Enterprise Strategy Group | **Getting to the bigger truth.™**

Technical Validation

베리타스가 구현하는 사이버 보안

베리타스 랜섬웨어 차단 솔루션

Craig Ledo, IT 검증 분석가

2022 년 9 월

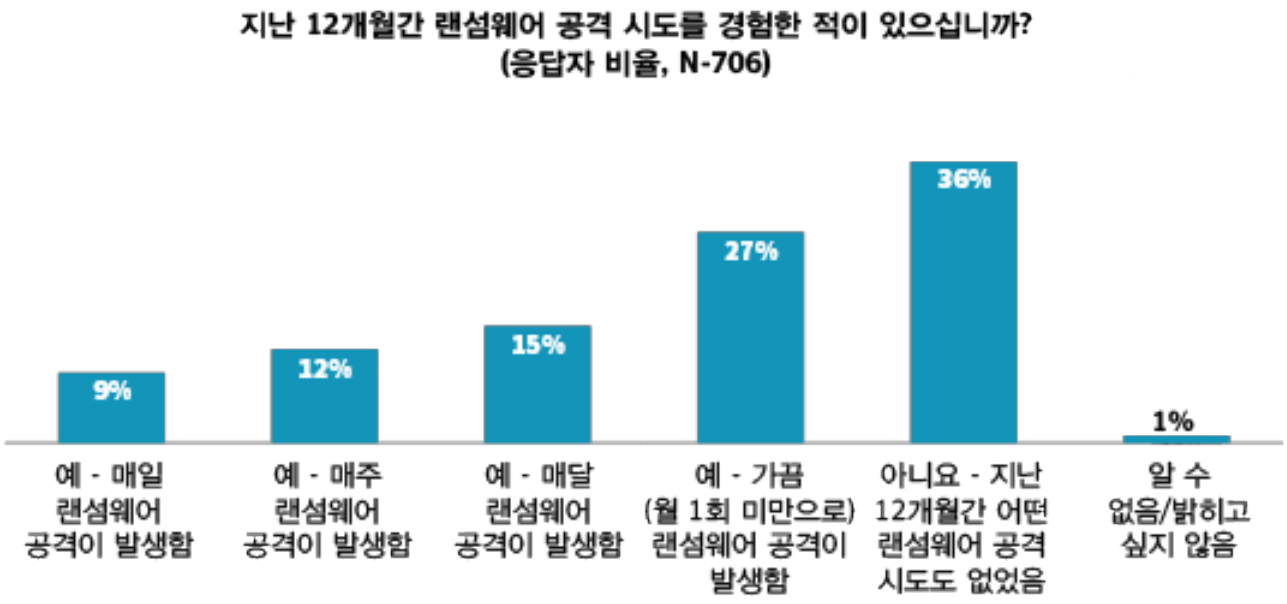
서론

본 ESG Technical Validation 에서는 데이터 보호, 위협 탐지, 확장 가능한 복구를 비롯해 베리타스의 사이버 보안 솔루션에 관한 상세한 평가를 제공합니다. 특히 이번 평가에서는 베리타스 사이버 보안 솔루션 포트폴리오 전체를 대상으로 12 가지 테스트 시나리오에 따라 검증합니다.

배경

랜섬웨어 공격은 여전히 비즈니스 리더와 IT 리더가 가장 우려하는 문제이며, 그럴만한 이유가 있습니다. 기업의 생명이라고 할 수 있는 데이터에 대한 액세스를 방해하기 때문입니다. 랜섬웨어 공격이 지속되면서 각 기업은 다운타임, 생산성, 디바이스 비용, 네트워크 비용, 사라진 기회, 지불된 몸값, 브랜드 가치 등과 관련된 막대한 비용을 치러야 했습니다. 데이터에 대한 진입점을 보호하기 위해 매년 수백만 달러를 쏟아붓는 상황이지만, 여전히 데이터 보호 강화의 전략적 가치를 과소평가하는 기업이 많습니다. ESG 연구 결과, 설문 응답자의 36%가 회사에서 지난 12 개월 동안 이러한 탐색 공격을 월 1 회 이상 겪었다고 밝혔습니다. 여기에는 매일 표적이 된 9%, 매주 공격을 받은 12%도 포함됩니다(그림 1 참조).[1]

그림 1. 보편적으로 발생하는 반복형 랜섬웨어 공격



출처: ESG(TechTarget, Inc.)

[1] 출처: ESG Research Report, 2022 Technology Spending Intentions Survey, 2021 년 11 월.

응답자 중 또 다른 27%의 그룹은 랜섬웨어 공격을 가끔씩 경험했습니다. 이에 따라 기업은 랜섬웨어 공격에 대한 강력한 사전 예방/방어 조치를 마련하여 사전에 가능성을 차단해야 합니다. 게다가 랜섬웨어 공격은 재발 위험이 크기 때문에 각별한 주의가 필요합니다.

랜섬웨어 공격이 극심해지고 데이터 유출 리스크가 커지는 만큼 혁신적인 다계층 레질리언스 전략을 마련하여 IT 서비스 보안, 레질리언스, 복구를 보장하는 한편 엔드유저가 기대하는 만족스러운 경험을 제공해야 합니다. 예컨대 소프트웨어 및 하드웨어 차원의 강화가 수행되고 변조 불가 및 삭제 불가 스토리지를 지원하는 솔루션이라면, 통합적인 다계층 사이버 보안 전략을 구사하는 데 도움이 됩니다.

베리타스 사이버 보안 솔루션 개요

베리타스는 통합 다계층 플랫폼 접근 방식을 통해 선제적 보호, 탐지, 백업 및 복구 기능을 완벽하게 통합 제공합니다. 특히 제로 트러스트 보안 모델을 적용하여 각 기업이 더 효과적인 액세스 제어를 구현하고 보안 침해를 억제하며 자산을 보호하고 피해 가능성을 최소화하도록 지원합니다.

보호

- 알려지지 않은 뜻밖의 위험으로부터 중요 데이터와 IT 인프라스트럭처를 확실하게 보호합니다. 이를 위해 통합 보호 기능을 지능적으로 적용하고 규모에 맞춰 자동으로 관리함으로써 해당 환경의 모든 구성 요소를 백업합니다.
- 백업 인프라스트럭처를 갖추고 데이터를 백업하는 기업은 백업 및 복구 인프라스트럭처를 성공적인 레질리언스 전략의 핵심 요소로 삼을 수 있습니다.
- Veritas NetBackup 은 엣지, 코어, 클라우드 전반에서 800 여 종의 데이터 소스, 1,400 여 곳의 스토리지 제공업체, 60 여 곳의 클라우드 제공업체를 지원하므로, 가장 까다롭고 광범위한 환경도 안전하게 보호합니다.
- 베리타스의 지능형 정책으로 더 차원 높은 지능화를 구현함으로써 관리자가 더 우수한 효율성을 확보할 수 있습니다.
- 베리타스는 데이터 무결성을 보장하는 에어갭(Air Gap) 솔루션을 통해 백업 파일을 안전한 상태로 유지하면서 악의적 의도를 가진 내부자의 접근을 차단합니다.
- 내부적으로 관리되는 컴플라이언스 클록 덕분에 백업 파일을 변조 및 삭제할 수 없습니다.

