COHESITY

# 사이버 볼트 평가를 위한 임원 가이드

# 요약: 사이버 레질리언스에 사이버 볼팅이 필수적인 이유

어떤 기업도 사이버 공격으로부터 안전할 수는 없으므로, 모든 조직에는 효과적인 대응과 복구가 필수적입니다. 공격자는 데이터를 보호하기 위한 바로 그 시스템까지도 표적으로 삼고, 몸값을 지불하도록 강요하기 위해 온갖 수단을 동원합니다. 하드웨어 장애 및 자연 재해로부터 보호하도록 설계된 기존의 백업 전략은 표적화된 다단계 사이버 공격으로부터 조직을 보호하는 데 거의 도움이 되지 않습니다. 랜섬웨어 공격이 발생하면 프로덕션 네트워크에 연결된 데이터의 백업 복사본이 암호화되거나 삭제될 수 있으며, 이로 인해 깨끗하고 신속한 복구가 거의 불가능해질 수 있습니다. IT 리더에게 중요한 것은 공격이 발생할 것인가가 아니라 언제 발생하느냐입니다. 귀사는 그 공격이 실제로 발생했을 때 자신 있게 복구할 준비가 되어 있습니까?

귀사와 같은 조직들이 데이터 보호 및 복구 방법을 재검토하게 됨에 따라, 사이버 볼팅은 최신 사이버 레질리언스 전략의 핵심 요소로 자리잡고 있습니다. 사이버 볼트는 다른 모든 수단이 실패하더라도 복구에 사용할 변경되지 않은 데이터 사본을 유지할 수 있게 보장해 줍니다. 볼팅은 파괴적인 사이버 공격에도 불구하고 깨끗하고 복구 가능한 데이터를 보장하는 데 필요한 분리, 검증 및 제어 기능을 제공합니다. 이것이 바로 동종 업계가 사이버 볼팅을 레질리언스의 필수 요소로 채택하는 이유입니다.

# 당면 과제: 재해 복구 보다 훨씬 더 복잡한 사이버 복구

조직들은 수년 동안 하드웨어 장애, 우발적 삭제 및 자연 재해에 대응하기 위해 백업 시스템을 설계해 왔습니다. 이러한 시스템은 종종 그 목적을 잘 수행해 왔습니다. 그러나 이것만으로는 오늘날 지배적인 파괴적 사이버 공격으로부터 데이터를 안전하게 보호하기에 충분하지 않습니다.

그 결과, 중요한 위험 요소가 등장했습니다. 즉, 백업 데이터도 프로덕션 데이터만큼 취약할 수 있다는 것입니다. 위협 행위자는 더 이상 프로덕션 데이터 암호화에만 집중하지 않습니다. 이들은 백업 리포지토리에 침투하고, 스냅샷 일정을 비활성화하고, 악성코드를 심고, 메타데이터를 손상시켜 복구 경로를 제거해 버립니다.

이러한 위험은 최신 데이터 보호 플랫폼을 갖추고 있더라도 존재합니다.

## 데이터 자산이 위험한 이유

여러분은 "전체 백업 데이터를 위해 모든 보안 추가 기능이 활성화된 안전한 데이터 플랫폼을 갖고 있는데 그 정도면 충분하지 않나?"라고 생각할지도 모릅니다. 짧게 답하자면, 그렇지 않습니다.

그러한 플랫폼은 위험과 공격 표면을 크게 줄여 주지만, 그 자체만으로는 노출을 배제하지는 못합니다.

그 이유는 다음과 같습니다.

- **공유된 연결 구조**: 대부분의 백업 시스템은 프로덕션 네트워크에 연결되어 있습니다. 해당 프로덕션 환경이 침해당하면 공격자는 이미 백업 데이터에 접근할 수 있는 경로를 확보하게 됩니다.
- **자격증명 중복**: 관리자용 자격증명은 여러 환경 간에 공유되는 경우가 많습니다. 일단 공격자가 접근권을 확보하면 프로덕션 데이터만큼이나 쉽게 백업 데이터를 삭제하거나 암호화할 수 있습니다.
- **거짓 불변성**: 일부 '불변성' 백업 데이터는 소프트웨어로만 잠겨 있습니다. 만일 스토리지 컨트롤 플레인 또는 API가 침해당하면 불변성 플래그가 해제될 수 있습니다.
- **잠재 위협의 잔존 가능성**: 많은 조직이 데이터 무결성을 검증하거나 잠복 멀웨어를 검사하지 않고 백업을 이용하여 복원하므로 복구 중 재감염 위험이 높아집니다.

