PURESTORAGE®

VEEAM

# 데이터보호 현대화전략

## - 새로운 위협 **Ransomware**

**김영석 부장**

System Engineer
Purestorage Korea

ykim@purestorage

2021.10.01

PURESTORAGE®

VEEAM

# Re-Define of backup data

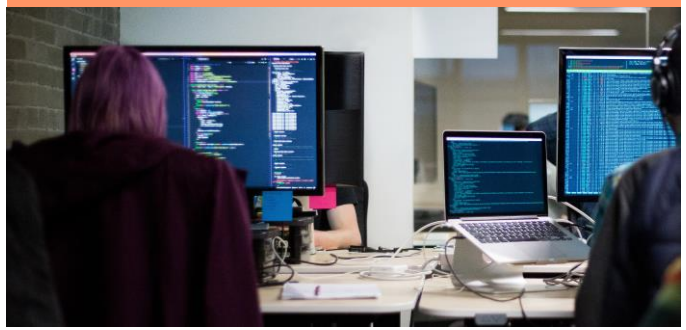
백업 데이터의 트랜드와 재정의

# 백업데이터에 대한 요구와 기대의 증가

현대사회에서 데이터의 재사용 요청이 증가 하고 있으며, 점차 백업성능에서 복구시간 및 성능으로 기업의 관심이 움직이고 있습니다.

**RAPID RESTORE**

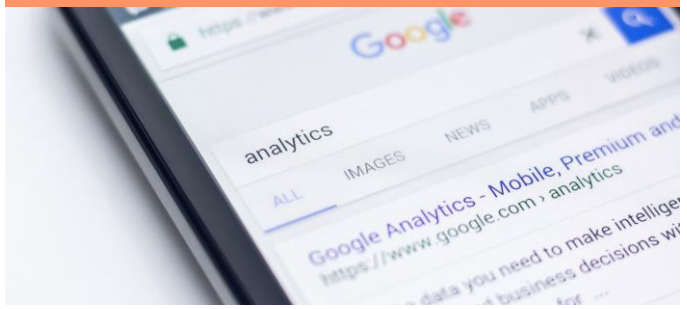

**TEST/DEV**



**GDPR & PRIVACY**

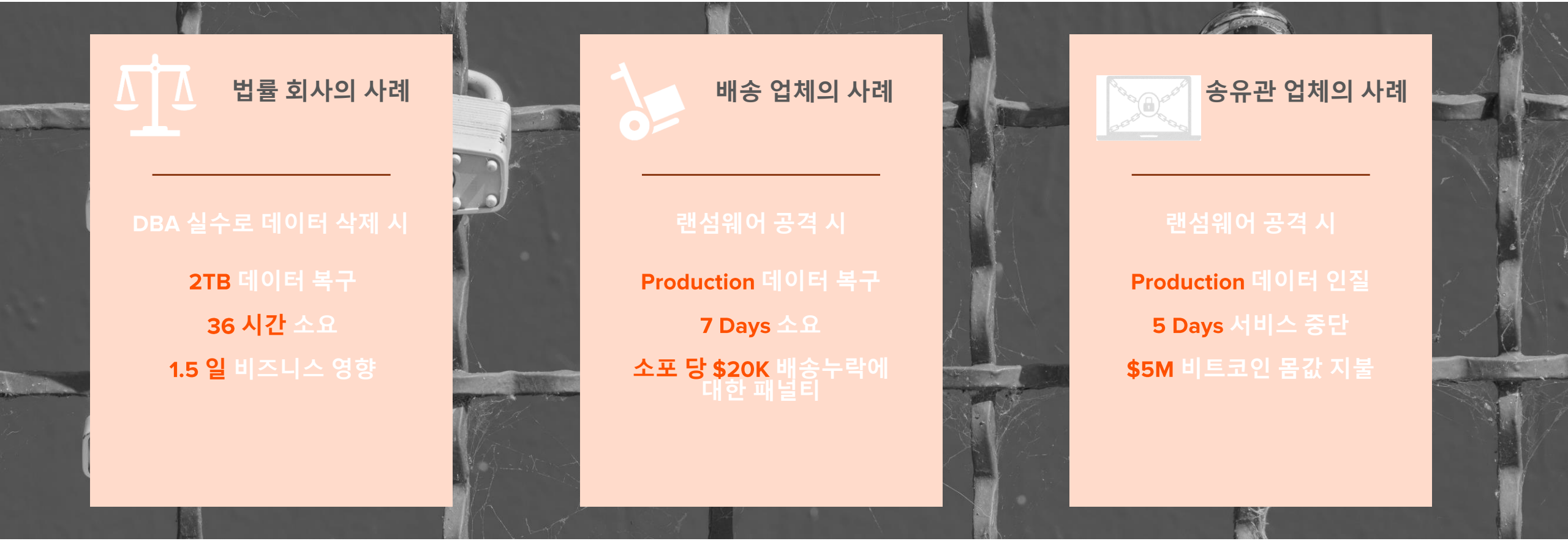

**MALWARE DETECTION**

**ANALYTICS**



# 비즈니스 보호는 백업만으로 부족합니다..

비즈니스 보호는 데이터 백업만으로 부족합니다. 중요한 것은 복구를 SLA에 맞출 수 있는가 하는 것입니다.



