Lösningsöversikt

CyberSense® för PowerProtect Cyber Recovery

AI-baserad maskininlärning, analys och utredningsverktyg för att upptäcka, diagnostisera och återställa efter cyberattacker

FÖRDELEN MED CYBERSENSE

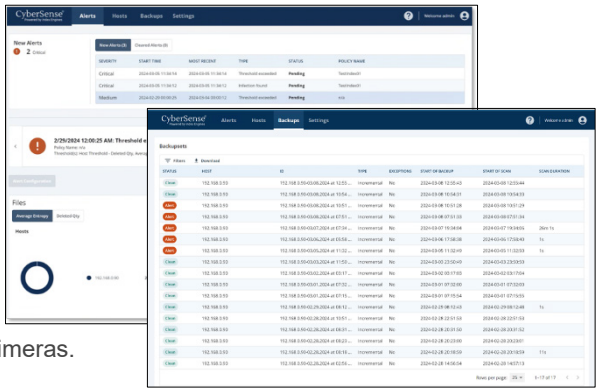
CyberSense® är helt integrerat med valvlösningen Dell PowerProtect Cyber Recovery.

- Med den här integreringen möjliggörs en automatiserad metod för regelbunden genomsökning av säkerhetskopierade data för att validera dataintegriteten och varna när misstänkt beteende upptäcks.
- CyberSense har kapaciteten att direkt söka igenom säkerhetskopierade avbildningar, inklusive Dell NetWorker, Avamar, PowerProtect Data Manager med mera, vilket gör det möjligt att analysera innehåll utan att behöva extrahera data.
- Det är endast CyberSense som levererar fullständig innehållsanalys vid varje datagenomsökning för att upptäcka även de mest sofistikerade utpressningsvirusattackerna som lätt kan förbli oupptäckta av enklare genomsökningsverktyg som endast inspekterar metadata.
- När en attack inträffar tillhandahåller CyberSense utredande rapporter efter attacken för att du ska kunna förstå attackens djup och bredd, samt en lista över de sista bra uppsättningarna säkerhetskopior före skadan för att underlätta återställningsprocessen.

CyberSense skiljer sig från andra dataanalysmetoder och ger en högre nivå av förtroende för integriteten hos säkerhetskopierade data, som snabbt kan återställas efter en attack.

När konventionella säkerhetsverktyg inte räcker till för att skydda data mot cyberattacker träder **CyberSense®** in för att upptäcka skadade data efter en attack med 99,5 % träffsäkerhet. CyberSense gör det enklare att återställa snabbt och på ett intelligent sätt. CyberSense fungerar som sista försvarslinjen och första återställningslinjen för tusentals organisationer över hela världen och säkerställer integriteten för deras datatillgångar. Däribland finns kärninfrastruktur, produktionsdatabaser och avgörande dokument, vilket ingjuter ett förtroende för att dessa data är rena från skadlig korruption.

I CyberSense används säkerhetskopiering av data för att övervaka hur data förändras över tid. Sedan används AI-baserad maskininlärning för att upptäcka tecken på skada som tyder på en utpressningsvirusattack. Maskininlärning undersöker sedan dessa över 200 innehållsbaserade analyser för att hitta korruption med 99,5 % träffsäkerhet, vilket hjälper dig att skydda den infrastruktur och det innehåll som är affärsavgörande för dig. Med CyberSense upptäcks även massradering, kryptering och andra misstänkta ändringar i kärninfrastrukturkomponenter (till exempel Active Directory, DNS osv.), användarfiler och avgörande produktionsdatabaser till följd av sofistikerade attacker. Om tecken på skada upptäcks genom CyberSense genereras en varning på instrumentpanelen med ytterligare information om attackens omfattning och inverkan.



När misstänkt beteende inträffar skapas utredande rapporter efter attacken i CyberSense för att diagnostisera cyberattackens räckvidd. Om skadade data upptäcks finns en lista över de senast fungerande uppsättningarna säkerhetskopierade data tillgänglig för att möjliggöra en snabb återställning så att avbrott i verksamheten och dataförlust minimeras.

