

Dell PowerProtect Cyber Recovery

Ett modernt och motståndskraftigt skydd för kritiska data mot utpressningsvirus och destruktiva cyberattacker.

VARFÖR CYBER RECOVERY?

Cyberattacker är utformade för att förstöra, stjäla eller på annat sätt äventyra dina värdefulla data – inklusive dina säkerhetskopior. En avgörande faktor i att kunna återuppta normal affärsverksamhet efter en attack är att skydda viktiga data och återställa dem med garanterad integritet. Hade ditt företag överlevt? Det här är komponenterna i en cybertålig lösning:

Dataisolering och styrning

En isolerad datacentermiljö som inte är ansluten till företags- eller säkerhetskopieringsnätverk och som endast behöriga personer har tillgång till.

Automatiserad datakopiering och luftgap

Skapa oföränderliga datakopior i ett säkert digitalt valv och processer som skapar ett operativt luftgap mellan produktions-/säkerhetskopieringsmiljön och valvet.

Intelligenta analyser och verktyg

Maskininlärning och fullständig indexering av innehåll med kraftfulla analysverktyg inom det säkra valvet. Automatiserade integritetskontroller för att fastställa om data har påverkats av skadliga program och verktyg för att stödja åtgärder vid behov.

Återställning och återskapande

Arbetsflöden och verktyg för återställning efter incidenter genom dynamiska återställningsprocesser och befintliga procedurer för katastrofåterställning.

Planering och utformning av lösningar

Expertvägledning för att välja kritiska datauppsättningar, program och andra viktiga tillgångar för att fastställa återställningstider och återställningspunkter samt effektivisera återställningen.

Utmaningen: Cyberattacker är datadrivna företags fiende

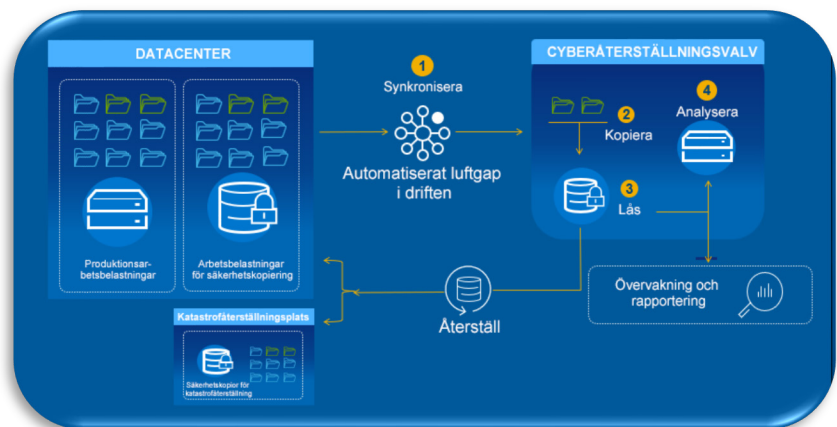
Data är den valuta som gäller i internetekonomin, och den utgör en kritisk tillgång som måste skyddas, behandlas konfidentiellt och göras tillgänglig med ett ögonblicks varsel. Dagens globala marknad är beroende av ett konstant dataflöde mellan och i sammankopplade nätverk, och försökt till digital omvandling utsätter känsligare data för risker.

Därför blir din organisations data ett attraktivt och lukrativt mål för cyberbrottslingar. Oavsett bransch eller storlek utsätts företag och myndigheter ständigt för förvanskade data, förlorade intäkter på grund av driftavbrott, skadat anseende och höga böter på grund av cyberattacker.

Det har blivit obligatoriskt för företags- och myndighetsledare att ha en strategi för cyberelasticitet, men många organisationer saknar förtroende för sina dataskyddslösningar. [Global Data Protection Index](#) rapporterar att 79 % av beslutsfattare inom IT är oroliga för att de kommer att uppleva en störande händelse under de kommande 12 månaderna, och 75 % är oroadade att deras organisationers befintliga dataskyddsåtgärder kanske inte räcker till för att hantera hot från skadliga program och utpressningsvirusattacker¹.

Så vad kan du göra för att skydda din organisation, dina kunder, dina anställda och dina värdefulla data?