### 법률 회사의 사례

DBA 실수로 데이터 삭제 시

**2TB** 데이터 복구

**36 시간** 소요

**1.5 일** 비즈니스 영향

### 배송 업체의 사례

랜섬웨어 공격 시

**Production** 데이터 복구

**7 Days** 소요

**소포 당 $20K** 배송누락에 대한 패널티

### 송유관 업체의 사례

랜섬웨어 공격 시

**Production** 데이터 인질

**5 Days** 서비스 중단

**$5M** 비트코인 몸값 지불

# 백업에 대한 이야기가 왜 필요할까요?

**23%**

**지금**
**서버 4대중 1대**
계획되지 않은
중단이 발생.

**63%**
**3대중 2개의 백업**
이 성공

x

**66%**
**3대중 2개의 복구**
시간을 초과

=

**42%**
**절반 이하** 만이
**SLA**내에 복구가 될 것



VEEAM | PURESTORAGE

# 시장에서 유일하게 성장하는(4x) Veeam !!

| **Company** | Vendor Revenue (US Dollar, M) | **Sequential Growth %** | YoY Growth % |
|---|---|---|---|
| Dell Technologies | 746.60 | +8.0% | -4.2% |
| Veeam | 563.61 | +21.5% | +17.9% |
| Veritas | 537.13 | +2.2% | -4.9% |
| IBM | 487.24 | -9.3% | -16.5% |
| Commvault | 340.43 | +6.0% | +5.1% |
| Others | 2,048.49 | +5.9% | +3.8% |
| Market Average | N/A | +5.6% | +0.4% |

Source: *IDC, Semi-Annual Software Tracker, 2020H2*
Note: Worldwide Data

**Veeam은 가장 빠른 매출 성장을 달성**

***-- 전세계 2020H2 순차 및 연단위 성장율 --***

**상위 5개 벤더**

PURESTORAGE®

# 새로운 위협 **Ransomware** 대응

Safemode & Rapid restore

**ran • som • ware**
**/ˈransəm , we(ə)r/**

***noun***

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

문제를 해결하기 위해 대량의 데이터를 예기치 않게 복원 해야함

## 美 최대 송유관 업체, 랜섬웨어 해커에 비트코인으로 50억 지급

입력 2021.05.20 09:18 | 수정 2021.05.20 09:23

사진=REUTERS

미국 최대 송유관을 운영하는 콜로니얼파이프라인이 랜섬웨어 공격을 한 해커들에게 440만달러(약 50억원)를 줬다고 시인했다. 지불은 비트코인으로 했다.

https://www.hankyung.com/international/article/202105209857i

## 美, 랜섬웨어 등 사이버공격에 군사적 대응

러먼도 상무장관, 이달 미·러 정상회담에서 의제로 상정
부티지지 교통장관, 민간기업 해킹 국가전체 영향 강조

박경희 기자 입력 2021-06-07 09:22

지나 러먼도 상무장관. 사진=로이터

지나 러먼도 상무장관은 6일(현지시간) 조 바이든 정부가 랜섬웨어(몸값을 요구하는 악성코드)에 의한 사이버공격을 방지하기 위해 군사적 대응을 포함한 모든 선택지를 검토하고 있다고 말했다.

https://news.g-enews.com/ko-kr/news/article/news_all/202106070909176635b5d048c6f3_1/article.html?md=20210607092215_R

## 미, 잇단 랜섬웨어 공격에 공개 경보...미·러 회담

송고시간 | 2021-06-04 00:29

뮤지복 기자

| 백악관, 민간기업에 철저 대비 촉구 서한 보내


사이버공격 받은 세계 최대 정육업체 JBS
(그림리 AFP/게티이미지=연합뉴스)

## [단독] LG 해외법인까지 해킹한 '랜섬웨어'..."파일 7개 유출"

신정은 기자 silver@sbs.co.kr 작성 2021.05.20 19:42 조회 1,083


토소웅 피지제거기

진짜 피르가즘 대박. 별짓을 해도 안빠지던...

SBS 연예뉴스
가십보단 팩트를, 재미있지만 품격있게!

## 대기업·공공기관도 랜섬웨어에 속수무책...민관, 한미 공조 나선 정부

CJ·LG 등 해외법인도 뚫렸다...계약서 등 내부 문서 유출
몸값 받으려고 사업 마비시켜..."공급망·ERP 등 노린 공격 ...
KISA·국정원, 실시간 정보 공유 나선다...AI·빅데이터도 동원
국정원, 6월 위협정보서비스 개시..."얼마나 빠르게 공유하...

등록 2021-06-03 오전 4:00:12
수정 2021-06-03 오전 4:00:12

이후섭 기자

N 기자구독

스크랩 URL복사

지금 열독 중

文대통령 "국민분노' 그냥 못넘

잡탕밥 배식에 방임 학대한 요

주가 급등 예측한 인공지능, 거

by Dable

[이데일리 이후섭 김국배 기자]


[이데일리 김정훈 기자]

https://www.edaily.co.kr/news/read?newsId=01151286629078112&mediaCodeNo=257&OutLnkChk=Y

## 랜섬웨어 새 국면...민감정보 빌미로 개인과 직접 '딜'

발행일 : 2021.06.04

[줌쇼TV] Zero Trust의 실제 적용을 위한 IBM의 최신 기술 (6/16 생방송)


