STONEFLY

공용스토리지(NAS), 해커의 집중 공격 대상이 되고 있다

최성재
스톤플라이 코리아 지사장

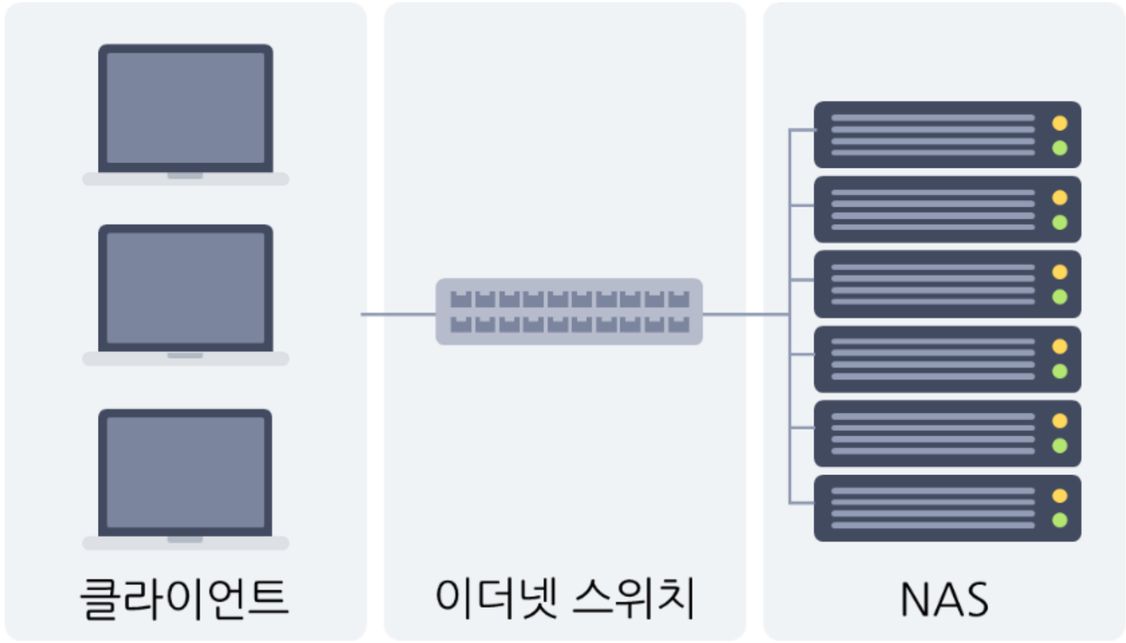
HiZEN
Service for human

CONTENTS

STONEFLY

NAS (Network Attached Storage)

- NAS (Network Attached Storage)란?
  - 네트워크에 연결되어 중앙 집중식으로 데이터를 저장하고 공유하는데 사용되는 스토리지 저장장치
- NAS (Network Attached Storage) 용도
  - 파일 공유
    - 사내외 협업을 위한 파일 공유
    - 프로젝트 파일 공유 등
  - 백업 저장소
    - 백업 및 아카이빙 용도로 사용
  - 웹 호스팅
  - 미디어 스트리밍
  - 어플리케이션 서버
  - 컨테이너 각종 레포지토리



NAS 보안가이드 - KISA

- 배경
  - 2021.8 정부 랜섬웨어 대응 강화방안
  - KISA에서는 중소기업의 정보시스템 보안수준 제고를 위해 원격 보안 점검 서비스 제공
  - 다수의 기업에서 랜섬웨어 공격을 대비해 nas를 백업 저장 매체로 운영
- 필요성
  - NAS는 기업 및 개인정보 등 중요 정보 저장소
  - 해킹에 취약점을 공격하는 랜섬웨어 발견
  - 해커들의 주요 공격 목표
  - 2024.2 보안 가이드 발표

NAS 서버 보안의 중요성

- ✓ 중요 데이터의 보호
- ✓ 개인 정보 보호
- ✓ 랜섬웨어 공격 방지
- ✓ 규정 준수 및 비스니스 연속성 보장

보안 정책,교육,모니터링 통해 위협 최소화
보안에 최적인 NAS를 고려

NAS 서버 보안 위협 요소

- ✓ 악성코드 (랜섬웨어 등) 감염
  - ✓ 파일을 중앙에서 관리하므로 확산 및 주요 공격 대상
- ✓ 데이터 유출
  - ✓ 취약한 암호와 접근제어로 인해 악의적으로 무단 접근 및 탈취
- ✓ 데이터 위변조
  - ✓ 데이터 위변조를 통해 중요 데이터 손실

NAS 서버 대상 해킹 사례

전 세계 웨스턴디지털 NAS 기기에 대한 데이터 삭제 공격 (21.6.28)

해킹을 통한 공장 초기화

대학.기업.연구소 원격 저장장치 해킹 피해(21.12.27 YTN)

연구 업무용 자료등 민감한 자료를 랜섬하고 금전 요구

큐냅과 시놀로지등 다수의 취약점 (22.5.2)