탐지

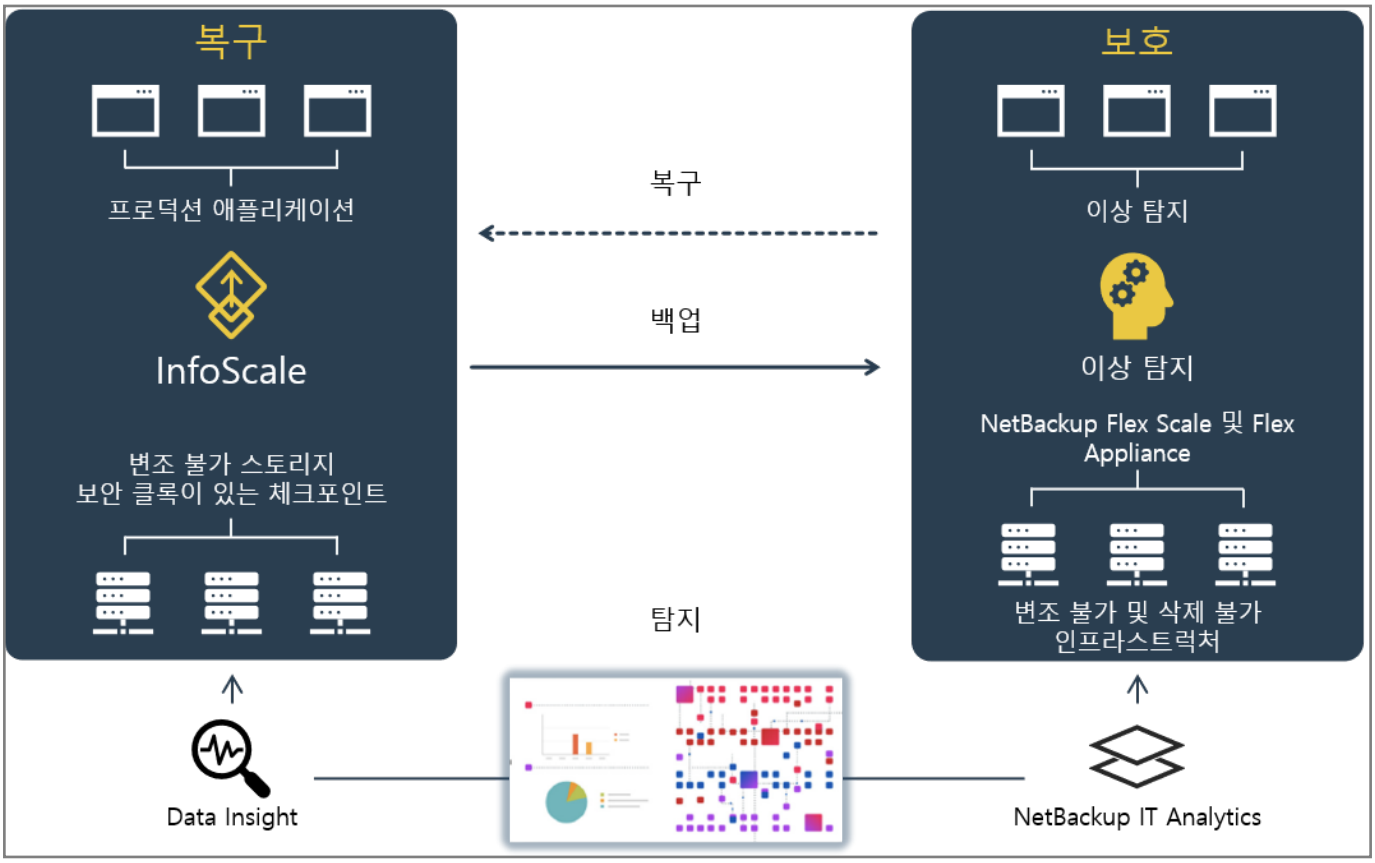
- 베리타스는 인프라스트럭처에 대한 완전한 가시성을 바탕으로 해당 기업 환경의 모든 미확인 데이터를 찾아내는 솔루션을 제공합니다.
- 베리타스를 선택한 고객은 환경의 모든 구성 요소가 안전한 상태이고 랜섬웨어가 발생해도 위협에 능히 대처할 수 있음을 확신합니다.
- 베리타스는 AI 를 활용하여 기본 데이터 및 백업 데이터에서 이상 요인과 악성 코드를 탐지합니다. 또한 이벤트에 의해 실행되는 악성 코드 검사 기능으로 사이버 범죄자나 악성 코드가 작동하기 전에 대응할 수 있게 합니다.

복구

- 베리타스 솔루션을 성공적인 레질리언스 전략의 핵심 요소로 삼는다면, 복구에 최적화된 환경이 구현됩니다.
- 베리타스는 보안 솔루션을 기본 제공하면서 랜섬웨어에 감염되지 않은 안전한 데이터 및 환경의 복구를 보장합니다.
- 공격이 환경 전체에 영향을 미치는 경우라도 데이터 센터 전체를 클라우드에, 온디맨드 방식으로 복구해야 합니다.
- 다른 한편으로 공격이 환경의 일부에만 영향을 미칠 경우도 있습니다. 따라서 유연성을 발휘하여 개별 데이터베이스 및 파일을 프로덕션으로 빠르게 복구하는 솔루션 구축이 중요합니다.
- 서버 전체가 암호화되는 경우에는 이 서버를 신속하게 다른 곳으로 복구하는 조치가 필요할 수 있습니다.
- 많은 애플리케이션 인스턴스를 다시 프로덕션 환경으로 복구해야 할 때도 있습니다.
- 베리타스는 오케스트레이션 기반 복구 및 일괄 복구를 비롯해 확장 가능한 방식으로 복구하는 솔루션을 제공합니다.

베리타스 솔루션은 데이터 상시 가용성 및 보호를 보장하고, 애플리케이션 고가용성 구현을 지원하며, 규모의 재약 없는 복구 기능을 제공합니다. 베리타스는 비즈니스 가치에 입각한 랜섬웨어 레질리언스 방식을 채택합니다. 즉, 랜섬웨어를 차단하고 탐지하며 랜섬웨어에 감염된 후에도 안전하게 복구하는 솔루션을 통해 강력한 레질리언스 전략을 이행합니다(그림 2 참조).

그림 2. 베리타스 사이버 레질리언스 솔루션 개요



출처: ESG(TechTarget, Inc.)

ESG Technical Validation

ESG 에서 데이터 보호, 위협 탐지, 확장 가능한 복구 기능을 비롯해 베리타스 사이버 보안 솔루션에 대한 기술 검증을 수행했습니다.

데이터 보호

베리타스는 다음과 같이 다양한 보안 제어 기능을 통해 데이터 보호를 뒷받침합니다.

- **ID 및 액세스 관리**: 역할 기반 액세스, SSO(Single Sign-On), 맞춤형 인증
- **데이터 암호화**: 전송 중인 데이터 및 저장된 데이터 암호화
- **변조 불가 이미지 관리 및 저장**: 스토리지에 구애받지 않는 유연한 이미지 관리, WORM(Write Once, Read Many) 스토리지에 이미지 저장
- **솔루션 하드닝**: NetBackup Flex 및 NetBackup Flex Scale 이 소프트웨어/하드웨어 차원의 강화를 거쳐 변조 불가 스토리지를 제공하는 완전한 보안 솔루션으로 거듭납니다.

특히 ESG 는 다음과 같은 주요 데이터 보호 기능을 검증했습니다.

클라우드 데이터 변조 불가

이 베리타스 솔루션은 사이버 범죄자의 침입 및 내부자에 의한 위협으로부터 데이터를 보호하기 위해 일정한 기간 동안 데이터를 변경할 수 없게 합니다. 한층 더 강력한 보안을 제공하기 위해 안전한 데이터 저장소에 백업 스토리지를 두며, 이 저장소는 NetBackup 스토리지 서비스를 통해서만 모니터링 및 액세스할 수 있습니다. 즉, 사용자와 파일 시스템 서비스에서는 액세스할 수 없습니다.

