VERITAS

가상 에어 갭(Air Gap) 및 격리 기술로 데이터 복구 향상

데이터의 안전한 카피본을 유지 관리하면서 사이버 공격의 영향을 차단합니다.

백서 | 2024년 4월

데이터 볼트를 생성해야 하는 이유

사이버 보안은 여전히 비즈니스 리더의 최우선 관심사입니다. 사이버 위협이 갈수록 지능화하면서 계속 피해를 극대화하는 기술로 업그레이드되고 있습니다. Gartner에 따르면, 2025년에는 이사회 중 40%가 사이버 보안 전담 위원회를 비롯해 사이버 보안 정책, 실행, 복구에 관한 별도의 리포팅 및 전략 수립을 담당하게 될 것입니다.[1] 사이버 범죄가 엄청난 속도로 증가하는 가운데 기업이 관련 리스크를 줄이고 피해 상황에서 복구하는 데 막대한 비용과 시간을 지출하고 있습니다. 2023년에 데이터 유출로 인한 전 세계 평균 비용은 미화 445만 달러로 3년 동안 15% 증가한 만큼[2], 리스크와 불확실성을 해소하며 환경에 대한 통제권을 유지하기 위한 전략을 서둘러 마련해야 합니다.

레질리언스 및 복구 계획에 대해 확신하려면, 먼저 신뢰할 만한 사이버 보안 프레임워크를 올바른 기술 및 프로세스와 함께 구현해야 합니다. 확신을 가지고 관리자 및 고위 경영진과 소통할 수 있는 사이버 보안 사고 대응 계획이 있으십니까? Gartner에 따르면[3], 2025년에는 CEO의 70%가 기업 차원에서 사이버 범죄에 대한 레질리언스 문화를 필수적으로 조성할 것입니다. 이제는 사이버 보안의 트렌드와 성공적인 복구 계획의 핵심 구성 요소를 제대로 이해해야 합니다. 경영진에게 랜섬웨어 공격을 확실히 차단하고, 올바른 복구 솔루션을 구현했음을 자신 있게 입증할 수 있어야 합니다.

에어 갭(Air Gap)이란 무엇이며 왜 중요합니까?

사이버 공격이 갈수록 지능화함에 따라 해커는 기본 데이터 스토리지뿐만 아니라 백업 데이터 스토리지까지 표적으로 삼기 시작했습니다. 기업의 재해 복구 전략에서도 이에 대비하는 것이 중요합니다. 대개 해커는 시스템에 침투한 다음 기본 및 백업 데이터에 액세스하여 공격할 수 있을 때까지 잠복합니다. 일단 해커가 데이터에 액세스하면 데이터를 손상시킬 수 있습니다.

NIST(National Institute of Standards and Technology)의 정의에 따르면, 에어 갭(Air Gap)은 두 시스템 간의 인터페이스입니다. 여기서 (a) 두 시스템은 물리적으로 연결되지 않고 (b) 어떤 논리적 연결도 자동화되지 않습니다. 즉, 이 인터페이스를 통한 데이터 전송은 사람의 통제 아래 수동으로만 가능합니다.[4] 과거에는 에어 갭(Air Gap)이 온도 조절기, 가전 제품 등의 운영 기술을 보호하는 최고의 기준이었지만, 이제는 거의 모든 것이 무선 또는 유선 네트워크를 통해 연결되므로, 복구에 사용할 안전한 데이터 카피본을 확보하려면 강력한 에어 갭(Air Gap) 프로세스가 반드시 필요합니다.

네트워크 환경에서 해커는 거의 모든 진입 지점을 악용할 수 있습니다. 모든 유무선 신호가 비활성화된 시스템에서도 가능합니다. 일부 IT 부서는 최고 보안 등급의 데이터를 다루는 가장 폐쇄적인 시스템에서 모든 USB 포트를 비활성화하고 페러데이 상자를 사용하여 모든 무선 전송을 차단하고 전자기 누출을 방지합니다.

