-pagina) hebben we een vergelijkbare procedure gevolgd als in de andere twee scenario's, maar in plaats daarvan hebben we ons gericht op SQL VM's en hebben we een script voor paginabeschadiging gebruikt in plaats van een versleutelingsscript. We hebben het script uitgevoerd op één VM.



Onze ervaring

Scenario 1: Het detecteren van versleutelde bestanden met afgeschermde bestandsnamen

Dit scenario simuleerde een kwaadaardige gebeurtenis die bestanden versleutelde en hun namen verborgen hield, wat de metadata van het bestand veranderde naast zijn inhoud. Dit type aanval staat meestal bekend als ransomware, een beveiligingsgebeurtenis waarbij schadelijke software de toegang tot een computersysteem blokkeert totdat de eigenaar of gebruiker van het systeem een vooraf bepaalde hoeveelheid geld betaalt. Volgens het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) zijn "de economische en reputatiegevolgen van ransomware en afpersing van data uitdagend en kostbaar gebleken voor organisaties van elke omvang tijdens de eerste verstoring en in sommige gevallen langdurig herstel".[29] Het gebruik van intelligente analysesoftware om versleuteling in back-ups te detecteren, kan de strategie voor databescherming van organisaties versterken, waardevolle en gevoelige informatie beschermen en de kans op kostbare downtime vanwege cyberaanvallen verminderen.

In onze tests hebben beide intelligente analytics-applicaties de versleutelde bestanden met gewijzigde bestandsnamen ontdekt. De oplossing van leverancier X had een uitgangsniveau van 15 back-ups nodig voordat infecties werden gedetecteerd (één volledige back-up en 14 incrementele back-ups), terwijl CyberSense infecties heeft gedetecteerd na slechts één volledige back-up, wat betekent dat de oplossing van leverancier X 14 extra back-ups nodig had in vergelijking met CyberSense.

Toen de oplossing van leverancier X ons waarschuwde voor de verdachte activiteit, gaf het alleen aan dat iets veel bestanden had verwijderd en een gelijk aantal bestanden had toegevoegd, wat verdachte activiteit was op basis van de entropiebeoordeling van de back-up.[30] De oplossing van leverancier X geeft niet aan dat de bestanden zijn versleuteld of dat de bestandsnamen zijn gewijzigd. Cyber Recovery met CyberSense waarschuwde ons daarentegen dat iets versleutelde en afgeschermde bestandsnamen had.

De resultaten voor leverancier X kunnen fout-positieve meldingen zijn. Met andere woorden, als we aannemen dat een organisatie dagelijkse back-ups uitvoert met de oplossing van leverancier X, kunnen ze 14 dagen geïnfecteerde bestanden hebben geaccepteerd voordat een afwijking werd gedetecteerd. CyberSense had daarentegen slechts één back-up nodig om te waarschuwen met informatie over de infectie en de details ervan. Herstel met Cyber Recovery vindt in dit stadium in ons voorbeeld plaats vanuit de geïsoleerde kluis. Hierdoor kan de organisatie er zeker van zijn dat het productienetwerk niet wordt blootgesteld aan de 14 geïnfecteerde back-ups, zoals de oplossing van leverancier X zou kunnen hebben gedaan.

Afbeelding 3: Het aantal back-ups dat elke oplossing vereist om een uitgangssituatie te creëren voor het detecteren van beschadiging.
Bron: Principled Technologies.

Scenario 2: Het detecteren van versleutelde bestanden met oorspronkelijke bestandsnamen

Dit scenario was vergelijkbaar met het eerste scenario, maar het script behield de oorspronkelijke bestandsnamen van de versleutelde bestanden. Deze wijziging had geen invloed op de metadata van de bestanden, alleen op de bestanden zelf. Een daad als deze kan timebomb ransomware zijn, waarbij de aanval een periode inactief blijft voordat deze wordt geactiveerd. Timebomb ransomware kan detectie omzeilen en zich richten op back-ups, waardoor de geïnfecteerde back-ups onbruikbaar worden wanneer de organisatie ze nodig heeft.[31] Zonder wijzigingen in de metadata kan het bestand op het oppervlak niet geïnfecteerd lijken, waardoor de inactieve aanval verborgen blijft.