다량의 취약점 발견, 오픈 소스 파일 서버의 취약점 공격

DeadBolt 랜섬웨어 (22.9.5)

SynoLocker, Qloacker, eCh0raix 랜섬웨어 등 지속적인 새로운 공격 및 변종

NAS 서버 보안의 취약점

취약점	상세내용
 약한 인증 및 취약한 비밀번호 사용	사용자 및 관리자의 암호가 간단하거나 약하게 설정된 경우, 공격자가 더 쉽게 시스템에 접근할 수 있다.
 암호화 부재	데이터가 암호화되지 않는 경우, 물리적 또는 원격 공격자가 데이터를 읽을 수 있다.
 소프트웨어 취약점 및 부족한 보안 업데이트 관리	NAS 시스템의 운영 체제, 앱 및 소프트웨어에 취약점이 발견될 수 있으며, 악용될 가능성이 있다. 보안 패치와 업데이트를 적용하지 않으면 취약점이 그대로 남아있을 수 있다.
 접근권한 및 파일공유 설정 오류	접근권한이 부적절하게 설정되거나 최소한으로 관리되지 않는 경우, 허가되지 않은 사용자가 데이터에 무단으로 접근할 수 있다. 파일 공유 설정이 부적절하게 구성되어 있는 경우, 중요한 데이터가 무단으로 공유될 수 있다.
 미처리된 공개 포트	미처리된 공개 포트로 인해 접근 제어가 부족하게 되어 공격자의 진입이 가능해질 수 있다.
 사용자 실수로 인한 악성코드 감염	사용자 부주의로 인해 악성 소프트웨어가 다운로드되거나 설치될 수 있으며, 데이터 손실 및 네트워크 감염의 위험을 초래할 수 있다. 특히 사용자를 속여 악성 링크를 클릭하게 만들거나 인증 정보를 빼내는 사회 공학 기술이 사용될 수 있다.

- 약한 인증 및 취약한 비밀번호 사용
- 암호화 부재
- 소프트웨어 취약점 및 업데이트 관리 부족
- 접근 권한 및 공유 설정 오류
- 미처리된 공개 Port
- 사용자 실수에 의한 악성코드 감염

* 출처: NAS 보안 가이드 - KISA

NAS 서버 보안 가이드

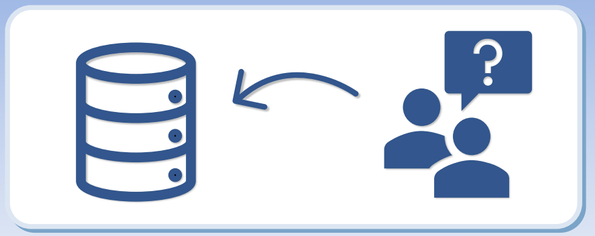
- 암호화 사용
- 접근제어 및 권한 관리
- 네트워크 보안
- 펌웨어 및 소프트웨어 업데이트
- 백업 및 복원 전략
- 감사 로깅 및 모니터링
- 업데이트된 안전한 앱 사용
- 랜섬웨어 방지

