기술 검증

# 퓨어스토리지를 통한 랜섬웨어 방어 및 복구

## 퓨어스토리지 랜섬웨어 소프트웨어 솔루션

크레이그 레도(Craig Ledo), IT 검증 애널리스트

2022년 7월

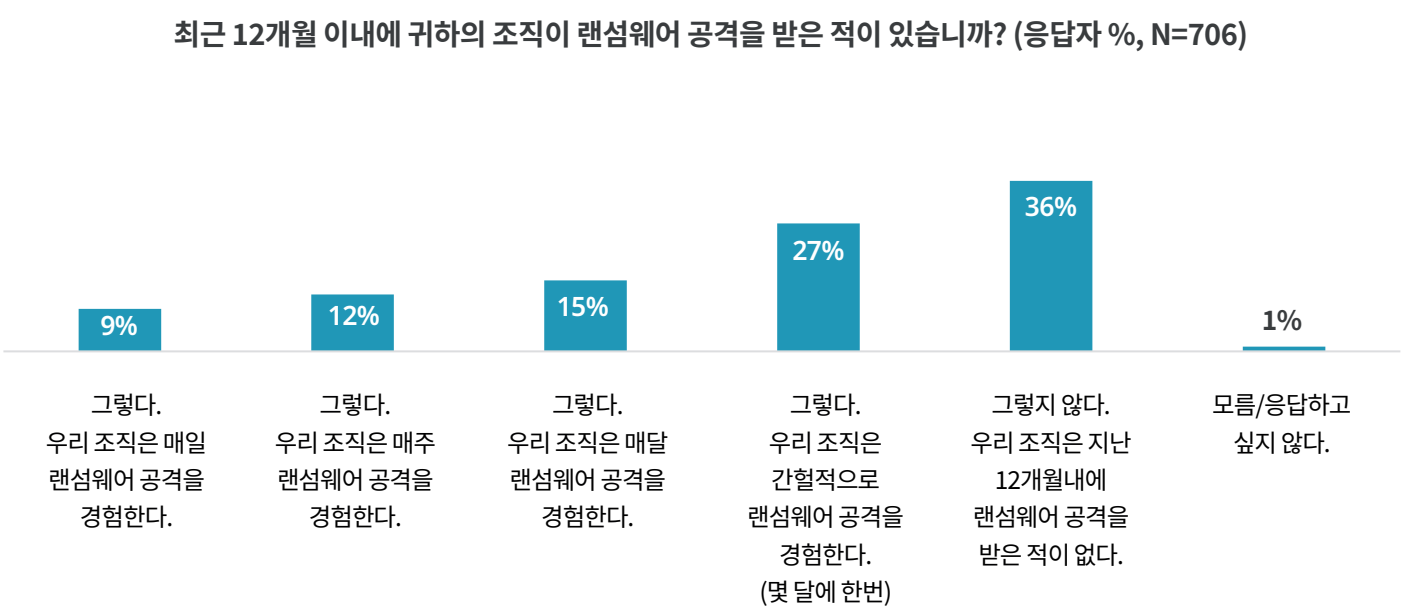
## 소개

이 ESG 기술 검증 보고서는 퓨어스토리지 솔루션의 랜섬웨어 완화 및 복구 역량을 세부적으로 평가한 결과를 문서화한 것입니다. ESG는 멀웨어 클렌징을 위한 오프라인 복원, 우선순위 시스템의 신속한 복구, 공간 효율적인 스냅샷을 통한 포렌식 지원 등 공격 전후 및 공격 중간에도 퓨어스토리지가 어떻게 랜섬웨어 보호를 제공하는지 평가했습니다.

## 배경

기술 검증랜섬웨어 공격은 기업과 IT 리더들에게 가장 중요한 문제입니다. 그리고 그럴 만한 이유가 있습니다. 랜섬웨어 공격은 조직의 생명줄이라고 할 수 있는 데이터에 대한 액세스를 방해하기 때문입니다. 최근 랜섬웨어 공격이 확산되면서 다운타임, 직원들의 시간, 장치 비용, 네트워크 비용, 기회 손실, 금전적 대가 등 막대한 피해가 발생했습니다. 많은 기업들은 데이터 진입점을 보호하기 위해 매년 수백만 달러를 지출하고 있지만, 데이터 보호 계획을 한 차원 끌어올림으로써 얻을 수 있는 전략적 가치를 과소평가하고 있습니다. ESG의 설문조사에서 응답자의 36%는 지난 12개월 동안 적어도 매달 탐색 공격을 경험했다고 답했으며, 그 중 9%는 매일, 12%는 매주 공격을 받은 것으로 나타났습니다.[1] (그림 1 참조)

