PURESTORAGE®

# 현대적 데이터 보호 전략

**사이버 위협에 현명하게 대응하는 기업 솔루션**

퓨어스토리지 강신우 부장

Sr.Systems Engineer

# 사이버 공격은 이미 현실입니다.


https://www.etnews.com/20210604000138

# RANSOM

몸값, 몸값을 치르고 석방됨

# MALWARE

악성 소프트웨어

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

# 랜섬웨어 공격화면 예시

## Your files have been locked!

### Whats happened?

All documents, photos, databases and other important files **encrypted**

### How to decrypt files?

The only way to decrypt your files is to **receive the A7poE9-Decryptor**

### Are you ready?

We guarantee that you can **recover all your files.**
But you have not so enough time.

Buy [redacted]-Decryptor

Price now: **0.4017 BTC** (~3500$)

You have: [redacted]

If payment isnt made in this time, the cost will be doubled: 0.8034 BTC (~7000$)

랜섬웨어는 항상 우리를 위협하고 있습니다.

# 백업이 최후의 방어선 입니다.

랜섬웨어 감염 시
유일한 복구 방법은,

**백업본에서 복원**하거나

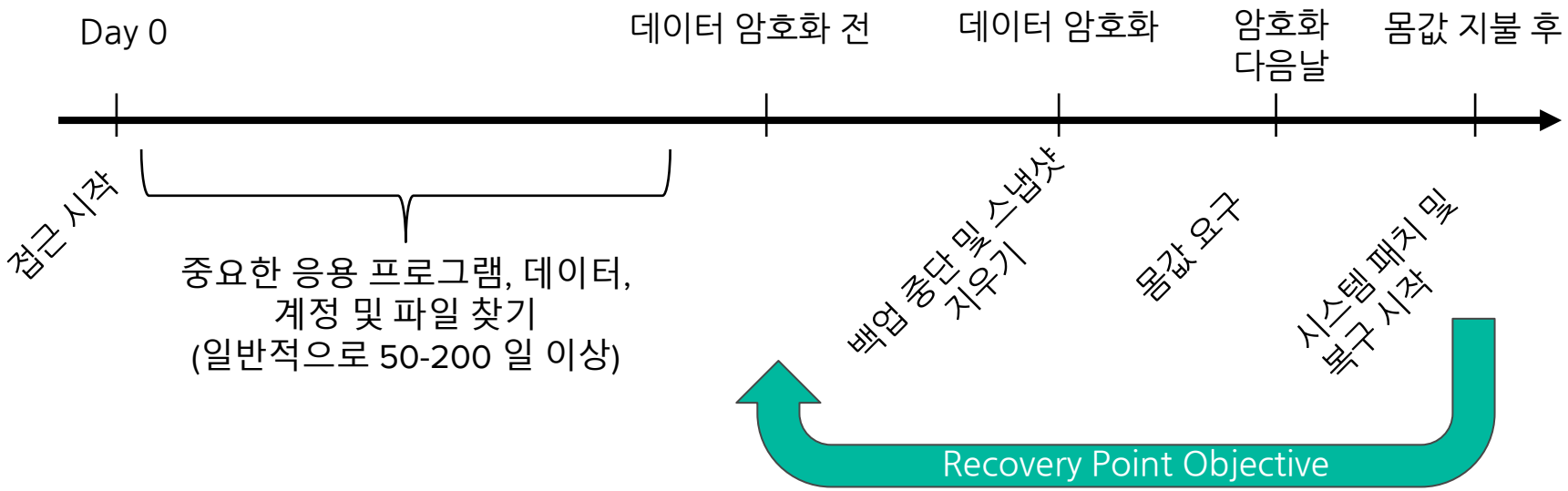
몸값을 지불하고
**기도하는 것**입니다..

# 해커는 당신의 백업을 찾고 있습니다

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

그리고 그 시간은 백업 복사본을 찾는데 사용됩니다...