<게티이미지뱅크>

https://www.etnews.com/20210604000138

# 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.

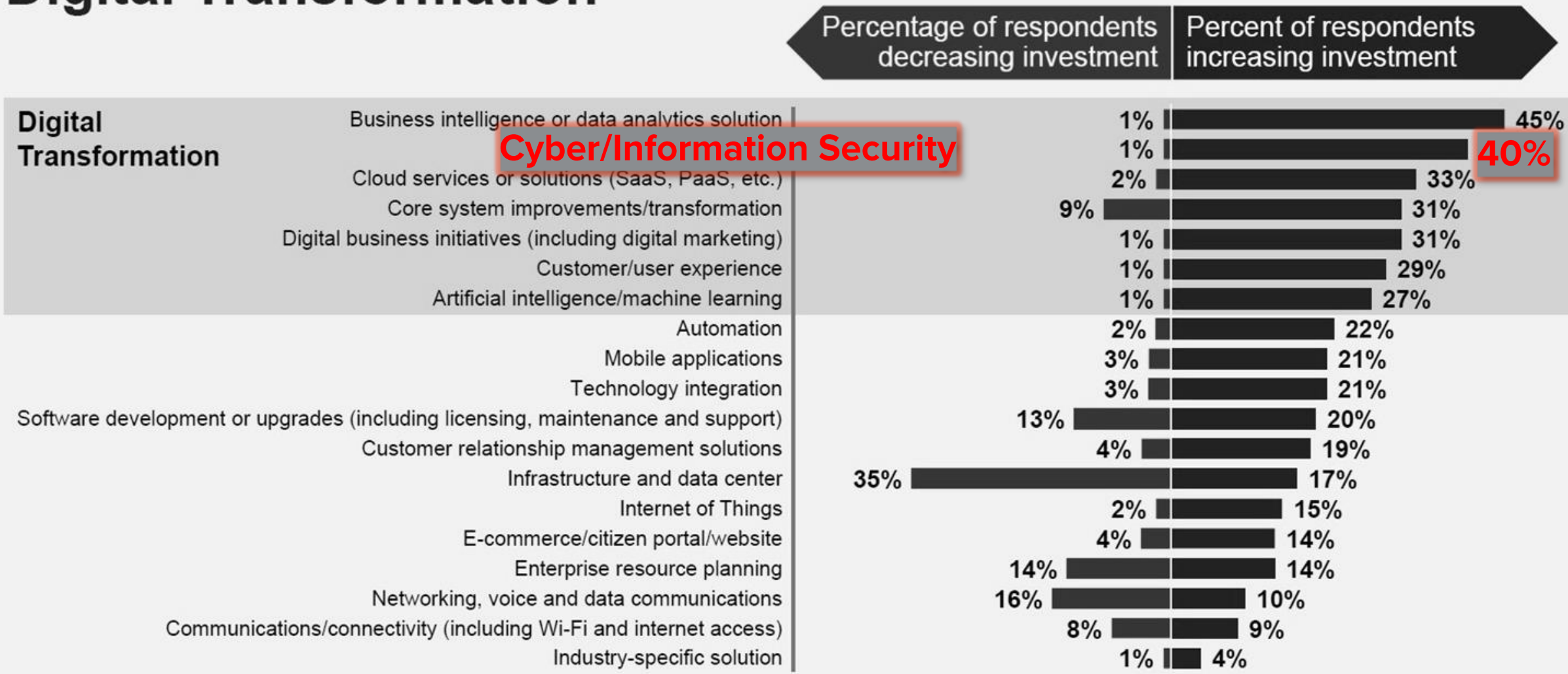
Buy [redacted]-Decryptor

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$)

# Rebalance Your Technology Portfolio Toward Digital Transformation



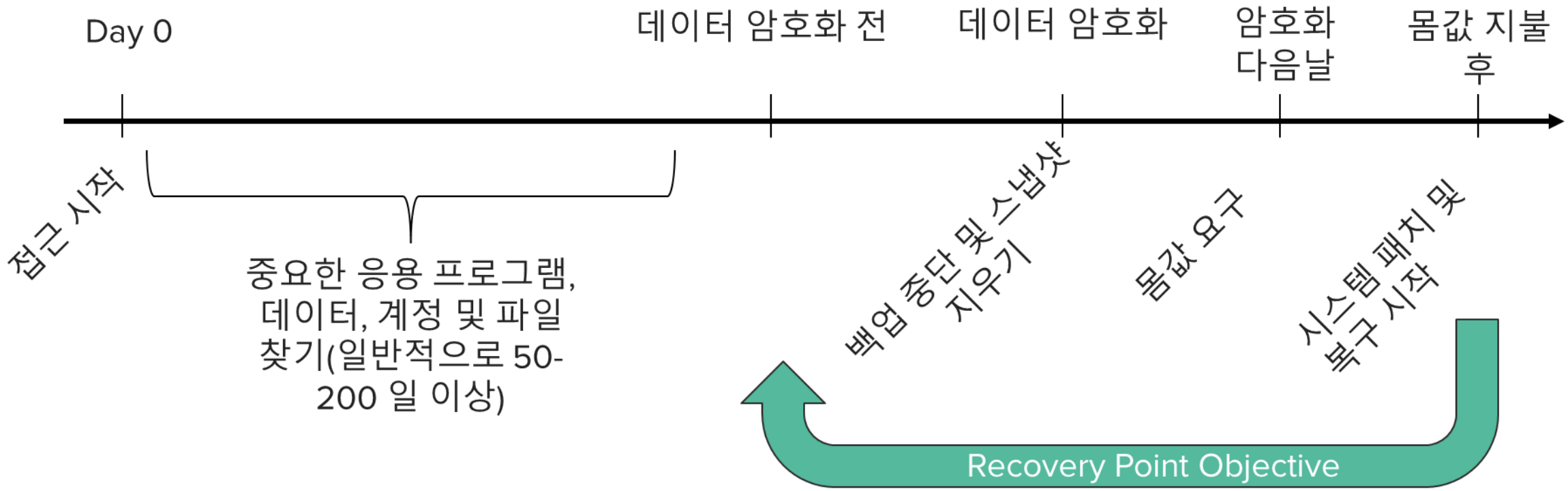

Q. What are the technology areas where your organization will be spending the largest amount of new or additional funding in 2019? n = 3,086; Base: Excludes don't know

Q. What are the technology areas where your organization will be reducing funding by the highest amount in 2019 compared with 2018? n = 2,819; Base: Excludes don't know