공격 차단 기능 강화

NetBackup Appliance 스택 전체가 보안을 위한 하드닝(hardening)을 거쳤습니다. 여기에는 Linux 운영 체제, 관리 액세스, 애플리케이션 바이너리, 구성 설정 등이 포함됩니다. STIG 지침에 부합하고 액세스 제어를 의무화하는 독점적인 보안 정책도 적용합니다. 또한 프로세스 및 리소스에 대한 액세스를 제한하고 중요한 사용자 및 시스템 작업에 대한 감사 추적을 유지 보수하는 침입 탐지/차단 서비스도 제공합니다.

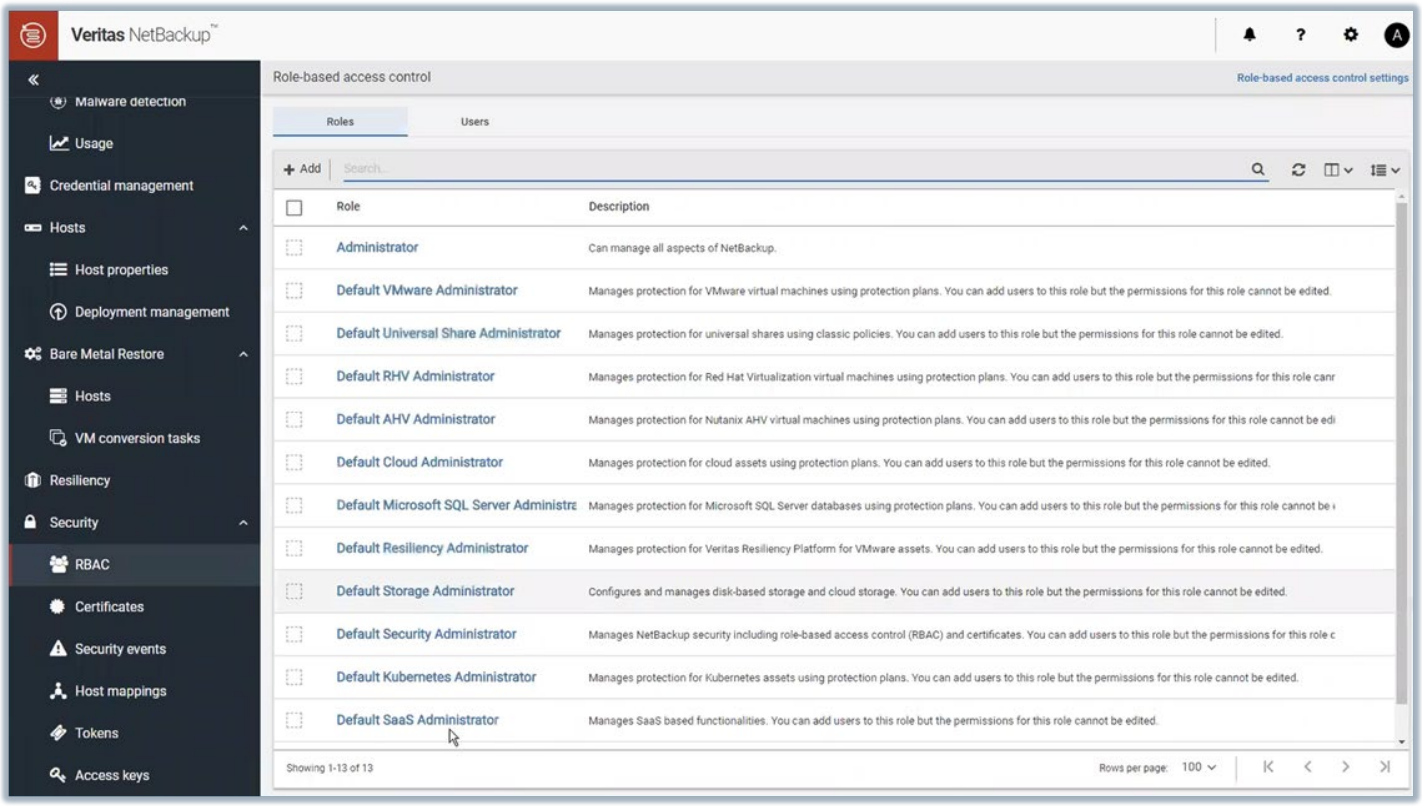
무단 변경 방지 하드웨어

변조 불가 스토리지를 호스팅하는 어플라이언스는 고강도 보안 모드로 전환하여 데이터와 인프라스트럭처를 모두 보호할 수 있습니다. 관리자는 OS 및 내부 구성 요소를 변경할 수 없습니다. 모든 엔드포인트에서 무단 액세스가 차단되며, 모든 서비스에 대한 액세스가 보호받고 인증됩니다.

보안 액세스 제어

이 솔루션은 그림 3 에 표시된 대로, 역할 기반 액세스 제어(RBAC) 템플릿을 제공합니다. 그러면 관리자가 사용자 또는 사용자 그룹에 적절한 액세스 권한이나 사용 권한을 손쉽게 제공할 수 있습니다. 관리자가 각 템플릿을 드릴다운하면서 세부적인 권한(예: NetBackup 관리, 보호, 보안, 스토리지)을 확인할 수도 있습니다. 관리자가 사용자/그룹 액세스 권한 또는 사용 권한을 맞춤형으로 생성하는 것도 가능합니다. 관리자는 맞춤형 역할에 따라 워크로드를 지정하거나(사용자가 관리할 수 있는 워크로드 자산 선택), 보호 계획을 지정하거나(사용자가 관리할 수 있는 보호 계획 선택), 인증 정보를 지정(사용자가 관리할 수 있는 인증 정보 선택)할 수도 있습니다.