# 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
Recovery Point Objective

# 공격을 받았다면 다음 두 가지 대응이 필요합니다.

랜섬웨어 공격에도
**유효하고 사용가능한 데이터 복사본**


복구 범위가 광범위하기 때문에
**가능한 가장 빠른 복구**

# 간단하고 위/변조불가능한 Snapshots

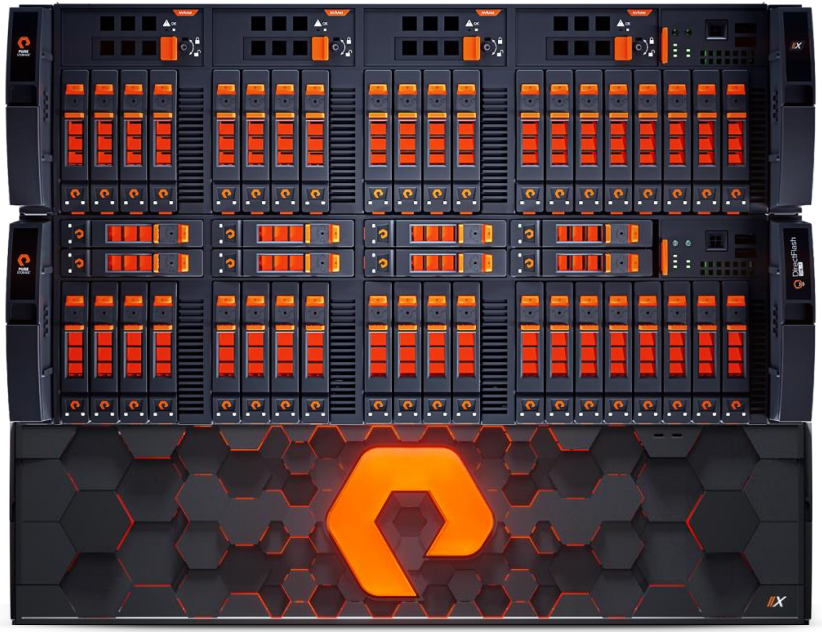
어느 볼륨이든 즉각 스냅샷 생성
예약된 공간 또는 계획이 필요 없음
성능 오버헤드 없음
유연한 consistency groups

