진정한 서비스 무중단을 위한 퓨어스토리지 데이터 보호 현대화 전략 소개

사이버공격에 대한 세이프모드 데이터 보호

강신우 부장

퓨어스토리지 코리아

PURESTORAGE®

PURE//ACCELERATE® techfest 22 seoul

세이프모드, 세이프모드, 세이프모드!

Status : Ransomware attack occured on 14th.

2022- 14 02:59:54 | 1949506 | customer | pureuser | purepgroup destroy

2022- 14 03:00:00 | 1949507 | customer | pureuser | purepgroup destroy

2022- 14 03:00:06 | 1949512 | customer | pureuser | purepgroup destroy

인도의 MSP 기업

FlashArray를 운영 스토리지로 사용

스냅샷 스케줄 및 SAFEMODE 2일 설정

1. **랜섬웨어 감염 / 스냅샷 삭제 확인**
2. Eradication Bucket **스냅샷 복원 및 서비스 재개**
3. SAFEMODE **기간 2일 → 3일로 변경**

RANSOM

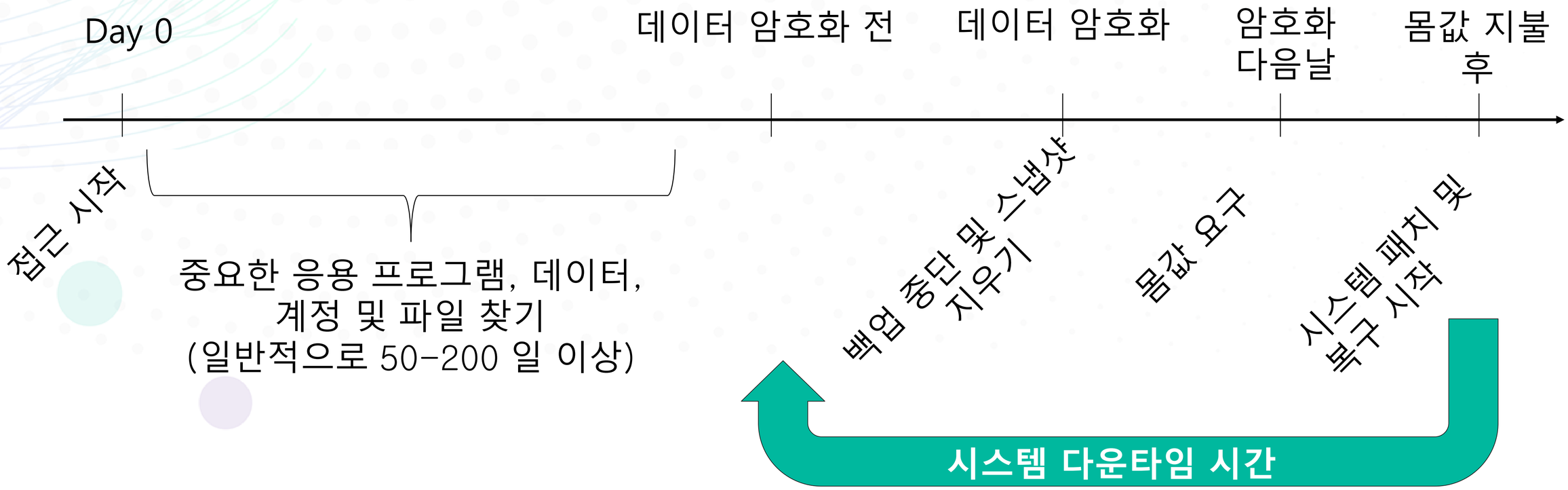
몸값, 몸값을 치르고 석방됨

MALWARE

악성 소프트웨어

일정 금액을 지불 할 때까지 컴퓨터 시스템에 대한 액세스를 차단하도록 설계된 일종의 악성 소프트웨어

랜섬웨어 공격 구조


Day 0
데이터 암호화 전
데이터 암호화
암호화 다음날
몸값 지불 후
접근 시작
중요한 응용 프로그램, 데이터, 계정 및 파일 찾기 (일반적으로 50-200 일 이상)
백업 중단 및 스냅샷 지우기
몸값 요구
시스템 패치 및 복구 시작
시스템 다운타임 시간

