랜섬웨어에 대응하는 강력한 데이터 보호방안

장유진 이사 | 베리타스코리아

VERITAS

피해 사례 - 국내 대기업

※ 출처: 전자신문, MBC뉴스, 뉴스1 , KISA(한국인터넷진흥원) 분석자료

주요 시스템이 랜섬웨어에 감염

- 외부에서 유입된 랜섬웨어로 인해 오프라인 점포 영업중단
- 웹서버를 통해 랜섬웨어에 감염

현재까지 해커로부터 지속적인 위협

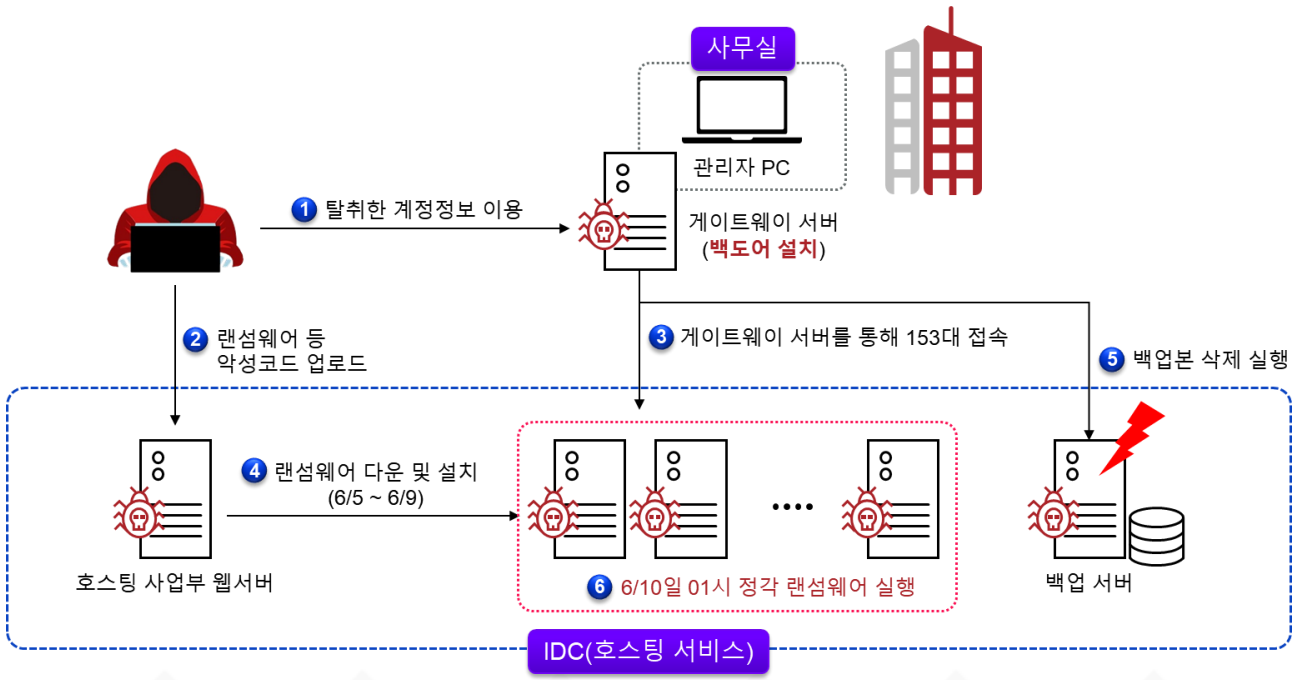
- 해커가 당 회사 측에 고객 개인정보 유출을 무기로 약 수백억원을 요구 중
- 랜섬웨어 감염으로 인해 대외적인 회사 이미지 실추

최후의 보루인 백업서버도 감염

- 백업서버도 감염되어 주요데이터의 복구 불가 (백업된 데이터 보호 기능 부재)
- 보안에 취약한 윈도우계열 백업서버는 지양 필요

VERITAS

피해 사례 - 국내 웹 호스팅 회사



모든 시스템이 랜섬웨어에 감염

- 탈취한 계정정보를 이용하여 웹호스팅 모든서버에 랜섬웨어 설치
- 게이트웨이 서버에 백도어 설치

해커의 지속적인 금전 요구로 회사 파산

- 회사 매출을 상회하는 금전 요구로 회사 파산 결정
- 랜섬웨어 감염으로 인해 입주 웹호스팅 고객사에 막대한 피해

최후의 보루인 백업서버도 감염

- 백업 서버에 접근하여 모든 백업본 삭제
- 백업된 데이터 보호 기능 등의 부재로 백업본을 통한 데이터 복구 실패

※ 출처: 한국랜섬웨어침해대응센터
※ 스마일서브 랜섬웨어 공격 분석 리포트: https://idchowto.com/?p=35203

동유럽지사 뚫은 해커, 본사 망 타고 국내 침투...서버·PC `먹통`

신찬옥 기자 | 입력 : 2020.02.06 17:54:11 수정 : 2020.02.07 00:43:51 0

지난해 글로벌 기업의 한국지사 인터넷망이 랜섬웨어에 감염돼 국내 제조공장 서버가 잠시 멈추는 사건이 발생했다. 서버 3대와 PC 100대가 먹통이 됐는데, 경로를 역추적해 보니 동유럽 지사를 뚫은 해커가 외국계 본사 전산망에 침투한 다음 한국까지 감염시킨 것으로 밝혀졌다. 랜섬웨어 해커조직이 전 세계를 상대로 무차별적인 `인질극`을 벌이고 있는 것이다.

랜섬웨어 해커그룹 `갠드크랩`은 작년 5월 `행복한 은퇴`를 선언했다. 이들은 전 세계에 랜섬웨어 소프트웨어(SW)를 무차별 살포해 불과 1년 만에 2조4000억원을 벌었다. 그들은 랜섬웨어 해결 암호를 넘겨주는 대가로 받은 비트코인을 현금화하는 데에도 성공했다는 편지를 남겼다. 보안업체 비트디펜더가 갠드크랩에 돈을 지불하고 암호화를 푸는 키를 받은 피해자를 국가별로 분석한 결과 한국이 11%로 가장 많았다. 한국은 기업의 정보화 수준이 높은 데다 인터넷 접근도도 뛰어나다 보니 해커들의 좋은 먹잇감으로 떠올랐다. 이 밖에 중국(7%), 인도(7%), 독일(7%), 미국(6%), 브라질(4%), 인도네시아(4%) 등이 뒤를 이었다.

