

랜섬웨어 레질리언스를 보장하는 4가지 방안

베리타스와 함께 랜섬웨어 위협에 한발 앞서 대비하세요.

랜섬웨어 및 악성 코드 공격이 날로 기승을 부리며 이제는 업종에 관계없이 모든 기업을 위협하고 있습니다. 올해 들어 랜섬웨어 공격이 185% 증가했으며¹, 그로 인한 경제적 피해가 200억 달러를 넘어설 것으로 보는 전망이 대부분입니다.² 공격자는 기업의 인프라스트럭처에 침투하고 마비시킬 더 새롭고 정교한 방법을 개발하느라 여념이 없습니다. 이러한 긴박한 상황에서 최상의 방어는 철저히 대비하는 것입니다.

베리타스는 백업 및 복구를 우선 순위에 두고 통합적인 멀티레이어 레질리언스 프레임워크를 근간으로 삼아야 한다고 조언합니다. 이를 위해 기업은 통합 사이버 보안 전략에서 보호, 탐지, 복구 영역에 주력해야 합니다. 베리타스 솔루션은 모든 중요 데이터를 보호하여 그 가치를 높이고, 잠재적 랜섬웨어 위협을 탐지하며, 오케스트레이션되고 자동화된 복구를 보장함으로써 고객이 빠르게 위기를 극복하고 정상적으로 운영하도록 지원합니다. 특히 다음과 같은 측면에서 랜섬웨어 레질리언스 전략에 베리타스를 고려해야 합니다.

랜섬웨어 레질리언스 보장을 위해 베리타스를 선택해야 하는 4가지 이유



1. 데이터를 더 이상 위협에 방치하지 마십시오. 베리타스는 비용 부담 없는 탁월한 변조 불가 기능을 활용하여 모든 중요 데이터를 확실히 보호합니다.

베리타스의 변조 불가 기술은 간편일수록이지 않습니다. 다양한 옵션과 유연성을 보장하므로, 변조 불가 기능을 갖춘 타사 하드웨어에 연결해야 하거나, 베리타스가 기본 제공하는 변조 불가 스토리지를 선호하는 누구라도 선택할 수 있습니다. 또한 AWS S3 Object Lock 지원으로 베리타스 변조 불가 기능이 한층 더 확장되었습니다.



2. 실제 공격 상황에서 귀중한 시간을 허비하지 마십시오. 베리타스 고객은 원클릭 방식의 오케스트레이션 복구 기능을 사용하여 모든 레벨에서 아무런 제약 없이 빠르게 복구할 수 있습니다.

버튼 하나만 누르면 모든 규모에서 효율적으로 다른 사이트나 클라우드에 완전한 오케스트레이션 복원이 자동으로 수행됩니다. 데이터 액세스는 물론 애플리케이션도 모든 필수 종속성을 그대로 유지하면서 중단 없이 실행됩니다. AWS S3 Object Lock에서 중복 제거 데이터의 전송과 저장을 지원하고, 이처럼 효율적으로 저장된 중복 제거 데이터를 사용하여 필요에 따라 데이터 센터 전체를 복원할 수 있는 벤더도 베리타스가 유일합니다. 베리타스는 신뢰할 수 있는 검증된 레질리언스 솔루션을 핵심 기술 요소로 활용하면서 데이터, 애플리케이션, 데이터 센터 등 원하는 모든 레벨에서 복구 프로세스 전체를 자동화하고 오케스트레이션하여 아무런 제한 없이 작업을 수행합니다.



3. 가시성을 놓치지 마십시오. 베리타스는 첨단 이상 탐지 기술, 상시 모니터링, 인프라스트럭처 인식 기능으로 모든 스토리지, 백업, 클라우드 벤더를 한눈에 보고 관리하도록 지원합니다.

