STONEFLY

AIR-GAP & IMMUTABLE

Secure Storage

BACKUP AND DISASTER RECOVERY SOLUTION

HiZEN
Service for human

CONTENTS

STONEFLY

보안 위협 - 랜섬웨어와의 전쟁

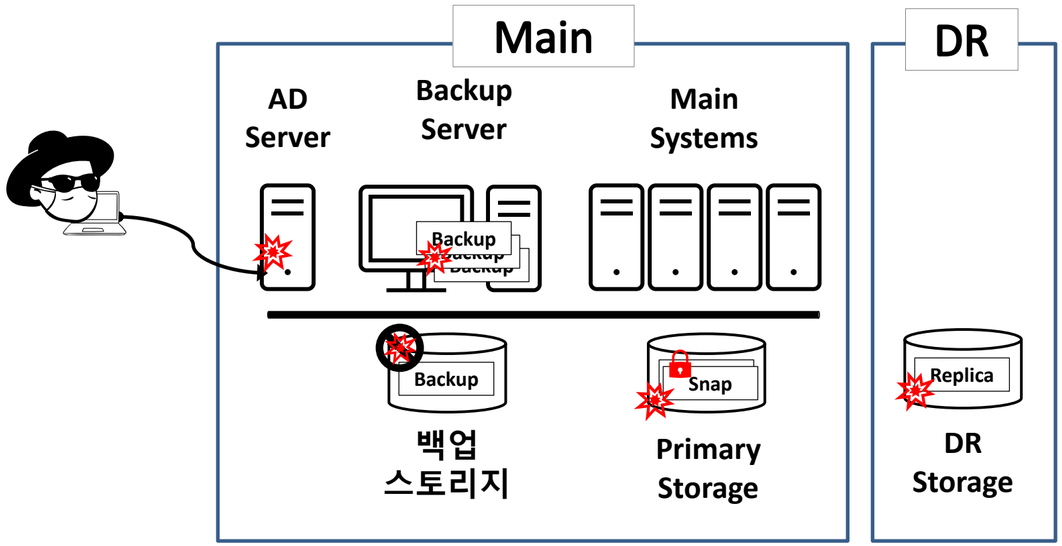
- 경제적 피해 (2021기준)
  - * 92.7% 증가 (2021년 랜섬웨어 공격)
  - * 6조 달러 (랜섬웨어 포함 사이버공격 피해액)
  - * 435만불 (데이터 유출로 인한 피해 업체당 평균)
  - * 국내 평균 업체 당 43억

LGU+, 해킹 대응 시스템 미흡 인정…"보안에 강한 회사 될 것" (2023.2)
https://news.tf.co.kr/read/economy/1999394.htm
전국 콜택시 업무 중단
https://newsis.com/view/?id=NISX20220719_0001948140&cID=10406&pID=13100
의료 기관 공격
https://www.boannews.com/media/view.asp?idx=108971&kind=1
PACS 서버 공격 사례
https://www.boannews.com/media/view.asp?idx=108000&kind=1

랜섬웨어 공격의 특징

- 한국 기업을 표적
  * 22건(2018) , 39건(2019), 127건(2020) 78건(2021 상반기) (출처: Korean Herald)
- 데이터 손실 (78%)
  * 랜섬웨어 공격에 의한 영향 중 데이터 손실이 가장 큰 영향을 미침
  * 생산성 손실(29%) (출처: Statista)
- 기업 네트워크 침투 성공 가능성 (93%)
  * 해커가 기업 네트워크에 침투해 랜섬웨어, 트로이목마, 스파이웨어 배포 (출처 Positive Technologies)
- 백업 저장소 공격에 집중
  * 랜섬웨어 공격의 95%가 백업 저장소 공격
  * 데이터 백업만으로는 데이터 손실을 방어할 수 없음 (출처 VEEAM의 2022년 보고서)

해외 중앙 도서관 보안 사고 사례



- 랜섬웨어를 통해 PC 감염
- Active directory의 제어 탈취
- 백업서버로 로그인하여 모든 백업된 데이터 삭제
- Primary Storage에 대한 로그인 후 스토리지의 스냅샷 삭제
- DR Storage array의 복제(replica) 삭제
- Primary Storage의 Storage LUN 암호화
- 장애 발생 후 암호키에 대한 금액 요구 메일

전형적인 해킹 시나리오

스톤플라이 소개

스톤플라이

캘리포니아 실리콘밸리에 본사를 둔
스톤플라이는 언제 어디서나 사용 가능한
고성능 보안 스토리지 솔루션을 제공하여
데이터 종속 프로세스 및 어플리케이션을
완벽하게 지원하고 있는 스토리지 전문 업체

www.iSCSI.com
www.stonefly.com

클라우드

프라이빗 및 퍼블릭 클라우드에서
블록, 파일, 오브젝트형태의
다양한 스토리지 서비스를 지원하며,
백업, 복제, 재해 복구등 고객의 Needs에 맞는
맞춤형 클라우드 스토리지 서비스 제공

스토리지

엔터프라이즈 iSCSI, 파이버 채널 SAN,
스케일 아웃 NAS 또는 세 가지 모두 선택
가능하며 우수한 성능, 중복성 및 확장성과
통합 모듈식 고 가용성 클러스터 또는
다중 노드 스케일 아웃 구성 제공

백업 & DR

단일 어플라이언스 또는 클라우드 솔루션의
전체 백업 및 재해 복구 솔루션을 제공하며,
하이퍼컨버지드 옵션 사용 시 물리적 시스템을
재해 복구 어플라이언스에서 직접 실행되는
가상 시스템으로 즉시 복구 서비스 제공

하이퍼컨버지드

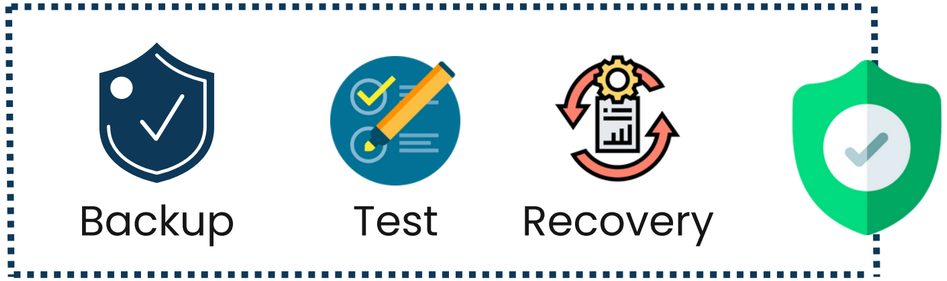
데이터 센터의 모든 서버 및 스토리지 시스템을
관리하기 쉬운 어플라이언스
또는 SAN 게이트 웨이로 통합하고,
가상화를 통해 완전한 하드웨어 활용 및
에너지 소비 절감