Auto Image Replication(AIR) 기술로 퍼블릭 클라우드를 비롯해 동일한 사이트나 서로 다른 사이트에 있는 백업 도메인 간에 백업 데이터를 복제할 수 있습니다. AIR로 백업의 오프라인 에어 갭(Air Gap) 카피본을 사용하면서 의도치 않은 소스에 의한 데이터 액세스 위협을 확실히 줄일 수 있습니다. 기업 소유의 데이터 센터와 퍼블릭 클라우드에서 데이터가 확산됨에 따라, 에어 갭(Air Gap) 구조를 구현하여 중요 데이터의 정상으로 확인된 최신(last-known-good) 카피본을 유지하는 백업 및 복구 솔루션을 갖추는 것이 중요합니다.

클라우드 데이터와 가상 에어 갭(Air Gap)

클라우드 우선 환경 확대: 기업의 85%가 2025년까지 클라우드 우선 환경으로 전환할 것으로 전망하며, 94%는 멀티 클라우드 전략을 구현하고 있습니다.[5] 클라우드 가속화 전략이 빠르게 증가하면서, 그로 인해 여러 상이한 툴과 의사 결정 기구가 생겨날 수 있습니다. 기본 데이터 리포지토리를 여러 퍼블릭 클라우드 옵션과 함께 다양화 및 최적화하는 동시에 데이터 복구 접근 방식을 최적화해야 하며, 이를 위해서는 해당 환경을 성공적으로 정상화하고 뒷받침할 최상의 솔루션이 필요합니다.

여기서 IRE(Isolated Recovery Environment) 기능이 진가를 발휘할 수 있습니다. IRE의 가상 에어 갭(Air Gap) 솔루션은 중요 데이터의 안전한 카피본을 생성합니다. 따라서 관리자는 안전한 파일 세트를 온디맨드 방식으로 확보하면서 멀티 클라우드 환경 내에서 랜섬웨어 공격의 영향을 무력화할 수 있습니다.

IRE(Isolated Recovery Environment)

기존 네트워크 격리 솔루션은 보안 지역 간의 연결을 물리적으로 또는 가상으로 차단하여 모든 송수신을 불가능하게 합니다. 이러한 방식으로는 격리된 환경으로의 데이터 전송이 제한됩니다. 또한 제3의 카피본이 필요한 경우 복구 시간 목표(RTO) 및 복구 시점 목표(RPO) 달성에 어려움이 있습니다. 이른바 소스에서 타깃으로 복제 데이터를 푸시(Push)하는 것으로, 소스 도메인에서 독립적으로 복제 작업을 처리한 다음 타깃 도메인에 전송하는 것입니다. 이러한 기존 방식에서는 연결이 중단되거나 차단될 경우 보안 환경으로 중요 데이터를 복제할 수 있는 시간이 제한적입니다.

그와 달리 풀(Pull) 복제 모델은 타깃에서 복제 요청을 시작합니다. Veritas NetBackup의 IRE 솔루션은 풀 복제 모델을 제공하여 데이터 이동을 최적화합니다. IRE의 MSDP(Media Server Deduplication Pool)로부터 데이터 전송 요청이 수행되며, 역방향 연결을 통해 더 효과적으로 데이터 흐름을 제어하여 가상으로나 물리적으로 확실하게 환경을 보호합니다. 이제 IRE에 대한 복제는 IRE 내에서 모두 제어 가능합니다. IRE의 가상 에어 갭(Air Gap) 일정을 통해 구체적으로 기간을 정의하는 것도 지원됩니다.

NetBackup IRE는 데이터 전송 중에도 침투할 수 없는데, 침입 차단 메커니즘, 데이터 전송 및 저장 시 암호화 등을 포함한 멀티레이어 보안을 구현했기 때문입니다. 데이터 여정의 전반에서 데이터는 어디서든 안전하고, 스토리지도 손상되지 않습니다. 따라서 악의적인 사용자나 권한 없는 사용자가 데이터를 읽거나 수정할 위험이 없습니다. 베리타스는 온프레미스와 클라우드 모두를 위한 데이터 격리 옵션을 제공합니다. NetBackup Recovery Vault는 완벽한 서비스형 클라우드 스토리지(Cloud storage-as-a-service)로, 랜섬웨어 차단을 위해 가상 에어 갭(Air Gap) 기술을 적용하고, 최적의 방식으로 확장 가능하며, 예측 가능한 비용으로 데이터 이동성을 보장합니다.

베리타스는 간단한 워크플로우를 통해 온프레미스 또는 클라우드의 모든 NetBackup을 IRE 프레임워크로 전환함으로써 다음과 같은 세 가지 핵심 원칙에 따른 랜섬웨어 레질리언스를 제공합니다.