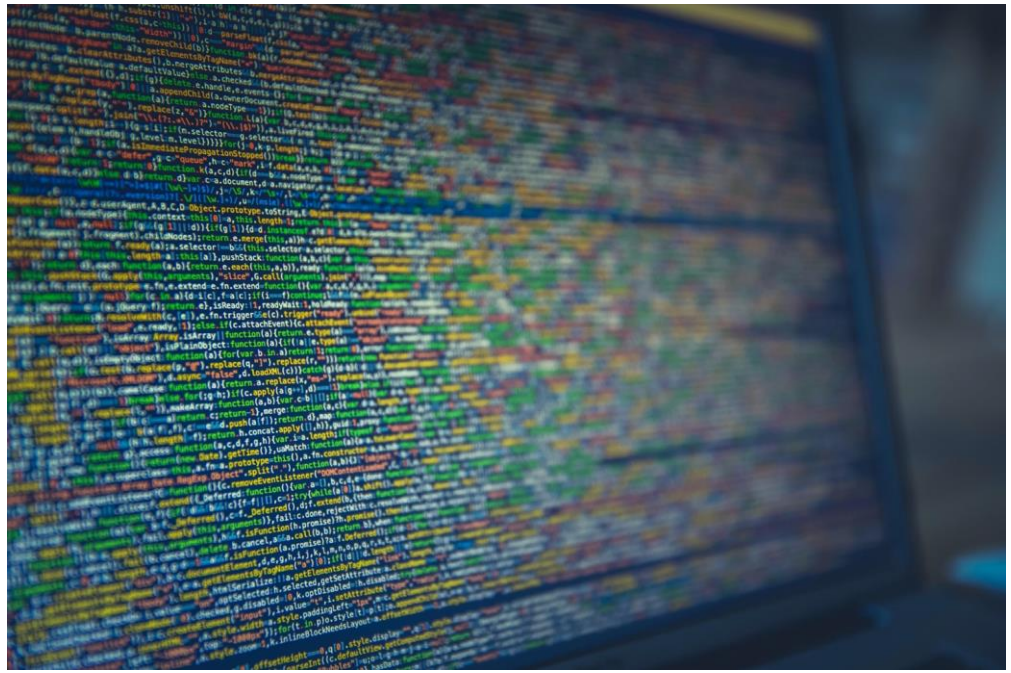



Gartner

# 랜섬웨어 공격 구조



# 공격을 받았다면 다음 두 가지 대응이 필요합니다.



랜섬웨어 공격에도
**유효하고 사용가능한 데이터 복사본**


복구 범위가 광범위하기 때문에
**가능한 가장 빠른 복구**

# FIRST LINE OF DEFENSE

## 항상 사용가능한 데이터 복사본

Nothing is faster than metadata.

# 간단하고 위/변조불가능한 **Snapshots**

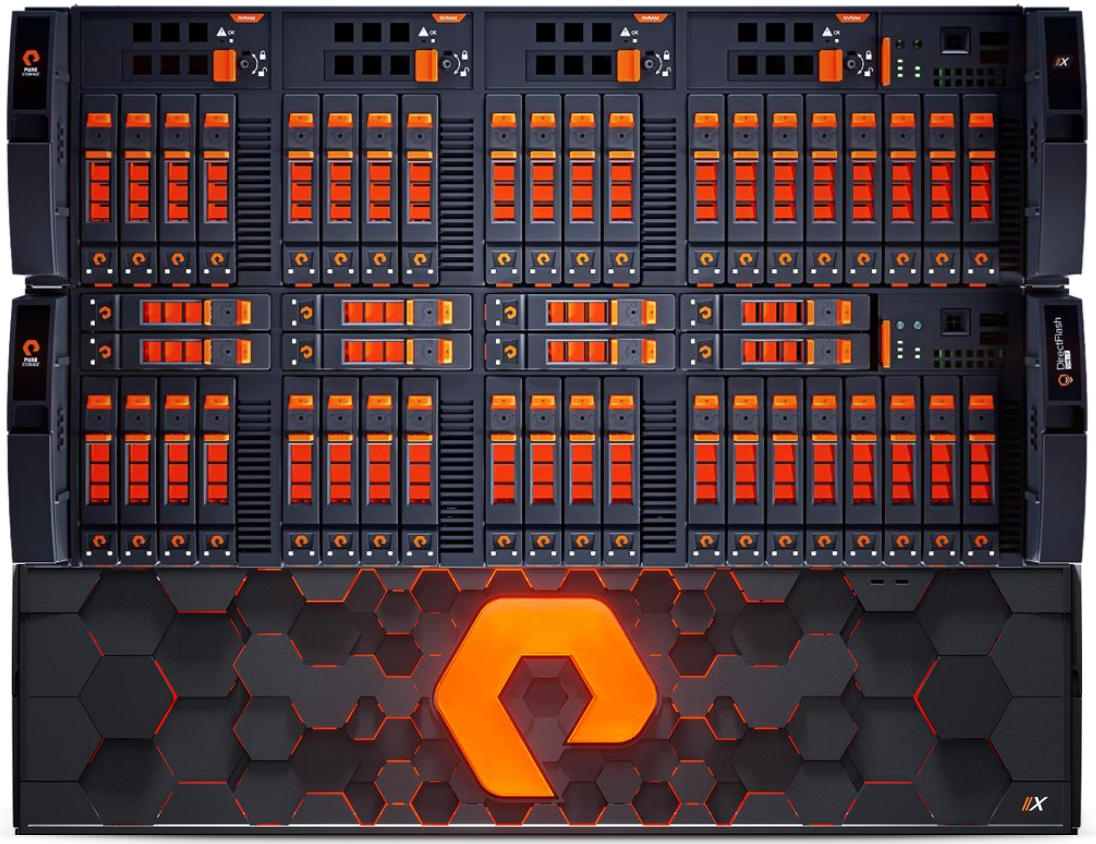
어느 볼륨이든 즉각 스냅샷 생성
성능 오버헤드 없음

완전한 새로운 볼륨 스냅샷
마운트, 읽기/쓰기, 스냅샷 재수행 가능

공간절약
항상 중복제거/압축 적용

언제 어디서든 복구 가능
모든 스냅샷에서 모든 볼륨 복구

FlashArray Volumes
**100% Metadata**



# FIRST LINE OF DEFENSE

## 항상 사용가능한 데이터 복사본

Nothing is faster than metadata.

# FlashArray with SafeMode Snapshots

Safemode Snapshot을 사용하여 해커에 의한 데이터 삭제를 막을 수 있습니다.




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

VEEAM



PURESTORAGE®

# Ransomware Attack without SafeMode

1. 해커가 FlashArray 데이터를 암호화합니다. 하지만 스냅 샷은 변경할 수 없습니다.