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 백업 아키텍처 지원

Data Center in the Box

하나의 시스템에서 모든 기능을 수행



주요 고객사

스톤플라이는 데이터 관리를 위한 전통적인 스토리지 및 클라우드 스토리지 솔루션을 제공합니다.
Fortune 500대 기업을 포함한 10,000개 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

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

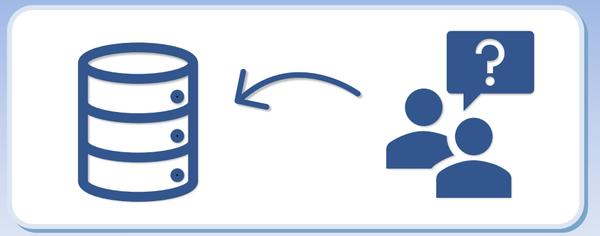
미국 연방수사국(FBI)
미국 국방정보시스템기구
미국 국방정보국
미국 항공우주국
미국 국방부
미국 해군
미국 해병
미국 국토안보부

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

스토리지 보안 취약점

1. 비 인가자의 스토리지 접근에 취약

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

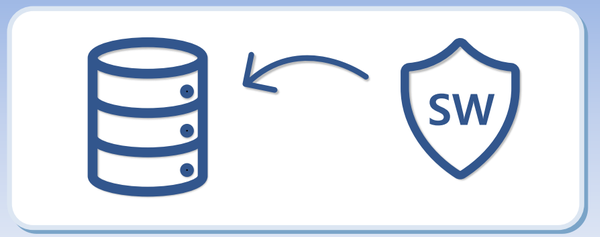


2. 스토리지 데이터의 안정적 보관 방법에 제약

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

3. 보안 강화를 위해 기능별 별도의 솔루션 제공

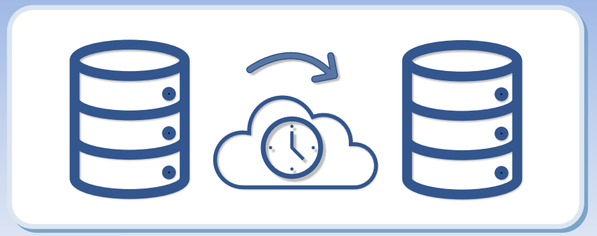
- 보안을 위한 별도의 솔루션이 필요
- 접근제어, Password 관리, 백신 등



스토리지 보안 전략

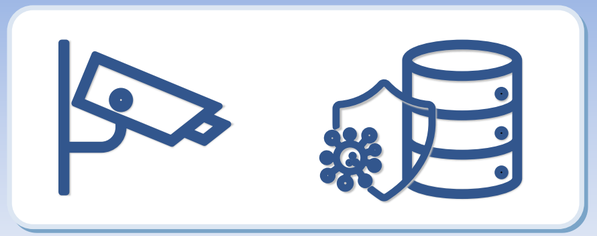
1. 물리 및 논리적 보안

- 스토리지 업계 최초의 물리적 보안
- Air Gap Fabric 미국 특허 출원 / 스톤플라이의 보안 및 데이터 보호기능



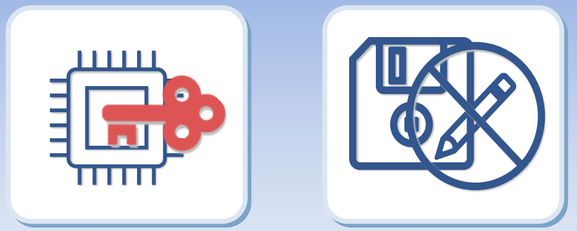
2. 실시간 감시

- 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)



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

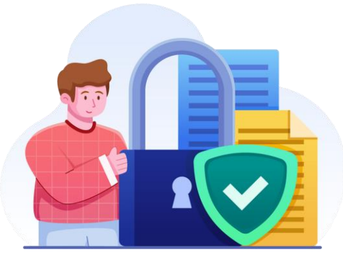
백업 및 아카이빙을 위한
오브젝트 스토리지 지원,
스톤플라이 자체
오브젝트 스토리지 및
AWS/Azure, S3호환
스토리지를 지원