In onze tests hebben beide intelligente analytics-applicaties de versleutelde bestanden ontdekt. Ook deze keer had de oplossing van leverancier X een uitgangssituatie van 15 back-ups nodig, waaronder 14 incrementele back-ups, voordat deze een afwijking kon detecteren. CyberSense had slechts één volledige back-up nodig voordat er een afwijking werd gedetecteerd.

Net als in het eerste scenario waarschuwde de oplossing van leverancier X ons alleen dat er iets was veranderd in veel bestanden, wat verdacht was op basis van de entropiebeoordeling van de back-up. Het gaf niet aan dat iets de bestanden had versleuteld, terwijl Cyber Recovery met CyberSense ons dit wel vertelde. Het detecteren van beschadiging op deze manier betekent dat CyberSense kijkt naar de inhoud van de bestanden, niet alleen naar de metadata op oppervlakteniveau. Dit type scan voegt een extra beveiligingslaag toe voor uw back-ups, en dus uw digitale infrastructuur of omgeving in het algemeen. Men zou kunnen suggereren dat CyberSense een "echte" intelligente analytics-applicatie is. Daarbij kunnen organisaties beschadiging sneller detecteren met CyberSense, aangezien de oplossing een veel kleiner aantal back-ups nodig had om een uitgangssituatie te creëren. Afhankelijk van het back-upschema van een organisatie kan dat vele dagen eerder zijn.

Afbeelding 4: Het aantal back-ups dat elke oplossing vereist om beschadiging te detecteren. Bron: Principled Technologies.

Scenario 3: Beschadiging van SQL Server-pagina detecteren

In dit scenario is een schadelijke gebeurtenis gesimuleerd waarbij een SQL Server-pagina wordt beschadigd. In SQL Server is de fundamentele eenheid van datastorage de pagina en de database leest of schrijft hele datapagina's.[32] Ook nu had deze wijziging geen invloed op de metadata van de bestanden, alleen op de bestanden zelf. Dit type aanval is algemeen bekend als een SQL-injectie, waarbij aanvallers zich richten op SQL-datagestuurde applicaties door schadelijke code in SQL-instructies te injecteren via invoer van webpagina's.[33] Zelfs als deze zijn geïnfecteerd, kunnen databases blijven draaien. Naast datadiefstal kan beschadiging van SQL Server-pagina's leiden tot problemen met de data-integriteit, dataverlies en onderbrekingen van de databasefunctionaliteit. Deze resultaten kunnen de reputatie van een organisatie schaden, operationele workflows verstoren, financieel verlies tot gevolg hebben en zelfs juridische aansprakelijkheid veroorzaken.

Hoewel CyberSense en de oplossing van leverancier X beide de versleuteling in de eerste twee scenario's hebben gedetecteerd, kon alleen CyberSense diep genoeg scannen om de beschadiging op de SQL Server-pagina in dit derde scenario te detecteren. Dit toont aan dat hoewel de twee oplossingen op sommige niveaus vergelijkbare detectiemogelijkheden bieden, CyberSense een diepere scan naar back-ups biedt voor mogelijk bedrijfskritische SQL Server-applicaties. Op deze manier voegt CyberSense een beveiligingslaag toe met diepere scans en uitgebreidere bescherming.

SQL Server is de drijvende kracht achter veel applicaties in de financiële sector, detailhandel, gezondheidszorg en andere sectoren. Omdat SQL Server kan fungeren als de back-end van de ontwikkelingsarchitectuur, kan een SQL Server-aanval leiden tot downtime, onderbrekingen van activiteiten en mogelijk een bedreiging vormen voor de omzet die deze applicaties genereren.

Herstellen met Dell PowerProtect Cyber Recovery

De strategie van Dell voor cybertolerantie biedt een breed scala aan herstelmogelijkheden. Deze herstelopties omvatten algemene branchemogelijkheden, zoals directe toegang of traditioneel herstel van de onveranderlijke back-ups die in productie worden onderhouden. Daarnaast biedt Dell unieke herstelmogelijkheden van de PowerProtect Cyber Recovery-oplossing. Omdat PowerProtect Cyber Recovery kopieën in isolatie onderhoudt en scant op integriteit met CyberSense, hebben organisaties direct na een aanval toegang tot de kopieën en kunnen ze deze gebruiken om herstelstappen te starten of onmiddellijk te herstellen naar alternatieve herstelplatforms, zoals cleanrooms.

