VERITAS

랜섬웨어 레질리언스 구현을 위한 Veritas Enterprise Data Services Platform

베리타스 백서 | 2020년 11월

목차

개요

기업의 규모나 유형에 관계없이 랜섬웨어는 현재 모든 기업의 최대 관심사입니다. 실제로 2021년에는 랜섬웨어 공격이 11초에 한 번꼴로 기업을 공격할 것으로 예측되면서, 랜섬웨어는 현재 가장 무서운 속도로 증가하는 사이버 범죄 유형으로 볼 수 있습니다. 공격자는 최강의 프론트라인 보안까지 무너뜨릴 수 있도록 교묘하고 지능적인 기술을 고안하는 중입니다. 여전히 피싱과 같은 오래된 수법도 사용되지만, 사회 공학을 접목하고 IoT 디바이스 및 인프라스트럭처 취약점을 노리는 새롭고 지능적인 공격 방식이 확산되고 있습니다. 이러한 상황을 감안할 때 IT 팀은 엔드포인트 보안만으로는 진정한 랜섬웨어 레질리언스를 실현할 수 없다는 사실을 인식해야 합니다.

많은 기업이 데이터 백업 및 복구를 랜섬웨어 공격에 대한 마지막 방어 수단으로 간주하고 있습니다. 베리타스는 통합적인 멀티레이어 사이버 보안 전략의 차원에서 효용성과 안정성을 모두 갖춘 데이터 백업 및 복구를 우선 순위에 둘 것을 조언합니다. 데이터 서비스가 중단되면 비즈니스도 멈추게 됩니다.

Veritas Enterprise Data Services Platform 솔루션은 레질리언스를 염두에 두고 개발된 만큼, 중단 없는 비즈니스를 보장하고 만일의 피해를 최소화하면서 고객의 신뢰를 받을 수 있습니다. 베리타스 솔루션은 고객의 요구 사항에 부합하는 다양한 보안 제어 기능으로 IT 시스템 및 데이터 무결성을 **보호**합니다. 이러한 툴은 사용자 활동 및 데이터 인프라스트럭처에 대한 완전한 가시성을 바탕으로 각종 위협 요소를 모니터링하고 **탐지**할 뿐만 아니라 백업 모니터링 기능을 통해 중요 데이터의 안전을 보장합니다. 베리타스와 Veritas NetBackup™ 소프트웨어는 수십 년간 레질리언스의 대명사로 간주되었습니다. 이렇듯 고객이 신뢰하는 베리타스 솔루션은 검증된 기술을 사용하므로, 규모에 관계없이 자동화 및 오케스트레이션 기능을 활용하여 빠르게 **복구**할 수 있습니다.

서론

본 백서는 통합, 컴플라이언스, 보안의 삼박자를 갖춘 업계 최고의 랜섬웨어 레질리언스 플랫폼으로 손꼽히는 Veritas Enterprise Data Services Platform 솔루션을 집중 조명합니다. 베리타스 툴을 선택한 고객은 확신을 가지고 리스크를 줄이는 데 주력하면서 랜섬웨어와 같은 현재와 미래의 보안 위협으로부터 데이터를 보호하고 성공적으로 복구할 수 있습니다. 이 문서는 비즈니스 및 기술 분야의 관계자를 위해 마련된 것으로, 여기에는 악성 코드를 차단하고 공격이 발생하더라도 데이터를 효과적으로 복구할 수 있도록 NetBackup을 비롯한 Veritas Enterprise Data Services Platform 솔루션에 관해 자세히 알아보려는 고객, 파트너, 기타 관계자가 포함됩니다.

본 백서는 아래와 같은 용도로 활용할 수 있습니다.

- IT 시스템을 **보호**하고 데이터 무결성을 유지할 방법 모색
- 위협 요소를 모니터링하고 최소화하면서 시스템의 이상 요소를 **탐지**할 수 있게 해주는 베리타스 솔루션 이해
- 해당 환경에 최적화된 복구가 이루어질 수 있도록 고객의 니즈에 가장 부합하는 **복구** 옵션 확인

물론 하나의 솔루션으로 모두 해결하는 만능 솔루션은 존재할 수 없으며, 본 백서에서 모든 내용을 다루지는 않습니다. 베리타스 고객은 다양한 솔루션 중에서 각 애플리케이션의 구체적인 복구 니즈에 가장 적합한 솔루션을 자유롭게 선택할 수 있습니다. 각 기업은 거시적이고 통합적인 관점을 방어 전략에 접목하여 방화벽, 이메일/스팸 필터, 악성 코드 차단 소프트웨어, 포인트 보호 소프트웨어를 추가해야 합니다. 지능적이고 교묘한 위협 요소와 그 기술에 뒤처지지 않도록 새로운 전략을 수립하고, 리허설을 통해 끊임없이 평가해야 합니다. 이제 기업의 백업 에코시스템을 한층 강화하기 위해 베리타스가 제안하는 베스트 프랙티스를 자세히 살펴보겠습니다.

그림 1. 기업의 백업 에코시스템을 위한 권장 베스트 프랙티스

베스트 프랙티스

미국 국립 표준 기술 연구소(National Institute of Standards and Technology, NIST)가 개발하고 제안한 사이버 보안 프레임워크를 활용하여 5대 핵심 기능, 즉 식별, 보호, 탐지, 대응, 복구를 중심으로 한 체계적인 통합 방법론을 마련할 수 있습니다. 베리타스도 이 방식을 수용하여 통합적인 NIST 프레임워크에 따라 베리타스 솔루션을 구현하는 것을 권장합니다.

기업의 백업 에코시스템에 대해서는 그림 1에 정리된 주요 베스트 프랙티스를 제안합니다.