완전한 기능을 갖춘 새로운 볼륨 스냅샷
마운트, 읽기/쓰기, 스냅샷 재수행 가능
서로에 대한 종속성 없음
모두 완전한 성능을 발휘

공간절약
전체 영역에서 Shared 영역 제외
항상 중복제거/압축 적용

언제 어디서든 복구 가능
즉시 복구 제공
모든 스냅샷에서 모든 볼륨 복구

## FlashArray Volumes
## **100% Metadata**



# FlashArray with SafeMode Snapshots

관리자 실수나 해커의 공격으로 인한 영구적인 데이터 손실 방지

최대 30일동안 변경/삭제할 수 없는 보안모드 스냅샷

빠른 데이터 복원

FlashArray //C

FlashArray //X

# FlashArray with SafeMode Snapshots




Snapshot Policy | Authorization | Tune Eradication Timer | Disable Eradication

## 위/변조 불가능한 스냅샷

유연하고 세분화된
스냅샷 정책

## 권한 있는 사용자 제한

최대 5명까지 승인된
컨택포인트, PIN code 제공

## 완전 삭제 타이머 설정

24시간에서 최대 30일까지
스냅샷 보관

## 변경되지 않는 안전한 데이터

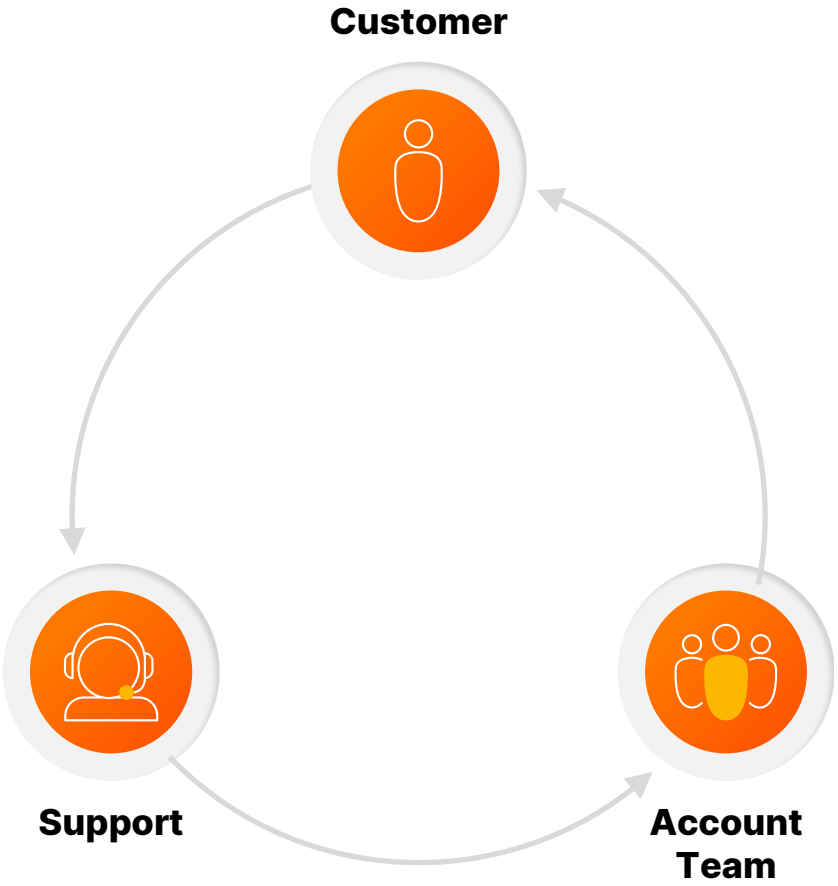
볼륨 수동 완전삭제
비활성화

# Authorization*

최대 5명까지 권한 있는 컨택포인트 설정

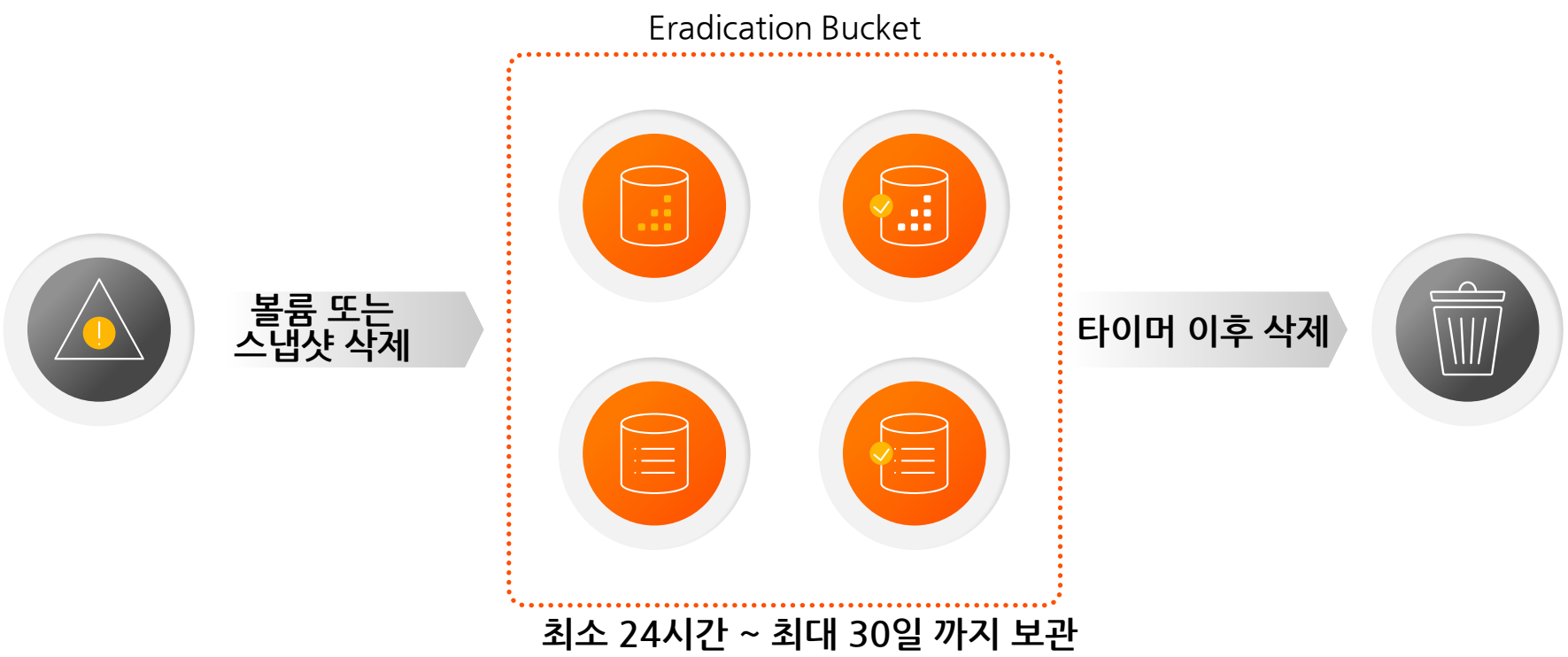
Email id와 특별한 PIN code로 확인

안전하고 쉽게 설정 가능




*Support required to enable or modify