- **보호**: 베리타스 제로 트러스트 보안 전략에 부합하는 다단계 인증(MFA) 및 역할 기반 액세스 제어(RBAC)를 지원하면서 격리된 복구 기능을 손쉽게 통합합니다.
- **탐지**: NetBackup IT Analytics는 랜섬웨어를 실시간으로 발견할 수 있는 이상 탐지 기능을 제공합니다. 통합된 NetBackup 악성 코드 검사 기능으로 복구에 앞서 악성 코드 검사를 수행하여 이상 점수에 따라 우선 순위를 지정할 수 있습니다.
- **복구**: 다양한 RPO 및 RTO 요구 사항을 관리하는 오케스트레이션을 통해 클라우드 또는 온프레미스의 데이터 세트 전체를 격리된 환경에 복구합니다.

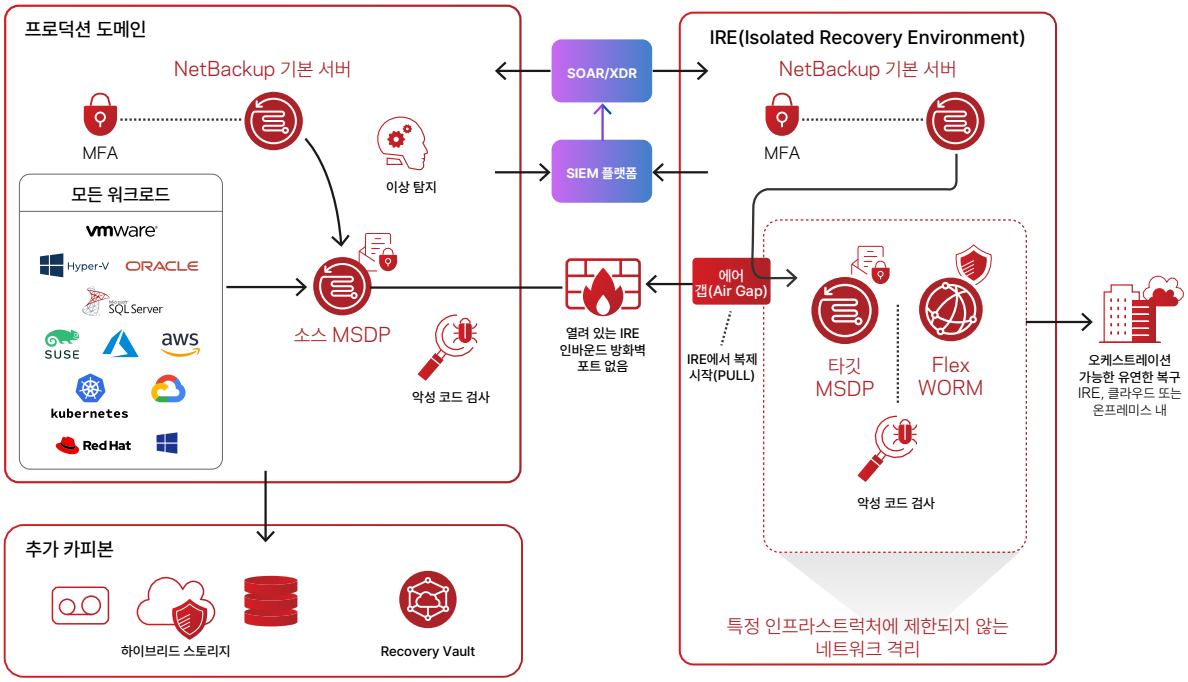

그림 1: NetBackup 가상 에어 갭(Air Gap) - IRE(Isolated Recovery Environment)

격리 환경을 통해 한층 더 강화된 레질리언스로 랜섬웨어 및 악성 코드에 대응할 수 있습니다.

제로 트러스트를 통해 보호 강화

제로 트러스트 정책은 훨씬 더 강력한 보호 기능을 제공합니다. 전사적 차원에서 제로 트러스트 마인드가 자리잡으면 심각한 공격의 리스크를 줄이는 데 효과적이라는 것이 여러 사례를 통해 입증되었습니다.