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

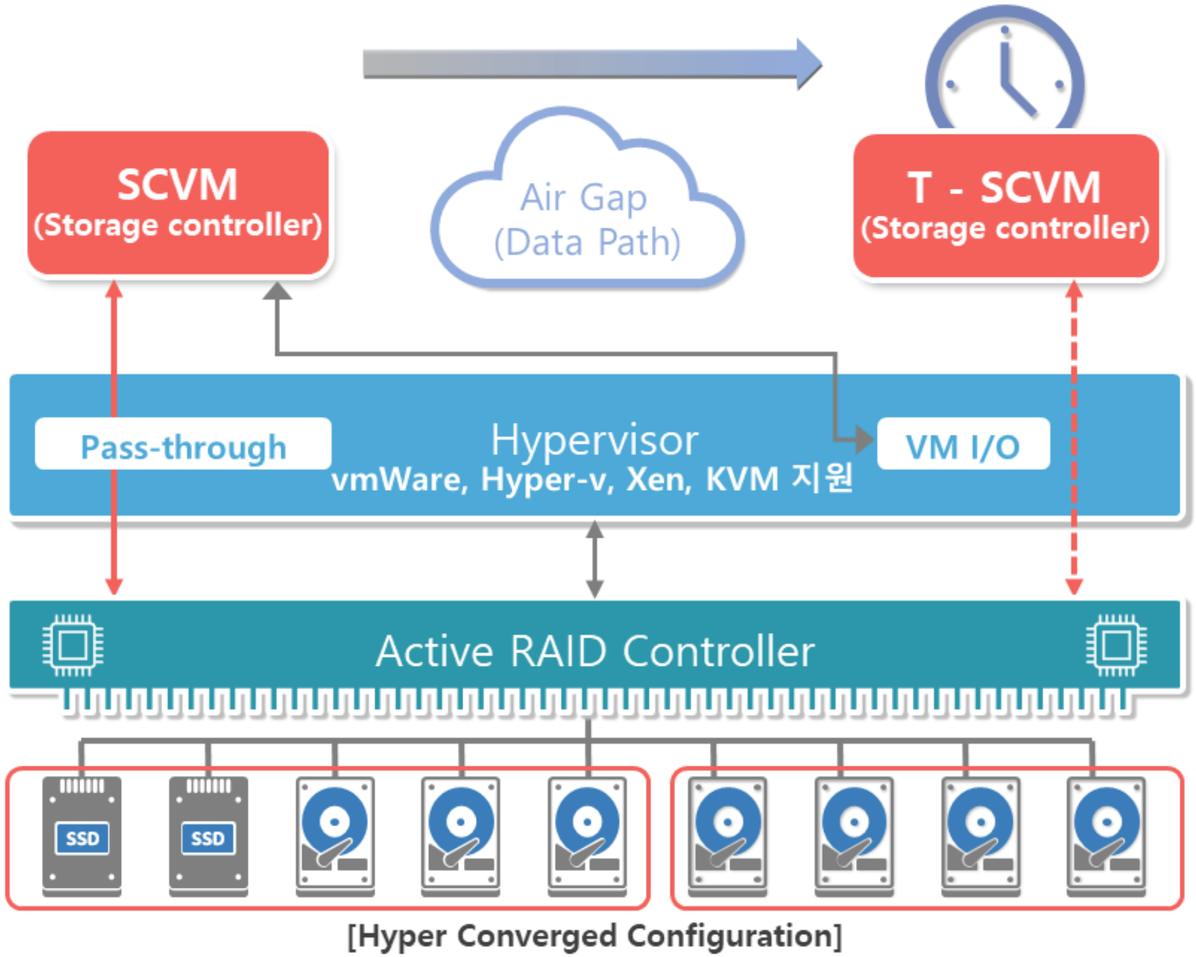
1. Air-Gap & Immutable Storage

- **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

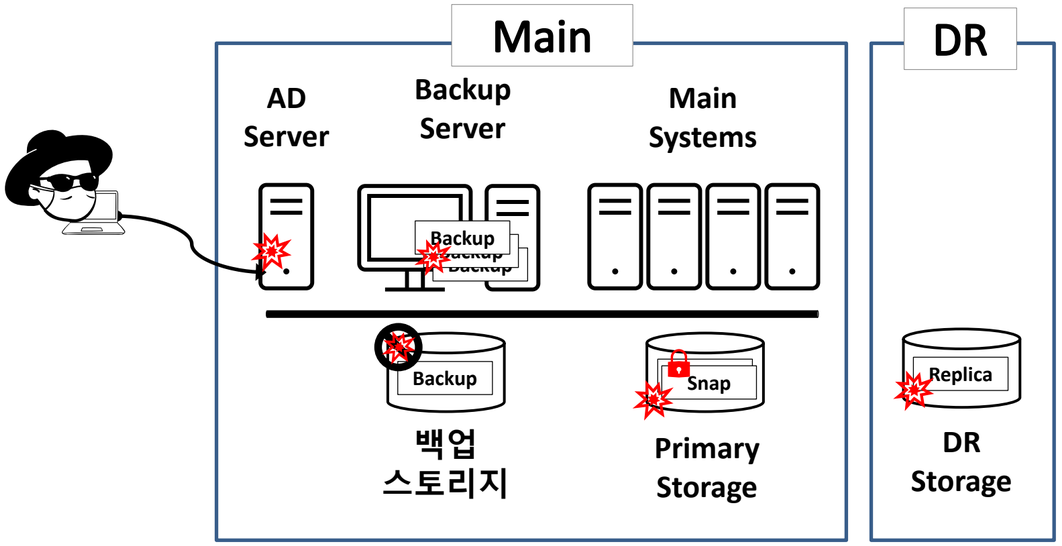
2. 볼륨 삭제 방지 기능

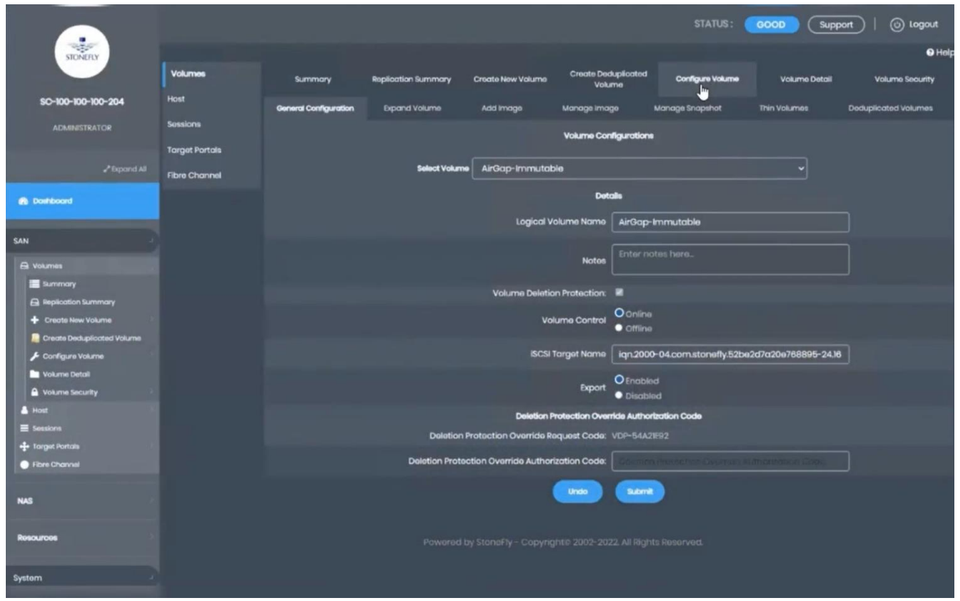
- **목적**
  * 랜섬웨어, 멀웨어, 해커,
    바이러스로부터 볼륨 보호

- **효과**
  * 해킹 또는 관리자의 실수에 의한 볼륨 삭제를 방지
  * 물리적인 위협까지 방어

- **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**
  - 데이터는 Immutable 기능을 통한 원본 내용 보장
  - 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)