# Tunable Eradication Timer*



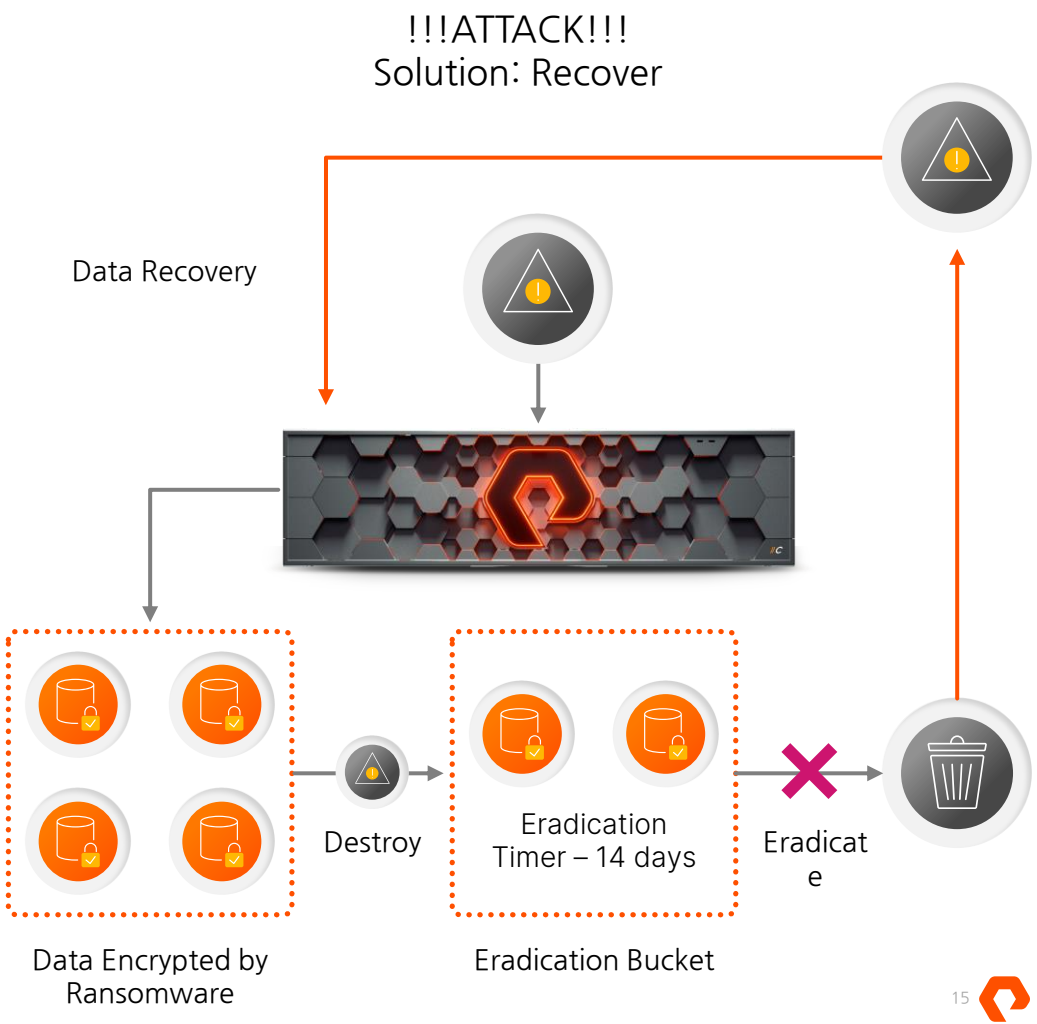
# SafeMode 스냅샷을 통한 랜섬웨어 복구

1. 악의적 인 공격자가 FlashArray 데이터를 암호화합니다. 스냅 샷은 변경할 수 없으므로 수정되지 않습니다.

2. 공격자는 암호화 된 모든 데이터를 파괴하거나 파괴하지 않을 수 있습니다. 변경 불가능한 모든 스냅 샷을 삭제합니다.

3. 스냅 샷 / 암호화 된 데이터는 더 긴 시간 (이 경우 14 일) 동안 삭제 버킷에 보관됩니다. 공격자는 수동으로 제거 할 수 없습니다.

4. 공격이 식별되면 삭제 버킷의 스냅 샷을 사용하여 데이터를 FlashArray로 다시 복구 할 수 있습니다. 몸값을 지불 할 필요가 없습니다 !!