* 출처: NAS 보안 가이드 - KISA

일반 스토리지 보안 취약점

1. 비 인가자의 스토리지 접근에 취약

- 비인가자의 스토리지 관리 콘솔 접근(Web 방식)
- 비인가 된 Application의 접근 통제 불가능

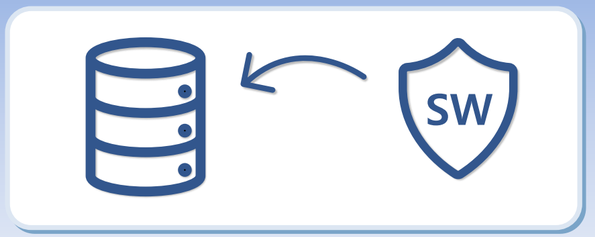


2. 스토리지 데이터의 안정적 보관 방법에 제약

- 삭제, 변조, 랜섬 등 **다양한 해킹에 대해 데이터 보관 기술의 한계**
- 변조나 삭제가 가능한 Snapshot 및 복제 등 이용

3. 보안 강화를 위해 기능별 별도의 솔루션 제공

- 보안을 위한 별도의 솔루션 별도의 솔루션이 필요
- 접근제어, Password 관리, 백신 등



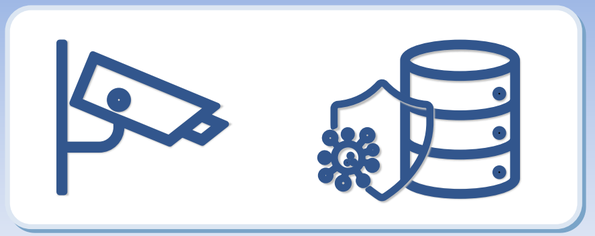
스토리지 보안 전략

1. 물리 및 논리적 보안

- 스토리지 업계 최초의 물리적 보안
- Air Gap Fabric 미국 특허 출원 / 스토리지 격리를 통한 보호

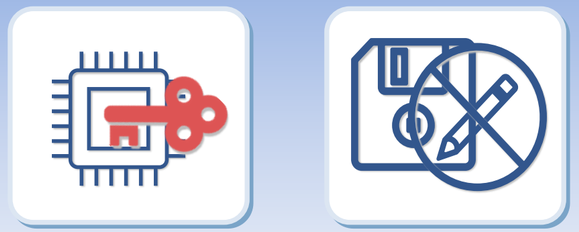
2. 실시간 감시

- 해킹 및 데이터 변조에 대한 실시간 감시
- 바이러스 **멀웨어 및 랜섬웨어 방지**



3. 데이터 변조 방지

- WORM 기능 **위/변조, 삭제할 수 없도록** 하는 스토리지 기능
- Object Lock down 데이터를 소프트웨어 설정 (논리적으로 분리)

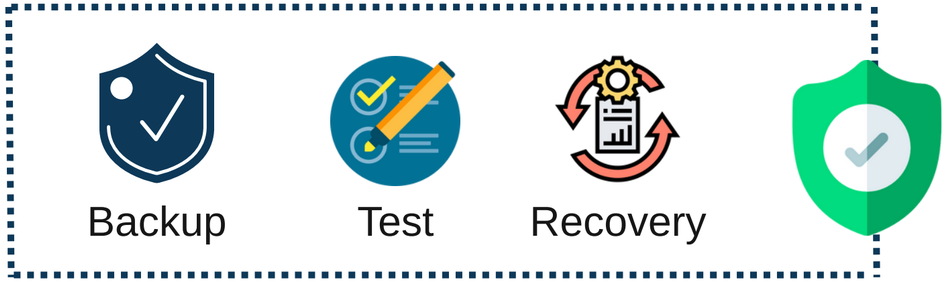


스톤플라이 소개

- 2000년 설립 (iscsi protocol 개발 업체)
- 20년 이상 SDS(storage define software)개발
- SAN/NAS/Object Storage등 고객의 모든 스토리지 Infra 지원
- 가장 강력한 Secure 아키텍처 지원

Data Center in the Box

하나의 시스템에서 모든 기능을 수행



Cybersecurity framework

스톤플라이는 미 NIST에서 규정을 준수합니다

" Cybersecurity Framework 2.0 준수"

Framework version 2.0

National Institute of Standards and Technology
U.S. Department of Commerce

미국 연방수사국(FBI)
미국 국방정보시스템기구
미국 국방정보국
미국 항공우주국
미국 국방부
미국 해군
미국 해병
미국 국토안보부

IT 보안을 위해 NIST에 규정한 표준 보안 프레임웍을 지원
(미 국방정보국등 다수 군 관련 고객사에
보안 프레임웍 준수 검증 후 납품 및 구축)

보안 – 스토리지

THREE TIERS OF STORAGE

1

SAN

블록 모드도 백업
레포지토리 및 DB를 저장
– 고성능 I/O 제공

2

NAS

네트워을 통해 백업 및
백업 데이터 복구 및
공유 지원

3

S3 Object Storage

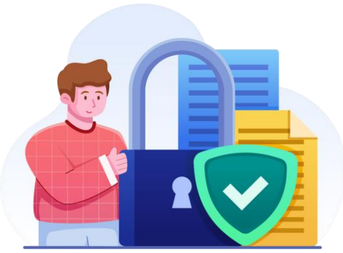
백업 및 아카이빙을 위한
오브젝트 스토리지 지원,
스톤플라이 자체
오브젝트 스토리지 및
AWS/Azure, S3호환
스토리지를 지원