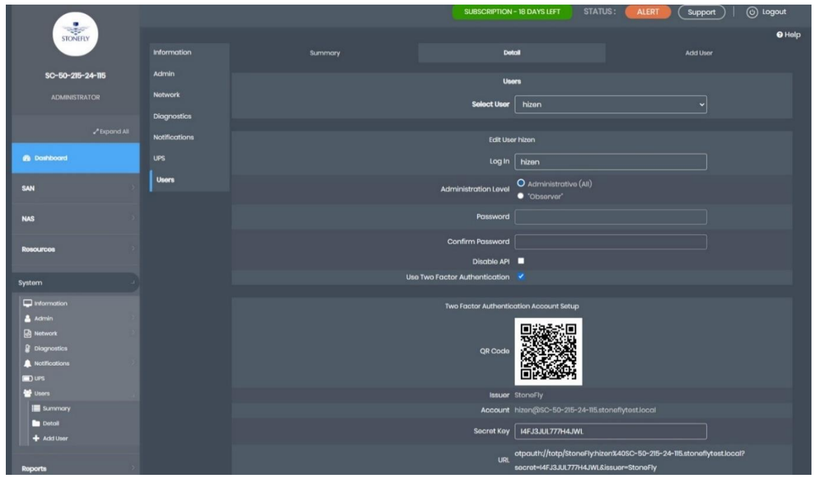
- **목적**
  * 해킹 혹은 운영상의 사고에 의한 패스워드 유출 시에도 완벽히 데이터를 보호

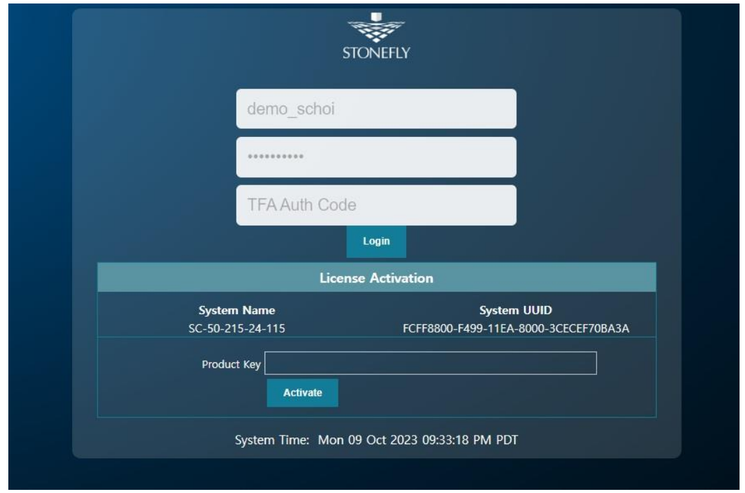
- **효과**
  * 패스워드 유출/악의적인 탈취 등 발생할 수 있는 패스워드 사고에 대비해 다중 인증을 함으로써 데이터를 안전하게 보호

- **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

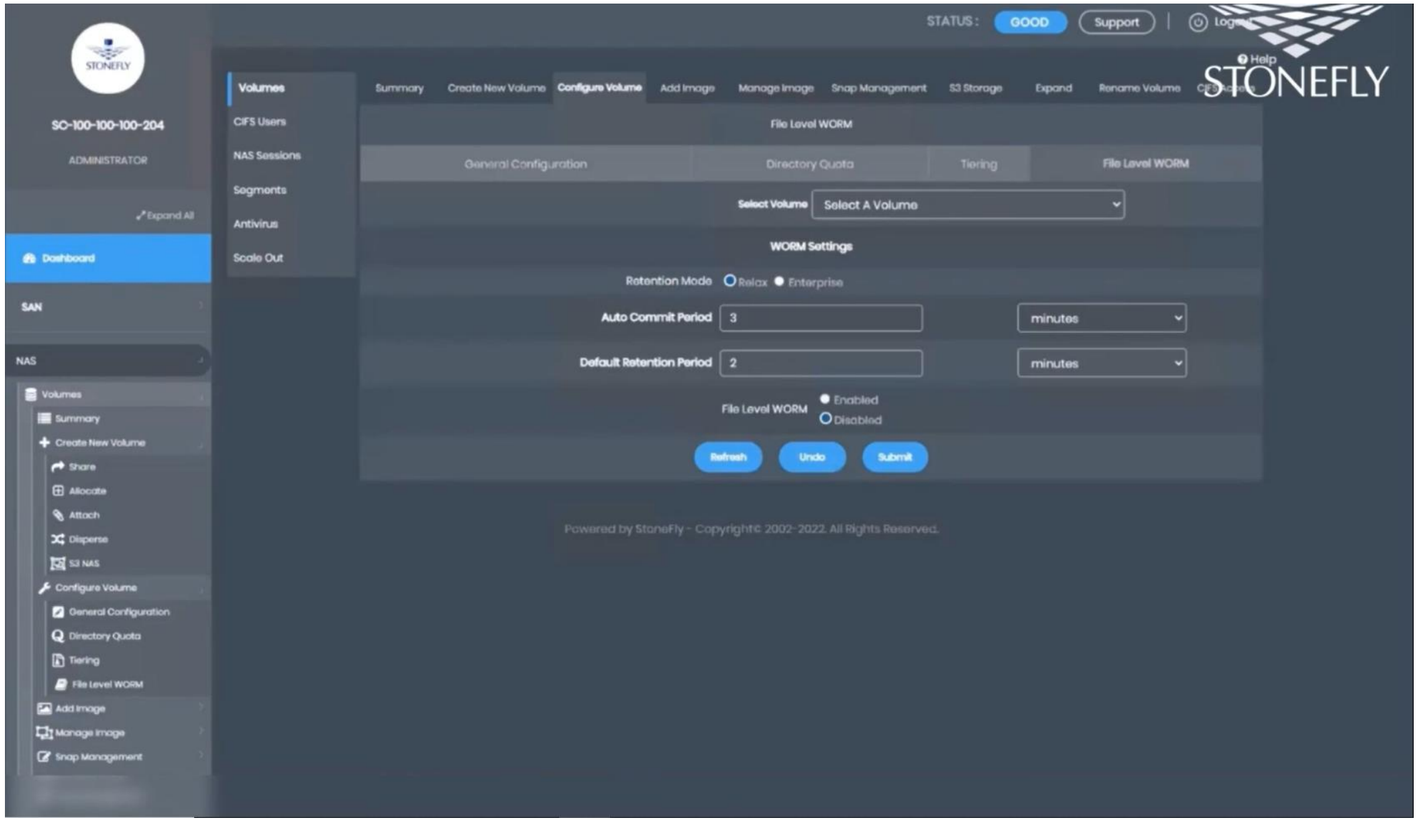
- **목적**
  * 랜섬웨어, 멀웨어, 해커, 바이러스로부터 악의적인 삭제/변조를 방지