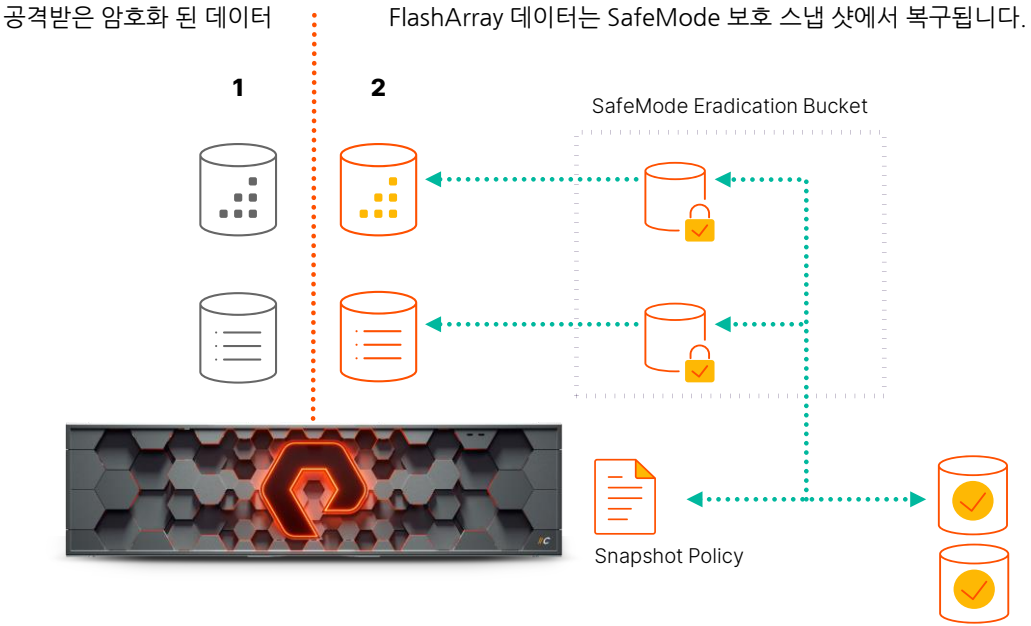


# Safemode 스냅샷 데이터 복구 절차

1. 손상되었거나 암호화 된 데이터를 제거

2. SafeMode 스냅샷에서 볼륨 복제

3. 서비스 중단 시점으로 즉각 복구



# RAPID RESTORE POWERED BY PURE

초고속 Scale-out 오브젝트 스토어


최대 백업 시간:
90 TB/HR

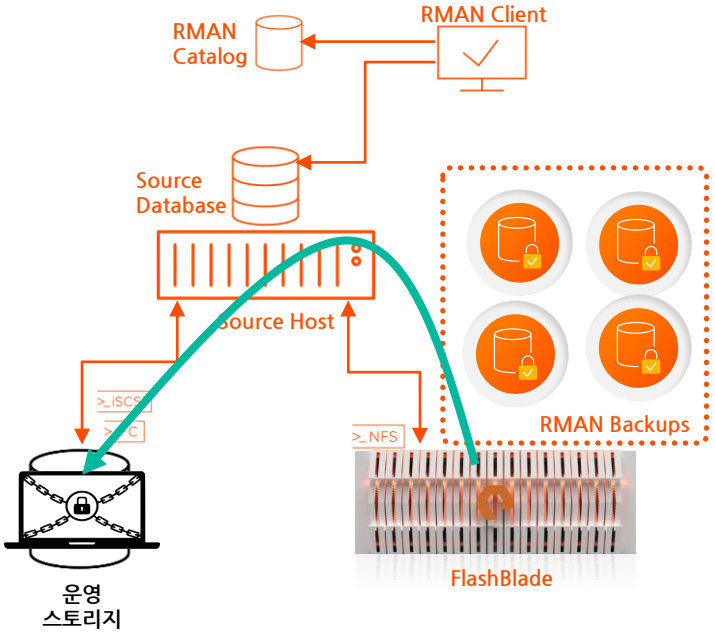
최대 복구 시간:
270 TB/HR

Scale-out 아키텍처:
용량 증가 시 성능도 같이 증가

SMB, NFS, S3

# 데이터 및 비즈니스 보호 - 초고속 백업 복구

대용량 Oracle DB에 대한 RMAN 기반 dNFS 기반 초고속 백업 복구




## 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)

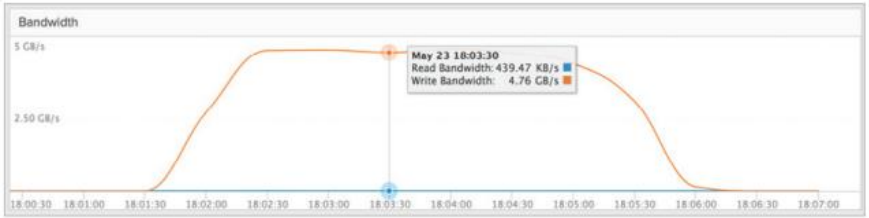
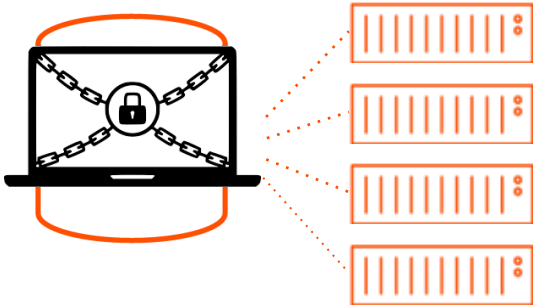


