

# RR4400 Backup Appliance

복잡한 복구 과정과 다운타임 최소화 재해복구(DR)솔루션

*“서버 자체 랜섬웨어 감염시에도 100% 복구 보장 유일 백업&DR 솔루션”*

아이비인포텍(주)



# 관리자를 위협하는 악성코드/랜섬웨어 대처는??

## 내 컴퓨터에 있는 파일은 안전할까요?

- 2015. 4. 21. 국내 모 커뮤니티 사이트에서 한글버전 랜섬웨어 “**크립토락커**” 유포
- 기존 랜섬웨어의 경우 이메일의 첨부파일을 통해 공격하였으나, 이번에는 **웹 사이트에 방문만 해도 자동으로 PC에 악성코드나 프로그램이 설치되는 방식으로 유포**
- DDoS 공격 기능을 갖춘 신종 랜섬웨어 등장

## ? 랜섬웨어란?



사용자의 문서 등 **중요 파일**을 **암호화**하여 파일을 사용할 수 없게 만든 후 **암호를 풀어주는 대가로 금전을 요구**하는 신종 악성코드



## <한글버전 랜섬웨어 크립토락커 감염 화면>



## 랜섬웨어 감염 피해를 예방하려면?



인터넷 익스플로러, 플래시 플레이어, 자바 등에 대한 최신 보안업데이트



백신 소프트웨어 최신 업데이트

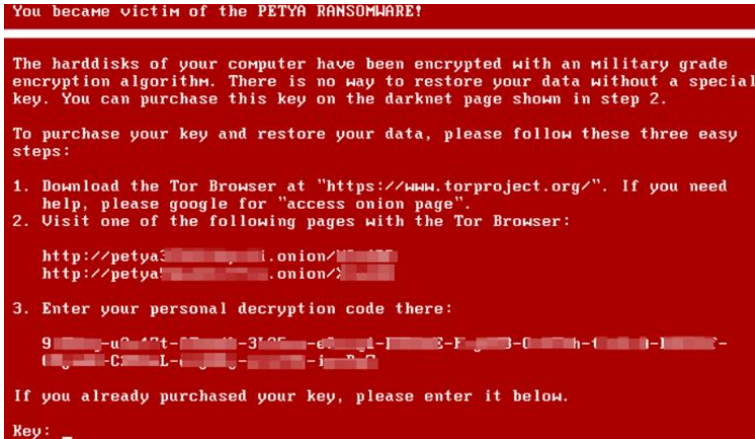


PC내 중요 파일 백업(가장 중요)

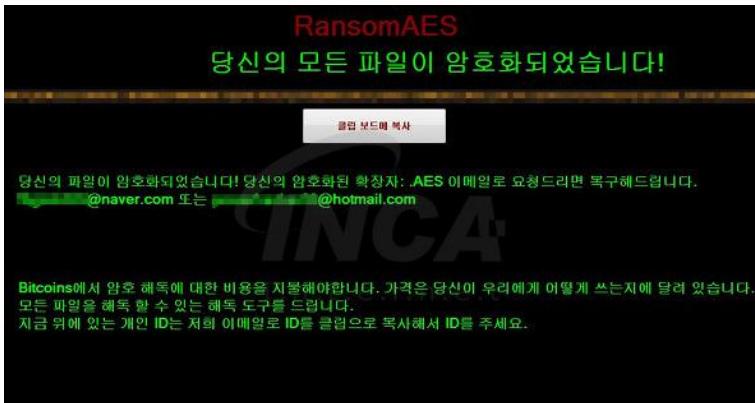
경기교육사이버안전센터(GECSC)

# 백업서버도 랜섬웨어에 안전하지 않습니다.

## 백업본 암호화, 복구 불가능

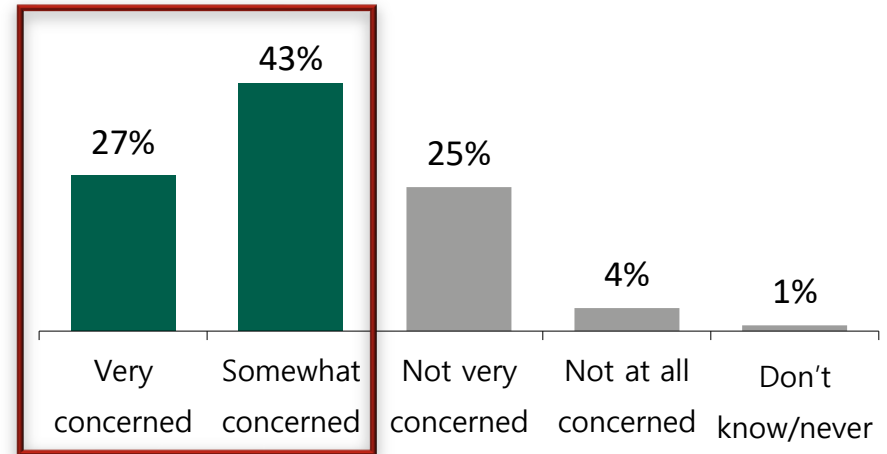


## 부팅 및 Disk 암호화 / 복구 불가능



## 백업저장소 암호화 / 복구 불가능

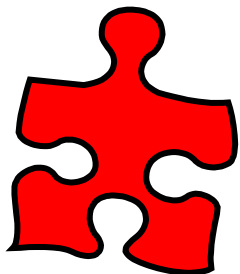
## 백업 DATA도 안전하지 않습니다.



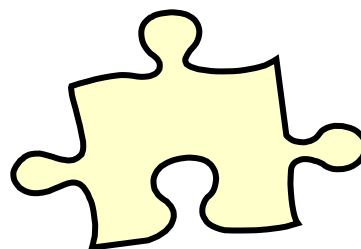
ESG 2018 Data Protection Landscape Report, October 2018

**70%의 고객은**  
백업의 오염에 대해  
우려하고 있습니다.

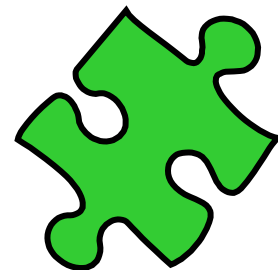
# 기존 전통적인 백업 솔루션의 복잡성 & 문제



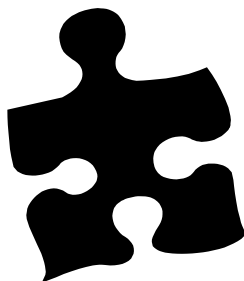
DATA 백업  
솔루션



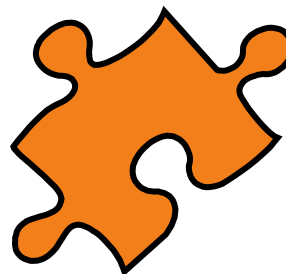
Backup Server 필요



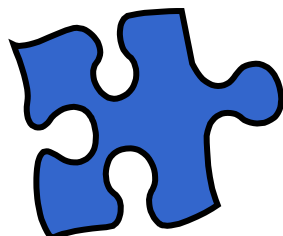
백업용 스토리지



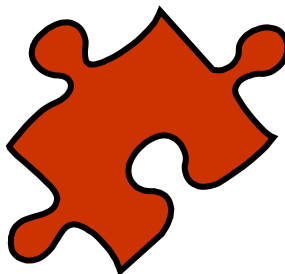
시스템 백업 솔루션



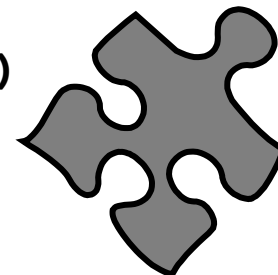
백업본 손실 대비  
DR  
대책(TAPE..복제)



서버 종설  
Client라이선스  
추가 구매



기술지원 이원화 문제  
(H/W, Backup S/W, DR S/W)



Physical vs. Virtual

# RR4400 백업 어플라이언스 개요

RR4400 Backup Appliance 시리즈는 검증된 서버 및 스토리지 플랫폼에 통합 백업 재해복구솔루션인 Quest Rapid Recovery 소프트웨어를 사전 탑재된 형태로 제공이 되며, 기본 제공되는 중복제거 백업 기술과 사용 편의성, 심플한 DR 복제 및 가상화 환경 백업을 기본 지원하여 도입 및 운영 환경의 비용 절감 효과 등을 기대할 수 있는 제품입니다.

