VERITAS

엔터프라이즈 하이브리드 클라우드 보안에 매우 중요한 변조 불가 백업

백서 | 2022년 12월

VERITAS ALTA

서론

연료를 수송하는 석유 가스 회사나 혈액형, 알레르기, 처방전과 같은 환자 데이터를 서버에 저장하는 병원에서 일한다고 상상해보십시오.

회사에서 랜섬웨어 공격을 받았습니다. 사이버 범죄자가 데이터를 공개하겠다고 협박하면서 수백만 달러를 요구합니다. 연료 수송 데이터를 추적할 수 없게 되었습니다. 지금 얼마나 이동하고 있을까요? 그리고 어디에 있을까요? 정상적으로 공급했습니까? 더 심각한 경우도 있습니다. 20건의 수술이 진행 중인 상황에서 갑자기 의료진이 환자 기록에 액세스할 수 없게 됩니다. 수술을 멈춰야 할까요, 아니면 계속 진행할까요? 랜섬웨어 공격자가 요구한 대로 돈을 지불하면, 제 시간에 데이터를 복원하여 생명을 살릴 수 있을까요?

스토리지와 백업만으로는 충분하지 않습니다. 기존 백업 및 복구 시스템으로는 기업이 공격을 받더라도 신속하게 운영을 재개하기 어렵습니다. 사이버 범죄자는 기업의 프로덕션 시스템과 인프라스트럭처는 물론 백업까지 표적으로 삼을 수 있음을 알게 되었습니다. 리포지토리와 스냅샷을 삭제하거나 암호화하여 사용 불가 상태로 만들 수도 있습니다. 백업 데이터가 취약해지는 것을 방지하려면 어떻게 해야 할까요?

관리자와 실무진이 기업 데이터를 보호하기 위해 노력해도 랜섬웨어, 악의적인 내부자, 사고에 의해 데이터가 삭제되곤 합니다. 거시적이고 통합적인 다계층 전략 수립이 필요하며, 비즈니스를 보호하는 최상의 방법입니다.

많은 기업이 백업 및 복구를 최후의 방어선으로 간주하지만, 베리타스는 백업 및 복구를 사이버 보안 전략의 최우선 요소로 다뤄야 한다고 생각합니다. 보안 공격과 손상은 언제든 일어나기 마련입니다. 이를 탐지하고 차단하는 게 중요하지만, 결국 가장 핵심적이고 확실한 방법은 운영 환경의 카피본을 안전한 장소에 보관하면서 확인하는 것입니다. 더 수월하고 효율적인 백업 및 복구 프로세스로 만드는 것이 당사의 목표입니다.

랜섬웨어에 감염되고 데이터 백업이 손상되면 순식간에 비즈니스가 마비될 수 있습니다. 운영이 중단되면 이를 해결하기까지 엄청난 시간과 비용이 듭니다. 사내에서 네트워크 공유를 사용하는 경우, 시스템에 보안 위반이 발생하면 악성 코드와 손상이 빠르게 확산될 위험이 있습니다.

