


미래를 보호하기 위한 준비

경쟁에서 앞서 나가는 방법





데이터 보호와 복구는 일회성 경주가 아니라 험난한 고비를 넘어야 하는 복잡한 여정입니다.

데이터에 대한 위협이 갈수록 증가하고 진화하는 중입니다. 공격자는 기업 운영의 핵심인 데이터를 공격하고 장악할 새로운 방법을 개발하고 있습니다.

데이터 보호는 개별 과제에 머무르지 않고 여러 가변적 속성을 가지고 진화하는 비즈니스 문화의 영역으로 자리잡았습니다. 워크로드의 다양성과 위치, 각 애플리케이션과 데이터의 중요도는 필요한 보호 수준 및 복구 방식을 평가하는 데 중요한 기준이 됩니다.

고가용성, 거버넌스, 컴플라이언스 등의 요인이 서로 작용하면서 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)에 영향을 미칩니다.

새도우 IT(shadow IT)와 기술 관련 부채가 폭발적으로 증가했습니다. 각 팀에서 엄청난 양의 데이터를 생성하면서 미션 크리티컬 데이터를 취약한 상태로 방치하는 오류까지 발생하게 됩니다. 기업은 어떤 데이터가 필수적인지 제대로 알지 못해 리스크 완화를 위한 우선 순위를 정하기 쉽지 않습니다.

미래 지향적으로 사고하고 각별한 관심을 기울이면서 시대의 변화에 앞서 나가면 그 과정에서 발생할 수 있는 여러 어려움에 대비할 수 있습니다.





현재 보유한 데이터 식별

무엇을 가지고 있는지 모르는 상태에서 제대로 보호할 수 있을까요?

수많은 앱과 플랫폼이 효율성을 높이고 더 효과적인 데이터를 제공하겠다고 약속합니다. 직원들이 사일로화된 상태에서 이러한 툴을 사용하면서 클라우드에 위치한 플랫폼에 고객 정보와 회사 데이터를 입력합니다. 그러면 어떻게 될까요? 소위 '데이터 확산(data sprawl)'의 딜레마, 그리고 멀티 클라우드 적용 범위에 관한 문제가 발생합니다.

공격자가 이러한 데이터를 유출할 수 있는데, 이는 해당 기업이 데이터를 제대로 보호하지 않기 때문입니다. 의심스러운 행동도 들리지 않습니다. IT 팀이 이를 감시할 필요성을 비롯해 그 존재 자체를 모르기 때문입니다. 그러던 중 재해가 발생하면, 중요 정보가 제대로 백업되지 않아 복구할 수 없다는 사실을 알게 됩니다.

재해가 발생했는데도 중요 정보가 제대로 백업되지 않아 복구가 불가능합니다.

데이터 확산, 즉 데이터가 건잡을 수 없게 증가하는 현상은 거버넌스 차원의 과제입니다. 이를 해결하려면 회사의 인프라스트럭처에 관한 가시성 향상을 비롯해 보다 강력한 체계와 직원 교육이 필요합니다.

보다 성공적인 결과를 얻으려면 데이터에 관한 컨텍스트를 확보하고 복잡한 절차와 관련 리스크를 측정하여 엡지, 코어, 클라우드의 백업 및 복구 전략을 실행할 방법을 결정해야 합니다.

주요 질문

- 어떤 데이터를 보유하고 있으며 위치는 있습니까?
- 데이터에 관한 가시성을 향상하려면 어떻게 해야 합니까?

베리타스 솔루션

베리타스 데이터 보호 솔루션으로 규모의 제약 없이 데이터를 보호할 수 있습니다. AI 기반 이상 탐지 엔진을 활용하여 방대한 데이터를 마이닝하고, 모니터링 및 리포팅을 자동화하며, 실행 가능한 인사이트를 찾아내고, 만일의 공격에 관한 조기 경보 체제를 구축할 수 있습니다.

베리타스 분석 솔루션은 각종 백업 및 스토리지를 모든 백업 벤더와 교차 참조하면서 문제를 놓치거나 취약한 상태로 두지 않습니다. 또한 타사 제품을 비롯한 모든 시스템을 검사 및 모니터링하면서 사각지대가 발생하지 않도록 차단합니다.

Veritas Data Insight는 리포팅의 가능성을 파악할 뿐만 아니라 잠재적 유해 데이터를 찾아내 민감한 데이터에 대한 액세스를 취소하고 데이터 소유자와의 협업으로 더 현명한 의사 결정을 내리며 컴플라이언스 표준을 준수할 수 있습니다. 리스크를 집중 조명하고 미확인 데이터를 발견하며 다양한 사용자 활동을 기록하면서 활동 패턴을 찾아내 이상 징후를 식별하고 감지합니다.