## 백업/DR 솔루션 탑재 - Quest Rapid Recovery

- 윈도우 및 Linux 환경 통합 이미지 백업 구현
- 대상 서버 수량에 제한 없는 무제한 Agent 모듈
- 중복 제거 스토리지 기술 기본 탑재
- 물리적 서버 및 가상화 서버의 통합 백업 및 보호
- 가상화대기 기능을 통한 즉각적인 서비스 재개 가능
- 모든 서버 재해 환경을 대비한 복구 시나리오 제공

## 관리 편의성 / DATA 복원 보장 / 최고의 기술지원

- 단일 관리 콘솔에서 백업, 복구, DR복제, P2V 제공
- **랜섬웨어 감염시에도 H/W 스냅샷을 통한 복원 보장**
- H/W와 S/W를 포함한 Appliance 전체를 IB인포텍에서 통합 기술지원

## H/W 도입 비용 및 운영 비용 감소

- OS, Server, Storage, Backup Solution, Anti Virus가 통합된 Appliance 타입으로 도입비용 절감
- 각각의 인프라를 별도로 운영하는데 소요되는 인건비 및 유지보수 비용을 크게 감소



# RR4400 백업 어플라이언스 - 주요 특징



## 심플한 구성

- System Pre-Installed (시스템 사전 설치 출고)
- 빠른 설치 및 백업 가능
- 빠른 백업 / DR 구성
- 단일 기술지원 제공
  - 하드웨어 장애
  - 소프트웨어 장애

## 비용 효율적

- 무제한 서버 Agent 지원 (기본 10TB 라이선스 제공)
- OS 시스템 / DATA 백업지원
- Windows / Linux 지원
- 가상화 백업 기능 기본 제공
- 중복제거 백업 기능을 통한 스토리지 용량 절감

## 빠른재해복구

- Virtual Standby 기능으로 장애 즉시 서비스 가능
- 원본 대상 서버 빠른 복구
- DR 복제 기능 무상 제공
- 백업 HW 스냅샷 기술로 랜섬웨어 감염시에도 100% 복구 가능

# RR4400 Backup Appliance 구성 (고급형)



고사양  
어플라이언스

검증된  
Backup  
S/W



안티  
랜섬웨어  
기능 탑재

뛰어난  
확장성



**Xeon Silver 4110 8Core 2.1Ghz \* 2CPU**  
(8C/16T, 11M Cache)



**Memory** - 64GB RDIMM, 2666MT/s



**SSD Disk** - 2 x 480 GB RAID 1 (OS)



**Backup Storage** - 기본 21TB / 스냅샷지원  
iSCSI 10Gb \* 2Port (6TB Disk \*5개) 12 Bay



**Ethernet** - 4 x 1Gb Ports



**Software** - Quest Rapid Recovery  
Windows 2016 STD + Win Defender (AV)



**Anti Ransomware 기능 탑재**  
H/W 스냅샷 기술을 통한 100% 복구 보장

추가  
옵션

10Gb Ethernet - 2 Port  
백업 DATA 소산용 RDX QuikStation



# RR4300 Backup Appliance 구성 (표준형)



고사양  
어플라이  
언스

검증된  
Backup  
S/W



안티  
랜섬웨어  
기능 탑재

뛰어난  
확장성



**Xeon E-2124 4Core 3.3GHz**  
(4C/4T, 8M Cache)



**Memory** - 32GB RDIMM, 2666MT/s



**Hard Disk** - 2 x 300 GB RAID 1(OS)



**Backup Storage** - 기본 11TB / 스냅샷지원  
4TB Disk\*4개, Raid 5 구성



**Ethernet** - 4 x 1Gb Ports



**Software** - Quest Rapid Recovery  
Windows 2016 STD + Win Defender (AV)



**Anti Ransomware 기능 탑재**  
H/W 스냅샷 기술을 통한 100% 복구 보장

추가  
옵션

10Gb Ethernet - 2 Port  
백업 DATA 소산용 RDX QuikStation



# RR4400 백업 어플라이언스 - 전체 기능 소개

## 시스템 이미지 백업 및 DR 복제, 랜섬웨어 완벽 대응

### 시스템 백업

- **Agent 기반 백업**
  - 물리적 머신
  - 가상 머신
  - 클러스터
- **Agentless 백업**
  - VMware ESXi
  - Hyper-V

### 복구

- **시스템 복구**
  - HW 시스템 및 VM 복구
  - BMR 및 이기종 복구
  - P2P, P2V, V2V, P2C 등
- **데이터 복구**
  - 파일레벨 복구
  - 메일단위 레벨 복원
- **VM Export**

### 원거리 복제

- **DR 복제 기능제공**
  - WAN 복제 기능 무상
  - 1:1, N:1, N:N 구성
  - 양방향 크로스 복제
- **WAN 최적화**
  - 네트워크 대역폭 조절
  - 중복제거 복제
- **지역적 사고/자연재해 대비**

### Archive

- **백업 소산(아카이브)**
  - Local
  - Network
  - Cloud Storage
- **RR4400의 추가 옵션 기능의 RDX QuikStation과 연동 소산 가능**
- **랜섬웨어 감염시 대비 2차 소산 기능**