MK 매일경제 MBN

※ 출처: https://www.mk.co.kr/news/it/view/2020/02/125572/

VERITAS

대부분의 랜섬웨어 공격이 야간 또는 주말에 발생

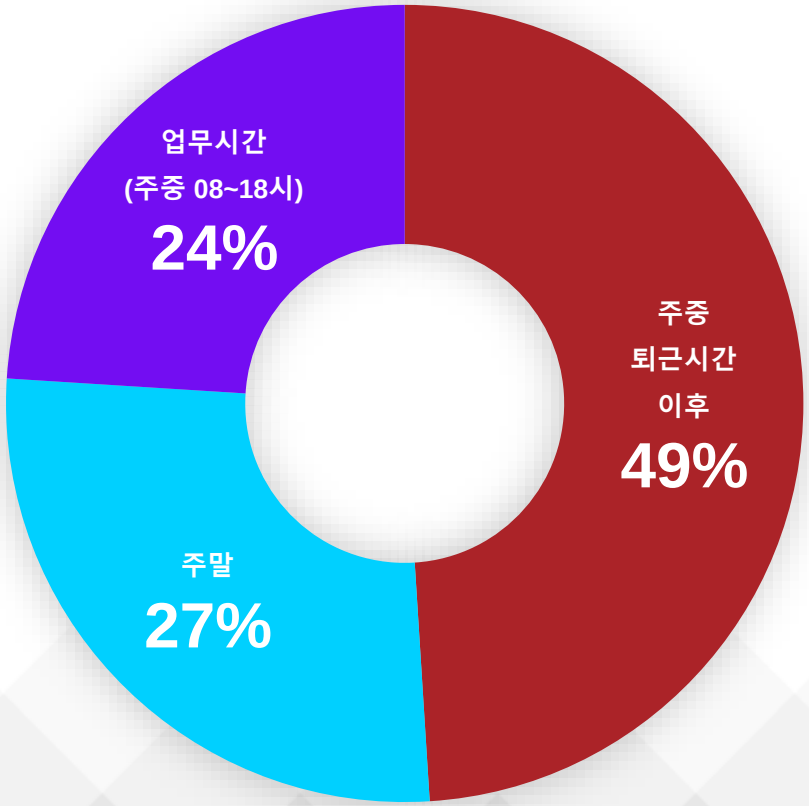
"엔터프라이즈 기업을 대상으로 하는 모든 랜섬웨어 공격 중 **76%**가 근무 시간 외에 발생하며, 49%가 주중 밤에 발생하고, 27%는 주말에 발생합니다."

FireEye

2017-2019 랜섬웨어 사건 대응 조사 결과

랜섬웨어 유포 시점

(근무시간 vs. 비근무 시간)



VERITAS

우리는 왜 랜섬웨어에 민감할까요?

데이터 중요성 증가

IT에 대한 기업 의존도 증가로 인해 비즈니스 연속성을 위한 필수 요건

민감한 정보

유출을 막아야 하는 고객 및 기업의 민감한 정보

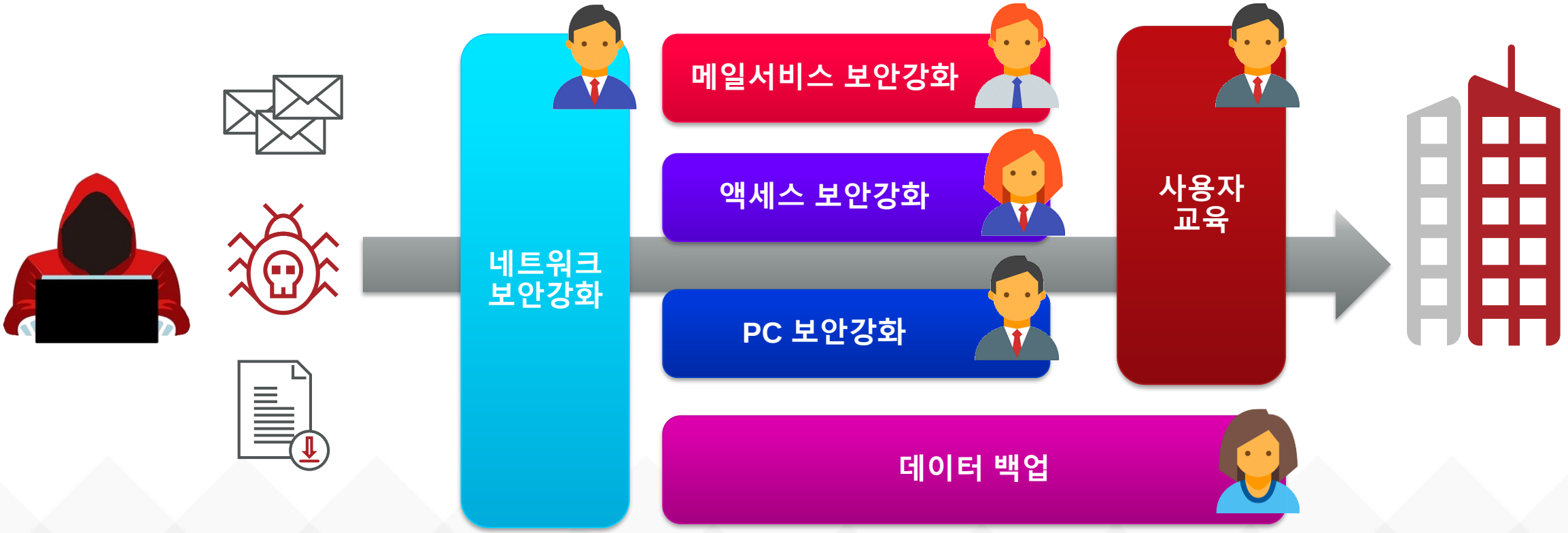
컴플라이언스 요건

규제 및 법적 요건 등으로 인해 보존되어야 하는 정보

데이터는 기업의 가치입니다.

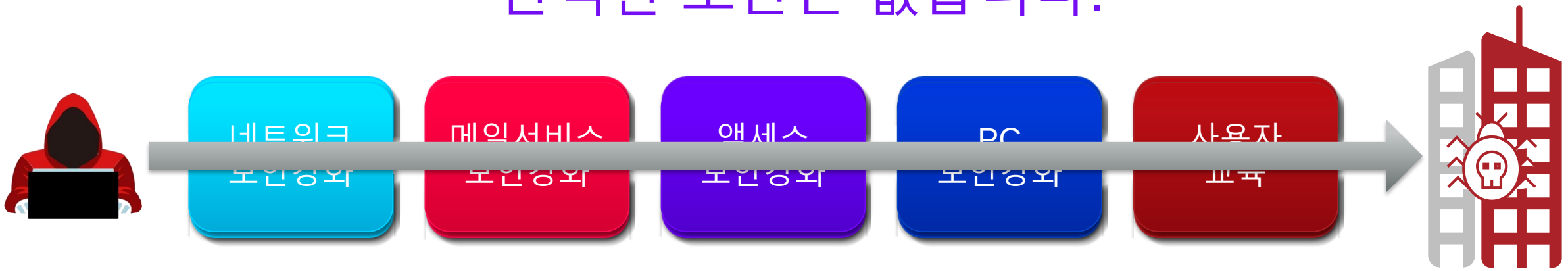
VERITAS

일반적인 대응 방법은 어떤 것들인가요?



랜섬웨어 대응에 “복구”가 가장 중요한 이유는?

완벽한 보안은 없습니다.

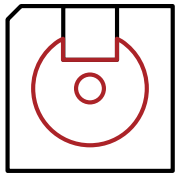


“보안된” **백업**은 필수입니다.

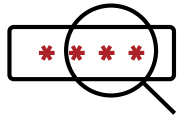
보안된 백업은 **“선택”**이 아닌 **“필수”**입니다.

VERITAS

랜섬웨어 대응을 위한 데이터 보호 방법은?