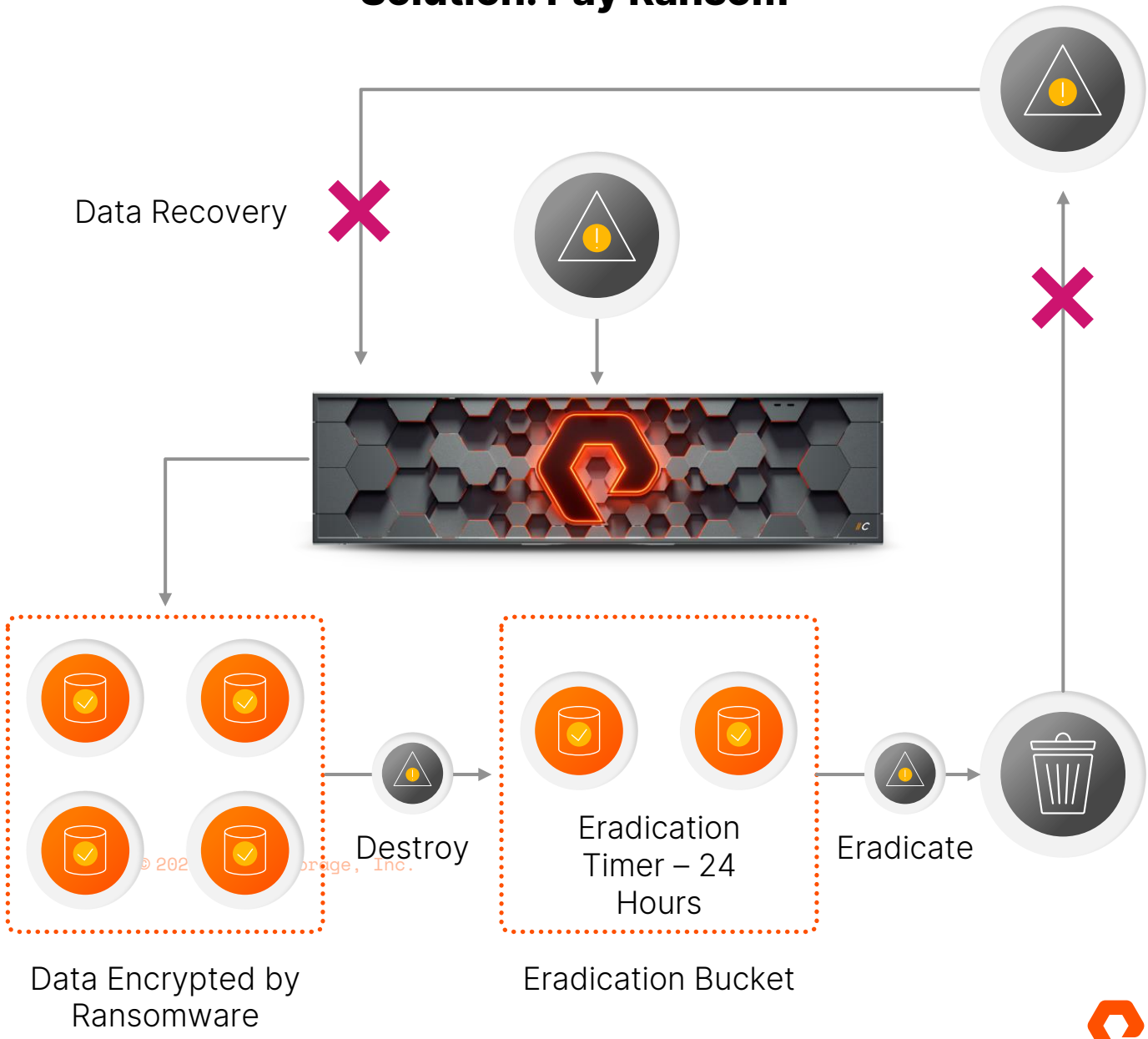
2. 해커는 변경 불가능한 모든 스냅 샷을 삭제합니다.

3. 스냅 샷 / 암호화 된 데이터는 휴지통에서 해커에 의해 수동으로 제거됩니다.

4. 스냅 샷이 없으면 데이터를 복구 할 방법이 없습니다.

VEEAM

**!!!ATTACK!!!**
**Solution: Pay Ransom**



# Ransomware Remediation with SafeMode

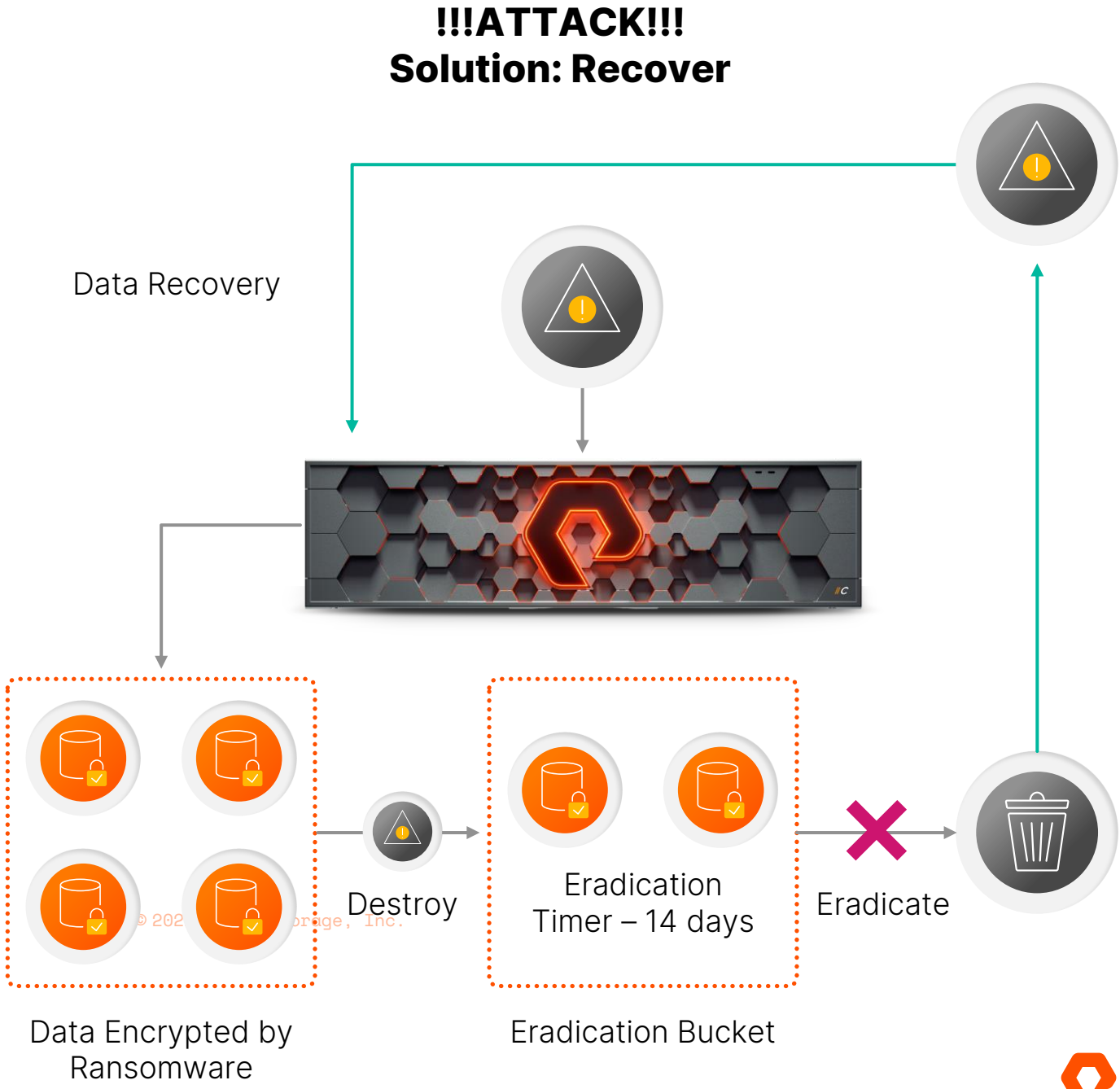
1. 해커가 FlashArray 데이터를 암호화합니다. 하지만 스냅 샷은 변경할 수 없습니다.