### 효율적인 백업 기능 탑재



중복제거 백업



백업데이터 압축



백업본 정합성 보장



백업본 암호화

### 랜섬웨어 완벽 대응



Windows Defender로 악성 코드 기본 차단

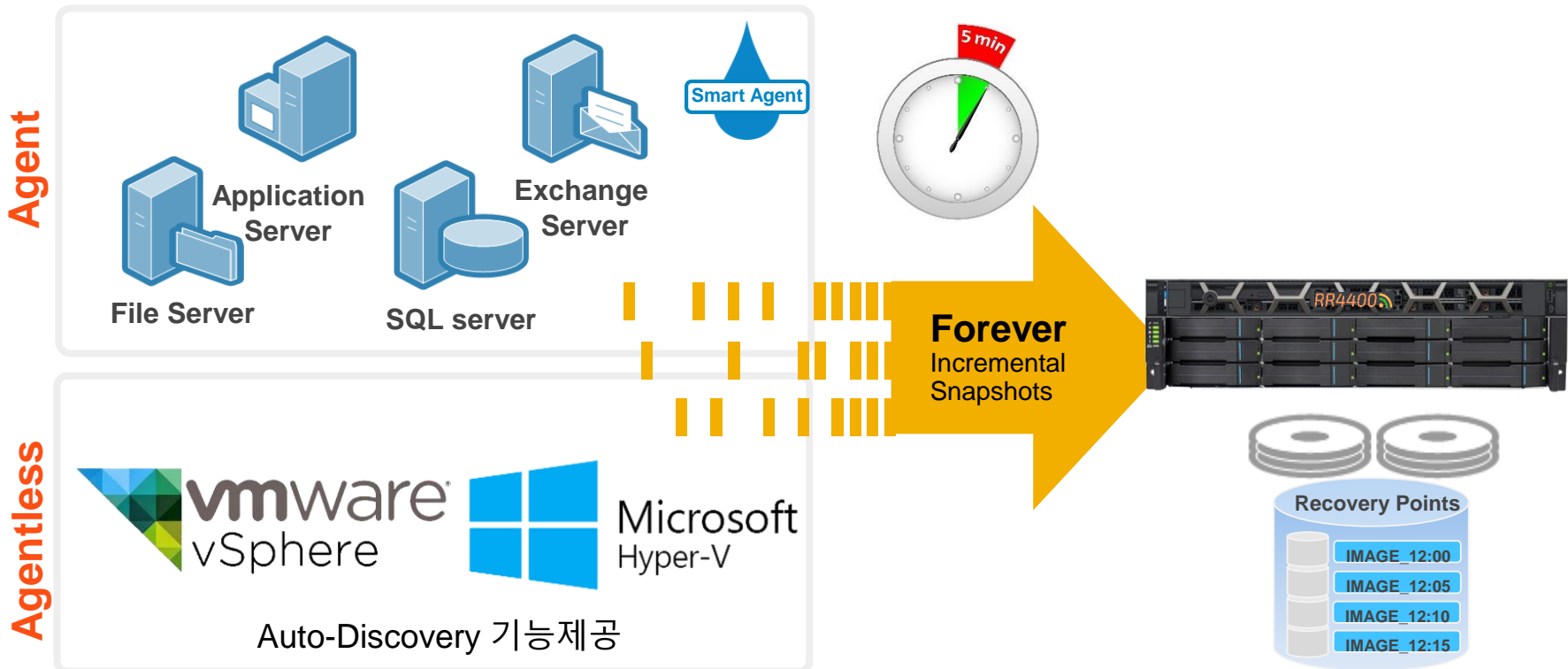


H/W 스냅샷 기술을 통한  
서버 및 백업 저장소 100% 복구 가능

# 기능 1. Windows 및 Linux 시스템 백업

## 이미지 스냅샷 백업 + 영구증분백업

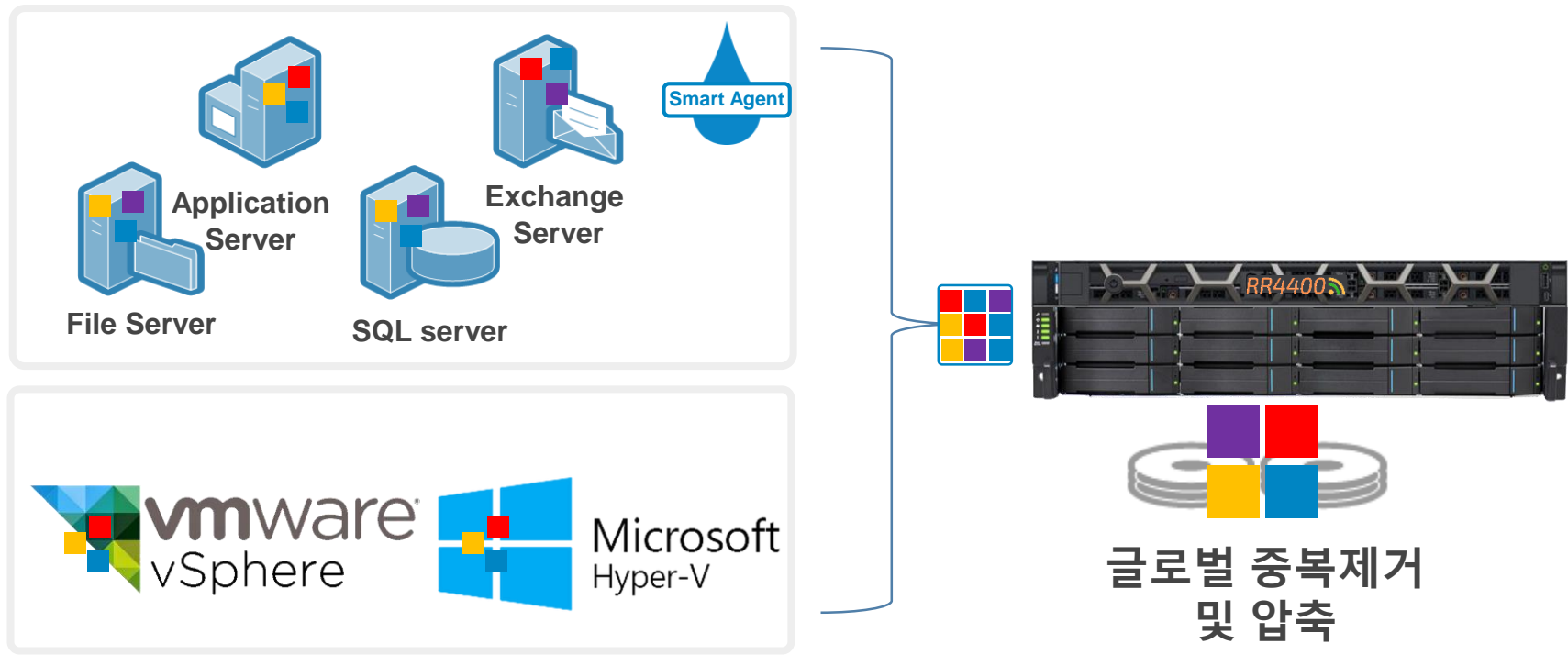
- 변경블록 이미지 스냅샷 백업: 저장 공간 및 백업 IO 최소화
- 스냅샷 백업은 5분 주기 생성: 손실 데이터(RPO) 최소 5분
- 풀백업이 없는 영구 증분 백업 방식으로 빠른 백업 가능



## 기능 2. DATA 중복제거 백업 저장소 기능

### 중복 제거 및 압축 백업

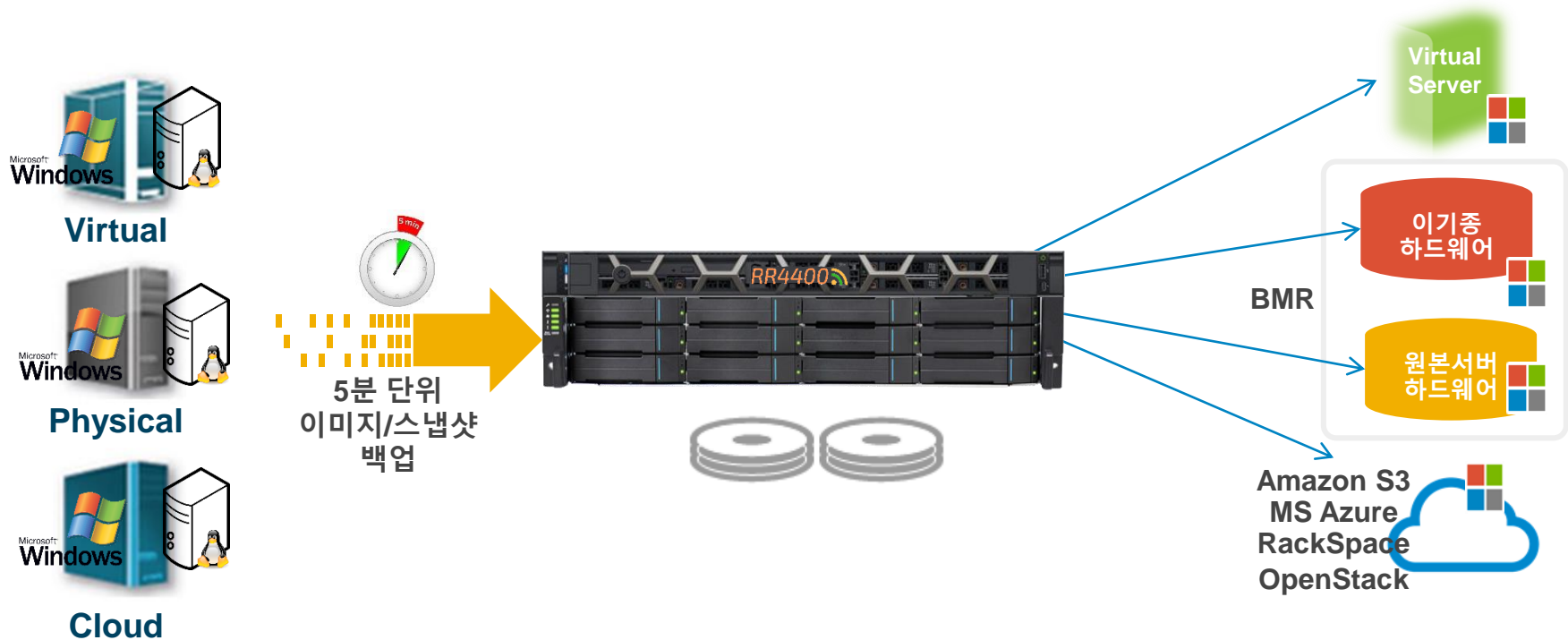
- 중복제거 및 압축을 통해 백업 스토리지 용량 절감(80% 이상의 효율)
- 백업 저장소에 저장되는 모든 데이터에 대한 글로벌 중복제거 가능
- 중복제거 및 압축을 통한 빠른 원거리 DATA 복제 가능