고객의 프로덕션 환경 및 백업 벤더(경쟁사 솔루션 포함)에 대한 리포트를 생성한 다음 모든 데이터 포인트를 상호 참조하면서 어떤 시스템도 빠짐없이 관리하는 기업은 베리타스가 유일합니다. 마치 파노라마처럼 탁월한 수준의 가시성을 제공하고, 이를 바탕으로 고객의 환경 전반을 철저히 보호합니다. 베리타스 솔루션 간의 긴밀한 협업을 통해 기본 데이터 환경과 데이터 보호(백업) 환경에서 인프라스트럭처 전체는 물론 개별 파일 내에서도 각종 이상을 밝혀낼 수 있습니다. 다양한 데이터 소스를 대상으로 이러한 취약점을 모니터링하고 리포팅하는 기능이 있어야 위협 경로를 제대로 관리할 수 있습니다. 베리타스는 가상 시스템을 자동으로 검색하여 보호하고 백업 모니터링 및 복구 준비도 지원하면서 고객이 안심할 만한 수준의 레질리언스를 실현합니다.





4. 데이터를 취약한 상태로 방치하지 마십시오. 베리타스가 제공하는 데이터 암호화 기능을 활용하면, 랜섬웨어 공격자에게 몸값을 지불할 필요가 없습니다.

베리타스는 어떤 경쟁사보다도 많은 네트워크 보안 및 산업 인증을 갖추고 데이터를 저장하거나 전송할 때마다 암호화하는 기능을 통해 어디서나 데이터 무결성을 보장하고 유지하는 제품을 개발합니다. 베리타스 제품으로 보호하는 백업 환경에서는 설령 랜섬웨어 공격이 발생해도 공격의 두 번째 주요 목적인 데이터 추출을 차단하므로, 경제적 피해를 방지하고 기업의 평판을 지킬 수 있습니다.

선제적이고 통합적인 접근 방식이 필요

업계에서 가장 포괄적이고 각종 요건에 부합하며 안전한 베리타스 랜섬웨어 레질리언스 솔루션을 선택한 고객은 실제 공격 상황에서도 두려움 없이 효과적으로 대처할 수 있습니다. NIST(National Institute of Standards and Technology) 프레임워크를 준수하는 베리타스 제품으로 엣지, 코어, 클라우드 등 데이터가 있는 곳이라면 어디서나 확실히 보호, 탐지, 복구할 수 있습니다.



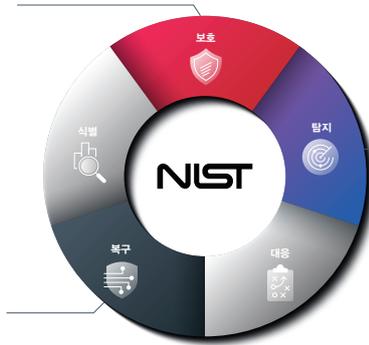
보호

시스템 강화 기능, 변조/삭제 불가 이미지 관리 및 저장 기능, 데이터 전송/저장 시 암호화 기능, 역할 기반 액세스 제어(RBAC)와 다단계 인증(MFA)을 포함하는 ID 및 액세스 관리(IAM)로 데이터 무결성 보장



복구

가장 규모가 크고 까다로운 멀티 클라우드/데이터 센터 환경에서도 전체 시스템 간 복구 자동화 및 오케스트레이션 수행. 유연한 복구 방식, 레질리언스 오케스트레이션 툴, Instant Rollback for VMware 기능으로 몇 초 내에 일괄 복구하도록 지원



탐지

머신러닝 기반 시와 예측 분석을 활용하여 기업 환경을 전반적으로 파악하고, 인사이트 발굴과 백업 감지 및 데이터의 이상 여부를 모니터링. 포괄적인 통합 뷰에서 시스템 활동을 상시 모니터링하고 리포팅하면서 각종 보안 위협 및 취약점 해결

리스크를 해소하고 불확실성을 제거하며 통제력을 유지할 방법은? <https://www.veritas.com/ko/kr/ransomware>에서 자세히 알아보십시오.

- <https://www.sonicwall.com/news/sonicwall-record-304-7-million-ransomware-attacks-eclipse-2020-global-total-in-just-6-months/>
- <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>

Veritas Technologies 소개

Veritas Technologies는 데이터 보호 및 가용성 분야의 글로벌 선도 기업으로, 포춘 500대 기업 중 87%를 포함한 5만개 이상의 전세계 기업이 베리타스 기술을 기반으로 IT 복잡성을 해결하고 데이터 관리를 간소화합니다. 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 데이터의 위치와 관계없이 데이터 보호를 자동화하고 복구를 조정하는 물론, 비즈니스 크리티컬 애플리케이션의 가용성을 항상 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 타겟, 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