- 버전 관리
  - 보안 업데이트가 포함된 최신 보안 패치 및 릴리스를 상시 적용하여 취약점으로 인한 리스크 최소화
  - 베리타스 지원 웹사이트 또는 Veritas Services and Operations Readiness Tools(SORT)를 활용하여 베리타스 기술 알림 모니터링
- ID 및 액세스 관리
  - 사용자가 반드시 각자의 인증 정보로 로그인하도록 규정
  - 역할 기반 액세스 제어(RBAC) 및 2단계 인증 구현: 각 사용자 유형에 필요한 기능으로 액세스 범위 제한, 단일 인증 정보 사용으로 인한 계정 도용 방지
  - 기본 제공된 일반 사용자 ID 및 암호(호스트 'admin', 'maintenance', RMM 'sysadmin', 'nbasecadmin' 계정 포함) 변경
- 변조 불가능한 스토리지(Immutable Storage)
  - 변조 불가능한 스토리지 기술로 백업을 암호화하거나 삭제하는 랜섬웨어 차단
- 데이터 암호화
  - 전송 시 암호화 기능을 구현하여 네트워크 내 데이터 유출 방지
  - 저장 시 암호화 기능을 구현하여 랜섬웨어 또는 기타 공격자의 데이터 유출 시도, 데이터 공개 위협, 기타 악의적 활동 차단
- 구성
  - 보안 구현 지침 준수
  - 방화벽을 활성화하여 포트 및 프로세스를 제한하는 방법으로 더 안전한 환경 구현
  - 기본 마스터 카탈로그 백업 정책 업데이트
  - NetBackup Key Management Server(KMS)를 위한 백업 정책 설정

- 구축
  - 미국 사이버 보안 및 인프라스트럭처 보안국(CISA)이 권장하는 "3-2-1" 데이터 백업 베스트 프랙티스 적용: 3개의 카피 데이터를 생성하여 2개는 서로 다른 미디어 유형에, 나머지 1개는 오프사이트에 보관
  - AIR(Auto Image Replication) 기술을 활용하여 다른 도메인에 복제

전략을 마련했으면 정기적인 테스트 및 리허설이 뒤따라야 합니다. 이러한 베스트 프랙티스를 통해 위협에 대응하는 시간을 단축하고 공격의 영향을 최소화할 뿐만 아니라 더 우수한 가시성을 확보하여 문제 영역을 찾아 해결하고 개선할 수 있습니다. 레질리언스 계획의 효용성은 최신 테스트에 좌우되므로, 주기적인 리허설을 통해 레질리언스 전략을 지속적으로 보완하는 것이 좋습니다.

보호, 탐지, 복구

베리타스는 고객의 고유한 니즈 및 요구 사항에 따라 커스터마이즈 가능한 여러 제품 기능 및 기술을 제공하면서 고객이 각종 공격을 차단, 탐지하고 사후 복구하도록 지원합니다. 베리타스 랜섬웨어 레질리언스 전략을 구성하는 3대 핵심 영역을 자세히 살펴보겠습니다.

보호

가장 중요한 자산인 데이터와 IT 인프라스트럭처를 예기치 않은 미지의 위험으로부터 보호하는 것이 일차 방어선이라면, 백업 인프라스트럭처와 백업 데이터는 공격 이후의 복구를 책임지는 마지막 방어선이라 할 수 있습니다. 복구의 성패를 좌우하는 것은 바로 백업입니다. NetBackup은 800여 종의 데이터 소스, 1,400개 이상의 스토리지 타깃, 60여 개의 클라우드 제공업체를 포함하여 엣지부터 코어 시스템 및 클라우드까지 포괄하는 가장 광범위한 지원을 제공합니다. 따라서 고객의 환경은 항상 안전하게 보호되며 언제나 복구 가능합니다.

뿐만 아니라 지능형 정책을 통해 Oracle 및 VMware 인스턴스를 자동으로 탐지하고 백업하면서 필요한 수준의 보호를 적용할 수 있습니다.

베리타스는 데이터 무결성에 중점을 두고 백업 파일을 안전한 상태로 유지하면서 악의적 의도를 가진 내부자의 접근을 차단합니다. 고객이 효과적으로 데이터를 보호하는 것이 무엇보다 중요한 만큼, 베리타스는 NetBackup을 포함하여 데이터 무결성을 위한 주요 기능을 Enterprise Data Services Platform의 핵심 요소로 삼았습니다.

또한 다양한 보안 제어 기능을 통해 데이터 보호를 지원하고 데이터 무결성을 유지합니다.

- **ID 및 액세스 관리(IAM)**
  - 역할 기반 액세스 — 사용자 유형별 니즈에 따라 맞춤 구성이 가능한 개별 단위 액세스 제어를 통해 누가 데이터에 액세스할 수 있는지 지정하고, 어떤 작업을 수행하거나 수행할 수 없는지 정의합니다(그림 2 참조).
  - SSO(Single Sign-On) — Active Directory 및 LDAP를 포함하여 SAML 2.0도 지원합니다. 각 기업은 인증 제공업체를 활용하여 2단계 인증을 구현할 수 있습니다.
  - 커스터마이즈 가능한 인증 — Veritas Flex Appliance는 인증 강도를 구성할 수 있도록 지원합니다.

그림 2. NetBackup의 액세스 권한 대시보드

- **데이터 암호화**
  - 전송 시 암호화 — 데이터가 인증된 환경으로 전송되고, 전송 중에도 데이터가 확실하게 보호됨을 보장합니다. 이 솔루션은 베리타스 또는 고객이 제공한 TLS 1.2 인증서를 활용하고 2048비트 키를 지원하면서 데이터가 반드시 암호화된 상태로 전송되게 합니다.
  - 저장 시 암호화 — 해커가 데이터에 접근하는 데 성공하더라도 데이터가 암호화된 상태이므로 익스플로잇이 불가능합니다. 베리타스는 AES 256비트 FIPS 140-2 암호화 및 자체 키 관리 기능을 제공할 뿐만 아니라 KMIP(Key Management Interoperability Protocol)를 통해 고객이 선호하는 키 관리 기술을 활용하도록 지원합니다.