그림 3. 보안 액세스 제어

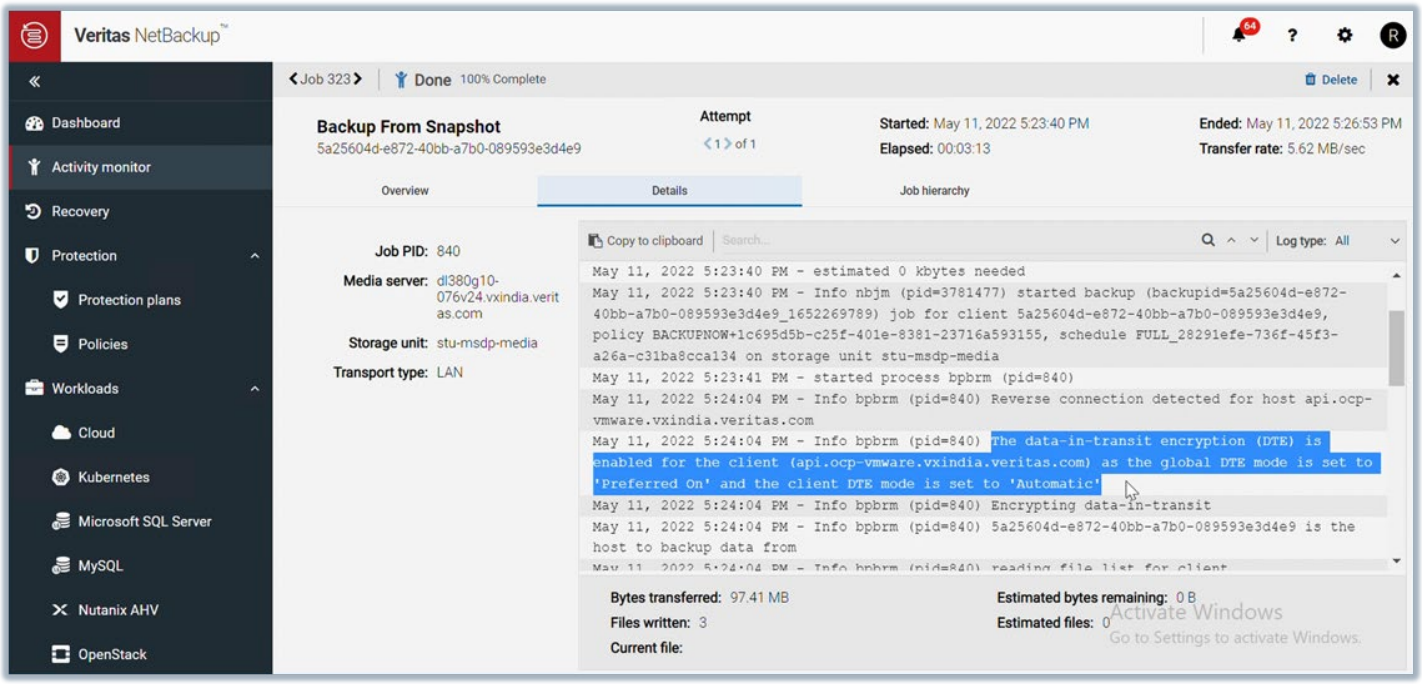


출처: ESG(TechTarget, Inc.)

현대화된 인프라스트럭처 보호

이 솔루션은 빅 데이터, 하이퍼컨버지드, 오픈 소스 MySQL/NoSQL 데이터베이스와 같은 최신 인프라스트럭처를 위해 차세대 데이터 보호 기술을 제공합니다. NetBackup 을 선택한 기업은 멀티 클라우드 워크로드, 가상 워크로드, 물리적 워크로드, 최신 워크로드를 해당 위치와 상관없이 단일 콘솔에서 모두 보호할 수 있습니다. 그림 4 는 스냅샷을 사용하는 백업을 보여줍니다. 이 백업은 클라이언트에 대해 전송 중 데이터 암호화(DTE) 기능이 활성화되어 있습니다. 글로벌 DTE 모드가 '기본적으로 켜짐(Preferred On)', 클라이언트 DTE 모드가 '자동(Automatic)'으로 설정되어 있기 때문입니다. 필요 시 사용자는 DTE 가 활성화된 백업에서 복원할 수 있습니다. 백업 이미지의 DTE 모드가 '켜짐(On)'으로 설정되어 있기 때문입니다.

그림 4. 최신 인프라스트럭처를 위한 보호



출처: ESG(TechTarget, Inc.)

주목해야 할 사항

랜섬웨어 공격이 진화를 거듭하며 더욱 지능화됨에 따라, 각 기업 역시 빠르게 변경되는 위협에 문제없이 적응하면서 서버 다운타임 및 데이터 유출을 방지하는 것이 중요합니다. 베리타스의 첨단 데이터 보호 및 보안 어플라이언스는 통합 이상 탐지, 악성 코드 검사, 제로 트러스트 아키텍처, 변조 불가/삭제 불가 스토리지 등과 같은 기능으로 랜섬웨어에 대응합니다.

보안 위협 탐지

베리타스는 다음과 같이 다양한 보안 제어 기능을 통해 위협 탐지를 뒷받침합니다.

- **백업 및 스토리지 인프라스트럭처 인식**: NetBackup IT Analytics 는 위협 완화 조치 외에도 연이어 장애가 발생하는 소스, 최신 버전의 백업이 없는 소스, 애플리케이션별 백업 실패 현황 등을 분석하는 엔드투엔드 백업 모니터링 솔루션입니다.
- **이상 탐지**: NetBackup 은 AI 를 활용하여 이상을 탐지합니다. 즉, 환경 전체를 대상으로 비정상적인 데이터를 탐지하고, 의심스러운 변칙 요소가 발견되는 경우 거의 실시간으로 알림을 전송합니다.
- **기본 스토리지 탐지**: 베리타스는 NetBackup 으로 보조 백업 데이터를 관리하고, Veritas Data Insight 로 기본 스토리지 데이터를 관리합니다. 후자의 경우, 사용자 및 데이터와 관련해 비정상적인 행동을 거의 실시간으로 탐지하고, 맞춤형 랜섬웨어별 쿼리 템플릿을 제공하며, 랜섬웨어 탐지에 유용한 파일 확장자 식별을 지원하면서 기존 보안 탐지 툴을 보완합니다.
- **악성 코드 탐지**: 베리타스는 보호받는 백업을 대상으로 자동 검사 및 온디맨드 검사를 모두 지원합니다. 자동 악성 코드 검사 기능은 사람의 개입 없이 인공 지능/머신러닝(AI/ML) 기술을 통해 악성 코드를 포착하고 검사합니다.

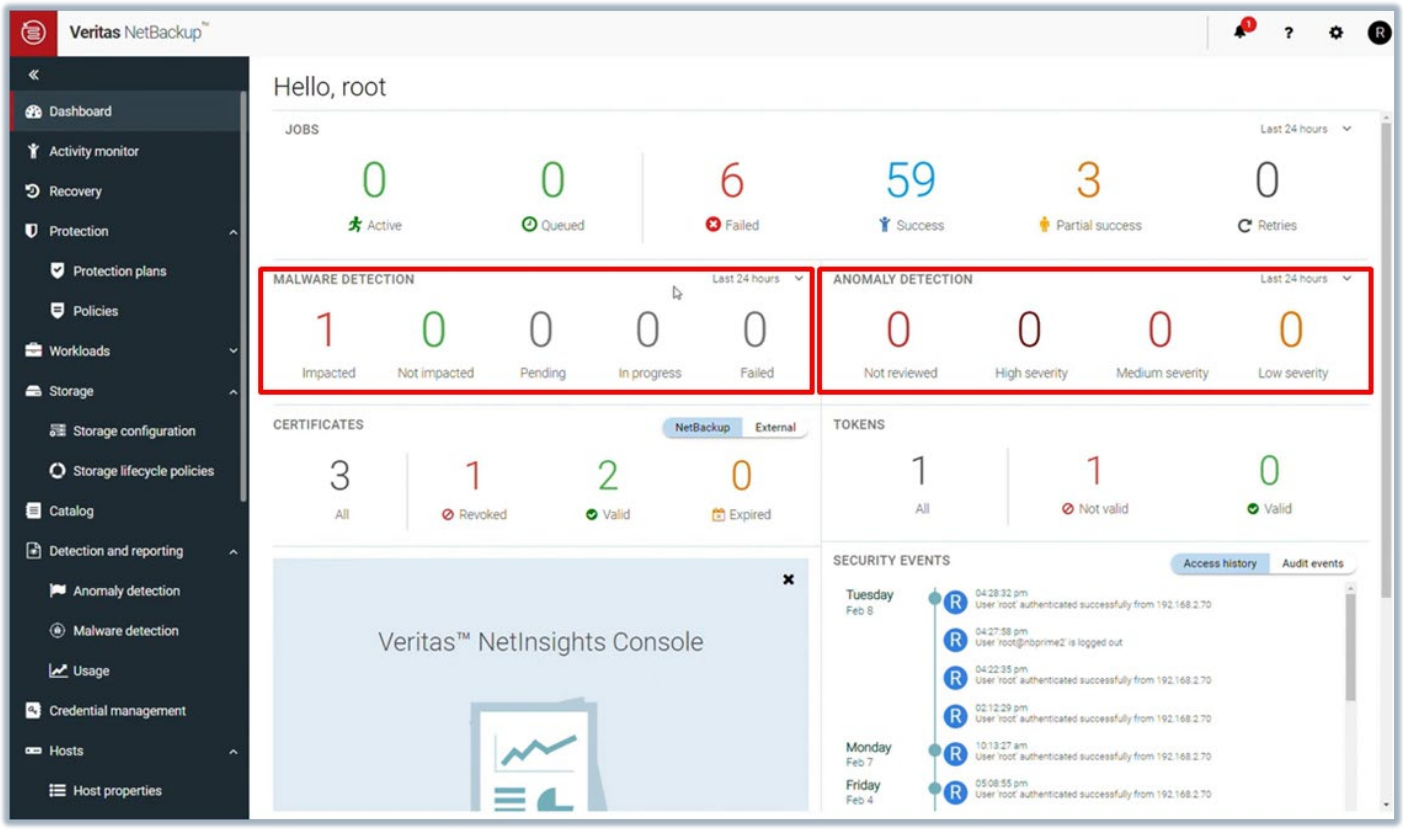
특히 ESG 는 다음과 같은 주요 위협 탐지 기능을 검증했습니다.