그림 1. 반복되는 랜섬웨어 공격




*출처: TechTarget, Inc.의 사업부 ESG*

또 다른 27%의 응답자는 좀 더 산발적으로 랜섬웨어 공격을 받았습니다. 많은 기업들이 랜섬웨어 공격을 받고 있는 상황에서 공격 전후 및 공격 중간에 강력한 방어 수단을 구현하여 공격이 성공할 수 없도록 만드는 것이 중요합니다. 한 번 공격을 받은 피해자는 재차 공격을 받을 수 있고, 실제로 그러한 경우가 자주 발생하기 때문입니다.

[1] 출처: ESG Research Report, 2022 기술 지출 의도 설문조사, 2021년 11월. 해당 기술 검증 보고서에 포함된 모든 ESG의 연구 참조 자료와 차트는 연구 보고서에서 발췌한 것입니다.

## 퓨어스토리지 랜섬웨어 솔루션 개요

퓨어스토리지는 랜섬웨어 수명주기의 모범 사례에서 세 가지 핵심 요소를 제공합니다.

- **핵심 요소 1 – 공격 전(예방적 유지관리):** 시스템 위생 및 패치 관리를 간소화하고 보안 정보 및 이벤트 관리(SIEM)을 구현하며 위협 식별을 위한 처리 속도를 높여 다중 인증을 설정합니다.
- **핵심 요소 2 – 공격 중(대응):** 저장 시 상시 실행되는 암호화로 애플리케이션 데이터, 백업 및 시스템을 잠그고 공격과 그 심각도를 파악하며 스냅샷이 수정 또는 삭제되는 것을 방지합니다.
- **핵심 요소 3 – 공격 후(복구):** 우선순위가 높은 시스템의 신속한 복구, 멀웨어 제거를 위한 오프라인 복원, 공간 효율적인 스냅샷을 통한 포렌식을 지원합니다.

퓨어스토리지는 랜섬웨어 공격 해결을 지원하는 세 곳의 주요 백업 기술 파트너를 보유하고 있습니다. (표 1 참조)