- **변조 불가능한 이미지 관리 및 스토리지**
  - 스토리지에 구애받지 않는 이미지 관리
    - NetBackup에는 OST(OpenStorage Technology) API가 포함되어 베리타스 또는 타사 스토리지 솔루션의 불변형 백업 이미지를 관리할 수 있습니다.
    - 1차, 2차(복제), 크로스 도메인 복제(AIR 사용)를 지원하므로 모든 백업 스토리지 계층에서 제한 없는 구성 옵션을 사용할 수 있습니다.
  - 이미지 스토리지
    - NetBackup Flex 운영 환경에서 변조 불가능한 스토리지를 제공하므로 악성 코드나 랜섬웨어가 백업 데이터를 암호화하거나 삭제하여 사용할 수 없게 만들까 염려하지 않아도 됩니다.
    - NetBackup Flex에 포함된 WORM 스토리지 서버에서 안전한 컨테이너 기반 MSDP 솔루션을 제공합니다.
    - NetBackup Flex는 엔터프라이즈 및 컴플라이언스 잠금 모드를 제공하므로, 보존 기간 중 삭제 가능 여부를 필요에 맞게 선택할 수 있습니다(그림 3 참조).
    - NetBackup Flex는 불변형 제어 기능을 평가하는 공신력 있는 Cohasset Associates의 타사 불변형 심사를 통과했습니다. 특히 SEC Rule 17a-4(f), FINRA Rule 4511(c), CFTC(Commodity Futures Trading Commission) 원칙(17 CFR § 1.31(c)-(d))을 준수합니다.
    - Cohasset Associates의 NetBackup 평가 결과는 https://www.veritas.com/ko/kr/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup에서 확인할 수 있습니다.

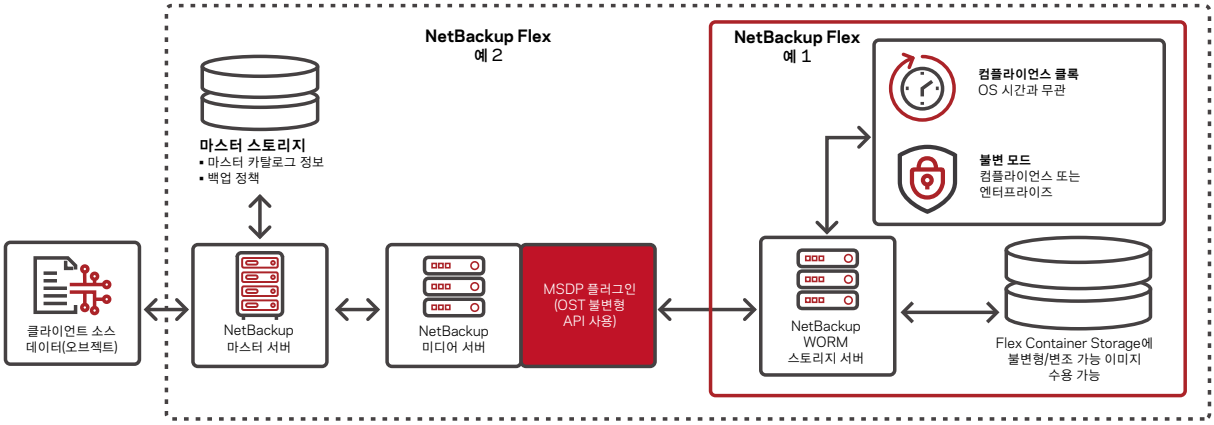


그림 3. 다양한 NetBackup Flex 구축 사례 중 2가지

- **솔루션 하드닝**

  NetBackup Flex는 소프트웨어 및 하드웨어 차원의 하드닝을 거쳐 변조 불가능한 스토리지를 제공하는 완벽한 보안 솔루션입니다. 이 솔루션은 안전한 WORM 스토리지 서버 및 하드웨어 보안 기능을 제공합니다.

  - 베리타스는 개발 주기 내내 아래와 같은 기능을 갖춘 검증된 타사 탐지 툴을 사용하여 NetBackup Flex 코드를 분석하면서 취약점이 있는지 확인합니다.
    - 정적 코드 분석
    - 런타임 취약점 검사
    - 침투 테스트
  - NetBackup Flex는 아래와 같은 다양한 보안 기능을 제공합니다.
    - OS 보안 하드닝: SELinux(Security-Enhanced Linux) 포함
    - 침입 탐지 시스템(IDS)/침입 차단 시스템(IPS)
    - 강력한 역할 기반 인증
    - 락다운(Lock down) 스토리지 어레이
    - 안전하고 견고하며 하드닝된 Veritas File System
  - 자세한 내용은 보안 구축에 관한 Veritas Flex Appliances with NetBackup Security 백서 및 Veritas Flex Appliances with NetBackup 백서를 참조하십시오.

탐지

많은 기업이 한정된 리소스로 갈수록 복잡해지는 IT 환경을 관리해야 하는 상황입니다. 기업은 랜섬웨어와 같은 보안 위협에 대처하면서 환경을 안전하게 보호하는 동시에 백업 및 스토리지 구성에 대한 일상적인 유지 보수 및 모니터링 작업을 간소화하려 합니다. 베리타스는 백업 인프라스트럭처를 인식하고 악성 코드 및 이상 요소를 탐지하는 솔루션을 제공합니다.

백업 및 스토리지 인프라스트럭처 인식

APTARE™ IT Analytics를 통해 모든 중요 데이터를 백업하는지 확인합니다. APTARE를 아래와 같이 활용할 수 있습니다.

- 인프라스트럭처에 포함된 모든 호스트 또는 가상 머신을 검색하고 NetBackup이 보호하는 가상 머신과 비교합니다.
- 백업에 누락된 호스트가 있으면 잠재적 리스크 플래그를 지정합니다.