## 비즈니스에 미치는 영향

결과는 신뢰 격차로 나타납니다. 즉, 백업 데이터의 무결성을 실제보다 훨씬 더 높게 인식하게 됩니다. 그로 인한 부정적 결과는 연쇄적으로 발생합니다.

- **다운타임 장기화**: 확인되지 않거나 손상된 백업 데이터는 복구 기간기 몇 시간에서 며칠 또는 몇 주로 연장됩니다.
- **운영상의 부담**: 팀은 복구 계획을 실행하는 대신 시스템 또는 데이터 세트를 다시 만드는 데 시간을 소비해야 합니다.
- **누적 비용**: 가동 중단 시간이 한 시간 늘어날 때마다 수익 손실, 규제 노출 및 브랜드 손상이 증가합니다.
- **신뢰 잠식**: IT 부서가 빠르고 깨끗한 복구 데이터를 제공할 수 없다면, 조직의 레질리언스에 대한 경영진과 이사회의 신뢰가 저하됩니다.

# 사이버 볼팅: 다른 모든 것이 실패했을 때의 최종 방어선

사이버 볼트는 이러한 신뢰 격차를 해결합니다. 사이버 볼트는 중요한 데이터의 깨끗한 사본을 격리 상태로 저장하므로 안전하고 변경 불가능한 저장소입니다. 이 볼트는 프로덕션 네트워크 및 기본 백업 시스템에서 의도적으로 분리되어 있습니다.

사이버 볼트를 채택하면 3-2-1 백업 규칙이 새롭게 구성됩니다. 즉, 세 개의 데이터 복사본을 서로 다른 두 종류의 매체에 보관하되, 그중 하나는 격리되고 불변성을 갖춘 오프사이트 복사본으로 유지하는 것입니다.

실제로 조직들은 이 최신 백업 규칙을 다음과 같이 구현합니다.

- **변경 불가능한 3개의 데이터 사본:** 각 사본은 WORM(Write-once, Read-Many) 또는 객체-수준 잠금 기능을 이용하여 보호하고, AI 기반 이상 탐지 및 정기적인 위협 스캔을 이용하여 지속적으로 검증함으로써 데이터가 깨끗한지 확인해야 합니다.
- **2개의 다른 미디어란 두 개의 서로 다른 플랫폼 또는 신뢰 경계에 데이터를 저장하는 것을 의미합니다.** 이 때의 사본은 동일한 컨트롤 플레인 또는 공격 표면을 공유하지 않는 별개의 시스템에 있어야 합니다. 여기에는 데이터 격리를 위해 설계된 디스크, 테이프 또는 클라우드 스토리지의 조합이 포함될 수 있습니다.
- **오프사이트 사본 1부의 격리:** 최종 사본은 논리적 또는 물리적 에어 갭으로 분리되어야 하며 격리형 보안 모델 및 제3자 수탁 관리를 통해 보호해야 합니다. 또한, 이 사본은 다단계 인증(MFA), 쿼럼 및 데이터 무결성 검사로도 보호해야 합니다.

이러한 발전사항들이 결합하여 3-2-1 규칙은 사이버 레질리언스의 핵심 요소가 되었습니다. 사이버 볼트는 중요한 데이터의 깨끗한 최종 복구 지점 역할을 합니다. 사이버 볼트는 불변성, 격리, 다양한 스토리지 도메인 및 엄격한 무결성 검증을 결합하여 조직으로 하여금 백업 자산이 침해된 최악의 시나리오에서도 파괴적인 사이버 공격으로부터 안전하게 복구할 수 있도록 해 줍니다.

# 사이버 볼팅 솔루션 평가

사이버 볼팅 솔루션을 선택할 때 IT 리더는 보안 아키텍처와 운영 준비태세를 모두 평가해야 합니다. 수백 명의 IT 리더들의 피드백에 의하면, 중요한 핵심 역량은 다음 다섯 가지입니다.