Lösningen: Dell PowerProtect Cyber Recovery



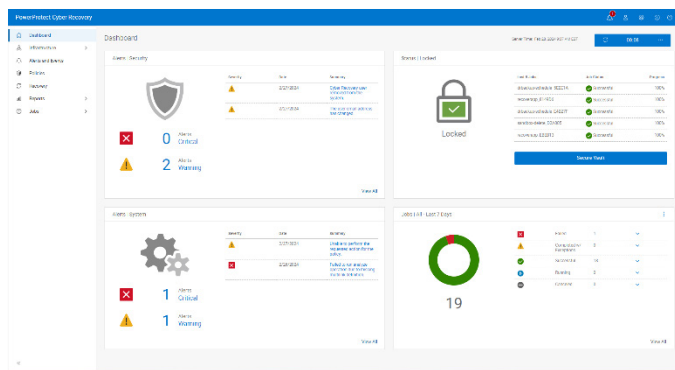
Minska affärsrisker orsakade av cyberattacker och skapa ett mer cybertåligt dataskydd genom att modernisera och automatisera återställnings- och affärskontinuitetsstrategier och utnyttja de senaste smarta verktygen för att upptäcka och skydda mot cyberhot.

Dell PowerProtect Cyber Recovery erbjuder beprövat, modernt, elastiskt och intelligent skydd för att isolera viktiga data, identifiera misstänkt aktivitet och snabba upp dataåterställning så att du snabbt kan återuppta normal verksamhet.

PowerProtect Cyber Recovery – oföränderlighet, isolering och intelligens

Cyber Recovery-valv

PowerProtect Cyber Recovery-valvet erbjuder flera lager av skydd för att ge motståndskraft mot cyberattacker, till och med från insiderhot. Med valvet flyttas viktiga data bort från angreppsytan så att de isoleras fysiskt i en skyddad del av datacentret och så att det krävs separata säkerhetsuppgifter och flerfaktorsautentisering för att komma åt dem. Bland ytterligare skyddsåtgärder finns ett automatiserat operativt luftgap för att ge nätverksisolering och eliminera hanteringsgränssnitt som skulle kunna äventyras. Med PowerProtect Cyber Recovery automatiseras synkroniseringen av data mellan produktionssystem, inklusive öppna system och stordatorer, och valvet, och det skapas oföränderliga kopior med låsta lagringspolicyer. Om en cyberattack inträffar kan du snabbt identifiera en felfri datakopia, återställa dina verksamhetskritiska system och få igång verksamheten igen.



CyberSense

PowerProtect Cyber Recovery är den första lösningen där CyberSense helt integreras. Med CyberSense läggs ett intelligent skyddslager till för att hitta skadade data när ett datacenter utsätts för en attack. Den här innovativa metoden ger fullständig indexerings av innehåll och använder AI-baserad maskininlärning (ML) för att analysera över 200 innehållsbaserade statistiska värden och upptäcka tecken på skada från utpressningsvirus. Med CyberSense hittas skadade data med upp till 99,5 % träffsäkerhet, vilket hjälper dig att identifiera hot och diagnostisera attackvektorer samtidigt som du skyddar ditt affärskritiska innehåll – allt inom valvets säkerhet.

Återställa och återskapa

Med PowerProtect Cyber Recovery får du automatiserade återställningsprocedurer för att affärskritiska system ska komma online igen snabbt och med förtroende. Återställningen är integrerad i incidenthanteringsprocessen. När en händelse har inträffat analyserar incidentsvarsteamet produktionsmiljön för att fastställa vad som ledde till händelsen. CyberSense tillhandahåller också utredande rapporter efter attacken för att du ska kunna förstå attackens djup och bredd, samt en lista över de sista fungerande uppsättningarna säkerhetskopior före skadan. Sedan, när produktionen är redo för återställning, får du genom Cyber Recovery hanteringsverktyg och tekniken med vilken den faktiska dataåterställningen utförs. Det automatiserar skapandet av återställningspunkter som används för återställning och säkerhetsanalys.

Planering och utformning av lösningar

Dells rådgivningstjänster, som finns som tillval, hjälper dig att avgöra vilka verksamhetskritiska system som ska skyddas och kan skapa beroendekartor för associerade program och tjänster, samt den infrastruktur som behövs för att återställa dem. Med tjänsten genereras även återställningskrav och alternativa utformningar, och teknikerna som behövs för att analysera, vara värd för och skydda dina data identifieras, tillsammans med ett affärsfall och en implementeringstidslinje.

För att skydda dina avgörande data från cyberattacker krävs beprövade, moderna och elastiska lösningar. PowerProtect Cyber Recovery gör att du snabbt kan identifiera och återställa data som du vet är tillförlitliga och säkra och återgå till normal affärsverksamhet efter en cyberattack.

¹ Baserat på en undersökning utförd av Vanson Bourne på uppdrag av Dell Technologies, "Global Data Protection Index 2023 Snapshot", gjord oktober 2023.



Mer information om Dell
PowerProtect
Cyber Recovery



Kontakta en Dell
Technologies-expert



Visa fler resurser



Var med i samtalet med
#PowerProtect