통합형 악성 코드 검사 및 이상 탐지

이상 탐지 기능은 악성 코드 탐지 기능과는 별도로 이미지 메타데이터를 추적합니다. 단, 악성 코드 탐지에서 이상 탐지 점수를 활용할 수 있습니다. 그림 5 에 표시된 대로, 악성 코드 탐지 이벤트는 '지난 24 시간'을 기준으로 영향 있음(Impacted), 영향 없음(Not Impacted), 대기 중(Pending), 진행 중(In Progress), 실패(Failed)로 분류됩니다. 이 시간 범위는 '지난 48 시간' 또는 '지난 72 시간'으로도 구성 가능합니다. 사용자가 각 영역(예: 영향 있음)으로 드릴다운하여 세부 정보를 확인할 수 있습니다. 영향을 받은 백업 이미지 각각에 대해 모든 카피본을 만료시키거나 감염된 파일을 조회하는 등의 사용자 조치가 수행될 수 있습니다. 악성 코드 탐지 대시보드는 클라이언트, 백업 시간, 검사 결과, 백업 유형, 검사 날짜, 악성 코드 애플리케이션 검사기, 영향을 받은 파일 수, 검사 호스트 이름, 백업 ID 와 같은 정보를 제공합니다. 악성 코드 검사 시간은 이미지 크기, 파일 개수 등 여러 요인에 따라 달라집니다.

그림 5 에 표시된 대로, 악성 코드 탐지 이벤트는 '지난 24 시간'을 기준으로 검토되지 않음(Not Reviewed), 심각도 높음(High Severity), 심각도 중간(Medium Severity), 심각도 낮음(Low Severity)으로 분류됩니다. 이 시간 범위는 '지난 48 시간', '지난 72 시간', '지난 7 일'로도 구성 가능합니다. 사용자는 검토 상태(검토되지 않음, 오탐지, 이상, 무시) 및 이상 심각도(높음, 중간, 낮음)를 기준으로 필터링할 수도 있습니다. 이상 탐지 대시보드는 작업 ID, 클라이언트 이름, 정책 유형, 개수, 점수, 이상 심각도, 이상 요약, 수신됨, 검토 상태, 정책 이름, 일정 이름, 일정 유형과 같은 정보를 제공합니다. 사용자는 이상과 관련하여 무시로 표시, 이상으로 확인, 오탐지로 리포팅과 같은 작업을 수행할 수 있습니다.

그림 5. 통합형 악성 코드 검사/이상 탐지 기능



출처: ESG(TechTarget, Inc.)

리포팅 및 알림

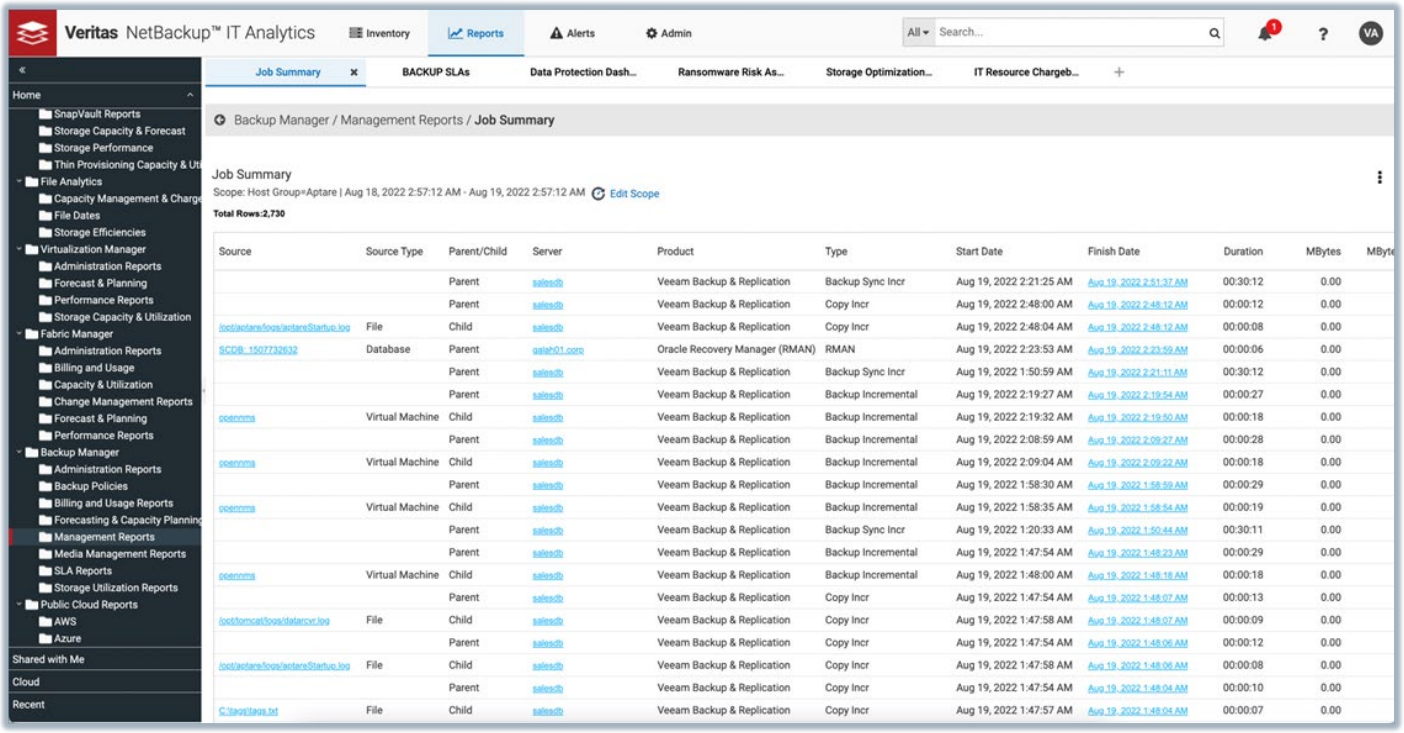
Veritas NetBackup IT Analytics 는 랜섬웨어 리스크 평가 대시보드를 즉시 사용할 수 있습니다. 이 대시보드는 사용자에게 미리 ID 가 부여된 리포트를 간략하게 제시하며, 리포트는 예측 분석을 통해 백업 환경 내의 잠재적 리스크를 규명합니다(그림 6 참조). 사용자는 다음과 같은 여러 데이터 포인트를 종합적으로 리포팅하는 이 분석 기능을 활용하여 백업 환경을 최적화하고 안전하게 보호할 수 있습니다.

