Oplossingsoverzicht

CyberSense® voor PowerProtect Cyber Recovery

Op AI gebaseerde machine learning, analyses en forensische tools om cyberaanvallen te detecteren, te diagnosticeren en achteraf te herstellen

HET VOORDEEL VAN CYBERSENSE

CyberSense® is volledig geïntegreerd met de Dell PowerProtect Cyber Recovery Vault oplossing.

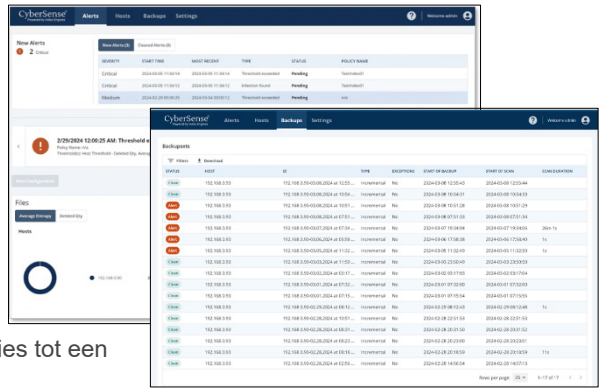
- Deze integratie maakt een geautomatiseerde aanpak mogelijk voor het regelmatig scannen van back-updata om de integriteit van de data te valideren en te waarschuwen wanneer verdacht gedrag wordt gedetecteerd.
- De mogelijkheid van CyberSense om rechtstreeks interne back-upimages te scannen, waaronder Dell NetWorker, Avamar, PowerProtect Data Manager en meer, maakt het mogelijk om inhoud te analyseren zonder dat de data opnieuw hoeft te worden gehydrateerd.
- Alleen CyberSense levert volledige contentanalyse bij elke scan van de data om zelfs de meest geavanceerde ransomware-aanvallen die gemakkelijk onopgemerkt kunnen blijven te detecteren met behulp van lichtgewicht scantools die alleen metadata inspecteren.
- Wanneer zich een aanval voordoet biedt CyberSense 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 om het herstelproces te versnellen.

CyberSense onderscheidt zich van andere benaderingen voor data-analyse en biedt een hoger niveau van vertrouwen in de integriteit van back-updata en dat deze snel kunnen worden hersteld nadat een aanval heeft plaatsgevonden.

Wanneer conventionele beveiligingstools tekortschieten in het beschermen van data tegen cyberaanvallen, komt **CyberSense®** in actie om databeschadiging na een aanval met een nauwkeurigheid van 99,5% te detecteren en intelligent en snel herstel mogelijk te maken. CyberSense fungeert als de laatste verdedigingslinie en eerste herstellinie voor duizenden organisaties over de hele wereld en waarborgt de integriteit van hun datamiddelen, inclusief kerninfrastructuur, productiedatabases en kritieke documenten, waardoor het vertrouwen wordt gewekt dat de data vrij zijn van kwaadaardige corruptie.

CyberSense maakt gebruik van databack-ups om te zien hoe data in de loop van de tijd veranderen en maakt vervolgens gebruik van op AI gebaseerde machine learning om tekenen van beschadiging te detecteren die duiden op een ransomware-aanval. Machine learning onderzoekt vervolgens deze 200+ op inhoud gebaseerde analyses om beschadigingen te vinden met een betrouwbaarheid van 99,5%, zodat u uw bedrijfskritieke infrastructuur en inhoud kunt beschermen. CyberSense detecteert massaverwijderingen, versleuteling en andere verdachte wijzigingen in de kerninfrastructuurcomponenten (waaronder Active Directory, DNS, enz.), gebruikersbestanden en kritieke productiedatabases als gevolg van ingewikkelde aanvallen. Als CyberSense tekenen van beschadiging detecteert, wordt er een waarschuwing gegenereerd in het dashboard met aanvullende informatie over de omvang en impact van de aanval.

Wanneer verdacht gedrag optreedt, levert CyberSense forensische rapporten na de aanval om de schade van de cyberaanval te diagnosticeren. Wanneer databeschadiging wordt gedetecteerd, is er een lijst beschikbaar met de laatst bekende goede back-updatasets ter ondersteuning van een snel herstel dat helpt om bedrijfsonderbrekingen en dataverlies tot een minimum te beperken.