랜섬웨어 공격화면 예시

PURESTORAGE®

랜섬웨어는 항상 우리를 위협하고 있습니다

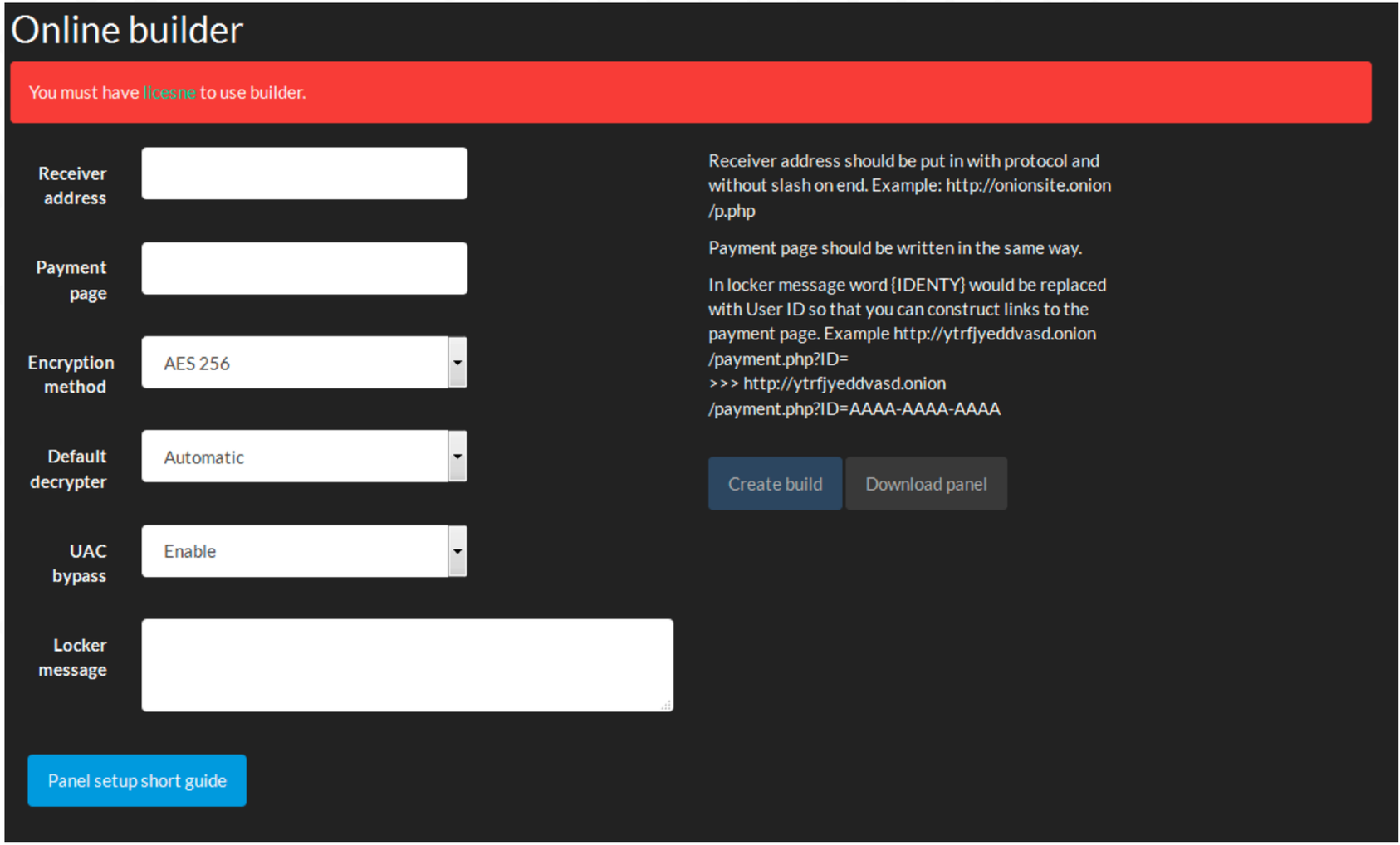
PURESTORAGE®

누구나 해커가 될 수 있습니다..