스톤플라이 랜섬웨어 보호 기술

1. Air-Gap & Immutable storage

2. Volume Deletion Protection

3. MFA (Multi-Factor Authentication)



4. Immutable File-Level WORM

5. Immutable Snapshot

6. Anti-Virus Scanner

7. Object Lock Down

8. Recycle bin

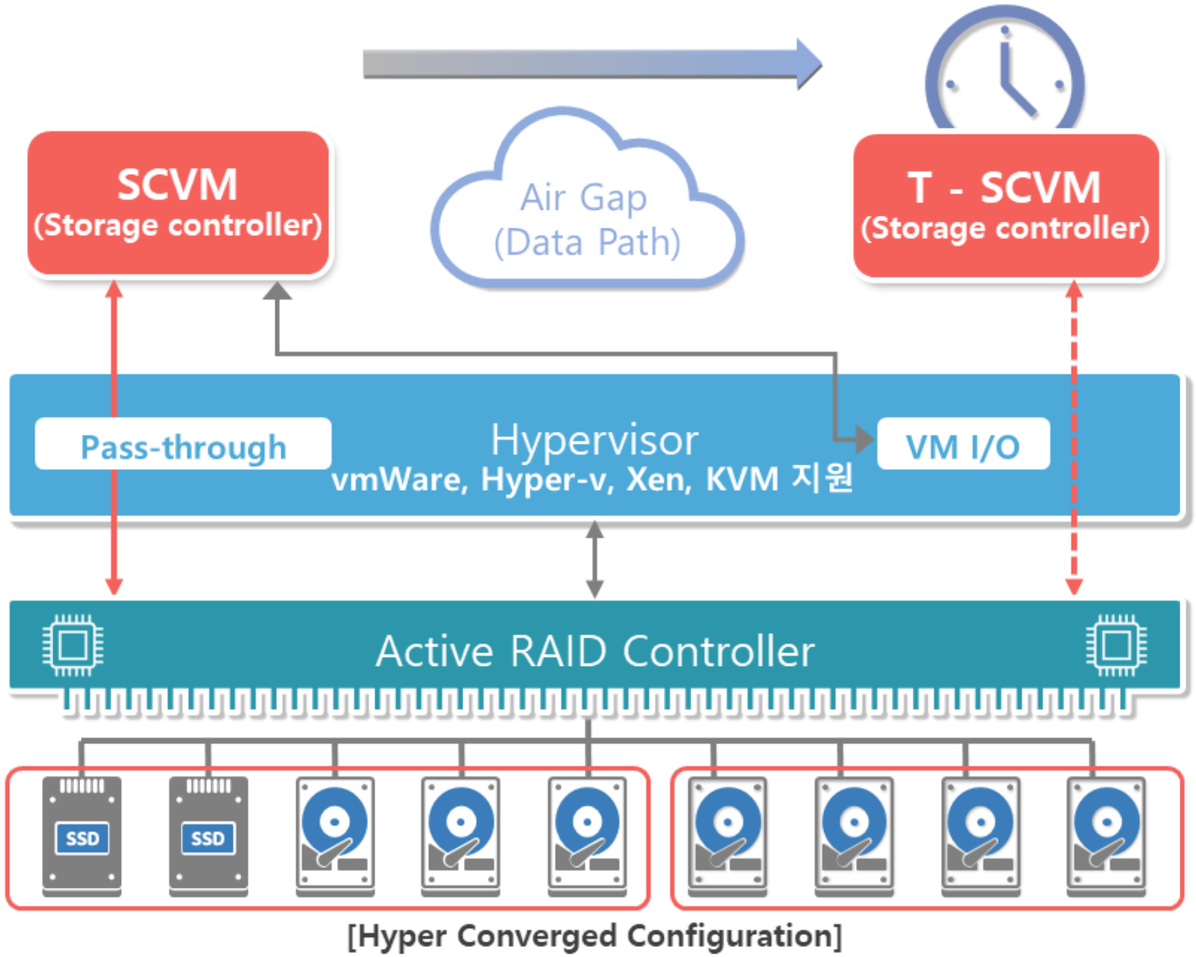
1. Air-Gap & Immutable Storage

- **목적**
  * 랜섬웨어, 멀웨어, 해커,
    바이러스로부터 데이터를 보호

- **효과**
  * Air-Gap을 통한 백업 데이터의 격리
  * 위변조 불가 속성을 이용하여 삭제 및 변조 불가

- **구조**
  * Repository Level
    - 백업 레포지토리를 격리
  * Controller Level
    - StoneFusion 컨트롤러 레벨에서 격리
  * Node Level
    - 물리적 노드간의 분리를 통한 격리

1. Air-Gap & Immutable Storage



[Hyper Converged Configuration]

#1

Air Gap 이 중간에 생성되고
데이터는 왼쪽에서 오른쪽으로 주기적으로 복제

#2

외부에서 T-SCVM 은 이더넷 연결이 단절된
상태로 보이므로 **스토리지의 존재 여부를 알 수 없다.**

#3

SCVM 스토리지의 저장 파일들이 바이러스 및
해커에 의해서 손상 될 경우 **다운 타임 없이**
바로 T-SCVM 를 으로 넘어 갈수 있다.