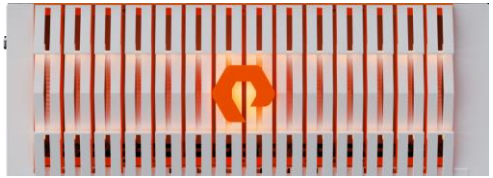

*Figure 6. FlashBlade bandwidth*

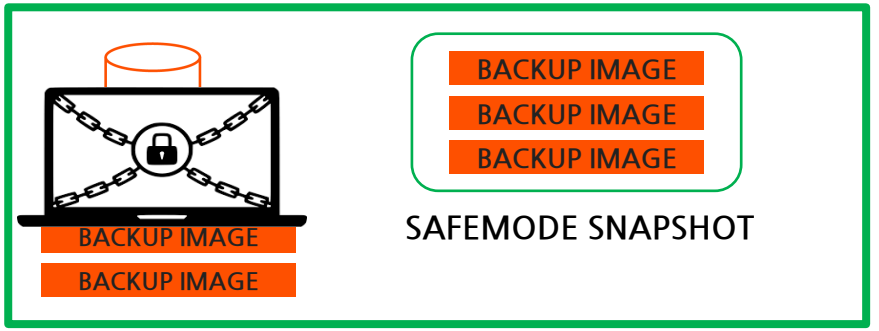

*Figure 12. FlashBlade bandwidth*

# RANSOMWARE ATTACK

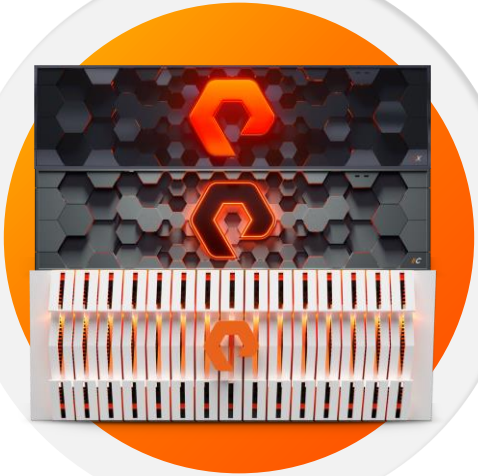


운영스토리지 백업 클라이언트






RANSOMWARE ATTACK ENCRYPTS PRIMARY & SECONDARY STORAGE



## Pure Storage SafeMode™ Snapshot

관리자 실수 또는 악의적인 공격으로 인한
데이터의 영구적인 손실 방지 기술

1~30일에 대한 데이터 위,변조 및 임의 삭제 방지를 통한 데이터 보호

FlashArray //C FlashArray //X FlashBlade //FB

Veeam COMMVAULT VERITAS ORACLE SQL Server

## Pure Storage RapidRestore

손상된 데이터를 초고속 복구 성능 기반
서비스 다운타임 최소화 기술

운영 데이터의 즉각적인 스냅샷 복구
최대 시간 당 270TB 데이터 복구 성능 제공(FlashBlade)

# 맺음말

*“ 단 두 종류의 회사가 있다.*
*해킹 당한 회사,*
*그리고, 해킹 당한 사실을 모르는 회사 ”*

***John Chambers***
*전 Cisco CEO 겸 회장*
*WEF 제 45차 연차총회, 다보스 포럼, 2015*

**피할 수 없다면, 대비해야 합니다!**

PURESTORAGE®

# Thank you!

- √ 공식 웹사이트 www.purestorage.com/kr
- √ 공식 유튜브 www.youtube.com/c/PureStoragekr
- √ 공식 페이스북 www.facebook.com/purestoragekorea
- √ 네이버 블로그 blog.naver.com/purestorage_korea