- **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

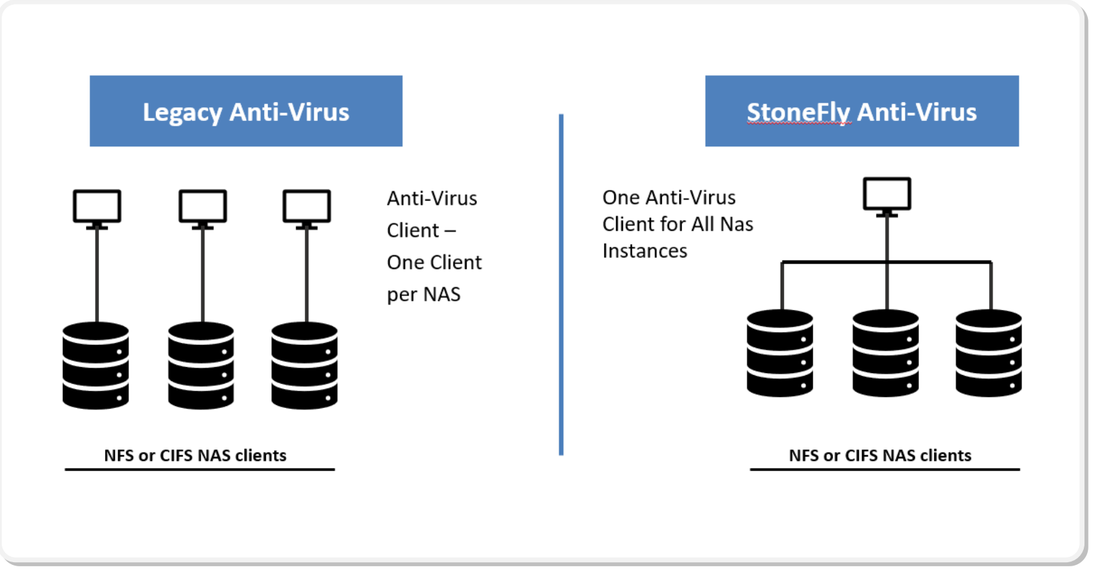
- **목적**
  * 랜섬웨어, 멀웨어등 바이러스로부터 볼륨 보호

- **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



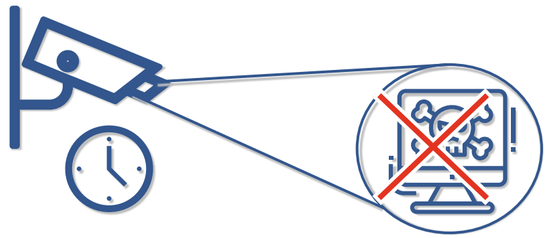
클라이언트의 부하 없음

#1 각 볼륨 별 실시간 혹은 Manual scan 가능

#2 각 볼륨 별 월 / 주 / 일/ 시간별 스케줄 가능

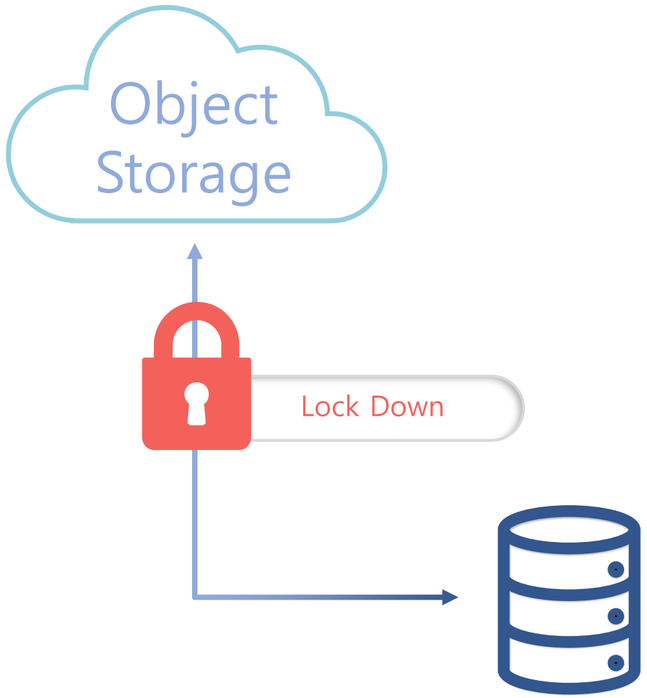
#3 Virus Database Online Update

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.

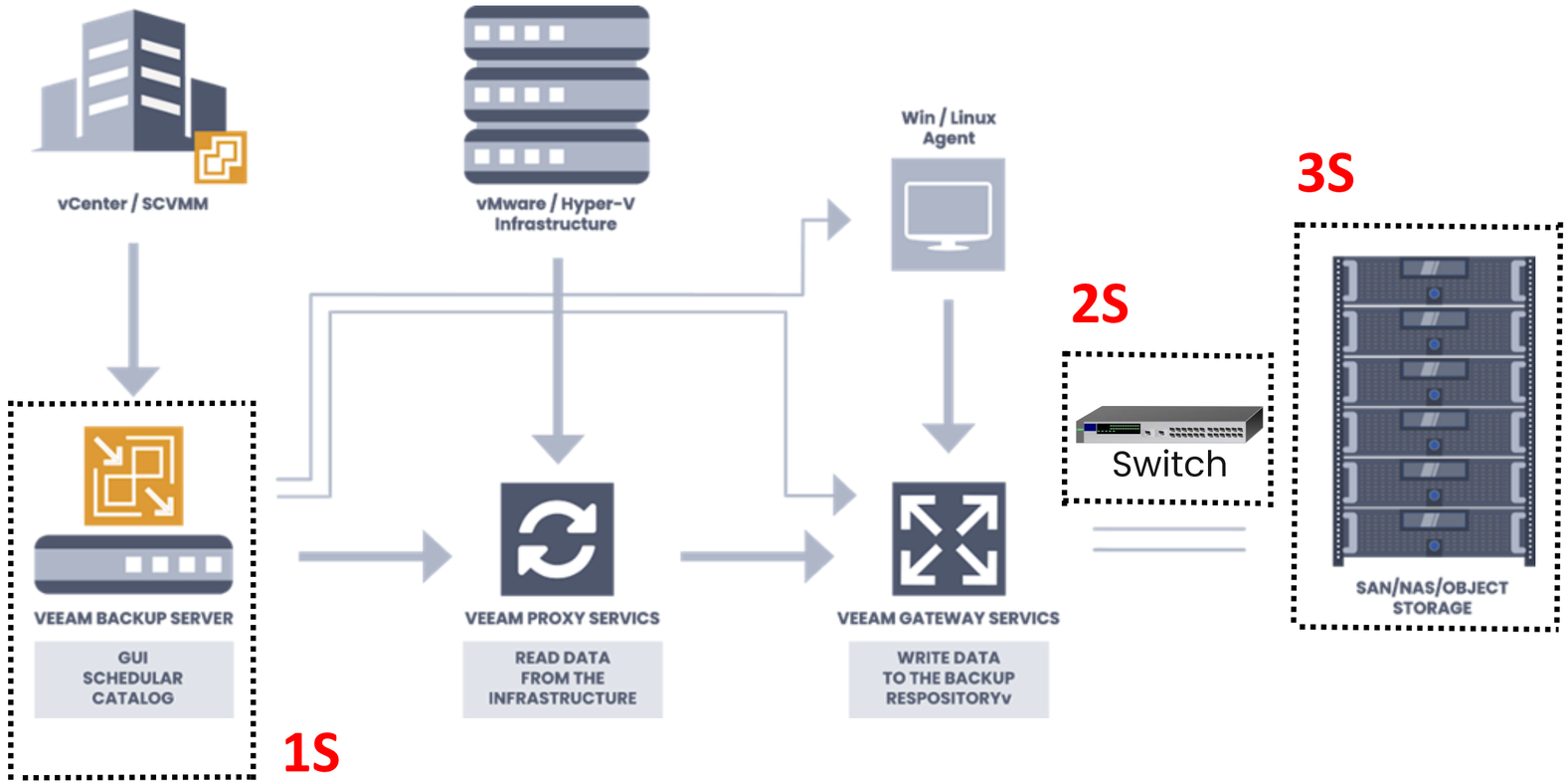
법적 보존은 보존 기간과 별개입니다.