De Cyber Recovery workflow

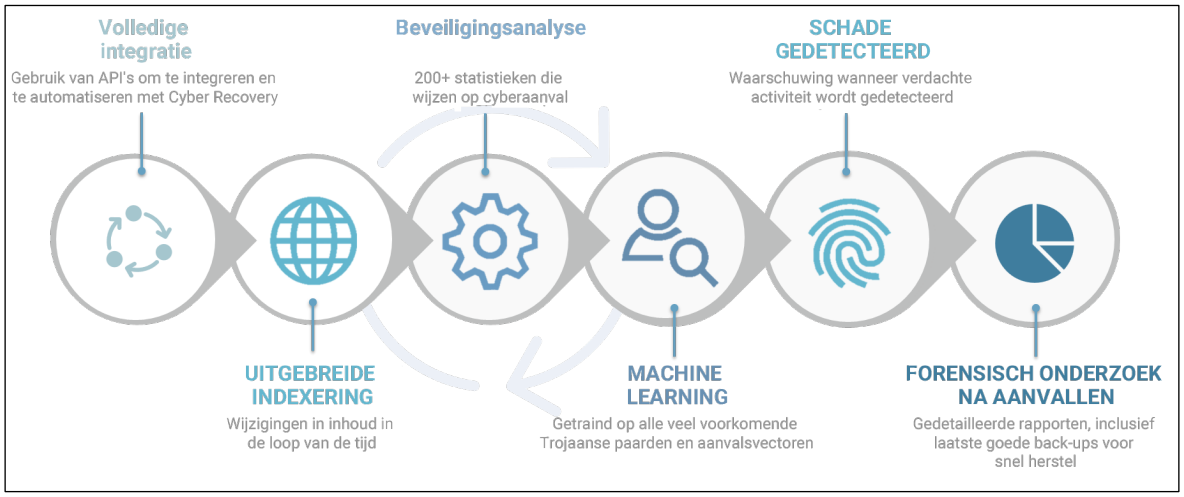
CyberSense integreert *naadloos* met Dell PowerProtect Cyber Recovery, bestanden en databases worden actief bewaakt om beschadiging door ransomware te detecteren via analyse van de integriteit van de data. **Zodra data zijn gerepliceerd naar de Cyber Recovery-kluis en de retentievergrendeling wordt toegepast, voert** CyberSense **automatisch een *uitgebreide* scan van de back-updata uit, waardoor point-in-time observaties van bestanden, databases en core-infrastructuur worden gemaakt.** Deze observaties stellen CyberSense in staat om wijzigingen in bestanden over de loop van de tijd nauwgezet te volgen, waardoor databeschadiging door zelfs de meest geavanceerde cyberbedreigingen effectief aan het licht komt.

De CyberSense-scan werkt rechtstreeks op data in de back-upimage, waardoor de oorspronkelijke back-upsoftware en rehydratatie van de data overbodig zijn. Met behulp van geavanceerde analyse identificeert CyberSense versleuteling/beschadiging van bestanden of databasepagina's, bekende malware-extensies, massale verwijdering/aanmaak van bestanden en meer.

Met behulp van op AI gebaseerde machine learning-algoritmen die zijn getraind met de nieuwste Trojaanse paarden en ransomware, neemt CyberSense deterministische beslissingen over databeschadiging die wijzen op een cyberaanval. In het geval van een aanval wordt er onmiddellijk een kritieke waarschuwing weergegeven in het dashboard van Cyber Recovery. Daarnaast biedt CyberSense forensische rapporten na de aanval, waardoor een snelle diagnose en herstelna ransomware-aanvallen mogelijk wordt om dataverlies tot een minimum te beperken.

Volledige contentanalytics

CyberSense is het enige product op de markt dat volledige op content gebaseerde analyses levert voor alle beschermde data. Met deze mogelijkheid onderscheidt CyberSense zich van andere oplossingen die een totaaloverzicht van de data krijgen en die analytics gebruiken die op basis van metadata duidelijke tekenen van beschadiging zoeken. Beschadiging op metadataniveau is niet moeilijk te detecteren; denk bijvoorbeeld aan een bestandsextensie wijzigen naar .encrypted of een ingrijpende wijziging van de bestandsgrootte. Dit soort aanvallen vertegenwoordigt niet de geavanceerde aanvallen die cybercriminelen tegenwoordig gebruiken.



CyberSense gaat verder dan alleen metadata-oplossingen, omdat de oplossing gebaseerd is op volledige contentanalytics om databeschadiging te detecteren. Bestanden en databases worden gecontroleerd op aanvallen die op content gebaseerde beschadiging van de bestandsstructuur of gedeeltelijke versleuteling in een document of pagina van een database omvatten. Deze aanvallen kunnen niet worden gevonden met behulp van analytics die niet in het bestand scannen om te vergelijken hoe de bestanden in de loop der tijd veranderen. Zonder volledige contentgebaseerde analytics zal het aantal fout-negatieve resultaten aanzienlijk zijn, wat ten onrechte vertrouwen inboezemt in uw data-integriteit en -beveiliging. Daarnaast kunnen aangepaste meldingen bij het bereiken van de drempelwaarde worden gemaakt op basis van het aantal of percentage gewijzigde bestanden of bestandstypen, toegevoegde of verwijderde bestanden en entropie over een host.

Ondersteunde datatypen

CyberSense genereert analyses op basis van een uitgebreide reeks gegevenstypen. Dit omvat kerninfrastructuur zoals DNS, LDAP, Active Directory, ongestructureerde bestanden zoals documenten, contracten, intellectueel eigendom en databases zoals Oracle, DB2, SQL, PostgreSQL, Epic Caché, enz.

Samenvatting

CyberSense is volledig geïntegreerd met Dell PowerProtect Cyber Recovery en controleert uw data en detecteert indicatoren van inbreuk en beschadiging. Met CyberSense krijgt u proactief inzicht in de omvang van een bezige cyberaanval, waardoor u gemakkelijker een plan kunt implementeren om snel een diagnose te stellen en van de aanval kunt herstellen. Zo kunt u bedrijfsonderbrekingen en de bijbehorende aanzienlijke kosten beperken.

Meer informatie over Dell PowerProtect Cyber Recovery	Neem contact op met een Dell Technologies expert	Meer informatie over CyberSense	Neem deel aan het gesprek via #PowerProtect