- **검색** – 사용자는 백업 환경에서 발생하는 모든 변경 사항을 트래킹하면서 랜섬웨어를 탐지하고 신속하게 대응할 수 있습니다. 특히 알려진 850 여 개의 랜섬웨어 확장을 찾아낼 수 있습니다.
- **리스크 시각화** – 사용자는 직관적인 그래프를 통해 해당 환경에서 발생한 모든 리스크의 이력을 조회하고, 백업 일정에서 누락된 호스트를 찾아 플래그를 지정하고, 백업이 실패한 애플리케이션을 시각화할 수 있습니다.
- **백업 모니터링** – 사용자는 실행 가능한 인사이트를 제공하는 요약 그래프를 참조하면서 백업 환경을 모니터링하고 변경 사항을 파악할 수 있습니다. 또한 성공한 것으로 확인된 백업의 기준선을 적용하면서 이상 요인을 찾아내 리스크를 완화할 수 있습니다.

NetBackup IT Analytics 는 확인된 랜섬웨어 확장자가 있는 파일을 찾아낼 뿐만 아니라 사용자가 이 정보를 유의미하게 구성하여 신속한 대응 계획을 실행할 수 있게 합니다. 사용자는 탐지된 랜섬웨어 파일의 정보를 호스트, 랜섬웨어 파일이 가장 많은 위치, 랜섬웨어 확장자 유형, 파일 소유자를 기준으로 구성할 수 있습니다.

NetBackup IT Analytics 는 성공한 백업을 탐색하여 오탐지 가능성을 파악합니다. 이를 위해 과거의 백업과 새로운 백업을 비교하여 작업 소요 시간의 큰 편차, 이미지 크기 변화, 정책 구성 변경 등의 이상 요인을 찾아냅니다. 사용자는 이러한 정보를 통해 중요 IT 서비스가 보호받고 있음을 확인합니다.

그림 6. 리포팅 및 알림



출처: ESG(TechTarget, Inc.)

주목해야 할 사항

앞서 언급한 대로, 랜섬웨어 공격이 계속 진화하면서 지능화됨에 따라, 베리타스는 애플리케이션 및 데이터 상태에 관한 통합 실시간 가시성을 제공합니다. 이를 위해 이상 요인을 탐지하고 맞춤형 인사이트를 제공하면서 기본 데이터와 백업 데이터 모두에서 악성 코드 침투를 찾아내도록 지원합니다.

확장형 복구

베리타스는 다음과 같이 다양한 기능을 통해 확장 가능한 방식으로 복구합니다.

- **NetBackup Resiliency**: NetBackup Resiliency 는 기업의 이기종 환경 전반에서 자동화된 오케스트레이션을 수행합니다. 이를 위해 일관성 있는 사용자 경험을 제공하고, 사용 가능한 옵션을 기반으로 최상의 복구 옵션을 제공합니다.
- **NetBackup Instant Rollback for VMware**: 빠른 속도로 가상 머신(VM)을 복구합니다. 즉, 역방향 변경 블록 트래킹 기능을 사용하여 복구해야 할 고유 블록을 파악한 다음 변경된 사항만 적용하는 방식으로 수초 만에 안전한 VM 으로 복원합니다.

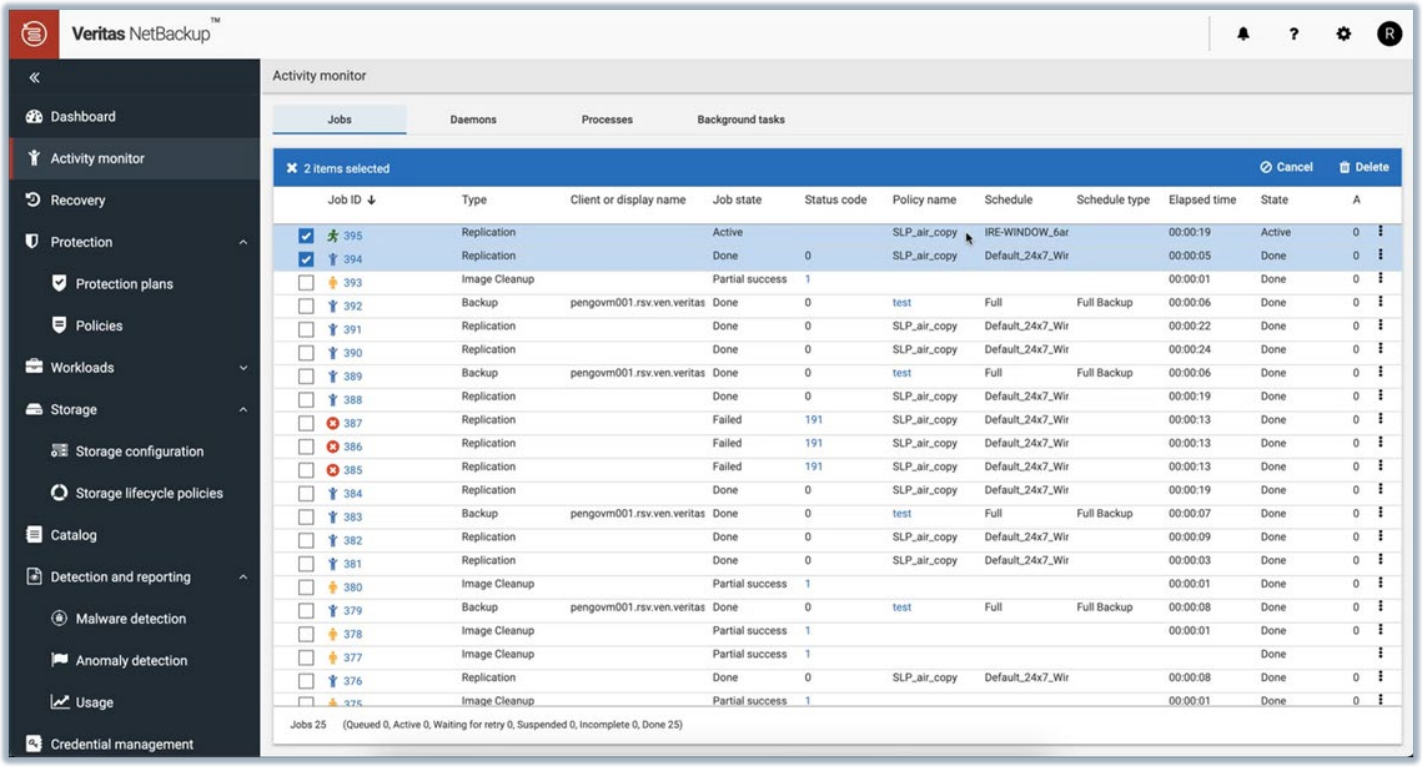
- **VM 복구**: 하나의 VMware VM 백업을 사용하여 전체 VM 복구, 개별 VMDK 복구, 파일/폴더 복구, 애플리케이션 전체 복구, 인스턴트 액세스 복구, 파일 다운로드 복구, 애플리케이션 GRT 복구, AMI 변환 복구의 8 가지 복구 유형을 지원합니다.
- **MSSQL 및 VMware 를 위한 인스턴트 액세스**: 백업에서 VM 데이터를 전송할 때까지 기다릴 필요 없이 거의 즉각적으로 VM 을 복구합니다. 예를 들면 1,600 개의 VM 을 복구할 수도 있습니다. 백업 스토리지에서 직접 VM 을 테스트하거나 복구하는 것도 가능합니다.
- **NetBackup CloudPoint**: NetBackup CloudPoint 는 클라우드 벤더에 구애받지 않고 클라우드 네이티브 스냅샷 기술을 활용하면서 하이브리드 및 멀티 클라우드 인프라스트럭처를 손쉽게 보호합니다.
- **Universal Share 와 보호 지점**: NetBackup Server 의 중복 제거 기반 스토리지를 보안 공유 형태로 프로비저닝함으로써 에이전트나 백업 API 가 없는 경우에도 데이터베이스 및 기타 워크로드를 보호할 수 있게 합니다.
- **NetBackup Universal Shares for Oracle**: Oracle 데이터베이스 관리자가 NetBackup Appliance 의 스토리지에서 직접 데이터베이스를 시작할 수 있게 합니다.
- **데이터 장기 보관 아카이브**: 데이터의 중복 제거 및 압축 기능을 갖춘 비용 효율적이면서 안정적인 솔루션을 제공합니다. 여기서는 오브젝트 스토리지 및 프라이빗/퍼블릭 클라우드를 사용할 수 있습니다. 기존 복구 방식으로는 개별 파일 복원, 서버/애플리케이션 전체 복원, 다른 사이트 위치/클라우드로의 재해 복구(DR) 복원 등이 있습니다. Veritas Resiliency Platform 에서 버튼 하나만 눌러 기존 복구 방식을 자동화하고 오케스트레이션함으로써 DR 프로세스를 간소화할 수 있습니다.
- **베어 메탈 복원(BMR)**: 서버 복구 프로세스를 자동화하므로 운영 체제를 다시 설치하거나 직접 하드웨어를 구성할 필요가 없습니다. 단일 작업으로 빠르게 시스템을 완전히 새로 재구축하면서 OS 및 애플리케이션 데이터를 복원할 수 있습니다.