1. **격리 및 액세스 제어:** 볼트 데이터는 프로덕션 네트워크에서 접근할 수 없어야 합니다. 강제된 에어 갭, 독립적인 ID 도메인, MFA 및 쿼럼 기반 관리 승인 기능이 있는지 확인하십시오.
2. **불변성 및 무결성:** 데이터는 변조가 불가능해야 하며, WORM 스토리지 및 보존 잠금 정책을 이용하여 관리자라도 수정 또는 삭제할 수 없도록 해야 합니다.
3. **자동화 및 오케스트레이션:** 볼트 복제, 검증 및 복구는 자동화되어 있어야 합니다. 정책 기반 오케스트레이션은 인적 오류를 줄이고 복구를 가속화할 수 있습니다.
4. **위협 차단:** AI 기반 이상 탐지 및 멀웨어 스캔 기능은 스냅샷의 잠재적 위협을 표시하여 깨끗하고 손상되지 않은 데이터만 저장 및 복원할 수 있게 해 줍니다.
5. **규정준수 및 보고:** 복구 가능성 및 레질리언스 준비태세를 입증하려면 변경 불가능한 감사 로그, 암호화 및 보존 관리 기능이 NIST SP 800-209, ISO 27040 및 DORA 와 같은 프레임워크에 부합해야 합니다.

## 평가 점수표 - 공급업체와의 협의 시 이 점수표를 사용하십시오.

**지침**

1. 각 범주별로 각 공급업체에 대해 1~5점의 점수를 부여합니다. 여기서 1점은 요건을 충족하지 못한 것이며, 5점은 요건을 완전히 충족하는 경우입니다.
2. 각 공급업체의 점수에 해당 범주의 **가중치**를 곱한 다음, 해당 가중 점수 셀에 결과를 기록합니다.
3. 각 공급업체에 대해 해당 열의 모든 **가중 점수**를 합산하고 그 합계를 표 하단의 **가중 합계** 행에 기록합니다.
4. **가중 합계**를 사용하여 공급업체를 전체적으로 비교하고, (수치화가 어려운) 정성적 관찰사항이나 위험은 별도로 기록합니다.

| | | 벤더 1 | | 벤더 2 | | 벤더 3 | | 벤더 4 | |
|---|---|---|---|---|---|---|---|---|---|
| **범주** | **가중치** | **점수** | **가중 점수** | **점수** | **가중 점수** | **점수** | **가중 점수** | **점수** | **가중 점수** |
| **격리도 / 에어 갭** | 10 | | | | | | | | |
| **불변성/WORM** | 10 | | | | | | | | |
| **접근 제어의 분리** | 10 | | | | | | | | |
| **강력한 인증(MFA / 쿼럼)** | 8 | | | | | | | | |
| **위협 탐지 / 이상 징후** | 8 | | | | | | | | |
| **감염된 스냅샷 복구 차단** | 8 | | | | | | | | |
| **복구 오케스트레이션** | 8 | | | | | | | | |
| **클린룸 / 검증** | 8 | | | | | | | | |
| **규정준수 / 감사 가능성** | 8 | | | | | | | | |
| **SaaS 단순성 / TTV** | 7 | | | | | | | | |
| **하이브리드 / 멀티클라우드 유연성** | 8 | | | | | | | | |
| **TCO / 운영 오버헤드** | 7 | | | | | | | | |
| **가중 합계** | | | | | | | | | |

## 최신 사이버 볼팅은 다음과 같은 측정 가능한 비즈니스 측면의 성과를 제공합니다.

- **레질리언스**: 백업 플랫폼이 손상되어도 복구 사본은 물리적 또는 논리적으로 격리된 채 그대로 유지됩니다.
- **연속성**: 백업 데이터를 볼트에 보관하면 해당 조직은 공격의 범위에 관계없이 복구용 데이터 사본을 확보할 수 있게 됩니다.
- **규정준수**: 변경 불가능한 스토리지 및 보존 정책의 강제 적용을 통해 데이터 보호 및 복구 준비태세에 대한 감사 가능한 증거를 확보할 수 있습니다.
- **신뢰 확보**: 복구 지점은 운영 환경의 피해 확산 범위 외부에 보존되며, 사용 전 검증이 가능하므로 복원된 데이터가 깨끗하고 손상되지 않는 것이 보장됩니다.