APTARE는 다음을 포괄하는 통합 백업 모니터링 기능을 제공합니다.

- 리스크 완화 분석(그림 4 참조)
- 연속적으로 오류가 발생한 소스
- 최신 백업이 없는 소스
- 애플리케이션별 백업 실패 횟수

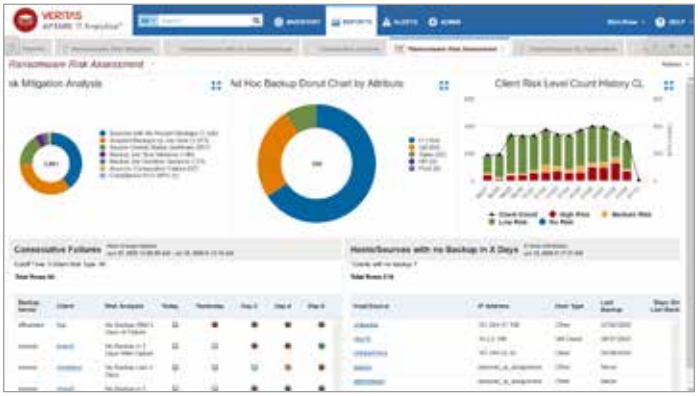


그림 4. APTARE의 랜섬웨어 리스크 평가 대시보드

APTARE는 성공한 백업을 조사하고 오탐지 가능성을 파악합니다. 이를 위해 과거의 백업과 새로운 백업을 비교하여 작업 소요 시간의 큰 편차, 이미지 크기 변화, 정책 구성 변경 등의 비정상적인 요소를 찾아냅니다.

자세한 내용은 랜섬웨어 레질리언스 강화: APTARE IT Analytics로 인프라스트럭처에 대한 완전한 가시성 확보를 참조하십시오.

악성 코드 및 이상 요소 탐지

Veritas Data Insight는 비정상적인 행위를 탐지하고, 커스터마이즈 가능한 랜섬웨어 전용 쿼리 템플릿을 제공하며, 파일 확장자를 식별하여 랜섬웨어 탐지를 지원하면서 기존 보안 탐지 툴을 보완합니다. Data Insight에 포함된 정책 기반 모니터링 및 알림 기능은 거의 실시간으로 작동하면서 사용자 계정에서 발생하는 악의적이거나 비정상적인 행위를 탐지할 수 있게 합니다. 이를 위해 모니터링 대상인 비정형 데이터 시스템을 검사하고, 모든 파일에서 수행된 모든 사용자 활동(읽기, 쓰기, 생성, 삭제, 이름 변경 등)에 대한 감사를 수집하며, 사용자별로 보안 및 파일 계수 작업도 수행합니다(그림 5 참조).

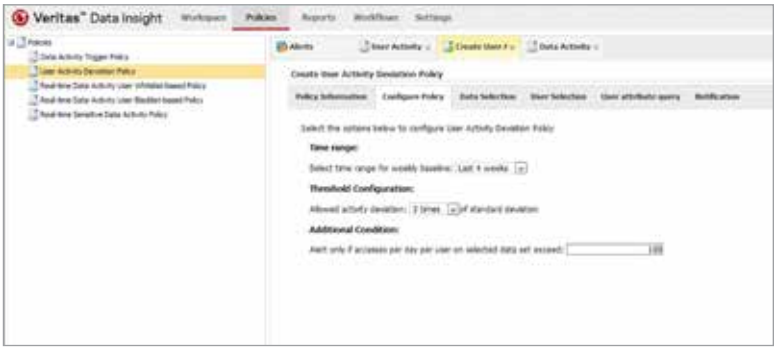


그림 5. Data Insight에 사용자 활동 탐지 정책 설정

이 기술은 지금까지 수집한 이력 데이터를 비교하고 통계적 표준 편차를 찾아내 비정상적인 행위 탐지를 지원할 뿐만 아니라 랜섬웨어 감염이 의심되는 계정을 파악합니다. Data Insight는 악성 사용자 계정 또는 랜섬웨어 관련 활동을 탐지하고 잠재적 랜섬웨어 파일의 위치도 알아낼 수 있습니다.

Data Insight에 대한 자세한 내용은 Veritas Data Insight를 통한 랜섬웨어 조기 탐지를 확인하십시오.

복구

Veritas Enterprise Data Services Platform은 신속한 복구에 필요한 유연성을 보장하는 다양한 솔루션을 활용하여 실제로 운용 가능한 비즈니스 레질리언스 전략을 마련합니다. 지금까지 기업은 백업 및 복구를 마지막 방어선으로 간주했으나, 베리타스 솔루션은 규모에 관계없이 모든 기업에서 통합 전략의 핵심 구성 요소로 복구를 포함합니다. 베리타스는 그림 6과 같이 복잡한 환경에서도 성공적으로 복구할 수 있는 솔루션을 제공합니다.

규모에 따른 복구 복잡성

이기종 환경 지원

혼합 시스템 환경(가상/물리적)

온프레미스, 하이브리드, 멀티 클라우드의 수많은 데이터 센터

복잡한 네트워크 및 스토리지 관리

종속 관계

다중 구성 요소 계층형 애플리케이션

여러 데이터 센터(온프레미스, 클라우드)에 분산된 인프라스트럭처

그림 6. 규모에 따른 복구 복잡성을 해결하는 베리타스 솔루션

NetBackup Resiliency

NetBackup Resiliency는 이기종 환경 전반을 자동으로 오케스트레이션하면서 일관성 있는 사용자 경험을 제공하고, 해당 기업의 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 따라 최상의 복구 옵션을 제안하는 방식으로 복구 관련 과제를 해결합니다(그림 7 참조).