# 기능 3. 어떤 상황에서도 빠른 복구 지원

## Universal Recovery

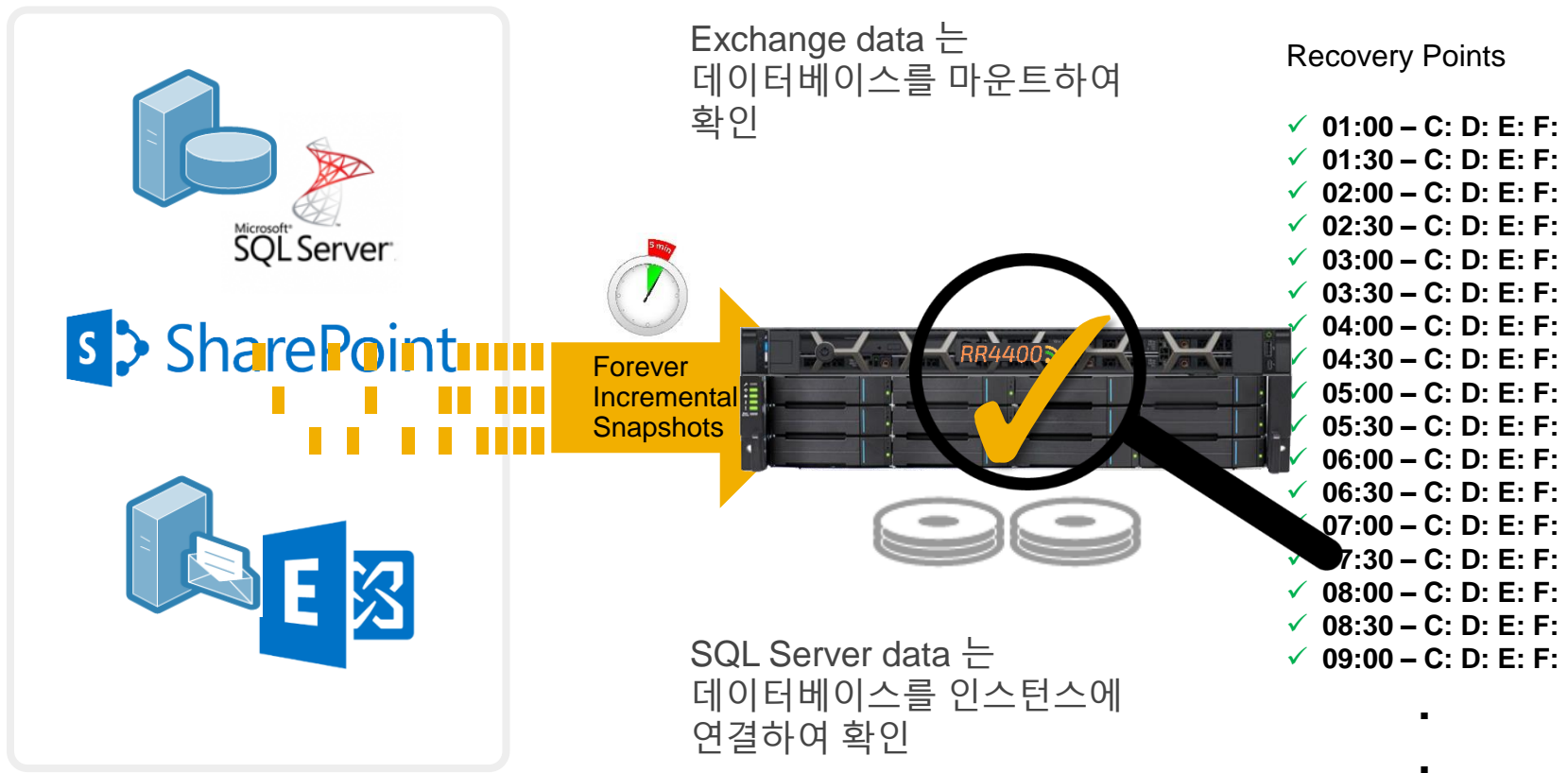
- 백업된 OS 는 이기종 HW 플랫폼에 복구 가능
- VM의 물리적 시스템으로 Migration 가능
- P2P, P2V, P2C, V2V, V2P, V2C, C2P, C2V 지원



## 기능 4. 백업 정합성 자동 검사 기능

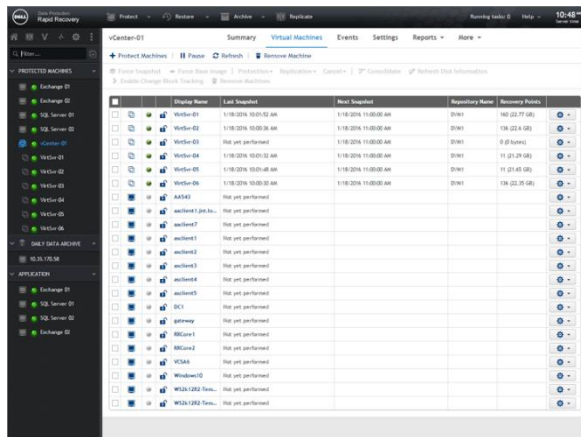
### Auto Verified Recovery™

- 백업된 Data 의 자동 정합성 검사 (실제 복구 가능 자동 검증)
- 중요 서버(메일,DB,웨어포인트) DATA 내 데이터 접근 복구 가능 검증



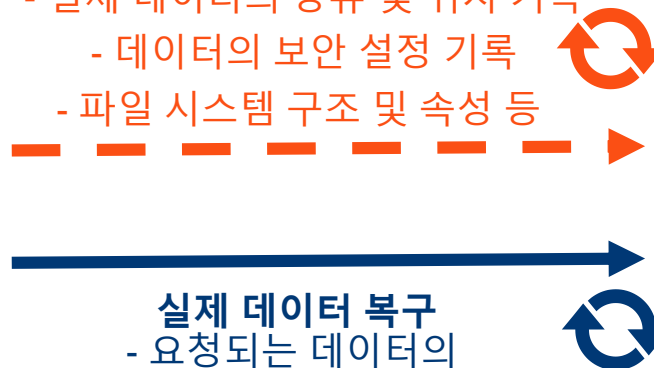
# 기능 5. 복원 작업 시작 후 즉시 서비스 기동 Live Recovery

- 복원 작업 시작 즉시 데이터 접근 및 서비스 기동(File, SQL, Exchange)
- 메타데이터 복구 및 백업된 볼륨을 복원 서버에 가상 마운트 및 서비스
- 복구 작업은 백그라운드로 수행, 복구 데이터는 요청된 우선 순위에 따라 복구되며, 변경 & 추가 생성 데이터 또한 최종 복구에 반영됨.