서비스 형 랜섬웨어는

누구든지 쉽게

악성코드를 만들 수 있습니다.



백업이 최후의 방어선 입니다.

랜섬웨어 감염 시
유일한 복구 방법은,

백업본에서 복원하거나

몸값을 지불하고
기도하는 것입니다..

PURESTORAGE®

3-2-1 백업전략을 통해 빠르게 데이터를 복원할 수 있습니다.

해커는 당신의 백업을 찾고 있습니다

해커는 데이터를 암호화하기 **전에** 시스템에서 200 일 이상을 보냅니다.

그리고 그 시간은 백업 복사본을 찾는데 사용됩니다...

PURESTORAGE®

97% 백업본 감염을 위한 랜섬웨어 공격 시도

73% 백업본에 대한 랜섬웨어 공격 성공

36% 조직에서 몸값을 지불했으나 데이터 복구 실패

PURESTORAGE®

Source: Veeam 2022년 랜섬웨어 동향 보고서

PURE//ACCELERATE® techfest22 seoul

공격을 받았다면 다음 두 가지 대응이 필요합니다.

랜섬웨어 공격에도
유효하고 사용가능한 데이터 복사본

대량의 데이터에 대한
초고속 데이터 복구

#1. 랜섬웨어 공격에도 유효하고 사용가능한 데이터 복사본

Snapshot Policy	Authorization	Tune Eradication Timer	Disable Eradication
위/변조 불가능한 스냅샷	권한 있는 사용자 제한	완전 삭제 타이머 설정	변경되지 않는 안전한 데이터
유연하고 세분화된 스냅샷 정책	최대 5명까지 승인된 컨택포인트, PIN code 제공	24시간에서 최대 30일까지 스냅샷 보관	볼륨 수동 완전삭제 비활성화

PURESTORAGE®

PURE//ACCELERATE® techfest22 seoul

Purity SafeMode 스냅샷

삭제 불가능한 골든-카피 스냅샷으로 신속한 데이터 복구 수행

- 사용자 실수 또는 사이버 공격으로 인한 영구적 데이터 손실 방지
- 관리자 권한으로도 삭제 불가능한 보안 스냅샷
- 올-플래시 기반 초고속 복구
- 어레이간 복제를 통한 3-2-1 데이터 보호 전략