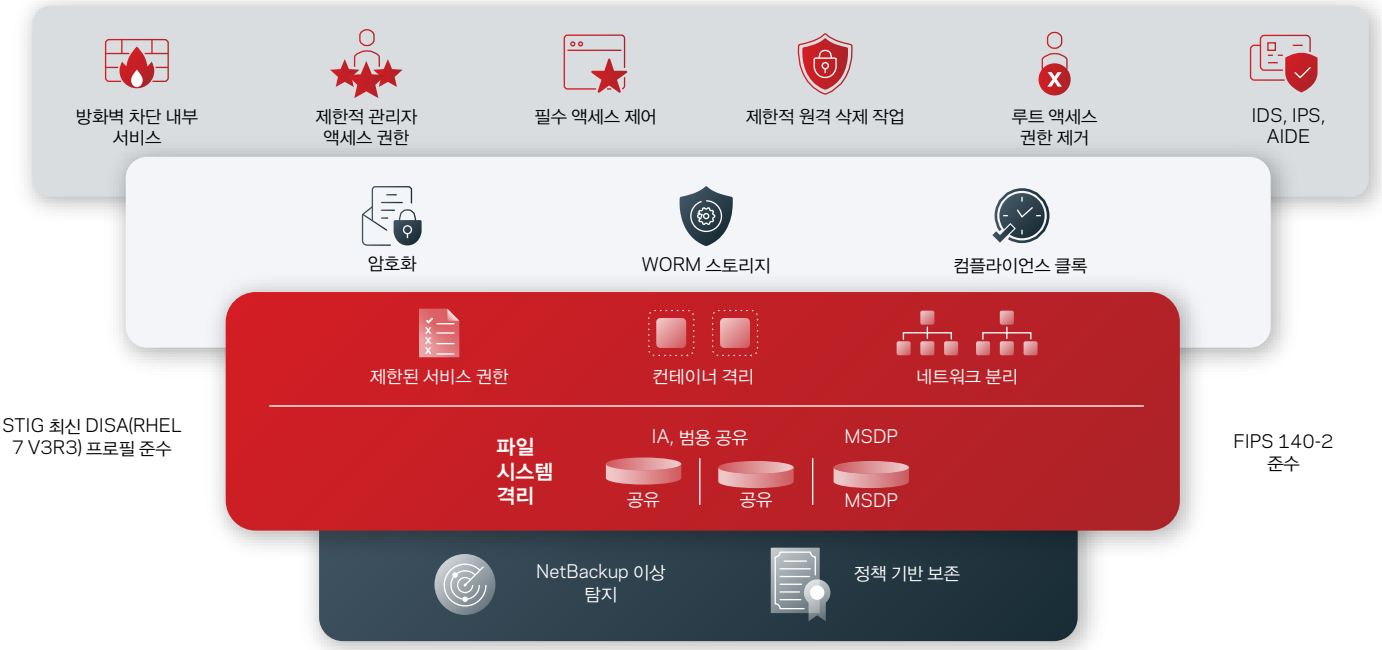

그림 1. 여러 보호 계층으로 랜섬웨어 공격을 차단하는 NetBackup Flex Scale의 제로 트러스트 모델

엔터프라이즈 클라우드 리스크

클라우드 스토리지에 데이터를 백업하는 옵션이 엔터프라이즈 비즈니스 커뮤니티에서 중요한 주제로 부상했습니다. 온프레미스 스토리지와 클라우드 스토리지를 비용 관련 이점, 단점, 리스크를 기준으로 비교하는 곳이 많습니다. 위치가 어디든 이러한 백업 옵션이 데이터 신뢰성을 보장하지 않습니다. Veritas NetBackup™ 솔루션은 AI 기반 머신 러닝을 접목하여 자율적인 데이터 관리를 지원합니다. 즉, 단일 관리 지점에서 퍼블릭 클라우드를 위해 이상 탐지, 에어 갭(Air Gap) 보호, 변조 불가 볼트(vault)를 제공합니다.

클라우드는 언제 어디서나 여러 디바이스를 통해 데이터에 액세스할 수 있다는 점에서 뛰어나지만, 그에 따른 위험 요소도 있습니다. 시스템이 손상되어 데이터 복구가 불가능해지기도 합니다. 변조 불가 스토리지가 데이터의 안전 및 보안을 보장할 유일한 해법이 될 수 있습니다. 베리타스는 엣지의 클라우드 네이티브 애플리케이션 및 데이터를 통해 온디맨드 방식으로 정보를 제공하는 방식으로, 데이터가 어디에 있더라도 확실히 보호할 수 있습니다.

데이터 보호의 관점에서 변조 불가 백업이란 일단 생성하면 변경하거나 삭제할 수 없는 데이터를 의미합니다. 따라서 기업이 누릴 수 있는 최고 수준의 데이터 보호를 제공합니다. 이 방식에서는 백업 데이터를 확실히 격리하여 보관하면서 손상을 방지하므로, (공격을 받더라도) 안전한 데이터로 복원을 진행할 수 있습니다.