2. 해커는 변경 불가능한 모든 스냅 샷을 삭제합니다.

3. 삭제된 볼륨은 휴지통에 보관되며 해커가 수동으로 삭제할 수 없습니다.

4. 공격이 식별되면 휴지통에 보관된 스냅샷을 활용하여 서비스를 즉시 복구 할 수 있습니다.

VEEAM



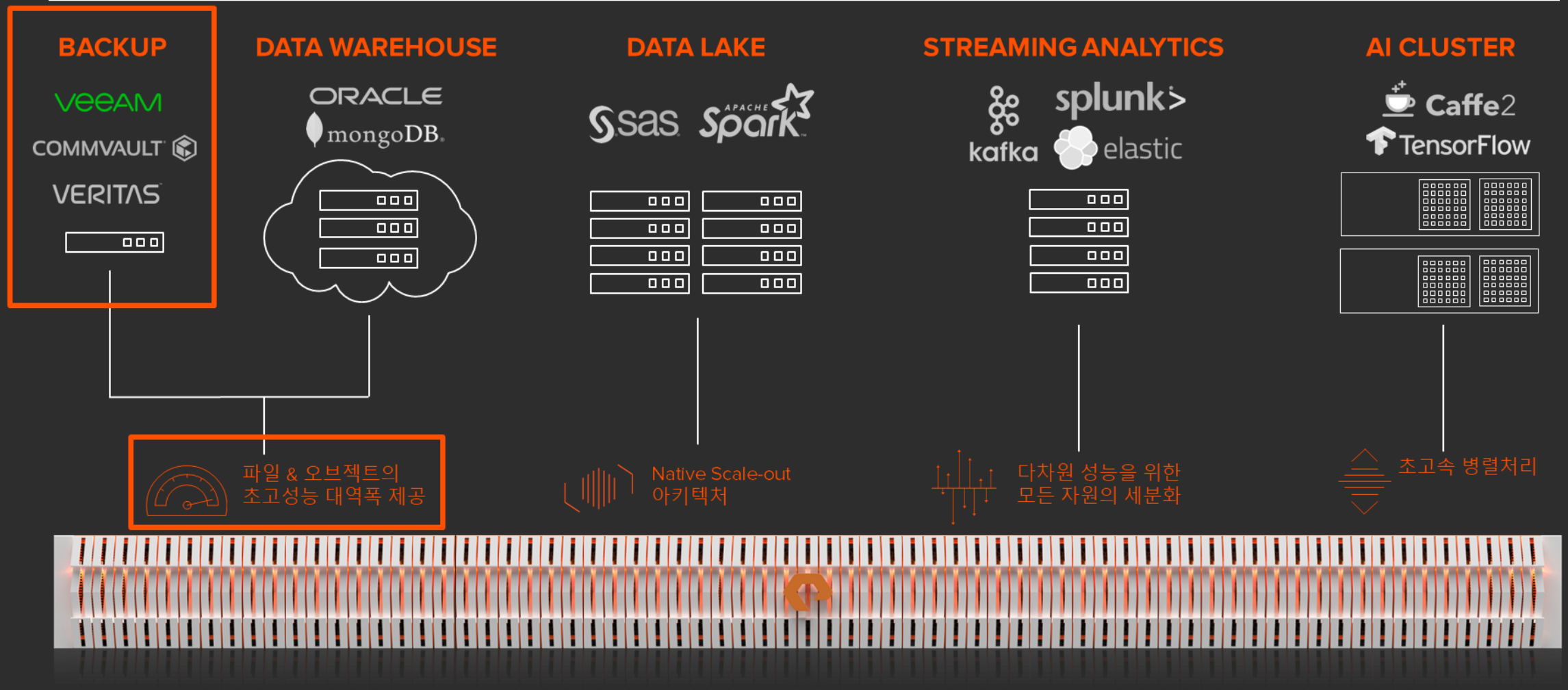
# SECOND LINE OF DEFENSE

## 가능한 가장 빠른 복구

Protecting Your Backups

# FLASHBLADE™

## 업계 최초의 DataHub 플랫폼




VEEAM

PURESTORAGE®

# 최대 시간당 270TB를 복구할 수 있는 Rapid Restore 스토리지


**최대 백업 속도:**
**90 TB/HR**

**최대 복구 속도:**
**270 TB/HR**

**Scale-out 아키텍처:**
**용량 증가 시 성능도 같이 증가**

**SMB, NFS, S3**

# SAFEMODE SNAPSHOTS

변경 불가능한 스냅샷

**(관리자도 삭제 불가능)**

스냅샷은 정책에 의해 생성/삭제 됨

정책은 Pure 본사와 회사 지정자 만 수정할 수 있습니다.