PURESTORAGE®

PURE//ACCELERATE® techfest22 seoul

#2. 대량의 데이터에 대한 초고속 데이터 복구

최대 백업 시간:
90 TB/HR

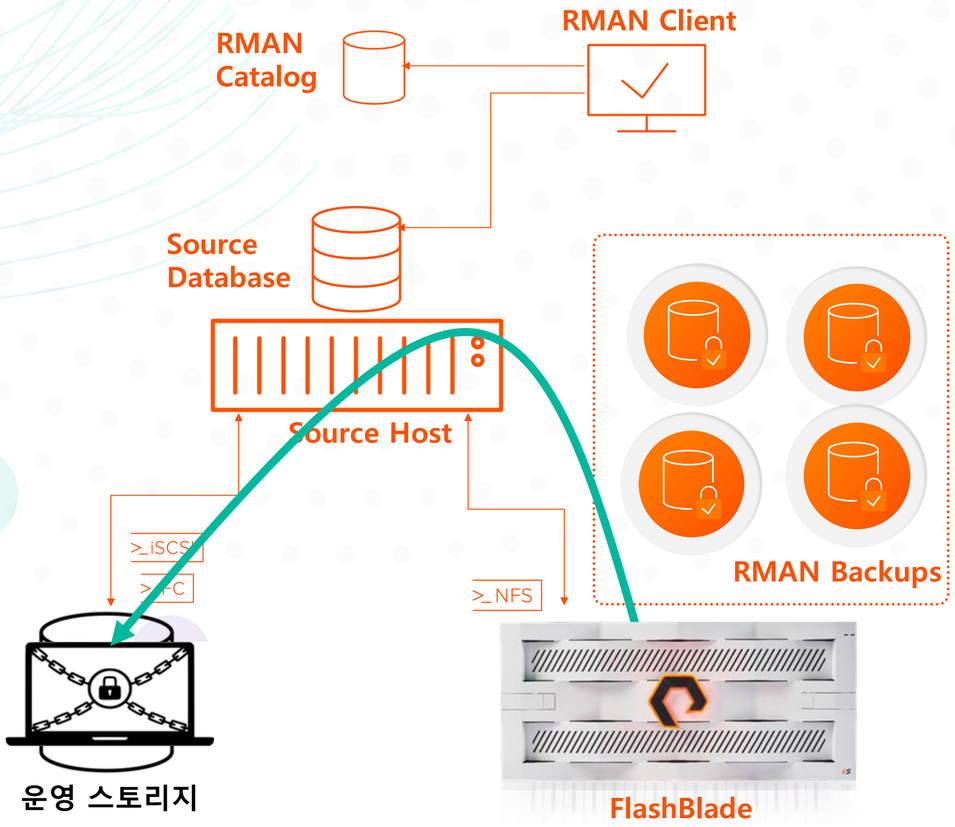
최대 복구 시간:
270 TB/HR

Scale-out 아키텍처:
용량 및 성능 확장

SMB, NFS, S3

데이터 및 비즈니스 보호 – 초고속 백업 복구

운영 데이터 랜섬웨어 감염 및 백업본 삭제 시, Eradication Bucket에서 RMAN 백업을 dNFS 기반 초고속 복구 수행



Oracle RMAN + dNFS

- 단일 파일 시스템 (15블레이드 기준)
- 초당 **4.5GB 백업** 성능(15TB/hr, 최대 90TB/hr)
- 초당 4GB 복구 성능 (최대 270TB/hr-대상 스토리지 성능)