사이버 볼팅은 IT 운영, 보안 및 규정준수 기능을 하나로 연결하여 위기가 발생하더라도 불확실한 도박이 아닌 깨끗한 복구가 보장됩니다.

# 백업 의존에서 레질리언스 기반 복구로 전환: Bethany 아동 건강 센터

많은 조직이 사이버 볼팅을 데이터 보호 전략의 표준 구성 요소로 통합하고 있습니다. 한 가지 예로, 복합적 의료 서비스가 필요한 아이들을 돌보는 오클라호마 주의 Bethany 아동 건강 센터가 있습니다. 이 센터는 중단 없는 치료를 지원하기 위해 사이버 공격이나 재해 발생 시 민감한 건강 데이터를 보호하고 신속하게 복원할 수 있어야 합니다. Bethany는 불변 백업을 온프레미스 및 격리된 클라우드 볼트인 Cohesity FortKnox 두 곳에 저장함으로써 이러한 요구사항을 충족하고 있습니다.

Bethany는 레질리언스를 높이기 위해 3개의 데이터 사본을 2개의 서로 다른 매체에 저장하고 1개의 사본을 외부에 보관하는 3-2-1 원칙을 따르고 있습니다. 두 개의 변경 불가능한 백업은 자체 서버에 보관하고 세 번째 백업은 Cohesity FortKnox에 저장해 두는 것입니다.

Cohesity FortKnox는 최고 수준의 보안이 요구되는 환경을 위해 AWS, Azure 및 GCP 전반에 걸쳐 DataProtect 및 NetBackup 환경에서 사용할 수 있는 관리형 사이버 볼팅 서비스와 온프레미스 솔루션을 제공합니다. FortKnox는 격리, 불변성 및 자동화를 결합하여 엔터프라이즈 규모에서 빠르고 깨끗하며 검증된 복구 능력을 제공합니다.

FortKnox는 새로운 방어 계층, 즉 중요한 데이터가 안전하고 규정에 부합하며 복구 가능성이 보장된 안전한 에어 갭 볼트를 추가해 줍니다.

# 사이버 레질리언스를 평가하기 위한 다음 단계

레질리언스 계획은 더 이상 적용되지 않는 가정에 의존할 수 없습니다. 사이버 공격이 점점 더 공격적으로 변함에 따라, 비즈니스 연속성은 최후의 보루이자 가장 안전한 데이터 사본의 견고성에 점점 더 좌우됩니다. 사이버 볼트는 사이버 복구 능력을 강화하고 가동 중단 시간을 줄이는 사전 예방적 접근 방식을 의미합니다.

먼저 다음 사항을 평가하는 것부터 시작하십시오.

- **SaaS, 온프레미스, 클라우드에 흩어져 있는 모든 데이터를 단 하나의 최신 플랫폼에서 백업하고 있습니까?**
- **MFA, 불변성, 역할 기반 접근 제어(RBAC)를 통해 플랫폼을 강화했습니까?**
- **3-2-1 백업 규칙을 준수하고 있습니까?**
- **프로덕션 네트워크로부터 백업 데이터를 분리하기 위해 어떤 격리 수단을 이용하고 계십니까?**
- **위협에 대비하여 백업 데이터를 얼마나 자주 스캔하고 있습니까?**
- **사이버 대응 계획을 얼마나 자주 테스트하십니까?**
- **최근 실시한 사이버 대응 테스트에서 얼마나 빨리 복구했습니까?**

이제 사이버 레질리언스를 기술적 목표에서 전략적 필수 요소로 끌어올릴 때입니다. 궁극적인 경쟁 우위는 가정이 아니라 준비태세에 있습니다.

**현대의 사이버 볼팅이 어떠한 위협에도 관계없이 데이터를 보호하고 복구 태세를 강화하며 안심하고 안전하게 운영할 수 있게 지원하는지 확인해 보십시오.**
**더 자세한 내용은 https://www.cohesity.com/ko-kr/platform/fortknox/**



COHESITY

cohesity.com/ko-kr
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500065-001-KO 2-2026