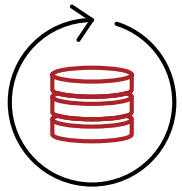


에어 갭(Air Gap)



자격증명 제한

여러 사본 생성

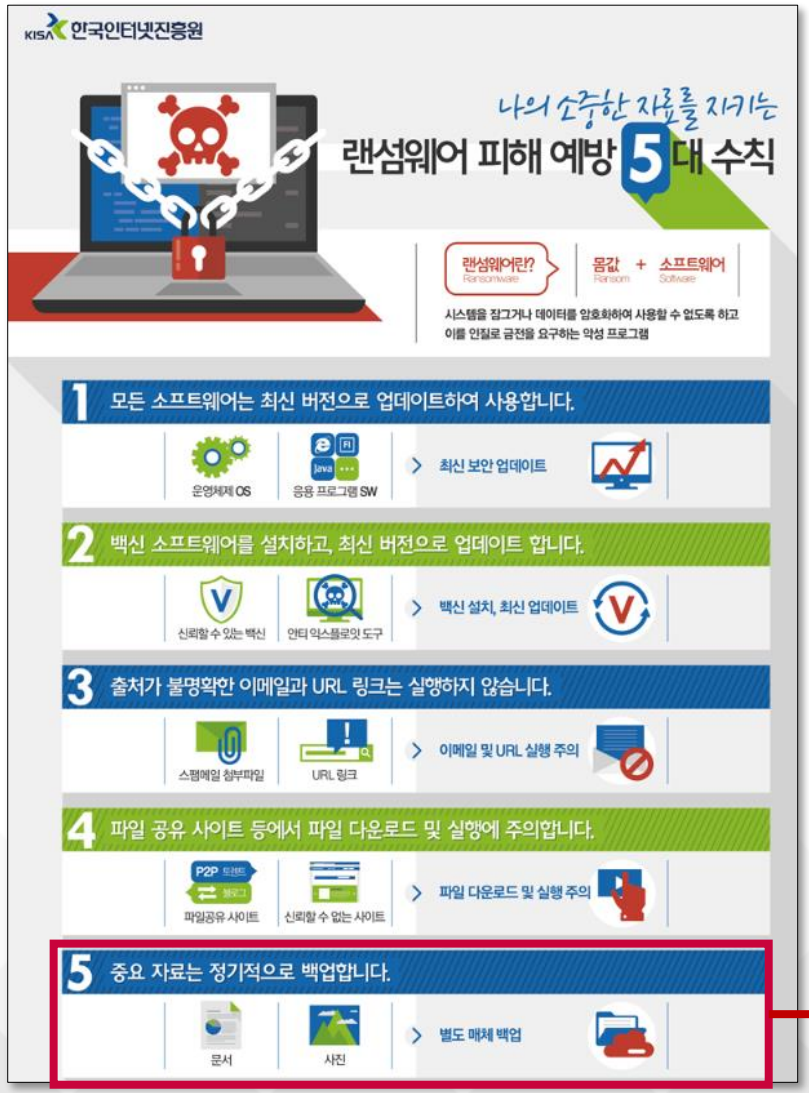


RPO 축소

모든 재해 상황에 대비할 수 있어야 합니다.

VERITAS

한국인터넷진흥원 (KISA)의 랜섬웨어 예방 5대 수칙



KISA의 권고안

랜섬웨어 대비를 위해 반드시 백업 수행

- 감염된 시스템은 2,3차의 공격 대상 & 숙주 역할이 될 수 있으므로 반드시 폐기
- 폐기(가능 시 OS재설치) 후 업무정상화를 위해 백업본으로 업무 정상화 필요

고객사 상존위험

외부 취약점을 통한 백업 오염 방지 필요

- 잘 받은 백업도 자회사 계정 취약점 또는 웹서버 통해 오염 및 백업본 삭제 가능성
- IDS/IPS기반 통제 & 허가 계정 외 백업 접근 통제(Lock Down)등의 대책 필요

랜섬웨어 예방관련 해결책

보안에 특화된 백업 방식 필요

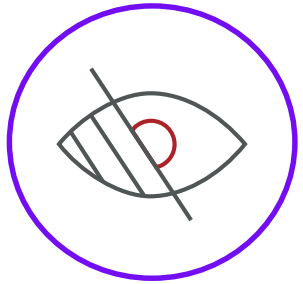
- IDS/IPS기반 통제, 허가 계정외 접근 차단
- 중요데이터에 대한 WORM & Lock Down
- 백업시스템의 원격 소산
- RPO/RTO 최소화를 위한 특수 백업 고려

※ 출처 : 한국인터넷진흥원 (KISA) 랜섬웨어 예방수칙 (https://www.boho.or.kr/ransomware/prevention.do)

강력한 랜섬웨어 대응과 신속한 복구까지 가능하려면?

PROTECT

시스템 경화 및
스토리지 불변성으로
모든 위치의 데이터 보호



DETECT

모니터링 및 리포팅을
통해 위협 및 취약성
완화

RECOVER

자동화된 오케스트레이션
복원을 통해
업무 연속성 확보

"만약"이 아니라, **"언제"**의 문제입니다.

VERITAS

기업의 모든 데이터는 보호되어야 합니다.

PROTECT

시스템 경화 및
스토리지 불변성으로
모든 위치의 데이터 보호

"기업의 모든 데이터는 보호되어야 하고, 어떠한 상황에서도 데이터를 복구할 수 있는 역량이 있어야 합니다."

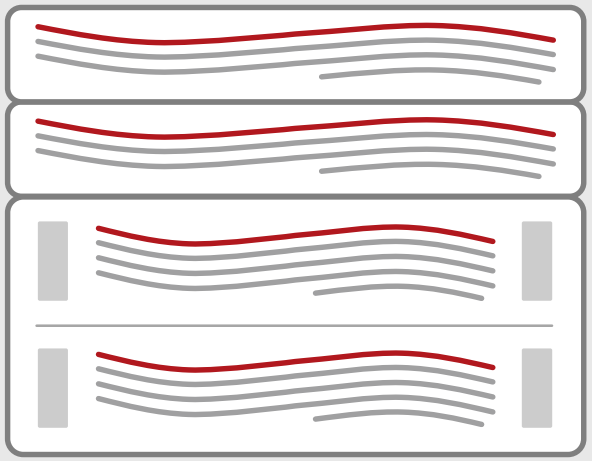
"만약"이 아니라, **"언제"**의 문제입니다.

VERITAS

NetBackup with Immutable Storage

Veritas
Flex Appliance 5150

Veritas
Flex Appliance 5340



NetBackup Immutable WORM Storage

- ✓ Primary, Secondary 백업에 대한 **WORM** 기능 & AIR 소산
- ✓ Intrusion Detection System (**IDS**) / Intrusion Protection System (**IPS**)
- ✓ **RBAC**: New Security Admin role 기능으로 접근 통제
- ✓ Flex 2.0은 **STIG**(Security Technical Implementation Guides)를 준수
- ✓ NBUA(Flex 5150, 5340), BYO MSDP, DellEMC DDBoost
- ✓ **Docker기반** Container Architecture로 **수분 이내에** Master, Media서버의 생성 및 배포 가능
- ✓ 보안관련 **각종 인증**(Cohasset등) 및 3rd 제품과의 SSO연동
- ✓ **Cohasset** immutability assessment (in compliance mode):
  - Securities & Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)
  - Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d)