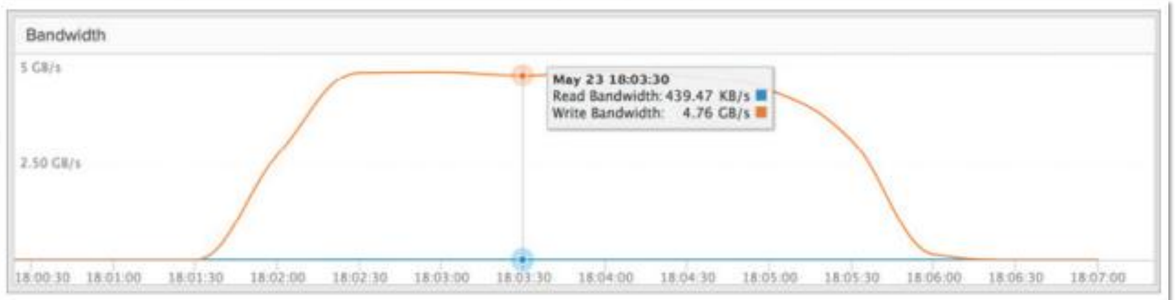


Figure 6. FlashBlade bandwidth

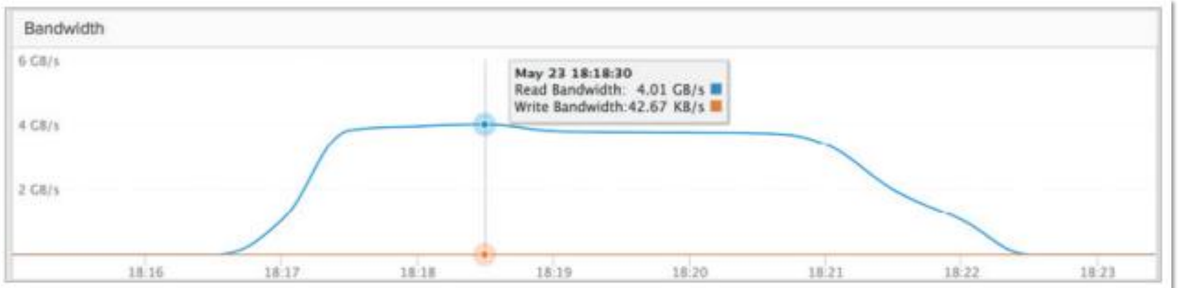


Figure 12. FlashBlade bandwidth

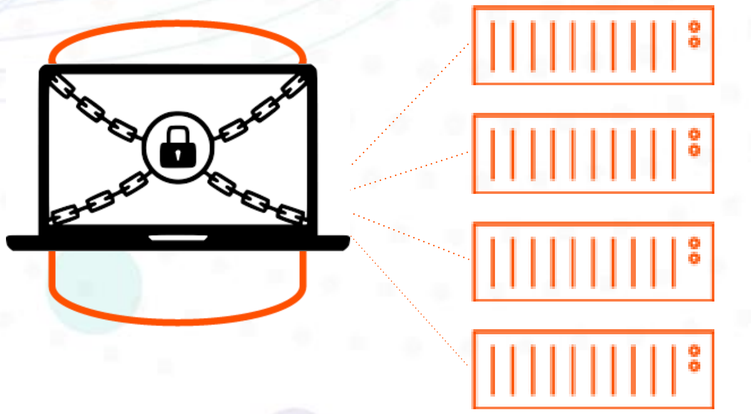
PURESTORAGE®

seoul

백업 이미지 공격 시에도, SafeMode 로 복구

백업본 감염 시, 복구 절차

1. 백업 소프트웨어 재설치
2. SAFEMODE 백업 리포지토리 연결
3. 암호화된 데이터 백업본으로 복구 수행



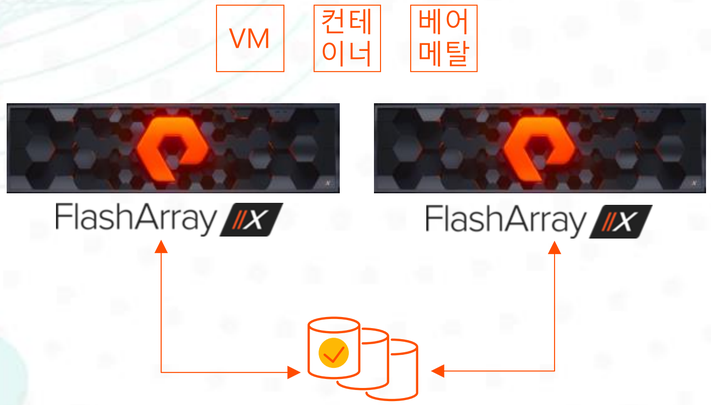
운영 스토리지 / 백업 저장소 모두 랜섬웨어 공격

PURESTORAGE®

PURE//ACCELERATE® techfest22 seoul

Summary: Safemode 기반의 3-2-1 전략 구축

3개 이상의 복제본



ActiveCluster 운영 스토리지 이중화

- 대상 업무: 운영 데이터
- 보호 방식: AADC 이중화 + 스냅샷 정책 설정
- 보호 용도: 논리적/물리적 장애
- 보호 레벨: 무중단 서비스

SafeMode를 통한 랜섬웨어 방지

2개 이상의 스토리지 저장소

초고속 백업 / 복구

- 대상 업무: DB(Oracle/MSSQL/etc.)
- 보관 주기: ~ 2주
- 백업 용도: 최근 데이터 고속 복구

SafeMode 를 통한 랜섬웨어 방지

1개 이상의 오프사이트 소산

Offsite 복제(온프렘/클라우드)

- 대상 업무: 전체 DR 통합
- 보관 주기: Daily / Monthly
- 백업 용도: 오프사이트 데이터 DR

SafeMode 를 통한 데이터 보호

DR 복제

3rd Party 백업 솔루션 연동

백업 솔루션 연동

- 대상 업무: 전체 통합 백업
- 보관 주기: 기업 SLA 준수(D/W/M/Y)
- 백업 용도: 백업 정책에 따른 데이터 보호

SafeMode 를 통한 백업 카탈로그 / 데이터 보호

PURESTORAGE®

PURE//ACCELERATE® techfest22 seoul

PURE//ACCELERATE®
tech fest 22
seoul

Thank you

PURESTORAGE®