데이터 지속성은 변조 불가 스토리지의 핵심 요소입니다. 즉, 데이터가 변경되지 않은 상태로 유지되도록 백업해야 합니다. 클라우드를 위한 Veritas Alta™ Data Protection, 온프레미스를 위한 Veritas NetBackup은 WORM(write once, read many) 형식으로 변조 불가 백업을 생성합니다. 이렇게 생성되는 스냅샷은 읽기 전용입니다.

민감한 성격의 데이터나 중요 데이터를 다루는 모든 기업은 신뢰할 수 있는 백업 방식의 도입에 관심 있습니다. 만약 데이터 유출 사고가 발생하면 백업이 손상되지 않았음을 어떻게 확신할 수 있을까요? 유출이 발생한 시기에 따라서는 마지막 백업 세트가 일부만 실행되었거나 손상되었을 수 있습니다. 변조 불가 잠금 모드(보존 잠금)는 에어 갭(Air Gap) 기능과 연계하여 백업에 대한 이상 탐지를 수행함으로써 어떤 하드웨어가 사용되더라도 데이터 보호 솔루션에서 중요한 차별화에 성공합니다.

변조 불가 스토리지의 특성은 비즈니스 연속성 계획 및 사이버 보안 전략에 적합합니다. 각 기업은 보안 위반 및 손상이 발견되는 즉시 억제하고 완화하는 능력을 갖춰야 합니다. 성공적으로 격리, 분리, 보호할 수 있는지는 기업의 계획 및 백업 요구 사항에 따라 달라집니다. 스냅샷과 백업이 얼마나 자주 수행되고, 이 백업(또는 다중 백업)은 어디에 저장됩니까?

데이터 손상은 여러 가지 이유로 발생할 수 있습니다. 많은 기업이 랜섬웨어와 해킹을 가장 경계하지만 감시받지 않는 액세스, 의도하지 않은 우발적인 삭제, 홍수 및 정전과 같은 자연 재해로 인해 데이터가 달라질 수도 있습니다. 변조 불가 스토리지, 즉 베리타스가 추구하는 변조 불가 백업의 이점은 어떤 이유로 복원하거나 다시 빌드하더라도 안전하고 믿을 수 있는 데이터를 얻는다는 것입니다.

그렇다면 관건은 타이밍입니다. 데이터가 손상되는 시점과 그 손상이 발견되는 시점이 다릅니다. 랜섬웨어 공격을 조사해보면, 공격이 탐지되기 몇 주 전에 악성 코드가 침투했을 수도 있습니다. 이 악성 코드가 시스템에 침투하여 은밀하게 정보, 데이터, 암호를 수집했을 가능성이 있습니다. 이 보안 위반이 격리된 백업에 그대로 복제되면 어떻게 될까요?

이에 따라 (온프레미스 또는 클라우드 모두에서) 올바른 데이터 거버넌스를 구현하고 성공적인 인프라스트럭처를 구축하는 것이 중요합니다. 여러 계층을 대상으로 데이터 분리를 적용하여 각 계층의 격리를 가능하게 하는 것은 통합 복구를 지원하는 방법 중 하나입니다. 그러면 백업과 복구를 분할하여 필요에 따라, 필요한 위치에 적용함으로써 시간과 비용을 절약할 수 있습니다. 관건은 오류의 원인이 되는 사람의 직접적인 개입을 최소화하면서 이러한 계층을 자동화하는 것입니다.

Veritas NetBackup으로 언제 어디서나 원하는 방식으로 이러한 백업을 구성하고 자동화할 수 있습니다. 복원이 필요할 경우 Veritas Alta™ Data Protection을 통해 클라우드 및 NetBackup, 즉 온프레미스에서 빠르고 쉽게 복구할 수 있습니다. 컨테이너를 사용하여 변조 불가 인프라스트럭처를 추가로 생성할 수 있습니다. 심각한 오류는 전체 시스템이 아닌 특정 컨테이너에서의 롤백으로 해결하고, 인스턴스를 신속하게 대체합니다.