Veritas IRE는 Flex Appliance의 컨테이너 기반 멀티 테넌트 WORM(Write Once Ready Many) 스토리지, 하드닝 OS, 제로 트러스트 아키텍처를 사용합니다. 사용자, 툴, 시스템을 대상으로 다단계 인증(MFA) 및 역할 기반 액세스 제어(RBAC) 기술을 적용하여 ID 및 액세스 관리(IAM) 체계를 한층 강화함으로써 매우 중요한 데이터 및 백업에 대한 액세스를 제한합니다. 특정 데이터에 액세스할 필요가 있는 사용자에게만 권한을 부여해야 하며, 암호 보안에도 각별한 주의를 기울여야 합니다.

제로 트러스트 기반의 강력한 IAM 제어, 권한 제어, 하드닝, 보안 하드웨어를 통해 이러한 영역에 대한 액세스를 차단할 수 있습니다. 그러면 보안 침해가 발생해도 공격 노출 및 영향 범위가 줄어듭니다. 여러 단계의 보안을 통해 영향을 최소화하기 때문입니다. 예를 들어, 사이버 범죄자가 기업의 시스템에 침투하는 데 성공하면 대개는 기업 환경 전반의 비즈니스 크리티컬 데이터, 기밀 정보, 백업 시스템을 찾습니다.

이상 탐지 및 악성 코드 검사

완전한 가시성, 지능형 이상 탐지, 악성 코드 검사 기능을 활용하여 모든 데이터가 어디에 있는지 확실하게 파악하면서 운영 복잡성을 줄이고 비용 관리를 최적화할 수 있습니다. 베리타스의 AI 기반 이상 탐지 기능은 환경 전체를 대상으로 이례적인 데이터 및 사용자 활동을 찾아내고, 의심스러운 활동이 발견되면 거의 실시간으로 알려줍니다. 이 기능을 통해 데이터를 항상 복구 가능한 상태로 유지할 뿐만 아니라, 랜섬웨어 발생 시 즉각적인 조치를 수행하여 악성 코드에 감염된 백업을 격리하고 악성 코드가 백업 데이터에 미치는 영향을 최소화할 수 있습니다. 또한 검사를 거쳐 안전한 것으로 확인된 전체 이미지를 복원하거나 개별 파일을 복원할 수 있습니다. 복원 대상 파일이 감염되었더라도 감염되지 않은 백업에서 복원하는 것이 가능합니다. 따라서 공격 표적이 된 시스템이 재감염 위험 없이 안전하고 효과적으로 데이터를 복구합니다.