데이터를 노리는 각종 위협 차단

사이버 범죄자는 사람이 네트워크의 가장 약한 고리라는 것을 알고 있습니다.

사이버 공격과 및 데이터 유출 사고 대부분은 사람의 상호 작용과 주의력 부재로 인해 발생합니다. 피싱이 효과적인 이유도 여기에 있습니다.

귀사는 어떤 방법으로 공격을 차단하십니까? ID 및 액세스 관리, 암호화 등의 요소는 중요한 보호 수단입니다. 다중 인증(Multi-Factor Authentication)과 역할 기반 액세스 제어를 구현하여 공격이 성공할 가능성을 줄일 수 있습니다. 데이터 저장 및 전송 시 데이터를 암호화하여 사용하기 어려운 데이터로 만들면, 데이터 유출을 방지하는 데 도움이 됩니다. 스마트 카드 인증, SSO(Single Sign-On), 권한 기준 액세스 관리 등을 통해 제로 트러스트(Zero Trust)의 '최소 권한(least privilege)' 원칙을 강력히 적용할 수 있습니다.

계층화된 예방 및 보호 전략으로 여러 수준에서 구현된 여러 솔루션을 사용합니다. 추가 인증을 위해 디바이스에 디지털 인증서를 발급해야 합니다. 백업 액세스에 이중 권한 부여를 적용하여 한층 더 확실하게 보호합니다.

보안 액세스를 관리하고 잘못된 구성으로부터 데이터를 보호하는 것이 무엇보다 중요합니다. 각 환경에서 리소스, 작업, ID를 식별하고 파악해야 온프레미스 및 클라우드에서 권한을 관리하고 올바르게 적용할 수 있습니다. 각종 시도와 변경의 진행 상황을 추적하고 모니터링하면서 보안 태세를 강화하고 실시간으로 개선할 수 있습니다.

주요 질문

- 피싱 및 악성 코드에 의한 보안 침해를 막기 위해 현재 어떤 노력을 하고 있습니까?
- 현재의 보호 방법에서 더 개선할 수 있는 점이 있을까요?

베리타스 솔루션

베리타스 데이터 보호 솔루션은 벤더에 독립적이며, 제로 트러스트 원칙을 기반으로 합니다. 네트워크를 보호하고, 데이터 전송 및 저장 시 AES 256비트 암호화로 보호하며, FIPS 140-2 인증 요건을 충족하고, 사용자 액세스를 제한하며, 역할 기반 액세스 제어 및 다중 인증을 지원합니다.

Veritas Data Insight는 프로덕션 데이터에 관해 실시간에 가까운 가시성을 제공하여 비정상적인 사용자 행동 및 알려진 랜섬웨어 확장자를 토대로 랜섬웨어를 식별할 수 있게 합니다. 과잉 노출된 데이터도 찾아내 공격 노출 범위를 제한하고 줄일 수도 있습니다.

베리타스 분석 솔루션은 단일 통합 대시보드에서 운영 인사이트 및 인텔리전스를 활용하면서 랜섬웨어, 보호받지 않는 시스템, 백업 관련 이상 요인을 파악합니다. 이를 바탕으로 스토리지를 최적화하고 비용을 줄이고 컴플라이언스 및 규제 요건에 선제적으로 대비할 수 있습니다.

Veritas Alta™ Classification은 데이터 보안 및 컴플라이언스에 걸림돌이 되는 요인을 해결합니다. 메타데이터 속성 및 사용자 행동 분석 정보를 수집하여 실행 가능한 인텔리전스를 제공하며, 데이터 소유권, 사용량, 액세스 제어를 확인하고, 개인 정보 보호 및 보안 관련 리스크를 줄입니다.





취약한 상태의 중요 데이터 파악

데이터는 멈춰 있지 않습니다. 따라서 전략과 솔루션도 달라져야 합니다.

확장성과 적응성을 갖춘 제품과 서비스를 구현해야 합니다. 멀티 클라우드 환경에서 여러 가지 통합을 구현해야 하는 부담 하에 성능을 제대로 유지하려면 유연성이 필요합니다.

특정 회사가 모든 솔루션을 단일 벤더에서 단일 조건에 구매할 것으로 단정해서는 안 됩니다. 비즈니스 개발은 그렇게 진행되지 않습니다. 매우 복잡한 양상을 띠며, 오래된 레거시 소프트웨어 및 기술과 정교한 최신 솔루션이 공존합니다.