베리타스가 구현하는 완벽한 변조 불가 모드

엔터프라이즈 클라우드 인프라스트럭처에서는 제대로 최적화된 기술 인터페이스와 함께, 자동화된 구축 전략, 즉 분할된 롤백, 스냅샷, 백업 및 복원 기능을 지원하는 전략으로 제로 트러스트 아키텍처를 유지해야 합니다. 수작업에 의한 개입과 액세스를 없애 서버 및 기타 리소스를 중앙에서 관리하고 감사할 수 있습니다. 이러한 방식으로 모든 서버에 일관성 있게 패치 및 소프트웨어 버전을 적용하면서 오류를 방지할 수 있습니다.

NetBackup과 NetBackup Flex는 유연하고 스토리지에 독립적인 변조 불가 백업 관리자인 OST(OpenStorage Technology) API를 사용합니다. 베리타스 스토리지와 기타 타사 스토리지를 사용하여 자동 이미지 복제(AIR)를 통해 1차 복제, 2차 복제(중복 제거), 및 크로스도메인(cross-domain) 복제를 지원함으로써 모든 백업 스토리지 계층에서 무제한 구성 옵션을 제공할 수 있습니다. 이러한 방식으로 온프레미스와 클라우드의 데이터에서 보안 및 컴플라이언스를 유지합니다. 그리고 Amazon(AWS) S3 오브젝트 잠금과 함께 사용할 수 있습니다. 기업은 변조 불가 이미지 정책을 관리하고 타사의 변조 불가 어플라이언스를 활용하면서 벤더에 독립적인 상태를 유지할 수 있습니다.

