DELL Technologies

솔루션 브리프

CyberSense® for Dell PowerProtect Cyber Recovery

사이버 공격을 탐지 및 진단하고 스마트하게 복구하기 위한 AI 기반 분석 및 포렌식 툴

CyberSense의 장점

CyberSense®는 Dell PowerProtect Cyber Recovery 볼트 솔루션과 완벽하게 통합됩니다.

- 백업 데이터의 정기적인 검사를 자동화하여 데이터 무결성을 검증하고 의심스러운 동작이 탐지되면 알림을 보냅니다.
- 데이터를 리하이드레이션할 필요 없이 Dell Avamar, NetWorker, Commvault, NetBackup 및 PowerProtect Data Manager의 백업 이미지 내에서 콘텐츠를 직접 검사합니다.
- 모든 데이터 검사를 통해 심층적인 전체 콘텐츠 분석을 제공하여 가장 정교한 랜섬웨어 공격도 탐지합니다.
- YARA 규칙 및 멀웨어 서명에 대한 맞춤형 알림을 통해 랜섬웨어 또는 내부 악의적 행위자의 알려진 동작을 탐지합니다.
- 공격 후 포렌식 보고서를 통해 더 빠르고 스마트한 복구를 용이하게 하여 공격의 수준과 범위를 상세하게 파악하며, 손상되기 전 마지막으로 양호한 백업 세트 목록을 제공합니다.

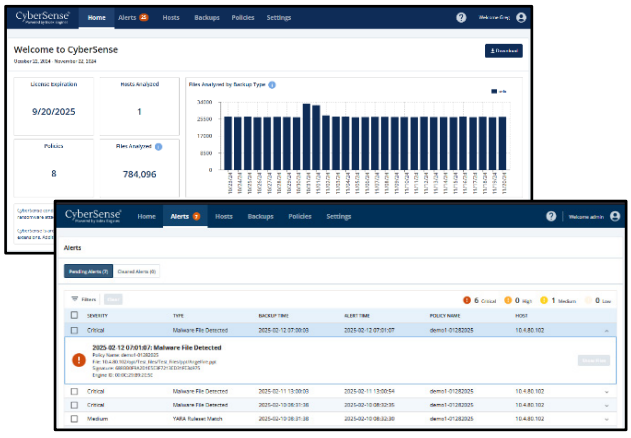
CyberSense는 다른 데이터 분석 접근 방식과 차별화되며, 백업 데이터의 무결성을 보존하고 공격이 발생했을 때 신속한 복구를 보장하는 더 높은 수준의 신뢰도를 제공합니다.

사이버 공격의 빈도가 계속 증가하고 사이버 범죄자의 회복탄력성이 높아짐에 따라 기존의 보안 툴은 사이버 공격으로부터 데이터를 보호하는 데 부족합니다.

CyberSense®는 공격 발생 후 99.99%의 정확도*로 데이터 손상을 탐지하므로, 지능적이고 신속한 복원이 가능합니다. 전 세계 수천 개 조직을 위한 1차 복구 역할을 수행하는 CyberSense는 핵심 인프라스트럭처, 데이터베이스 및 중요 문서를 비롯한 데이터 자산의 무결성을 보장하여 데이터가 악의적으로 손상되지 않는다고 안심할 수 있게 해줍니다.

CyberSense는 Cyber Recovery 볼트의 데이터 백업을 검사하여 시간이 지남에 따라 데이터가 어떻게 변경되는지 관찰합니다. 그런 다음 머신 러닝과 AI를 활용하여 랜섬웨어 공격을 나타내는 손상 징후를 탐지합니다. 데이터는 200가지 이상의 콘텐츠 기반 분석 정보와 비교하여 99.99%의 신뢰도*로 손상을 찾아내 비즈니스 크리티컬 인프라스트럭처와 콘텐츠를 보호할 수 있도록 지원합니다. CyberSense는 핵심 인프라스트럭처(Active Directory, DNS 등 포함), 파일 리포지토리, 파일 시스템 및 중요 운영 데이터베이스에서 교묘한 공격으로 인한 대량 삭제, 암호화 및 기타 의심스러운 변화를 탐지합니다.

의심스러운 동작이 발생하면 CyberSense는 공격 후 포렌식 보고서를 제공하여 사이버 공격의 영향 범위를 진단합니다. 데이터 손상이 탐지되면 마지막으로 양호하게 수행된 백업 데이터 세트 목록을 사용하여 신속한 선별적 복구를 지원하기 때문에 비즈니스 중단 및 데이터 손실을 최소화함으로써 사이버 복구의 비용을 낮출 수 있습니다.