따라서 데이터의 우선 순위를 정하고, 충족해야 할 컴플라이언스 및 규정의 수준을 파악해야 합니다. 백업 관리 방안, 궁극적으로는 복구 시간에 영향을 미칠 백업의 확장성과 규모를 다룰 방법도 결정합니다. 대역폭 용량이 백업 및 복구에 미칠 영향을 알고 있으면, 중요 워크플로우를 가장 효율적으로 백업하고 복구할 방법을 결정하는 데 도움이 됩니다.

주요 질문

- '중단 없이 순조롭게 운영'하는 데 가장 중요한 데이터는 무엇입니까?
- 데이터 백업의 우선 순위는 어떻게 정해야 합니까?

베리타스 솔루션

베리타스 데이터 보호 솔루션은 특정 벤더에 종속되지 않습니다. 비용 효과적이고 구축 및 관리하기 용이한 안정적인 보존 및 보호 워크플로우를 제공합니다. 멀티 클라우드 및 하이브리드 클라우드 환경을 간소화하여 단일 플랫폼으로 통합할 수 있습니다.

Veritas Alta™ Shared Storage는 비즈니스 크리티컬 애플리케이션을 위해 설계되었습니다. 엔터프라이즈 환경에 최적화된 이 공유 스토리지 솔루션은 비용 증가 없이 탁월한 성능과 레질리언스를 제공합니다. 애플리케이션 관리자와 인프라스트럭처 관리자는 이 솔루션을 활용하여 중요 데이터를 보호할 수 있습니다. 암호화, WORM(Write-Once, Read-any) 기능, 일관성 있는 스냅샷, 데이터베이스 가속화 기능도 제공합니다.

Veritas Alta™ SaaS Protection은 직원이 퇴사한 후에도 Microsoft 365 계정에 저장된 데이터를 유지하고 액세스할 수 있게 합니다. 이를 위해 별도의 라이선스를 유지하거나 구입하지 않아도 됩니다. 세분화된 단계 복구 방식으로 클라우드나 온프레미스에서 선호하는 위치에 풀더, 메일박스, 사이트를 복원합니다. 백업 스토리지를 최대 페타바이트급으로, 수십 억 개의 오브젝트도 수용할 만한 규모로 확장하면서 성능과 유연성을 극대화합니다. 증분 백업을 더 정기적으로 수행하면서 RPO 및 RTO를 최소화하고 사이트 컬렉션을 대상으로 상시 데이터 보호 기능을 구현할 수 있습니다.





데이터와 백업의 가용성 및 효율성 제고

데이터는 백업되어 있습니다. 그렇다면 재해 상황에서 데이터를 복원하는 것이 힘든 이유는 무엇일까요?

방대한 데이터를 마이그레이션하려면(예: 보조 스토리지로 이동) 상당한 시간과 컴퓨팅 리소스가 필요합니다. 게다가 한 번으로 종료되지 않습니다. 더 확실한 보호를 위해 3-2-1 백업 규칙을 따른다면 서로 다른 두 가지 스토리지 유형에, 하나 이상의 오프사이트에 백업해야 하므로 세 차례 수행하게 됩니다.

마이그레이션 과정에서 여러 요인으로 인해 전체 백업에 문제가 발생할 수 있으므로 고가용성과 페일오버가 중요합니다. 마치 주전자에서 컵에 물을 붓는 것과 비슷합니다. 한 컵에 넘치면 다른 컵에 이어서 부을 수 있습니다. 로드 밸런싱은 특정 시스템에서 요청을 처리할 수 있는지 평가하면서 워크로드를 분산합니다. 여러 서버를 클러스터링하여 고가용성을 보장하고 페일오버를 지원할 수 있습니다. 한 서버에 장애가 발생하면 다른 서버가 대신할 수 있으며, 그 어떤 것도 놓치지 않습니다.

주요 질문

- 백업 효율을 높일 수 있는 기회는 무엇입니까?
- 백업이 악성 코드에 감염되지 않고 손상되지 않은 안전한 상태인지 어떻게 알 수 있습니까?

베리타스 솔루션

베리타스 데이터 보호 솔루션은 3-2-1+1 백업 전략을 원활하게 지원하며, 기본 제공되는 침입 차단 시스템, 삭제 불가 스토리지를 위한 에어 갭 방식의 격리 복구 환경, 기본 제공되는 격리된 변조 불가 데이터 볼트로 한층 강력한 보안을 제공합니다.