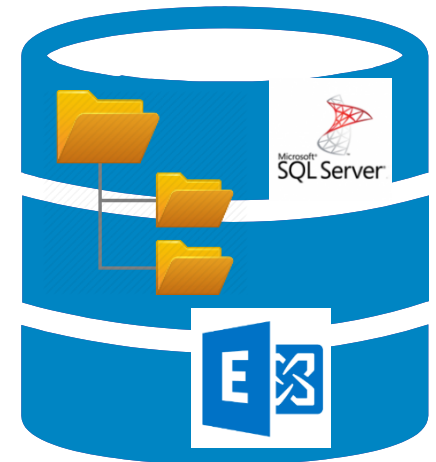


## Rapid Recovery Console

- 메타데이터 복구**
- 실제 데이터의 종류 및 위치 기록
  - 데이터의 보안 설정 기록
  - 파일 시스템 구조 및 속성 등



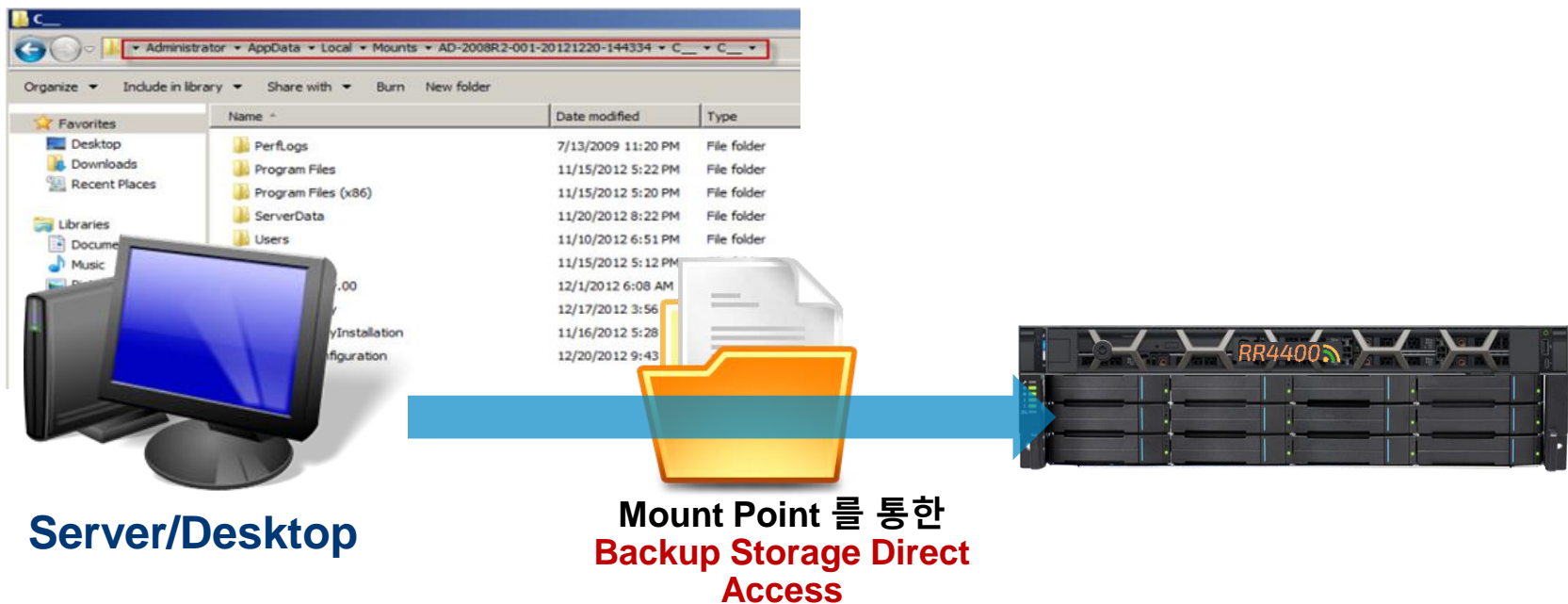
- 실제 데이터 복구**
- 요청되는 데이터의 우선순위에 따른 복구작업
  - 애플리케이션 및 사용자는 모든 데이터를 투명하게 사용할 수 있음



백업 저장소 내 복구 대상 볼륨을  
실제 서버에 가상 마운트

## 기능 6. 개별 객체 단위 복구 Individual Object Restore

- 개별 객체 단위 복원용 유틸리티 LMU(Local Mount Utility) 제공
- 대상 시스템의 신속한 복구: File & 폴더, Sharepoint, Exchange Mailbox
- Network drive 형태로 백업 데이터가 제공됨

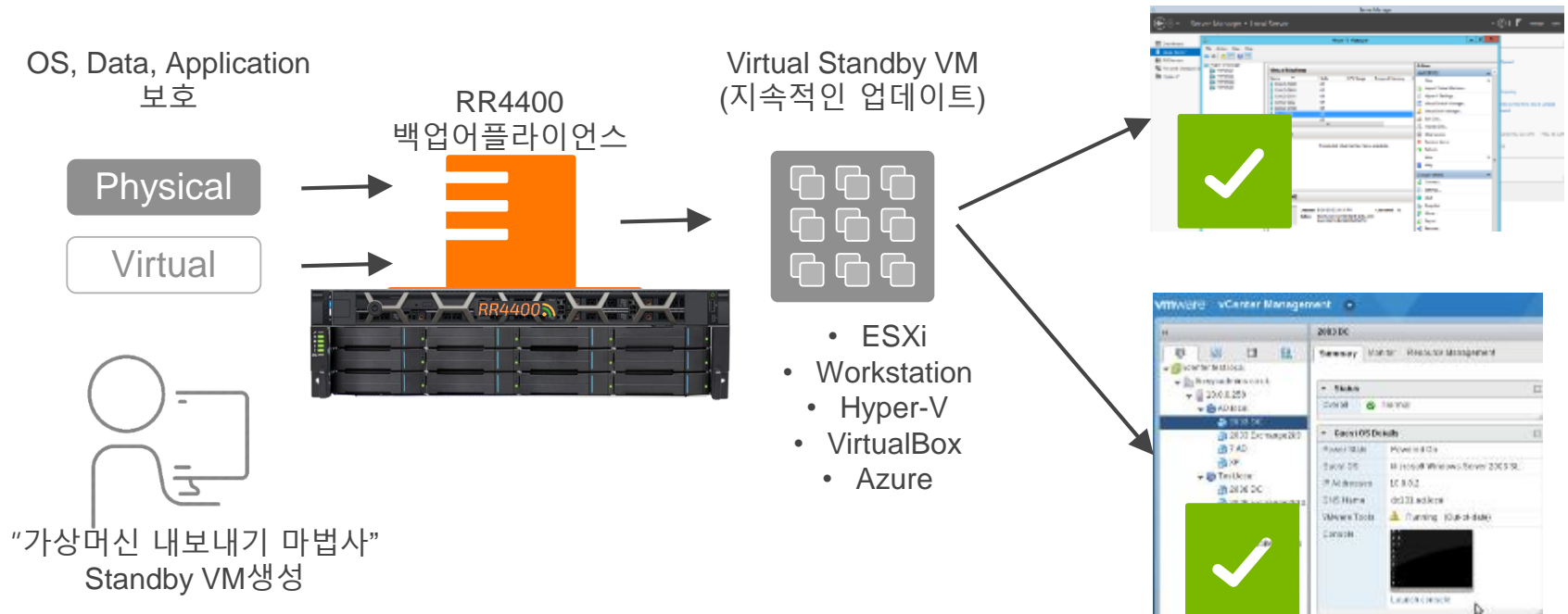




# 기능 7. 가상시스템 대기 기능

## Virtual Standby

- 백업된 데이터를 Virtual Machine 으로 P2V 변환 및 운영
- 백업 즉시 자동으로 증분 P2V를 통해 VM 업데이트
- 서버 장애시 Standby VM을 가동하여 매우 빠른 서비스 재개
- VMware, Hyper-V, VirtualBox 및 Azure 가상화 환경으로 직접 배치



## 기능 8. 원거리 DR 복제 기능

### WAN DR Replication

- DATA 중복 제거 복제 기술로 적은 Network 대역폭으로도 원거리 복제
- M:N의 유연한 복제 토폴로지 구성을 통해 다양한 형태의 Replication 구현
- 복제 라이선스 무상 제공