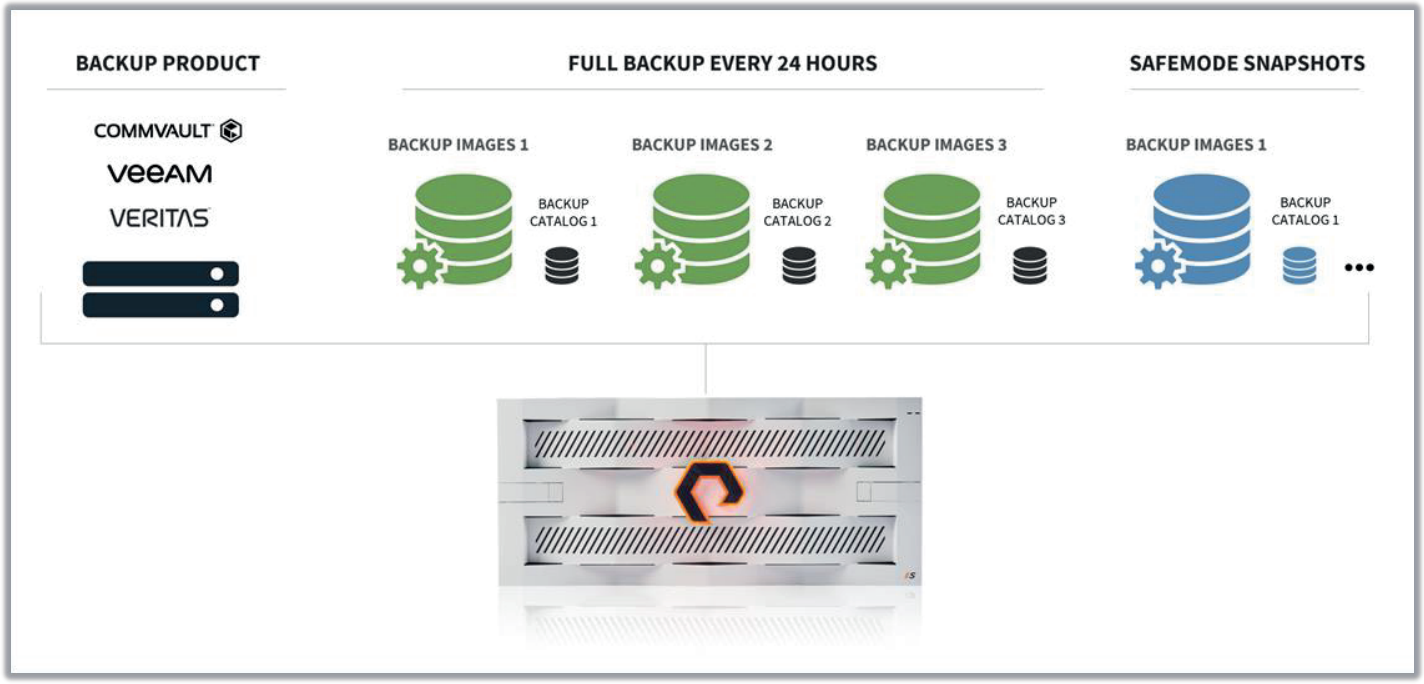
**표 1. 퓨어스토리지의 랜섬웨어 솔루션**

| | 플래시어레이//C | 플래시블레이드//S | 플래시리커버 |
|---|---|---|---|
| **TAP 파트너** | Veeam | Commvault | Cohesity |
| **설치 공간** | Veeam섀시용 3U, 쉘프당 3U, 9U에서 최대 2.3PB 원시 용량 (퓨리티 6.3.2 이상 설치) | 5U 섀시, 원시 용량 최대 1928TB | 4RU로 64TB의 가용 용량 지원에서 40RU까지 확장하여 9PB의 가용 용량 지원 가능<br><br>2RU 단위로 증가되는 분리 아키텍처를 통해 제약 없이 필요한 모든 빠른 복원 요구 충족 및 적정 컴퓨팅 규모 산정 |
| **성능** | 시간당 최대 10TB 복원 | 블레이드 수에 따라 확장 복원 가능 및 데이터 이동 시간당 10TB | 블레이드 수에 따라 확장 복원 가능 및 데이터 이동 시간당 10TB |
| **연결성** | 블록, IP | IP | IP |
| **프로토콜** | 블록, NFS | S3 | NFS |

*출처: TechTarget, Inc.의 사업부 ESG*

퓨어스토리지를 사용하면 플래시블레이드(FlashBlade)와 플래시어레이(FlashArray)를 구동하는 퓨리티(Purity) 운영 환경에 내장된 퓨어 세이프모드(SafeMode) 기능을 통해 랜섬웨어 공격을 완화할 수 있습니다. 이를 통해 조직은 Commvault, Veeam 또는 Veritas 데이터 보호 소프트웨어를 사용하여 전체 백업을 수행한 후, 애플리케이션 데이터, 백업 및 관련 메타데이터 카탈로그에 대한 읽기 전용 스냅샷을 생성할 수 있습니다. 세이프모드 스냅샷은 변경, 암호화 또는 삭제가 불가능합니다. 세이프모드로 지원되는 복사본은 권한이 있는 사람만 퓨어스토리지의 기술 지원팀과 함께 수동으로 액세스, 삭제 또는 변경할 수 있습니다. 이를 통해, 자동 설정, 간편한 설치, 복구용의 깨끗한 복사본 제공 등 가상 에어 갭을 확보할 수 있습니다. (그림 2 참조)

그림 2. 퓨어스토리지 랜섬웨어 솔루션 개요




*출처: TechTarget, Inc.의 사업부 ESG*

세이프모드는 다음과 같은 이점을 제공합니다.

- **보호 강화:** 랜섬웨어는 세이프모드로 생성된 스냅샷을 (삭제), 폐기, 수정 또는 암호화할 수 없습니다.
- **백업 통합:** 백업은 데이터 보호 프로세스를 관리하는 데 사용되는 백업 제품 또는 네이티브 유틸리티에 관계없이 동일한 스냅샷 프로세스를 사용합니다.
- **애플리케이션 데이터 보안:** 네이티브 데이터베이스와 애플리케이션의 백업을 보호합니다.
- **유연성:** 스냅샷 케이던스와 폐기 일정은 사용자 지정이 가능하며 설정이 쉽습니다.
- **신속한 복원:** 데이터와 함께 확장되는 대규모 병렬 아키텍처와 탄력적인 성능을 활용하여 백업 및 복구 속도를 가속화할 수 있습니다.
- **투자 보호:** 플래시블레이드와 플래시어레이에는 모두 세이프모드 기능이 내장되어 있기 때문에 추가 비용이 들지 않습니다. 기존 퓨어스토리지 서브스크립션이나 유지보수 지원 계약에는 지속적인 개선이 포함됩니다.
- **호환성:** 세이프모드는 Commvault, Rubrik, Veeam, Veritas의 다양한 데이터 보호 솔루션과 원활하게 통합됩니다.