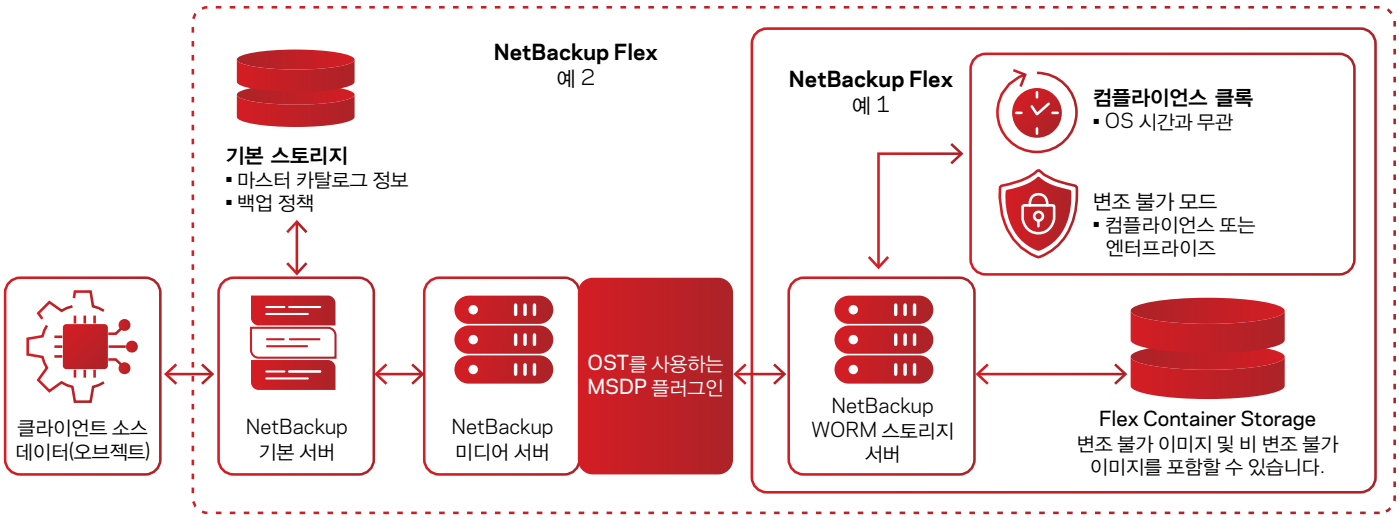

그림 2. Veritas Flex Appliance가 기본 제공하는 다양한 보안 기능

NetBackup Flex와 NetBackup Flex Scale은 컨테이너 기술을 기반으로 멀티테넌트 기능으로 데이터 보호를 확장하여 데이터 센터 비용을 절감하고 관리 효율을 향상하고 랜섬웨어 및 각종 보안 위협에 대한 레질리언스를 제공합니다. 이를 통해 기업은 통합 복구 전략으로 비즈니스 연속성을 유지하고, 다운타임 및 수익 손실을 줄이고, 리스크를 최소화하고, 규제 및 회사 차원의 거버넌스 정책을 이행할 수 있습니다. 클라우드를 포함하는 다중 지점 백업 리포지토리로 에어 갭(Air Gap) 솔루션을 제공합니다. 정책 기반 보존 잠금, 역할 기반 액세스 제어, 암호 정책 관리, STIG(Security Technical Implementation Guide) 하드닝 사이버 보안 기능도 갖추었습니다.

엔터프라이즈 및 컴플라이언스 잠금 모드를 통해 해당 기업에 적합한 변조 불가 강도를 선택할 수 있습니다. 컴플라이언스 모드는 미리 정의된 보존 기간에 루트 사용자를 비롯하여 어떤 사용자도 데이터를 삭제할 수 없는 변조 불가 스토리지를 지원합니다. 엔터프라이즈 모드는 미리 정의된 보존 기간에 데이터가 삭제되지 않도록 보호합니다. 특별한 권한을 가진 사용자만 이중 인증을 거쳐 보존 설정을 변경하거나 데이터를 삭제할 수 있습니다. 보존 시간을 바꾸거나 데이터를 수정하거나 삭제하려면, 서로 다르지만 합당한 RBAC(role-based access control) 레벨에 있는 두 사람이 동의해야 합니다.

