Dell PowerProtect Backup Services로 랜섬웨어 복구 가속화

며칠이 아니라 몇 시간 만에 랜섬웨어로부터 복구

주요 기능

더 잦고 교묘해진 랜섬웨어 공격으로 인해 해결 비용이 늘어나고 있음

- 감염되지 않은 백업 또는 파일을 신속하게 식별하고 복원할 수 없음
- 감염이 확산되어 복구 데이터로부터 재감염됨
- 데이터 손실, 전체 데이터 세트 복구 불가
- 인시던트 대응을 조율하기 어려움
- 더 빠른 RPO/RTO 시간이 요구됨
- 비용이 많이 드는 비즈니스 다운타임으로 인한 수익 손실과 브랜드 명성 훼손
- 부적절한 데이터 보호로 인한 법적 제재 및 행정 처벌

당면 과제

랜섬웨어는 모든 기업에 심각한 위협입니다. 사이버 공격은 자주 발생하며 치명적인 피해를 초래할 수 있습니다. 79%의 조직들이 향후 12개월 안에 운영 중단 사고를 겪을 것을 우려하고 있습니다1. 데이터를 잃는 기업은 재해 발생 후 파산을 신청해야 할 정도의 위험에 노출됩니다. 랜섬웨어 공격은 더 빈번하게 발생하고 있을 뿐만 아니라 기술적으로 더 발전했으며 해결하는 데 더 많은 비용이 듭니다.

솔루션

신속하고 안정적인 복구가 가능하면 랜섬을 지불해야 할 이유가 없습니다. 보안 인시던트나 사이버 공격이 발생할 때 조직은 이를 복구하기에 앞서 피해 범위와 근본 원인을 파악해야 합니다. 워크로드와 가상 머신에 대해 24/7 제공되는 깨끗한 에어 갭 스냅샷, 사용자 및 데이터 이상 징후에 대한 지속적인 모니터링, 보안 툴과의 통합 그리고 클린 데이터의 자동 복구 덕분에 보안 태세를 개선하고 치명적인 시련을 극복 가능한 인시던트 정도로 낮출 수 있습니다.

기능

모든 워크로드:

• 변경 불가능한 에어 갭 백업을 24x7 사용할 수 있음

• 며칠 또는 몇 주가 아닌 몇 시간의 RPO/RTO로 온프레미스 또는 클라우드 내에서 클린 데이터 복구

• MDDR(Managed Data Detection and Response) 서비스가 백업 환경에 대한 24x7x365 실시간 모니터링을 제공함

• 운영 조직의 데이터를 사용하고 다수의 복제본을 만들어 여러 위치에 저장하는 방법으로 모든 AWS 리전/어카운트에 걸쳐 워크로드와 VM을 복원한다면 조직을 커다란 위험에 노출시키는 것임

주요 워크로드를 위한 랜섬웨어 복구 가속화:

• ML 기반 알고리듬으로 이상 징후를 모니터링하고 사전 예방적으로 탐지

• SIEM 및 SOAR 통합을 통해 대응 및 복구 활동 조율

• 복구 전에 스냅샷에서 멀웨어를 검사하고 감염된 스냅샷과 파일을 백업에서 삭제

• 골든 스냅샷에서 지정된 기간 내에 모든 파일의 최신 클린 버전을 자동으로 복구

보호

랜섬웨어로 인한 피해를 방지하기 위한 첫 번째 단계는 변경 불가능한 에어 갭 데이터 복사본을 확보하는 것입니다. 회복탄력성이 뛰어난 클라우드 인프라스트럭처를 기반으로 하는 Dell PowerProtect Backup Services를 사용하면 랜섬웨어가 백업 데이터를 암호화할 수 없습니다. 다단계 인증, 엔벨로프 암호화, 별도의 계정 액세스를 포함하는 제로 트러스트 아키텍처는 랜섬웨어가 훼손된 기본 환경 자격 증명을 사용하여 백업 환경 또는 데이터를 변조하지 못하도록 합니다. 마지막으로, 과도한 삭제 방지 및 소프트 삭제(휴지통) 기능은 백업이 삭제되지 않도록 추가적인 보안 계층을 제공합니다.

