Executive summary

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.

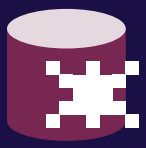
Dell PowerProtect Cyber Recovery is een oplossing voor databeheer, -bescherming en -herstel die organisaties helpt hun data en applicaties te beschermen tegen ransomware, destructieve cyberaanvallen en onverwachte gebeurtenissen. De oplossing maakt gebruik van een multi-copy aanpak, wat betekent dat 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. Deze functies omvatten Retention Lock, DDBoost, op rollen gebaseerde toegangscontrole (RBAC), dubbele autorisatie en meer.

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 vaak 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 fysieke en logische isolatie bieden, in de vorm van air gaps, om data te beschermen. 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.[2] Door de toegang tot de herstelomgeving vanuit het productienetwerk te elimineren, kan een organisatie het aanvalsoppervlak verkleinen.

Onveranderlijkheid*

Het onveranderlijk maken van back-ups helpt ervoor te zorgen dat een organisatie deze back-ups kan vertrouwen voor herstel. Operationeel gezien helpt onveranderlijkheid de authenticiteit en betrouwbaarheid van data te behouden. DD-systemen, inclusief systemen in PowerProtect Cyber Recovery-oplossingen, kunnen onveranderlijkheid bieden in de manier waarop ze data opslaan met behulp van logische partities van het bestandssysteem genaamd MTrees. De 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.[3]

*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 databeschermings-, storage- en andere infrastructuurproducten beveiligingslekken ondervinden. Het is belangrijk dat klanten beveiligingsupdates installeren zodra deze door Dell beschikbaar worden gesteld.

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.

We hebben CyberSense en een vergelijkbaar werkende tool van het databeheerplatform van een concurrent (die we 'leverancier X' noemen) getest voor een apparaat van vergelijkbare grootte. In onze tests hebben we vastgesteld dat PowerProtect Cyber Recovery een infectie heeft gedetecteerd in SQL-databasepagina's, iets wat de oplossing van leverancier X niet kon doen. PowerProtect Cyber Recovery had ook minder back-ups nodig dan de oplossing van leverancier X om beschadiging van de data te bepalen.

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, "MTree Replication", geraadpleegd op 11 september 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. Principled Technologies, "Dell EMC Cyber Recovery beschermde onze testgegevens tegen een cyberaanval", geraadpleegd op 21 augustus 2023, http://facts.pt/rkew01n.

▶ Bekijk de oorspronkelijke, Engelse versie van deze samenvatting

Lees het rapport ▶

Principled Technologies®

Facts matter.®