백업 데이터 및 메타데이터를 보호합니다.

**FlashBlade 에 포함된 기능으로 무상 제공합니다.**

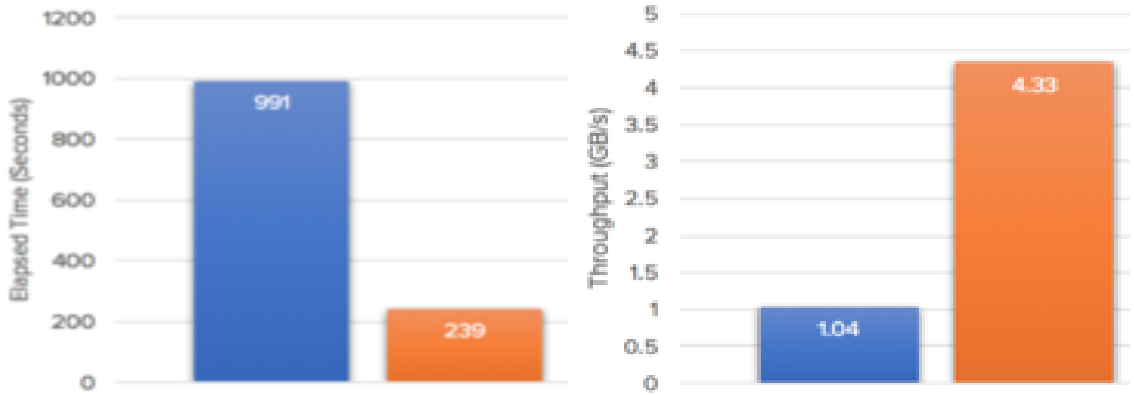
VEEAM

PURESTORAGE®

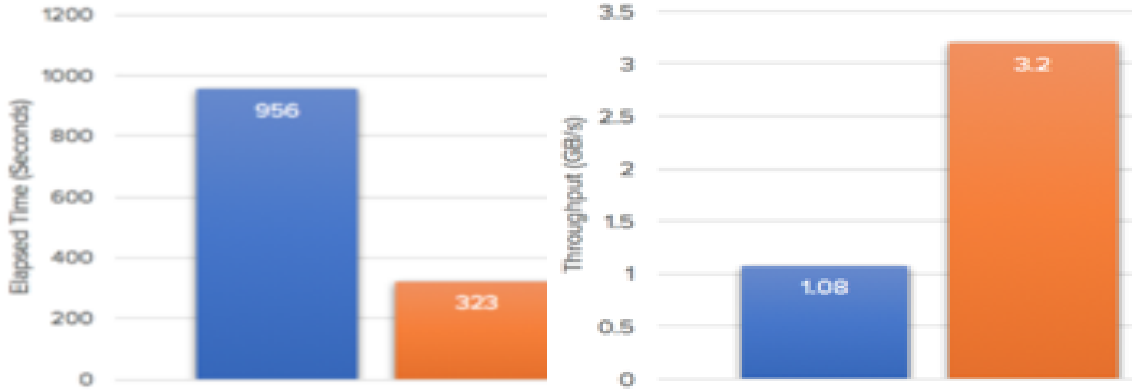
# DNFS VS. KNFS 성능 검증 결과

국내 실 고객사 RMAN 백업 시간이 기존 **17시간에서 2시간으로 단축**

## 백업 성능 차이




## 복구 성능 차이




- **A사 RMAN Backup 성능 개선 효과**

### Kernel NFS

| Number of Host | Number of Channel | Bandwidth | | Estimated Backup window |
|---|---|---|---|---|
| 1 Host | 4 Channels | 172 MB/s | 619GB/h | 17 hr 35 m |
| | 8 Channels | 266 MB/s | 957.6GB/h | 11 hr 20 m |
| | 16 Channels | 608 MB/s | 2,188GB/h | 5 hr |

### Direct NFS

| Number of Host | Number of Channel | Bandwidth | Estimated Backup Window |
|---|---|---|---|
| 1 Host | 4 Channels | 837.11 MB/s | 3 hr 40 m |
| | 16 Channels | 1.4 GB/s | 2 hr 10 m |
| 2 Hosts | 16 Channels | 2.7 GB/s | 1 hour 10 min |