## ESG 기술 검증

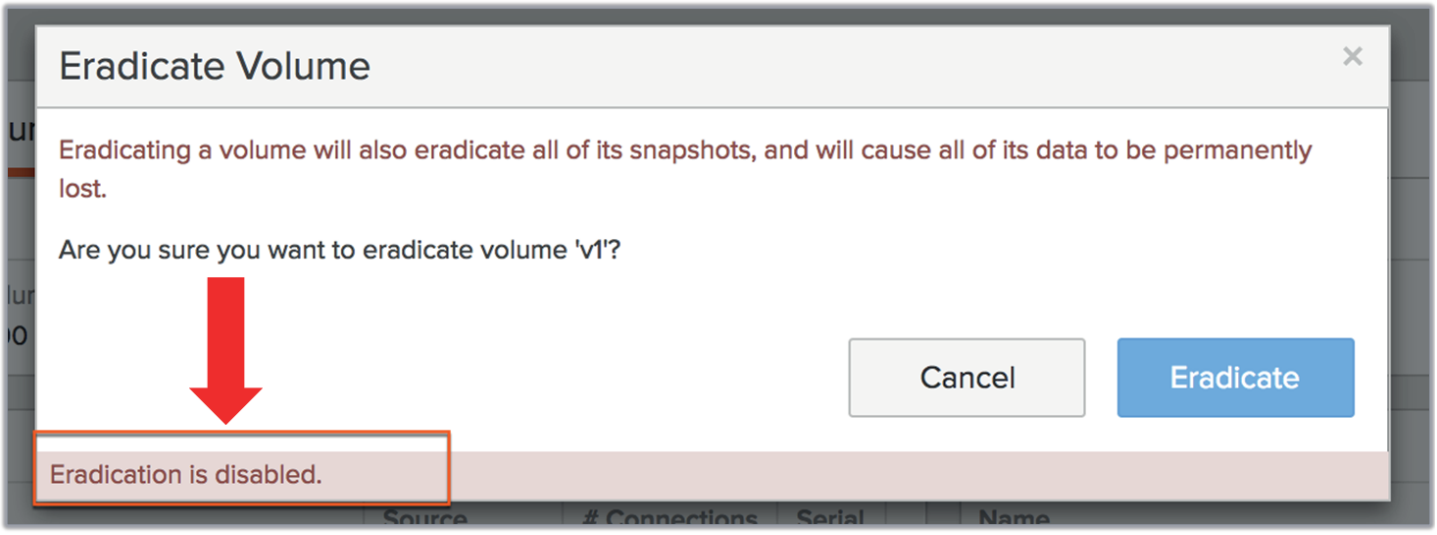
ESG는 랜섬웨어 공격 후 복구에 초점을 맞춰 퓨어스토리지 랜섬웨어 솔루션의 기술적 검증을 수행했습니다. 여기에는 멀웨어 제거를 위한 오프라인 복구, 우선순위 시스템을 위한 신속한 복구, 공간 효율적인 스냅샷을 통한 포렌식 지원 등이 포함됩니다.

### 멀웨어 제거를 위한 오프라인 복원

공격이 진행되는 동안 조직은 손상된 네트워크 시스템을 격리, 연결 해제 및 정리해야 합니다. 공격이 끝나면 조직은 네트워크에 있는 모든 시스템을 철저히 점검하여 아티팩트나 멀웨어가 남아 있지 않도록 해야 합니다. 이러한 단계는 조직이 여러 시스템을 종료하고 마이그레이션을 수행하여 데이터를 복원한 다음 네트워크를 다시 온라인 상태로 전환하여 자동화된 랜섬웨어가 재활성화 하는 것을 방지하는 데 도움이 됩니다. 따라서 조직에서는 백업에서 데이터를 복원하고 가동 준비가 되기 전 환경을 완전하게 '소독'해야 합니다.

퓨어스토리지는 랜섬웨어 공격자의 암호화로부터 데이터를 안전하게 보호된 방식으로 저장하며, 다중 인증 방식을 활용하여 관리자 액세스 권한을 보유한 사용자나 프로세스가 퓨어스토리지 지원 팀의 수동 상호 작용과 개입 없이 데이터를 완전히 삭제할 수 없게 합니다. 예를 들어 그림 3에서처럼 스냅샷 삭제(영구 폐기)가 비활성화됩니다.