대신 명시 적으로 제거 할 때까지 법적 보존이 유지됩니다.

백업 시스템의 보안

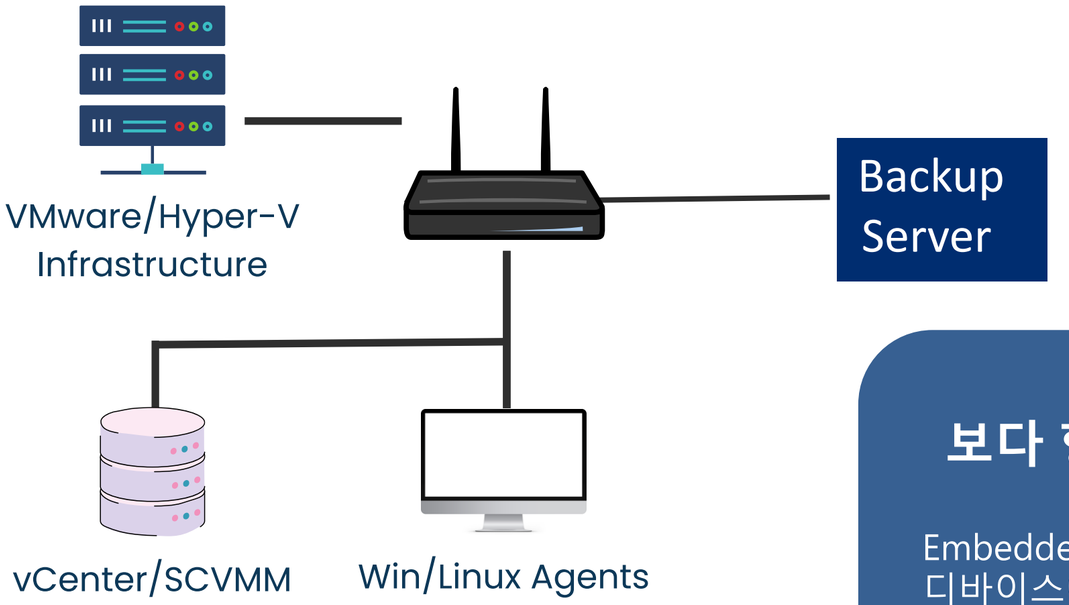
3가지 측면에서 보안적 취약성

1. 백업서버
2. 스위치
3. 백업저장장치



보안 – 백업 서버

가상화기반에 통합된 보안이 강화된 백업 서버



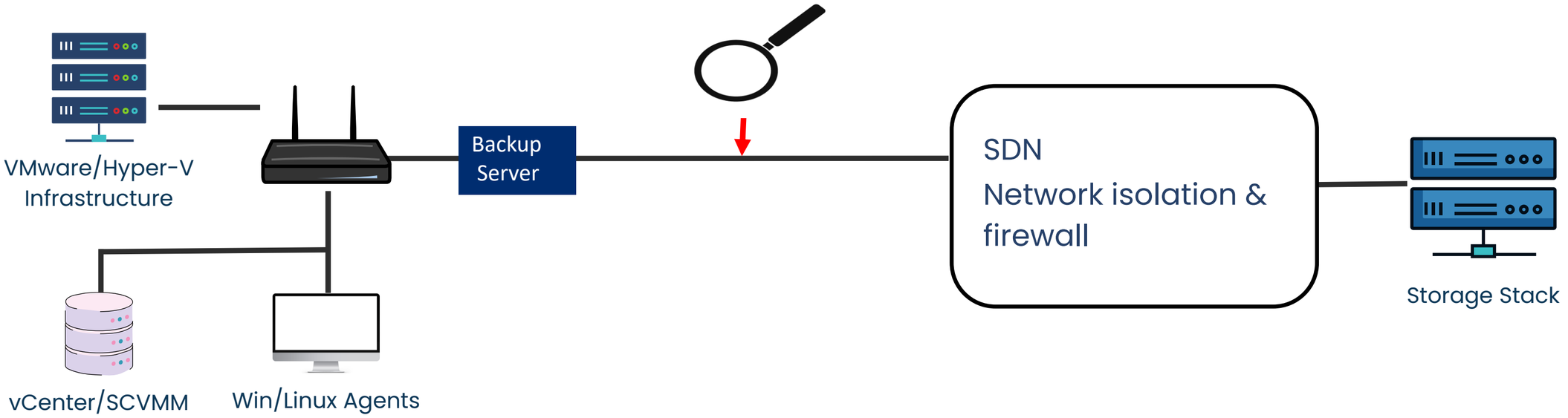
보다 향상된 보안 제공

Embedded 된 백업 서버는 모든 디바이스에 접근 가능하나 불필요한 services, ports, 실행파일 등을 제거 함으로써 보안을 강화 시킵니다.

