DELL Technologies

Oplossingsoverzicht

CyberSense® voor Dell PowerProtect Cyber Recovery

Door AI aangedreven analyses en forensische tools om cyberaanvallen slimmer te detecteren, te diagnosticeren en achteraf ervan te herstellen

HET VOORDEEL VAN CYBERSENSE

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

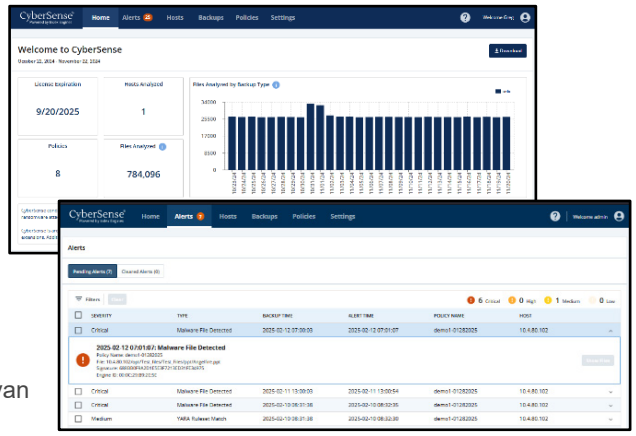
- Automatiseert het regelmatig scannen van back-updata om de data-integriteit te valideren en te waarschuwen wanneer verdacht gedrag wordt gedetecteerd.
- Scan rechtstreeks content in back-upimages van Dell Avamar, NetWorker, CommVault, NetBackup en PowerProtect Data Manager zonder dat u de data hoeft te rehydrateren.
- Levert diepgaande analyse van volledige content bij elke datascan om zelfs de meest geavanceerde ransomware-aanvallen te detecteren.
- Aangepaste waarschuwingen voor YARA-regels en malwarehandtekeningen om bekend gedrag van ransomware of interne kwaadwillenden te detecteren.
- Bevordert een slimmer en sneller herstel met 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.

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.

Naarmate de frequentie van cyberaanvallen blijft toenemen en cybercriminelen veerkrachtiger worden, schieten conventionele beveiligingstools tekort bij het beschermen van data tegen cyberaanvallen.

CyberSense® detecteert databeschadiging na een aanval met 99,99% nauwkeurigheid* en maakt intelligent en snel herstel mogelijk. CyberSense fungeert als eerste herstellinie voor duizenden organisaties over de hele wereld en waarborgt de integriteit van datamiddelen, inclusief kerninfrastructuur, databases en kritieke documenten, zodat u erop kunt vertrouwen dat de data vrij zijn van kwaadaardige corruptie.

CyberSense scant back-ups van data in een Cyber Recovery-kluis om te zien hoe data in de loop van de tijd veranderen. Het maakt vervolgens gebruik van machine learning en AI om tekenen van beschadiging te detecteren die wijzen op een ransomware-aanval. Data worden vergeleken met meer dan 200 op inhoud gebaseerde analyses om beschadigingen te identificeren met een betrouwbaarheid van 99,99%*, 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.), bestandsrepository's, bestandssystemen en kritieke databases als gevolg van geavanceerde aanvallen.



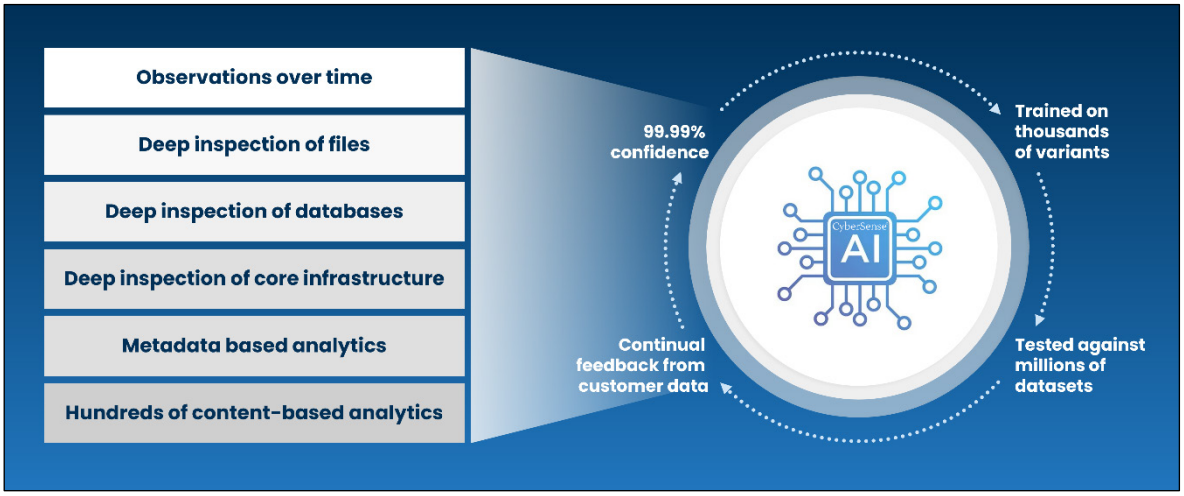
Wanneer verdacht gedrag optreedt, levert CyberSense forensische rapporten na de aanval om de schade van de cyberaanval te diagnosticeren. Wanneer databeschadiging wordt gedetecteerd, is er een lijst beschikbaar met de laatst bekende goede back-updatasets ter ondersteuning van een snel herstel dat helpt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

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.** CyberSense volgt wijzigingen in bestanden over de loop van de tijd nauwgezet, waardoor databeschadiging door zelfs de meest geavanceerde cyberbedreigingen effectief aan het licht komt.

Volledige contentanalytics

CyberSense is het enige product op de markt dat volledige op content gebaseerde indexeringen en analyses levert voor alle beschermde data. De diepgaande AI-analyse van CyberSense onderzoekt alle data en er wordt een waarschijnlijkheidsbeslissing gegenereerd met een nauwkeurigheid van 99,99%* over de vraag of de data betrouwbaar zijn of beschadigd zijn door ransomware. 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 en detecteert beschadigde data met behulp van volledige contentanalyses. Het controleert bestanden en databases op wijzigingen die wijzen op een aanval, inclusief volledige of gedeeltelijke bestandsbeschadiging. Traditionele analyes missen deze dreigingen, wat leidt tot vals vertrouwen. Aangepaste drempelwaardewaarschuwingen kunnen worden ingesteld op basis van wijzigingen in bestanden, toegevoegde bestanden of verwijderde bestanden. Aangepaste YARA-regels en malwarehandtekeningen kunnen ook worden geïmplementeerd voor zowel voorwaartse als achterwaartse detectie van malware in back-ups.

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 analyseert de data in uw kluis en detecteert gedragsindicatoren van inbreuk en beschadiging. Met CyberSense krijgt u proactief inzicht in de omvang van een actieve 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

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

DELL Technologies