그림 3. 비활성화된 스냅샷 삭제




*출처: TechTarget, Inc.의 사업부 ESG*

## 이것이 중요한 이유

ESG의 설문 조사에 따르면, 2022년에 조직들이 가장 크게 지출을 증가할 계획인 사이버 보안 영역은 클라우드 애플리케이션 보안(응답자의 62%)과 데이터 보안(58%)이며, 클라우드 인프라 보안(56%)이 그 뒤를 따랐습니다. 이는 사이버 보안에 대한 총체적인 접근 방식을 취함으로써 지속적으로 급증하고 있는 랜섬웨어 공격을 포함해 점점 증가하는 보안 위협으로부터 조직을 보호하는 것이 얼마나 중요한지를 보여줍니다.

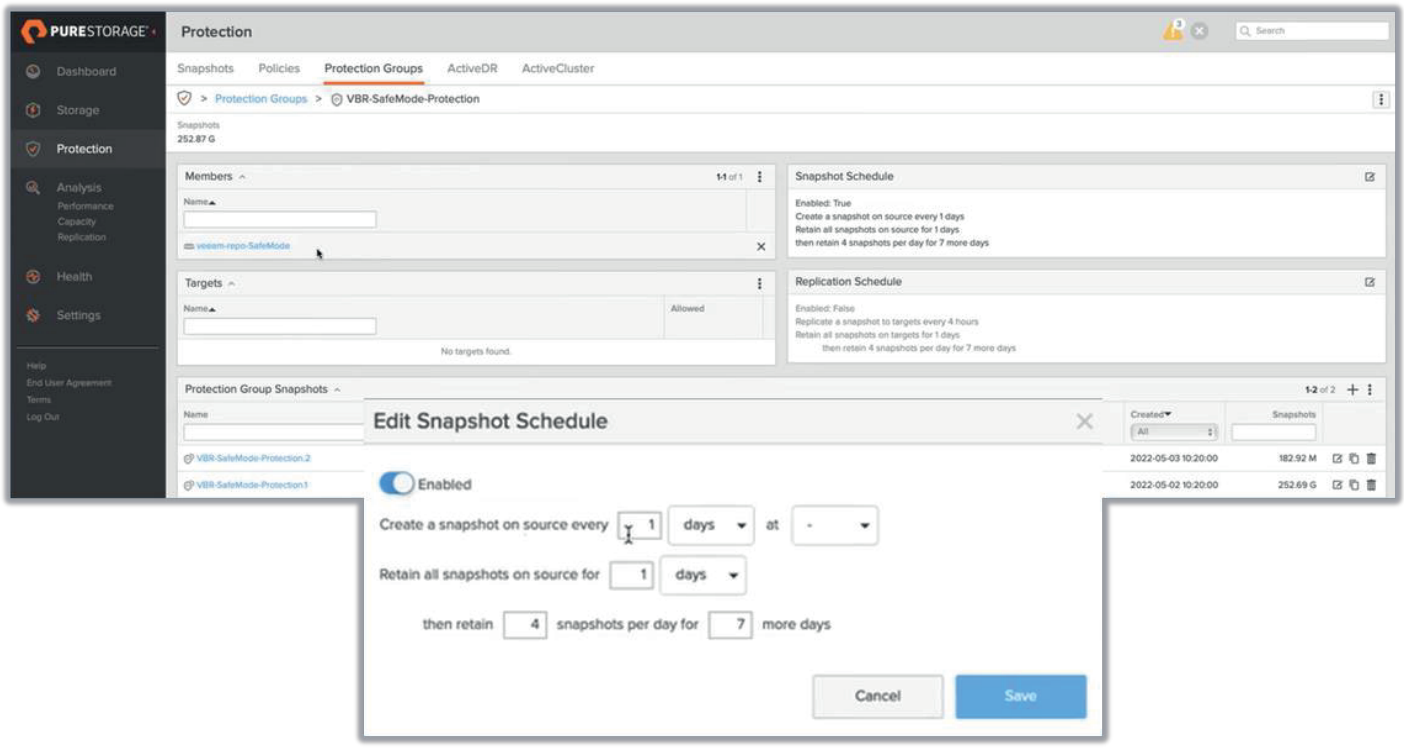
## 우선적인 시스템을 위한 빠른 복원

플래시어레이, 플래시블레이드, 또는 플래시리커버(FlashRecover)에 내장된 퓨어스토리지의 세이프모드는 변경할 수 없는 스냅샷 등 관리자의 실수 또는 악의적인 공격으로 인한 데이터의 영구적 손실을 방지합니다.