Veritas InfoScale은 프로덕션 데이터의 공격 노출 범위를 줄이도록 지원하며, 프로덕션 데이터를 I/O 활동으로부터 격리하고 스냅샷 및 데이터 미러링도 수행할 수 있게 합니다. 아울러 까다로운 RTO 및 RPO도 달성할 수 있도록 복구를 최적화합니다. 자동화된 스크리핑을 사용하여 격리된 볼륨을 대상으로 악성 코드 검사를 수행하면서 악성 코드가 없음을 확인할 수 있습니다.

Veritas NetBackup Flex 및 Flex Scale은 하드웨어에서 여러 장애 지점을 제거하여 보안을 한층 더 강화하면서 각종 구성 요소를 클러스터링하여 상시 가용성을 제공합니다.

베리타스 분석 솔루션은 성공한 것으로 확인된 백업의 기준선을 정한 다음 이를 향후 백업과 비교하여 이상 요인을 찾아낼 수 있게 합니다. 애플리케이션별로 백업을 분류하여 단일 대시보드에서 모든 애플리케이션의 복원 가능 여부를 파악할 수도 있습니다.





에어 갭 및 변조 불가 데이터 볼트로 데이터 보호

백업 데이터가 암호화 시도에 취약해지지 않도록 보호하려면 어떻게 해야
합니까?

회사 차원에서 충실하게 데이터를 백업하더라도 사람의 실수나 장비 고장이
발생할 수 있습니다. 실수로 데이터가 삭제되거나 수정될 위험성이 큼니다.

따라서 데이터를 변경할 수 없는 방식으로 백업을 수행해야 합니다. 변조 불가
스토리지에 파일을 저장함으로써 손상 및 사이버 공격에 관한 우려를 덜 수
있습니다.

변조 불가 백업은 기업에 최고 수준의 데이터 보호를 제공합니다. 데이터
영구성은 변조 불가 스토리지의 핵심 요소 중 하나입니다. 즉, 파일이
우발적으로나 의도적으로 변경되지 않게 합니다. 그러면 사이버 보안 및 재해
복구 전략을 뒷받침할 보다 효율적이고 효과적인 프로세스가 마련됩니다. 그
결과, 고객이 경제적 손실과 다운타임을 방지할 수 있습니다.

에어 갭 솔루션으로 보안을 한층 더 강화하면, 변조 불가 백업 데이터가
격리된 상태에서 손상될 위험이 없습니다. 따라서 안전하게 데이터를 복원할
수 있습니다.

주요 질문

- 백업이 손상되지 않도록 어떻게 보호하고 있습니까?
- 데이터에 대한 에어 갭 및 격리를 요구하는 컴플라이언스 표준이
있습니까?

베리타스 솔루션

베리타스는 NIST 원칙에 따라 탁월한 변조 불가 모드, 가시성,
고속 복구, 삭제 불가 모드를 제공합니다. 온/오프사이트
솔루션을 위해 테이프 기반 백업, 클라우드 기반 잠금식
오브젝트 스토리지, 효율적인 데이터 스토리지(AWS S3
Object Lock) 등 다양한 방식을 지원합니다.

베리타스 데이터 보호 솔루션은 불필요한 리소스 액세스 동작을
사전에, 운영 체제보다 먼저 차단합니다.

Veritas Flex는 변조 불가 데이터 볼트로 격리된 복구
환경(IRE)을 구현할 수 있게 합니다. 그러면 격리된 변조 불가
환경으로부터 중요 백업 데이터의 안전한 카피본을 확보할
수 있습니다. 이 IRE 아키텍처가 중요한 백업을 보호할 뿐만
아니라, 안전한 복구를 위한 오케스트레이션 또는 사이버
레질리언스 복구 계획의 리허설에 사용 가능한 안전한 공간도
마련합니다. 인프라스트럭처에 독립적인 베리타스의 가상 에어
갭(Air Gap) 기술이 한층 더 강력한 보호 및 격리 기능으로
각종 공격을 차단합니다.





재해 복구 프로세스 정의

이상적인 복구 솔루션이라면 모든 워크로드를 지원해야 합니다.

손쉬운 통합을 지원하고 기대에 부합하는 RPO 및 RTO를 달성하며 모든 스토리지를 지원하고 단일 통합 대시보드에서 모든 보호 항목을 관리할 수 있는 프로세스를 생성해야 합니다. 이러한 프로세스를 정의할 때 다음과 같은 요인도 고려해야 합니다.

