

Dell PowerProtect Cyber Recovery

Moderne en veerkrachtige bescherming voor essentiële data tegen ransomware en vernietigende cyberaanvallen

WAAROM CYBER RECOVERY?

Cyberaanvallen zijn ontworpen om uw waardevolle data in gevaar te brengen. Ook uw back-ups zijn niet veilig. Uw essentiële data beschermen en herstellen met gegarandeerde integriteit is cruciaal om de normale bedrijfsactiviteiten na een aanval te herstellen.

Dit zijn de onderdelen van een cybertolerante oplossing:

Onveranderlijkheid van data

Maak onveranderlijke datakopieën om de integriteit en vertrouwelijkheid van data te behouden met beveiligingslagen en -controles.

Geautomatiseerde data-isolatie

Isoleer automatisch onveranderlijke datakopieën van de productieback-upomgeving naar een veilige digitale kluis met verhoogde beperkte toegang.

Intelligente analytics

Geautomatiseerde integriteitscontroles met behulp van op AI gebaseerde machine learning en volledige contentindexering met krachtige analytics binnen de veilige omgeving van de kluis om te bepalen of data zijn beïnvloed door malware.

Herstel en probleemoplossing

Workflows en hulpmiddelen voor het uitvoeren van herstel na een incident met behulp van dynamische herstelprocessen en uw bestaande noodherstelprocedures.

Oplossingsplanning en -ontwerp:

deskundige begeleiding bij het selecteren van essentiële datasets, applicaties en andere essentiële assets om RTO's en RPO's te bepalen en herstel te stroomlijnen.

De uitdaging: cyberaanvallen zijn de vijand van datagestuurde organisaties.

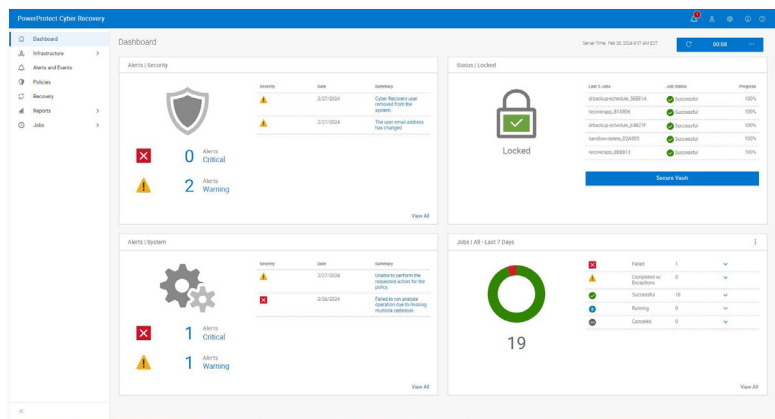
Data zijn de valuta van de digitale economie en een vitaal bezit dat moet worden beschermd, vertrouwelijk en gemakkelijk toegankelijk moet worden gehouden. De moderne internationale markt is afhankelijk van de continue stroom van data over onderling verbonden netwerken. Digitale transformatie-initiatieven en het toenemende gebruik van generatieve AI verhogen de blootstelling van gevoelige informatie.

Dit maakt de data van uw organisatie een aantrekkelijk en lucratief doelwit voor cybercriminelen. Ongeacht de branche of de omvang van de organisatie stellen cyberaanvallen bedrijven en overheden voortdurend bloot aan datalekken, misgelopen omzet door downtime, reputatieschade en dure wettelijke boetes.

Een strategie voor cybertolerantie is absoluut essentieel geworden voor ondernemers en overheden, maar veel organisaties hebben geen vertrouwen in hun oplossingen voor databescherming. De [Global Data Protection Index](#) meldt dat 79% van de IT-besluitvormers zich zorgen maakt over een verstorende gebeurtenis in de komende 12 maanden, en 75% is bezorgd dat de bestaande maatregelen voor databescherming van hun organisatie mogelijk niet voldoende zijn om malware- en ransomwarebedreigingen het hoofd te bieden¹.

De oplossing: Dell PowerProtect Cyber Recovery

Om de zakelijke risico's als gevolg van cyberaanvallen te verminderen en een cyberbestendige benadering van databescherming te creëren, kunt u uw strategieën voor herstel en bedrijfscontinuïteit moderniseren en automatiseren en gebruikmaken van de nieuwste intelligente tools om cyberbedreigingen te detecteren en te bestrijden.