또한 플래시어레이는 운영 데이터의 변경 불가능한 보호 기능(운영의 경우 10~30일 이상)과 운영 데이터의 즉각적인 스냅샷 롤백 또는 플레시어레이//C당 시간당 최대 8.7TB의 복구 역량을 지원합니다. 퓨어스토리지의 플래시블레이드는 변경할 수 없는 파일 시스템 보호 기능(최대 400일까지 데이터베이스 덤프 및 백업)과 즉각적인 파일 시스템 스냅샷 롤백 또는 시간당 최대 270TB의 대규모 복구 역량을 제공합니다. 또한, Cohesity 기반의 플래시리커버는 변경 불가능한 데이터보호 기능과 1,000개 이상의 가상머신(VM)을 3.5시간 내에 또는 하루당 1PB 이상 복구할 수 있습니다.

그림 4는 관리자가 세이프모드 보호 그룹을 설정하고 구성원(이 경우 Veeam 저장소)을 추가할 수 있는 퓨어스토리지 Protection 화면을 보여줍니다. 관리자는 매일 스냅샷 소스를 생성하는 등 스냅샷 스케줄을 설정하고 X일 동안 소스에 모든 스냅샷을 보존할 수 있습니다.

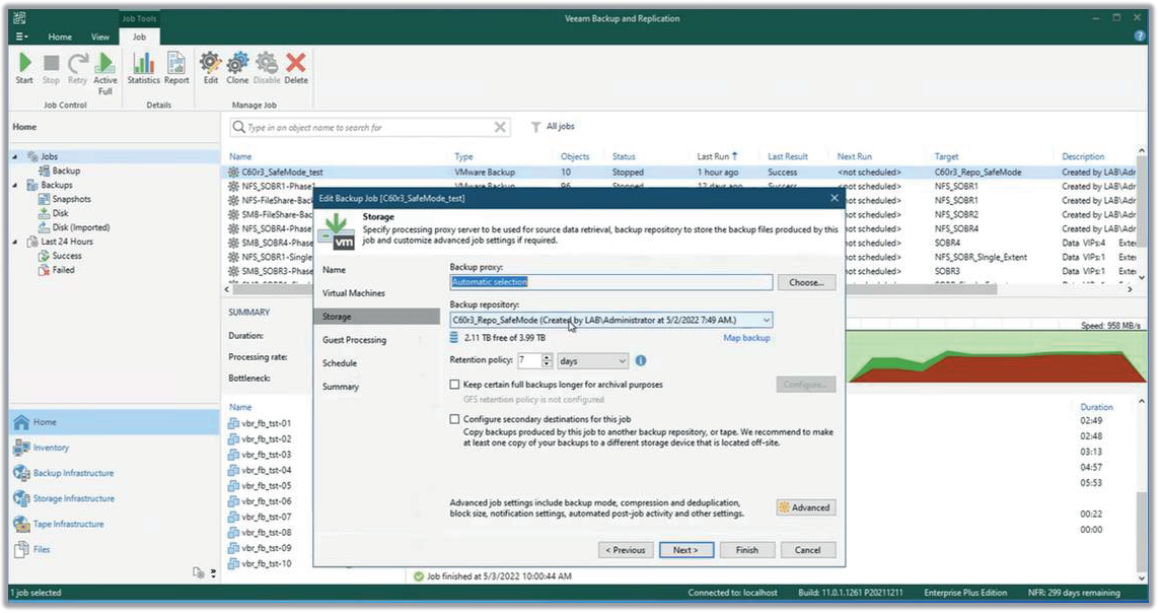
그림 4. 세이프모드 보호 그룹 설정




*출처: TechTarget, Inc.의 사업부 ESG*

그림 5는 백업 프록시, 백업 저장소 및 보존 정책(이 경우 7일)을 포함하는 Veeam 백업을 보여줍니다.