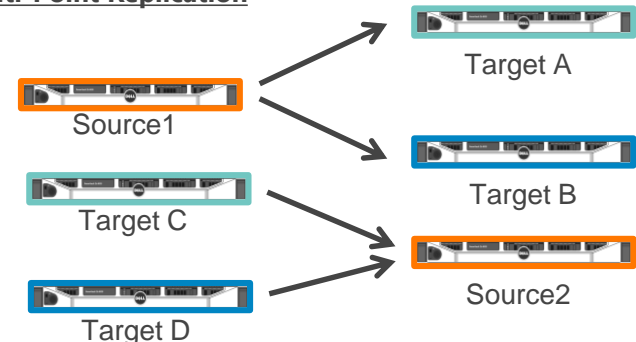
#### Simple Replication



#### Cascaded Replication



#### Multi-Point Replication



# 기능 9. 가상화 DR 센터 구성

## WAN 복제 + Virtual Standby = Virtual DR Center

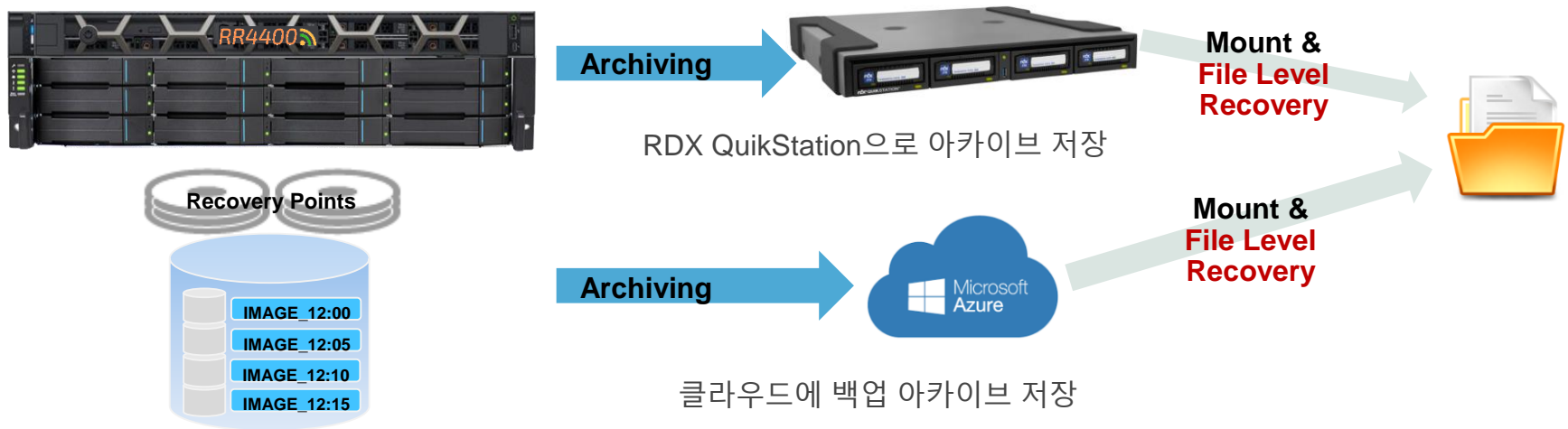
- 원거리 복제 기능과 가상화 대기 기능을 활용한 원거리 DR 센터 구성



# 기능 10. 백업 DATA 소산 저장 기능

## Archive

- 중복제거 백업 저장소의 백업본을 다른 곳으로 복제 저장 하는 기능
- RR4400 의 추가 확장 옵션인 RDX QuikStation 으로 빠른 소산 가능
- 주요 클라우드 환경(AWS, Azure 등)에 대한 Cloud Connector 제공
- 저장된 아카이브는 직접 마운트하여 파일 단위 및 BMR 복구 가능



# 기능 11. 스냅샷을 통한 랜섬웨어 방어 -100% 복원 기능

## Storage Snapshot Protection

- 백업 저장소는 어플라이언스의 전용 스토리지에 구성됨.
- 백업 전용 스토리지는 H/W 스냅샷 기능을 통해 보호 됨.
- 랜섬웨어 감염시 스냅샷을 통해 100% 서버 및 백업저장소 복원 가능

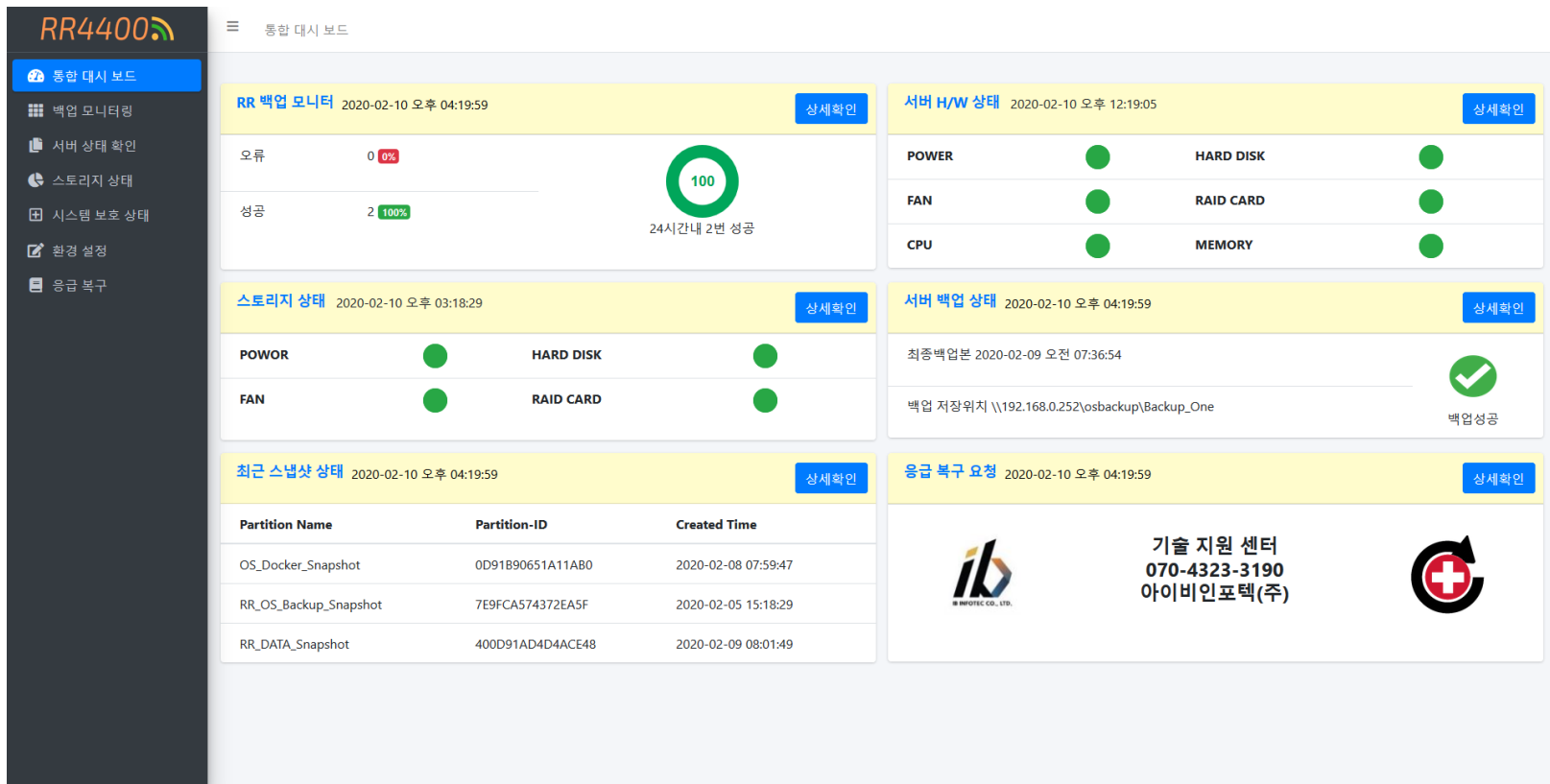


# RR4400 Backup – 가장 심플한 재해복구 솔루션



**“어떠한 상황에서도 복구가 가능한 매우 쉬운 재해복구(DR) 솔루션”**

# RR4400 주요 UI - 통합 대시 보드



- 백업 현황, 서버 및 스토리지 하드웨어 현재 상태를 통합 확인
- 어플라이언스 자체 OS 백업 상태 및 스토리지 스냅샷 확인 가능



# RR4400 주요 UI – 백업 모니터링

**RR4400**

**보호된 컴퓨터**

표시 이름	리포지토리 이름	마지막 스냅샷	다음 스냅샷	복구 지점	버전
192.168.0.57					(없음)
VEEAM_jbyoon	repo	아직 수행되지 않음	2020-02-10 오후 5:00:00	0 (0 바이트)	(없음)
Veeam_M	repo	2020-02-10 오후 4:18:04	2020-02-10 오후 5:00:00	8 (92.79 GB)	(없음)

**복구 지점 전용 시스템**

표시 이름	리포지토리 이름	복구 지점
BK_Test	repo	13 (33.69 GB)
RR4400_VM	repo	6 (47.01 GB)
VM-TEST	repo	60 (6.62 GB)

**DVM 리포지토리**

이름	사용 공간	보호된 데이터	시스템	복구 지점	압축률
repo	129.49 GB used of 4.84 TB	180.12 GB	5	87	28%

**경고**

날짜	메시지
2020-02-10 오후 4:18	'Veeam_M'에서 '\\Hard disk 1\Volume 1 Recovery; \\Hard disk 1\Volume 2 NO NAME; \\Hard disk 1\Volume 3' 백업을 전송하는 중
2020-02-10 오후 4:07	'Veeam_M'에서 '\\Hard disk 1\Volume 1 Recovery; \\Hard disk 1\Volume 2 NO NAME; \\Hard disk 1\Volume 3' 백업을 전송하는 중
2020-02-10 오후 4:06	vCenter/ESXi 가상 시스템 'Veeam_M'(가) 보호되었습니다.
2020-02-10 오후 4:06	Agent 'Veeam_M'의 상태가 변경되었습니다.
2020-02-10 오후 4:06	보호된 컴퓨터 전송 구성이 업데이트되었습니다.