물리적으로 스토리지간 Air Gap 백업 가능

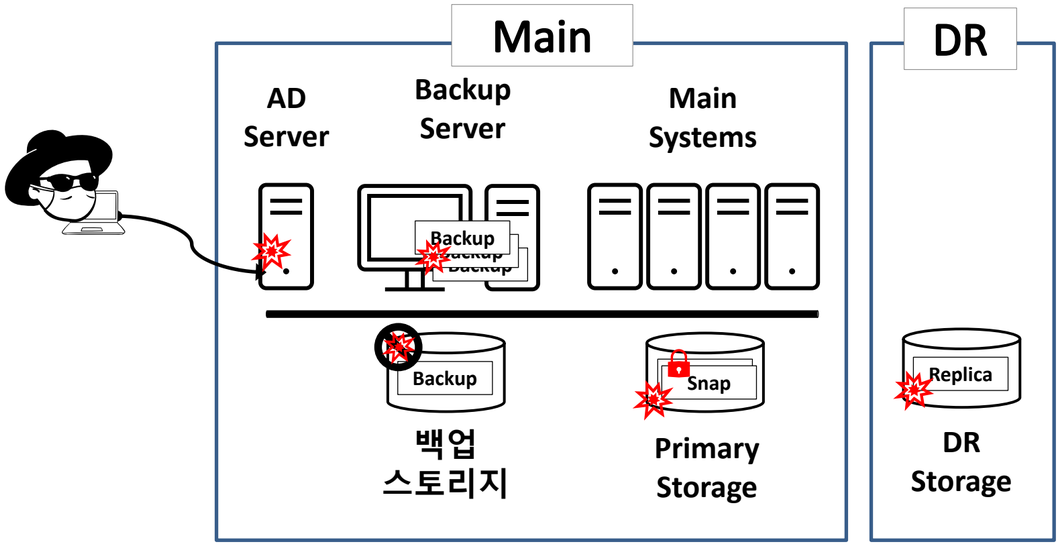
2. 볼륨 삭제 방지 기능

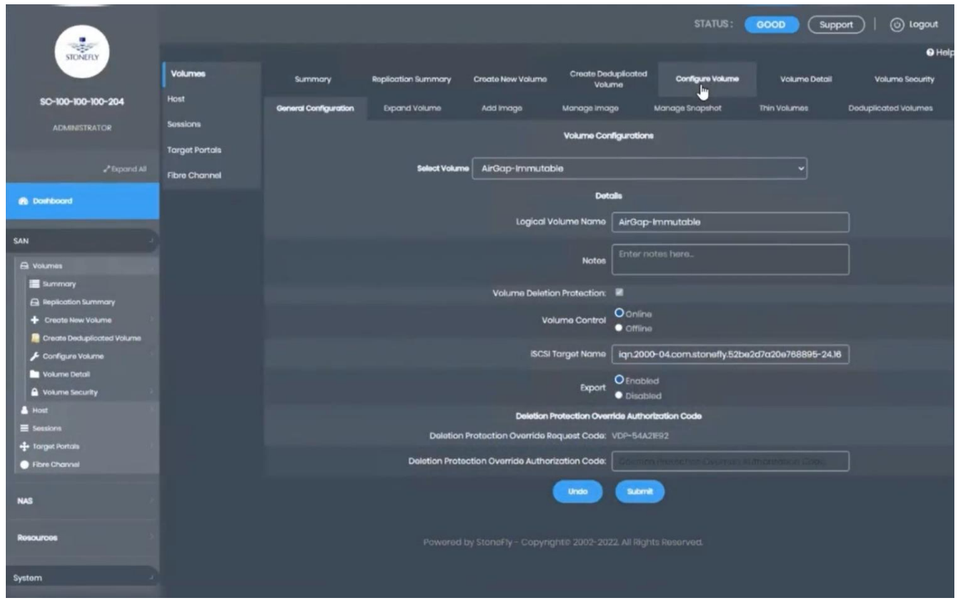
- **목적**
  * 랜섬웨어, 멀웨어, 해커,
    바이러스로부터 볼륨 보호

- **효과**
  * 해킹 또는 관리자의 실수에 의한 볼륨 삭제를 방지
  * 권한을 가진 관리자도 삭제 불가

- **구조 및 동작**
  * 볼륨 생성시 삭제 불가능 옵션 선택
  * 삭제 필요 시 스톤플라이 본사 Tech Support를
    통해 이메일 및 유선 통화를 통해 인증 후
    삭제 코드 수령

2. 볼륨 삭제 방지 기능





- **해커**
  * 백업 데이터/레포지토리 삭제 수행 – 성공
  * 백업 스토리지 해킹: 볼륨 삭제 - 실패
- **스톤플라이 대응**
  * 인가자도 삭제 불가능
  * 볼륨 생성시 삭제 불가로 구성

- 볼륨 생성시 삭제 불가능 옵션
- 고객의 필요에 의해 삭제 요청 시 본사와 이메일 및 전화 통화로 고객 확인 후 삭제 코드 발송

3. 다중 인증 (MFA)

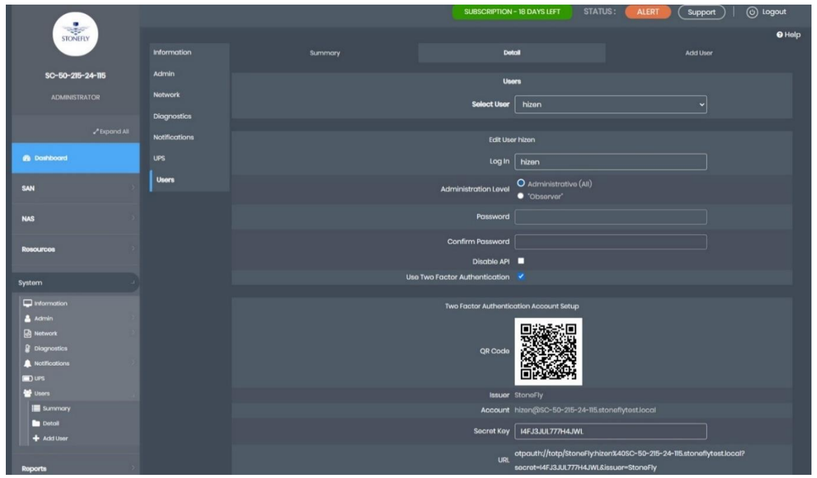
- **목적**
  * 해킹 혹은 운영상의 사고에 의한 패스워드 유출 시에도 완벽히 데이터를 보호