Vergelijk dit onmiddellijke gebruiksscenario met een organisatie die alleen toegang heeft tot data in productie of de public cloud. De organisatie kan geen veilige toegang krijgen tot data die zijn opgeslagen in het gecompromitteerde gebied totdat ze de hoofdoorzaak hebben vastgesteld en hersteld; de persistentie van kwaadwillende actoren hebben afgesloten; forensische images voor verzekeraars en hun juridische afdeling hebben gemaakt; de data opnieuw hebben gescand; en over voldoende beschikbare infrastructuur (AD, DNS) beschikken om toegang te krijgen tot de back-upinfrastructuur. Dit proces kan dagen of weken in beslag nemen, afhankelijk van de omvang en complexiteit van de aanval.

Hoe het werkt

Tijdens normale productie maakt PowerProtect Cyber Recovery automatisch herstelpunten voor herstel- en beveiligingsanalyses. In het geval van een cyberaanval gebruikt Cyber Recovery de geautomatiseerde herstelprocedures en deze herstelpunten om bedrijfskritieke systemen weer online te brengen. CyberSense en forensische rapporten helpen cyberbeveiligings- en herstelteams de impact van de aanval te diagnosticeren. Zodra de productieomgeving schoon is en klaar is voor herstel, biedt Cyber Recovery de tools en technologie die het werkelijke dataherstel uitvoeren.

Na een cyberaanval spelen verschillende databeschermingsfactoren een rol bij het bepalen van de herstelsnelheid (de cyberhersteltijd of CRT) en het punt in de tijd waarnaar gebruikers kunnen terugkeren na een destructieve aanval (het cyberherstelpunt of CRP). Voor een Cyber Recovery-oplossing omvatten deze factoren het volgende:

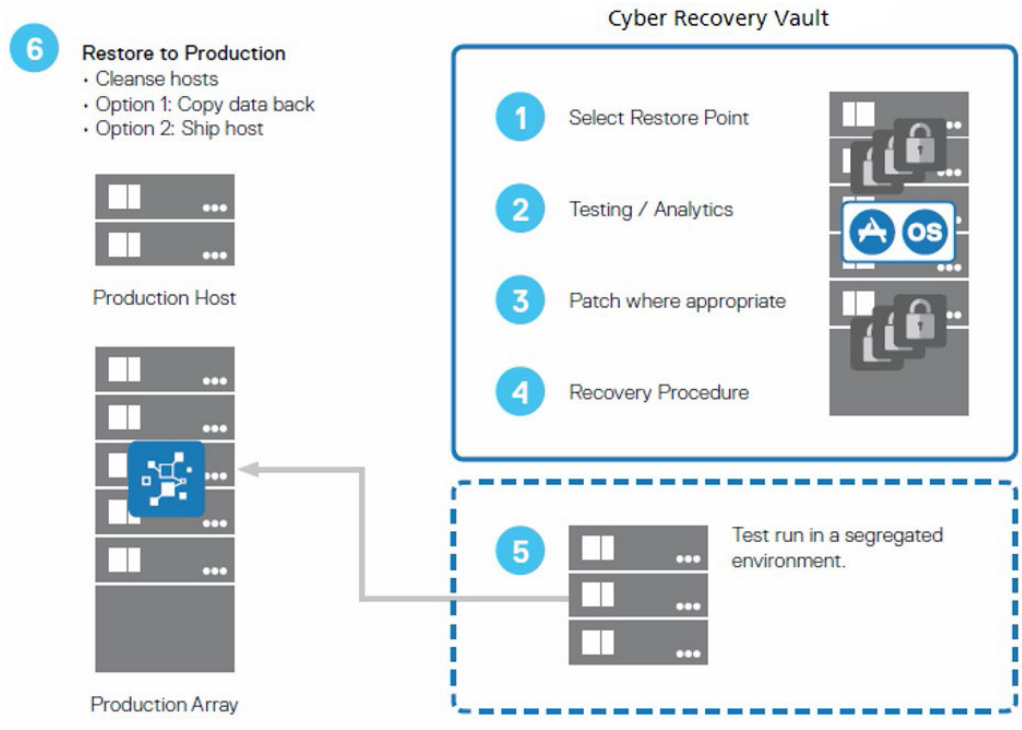
- **Destruction Detection Objective (DDO):** dit is een doorlopend venster op basis van de hoeveelheid tijd tussen een aanval en de detectie van de aanval. Analytics en andere Cyber Recovery-mechanismen moeten binnen deze periode werken.
- **Destruction Assessment Objective (DAO):** dit is de hoeveelheid tijd die na een inval aan het cyberbeveiligingsteam wordt toegewezen om de omvang van de schade en mogelijke reacties te bepalen.
- **Cyber Recovery-synchronisatie-interval:** dit is de frequentie waarmee de Cyber Recovery-oplossing data van de productieomgeving naar de kluis kopieert. De timing is gebaseerd op een eerder vastgesteld beoogd herstelpunt (RPO) voor de oplossing. De bewaarperiode van kopieën verschilt per oplossing, maar varieert meestal van een week tot een maand.
- **Aantal kopieën van Cyber Recovery-data:** dit is het aantal datakopieën in de Cyber Recovery-kluis. In combinatie met het synchronisatie-interval geeft deze statistiek een grove indicatie van hoe ver terug in de tijd een organisatie data kan herstellen. Zo kunnen gebruikers met zeven kopieën in combinatie met een interval van 24 uur data herstellen die maximaal een week oud is.