- Quest Rapid Recovery S/W 통합, 뛰어난 백업 및 복구 기능 제공
- 대상 서버의 상세 백업 현황 및 백업 설정 중앙관리 제공

# RR4400 주요 UI – 어플라이언스 H/W 상태 모니터링

The screenshot displays the RR4400 Backup Appliance web interface, divided into two main sections: Server Status and Storage Status.

**SERVER STATUS INFORMATION**

Power Supply Status

<Sensor Name>	<Status>	<Type>
Power Supply 1	OK	AC
Power Supply 2	Absent	AC

FAN Status

<Sensor Name>	<Status>
Fan 1A	OK
Fan 2A	OK
Fan 3A	OK
Fan 4A	OK
Fan 5A	OK
Fan 6A	OK
Fan 7A	OK
Fan 1B	OK
Fan 2B	OK
Fan 3B	OK

SERVER RAID CONTROLLER STATUS

RAID.Integrated.1-1	
Name	PERC H310 Mini
Status	OK

**STORAGE STATUS INFORMATION**

Storage H/W Information

Name	RR4400Stor
Logo	GSePro1004
Vendor	IFT
Unique-ID	A6830
Model	GSePro1004P
CPU-Type	IntelAvoton
Cache	8192MB
FW-version	1.45R.02
BR-version	1.23C
SN	9059760(m8A3D80)
NVRAM-ID	V2.74.300
Location	SlotA
Host-Board	---
buzzerState	---

Storage Disk Status

Index	J/BOD	Slot	Ch-ID	Size	Speed	LD	Status
0	---	1	4-0	3815191MB	300MB	7A3FF3C5	On-Line
1	---	2	5-0	3815191MB	300MB	7A3FF3C5	On-Line
2	---	3	6-0	3815191MB	300MB	7A3FF3C5	On-Line
3	---	4	7-0	---	---	---	Absent

Partition Information

Ch	Target	LUN	Media	Name	ID	Host-ID
1	0	0	PART	RR_DATA_Stor	42EA26CE51FC937	---
77	0	6	PART	RR_OS_Stor	4FF03C5E078E76CA	---
77	0	7	PART	Docker	2D457CEB13FA3676	---

Snapshot Information

Partition NAME	Snapshot-ID	스냅샷 생성 시간	복구
OS_Docker_Snapshot	0D91890651A11AB0	2020-02-08 07:59:47	시작
OS_Docker_Snapshot	2B36C5684EB2CB16	2020-02-01 07:59:52	시작

- 어플라이언스의 서버 및 스토리지 H/W 상세 상태 모니터링
- 각 부품의 현황 및 장애 확인 가능

# RR4400 주요 UI - 시스템 보호 상태

**RR4400** 시스템 보호 상태

**백업서버 OS백업 상태**

**Factory Backup**

백업 완료 시간: 2020-02-08 오후 02:47:11

백업 저장소 위치: \\192.168.0.252\osbackup\Backup\_Factory

강제 삭제

**Middle Backup**

백업 완료 시간: 2020-02-08 오후 03:18:58

백업 저장소 위치: \\192.168.0.252\osbackup\Backup\_Two

**Last Backup**

백업 완료 시간: 2020-02-09 오전 07:36:54

백업 저장소 위치: \\192.168.0.252\osbackup\Backup\_One

수동 백업 실행 | 백업 로그 리셋

**스토리지 스냅샷 상태**

**Docker Snapshot**

Partition NAME	스냅샷 생성 시간
OS_Docker_Snapshot	2020-02-08 07:59:47
OS_Docker_Snapshot	2020-02-01 07:59:52

Docker 복구는 아이비인포텍에 별도 기술 지원 요청을 하십시오

**OS Backup Snapshot**

Partition NAME	스냅샷 생성 시간	복구
RR_OS_Backup_Snapshot	2020-02-05 15:18:29	시작
RR_OS_Backup_Snapshot	2020-02-01 19:09:46	시작

**RR Backup Repository Snapshot**

Partition NAME	스냅샷 생성 시간	복구
RR_DATA_Snapshot	2020-02-09 08:01:49	시작
RR_DATA_Snapshot	2020-02-08 20:01:51	시작

상세 스냅샷 확인

**경고**

스냅샷 복구시 현재 시점 이후 복구 지점은 자동 삭제됩니다.  
예를 들어 5시 10분, 20분 복구 시점에서 10분 시점으로 복구하면  
20분 시점은 사라집니다. 계속 하시겠습니까?

Cancel | OK

- 백업서버 OS 보호 및 스토리지 보호를 위한 스냅샷 복구 기능
- OS 영역 또는 DATA 영역 랜섬웨어 감염시에도 100% 복구 가능

# RR4400 주요 UI – 환경 설정

RR4400

환경 설정

**백업 서버 정보**

Backup Site:

백업 관리자 ID/PW:

**Storage 정보**

Storage Site:  [접속하기](#)

Storage 관리 ID/PW:

**응급 복구 정보**

iDRAC 관리 IP:

접속 ID/PW:

OS Backup 저장소 ID/PW:

**Partition Information**

Storage Type	NAME	ID
Server OS Stor	<input type="text" value="RR_OS_Stor"/>	<input type="text" value="4FF03C5E078E76CA"/>
RR DATA Stor	<input type="text" value="RR_DATA_Stor"/>	<input type="text" value="42EA26CE651FC937"/>
Docker Stor	<input type="text" value="Docker"/>	<input type="text" value="20457CEB13FA3676"/>

**스크립트 경로**

Shell 스크립트 경로:

스토리지 CLI 경로:

서버 CLI 경로:

**OS Backup 저장소 위치**

초기화 이미지:

백업 저장소 1:

백업 저장소 2:

[저장하기](#)

- 서버 및 스토리지 OEM 파트너로 빠른 환경설정 및 구성 가능
- 모든 구성은 단 하나의 페이지에서 설정

# RR4400 주요 UI - 응급 복구 기능

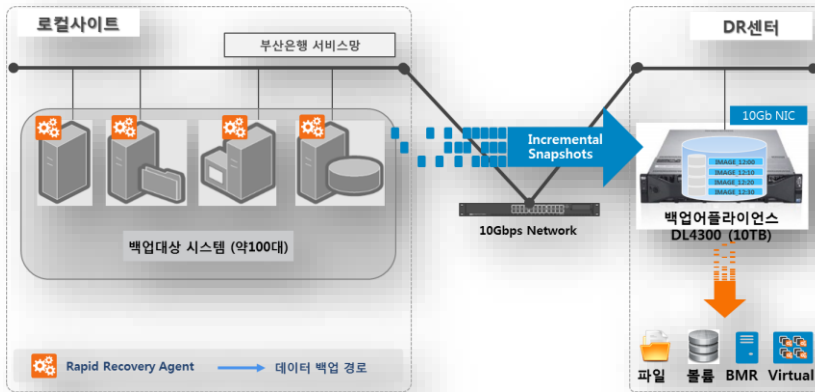
The screenshot displays the iDRAC Enterprise web interface. The top navigation bar includes links for Dashboard, System, Storage, Configuration, Maintenance, and iDRAC Settings. The main content area is divided into several sections:

- Dashboard:** Features buttons for Graceful Shutdown, Identify System, and More Actions.
- Health Information:** A green banner indicates "SYSTEM IS HEALTHY". Below this, two panels show "System Health" and "Storage Health", both marked as "Healthy".
- Recent Logs:** A table listing system events with severity indicators (green checkmarks for success/info, red X for error/warning).
- System Information:** A sidebar menu listing details such as Power State, Model, Host Name, Operating System, and various firmware versions.
- Remote Console:** A large window on the right shows a live video feed of a server's display. The display shows a desktop background of a beach scene, a clock reading 4:14, and the date 2월 10일 월요일. Below the console, a timeline of events is visible, including "Sat 27 Jul 2019 05:52:22" and "Thu 01 Jan 1998 01:24:38".