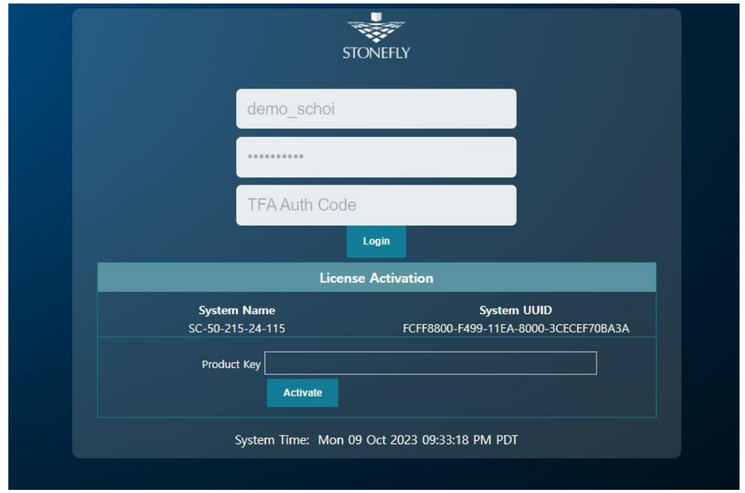
- **효과**
  * 패스워드 유출/악의적인 탈취 등 발생할 수 있는 패스워드 사고에 대비해 다중 인증을 함으로써 데이터를 안전하게 보호

- **구조 및 동작**
  * 콘솔 관리자 및 유저 생성 시 MFA 설정
  * 콘솔 Login시 패스워드 뿐만 아니라 MFA Code 인증 요청
  * Google Authentication 등 다양한 인증 앱과 연동 가능

3. 다중 인증 (MFA)

콘솔 접근을 위해 “다중인증(MFA)”를 이용한 보안 강화





- 유저 생성시 MFA Code 확인
- Google Authentication등 각종 인증 앱 사용 가능

콘솔 로그인 화면

Login 시 암호 및 Code입력

4. Immutable File-Level WORM Storage

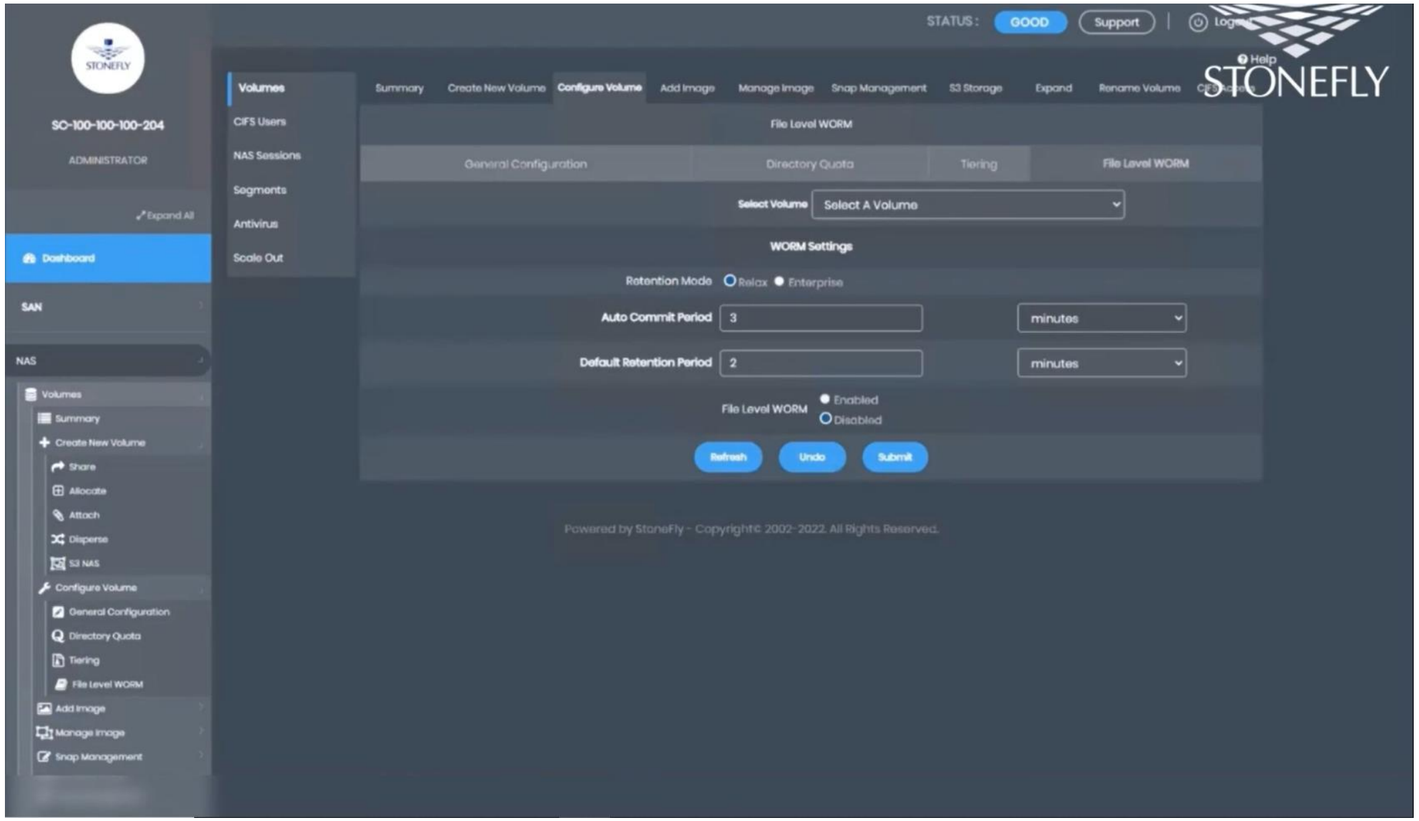
- **목적**
  * 랜섬웨어, 멀웨어, 해커, 바이러스로부터 악의적인 삭제/변조를 방지