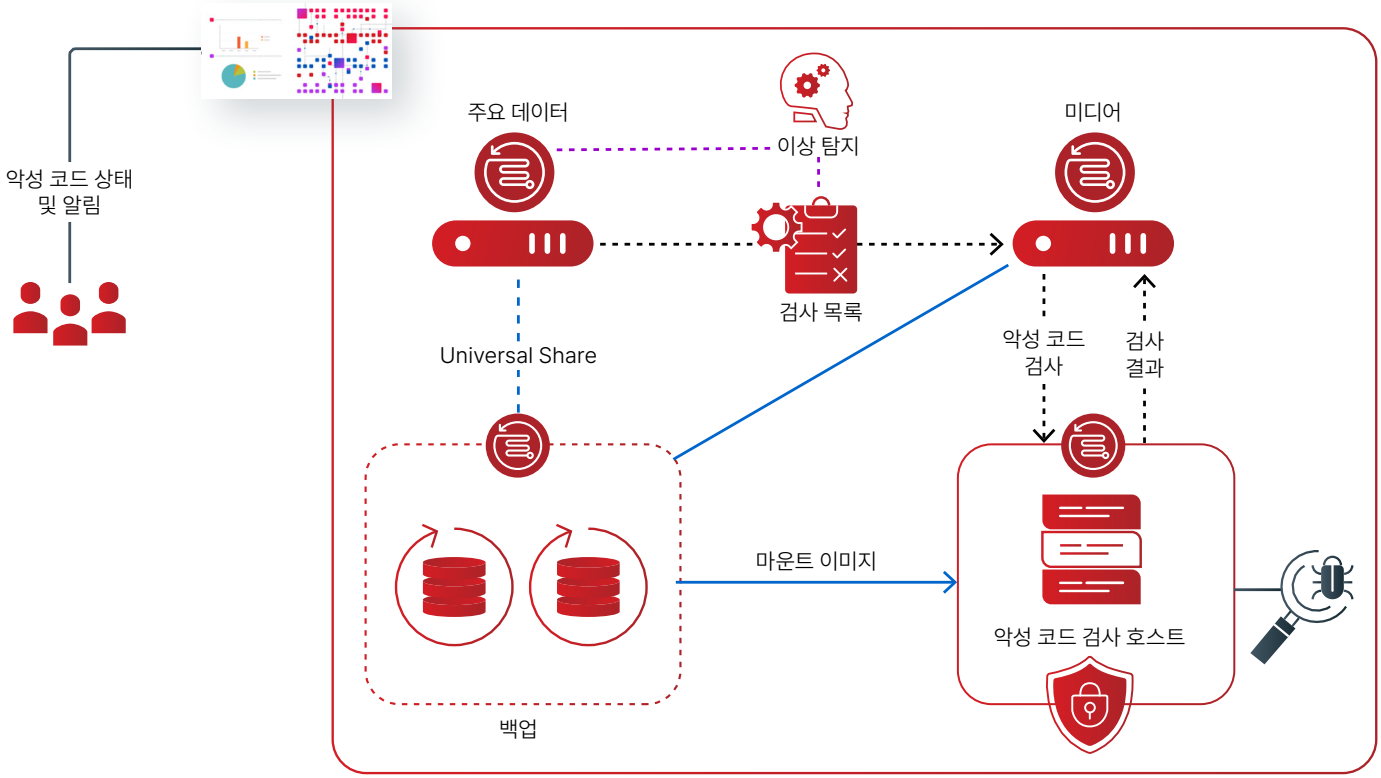

그림 2: NetBackup에 악성 코드 검사 통합

변조 불가 및 삭제 불가 스토리지를 사용한 복구

변조 불가 및 삭제 불가 스토리지를 사용하면 일정 기간 동안 (혹은 영구적으로) 그 어떤 것으로도 데이터를 변경, 암호화하거나 삭제할 수 없습니다. 또한 데이터를 조작하거나 무단 접근할 수 없도록 차단합니다. NetBackup Recovery Vault는 고객의 IRE 전략에 맞춰 필요에 따라 확장 또는 축소할 수 있는 변조 불가/삭제 불가 클라우드 기반 스토리지 솔루션을 제공합니다.

IRE를 통해 확신을 가지고 복구 수행

NetBackup IRE(Isolated Recovery Environment)로 리스크를 줄이고 불확실성을 해소하면서 계속 확실하게 통제할 수 있습니다. 베리타스 솔루션으로 멀티 클라우드 환경에서 제로 다우트(Zero Doubt) 사이버 레질리언스를 확보하는 방법에 대한 자세한 내용은 veritas.com/ko/kr을 방문하거나 베리타스 팀에 문의하십시오.

빈틈없는 엔터프라이즈 레질리언스 전략 구현. 자세히 보기 >

1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. https://www.ibm.com/reports/data-breach
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10

Veritas Technologies 소개

Veritas Technologies는 데이터 보호 및 가용성 분야의 글로벌 선도 기업으로, 포춘 100대 기업 중 91%를 포함한 전 세계 8만여 개 기업에서 베리타스 기술을 기반으로 IT 복잡성을 해결하고 데이터 관리를 간소화합니다. 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 데이터의 위치와 관계없이 데이터 보호를 자동화하고 복구를 조정함은 물론, 비즈니스 크리티컬 애플리케이션의 가용성을 항시 보장하고 기업이 데이터 규제 변화를 준수하는 데 필요한 인사이트를 제공합니다. 더불어 높은 신뢰성과 모든 요구사항을 충족하는 배포 모델을 제공하는 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 800개 이상의 데이터 소스와 100개 이상의 운영체제(OS), 1400개 이상의 스토리지 타깃을 지원합니다. 보다 자세한 정보는 베리타스 홈페이지(www.veritas.com/ko/kr) 또는 베리타스 트위터(@veritastechllc)에서 확인하실 수 있습니다.

VERITAS

Veritas Korea Ltd.
서울시 송파구 올림픽로 300
롯데월드타워 35층
Tel: 02-3468-2100
www.veritas.com/ko/kr

V1626 04/24