PowerProtect Cyber Recovery biedt bewezen, moderne, veerkrachtige en intelligente bescherming waarbij essentiële data wordt geïsoleerd, verdachte activiteiten geïdentificeerd en dataherstel versneld. Zo kunt u uw essentiële data slimmer herstellen en snel uw normale bedrijfsactiviteiten hervatten. Op basis van [onderzoek van Forrester Consulting](#) helpt PowerProtect Cyber Recovery downtime met 75% te verminderen in het geval van een cyberaanval en het aantal uren dat aan herstel wordt besteed met 80% te verminderen.²

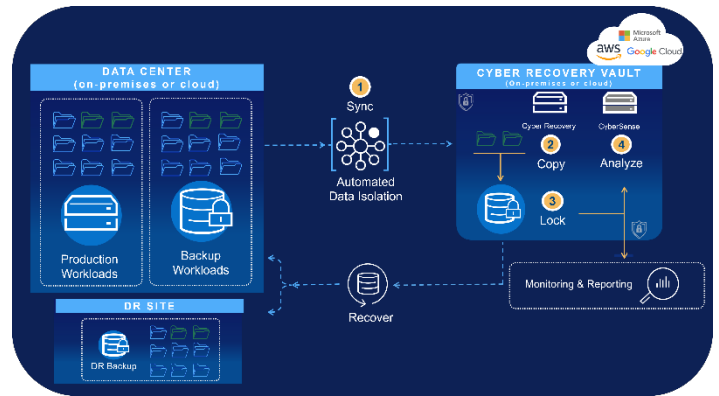
PowerProtect Cyber Recovery – Onveranderlijkheid, isolatie en intelligentie

Onveranderlijkheid - PowerProtect Data Domain

PowerProtect Data Domain is de basis van Dell PowerProtect Cyber Recovery. Met meerdere Zero Trust-beveiligingslagen biedt het onveranderlijke back-upkopieën om de integriteit en vertrouwelijkheid van data te garanderen. Functies zoals hardware Root of Trust, beveiligd opstarten, versleuteling, bewaervergrendeling, rolgebaseerde toegang en meervoudige verificatie zorgen ervoor dat uw data kunnen worden hersteld.

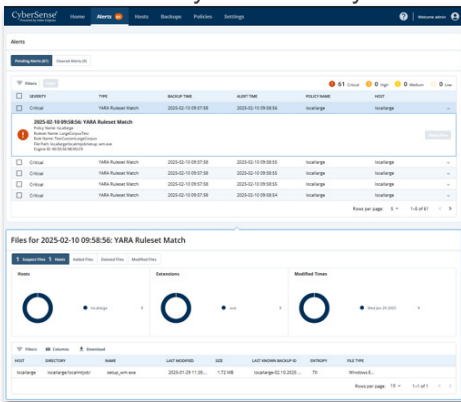
Isolatie - Cyber Recovery kluis

De PowerProtect Cyber Recovery kluis is een geïsoleerde omgeving die meerdere beschermingslagen biedt om veerkracht te bieden tegen cyberaanvallen, zelfs bij een bedreiging van binnenuit. De geautomatiseerde data-isolatie kopieert (Sync) kritieke back-updata (inclusief open systemen en mainframe) veilig naar een fysiek geïsoleerde kluis, weg van het aanvalsoppervlak van de productie, waardoor het beheerpad nooit wordt blootgesteld aan een bedreigingsactor. Vervolgens wordt automatisch een onveranderlijke kopie gemaakt om te voorkomen dat de data worden gewijzigd. Met speciaal beheer, netwerk en services die onafhankelijk zijn van de productieomgeving, zijn afzonderlijke beveiligingsreferenties en meervoudige verificatie vereist voor toegang tot de data voor herstel- en testbewerkingen.



Intelligentie - CyberSense®

PowerProtect Cyber Recovery is de eerste oplossing die CyberSense® volledig integreert voor slimmer herstel tegen cyberdreigingen, allemaal binnen de beveiliging van de Cyber Recovery kluis. CyberSense gaat verder dan alleen metadata-oplossingen. Met volledige contentanalytics detecteert het de databeschadiging na een aanval met een nauwkeurigheid van 99,99%³ en maakt het intelligent en snel herstel mogelijk. CyberSense maakt gebruik van onveranderlijke databack-ups om te observeren hoe data in de loop van de tijd veranderen en gebruikt op AI gebaseerde machine learning om tekenen van corruptie te detecteren die wijzen op een ransomware-aanval. CyberSense detecteert massaverwijderingen, volledige en gedeeltelijke versleuteling en andere verdachte wijzigingen in de kerninfrastructuur (waaronder Active Directory, DNS, enz.), gebruikersbestanden en databases als gevolg van geavanceerde aanvallen. Er kunnen aangepaste drempelwaarschuwingen worden gemaakt en als tekenen van beschadiging worden gedetecteerd, maken het waarschuwingsdashboard en de forensische rapporten na de aanval een snelle diagnose van de omvang en impact van de aanval mogelijk, inclusief de identificatie van een schone kopie van data om uw essentiële systemen te herstellen. Aangepaste YARA-regels en het zoeken naar malwarehandtekeningen helpen organisaties om zichzelf proactief te beschermen tegen cyberdreigingen.



Implementatieopties voor PowerProtect Cyber Recovery

Cyber Recovery in hybride en multicloudomgevingen

Essentiële data kunnen op veel verschillende locaties in een bedrijf aanwezig zijn, of het nu on-premise is, in verschillende datacenters of wereldwijd in meerdere clouds en regio's. Ongeacht de locatie moeten de data veilig en onaangetaast zijn wanneer herstel na cyberaanvallen nodig is.