- **효과**
  * 해킹 또는 사용자의 실수에 의한 파일 변조 및 삭제를 방지
  * 보관 규정 등 다양한 컴플라이언스에 맞게 원본 파일을 일정 기간 보관하고 저장

- **구조 및 동작**
  * 볼륨 특성에 WORM(Write Once Read Many) 속성 부여
  * 파일의 보관 주기 및 정책 설정
  * 파일 저장 후 변조 삭제 요청 시 에러 발생
  * 보관 기간이 지난 후 삭제 요청 시 삭제 가능

4. Immutable File-Level WORM Storage

- **볼륨 속성**
  * Retention Mode
  * Relax
    – 보관 주기 변경 가능
  * Enterprise
    – 보관주기를 줄이는 것은 불가능
  * Auto Commit Period
    – 파일 생성 후 보관주기 설정이 적용되는 시점
  * Default Retention Period
    – 보관 주기 (초/분/시/일/월/년)



5. Immutable Snapshot

- **목적**
  * 특정 시점의 데이터로 복구

- **효과**
  * 랜섬웨어/해킹에 의해 데이터가 삭제되더라도 피해 발생 전 상황으로 즉각적인 복구 가능
  * 운영 관리의 실수에 의한 데이터 손상 시 즉시 복구

- **구조 및 동작**
  * 해당 볼륨에 Immutable Snapshot Setting
  * Snapshot 주기/보관 주기 셋팅
  * 해당 스냅샷은 보관 주기 동안 삭제 또는 변조를 시도하더라도 불가
  * 볼륨당 64개 Snapshot 최대 8개 볼륨 가능