VERITAS

WORM 스토리지 기능을 통한 보호 – Immutable Storage

불변 스토리지 모드(WORM) 지원

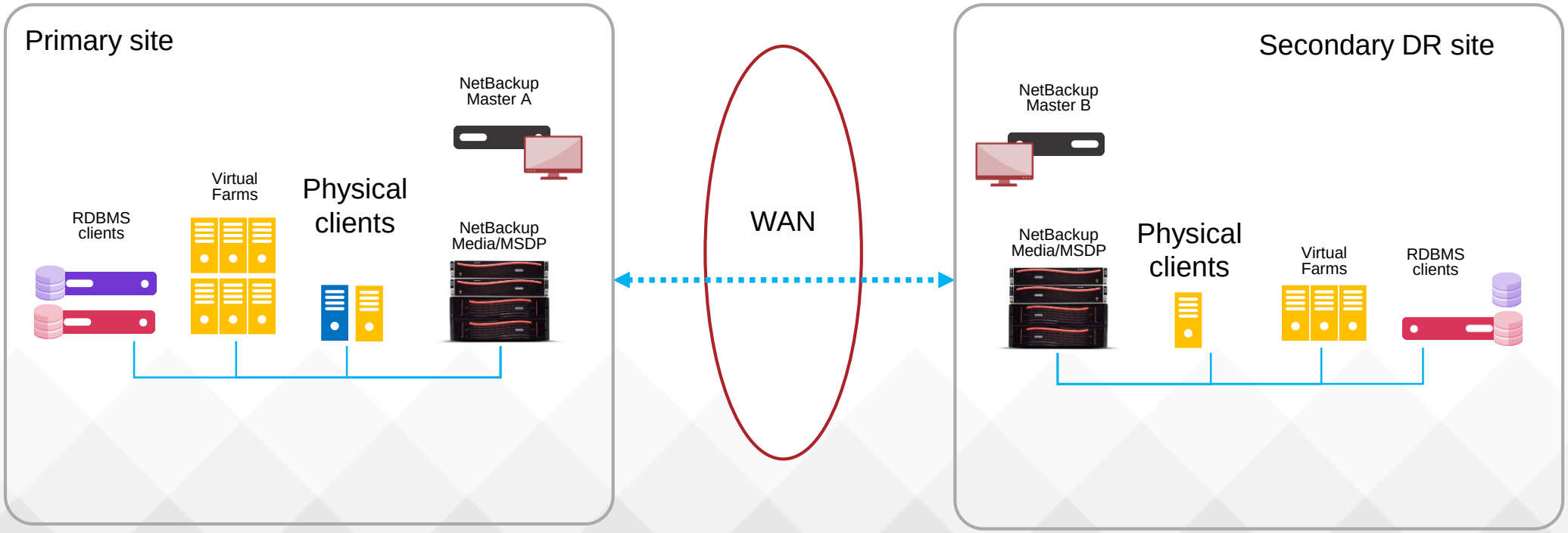
- BYO, Flex 5150 & 5340 Appliance
- OS 시간과 무관한 자체 Compliance Clock을 통해 불변 기간 설정
- 2가지 WORM 기능 제공
  - Compliance: WORM 보존 기간 동안 삭제 불가능
  - Enterprise: WORM 보존 기간 중 삭제 가능

지원 환경

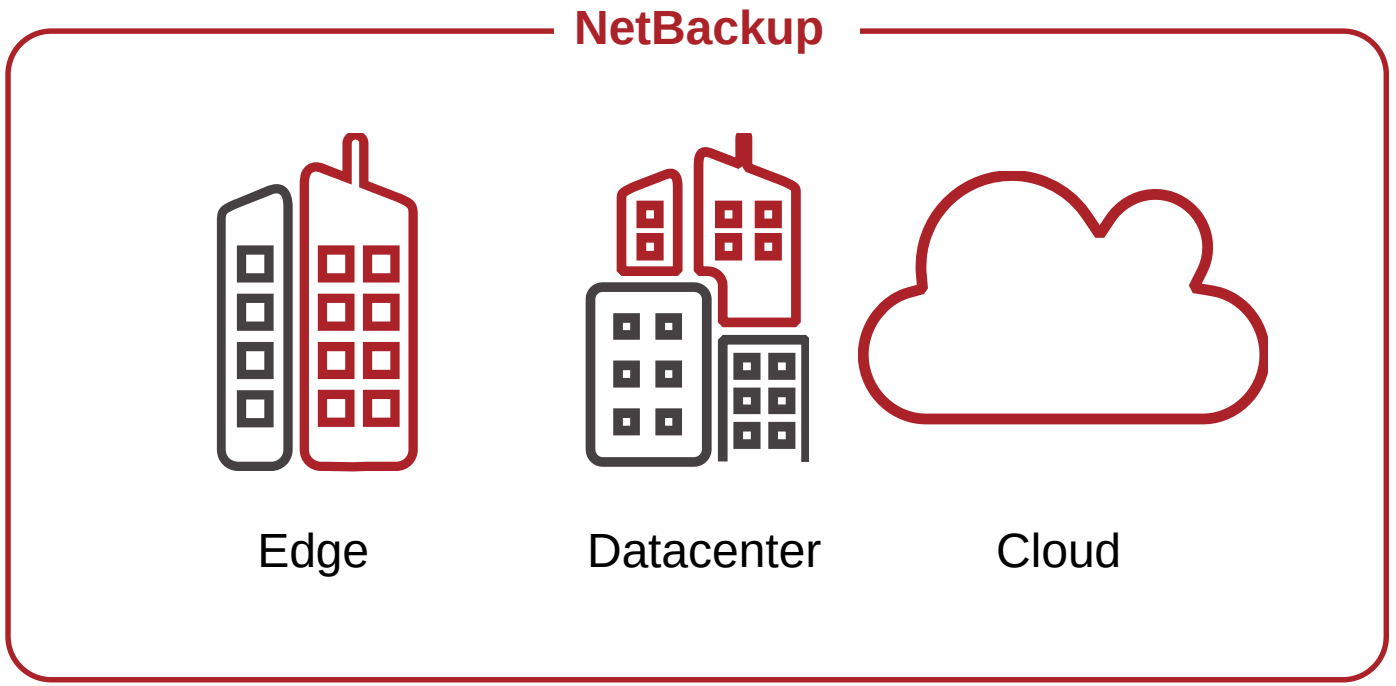
- NetBackup v8.3 이상
- BYO MSDP, Dell DataDomain DDBoost
- Flex 5150 & 5340 Appliance
  - Flex v2.0 이상
  - MSDP에 대해서 WORM 설정 가능

NetBackup AIR를 통한 Air Gap 백업 구현

- offsite tape는 정의상 Air-gap을 지원하는 것을 의미
- NetBackup "AIR"는 별도의 독립적인 NetBackup 도메인(offsite “Air-gap” 복사본)에 백업 이미지를 복제하는 기능



금융인프라 보안 요구사항 충족을 위한 최적의 백업



Enterprise Data Services Platform powered by NetBackup

VERITAS

랜섬웨어 완벽 대응 보안 백업 솔루션

Ransomware Free

- **침입 차단(IPS) 및 탐지(IDS) 기능** 기본 탑재
  - 랜섬웨어가 시스템에서 데이터를 삭제하거나 실행되는 것을 차단(랜섬웨어 실행파일 차단)
  - 해킹시도 원천적 차단
- CC 인증된 Symantec Data Center Security 기본 탑재