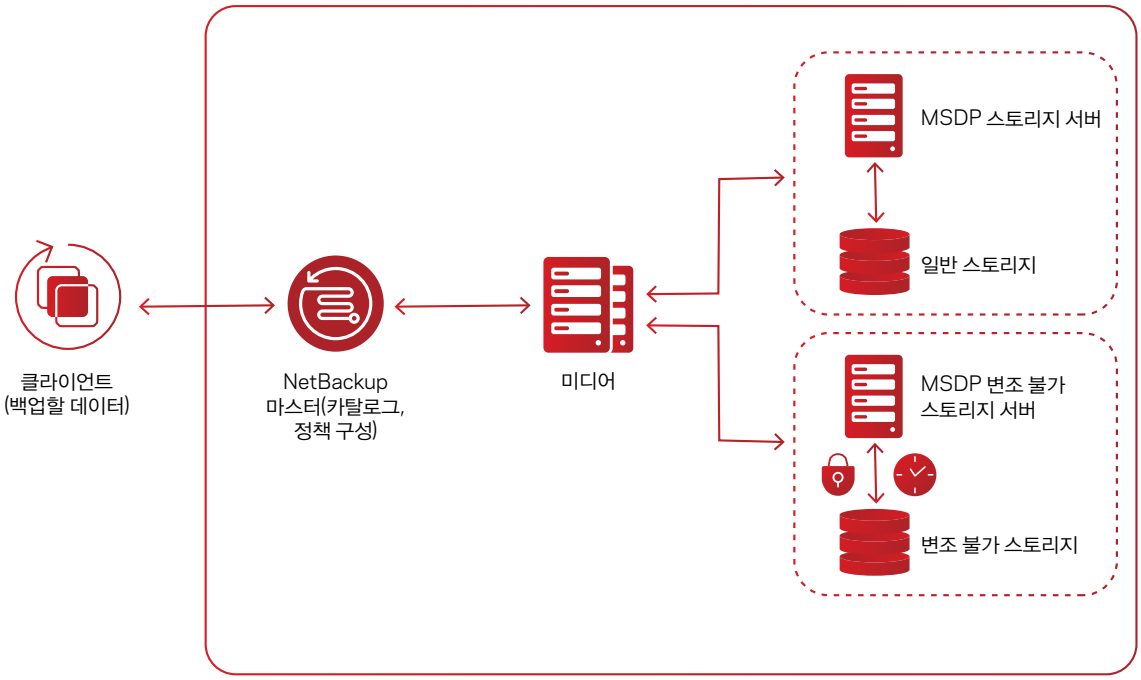

그림 3. 베리타스가 랜섬웨어 공격으로부터 IT 서비스를 보호하는 방법

단일 솔루션으로 다양한 기능 지원

단일 공통(one-size-fits-all) 아키텍처를 사용하는 곳은 거의 없습니다. 환경 내에 수많은 애플리케이션이 있고 다양한 차이점이 있는 만큼, 각 기업은 이러한 구조를 통합할 방법을 계속 모색합니다. 그러면 데이터 보호 전략이 인프라스트럭처 스택 전체를 포괄함을 확신하면서 안심할 수 있기 때문입니다. 베리타스는 변조 불가 모드가 필요한 경우를 위해 온프레미스와 클라우드에서 변조 불가 모드/WORM을 지원합니다. 그와 함께 타사 검사 기능도 활용 가능한 악성 코드 검사도 기본 제공하므로, 악성 코드를 탐지하는 변조 불가 볼트(vault)를 구현할 수 있습니다.

그리고 Flex WORM 스토리지 서버에 IRE(Isolated Recovery Environment)를 구성하여 프로덕션 환경과 IRE의 MSDP(Media Server Deduplication Pool) WORM 스토리지 서버에 있는 보호 받는 데이터 카피본 사이에 에어 갭(Air Gap)을 생성할 수 있습니다. 프로덕션 환경에서 이 기능을 위해 별도의 단계를 거칠 필요 없습니다. 모든 명령은 MSDP WORM 스토리지 서버 셸에서 실행됩니다.

변조 불가 백업에서는 해당 데이터 백업이 진짜이고 정확하고 보존된 것임을 보장합니다. NetBackup Flex Appliance 역시 FIPS(Federal Information Processing Standards) 140-2에 따라 데이터 전송 및 저장 시 암호화합니다. 정부/공공 기관, 금융 기관, 의료 기관은 이 인증을 통해 제3의 기업이 취급하는 데이터가 안전하게 저장되고 암호화되며 적정 수준의 기밀성, 무결성, 신뢰성을 갖추었음을 확인합니다. 그리고 NetBackup 및 Flex Appliance 변조 불가 솔루션은 (컴플라이언스 모드에서) 다음과 같은 Chasset Associates 변조 불가 평가[1]를 완료했습니다.

- SEC(Securities and Exchange Commission) - 17 CFR § 240.17a-4(f)
- FINRA(Financial Industry Regulatory Authority) Rule 4511(c)
- CFTC(Commodity Futures Trading Commission) - 17 CFR § 1.31(c)-(d)