성능 향상

가상화 내 백업 Agent(Data Mover등) 내부 통신을 통해 보다 빠른 백업 성능 제공

보안 – Network



01 SDN은 악의적인 패킷(랜섬웨어/멀웨어)을 식별하고 방어

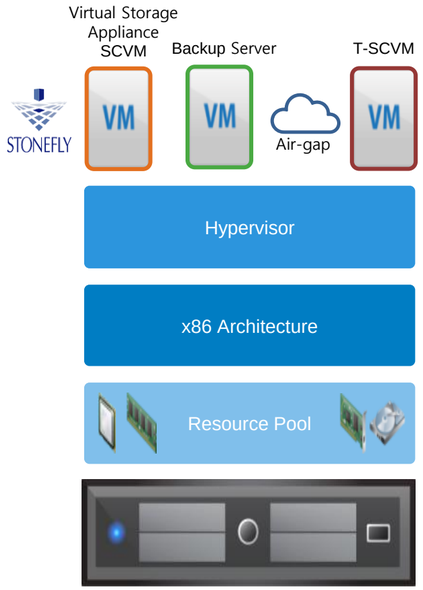
02 정상과 비정상 패킷의 판별 후 모든 정상적인 패킷에 대한 Hash를 부여함으로써 Secure TCP/IP 통신을 보장

03 백업 서버와 스토리지간의 보안 통신은 중간자 공격과 같은 위협을 방지

StoneFly DR365 Backup & Disaster Recovery Appliance Architecture

백업 스토리지 서비스 구성

백업 어플라이언스 구성



- SCVM 과 Backup Server VM
- 모든 백업 스토리지는 SCVM에서 관리
- Path-through를 통한 스토리지 access

강력한 데이터 보호

- 이중 인증
  * Veeam Connection를 통한 접근 관리로 백업 데이터를 보호합니다.
- 스토리지 컨트롤러 잠금 (Lock Down)
  * Object Lockdown 및 File Lockdown 지원
  * 접근 제한, 위변조 금지를 통한 멀웨어 차단 지원
- 위변조 불가능 스냅샷
- WORM Volume을 통한 위변조 방지
- 중요 볼륨에 대한 삭제 불가 기능(본사 지원을 통해서만 삭제 가능)
- Multi 인증 절차를 통한 볼륨 접근 및 사용 가능
- Air-Gaps : SCVM과 백업서버 통신 간 방화벽 지원 및 내부 SCVM과 격리를 통한 외부 침입을 원천적으로 차단
- 안티바이러스 탑재 (랜섬웨어, Malware 스캔)
- Recycling storage
- Invalid injection for execution 방지
  * 사전 정의된 서비스 수행 지정

