Sammanfattning

Förbättra cyberelasticitet och skydda data från cyberutpressningsvirushot genom att använda ett isolerat valv, AI-baserad ML-analysmjukvara med mera

Med Dell Technologies PowerProtect Cyber Recovery med CyberSense

I takt med att cyberhoten ständigt växer och attackmetoderna utvecklas måste dataskyddsplanerna ha en strategi som skyddar och analyserar alla IT-komponenter, från de ytligaste till de djupaste delarna. Dell PowerProtect Cyber Recovery kan hjälpa till att skydda de mest kritiska och känsliga data samtidigt som det bidrar till att säkerställa korrekt återställning efter en cyberattack eller annan störning.

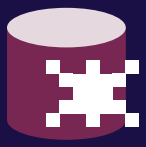
Dell PowerProtect Cyber Recovery är en datahanterings-, skydds- och återställningslösning som hjälper organisationer att skydda sina data och program mot utpressningsprogram, skadliga cyberattacker och oväntade händelser. Lösningen använder en metod med flera kopior. Det innebär att först skapas säkerhetskopior som sedan kopieras till isolerad lagring där den skyddas och analyseras. PowerProtect Cyber Recovery består av många komponenter, bland annat ett eller flera lagringsvalv som kan vara placerade antingen lokalt i en PowerProtect DD (tidigare känd som Data Domain) eller i molnet via mjukvarudefinierad Dell APEX Protection Storage for Public Cloud (tidigare känd som DD Virtual Edition). I båda fallen är valvet driftsmässigt avgränsat, alltså isolerat från produktionsmiljön – potentiellt fysiskt avgränsat i den lokala miljön och logiskt avgränsat i APEX-miljön. Det gör det extremt svårt för illvilliga aktörer eller obehöriga användare att logga in och kompromettera säkerhetskopior.

PowerProtect Cyber Recovery omfattar även CyberSense, en helt automatiserad och integrerad intelligent motor för säkerhetsanalyser som automatiskt skannar data, filer, databaser och bilder i valvet för tecken på skada vid en utpressningsattack. CyberSense tillhandahåller fullständig innehållsanalys med observationer från filer som används som indata för den AI-baserade maskininlärningsmodellen (ML). Det upptäcker skadlig aktivitet som omfattar massradering, kryptering och andra misstänkta förändringar i kärninfrastrukturen (inklusive Active Directory och DNS), användarfiler och avgörande produktionsdatabaser som kan tyda på utpressningsvirus eller en skadlig attack. När CyberSense upptäcker skadliga mönster genereras en varning på PowerProtect Cyber Recovery-instrumentpanelen som ger ytterligare information om attackens storlek och inverkan.[1]

PowerProtect Cyber Recovery hjälper företag att minska cyberattacker, förbättra dataelasticiteten med flera kopior av datasäkerhetskopiering på olika platser, minska driftavbrott och upprätthålla affärskontinuitet. I den här rapporten används allmänt tillgängliga data för att lyfta fram viktiga dataskyddsfunktioner och funktionalitet där vi presenterar våra resultat från en konkurrenskraftig analys av CyberSense.

Skydda känsliga data

Kryptera oföränderliga data under drift under säkerhetskopiering och replikering till fysiskt och logiskt isolerade valv



Identifiera skadade SQL Server-sidor

CyberSense hittade en infektion där en konkurrerande lösning inte kunde

Identifiera okorrumperade säkerhetskopior

CyberSense identifierade den senaste icke-infekterade säkerhetskopian för återställning

Säkerhet

Dell PowerProtect Cyber Recovery erbjuder flera säkerhetsfunktioner som hjälper till att skydda kritiska data från utpressningsvirus och andra sofistikerade hot. Det förhindrar att obehöriga användare får åtkomst till känslig information och ser till att återställningen går snabbt så att företag kan återuppta normal drift.