black hat USA

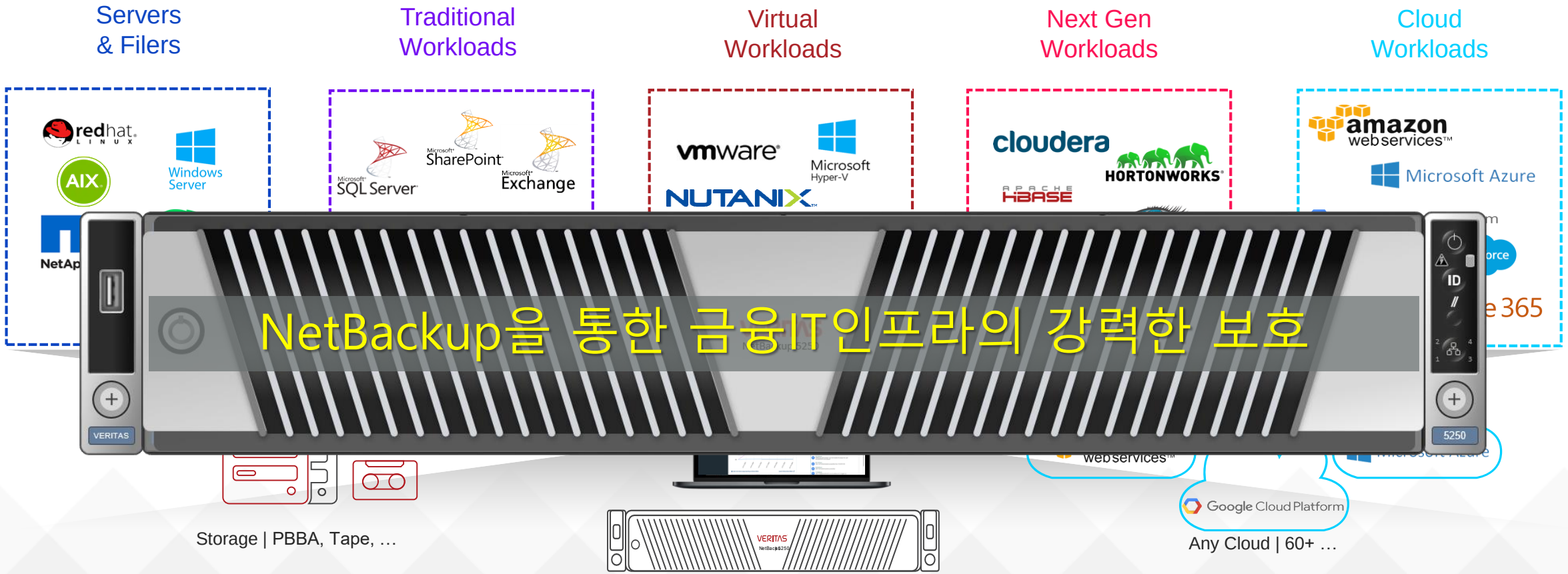
PASSED

* NetBackup 어플라이언스는 17,000번 이상의 해킹 시도를 모두 막아내 보안성을 입증하였습니다. – 2014 년 8 월, Black Hat USA 2014

VERITAS

랜섬웨어 완벽 대응 보안 백업 솔루션

Ransomware Free



Cloud Native
Marketplaces

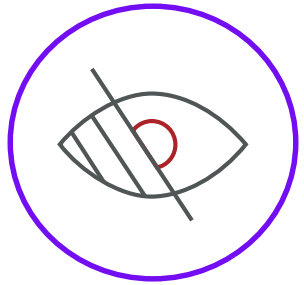
VERITAS

“Veritas NetBackup Appliance는 업계 인증된 보안 솔루션이 기본 내장돼 있기 때문에, 백업된 데이터뿐만 아니라 백업 어플라이언스의 보안성까지 강화해줍니다. 이에 모든 유형의 사이버 보안 위협으로부터 데이터를 안전하게 보호할 수 있고, 언제든지 신속하게 데이터를 복구할 수 있는 환경을 유지할 수 있습니다.”

㈜간삼건축종합건축사사무소

김명석, 간삼건축 경영기획부문 수석

피해를 신속하게 감지하고 대응할 수 있어야 합니다.



DETECT

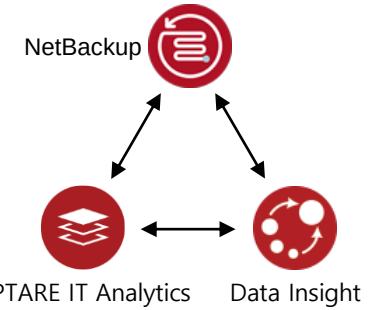
모니터링 및 리포팅을 통해 위협 및 취약성 완화

"랜섬웨어 침해가 발생된다는 것은 보안 솔루션에서 이를 탐지하지 못하였다는 것입니다. 이러한 상황에서 신속한 대응 체계를 갖춰야합니다."

"만약"이 아니라, **"언제"**의 문제입니다.

VERITAS

IT 환경 분석을 통한 비즈니스 문제 해결



APTARE IT Analytics, Data Insight

CHARGEBACK

고객/지역/부서 단위 과금을 청구하거나 사용량을 제시

COMPLIANCE

보호 정책에 누락된 클라이언트에 대한 가시성을 제공하여, 규정 및 정책 위반 또는 랜섬웨어 공격 예방

RECLAMATION

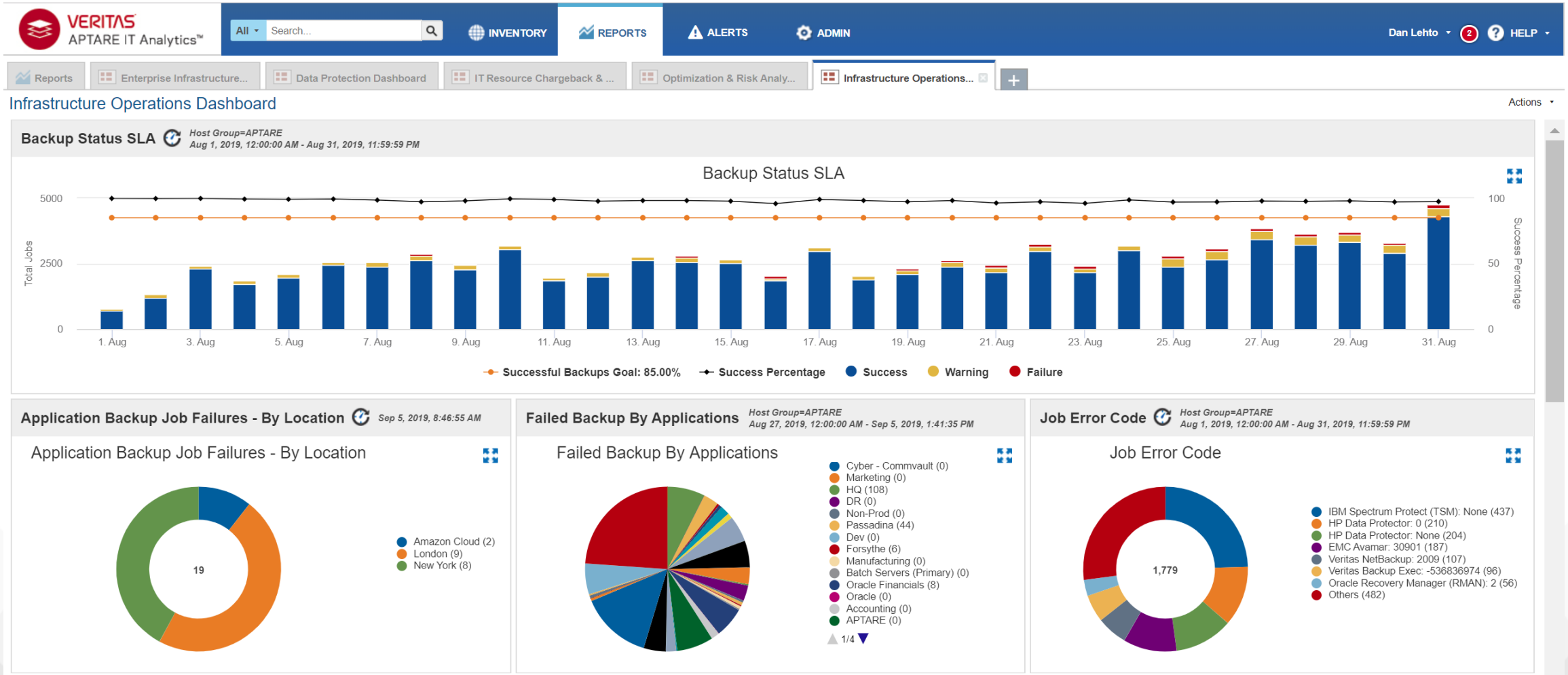
미사용 스토리지 공간 회수, 오래된 데이터 또는 비효율적 백업을 파악하여 비즈니스 성과 및 ROI 가속화