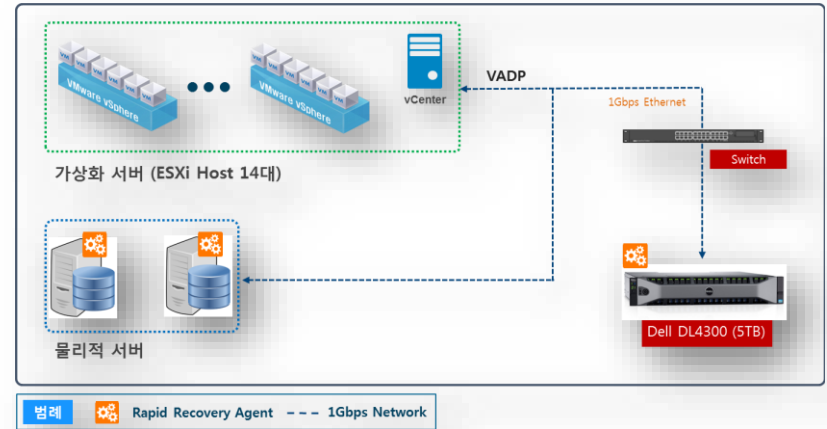
- 랜섬웨어 감염시에도 Dell의 iDRAC 기능으로 OS 복구 가능
- OS 백업 저장소 감염시에도 스토리지 자체 OS로 스냅샷 복구

# 고객 구축 사례

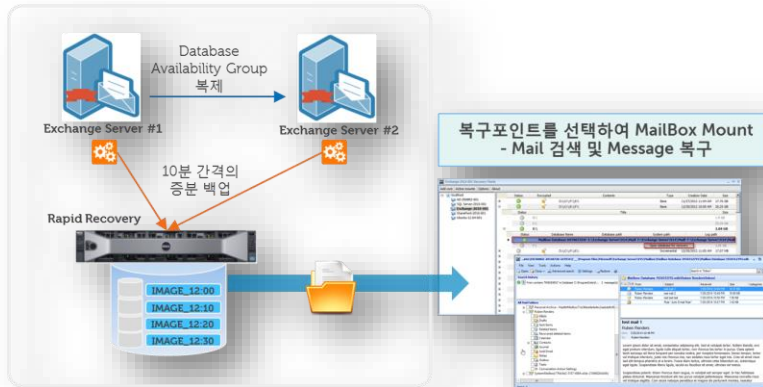
## B 은행



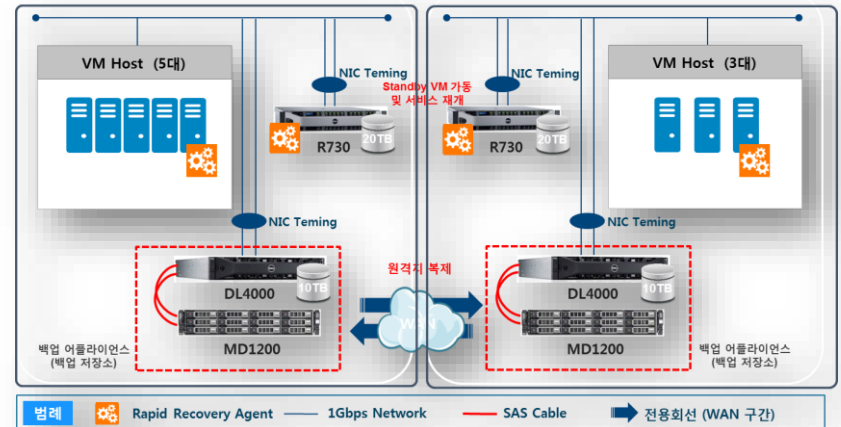
## K 은행



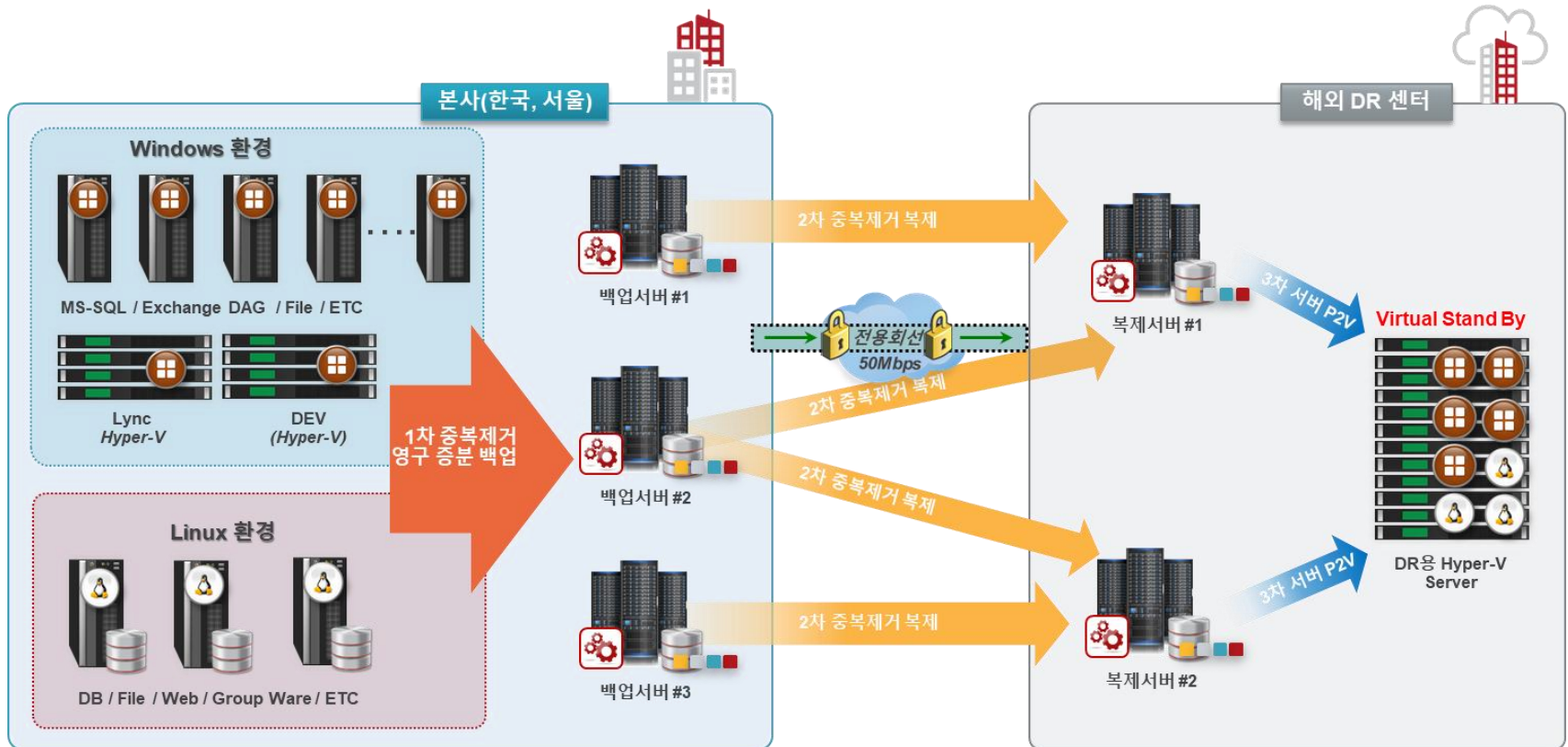
## Y 완구



## 공공기관



# 고객 구축 사례



## 본사 서버 50대

MS Active Directory / MS Exchange DAG  
MS Lync / MS SQL & Oracle  
Hyper-V / Linux GroupWare / ETC.

총 DATA 40TB

인도네시아

## 인도네시아

단 1대의 Hyper-V 서버

24Core \* 4장 = 96Core / RAM 2TB

일부서버 제외 1일내 복제



# 감사합니다.



아이비인포텍(주)

윤주병 대표 / jbyoon@ibinfo.co.kr