NetBackup Resiliency는 가장 효율적인 RTO를 달성하고자 고객의 데이터 센터 전 범위에서 RTO, 워크로드, 애플리케이션을 파악하여 최상의 복구 방법을 결정합니다.

NetBackup Resiliency는 워크로드, 애플리케이션, 관련 데이터까지 포괄하는 이기종 환경의 전 범위에 대한 오케스트레이션을 지원합니다. NetBackup의 자동화된 복제, 스토리지 기반 복제 또는 Resiliency의 기본 제공 데이터 무버를 활용하여 해당 애플리케이션의 요구 사항에 부합하는 RTO 및 RPO를 선택할 수 있습니다.

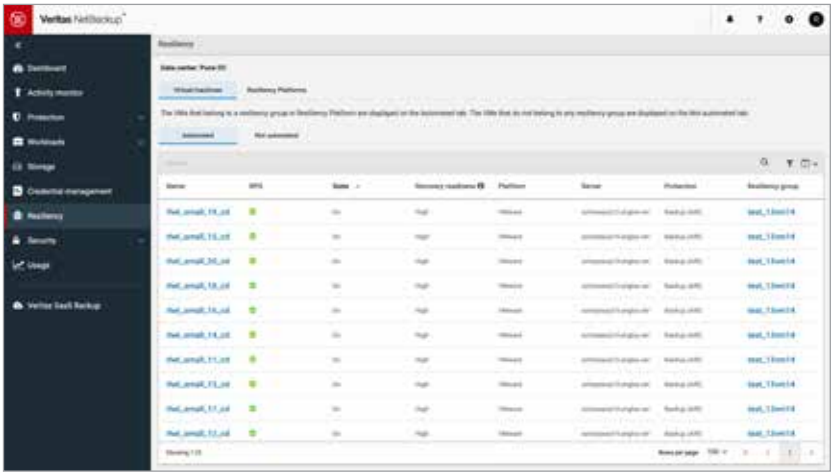


그림 7. NetBackup의 레질리언스 대시보드

구체적으로 이 솔루션은 멀티레이어 애플리케이션을 위한 재해 복구 보호 솔루션인 VBS(Virtual Business Services)와 런북 역할을 담당하는 레질리언스/대피 계획(Resiliency and Evacuation Plans)을 활용하여 규모에 상관없이 데이터 센터 간 복구 또는 클라우드 인프라스트럭처에 대한 복구를 자동화합니다.

격리된 네트워크에서 푸시 버튼 방식의 리허설을 통해 검증하는 것도 가능합니다. 기업의 랜섬웨어 복구 시나리오에서는 프로덕션 모드로 복귀하기에 앞서 커스터마이즈된 스크립트를 사용하여 워크플로우에 포함된 타사 바이러스 검사 솔루션과 통합하는 방식으로 악성 코드 검증을 진행할 수 있습니다.

RPO 관점에서 보면 NetBackup의 CDP(Continuous Data Protection)를 통해 레질리언스를 한층 더 강화할 수 있습니다. 제로에 가까운 RPO에서 VMware 가상 머신(VM)에 대한 개별 단위 복구가 가능하기 때문입니다. CDP는 Resiliency의 실시간에 가까운 데이터 복제 작업에 개별 단위 복구 지점을 사용하여 이기종 환경 어디서든 애플리케이션을 위한 복구 기능을 보장합니다(그림 8 참조). 이 기능으로 복제가 수행된 경우에는 악성 코드에 감염되거나 손상되더라도 복구할 수 있습니다.

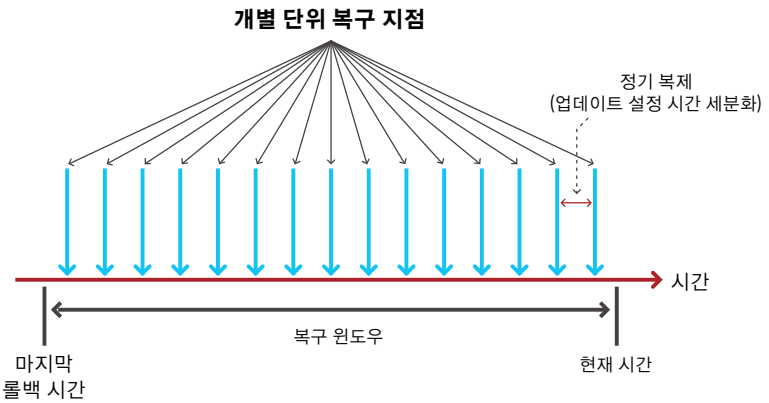
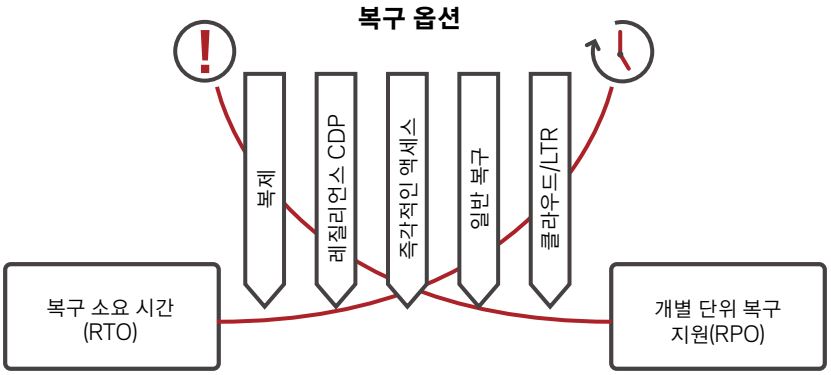


그림 8. NetBackup의 CDP(지속적인 데이터 보호) 방식 개요

NetBackup이 지원하는 또 다른 복구 방법

베리타스는 그 밖의 다양한 복구 방식으로 고객의 RTO 및 RPO를 충족하므로, 고객은 자유롭게 해당 기업에 가장 적합한 복구 방식을 선택할 수 있습니다. 그림 9는 RPO 및 RTO를 기반으로 하는 최적의 복구 옵션을 보여줍니다.