Arbetsflödet för Cyber Recovery

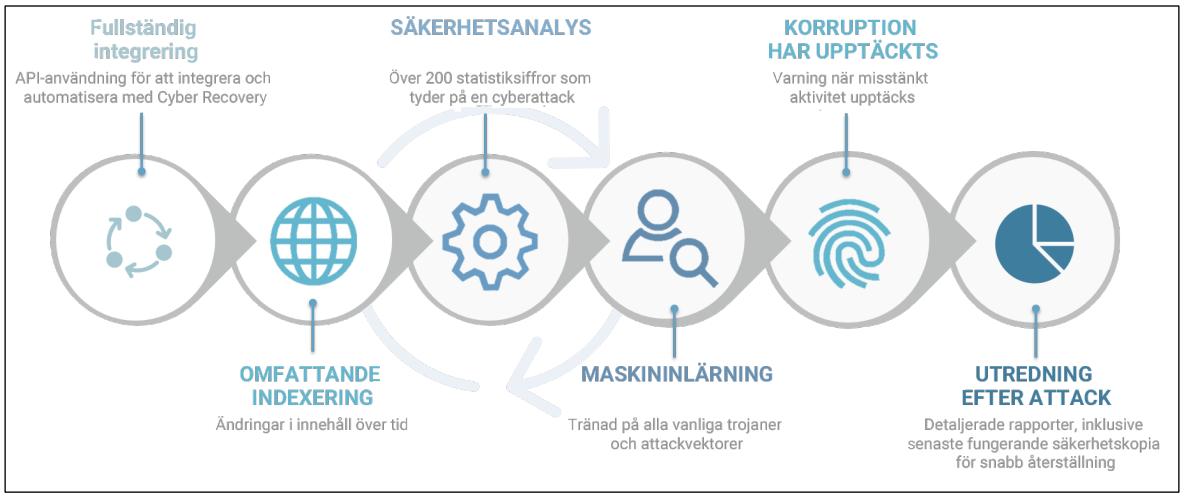
CyberSense integreras sömlöst med Dell PowerProtect Cyber Recovery så att filer och databaser övervakas aktivt genom att integritetsanalyser för att upptäcka skada från utpressningsvirus. När data har kopierats till Cyber Recovery-valvet och kvarhållningslåset har tillämpats initieras automatiskt en omfattande genomsökning av säkerhetskopierade data i CyberSense. Tidspunktsbaserade observationer av filer, databaser och kärninfrastrukturer skapas. Dessa observationer gör det möjligt för CyberSense att tillhandahålla noggrant spårade ändringar i filer över tid, vilket är ett effektivt sätt att röja skadade data, även från de mest sofistikerade cyberhoten.

CyberSense-genomsökningen körs direkt på data i säkerhetskopieringsavbildningen, vilket eliminerar behovet av den ursprungliga mjukvaran för säkerhetskopiering och extrahering av data. Genom avancerad analys identifieras kryptering/skada av filer eller databassidor i CyberSense, känns kända tillägg för skadlig kod igen, och massradering/skapande av filer med mera kan upptäckas.

Med hjälp av AI-baserade maskininlärningsalgoritmer som tränats med de senaste trojanerna och de senaste utpressningsvirusen fattas deterministiska beslut om datakorruption som tyder på en cyberattack i CyberSense. I händelse av en attack visas en kritisk varning omedelbart på Cyber Recovery-instrumentpanelen. Dessutom får du utredande rapporter efter attacker i CyberSense, vilket underlättar snabb diagnos och återställning från utpressningsvirusattacker för att minimera dataförlust.

Fullständig innehållsanalys

CyberSense är den enda produkten på marknaden som levererar analys baserat på fullständigt innehåll av alla skyddade data. Den här funktionen skiljer CyberSense från andra lösningar som har en översikt över data och använder analyser som letar efter uppenbara tecken på skada baserat på metadata. En skada på metadatanivå, till exempel en ändring av ett filtillägg till krypterad eller en avsevärd ändring i filstorlek, är inte svår att upptäcka. Dessa typer av attacker representerar inte de sofistikerade attacker som cyberbrottslingar använder idag.



CyberSense går längre än lösningar som enbart är metadatabaserade, eftersom det bygger på analys av fullständigt innehåll för att upptäcka skadade data. Filer och databaser granskas för attacker, däribland innehållsbaserad skada på filstrukturen eller delkryptering i ett dokument eller en sida av en databas. Dessa attacker kan inte upptäckas med hjälp av analyser som inte genomsöker filens innehåll för att jämföra förändringen över tid. Utan fullständigt innehållsbaserad analys blir antalet falska negativa resultat betydande, vilket ger en falsk känsla av förtroende om din dataintegritet och säkerhet. Dessutom kan anpassade tröskelvärdesvarningar skapas baserat på antalet eller procentandelen ändrade filer eller filtyper, tillagda eller borttagna filer och en värds entropi.

Datatyper som stöds

Med CyberSense genereras analyser från ett omfattande utbud av datatyper. Däribland finns kärninfrastruktur såsom DNS, LDAP och Active Directory, ostrukturerade filer såsom dokument, kontrakt och upphovsrätter samt databaser såsom Oracle, DB2, SQL, PostgreSQL, Epic Caché, osv.

Sammanfattning

CyberSense är helt integrerat med Dell PowerProtect Cyber Recovery, så att dina data granskas och indikatorer på intrång och skada upptäcks. Med CyberSense kan du proaktivt förstå omfattningen av en cyberattack medan den sker, vilket underlättar implementeringen av en plan för att snabbt diagnostisera och återställa. På så sätt minskar du avbrott i verksamheten och tillhörande betydande utgifter.

Mer information om Dell PowerProtect Cyber Recovery	Kontakta en Dell Technologies-expert	Mer information om CyberSense	Var med i samtalet med #PowerProtect