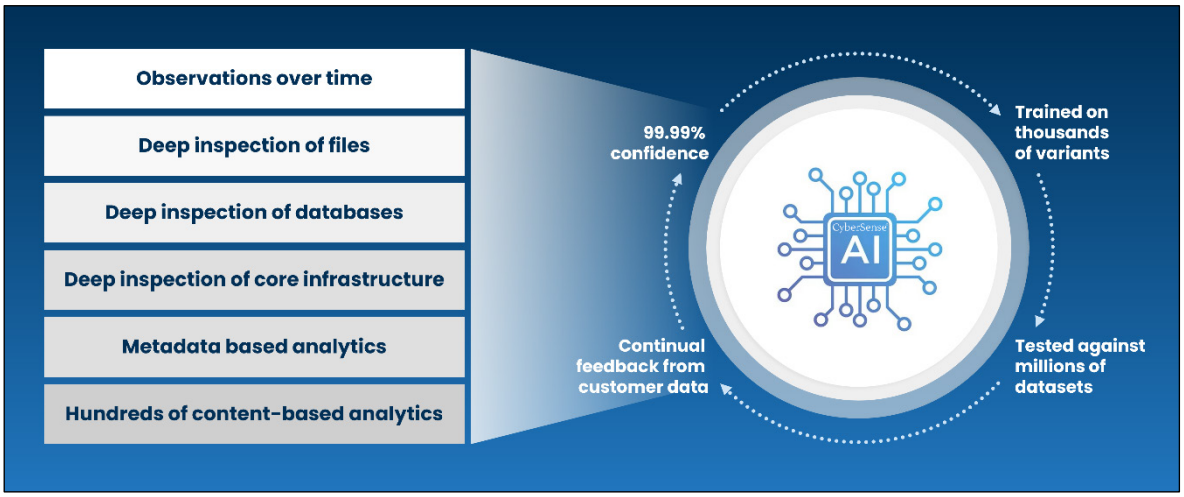
Cyber Recovery 워크플로

CyberSense는 Dell PowerProtect Cyber Recovery와 원활하게 통합되어 파일 및 데이터베이스를 능동적으로 모니터링하고 데이터 무결성을 분석하여 랜섬웨어 손상을 탐지합니다. 데이터가 Cyber Recovery 볼트에 복제되고 보존 잠금이 적용되면 CyberSense가 자동으로 백업 데이터에 대한 포괄적인 검사를 시작하여 파일, 데이터베이스 및 핵심 인프라스트럭처에 대한 시점 관찰 정보를 생성합니다. CyberSense는 시간 경과에 따른 파일의 변화를 세심하게 추적하여 매우 교묘한 사이버 위협에 의한 데이터 손상도 효과적으로 발견합니다.

© 2025 Dell Inc. or its subsidiaries.

전체 콘텐츠 분석

CyberSense는 보호되는 모든 데이터에 대한 전체 콘텐츠 인덱스 및 분석을 독보적으로 제공합니다. CyberSense의 심층 AI 분석은 전체 데이터에 걸쳐 실행되며, 데이터의 무결성 여부 또는 랜섬웨어에 의해 손상되었는지 여부에 대해 99.99%의 정확도*로 확률적인 결정을 내립니다. 이는 CyberSense의 차별화되는 지점으로, 기존의 다른 솔루션은 전체 데이터가 아닌 중요한 데이터를 선별하여 조회하고 메타데이터를 기반으로 손상 징후를 식별합니다. 메타데이터 수준 손상은 탐지하기가 어렵지 않습니다. 예를 들면 파일 확장명이 .encrypted로 변경되거나 파일 크기가 크게 변경됩니다. 오늘날 사이버 범죄자들은 이러한 유형의 공격을 사용하지 않고 더욱 교묘한 방식으로 공격합니다.



CyberSense는 메타데이터 전용 솔루션을 넘어 전체 콘텐츠 분석을 사용하여 데이터 손상을 탐지합니다. 파일 및 데이터베이스를 감사하여 전체 또는 부분 파일 손상을 포함하여 공격을 나타내는 변경 사항을 확인합니다. 기존 분석은 이러한 위협을 놓치며 잘못된 신뢰도를 갖게 합니다. 사용자 지정 임계값 알림은 파일 변경, 추가된 파일 또는 삭제된 파일에 따라 설정할 수 있습니다. 또한 백업에서 멀웨어의 정방향 및 역방향 탐지를 위해 맞춤형 YARA 규칙 및 멀웨어 서명을 구현할 수 있습니다.

지원되는 데이터 유형

CyberSense는 광범위한 데이터 유형에서 분석 정보를 생성합니다. 여기에는 DNS, LDAP, Active Directory와 같은 핵심 인프라스트럭처와 문서, 계약서, 지적 재산과 같은 비정형 파일을 비롯하여 Oracle, DB2, SQL, PostgreSQL, Epic Caché 등의 데이터베이스가 포함됩니다.

Summary

Dell PowerProtect Cyber Recovery와 완벽하게 통합된 CyberSense는 볼트 데이터를 분석하고 침해 또는 손상의 징후를 탐지합니다. CyberSense는 진행 중인 사이버 공격의 영향 범위를 사전 예방적으로 파악하여 신속한 진단 및 복구 계획을 구현하도록 지원하여 비즈니스 중단과 이로 인한 막대한 비용을 줄입니다.

Dell PowerProtect Cyber Recovery에 대한 자세한 정보

문의 CyberSense에 대한

자세한 정보

대화 참여:
#PowerProtect

* Index Engines 의뢰로 작성된 ESG 보고서 “Index Engines’ CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption” 기준. 2024년 6월

© 2025 Dell Inc. or its subsidiaries. All Rights Reserved. Dell 및 기타 상표는 Dell Inc. 또는 해당 자회사의 상표입니다. 기타 상표는 해당 소유주의 상표일 수 있습니다.