RTO 및 RPO 목표에 따라 최적의 옵션 결정

그림 9. RTO 및 RPO에 따라 최적의 복구 옵션 선택

VM 복구 — VMware 가상 머신(VM) 백업 1개로 전체 가상 머신, 개별 VMDK, 파일/폴더, 전체 애플리케이션, 즉각적인 액세스, 파일 다운로드, 애플리케이션 GRT, AMI 변환의 8가지 복구 유형을 시도할 수 있습니다. 그밖에 vTPM도 지원하면서 고도의 보안이 필요한 환경에 대한 백업 및 복구를 보장합니다.

즉각적인 액세스 — Instant Access for VMware를 통해 백업에서 가상 머신 데이터를 가져올 때까지 기다릴 필요 없이 원하는 모든 시스템을 즉시 복구할 수 있습니다. 백업 스토리지에서 직접 백업을 사용하여 가상 머신을 테스트하거나 복구할 수도 있습니다. 이러한 가상 머신은 VMware 인프라스트럭처의 정규 게스트로 자동 표시됩니다. 또한 웹 UI에서 개별 파일을 탐색하고 복구할 수도 있습니다. 빠른 복구가 절실한 시나리오에서는 VMware Storage vMotion을 활용하여 백업 스토리지의 가상 머신을(사용 중에도) 프로덕션으로 마이그레이션할 수 있습니다.

보호 대상 VMware 가상 머신에
사용 가능한 복구 지점 탐색

복구할 파일 또는 폴더 선택

다운로드할 파일 또는 폴더 목록 확인

NetBackup Instant Access에서 파일을
패키지로 추출하기 위해 백업 이미지 마운트

패키징된 파일 또는 폴더는 다운로드 가능한 상태

그림 10. VMware Instant Access로 인프라 전 범위의 가상 머신 백업

전체 구성 및 자세한 정보는 Veritas NetBackup for VMware 관리자 설명서를 확인하십시오.

같은 기술을 사용하는 Instant Access for MSSQL의 경우 백업 스토리지를 활용하여 데이터베이스를 즉시 사용 가능하게 하고 데이터베이스 요소에 대한 개별 단위 복구를 수행합니다(그림 11 참조). Instant Access for VMware와 마찬가지로 개발/테스트 리소스를 빠르고 쉽게 복구하도록 지원합니다. 이러한 리소스는 사용자가 또는 사용자를 위해 온디맨드 방식으로 프로비저닝한 후 나중에 클릭 한 번으로 손쉽게 정리할 수 있습니다(그림 12참조).