- 오케스트레이션 기반 복구(복구 순서 결정)
- 지능형 중복 제거
- 스냅샷 통합
- 스토리지 계층화
- 온프레미스 및 클라우드 스토리지에 이미지, 카탈로그, 스냅샷 자동 복제
- 컨테이너 지원
- 데이터 인사이트 및 분석
- 온프레미스 및 유연한 클라우드를 위한 보안/컴플라이언스
- 암호화로 데이터 및 백업 시스템 보호

제로 트러스트, 다계층 데이터 보안, 지능형 자동화를 활용하면서 비즈니스 운영의 레질리언스를 보장할 수 있습니다. 멀티 클라우드 인텔리전스를 활용하고 사이버 방어 체계를 업그레이드하는 동시에 비용을 절감하고 통합 솔루션을 활용합니다. 클라우드 기반 워크로드에 대한 백업 및 복구를 통합하고 워크로드 마이그레이션을 자동화하며 클릭 한 번으로 복구, 맞춤형 스크립팅, 리허설까지 해결하는 편리한 재해 복구 기능을 구현함으로써 비용을 최소화하고 갈수록 진화하는 규정도 준수합니다.

주요 질문

- 복구하는 데 소요되는 시간이 어느 정도입니까?
- 복구 우선 순위는 어떻게 됩니까?

베리타스 솔루션

베어 메탈 복구를 선택하거나 일부 파일만 영향을 받았다면 개별 단위 파일 복구를 선택할 수 있습니다. VM에 대한 즉각적인 롤백도 제공하므로 수백 개의 VM을 수분 내로 복구하고 동시에 롤백할 수 있습니다.

향상된 데이터 레질리언스 기능과 Veritas Resiliency Platform을 통해 애플리케이션 간에 서로 다른 복구 우선 순위를 지정하고 비즈니스 중요도에 따라 순차적으로 멀티 티어 애플리케이션을 복구할 수 있습니다. 상시 데이터 보호 체크포인트로 RPO가 짧은 복구도 지원합니다.

Veritas NetBackup Flex와 Flex Scale은 하드닝된 운영 체제, 제로 트러스트 아키텍처, 번조/삭제 불가 스토리지로 구성됩니다. IRE와 번조 불가 데이터 볼트를 통해 격리된 에어 갭(Air Gap) 솔루션을 제공하며, 이는 외부에서 검색되지 않습니다. 악성 코드 및 이상 검사 기능으로 백업 데이터의 안전성을 확인할 수 있습니다. 즉, 온사이트 및 클라우드의 모든 환경에서 즉각적인 복구가 가능합니다.





레질리언스 리허설

리허설의 목적은 복원이 아니라 다운타임을 방지하는 데 있습니다.

사이버 범죄자는 표적으로 삼은 기업이 복구에 최적화되어 있지 않길 바랍니다. 이들은 해당 기업이 몸값을 지불하도록 피해와 다운타임을 극대화하려 합니다. 반면, 철저히 복구를 준비하고 리허설을 마친 기업은 훨씬 유리한 위치를 확보한 셈입니다. 신속한 복구를 위해서는 전체 환경에 대한 사이버 보안 대응 계획이 필요하며, 여기에는 조기에 자주 테스트하는 것도 포함됩니다. 정기적인 리허설 및 복구 훈련을 통해 다운타임을 단축하고 혼란을 최소화하며 공격이 미치는 영향을 줄일 수 있습니다.

하이브리드 및 멀티 클라우드 시스템의 수요가 증가하므로, 여러 프레임워크를 관리하는 것은 물론 여러 클라우드 및 스토리지 시스템을 조정하는 기능이 필요합니다. 팀마다 여러 서버와 애플리케이션을 관리하고 확장해야 합니다.

자동화를 활용하여 환경의 복잡성을 해소하고 잠재적 위협을 파악하며 선제적으로 리허설을 관리함으로써 상시 대비 태세를 유지하고 다운타임을 최소화할 수 있습니다.

주요 질문

- 다운타임을 줄이려면 어떻게 해야 하나요?
- 보다 빠르게 문제를 해결하려면 어떻게 해야 하나요?

베리타스 솔루션

Veritas NetBackup Flex와 Flex Scale은 손쉽게 확장할 수 있는 아키텍처를 통해 데이터 보호 가능성을 극대화합니다. 변조 불가 모드, 자동 프로비저닝, 로드 밸런싱의 다층적 접근 방식으로 완벽한 통합 데이터 보호 솔루션을 구축할 수 있습니다.

