VERITAS

사이버 위협 레질리언스 6단계

사이버 위협에 한발 앞서 대비하도록 지원하는 베리타스

랜섬웨어와 악성 코드 공격이 갈수록 기승을 부리면서 이제 모든 기업과 업종을 막론하고 중대한 위협이 되었습니다. 2021년에는 1초마다 19건의 랜섬웨어 공격이 발생했고[1], 올해에는 그 경제적 피해가 200억 달러를 넘어설 것이라는 전망이 지배적입니다.[2] 공격자는 기업의 인프라스트럭처를 침투하여 마비시킬 더 새롭고 정교한 방법을 개발하는 데 집중하고 있습니다. 이처럼 긴박한 상황에서 최상의 방어는 철저히 대비하는 것입니다.

베리타스는 백업 및 복구를 우선시하면서 통합적인 다계층 레질리언스 프레임워크의 근간으로 삼아야 한다고 조언합니다. 즉, 기업의 통합 사이버 보안 전략에서 보호, 탐지, 복구 영역에 주력해야 합니다. 베리타스 솔루션은 모든 중요 데이터를 보호하여 그 가치를 높이고, 잠재적 랜섬웨어 위협을 탐지하며, 복구를 오케스트레이션하고 자동화함으로써, 고객이 빠르게 위기를 극복하고 정상적으로 운영하도록 지원합니다. 특히 다음과 같은 이유로 랜섬웨어 레질리언스 전략에 베리타스를 고려해야 합니다.

사이버 위협 레질리언스를 위해 베리타스를 선택해야 하는 6가지 이유

1. 가시성을 양보하지 마십시오.

첨단 상시 모니터링 및 인프라스트럭처 인식 기능으로 단일 통합 뷰에서 모든 스토리지, 백업, 클라우드 벤더를 관리합니다.

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

2. 회사를 취약한 상태로 방치하지 마십시오.

베리타스는 네트워크 보안, ID 및 액세스 관리(IAM), 데이터 암호화 기술로 공격 범위를 최소화하고 대규모 장애를 방지합니다.

대부분 경쟁사보다 더 확실하게 검증된 안정성 및 복구 기능을 근간으로 다계층 보안을 비롯해 표준 및 고급 기능, 즉 다단계 인증(MFA), 역할 기반 액세스 제어, 통합 보호 및 탐지, 보안 컴플라이언스 클록(특허 출원 중), 제한적 원격 액세스 기능으로 어디서나 데이터를 보호하는 제품을 설계하고 제공합니다. 더 나아가 베리타스는 타사 기술에 대한 의존도가 가장 낮은 벤더로, 공격 범위에 대한 지속적인 감시와 통제를 지원합니다. 베리타스 제품이 보호하는 백업 환경에서는 설령 랜섬웨어 공격이 발생해도 그 두 번째 목적인 데이터 추출을 차단하므로, 경제적 피해를 방지하고 기업의 평판을 보호할 수 있습니다.

3. 데이터를 위험한 상태로 방치하지 마십시오.

베리타스는 비용 부담 없는 특별한 변조 불가(immutability) 기능을 활용하여 모든 중요 데이터를 확실히 보호합니다.

베리타스의 변조 불가 기술은 천편일률적이지 않습니다. 다양한 옵션과 유연성을 보장하므로 변조 불가 기능을 갖춘 타사 하드웨어에 연결해야 하거나 베리타스가 기본 제공하는 변조 불가 스토리지를 선호하는 어떤 경우에도 선택할 수 있습니다. Object Lock Technologies 지원으로 베리타스 변조 불가 기능이 한층 더 확장되었습니다.

4. 해커가 이미 시스템에 침투했을 가능성도 고려하십시오.

베리타스는 AI 기반 이상 탐지 및 악성 코드 검사 기능을 제공합니다. 따라서 고객 환경 전반에서 비정상적인 상황이 발생할 경우 신속하게 알려주므로, 고객이 매우 유리한 입장에서 대응할 수 있습니다.

타사 백업 제품을 비롯한 모든 시스템을 상시 검사하고 모니터링하면서 해당 환경의 의심스러운 이상 요인을 거의 실시간으로 알려주는 기업은 베리타스가 유일합니다. 베리타스가 제공하는 자동화된 온디맨드 악성 코드 검사는 인공 지능 및 머신 러닝을 활용하여 악성 코드를 빠르고 정확히 찾아냅니다.

5. 실제 공격 상황에서 귀중한 시간을 허비하지 마십시오.

베리타스 고객은 원클릭 방식의 오케스트레이션 복구 기능을 사용하여 어떤 레벨에서도, 아무런 제약 없이 빠르게 복구할 수 있습니다.

간단히 버튼 하나만 누르면 다른 사이트나 클라우드에 완전한 오케스트레이션 복원이 자동으로 수행되며, 어떤 규모에서도 효율적으로 수행됩니다. 데이터 액세스는 물론 애플리케이션도 모든 필수 종속성을 그대로 유지하면서 중단 없이 실행됩니다. Object Lock Technologies가 중복 제거 데이터의 전송과 저장을 지원하고, 효율적으로 저장된 중복 제거 데이터를 사용하여 필요에 따라 데이터 센터 전체를 복원할 수 있는 벤더 역시 베리타스가 유일합니다. 베리타스는 신뢰할 수 있는 검증된 레질리언스 솔루션을 핵심 기술 요소로 활용하면서 데이터, 애플리케이션, 데이터 센터 등 어떤 레벨에서도 아무런 제한 없이 복구 프로세스 전체를 자동화하고 오케스트레이션합니다.

6. 사이버 공격이 실현되기 전에 미리 복구 오케스트레이션을 실행하고 검증해야 합니다.

비즈니스의 모든 단계별 리허설을 포함하는 DR 테스트

베리타스는 가동 중단 없는 DR 테스트를 쉽고 효율적으로 실행하도록 지원하는 유일한 벤더입니다. 이 테스트에서는 비즈니스의 모든 단계를 대상으로 검증된 자동 리허설 기능을 활용할 뿐만 아니라 프로덕션 환경에 속하지 않는 리소스, 이를테면 네트워크 펜싱, 샌드박스 환경 등을 NetBackup과 함께 활용합니다.

베리타스의 선제적인 다계층 사이버 레질리언스 접근 방식 필요

베리타스는 사전 예방적으로 데이터를 보호하고, AI를 활용하여 각종 위협을 탐지하며, 어떤 규모에서도 업계 최고 수준의 신속한 보안을 구현하면서 차원 높은 사이버 레질리언스를 실현합니다. 리스크를 해소하고 불확실성을 제거하며 통제력을 유지할 방법에 대한 자세한 내용은 https://www.veritas.com/ko/kr/solution/ransomware에서 확인하십시오.

1. https://www.sonicwall.com/resources/white-papers/2022-sonicwall-cyber-threat-report/
2. 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 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

Copyright © 2022 Veritas Technologies LLC. All rights reserved. Veritas, Veritas 로고, NetBackup은 미국 및 기타 국가에서 Veritas Technologies LLC 또는 그 자회사의 상표 또는 등록 상표입니다. 다른 이름은 해당 회사의 상표일 수 있습니다.

V1550 04/22