CISO들이 백업 데이터를 보안 자산으로 전환하는 3가지 방법

개요

백업 데이터는 전략적 우위를 제공할 수 있습니다. 조직은 여기에 담긴 풍부한 과거 인사이트를 활용하여 위협 탐지를 강화하고, 사고 대응을 가속화하며, 전반적인 보안 레질리언스를 강화할 수 있습니다.

다음은 백업 데이터를 강력한 보안 이점으로 전환하는 세 가지 방법입니다.

1. 향상된 위협 헌팅

위협 헌팅에 고급 백업 시스템을 사용하면 몇 가지 주요 이점이 있습니다. 주요 환경과의 격리를 통해 공격자, 특히 EDR 및 XDR 도구를 우회하기 위해 랜섬웨어 서비스형(RaaS) 플랫폼에 회피 기술을 내재화한 랜섬웨어 갱단도 피할 수 없는 은밀하고 수동적인 위협 헌팅이 가능해집니다. 또한 백업은 과거 및 조직 전체의 가시성을 제공하므로 분석가는 악의적인 활동의 장기적 패턴과 겉보기에는 관련이 없어 보이는 이벤트 간의 연결성을 찾아낼 수 있습니다.

2. 향상된 데이터 컴플라이언스

AI 강화 보안 도구가 주목을 받음에 따라, DSPM(Data Security Posture Management) 솔루션을 고급 백업 시스템과 통합하면 데이터 보호를 크게 강화할 수 있습니다. DSPM 도구는 민감한 데이터를 식별하고 해당 데이터의 위치, 사용자 및 보안 태세에 대한 가시성을 제공합니다. 최신 백업 시스템과 결합하면 보안 및 컴플라이언스 리더는 보호되지 않은 자산을 신속하게 파악하고, 데이터 중요도에 따라 백업 및 복구를 최적화하며, 침해의 영향 범위를 평가해 사고 대응을 가속화할 수 있습니다.

3. 종합적인 사고 대응 및 복구

강력한 사고 대응 및 복구 전략은 보안 사고가 조직에 미치는 영향을 최소화하는 데 매우 중요합니다. 백업 데이터는 복구가 신속하고 완전하게 이루어지도록 보장하여 가동 중단 시간과 데이터 손실을 줄이는 데 중요한 역할을 합니다. 데이터 복원 외에도 고급 백업 시스템은 사고 대응에도 유용합니다. 위협을 조기에 탐지하고 이러한 위협을 SOC 도구와 공유하여 더 빠른 분류를 지원할 수 있습니다. 사고 대응자는 백업 스냅숏 전반에서 파일 시스템 포렌식을 수행하여 공격 타임라인에 대한 더 깊은 인사이트를 얻고, 네트워크에서 여전히 활동 중일 수 있는 공격자의 간섭을 받거나 공격자에게 들키지 않고 안전하고 격리된 환경에서 IOC를 추적할 수 있습니다.

자세히 알아보기

이는 백업 데이터가 보안 자산이 될 수 있는 방식 중 세 가지에 불과합니다. **백서를 다운로드하여 자세한 내용을 알아보십시오.**

COHESITY

cohesity.com

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

9100082-002-KO 4-2025