Veritas InfoScale 및 Veritas Alta™ Application Resiliency는 해당 환경이 정상적으로 작동할 뿐만 아니라 최적의 상태로 작동하도록 지원합니다. 주요 비즈니스 애플리케이션과의 긴밀한 통합을 통해 가동 시간 및 페일오버를 극대화함으로써 최고 수준의 가용성 및 재해 복구 기능을 제공하는 통합 인프라스트럭처 솔루션입니다. 이러한 통합 플랫폼에서 업계 요구 사항에 따라 다음과 같은 기능으로 보호 수준을 유연하게 조정할 수 있습니다.

- 데이터 무결성 준수
- 수작업을 최소화하기 위해 자동화된 멀티 티어 애플리케이션 런북
- 워크로드가 여러 플랫폼 간에 원활하게 이동할 수 있는 이동성
- 기존 시스템 및 환경과의 원활한 통합





백업 및 복구 최적화

전사적 범위에서 데이터 보호를 관리해야 하는 부담을 덜어줍니다.

병목 지점을 찾아내고 가장 시간이 많이 걸리는 프로세스가 어디에 있는지 알아내려면 데이터 오케스트레이션이 수행되어야 합니다. 오케스트레이션으로 서버 프로비저닝, 데이터베이스 관리, 애플리케이션을 비롯한 여러 프로세스를 자동화하여 시간을 절약할 수 있습니다. 이를 통해 취약점 검사, 로그 검색, 보안 톨 연결 등의 작업을 처리하고 시스템을 통합하여 각 팀에서 과도한 업무에 시달리지 않게 할 수 있습니다.

올바른 솔루션을 선택하면 더 수월하게 데이터를 관리할 수 있으나, 이는 계속 풀어야 할 숙제입니다.

올바른 분석을 활용하여 해당 환경의 필수 요소에 관한 가시성 확보할 수 있습니다. 보다 면밀한 분석을 통해 가동률이 저조하거나 구성이 잘못되었거나 인덱싱되지 않은 항목도 찾아낼 수 있습니다. 이는 IT 팀에서 문제를 해결하고 용도 변경 가능한 리소스를 파악하여 비용을 절감하는 데 도움이 됩니다.

실행 가능한 인사이트를 발굴하여 가동률, 성능, 레질리언스를 향상할 뿐만 아니라 장애를 예측하고 SLA 관련 리스크를 완화하기 위한 선제적 권장 조치를 마련합니다.

지능형 자동화로 수동 프로세스로 인한 비효율성을 해소하고 무궁무진한 가능성을 모색할 수 있습니다.

민첩하면서도 안전한 백업 및 복구 기능을 구현하고 구축함으로써 완전한 데이터 보호 및 최적화를 수행할 수 있습니다.

리소스를 효율화하고 비용을 줄이고 단일 통합 콘솔의 뷰에서 엣지, 코어, 클라우드 등 네트워크 전반을 모니터링합니다.

베리타스 솔루션

Veritas Data Insight를 통해 각종 활동을 분석하고 사용량 및 협업까지 면밀하게 살펴볼 수 있습니다. 이는 사용자를 분류하고 활동 패턴을 보다 잘 파악하는 데 도움이 됩니다. 중복되거나 오래되었거나 불필요한 데이터를 식별합니다. 또한 리스크 점수를 활용하여 잠재적 위협을 평가하고 고위험 데이터의 우선 순위를 지정합니다. 베리타스 컴플라이언스 솔루션과 연계하여 세부적인 감사 추적을 생성하고 통합 파일 분석, 데이터 유출 방지, 아카이빙 기능도 활용할 수 있습니다.

베리타스 분석 솔루션으로 위험한 상태의 애플리케이션과 서비스를 신속하게 찾아낼 수 있습니다. 모든 환경에서 백업을 모니터링 및 최적화하고 위치, 환경, 애플리케이션별로 영향을 받는 호스트를 효율적으로 찾아내면서 더 신속하게 복구합니다.

주요 질문

- 신속하게 복구할 수 있도록 데이터가 최적화되었습니까?
- SLA를 잘 알고 있습니까?





빈틈없는 사이버 레질리언스 전략을 구현하십시오. >

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 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](https://twitter.com/veritastechllc))에서 확인하실 수 있습니다.

VERITAS™

서울시 송파구 올림픽로 300
롯데월드타워 35층
Tel: (82)-2-3703-7622
www.veritas.com/ko/kr