특히 ESG 는 다음과 같은 주요 확장형 복구 기능을 검증했습니다.

IRE(Isolated Recovery Environment)

Veritas NetBackup Isolated Recovery Environment 는 복잡한 다계층 환경에 포함되었을 수 있는 가상 머신(VM) 수천 대를 대상으로 복구 계획을 수립하고, 격리된 환경에서 리허설을 반복 실행하는 것이 가능합니다(그림 7 참조). 이 기능은 기본 제공되는 변조 불가/삭제 불가 모드, 타사 하드웨어 변조 불가 모드, 클라우드 기반의 잠긴 오브젝트 스토리지 변조 불가 모드, SaaS 워크로드 백업을 위한 변조 불가 모드를 지원할 수 있습니다. 아울러 NetBackup 은 중복 제거된 데이터를 직접 전송하고 효율적으로 AWS S3 Object Lock 에 저장할 수도 있습니다.

그림 7. IRE(Isolated Recovery Environment)

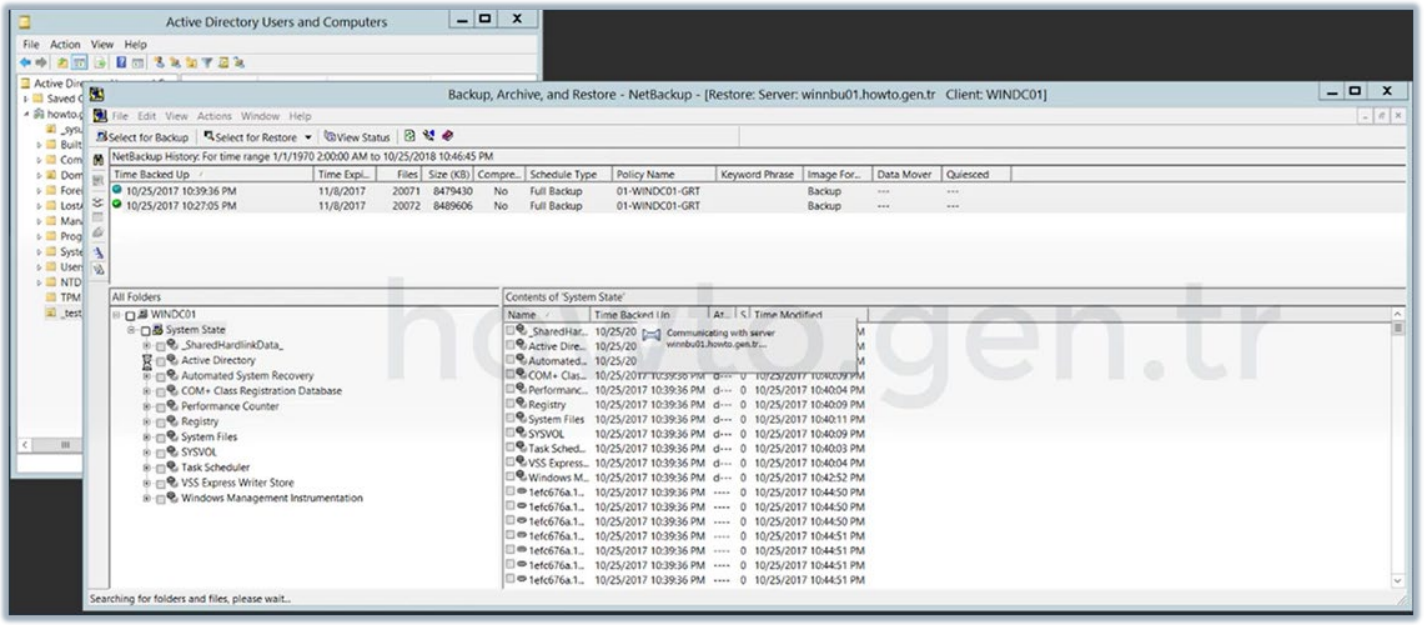


출처: ESG(TechTarget, Inc.)

손실된 Active Directory 복구

Veritas NetBackup 솔루션은 Active Directory 백업을 탐색하여 손실된 Active Directory 가 있는 경우 이를 복구할 수 있습니다(그림 8 참조). 사용자는 적합한 Active Directory 백업을 시작하기만 하면 됩니다. 요청된 작업이 성공적으로 완료되었다고 표시될 때까지 복원 작업의 진행률을 확인할 수도 있습니다.