6. Anti-Virus Scanner

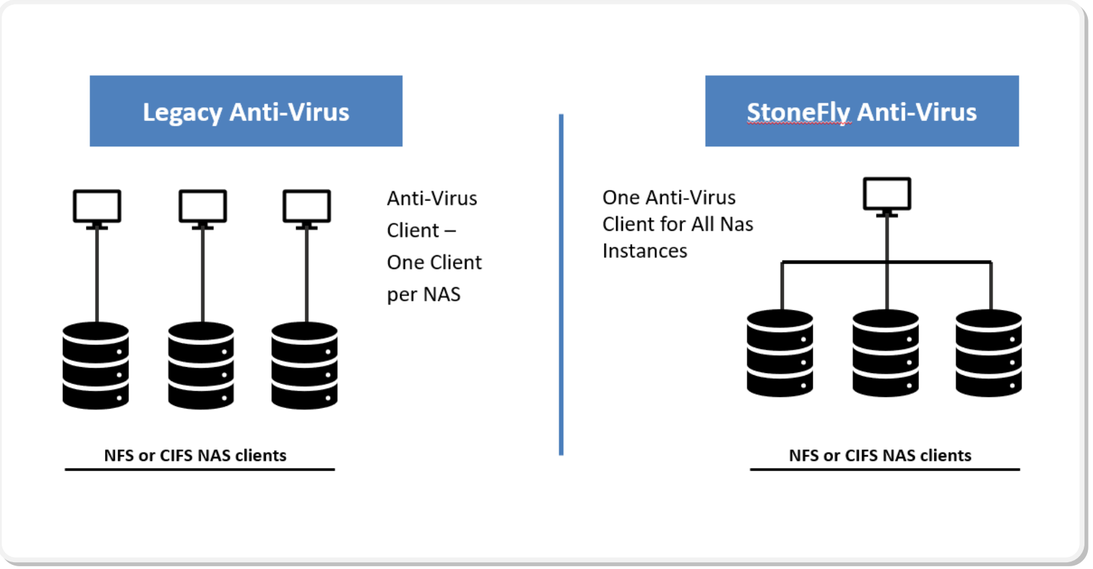
- **목적**
  * 랜섬웨어, 멀웨어등 바이러스로부터 볼륨 보호

- **효과**
  * 다양한 경로로 감염되는 바이러스로부터 보호

- **구조 및 동작**
  * 해당 볼륨에 대한 안티 바이러스 스캔
    – ON
  * Manual / Schedule Scan 선택
  * 바이러스 발견 시
    – Warning/격리/삭제 가능

6. Anti-Virus Scanner

전송 가능한 스토리지로
"데이터 손상" 및 "랜섬웨어"로 부터 자동 데이터 보호



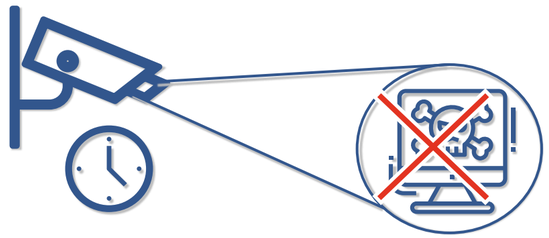
클라이언트의 부하 없음

#1 각 볼륨 별 실시간 혹은 Manual scan 가능

#2 각 볼륨 별 월 / 주 / 일/ 시간별 스케줄 가능

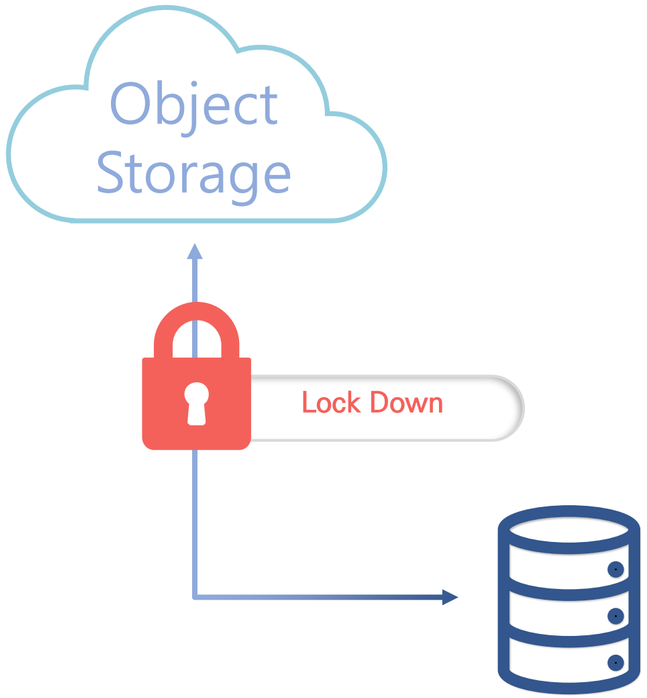
#3 Virus Database Online Update

Ransomware 유형



- Encryption Ransomware
- Lock Screen Ransomware
- Master Boot Record(MBR) Ransomware

7. Object/File Level Lock Down



Object Lock을 사용하여

"WORM 모델을 기반으로 객체를 저장"

#1

저장되어 있는 데이터는 정해진 시간 동안
무기한으로 객체를 삭제 및 덮어쓰지 않도록 할 수 있다.

이 기간 동안 객체는 WORM으로 보호되며 덮어 쓰거나 삭제할 수 없습니다.

#2

법적 보존은 보유 기간과 동일한 보호 기능을 제공하지만,
유효 기간이 없습니다.

법적 보존은 보존 기간과 별개입니다.

대신 명시 적으로 제거 할 때까지 법적 보존이 유지됩니다.

주요 고객사

스톤플라이는 데이터 관리를 위한 전통적인 스토리지 및 클라우드 스토리지 솔루션을 제공합니다.
Fortune 500대 기업을 포함한 3,000개 이상의 고객과 함께하고 있습니다.

마이크로소프트 애저 | 아마존 웹 서비스 | 미국 연방수사국(FBI) | 미국 국방정보시스템기구 | 미국 국방정보국 | 미국 항공우주국

미국 국방부 | 미국 해군 | 미국 해병 | 미국 국토안보부 | 디즈니 | 워너 브라더스

BBC 방송국 | 월드 텔레콤 | 국세청 | 네이버 | 기술보증기금 | 삼성전자

STONEFLY

Any Questions?

(주)하이젠 www.hizen.co.kr 영업문의 : 02-3462-6264 , sales@hizen.co.kr

전시 부스 (하이젠 / 스톤플라이)