스톤플라이 확장성

01

Scale up

- 단일 노드에서 최대 256 개 디스크 확장
- 20TB HDD 기준 최대 5.1PB까지 확장 가능

02

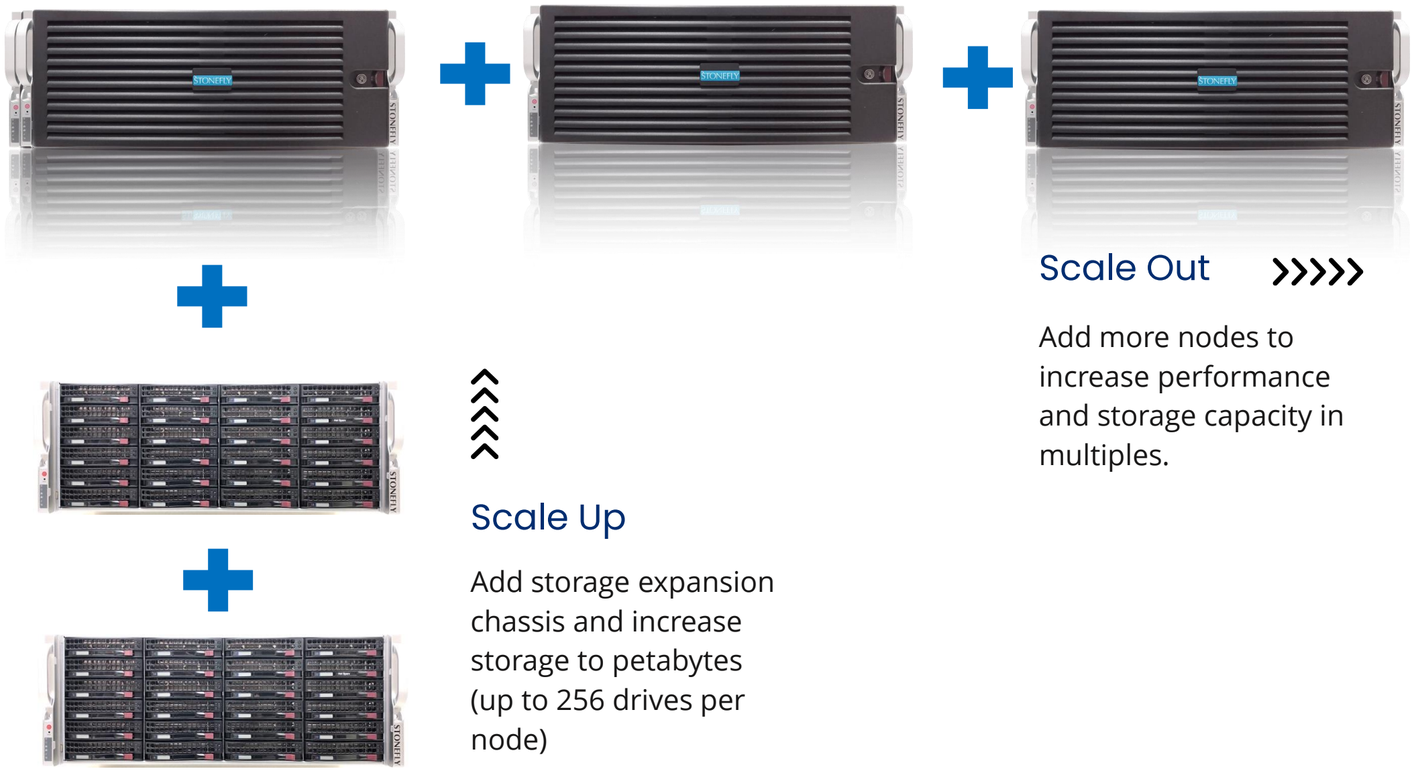
Scale out

- 최대 256 노드 확장
- N+1, N+N 구조로 고가용성 보장

03

Network

- SAN – 16Gbps, 16 ports
- LAN – 1/10/40/100Gbps, 최대 16Port 지원



JBOD –Disk Bay

Scale Up

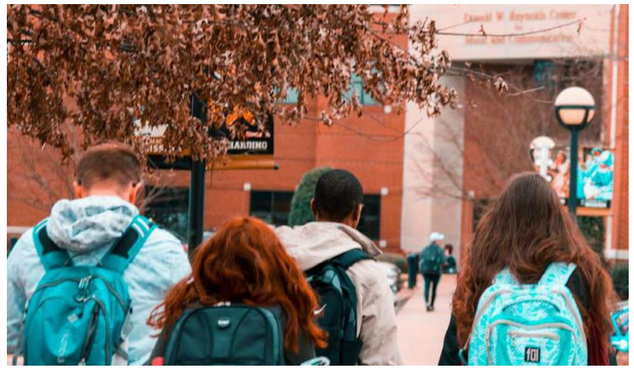
Add storage expansion chassis and increase storage to petabytes (up to 256 drives per node)

Scale Out

Add more nodes to increase performance and storage capacity in multiples.

고객 성공 사례 - 1

학교



- 각종 자료 및 장학금 프로그램에 지속적으로 액세스 할 수 있는 IT인프라를 유지관리
- 현재 IT시스템을 완전히 변경하지 않고도 랜섬웨어 공격과 데이터 관리
- 경제성

솔루션

DR365

- 백업 Solution + Secure Storage
- Air-Gap 기능을 통한 완벽한 데이터 보호

결과

- 자동 에어 갭 및 격리로 랜섬웨어 보호
- 파일 잠금 및 S3 객체 잠금을 지원하는 불변의 Write-Once-Read-Many(WORM)볼륨 제공
- 즉각적인 VM복구, 세분화 된 파일 수준 복원 등으로 복구시간 단축(RTO)

고객 성공 사례 - 2

병원

- 사이버 공격으로부터 환자의 기밀 정보와 의료기록 보호
- 백업 및 재해복구(DR) 시스템이 충분하지 않다고 판단
- 랜섬웨어 공격 시 가동중지시간을 최소화 하고 중요한 시스템을 복원할 수 있는 백업 및 DR 솔루션
- 경제적이며 데이터 규정 준수에 맞는 솔루션

솔루션

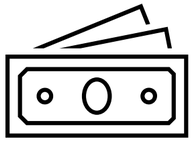
스톤플라이 Veeam 지원 백업 및 DR 솔루션 (DR365)

- 에어 갭, 불변성, 델타 기반 스냅샷, 암호화 및 S3 객체 잠금 기능이 내장됨
- 수십테라바이트 규모의 의료 기록과 VMware 하이퍼바이저에서 실행되는 20개의 가상 머신(VM)을 백업하고 온프레미스 및 클라우드에 복사본을 저장

결과

- 자동화 된 에어 갭핑, 격리 및 랜섬웨어 보호
- 파일 잠금 및 S3 개체 잠금 기능을 갖춘 변경 불가능한 WORM 볼륨 제공
- 즉각적인 VM복구, 세분화된 파일 수준 복원 등과 같은 기능으로 복구시간단축(RTO)
- 랜섬웨어 공격으로부터 시스템을 몇 분 안에 복원함

고객 성공 사례 - 3



금융회사

- 기존 서버 인프라가 수명을 다해 향상된 보호 기능과 능력이 있는 새로운 서버 원함
- 백업대상 스토리지
- 데이터 침해와 손실 위험을 최소화하기 위한 온프레미스 솔루션

솔루션

스톤플라이 NAS 스토리지

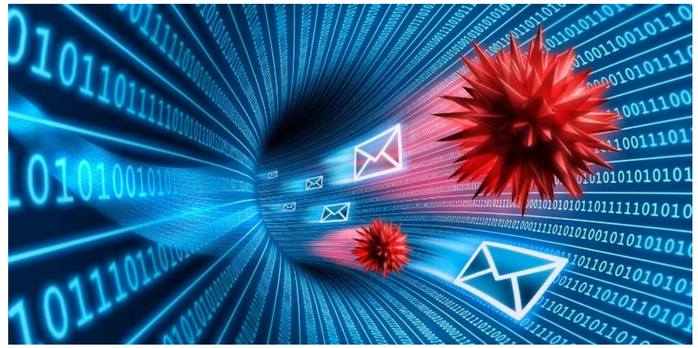
- Dual Node Shared Nothing 클러스터형 NAS 어플라이언스

결과

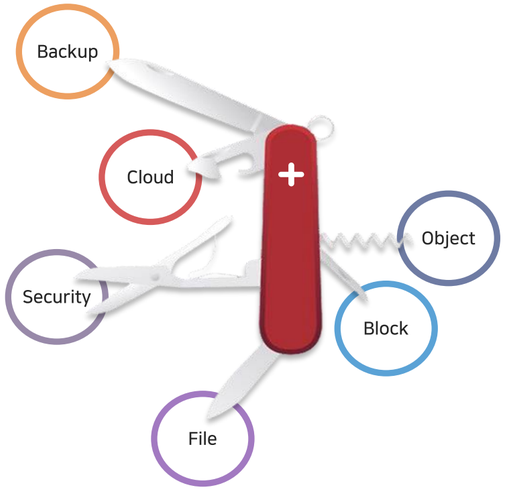
- 한 어플라이언스에 장애가 발생하더라도 다른 어플라이언스는 복구가 가능하여 비즈니스를 계속 운영할 수 있어 데이터 리던던시를 확보
- 데이터 스토리지 인프라의 내결함성으로 오류와 장애에 강함
- 델타 기반 스냅샷으로 데이터 손실 방지 보장 및 짧은 시간내에 시스템 복원

Why StoneFly

- **보안에 특화**
  * 고객사에서 발생 가능한 모든 보안 사고에 대비해 고객 데이터의 안전을 보장
  * 랜섬웨어/해킹에 의해 데이터가 삭제되더라도 피해 발생 전 상황으로 즉각적인 복구 가능
  * 운영 관리의 실수에 의한 데이터 손상 시 즉시 복구



- **기존 환경 변화를 최소화하고 고객별 맞춤화**
  * 현재 사용 중인 인프라 변경을 최소화한 구성 제안 가능
  * SAN/NAS/Object Storage/WORM등 고객의 요구 사항에 맞는 제품 구성
  * CPU/Memory/Disk/Network/Node 구성등



STONEFLY

Any Questions?

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