PowerProtect Cyber Recovery is beschikbaar en verhandelbaar via public-cloudmarktplaatsen voor *AWS*, *Microsoft Azure* en *Google Cloud* om snelle toegang te bieden en data te beschermen in een Cyber Recovery kluis in de cloud. PowerProtect Cyber Recovery automatiseert de synchronisatie van essentiële data tussen productiesystemen en de Cyber Recovery kluis in de public cloud. In tegenstelling tot standaard cloudgebaseerde back-upoplossingen wordt de toegang tot beheerinterfaces vergrendeld door netwerkbeheer en kunnen afzonderlijke beveiligingsreferenties en meervoudige verificatie nodig zijn voor toegang. Het verspreiden en dupliceren van data over meerdere clouds kan leiden tot beveiligings- en nalevingsrisico's, mogelijke synchronisatieproblemen en hogere resourcekosten. Deze aanpak kan ook de zichtbaarheid van uw verschillende omgevingen verminderen, wat leidt tot onvoldoende bescherming tegen voortdurend evoluerende cyberdreigingen.

Dell PowerProtect Data Domain All-Flash Ready Node

Terwijl essentiële data blijven groeien, is de mogelijkheid om snel en efficiënt te herstellen van een cyberaanval van cruciaal belang voor het waarborgen van bedrijfscontinuïteit en cybertolerantie. Organisaties die het beheer van essentiële data uitbreiden, moeten uitblinken in het ophalen van hun data uit geïsoleerde herstelomgevingen, zoals de Cyber Recovery kluis. Dell PowerProtect Data Domain All-Flash Ready Node biedt een gestroomlijnde, energiezuinige en kosteneffectieve oplossing voor cyberherstel met verbeterde CyberSense-analytics en snelle herstelmogelijkheden om te voldoen aan SLA's van organisaties. Door minder hardware, ruimte en energie te gebruiken, kunnen organisaties de toegangssnelheden voor data verbeteren, de operationele efficiëntie verhogen en de data-integriteit garanderen, wat uiteindelijk leidt tot minder downtime en lagere algehele onderhoudskosten.

PowerProtect Cyber Recovery – Weer aan de slag

Herstel en probleemoplossing

PowerProtect Cyber Recovery biedt geautomatiseerde herstelprocedures om bedrijfskritieke systemen snel en met vertrouwen weer online te brengen. Herstel wordt geïntegreerd in uw incidentresponsproces. Nadat een incident heeft plaatsgevonden, analyseert het incidentresponsteam de productieomgeving om de hoofdoorzaak van de gebeurtenis te bepalen. CyberSense biedt ook forensische rapporten na de aanval om de diepte en breedte van de aanval te begrijpen en biedt een lijst van de laatste goede back-upsets voordat er schade was. Wanneer de productie klaar is voor herstel, biedt Cyber Recovery beheertools en de technologie die het daadwerkelijke dataherstel uitvoert.

Oplossingsplanning en -ontwerp

Met Dell Professional Services for Cyber Recovery kunt u bepalen welke bedrijfskritieke systemen u moet beschermen. Ook kunnen we afhankelijkheidsoverzichten maken voor de bijbehorende applicaties en services, evenals de infrastructuur die nodig is om deze te herstellen. De service genereert ook herstelvereisten en ontwerpalternatieven, en identificeert de technologieën voor het analyseren, hosten en beschermen van uw data, samen met een business case en implementatietijdlijn.

Conclusie

Branche-initiatieven zoals Sheltered Harbor maken gebruik van PowerProtect Cyber Recovery om klanten, financiële instellingen en het vertrouwen van het publiek in het financiële systeem van de VS te beschermen in het geval van een cyberaanval die ervoor zorgt dat essentiële systemen uitvallen, inclusief back-ups. Met duizenden klanten geeft Cyber Recovery met CyberSense vertrouwen aan bedrijfsleiders en heeft het bewezen het herstel van data te versnellen in het geval van een cyberdreiging.

Met PowerProtect Cyber Recovery kunt u erop vertrouwen dat u na een cyberaanval snel bekende goede data kunt identificeren en herstellen en de normale bedrijfsactiviteiten kunt hervatten.

Het is tijd om weer aan de slag te gaan.



Meer informatie over
Dell PowerProtect
Cyber Recovery



Neem contact op met
een Dell
Technologies expert



Bekijk meer
informatiebronnen



Neem deel aan
het gesprek via
#PowerProtect

¹Gebaseerd op onderzoek van Vanson Bourne in opdracht van Dell Technologies, "Global Data Protection Index 2024 Snapshot", Oktober 2023.

²Onderzoek door Forrester Consulting in opdracht van Dell Technologies, "The Total Economic Impact of Dell PowerProtect Cyber Recovery", augustus 2023

³Gebaseerd op een ESG-rapport in opdracht van Index Engines, "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption", Juni 2024