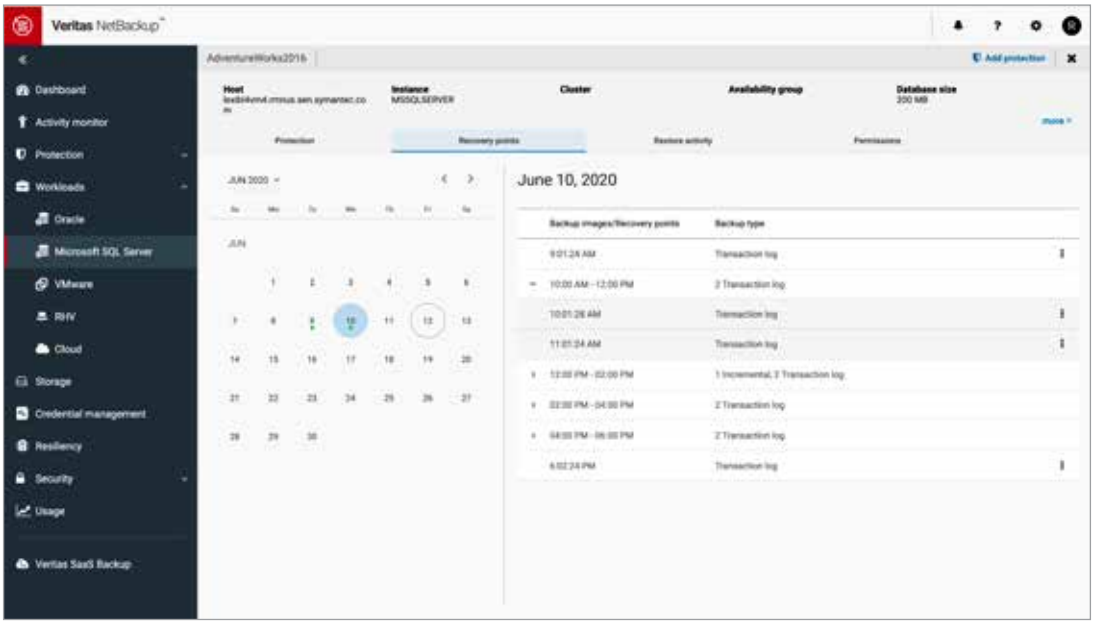


그림 11. VMware Instant Access로 인프라스트럭처 전 범위의 가상 머신 백업

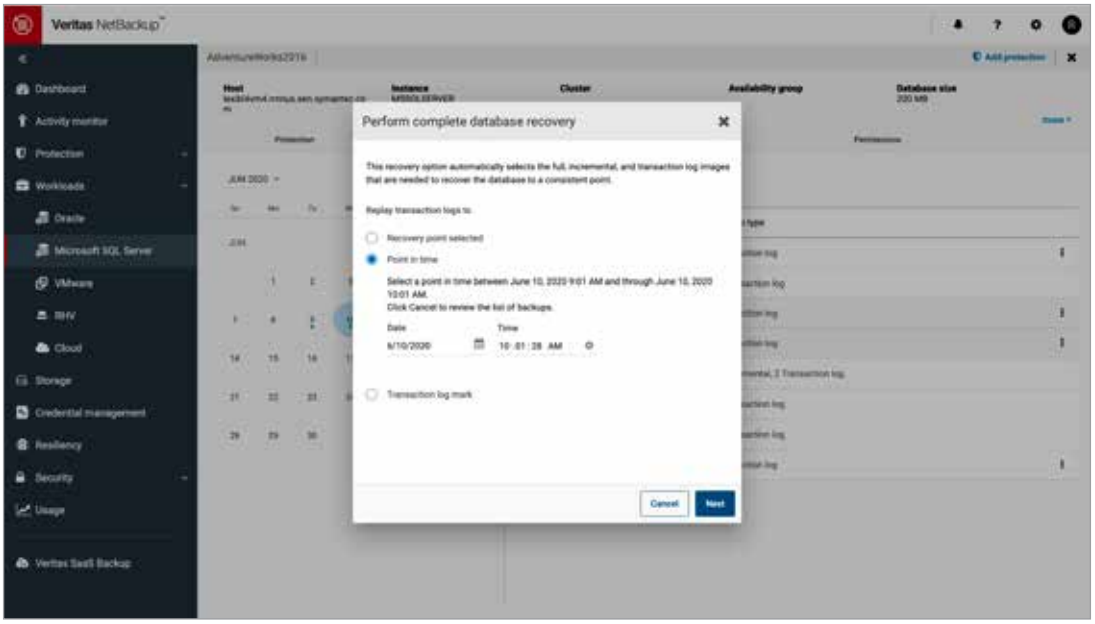


그림 12. Instant Access for MYSSQL로 전체 데이터베이스 복구 수행

NetBackup CloudPoint — 컨테이너 기술 및 클라우드 서비스 제공업체를 활용합니다. CloudPoint는 스토리지 플랫폼에 관계없이 클라우드 벤더에 구애받지 않고 클라우드 네이티브 스냅샷 기술을 사용하면서 하이브리드 및 멀티 클라우드 인프라스트럭처를 손쉽게 보호할 수 있게 지원합니다. 뿐만 아니라 CloudPoint는 퍼블릭 클라우드에서 기초적인 기능을 제공하는 데 머무르지 않고 애플리케이션 인식 스냅샷, 단일 파일 복구, 다중 영역 스냅샷 마이그레이션도 지원합니다. CloudPoint는 다중 계정을 지원하여 백업을 다른 계정에 안전하게 저장하므로 일부 계정이 감염되더라도 피해를 최소화할 수 있습니다.

Universal Share — 이 MSDP 기능은 NetBackup 서버에서 중복 제거 기반 스토리지를 보안 공유 형태로 프로비저닝함으로써 에이전트 또는 백업 API가 없는 곳에서도 데이터베이스 및 기타 워크로드를 보호하게 해줍니다. Universal Share를 NAS로 활용하면서 압축 및 중복 제거를 사용하여 데이터를 저장할 수 있습니다. NetBackup 웹 UI에서 완벽하게 API를 지원하고 공유 및 보호 지점을 통합 관리하며 사용자 할당량 및 Active Directory 통합도 지원하므로, NetBackup HA Appliance를 통해 차원 높은 관리를 수행할 수 있습니다.

자세한 내용은 Veritas NetBackup Administrator's Guide의 Universal Shares 섹션을 참조하십시오.

Universal Shares를 위한 보호 지점 — 공유에 있는 데이터에 대해 특정 시점의 카피본을 생성하고 즉시 백업 이미지를 생성한 다음 여느 백업처럼 활용할 수 있습니다.

CoPilot for Oracle — Oracle CoPilot의 기능을 기반으로 하는 최신 버전은 Oracle DBA를 통해 NetBackup Appliance 스토리지에서 직접 데이터베이스를 시작할 수 있도록 지원합니다.

자세한 내용은 Veritas NetBackup™ for Oracle Administrator's Guide를 참조하십시오.

데이터 장기 보관(LTR) 아카이브 — 이 옵션은 데이터를 장기간 보관해야 하는 경우 데이터 압축 및 중복 제거를 지원하면서 경제성과 내구성을 모두 갖춘 솔루션을 제공합니다. 이 방식에서는 오브젝트 스토리지 및 프라이빗/퍼블릭 클라우드도 활용할 수 있습니다. 프라이빗 클라우드 활용 사례의 경우 Veritas Enterprise Data Services Platform의 Veritas Access Appliance가 제공하는 LTR을 이용하면 됩니다. 복구 방식을 결정할 때 장기간 데이터 보관이 필요한 헬스케어 시스템 및 기타 기업의 경우 LTR 솔루션이 경제적인 최상의 선택이 될 수 있음을 기억하십시오.

베리타스는 테이프 기술을 선호하는 고객을 위해 안정적인 에어 갭(Air-gap) 솔루션으로 랜섬웨어로부터의 복구를 지원하는 가장 통합적인 테이프 기반 솔루션을 제공합니다.

일반 복구 — 특정 파일에 대한 개별 단위 복원, 전체 서버/애플리케이션 복원, 다른 사이트 위치나 클라우드에 대한 재해 복구(DR) 복원이 포함됩니다. Veritas Resiliency Platform에서는 버튼 하나만 누르면 기존 복구를 자동화하고 오케스트레이션할 수 있어 DR 프로세스가 간소화됩니다.

베어 메탈 복원(BMR) — 랜섬웨어로부터 복구할 때 감염된 하드웨어를 불가피하게 활용해야 하고 리소스마저 한정되어 있다면 BMR이 진가를 발휘할 수 있습니다. BMR은 서버 복구 프로세스를 자동화하므로 직접 운영 체제를 재설치하거나 하드웨어를 구성하지 않아도 됩니다. 시스템이 손상되어 완전히 덮어써야 할 경우 BMR을 통해 신속하게 완전히 새로운 시스템으로 재구축하면서 OS 및 애플리케이션 데이터를 한꺼번에 복구할 수 있습니다.