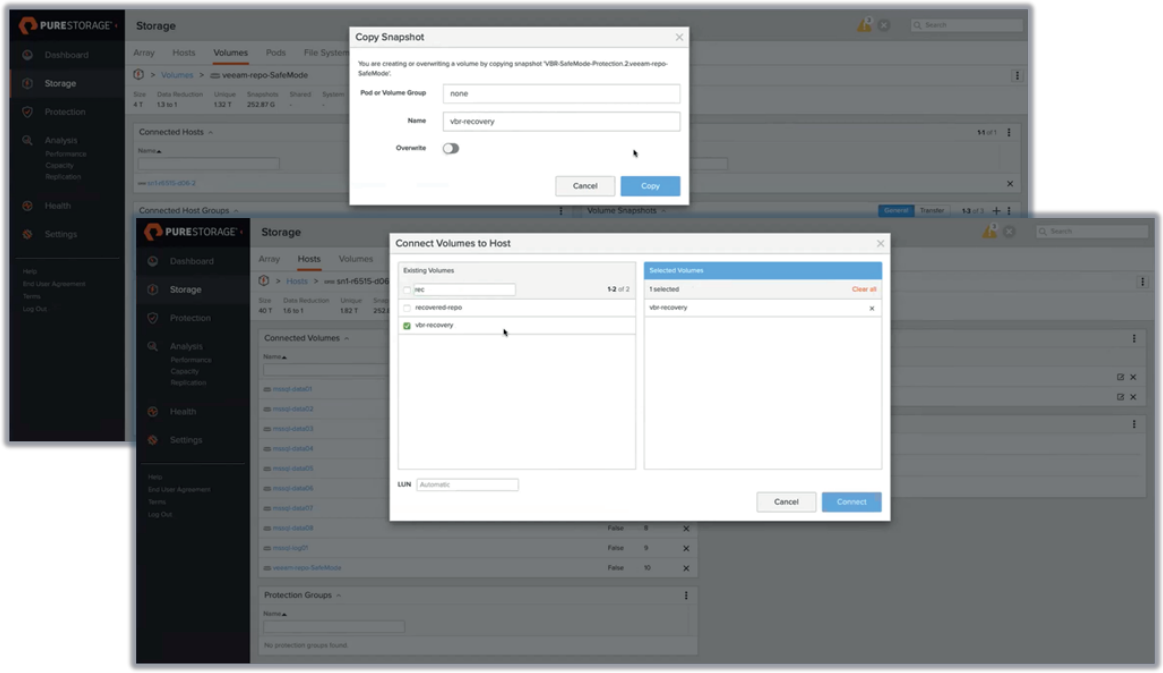
그림 5. Veeam 백업 작업




*출처: TechTarget, Inc.의 사업부 ESG*

그림 6은 랜섬웨어 공격을 받은 조직이 스냅샷을 일반 볼륨에 신속히 복제하고 호스트에 연결하는 방법을 보여줍니다.