그림 8. 손실된 Active Directory 복구

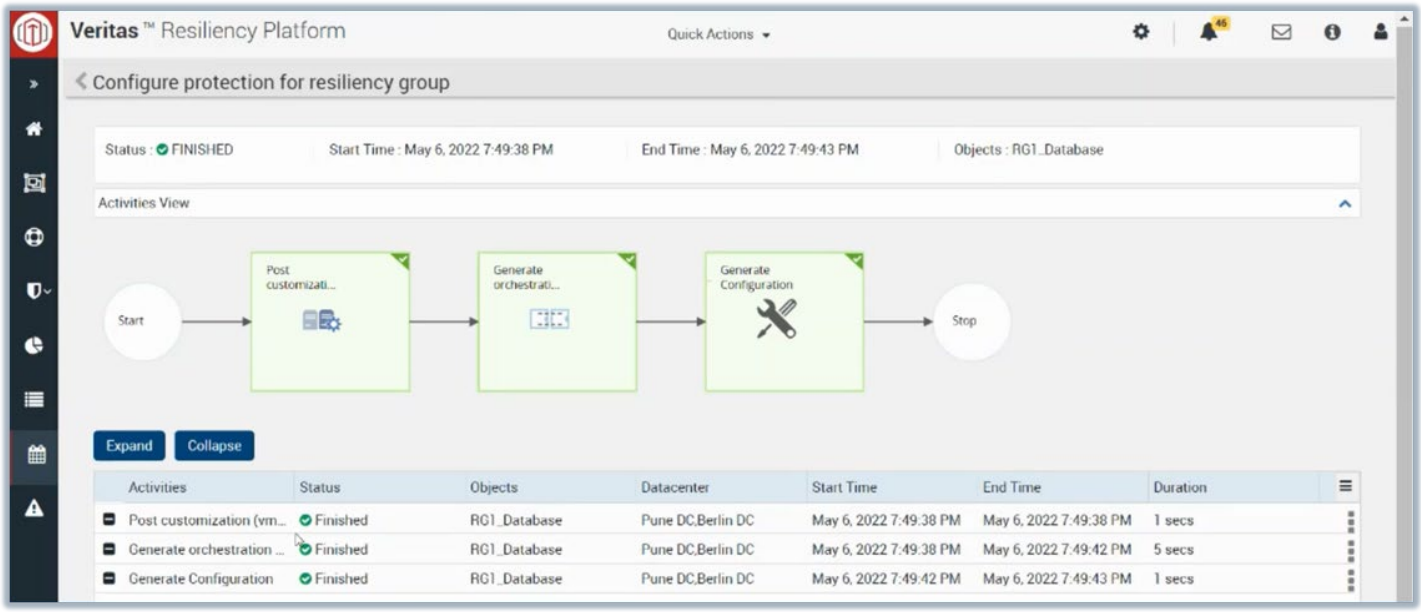


출처: ESG(TechTarget, Inc.)

계층화된 복구 오케스트레이션

사용자는 Veritas NetBackup Resiliency 의 가상 비즈니스 서비스(Virtual Business Services)를 활용하여 다계층 애플리케이션 복구를 단일 통합 엔티티처럼 관리할 수 있습니다. 또한 가상 비즈니스 서비스에서 여러 시스템 전반의 복잡한 다계층 애플리케이션의 복구를 완전히 자동화할 수 있습니다. 그러면 랜섬웨어 공격이 발생하더라도 더 쉽고 빠른 복구가 가능할 뿐만 아니라 애플리케이션 다운타임이 최소화됩니다. 즉, Veritas Resiliency Platform 에서 계층형 복구 오케스트레이션을 수행합니다. 이를테면 가상화 및 프라이빗 클라우드(예: VMware vCenter 추가), NetBackup 기본 서버, 네트워크(예: 네트워크 페어링), 물리적 서버, 데이터베이스 등을 구성합니다. 그림 9 에서는 완료된 레질리언스 그룹 보호 구성을 확인할 수 있습니다.

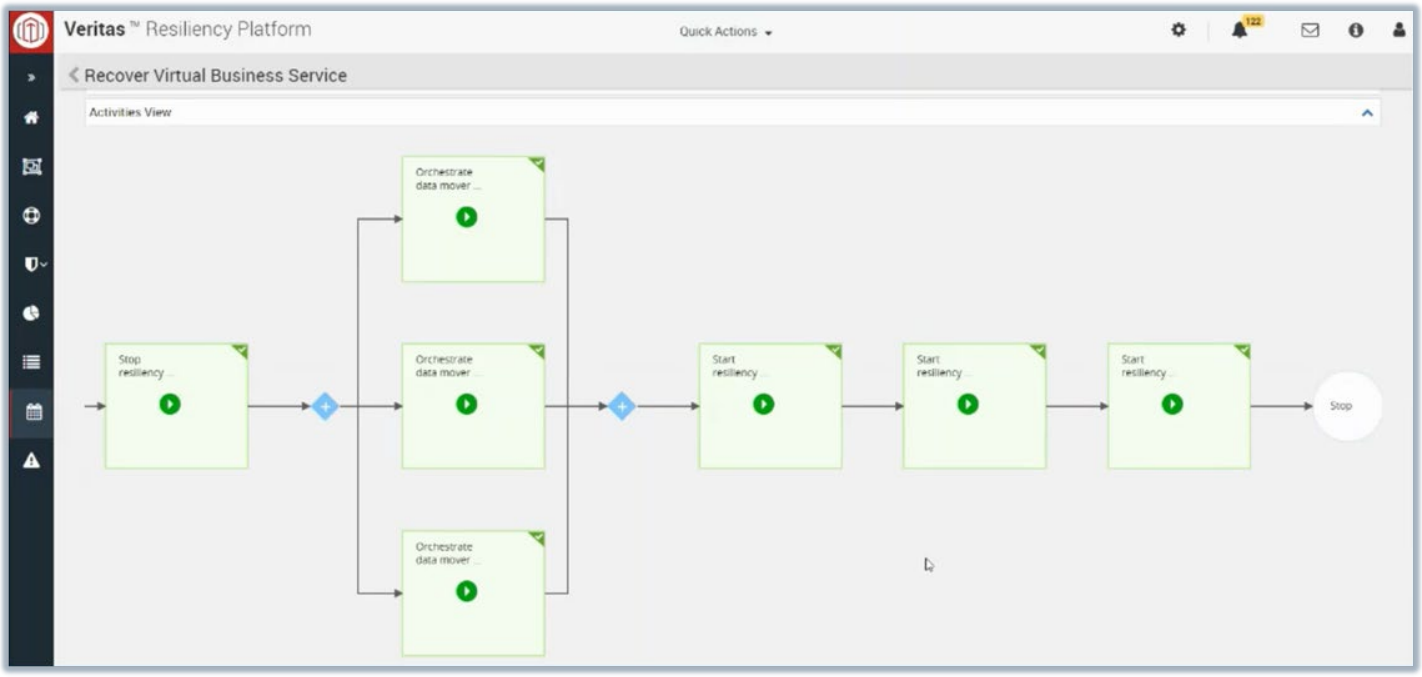
그림 9. 계층형 복구 구성



출처: ESG(TechTarget, Inc.)

레질리언스 그룹 보호 구성을 완료했다면 이제 계층형 가상 비즈니스 서비스를 설정해야 합니다. 그런 다음 사용자는 가상 비즈니스 서비스의 계층형 복구를 오케스트레이션할 수 있습니다(그림 10 참조).

그림 10. 계층형 복구 오케스트레이션



출처: ESG(TechTarget, Inc.)

주목해야 할 사항

랜섬웨어 공격이 갈수록 증가함에 따라, 기업은 통합 랜섬웨어 레질리언스 및 복구 전략을 갖춰야 합니다. 베리타스는 애플리케이션의 가용성은 물론 데이터의 보안 및 무결성까지 보장하는 스토리지 레질리언스, 변조 불가, 데이터 격리 기능을 통합 제공하면서 기본 데이터를 위한 차원 높은 스토리지 및 고속 복구를 지원합니다.

결론

랜섬웨어나 악의적인 의도를 가진 내부자는 기업에 심각한 위협이 됩니다. 새로운 운영 체제 취약점이 끊임없이 등장하고 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.

ESG 는 데이터 보호, 위협 탐지, 확장 가능한 복구 등을 포함하는 12 가지 테스트 시나리오를 통해 베리타스의 사이버 보안 솔루션을 검증했습니다. 거시적 관점의 다계층 통합 사이버 보안 전략은 악성 코드 침투로 인한 다운타임 및 데이터 유출을 차단하는 최상의 방어 체계입니다. 베리타스는 이러한 복잡성을 이해하고 기업이 전체 사이버 보안 전략의 일환으로 IT 서비스를 보호할 수 있도록 지원하는 전사적 토대를 마련합니다. 베리타스 사이버 보안 전략은 기업의 IT 서비스에서 고가용성과 레질리언스를 구현하고 랜섬웨어로부터 확실히 보호하는 데 필요한 툴과 기능을 제공하면서 안전을 보장합니다.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2022 TechTarget, Inc. All Rights Reserved.