EFFICIENCY

관리자가 SLA를 충족하지 못하는 이유와 이를 해결하는 방법을 빠르고 정확하게 파악

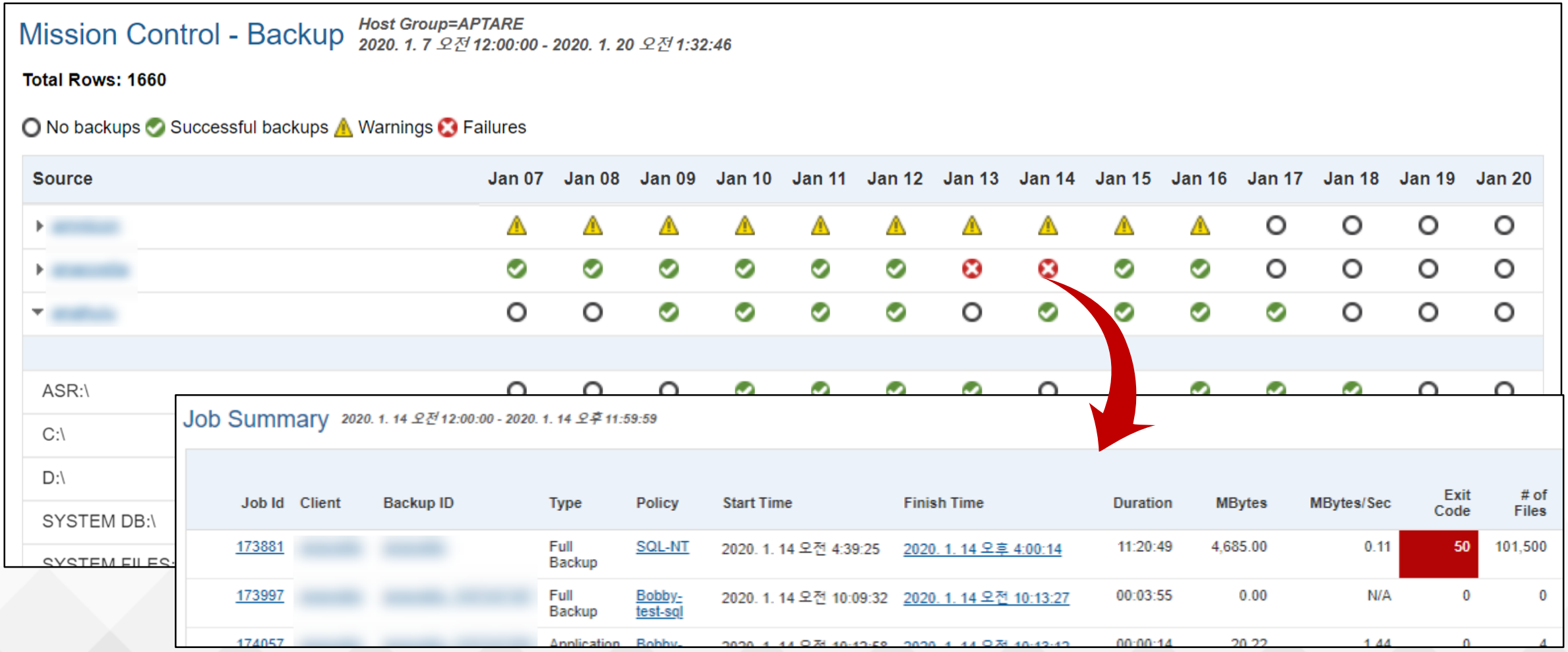
VERITAS

통합된 데이터 보호 업무 분석 – APTARE IT Analytics

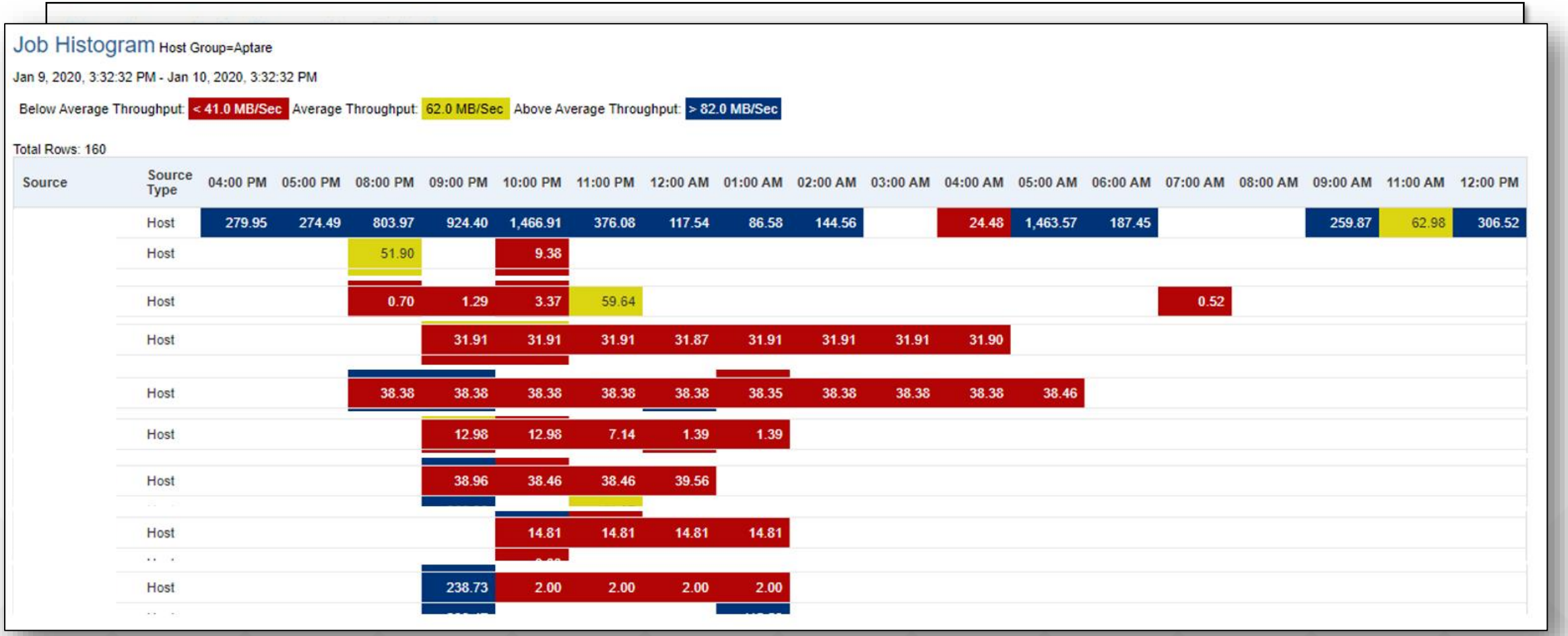


VERITAS

환경 내의 리스크를 빠르게 식별



급격한 백업 소요시간 증가 대상 파악



Job Histogram Host Group=Aptare

Jan 9, 2020, 3:32:32 PM - Jan 10, 2020, 3:32:32 PM

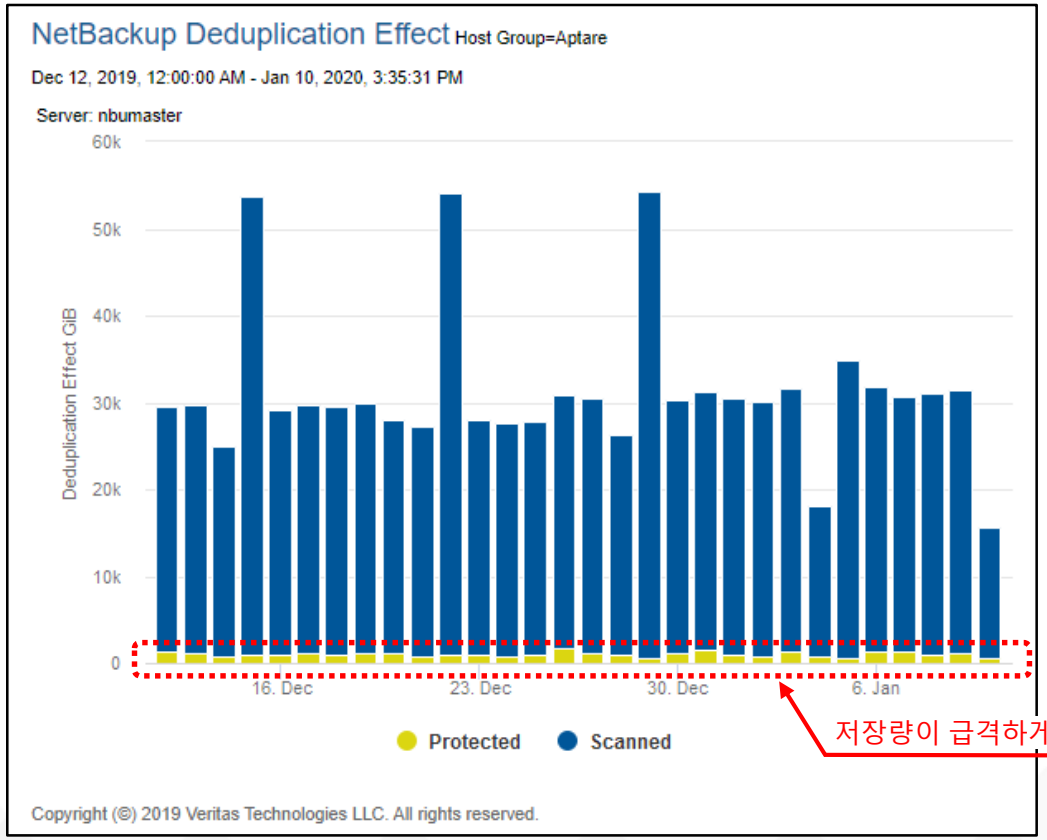
Below Average Throughput: < 41.0 MB/Sec Average Throughput: 62.0 MB/Sec Above Average Throughput: > 82.0 MB/Sec

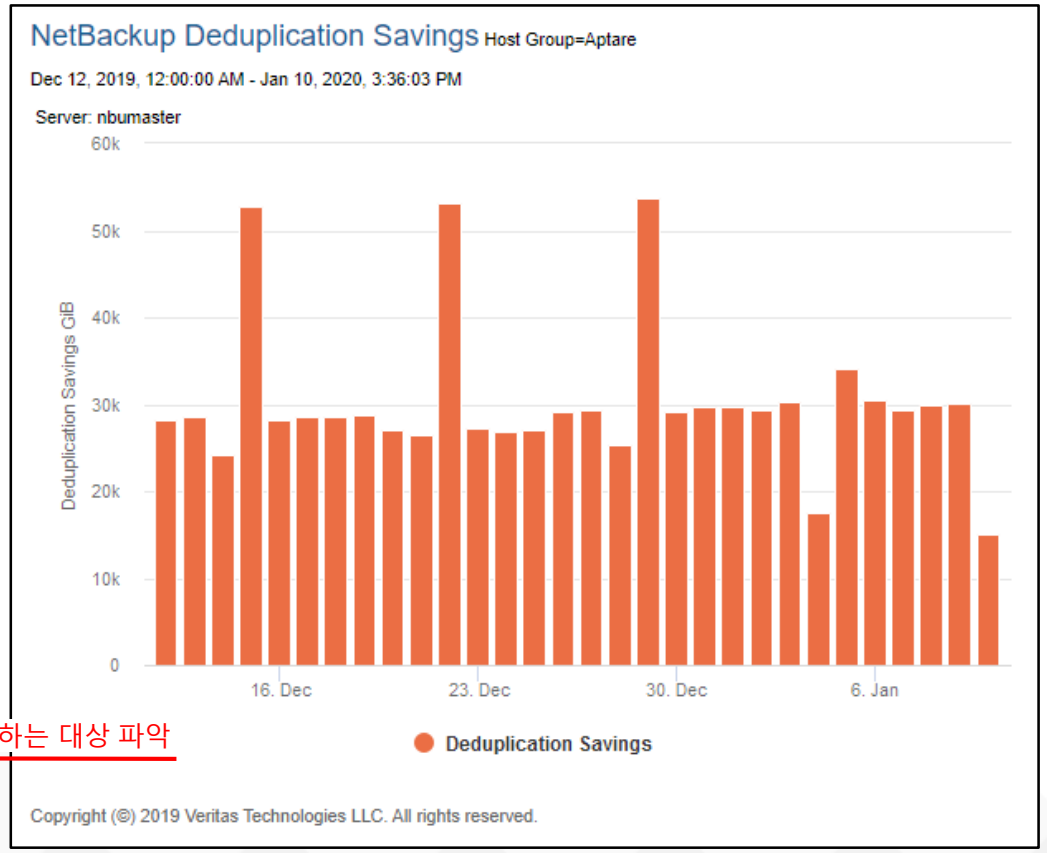
Total Rows: 160

Source	Source Type	04:00 PM	05:00 PM	08:00 PM	09:00 PM	10:00 PM	11:00 PM	12:00 AM	01:00 AM	02:00 AM	03:00 AM	04:00 AM	05:00 AM	06:00 AM	07:00 AM	08:00 AM	09:00 AM	11:00 AM	12:00 PM
	Host	279.95	274.49	803.97	924.40	1,466.91	376.08	117.54	86.58	144.56		24.48	1,463.57	187.45			259.87	62.98	306.52
	Host			51.90		9.38													
	Host			0.70	1.29	3.37	59.64								0.52				
	Host				31.91	31.91	31.91	31.87	31.91	31.91	31.91	31.90							
	Host			38.38	38.38	38.38	38.38	38.38	38.35	38.38	38.38	38.38	38.46						
	Host				12.98	12.98	7.14	1.39	1.39										
	Host				38.96	38.46	38.46	39.56											
	Host					14.81	14.81	14.81	14.81										
	Host				238.73	2.00	2.00	2.00	2.00										

VERITAS

데이터 저장용량 변화 관리





저장량이 급격하게 증가하는 대상 파악

업무 연속성을 위해 서비스는 신속하게 복구되어야 합니다.

