Lösningsöversikt

CyberSense® för Dell PowerProtect Cyber Recovery

AI-förstärkt analys- och utredningsverktyg för att upptäcka, diagnostisera och återställa på ett smartare sätt efter cyberattacker

FÖRDELEN MED CYBERSENSE

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

- Automatiserar regelbunden genomsökning av säkerhetskopieringsdata för att validera dataintegritet och varna när misstänkt beteende upptäcks.
- Skanna innehåll direkt inom säkerhetskopieringsavbildningar från Dell Avamar, NetWorker, Commvault, NetBackup och PowerProtect Data Manager, utan att behöva återhydrera data.
- Ger djupgående analys av allt innehåll vid varje genomsökning av data för att upptäcka även de mest sofistikerade attackerna från utpressningsprogram.
- Anpassade varningar för YARA-regler och signaturer för skadliga program för att upptäcka känt beteende från utpressningsprogram eller interna illvilliga aktörer.
- Underlättar en smartare och snabbare återställning med kriminaltekniska rapporter efter attacken för att få detaljerade insikter om attackens djup och bredd, samt ger en lista över de senaste bra uppsättningarna av säkerhetskopieringar före skadan.

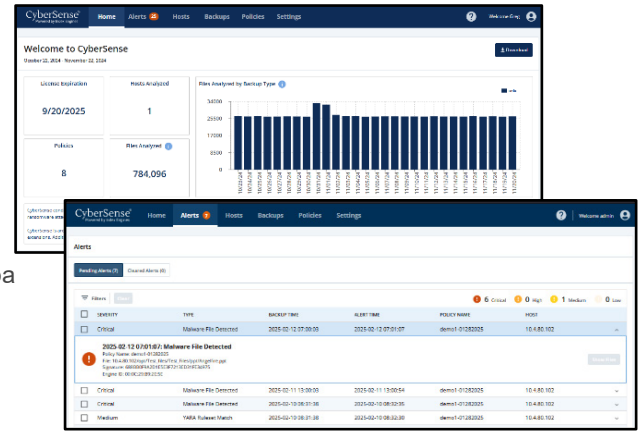
CyberSense skiljer sig från andra dataanalysmetoder och ger en högre nivå av förtroende för integriteten hos säkerhetskopierade data, som snabbt kan återställas efter en attack.

I takt med att frekvensen av cyberattacker fortsätter att öka och cyberbrottslingar blir mer motståndskraftiga är konventionella säkerhetsverktyg inte tillräckliga för att skydda data mot cyberattacker.

CyberSense® går in för att upptäcka skadade data efter en attack med 99,99 % noggrannhet* och underlättar smart och snabb återställning. CyberSense fungerar som första återställningslinjen för tusentals organisationer över hela världen och säkerställer integriteten för datatillgångar. Däribland finns kärninfrastruktur, databaser och avgörande dokument, vilket ingjuter ett förtroende för att dessa data är rena från skadlig korruption.

CyberSense söker igenom datasäkerhetskopior i ett Cyber Recovery-valv för att observera hur data ändras över tid. Den använder sedan maskininlärning och AI för att upptäcka tecken på korruption som tyder på en attack av utpressningsprogram. Data jämförs med över 200 innehållsbaserade analyser för att identifiera korruption med 99,99 % 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.), fildatalager, filsystem och avgörande databaser till följd av sofistikerade attacker.

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 snabba återställningar så att avbrott i verksamheten och dataförlust minimeras – vilket i sin tur sänker kostnaden för cyberåterställning.

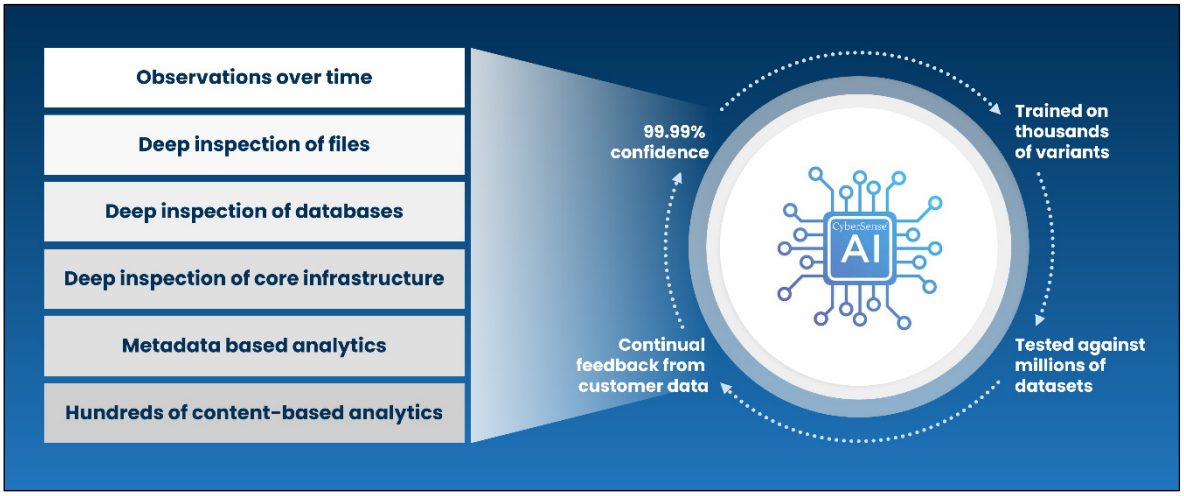


Arbetsflödet för Cyber Recovery

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. CyberSense spårar noggrant ändringar i filer över tid, vilket är ett effektivt sätt att röja skadade data, även från de mest sofistikerade cyberhoten.

Fullständig innehållsanalys

CyberSense är den enda produkten på marknaden som levererar indexering och analys baserat på allt innehåll av alla skyddade data. CyberSense djupgående AI-analys körs genom de fullständiga data som finns och ett slumpmässigt beslut genereras med 99,99 % noggrannhet* om huruvida data har integritet eller om de har skadats av utpressningsprogram. 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 bara metadatalösningar och upptäcker skadade data med hjälp av analys av allt innehåll. Den granskar filer och databaser för ändringar som tyder på en attack, inklusive fullständig eller partiell filskada. Traditionella analystekniker missar dessa hot, vilket leder till falskt förtroende. Anpassade tröskelvarningar kan ställas in baserat på förändringar i filer, tillagda filer eller borttagna filer. Anpassade YARA-regler och signaturer för skadliga program kan också implementeras för både framåt- och bakåtdetektering av skadliga program i säkerhetskopior.

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 i valvet analyseras och beteendemässiga indikatorer på intrång och skada upptäcks. Med CyberSense kan du proaktivt förstå omfattningen av en cyberattack medan den sker, underlätta 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 av Dell Technologies experter	Mer information om CyberSense	Var med i samtalet med #PowerProtect

* Baserat på en ESG-rapport som beställts av Index Engines: ”Index Engines’ CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption”. juni 2024