Funktionerna i PowerProtect DD-enheter kan vara avgörande för den säkerhet, integritet och återställning som PowerProtect Cyber Recovery-lösningar ger. Dessa funktioner inkluderar Retention Lock, DDBoost, rollbaserad åtkomstkontroll (RBAC), dubbel auktorisering med mera.

Isolering

Dataisolering avser separation av och begränsad åtkomst till data som skapats av hinder eller gränser för att förhindra obehörig åtkomst. Isolering använder ofta tillfälliga nätverksanslutningar istället för beständiga anslutningar.

Dataisolering hjälper viktiga data att förbli oanslutna från ett infekterat nätverk där en hotaktör kan försöka ändra konfigurationer, ta bort data, ändra policyer eller söka igenom nätverkstrafik för användaruppgifter. Isolering bidrar också till att minska angreppsytan, och ger därmed hotaktörer färre möjligheter att få åtkomst och kontroll. Dessutom kan företag begränsa åtkomsten till endast behörig personal, något som hjälper till att förhindra att obehöriga användare skriver över data.

Utöver de funktioner vi noterade kan PowerProtect Cyber Recovery erbjuda fysisk och logisk isolering i form av luftgap för att skydda data. En lokal PowerProtect DD som är fysiskt isolerad kan fungera som ett valv där användare eller system från produktionsmiljön inte kan komma åt komponenterna, och valvet är fysiskt frånkopplat från produktionsnätverket.[2] Genom att eliminera åtkomst till återställningsmiljön från produktionsnätverket kan företaget minska angreppsytan.

Oföränderlighet*

Genom att göra säkerhetskopior oföränderliga och därmed skrivskyddade, säkerställer man ett företag kan lita på dessa säkerhetskopior för återställning. Driftsmässigt bidrar oföränderlighet till att upprätthålla datans äkthet och tillförlitlighet. DD-system, inklusive systemen i PowerProtect Cyber Recovery-lösningar, kan ge oföränderlighet i hur de lagrar data med hjälp av logiska partitioner i filsystemet som kallas MTrees. Lösningarna använder även MTree-replikering för att kopiera oföränderliga datakopior från en produktions-DD till en annan DD i valvet via DDBoost-protokollet.[3]

* Dells produkter är utformade för att stödja kundernas arbete med att skydda sina kritiska data. Precis som alla elektroniska produkter kan dataskydd, lagring och andra infrastruktursprodukter utsättas för säkerhetshot. Det är viktigt att kunderna installerar säkerhetsuppdateringar så snart de görs tillgängliga av Dell.

CyberSense

Det krävs en omfattande strategi för att skydda dina data som ger säkerhet på alla nivåer. Trots självkorrigering, säkerhet, oföränderlighet och isolering i en Dell PowerProtect Cyber Recovery-lösning kan mindre uppenbara attacker fortfarande dyka djupare in i en företagsinfrastruktur, till exempel på nivå för säkerhetskopiering av data. Det kanske inte upptäcks förrän produktionsdata eller en hel användargrupp har kompromitterats. Dell PowerProtect Cyber Recovery-lösningar ger en sista försvarslinje mot cyberattacker och en effektiv metod för att påskynda återställningen via CyberSense.

Vi testade CyberSense och ett liknande verktyg från datahanteringsplattformen hos en konkurrent (som vi kallar "leverantör X") för en enhet i samma storlek. I våra tester upptäckte vi att PowerProtect Cyber Recovery identifierade infektion på SQL-databassidor – något som leverantör X-lösningen inte kunde göra. PowerProtect Cyber Recovery krävde också färre säkerhetskopieringar än leverantör X-lösningen för att fastställa om data var skadade.

1. Dell, "CyberSense® for PowerProtect Cyber Recovery", hämtat den 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", hämtat den 11 september 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack", hämtat den 21 augusti 2023, http://facts.pt/rkew01n.

▶ Se den ursprungliga, engelska versionen av den här sammanfattningen

Läs rapporten ▶

Principled Technologies®

Facts matter.®