감지

랜섬웨어 공격을 최대한 빨리 탐지하면 인시던트 대응 팀에 도움이 되고 감염 확산을 방지할 수 있습니다. Dell PowerProtect Backup Services 랜섬웨어 복구 가속화 모듈은 백업 환경의 보안 태세를 모니터링하는 보안 명령 센터를 제공합니다. 액세스 통찰력과 이상 징후 탐지를 통해 환경 및 데이터 전반에서 비정상적인 활동을 신속하게 식별할 수 있습니다. 사용자 및 API의 모든 액세스 시도에 대해 위치, ID 및 활동 정보를 확인합니다. 비정상적인 데이터 활동(예: 삭제, 암호화 등)에 대한 알림을 제공하는 독점 ML 알고리듬을 통해 이상 징후를 탐지합니다. 이 알고리듬은 특정 백업 환경에 대한 패턴을 학습하므로 규칙을 설정하거나 튜닝할 필요가 없습니다. 또한 엔트로피 기반 통찰력을 사용하여 거짓 양성을 줄입니다.

응답

보안 또는 IT 분석가가 의심스러운 이벤트를 탐지하는 경우 또는 더 나아가 랜섬웨어 인시던트가 발생했음을 확인하는 경우, 대응 속도가 매우 중요합니다. 탐지 및 대응 오케스트레이션에 사용할 수 있는 중요한 기본 환경 보안 툴이 많이 있지만, 보조 데이터(백업 시스템)의 분석 및 로그 변경 데이터는 조사, 대응 및 포렌식 활동에 큰 도움이 됩니다. Dell PowerProtect Backup Services 랜섬웨어 복구 가속화 모듈은 강력한 API 통합을 즉시 제공하므로 솔루션을 전체 보안 생태계에 쉽게 맞출 수 있습니다. SIEM 및 SOAR 솔루션을 사용하여 대응 활동을 조율하면 MTTR(Mean Time to Response)을 크게 줄일 수 있습니다. 감염된 시스템 또는 스냅샷을 격리하거나 사전 정의된 랜섬웨어 플레이북을 기반으로 백업에서 IOC를 검사하는 것과 같은 작업을 자동으로 완료할 수 있기 때문입니다.

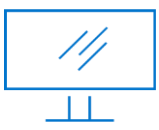
복구

초기 대응 단계를 지나면 이제 복구라는 쉽지 않은 작업이 기다리고 있습니다. 많은 기업에서 이 프로세스는 수작업으로 이루어지며 시간이 많이 소요됩니다. 악의적인 공격자와 랜섬웨어가 숨어 있던 기간이 몇 주 전부터 몇 달 전까지일 수도 있으므로 클린 데이터를 찾기 위해 얼마나 더 멀리 과거로 돌아가야 할지를 알기 어렵습니다. 최상의 스냅샷을 찾아낸 후에도 숨겨진 멀웨어가 재감염을

일으킬 수 있습니다. 어쨌든 2주 전이라는 복구 시점은 대부분의 비즈니스 사용자들에게는 받아들일 수 없는 것입니다. 하지만 랜섬웨어 사건 후 최신 데이터를 찾고 확인하는 것은 수동적이고 지루한 일이며 종종 불가능하기도 합니다.

Dell PowerProtect Backup Services는 효과적인 백업 아키텍처와 자동화된 툴을 통해 이러한 부담을 덜어줌으로써 복구 속도를 높입니다. Dell PowerProtect Backup Services 클라우드 플랫폼은 워크로드를 클라우드에 직접 백업하여 랜섬웨어 공격 발생 시 즉시 복구할 수 있도록 합니다.

랜섬웨어 복구 가속화 모듈을 사용하면 복구 데이터를 안전하게 보호함으로써 안심하고 복구할 수 있습니다. 내장된 안티바이러스 탐지 기능을 사용하거나 자체 포렌식 조사 또는 위협 인텔리전스 피드의 위협 인텔리전스를 사용하여 스냅샷에서 멀웨어와 IOC를 검사할 수 있습니다. 복구 전에 스냅샷을 검사하면 재감염이 제거됩니다.



자세한 정보
PowerProtect Backup Services 정보

문의 Dell Technologies 전문가