RECOVER

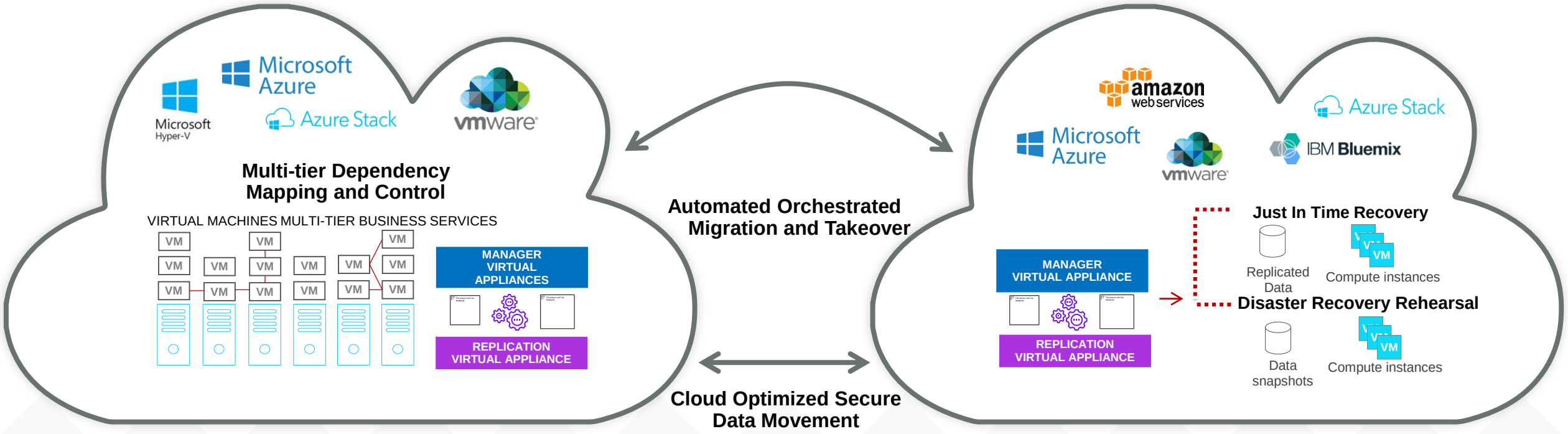
자동화된 오케스트레이션
복원을 통해
업무 연속성 확보

"랜섬웨어 침해 사고가 발생되더라도
기업의 업무 연속성은 보장되어야
하고, 이를 위한 방안이 필요합니다."

"만약"이 아니라, **"언제"**의 문제입니다.

VERITAS

자동화된 오케스트레이션 재해 복구 | Resiliency Platform

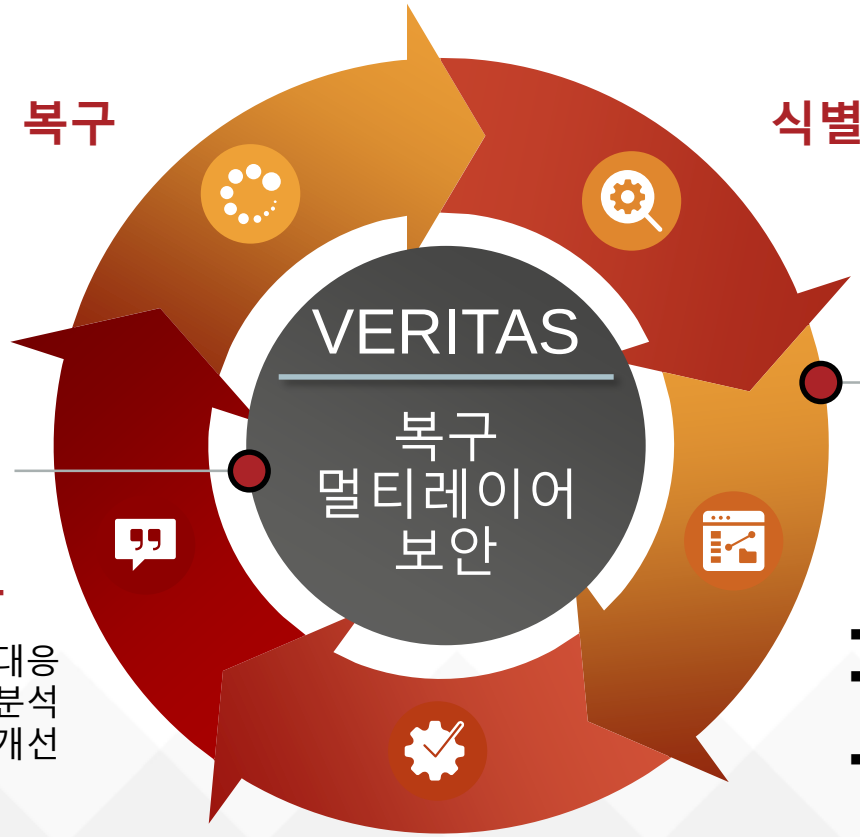


On premises, traditional, public or private cloud

VERITAS

랜섬웨어 대응에 대한 Veritas 접근방식

- 백업 솔루션을 최적화하고 사이버 보안 기술과 통합하여 백업 데이터 및 시스템을 보호하는 방법에 대한 지침을 제공하는 기술 및 프로세스의 통합 접근 방식



복구

NBU
NBU ▪규모에 따른 신속한 복원
▪백업 데이터에 대한 즉각적이고 빠른 액세스
DLO ▪롤백 능력
VRP ▪자동화된 오케스트레이션 복구
Service ▪최적화된 DR 정책 및 아키텍처
Service ▪랜섬웨어에 대한 복구 서비스

식별

▪사이버 보안 및 DP 및 DR / BCP와 연계된 거버넌스 Service
▪리스크 관리 전략 Service

VERITAS CONSULTING

VERITAS PRODUCTS

보호

▪Awareness and Training Service
▪데이터 보호 / 데이터 DR / 자동화된 복원 테스트 강화 NBU VRP Service
▪에어갭과 WORM NBU

응답

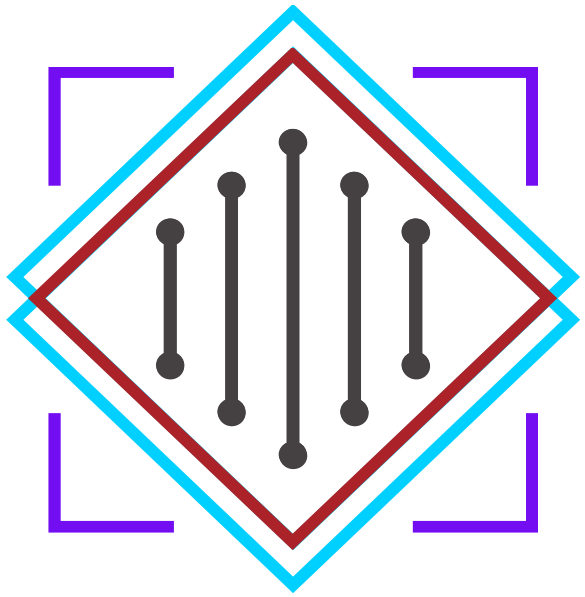
Service ▪BCP / DR 및 위기 관리를 통한 대응 계획 및 분석
Service ▪DP를 통한 대응 계획 개선

감지

▪DP와 사이버 보안의 이벤트 상관관계 Service
▪데이터 패턴 및 항목 유형 감지 INFOMAP APTARE
▪DP 시스템의 침입 탐지 및 예방 NBU

15x

A LEADER IN GARTNER'S MQ FOR DATA CENTER BACKUP AND RECOVERY SOLUTIONS



#1

MARKET SHARE FOR BACKUP AND RECOVERY SOFTWARE

VERITAS™

ENTERPRISE DATA SERVICES PLATFORM

800+

Data Sources

1400+

Storage Targets

60+

Clouds

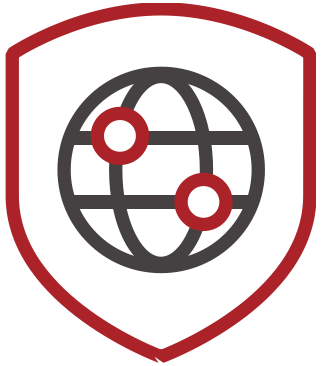
EVERY

Deployment Model

VERITAS™

Summary

Data must be protected



Data must be resilient

Data must be recoverable

NetBackup을 통해 랜섬웨어에 대응하는 강력한 보호

- 해커들의 최종 목표인 금융IT인프라에 대한 외부 위협 대응이 필요 / NetBackup으로 해결 가능

NetBackup을 통한 보안 백업

- Immutable Storage(WORM), IDS/IPS, RBAC등 각종 보안 기능, 보안 관련 외부 인증

NetBackup을 통한 통합 (백업+보안+α)

- 완수해야 할 목표가 많아진 복잡한 IT 시장에서 최적의 백업 솔루션

VERITAS

감사합니다

VERITAS