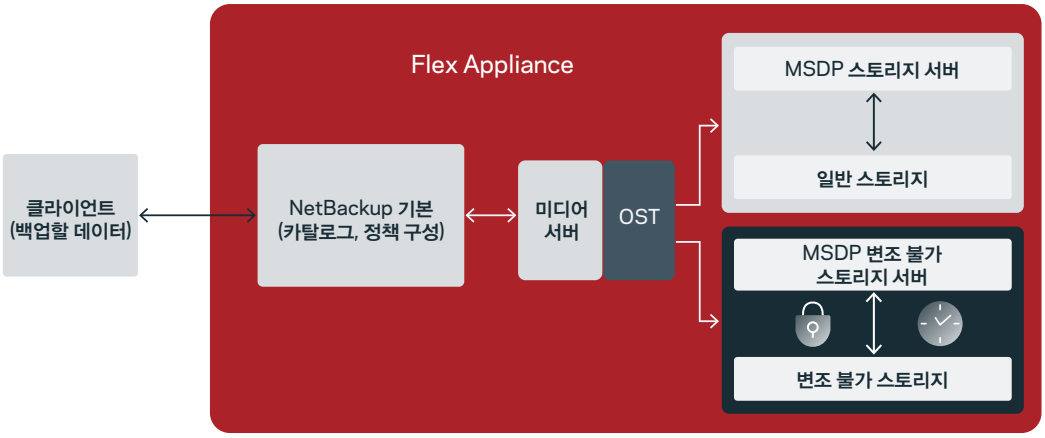

그림 4. NetBackup 잠금 모드

Veritas NetBackup은 온프레미스, 하이브리드, 멀티 클라우드 환경 전반에서 규모의 제약 없이 재해 복구(DR)를 지원하면서 구체적인 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)를 준수합니다. NetBackup이 다양한 복구 옵션을 지원하므로 기업의 복구 요구 사항에 가장 적합한 방식을 선택하면 됩니다. 예를 들어, 클라우드에서는 Veritas Alta™ Application Resiliency로 규모의 제약 없는 복구, 온프레미스에서는 NetBackup Resiliency를 활용합니다.

클라우드를 위한 Veritas Alta™ Analytics와 온프레미스를 위한 IT Analytics로 데이터 인프라스트럭처 전체를 모니터링하고 리포팅하면서 격차의 발생이나 사일로화를 방지합니다. 온프레미스와 클라우드 어디서나 Veritas NetBackup으로 기술 스택의 모든 지점을 통합하여 신뢰성과 성능을 극대화합니다. Veritas NetBackup Flex Appliance는 특별히 설계된 컴플라이언스 클록이 내장되어 있습니다. VxFS(Veritas File System)를 기반으로 하는 이 기술은 OS에 독립적이고 관리자도 변경할 수 없는 보존 기간을 관리하는 데 사용됩니다.

결론

베리타스는 OS 하드닝, 컨테이너 격리, 제로 트러스트 보안 모델의 조합을 통해 보호에 필요한 다계층 인프라스트럭처 변조 불가 및 삭제 불가 모드를 제공합니다. 베리타스는 이 문제의 복잡성을 고려하면서 고객이 더 수월하게 탐색하고 처리할 수 있게 합니다.

기업이 충실하게 데이터를 백업하더라도 사람의 실수나 장비 고장이 일어나기 마련입니다. 사고로 데이터가 삭제되거나 수정될 위험성이 큽니다. 변조 불가 스토리지에 파일을 저장함으로써 손상 및 사이버 공격에 관한 걱정을 덜 수 있습니다. Veritas NetBackup은 우발적으로나 의도적으로 파일을 변경할 수 없게 함으로써 사이버 보안 전략을 뒷받침할 더 효율적이고 효과적인 프로세스를 마련합니다. 그리하여 고객이 경제적 손실과 다운타임을 방지할 수 있게 합니다.

자세한 내용은 veritas.com/solution/cloud-data-security 사이트에서 확인하십시오.

1. veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup

Veritas Technologies 소개

Veritas Technologies는 데이터 보호 및 가용성 분야의 글로벌 선도 기업으로, 포춘 500대 기업 중 87%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 타깃, 60개 이상의 클라우드 플랫폼을 지원합니다. 보다 자세한 정보는 베리타스 홈페이지(www.veritas.com/kr) 또는 베리타스 트위터(@veritastechllc)에서 확인하실 수 있습니다.

VERITAS

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

V1673 12/22