Naast de herstelvereisten kan het type data dat de oplossing beschermt, helpen bij het bepalen van het synchronisatie-interval en de bewaartijd van de data. Volgens de Cyber Recovery handleiding met oplossingen kunnen gebruikers voor de grootste herstelflexibiliteit data die de oplossing beschermt, indelen in een van de volgende back-upstromen:[34]

- Binaire en uitvoerbare back-ups, inclusief distributies van besturingssystemen op basisniveau en applicatiebestanden
- Back-ups van volledige applicaties en bestandssystemen, inclusief images en applicatiespecifieke data

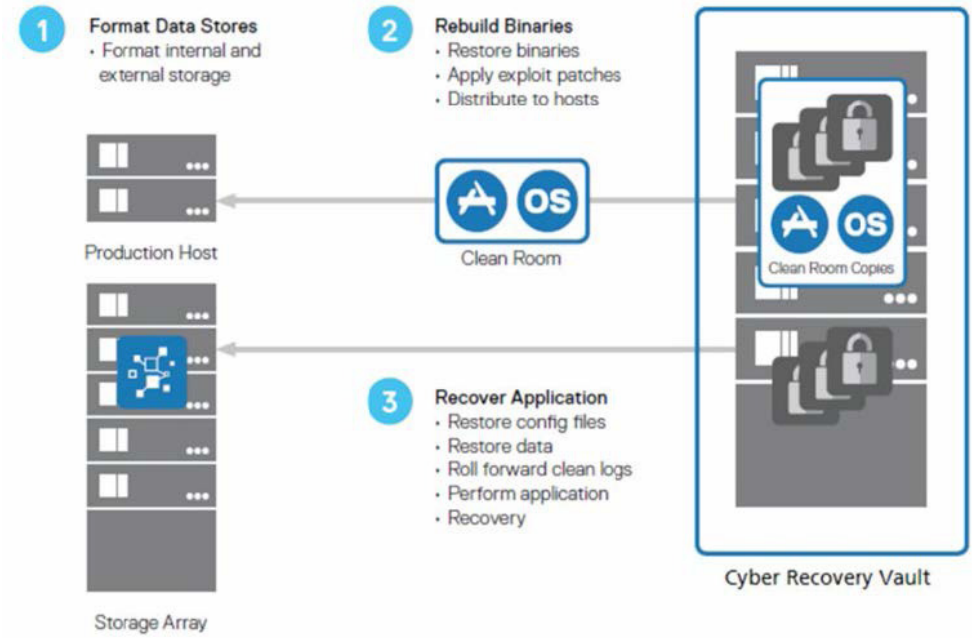
Deze afzonderlijke back-upstromen leiden tot twee verschillende herstelstrategieën:

1. **Binaire bestanden van data en applicaties herstellen in de Cyber Recovery-kluis:**
   De oplossing identificeert bruikbare herstelpunten, samen met malware en waar deze zich hebben voorgedaan, en besluit of de malware van de back-upimage moet worden verwijderd of opnieuw moet worden opgebouwd met behulp van kluiskopieën van Cyber Recovery. Na het toepassen van beveiligingspatches herstelt de oplossing data naar een herstelhost met behulp van het DR-runbook voor de applicatie en bepaalt vervolgens of het herstelproces de effecten van de malware heeft weggenomen. Vervolgens wordt de applicatie getest met vault compute en wordt de productieomgeving opgeschoond of opnieuw geïmplementeerd. Tot slot verbindt Cyber Recovery de herstelhost met productie en kopieert de applicatie en data terug naar de productieomgeving. Afbeelding 5 toont dit proces.



Afbeelding 5: Het proces voor het herstellen van binaire bestanden van data en applicaties. Bron: Dell Technologies.[35]

2. **Volledig opnieuw opbouwen vanuit de Cyber Recovery-kluis:**
   Bij deze aanpak herformatteert de Cyber Recovery-oplossing de productiesystemen op basis van het schadeniveau dat wordt bepaald door de forensische beoordeling tijdens incidentrespons. De oplossing bouwt vervolgens binaire bestanden opnieuw op via kopieën in de Cyber Recovery-kluis en past beschikbare beveiligingspatches toe. Ten slotte worden de juiste kopieën van applicaties, data en configuratiebestanden in de productieomgeving hersteld met behulp van de bijbehorende DR-runbooks voor de applicatie. Afbeelding 6 toont dit proces.



Afbeelding 6: Het proces voor volledig opnieuw opbouwen vanuit de Cyber Recovery-kluis. Bron: Dell Technologies.[36]

De Cyber Recovery-oplossingen omvatten fysieke of virtuele herstelhosts (of beide) die de Cyber Recovery-software kan gebruiken voor herstel. Deze hosts omvatten zowel een back-up-applicatieherstelserver. Dit is een aangewezen server waarop de back-up-applicatie en de back-up-applicatiecatalogus worden hersteld, en een applicatieherstelserver. Organisaties kunnen meerdere servers implementeren, afhankelijk van de herstelvereisten van de oplossing. De Cyber Recovery-software kan sandbox (een testomgeving voor het veilig uitvoeren van nieuwe of niet-geteste software)-datakopieën beschikbaar maken voor elke host om data in de kluis te herstellen, zoals bestandssysteemdata; IBM, CommVault en Veritas back-updata; of data die worden beschermd door Dell NetWorker, Dell Avamar, een Dell PowerProtect DP-apparaat of Dell PowerProtect Data Manager software. Na het herstellen van een back-upapplicatie in de kluis kan de oplossing die data terugzetten naar extra herstelhosts in de kluis.

Organisaties bepalen van tevoren de grootte van de back-upapplicatieherstelserver, zodat gebruikers alle back-upapplicaties kunnen herstellen die de Cyber Recovery-oplossing beschermt. Op dezelfde manier is de applicatieherstelserver een aangewezen server waarnaar de oplossing applicaties herstelt. Voor sommige applicaties moeten klanten mogelijk eerst andere afhankelijke applicaties herstellen. De infrastructuur binnen de kluis kan het herstel van de grootste productieapplicatie ondersteunen die de oplossing beschermt.