그림 6. 신속한 복구 복사 및 연결




*출처: TechTarget, Inc.의 사업부 ESG*

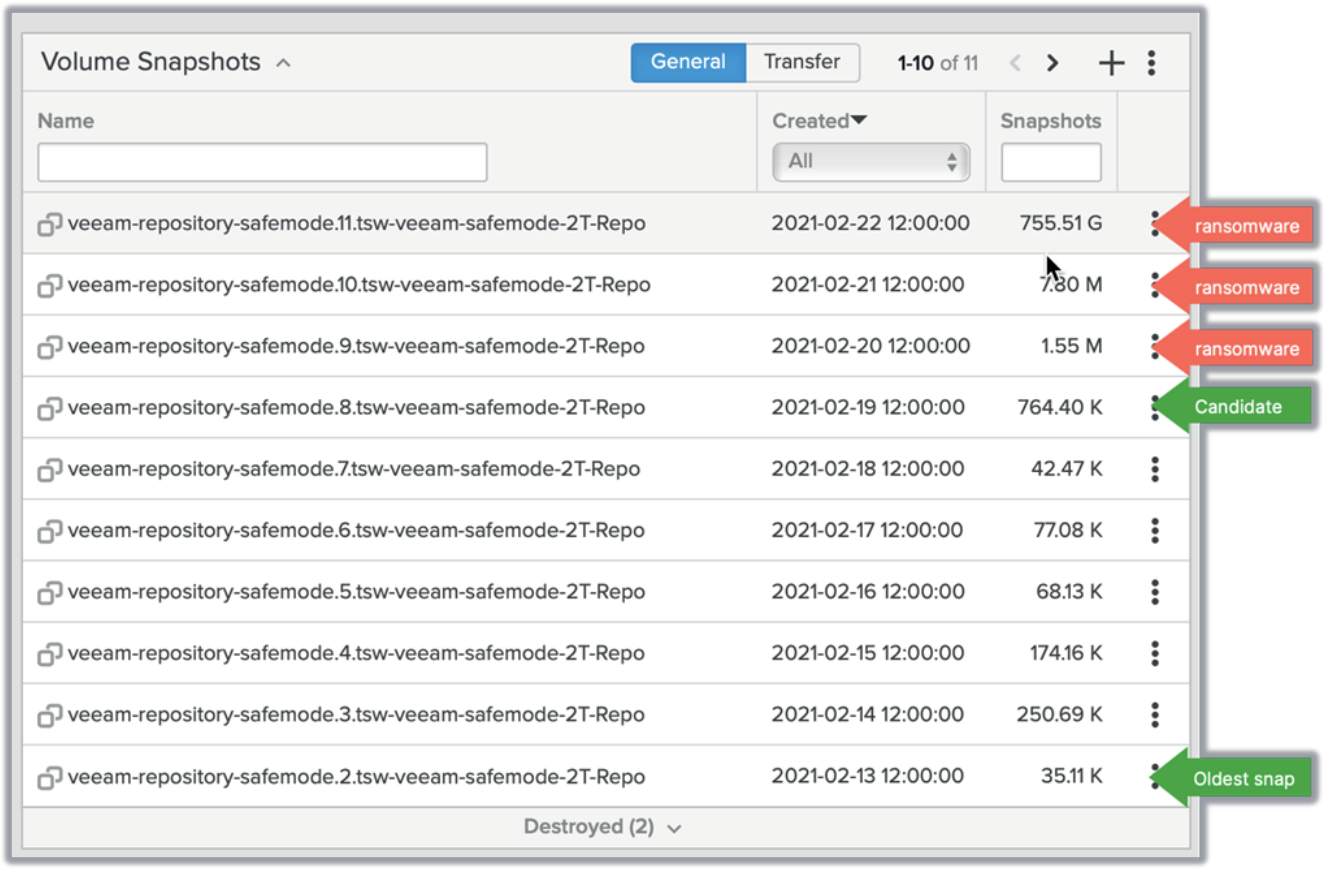
## 이것이 중요한 이유

보안 위협이 지속적으로 증가하고 있다는 점을 감안하면, 2022년 IT 투자를 정당화하는 데 가장 중요한 고려 사항을 묻는 질문에 '사이버 보안 개선'이 설문 조사 응답자(44%)들 사이에서 가장 보편적인 대답이었다는 점은 은 놀라운 일이 아닙니다. 퓨어스토리지는 우선적인 시스템에 대한 신속한 복구를 제공하여 사이버 보안을 개선하는 데 도움을 줍니다.

### 공간 효율적인 스냅샷을 통한 포렌식 지원

또한 스냅샷 및 백업 데이터의 포렌식 분석에 사용할 수 있는 적절한 샌드박스 환경을 갖추는 것도 중요합니다. 포렌식 리뷰와 클린징을 수행하여 공격자가 남긴 확인된 손상 징후를 제거해야 직접 복원할 수 있습니다. 복원 과정에서 적절한 가시성을 제공하는 견고한 로깅 환경을 갖추는 것이 중요합니다. 퓨어스토리지는 조직이 복구성을 위한 출발점을 확보하고 시스템을 신속하게 백업 및 실행할 수 있는 빠른 복구 솔루션을 제공합니다. (그림 7 참조)

그림 7. 일별 저장소 스냅샷 분석




*출처: TechTarget, Inc.의 사업부 ESG*

## 이것이 중요한 이유

높은 심각성 때문에 랜섬웨어 공격을 차단하는 것은 기업의 최우선 과제 중 하나입니다. 백업하고 운영을 재개한 후, 조직은 발생한 상황을 검토하고, 이를 통해 배우고, 그에 따라 시스템과 정책을 수정하여 조직이 학습한 대로 계속 운영할 수 있도록 하는 것이 중요합니다. 이러한 사후 평가에서는 기술 뿐 아니라 사람과 과정도 고려해야 합니다. 퓨어스토리지는 포렌식 검토를 수행하여 공격자가 남긴 멀웨어를 식별 및 제거하여 성공적인 복원을 가능케 합니다.

### 더 큰 진실

기업은 랜섬웨어 공격이 발생하는 이유와 방법을 이해하고, 공격 전과 도중, 공격 후에 해야 할 일을 파악해야 합니다. 이를 통해 공격이 발생하지 않도록 대비하거나 신속하게 복구할 수 있습니다.

이러한 조치에는 적절한 인력, 프로세스 및 기술을 사용하는 것이 포함되어야 합니다. 이외에도 조직은 강력한 암호를 설정하고 제대로 관리해야 하며 소프트웨어 및 자산의 인벤토리를 구축하여 이를 보호하고 공격 표면을 최소화해야 합니다.

ESG는 이번 분석을 통해 퓨어스토리지 랜섬웨어 소프트웨어 솔루션이 멀웨어 클렌징을 위한 오프라인 복원, 우선순위 시스템의 신속한 복구, 공간 효율적인 스냅샷을 통한 포렌식 지원을 비롯해 공격 전후 및 도중에도 랜섬웨어 보호를 제공한다는 점을 확인하였습니다.





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