결론

랜섬웨어나 악의적인 의도를 가진 내부자는 기업에 심각한 위협이 됩니다. 새로운 운영 체제 취약점이 끊임없이 나타나고 알려진 악성 코드 및 랜섬웨어의 변종도 수시로 개발되고 있습니다. 이제 랜섬웨어는 거대 시장이 되었습니다. 이는 공격자가 기업의 인프라스트럭처에 침투하고 비즈니스를 중단시킬 새로운 방법을 계속 개발할 충분한 동기를 제공합니다.데이터 보호를 위한 시스템 및 백업 관리자의 노력에도 불구하고 랜섬웨어 및 악의적인 내부자 공격이 지속되면서 기업의 가장 중요한 자산인 데이터에 막대한 피해를 입히고 있습니다. 이런 이유로 거시적 관점의 멀티레이어 통합 전략이 필요하며, 이는 최상의 방어 수단이 됩니다.

베리타스는 고객을 위해 이러한 프로세스를 간소화했습니다. Veritas Enterprise Data Services Platform 솔루션은 레질리언스를 염두에 두고 개발된 만큼, 단일 통합 플랫폼에서 IT 시스템 및 데이터 무결성을 보호하고, 보안 위협을 탐지하기 위해 계속 모니터링하고 리스크를 해소하며, 자동화 및 오케스트레이션을 통해 신속하게 복구를 수행합니다. 베리타스 솔루션은 취약점을 줄이고 데이터 누락 및 잠재적 공격 범위를 제거하면서 손쉬운 확장, 업그레이드, 유지 보수를 지원합니다. 엣지는 물론 코어 시스템, 클라우드까지 전 범위에서 모든 데이터를 확실하게 보호합니다.여전히 많은 기업이 백업 및 복구를 랜섬웨어 공격에 대한 마지막 방어선으로 간주하지만 베리타스는 보호, 탐지, 복구를 포괄하는 멀티레이어 사이버 보안 전략의 핵심 요소로서 효용성과 안정성을 모두 갖춘 백업 및 복구를 구현하도록 조언합니다.

베리타스 솔루션에 대해 자세히 알아보려면 https://www.veritas.com/ko/kr/ransomware에서 확인하거나 https://www.veritas.com/ko/kr/form/requestacall/requestacall에 문의하시기 바랍니다.

참조

정부/공공 기관

- National Cybersecurity Center of Excellence(NCCoE)는 National Institute of Standards and Technology(NIST) 산하 기관으로 Data Integrity, Recovering from Ransomware and Other Destructive Events라는 제목의 특별 간행물을 제작했습니다. 총 3부로 구성된 이 자료는 기업이 악성 코드를 차단하기 위해 구사할 수 있는 전략 및 사이버 보안 사고의 사후 복구 단계를 자세히 다룹니다.

  NIST Special Publication 1800-11

  Data Integrity: Recovering from Ransomware and other Destructive Events(기본 페이지)

  - NIST SP 1800-11a: 개요
  - NIST SP 1800-11b: 접근 방식, 아키텍처, 보안 특성 – 구축 항목 및 그 이유
  - NIST SP 1800-11c: 방법 안내 – 샘플 솔루션 구축 지침

- United States Computer Emergency Readiness Team: Data Backup Options
  https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

베리타스

- Insider Threat 101: Detect and Protect with Veritas Data Insight
  https://www.veritas.com/product/information-governance/data-insight/insider-threat

  랜섬웨어 리포트 템플릿에 대한 자세한 내용은 사용자 가이드의 아래 섹션을 참조하십시오.

  - Data Insight 맞춤형 리포트 소개
    https://www.veritas.com/content/support/en_US/doc/133376979-133376982-0/DI_6_1_2_v109979856-133376982
  - DQL 쿼리 템플릿 소개
    https://www.veritas.com/content/support/en_US/doc/133376979-133376982-0/DI_6_1_2_v109979871-133376982

- Veritas Flex Appliances with NetBackup Security
  https://www.veritas.com/content/dam/Veritas/docs/white-papers/v1108-ga-ent-wp-flex-security-en.pdf
- Veritas Flex Appliances with NetBackup
  https://www.veritas.com/content/dam/Veritas/docs/white-papers/v1111-ga-ent-wp-flex-design-guide-2020-en.pdf
- Veritas Data Insight Administrator's Guide
  https://www.veritas.com/support/en_US/doc/133377453-133377456-0/
- Veritas Data Insight User's Guide
  https://www.veritas.com/support/en_US/doc/133376979-133376982-0/
- Veritas NetBackup Administrator's Guide, Volume I
  https://www.veritas.com/support/en_US/doc/18716246-132504715-0/
- Veritas NetBackup Appliance Administrator's Guide
  https://www.veritas.com/support/en_US/doc/75895731-133007275-0/
- Veritas NetBackup Appliance Fibre Channel Guide
  https://www.veritas.com/support/en_US/doc/99943943-132539628-0/
- Veritas NetBackup Appliance Security Guide
  https://www.veritas.com/support/en_US/doc/96220900-132543872-0/
- Veritas NetBackup Cloud Administrator's Guide
  https://www.veritas.com/support/en_US/doc/58500769-132715871-0/
- Veritas NetBackup Deduplication Guide
  https://www.veritas.com/support/en_US/doc/25074086-131900563-0/

- Veritas NetBackup Security and Encryption Guide
  https://www.veritas.com/support/en_US/doc/21733320-139202231-0/index
- Veritas NetBackup for Oracle Administrator's Guide
  https://www.veritas.com/support/en_US/doc/16226115-133434979-0/
- Veritas NetBackup for VMware Administrator's Guide
  https://www.veritas.com/support/en_US/doc/21902280-133434834-0/

1. https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-

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

V0827 11/20