# 고성능 SQL 백업 솔루션

SafeMode를 이용하여 향상된 랜섬웨어 복구 기능 제공

빠른 SQL 백업 및 복원을 통해 가장 까다로운 대규모 SLA 충족

4배 백업 성능 개선
70TB/hr 백업, 43TB/hr 복구 성능
6x9 엔터프라이즈 가용성
성능 영향없는 상시 데이터 암호화


Backup Speeds

>70 TB/hr

Restore Speeds

Up to 43.78 TB/hr*



*Restore Speeds may vary depending on SQL Server source storage array

# 현대화된 백업 아키텍처: 초고속 복구

**SaaS 회사의 데이터 및 클론 환경 복구하는 데 30 시간에서 30 분으로 절감 (50배 이상 개선)**

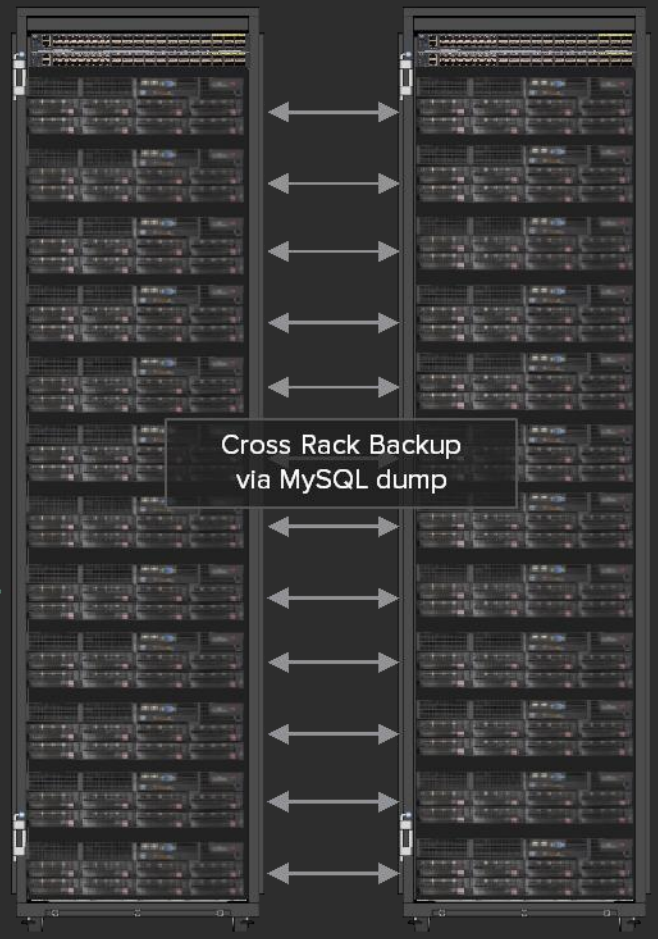
## 재래식 아키텍처

3RU Servers

$45k per Server

서버 당 6개 SSD
(3개는 DB, 3개는 복구용)

**완전 복구 또는 Test/Dev를 위한 클론 구성에 38시간 소요**




## 현대화 아키텍처

1RU Servers

$10k per Server

서버 당 2 SSD
(DB 어플리케이션 용도)

FlashBlade로 백업 수행

**완전 복구 또는 Test/Dev를 위한 클론 구성에 0.5 시간 소요**

**랙 당 3배 더 많은 서비스 제공**

VEEAM

PURESTORAGE®

PURESTORAGE®

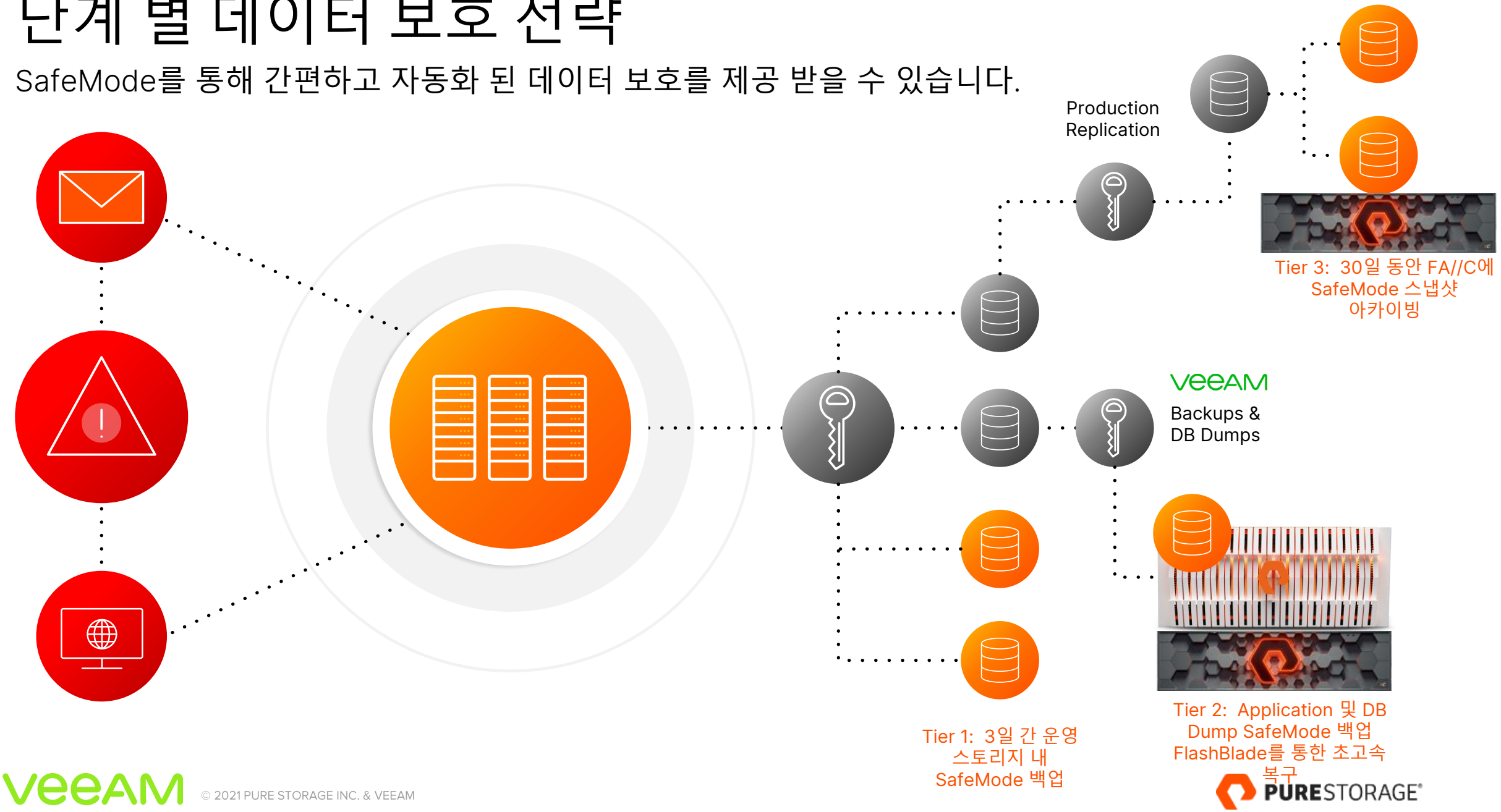
VEEAM

# 데이터보호 현대화전략

## 단계 별 데이터 보호 전략

# 단계 별 데이터 보호 전략

SafeMode를 통해 간편하고 자동화 된 데이터 보호를 제공 받을 수 있습니다.




VEEAM

홈페이지 : www.purestoreage.com/KR
대표이메일 : Korea@purestorage.com