Conclusie

Organisaties moeten bij het opstellen van een databeschermingsplan rekening houden met veel aanvalsvectoren. Dit omvat het beschermen van alle data, maar het belangrijkste, de essentiële data die noodzakelijk zijn voor activiteiten. PowerProtect Cyber Recovery isoleert de kritieke data en zorgt voor een correct herstel van data in het geval van een cyberaanval. Cyber Recovery gebruikt ML-gebaseerde analyses in CyberSense om de integriteit van de data in de kluis te bepalen en schone back-updata te identificeren voor herstel. In onze tests hebben we vastgesteld dat PowerProtect Cyber Recovery een infectie heeft gedetecteerd in SQL-databasepagina's, iets wat een concurrerende oplossing niet kon doen. PowerProtect Cyber Recovery had ook minder back-ups nodig dan een concurrerende oplossing om beschadiging van de data te bepalen. Naast dit alles en meer biedt de Cyber Recovery-oplossing vele herstelopties, waarbij wordt uitgegaan van onaangetaste data uit de kluis voor een efficiënte en soepele terugkeer naar de bedrijfsactiviteiten.

---

1. Dell, "CyberSense® for PowerProtect Cyber Recovery", geraadpleegd op 8 september 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", geraadpleegd op 23 augustus 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Dell PowerProtect Cyber Recovery handleiding met oplossingen".
4. Cohasset Associates, Inc, "Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) en FINRA 4511(c)", geraadpleegd op 27 oktober 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, "Data Domain: Retention Lock Frequently Asked Questions," geraadpleegd op 12 september 2023, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, "Data Domain: Retention Lock Veelgestelde vragen."
7. Dell, "Encryption types offered by DD series encryption appliance", geraadpleegd op 8 september 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, "Dell EMC Data Domain – Security Configuration Guide", geraadpleegd op 11 september 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, "Role Based Access Control (RBAC) in Data Domain", geraadpleegd op 11 september 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, "Dell EMC Data Domain – Security Configuration Guide".
11. Dell, "MTree Replication", geraadpleegd op 11 september 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, "Dell EMC Data Domain - DataDomain MTree overview and limits", geraadpleegd op 11 september 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", geraadpleegd op 13 december 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, "NetBackup™ Security and Encryption Guide", geraadpleegd op 13 december 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528 .
15. Principled Technologies, "Dell EMC Cyber Recovery beschermde onze testgegevens tegen een cyberaanval", geraadpleegd op 21 augustus 2023, http://facts.pt/rkew01n.
16. Dell, "Dell PowerProtect Cyber Recovery", geraadpleegd op 12 september 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman en Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware," geraadpleegd op 14 december 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman en Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware."
19. Nikitha Okmar, "Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era", geraadpleegd op 13 december 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, "How to protect your data from ransomware and encryption Trojans", geraadpleegd op 13 december 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, "Rest easy with immutable, off-site data storage", geraadpleegd op 13 december 2023, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, "NetBackup Isolated Recovery Environment", geraadpleegd op 13 december 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf .
23. CSI Group, "Dell Cyber Recovery Vault (overview by CSI)", geraadpleegd op 23 augustus 2023, https://youtu.be/ej5nZzWNRM0.
24. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
25. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
26. Dell, "CyberSense® for PowerProtect Cyber Recovery".
27. Dell, "CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines," geraadpleegd op 13 september 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, "CyberSense for Dell Cyber Recovery", geraadpleegd op 25 september 2023, https://indexengines.com/csmatrix.
29. CISA, "#StopRansomware Guide", geraadpleegd op 1 augustus 2023, https://www.cisa.gov/stopransomware/ransomware-guide.
30. "In beveiliging gebruiken de meeste mensen Shannon Entropy, een specifiek algoritme dat een waarde tussen 0 en 8 teruggeeft. Hoe hoger het getal, hoe willekeuriger de data is, en vaak betekent een hoger getal dat de data is ingepakt of gecodeerd." Mueller, Clint, "How to use Entropy Analysis in Penetration Testing", 28 augustus 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, "How to Protect Your back-ups from ransomware in 2023", 1 augustus 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, "Pages and extents architecture guide", geraadpleegd op 3 augustus 2023, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, "SQL Injection", geraadpleegd op 3 augustus 2023, https://www.w3schools.com/sql/sql_injection.asp .
34. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
36. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".

Lees de wetenschap achter dit rapport ▶

▶ Bekijk de oorspronkelijke, Engelstalige versie van dit rapport via https://facts.pt/64FU3b2

Dit project is uitgevoerd in opdracht van Dell Technologies.

Principled Technologies®

Facts matter.®