[Keynote Wrap-up]
국내 랜섬웨어 및 사이버공격 사례 소개

VERITAS ASCEND SOLUTION DAYS

천대영 이사

베리타스코리아 기술영업본부

GET REAL
ABOUT CYBER RISK

"국내 ○ ○ ○ ○ ○ 기업 1위 '○ ○ ○'의 **공식 홈페이지와 모바일 앱이 닷새째 먹통**이 이어지고 있어 고객과 가맹점주의 피해가 계속 늘고 있다.

전산망 먹통의 이유가 **랜섬웨어 공격**으로 알려지면서 지난 2019년 시스템 장애를 경험한 ○ ○ ○ 이 '시스템 장애와 보안위협 대책 마련'에 미흡한 것 아니냐는 지적이 나오고 있다."

랜섬웨어 조직
Black Suit

NOV 23

랜섬웨어 공격

- 가상 호스트 및 **주요 시스템 암호화**
- 홈페이지 및 모바일 앱 **서비스 중단**
- 시스템 디스크 파손

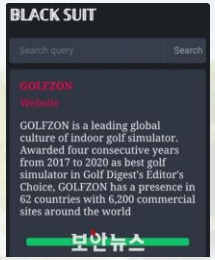
6 DAYS
Total Downtime

불특정 다수에게 상황을 악용한 해당 기업 사칭 **스미싱 문자 발송**

NOV 28

백업본을 통한 서비스 복구 완료

DEC 8



협상 결렬에 따른 보복성으로 **탈취 데이터를 다크웹 릭(leak)에 공개**

* 우먼타임스, http://www.womentimes.co.kr/news/articleView.html?idxno=67249
* 보안뉴스, https://www.boannews.com/media/view.asp?idx=124630&kind=

VERITAS ASCEND SOLUTION DAYS

랜섬웨어 피해 복구 절차

네트워크 연결 차단

- 피해 확산을 차단하기 위한 선제적 조치 수행
- 피해 범위 파악 및 목록화
- 백업 상태 확인

OS 재설치

- 하드웨어 교체(필요시)
- 기존 시스템 포맷 후 운영체제 재설치
- 최신 업데이트 적용

App 재설치

- 보안 솔루션 설치 및 최신 업데이트 적용
- 어플리케이션 재설치 및 구성

데이터 복원

- 데이터 복원
- 복원 과정에서 실시간 멀웨어 스캔을 통한 안정성 확보

“사이버 재해 상황에 대응 가능한 데이터 생존 전략 유지 필요”

VERITAS ASCEND SOLUTION DAYS

"국내 최대 패션/유통 그룹이 랜섬웨어 공격으로 오프라인 매장에서 전산 오류가 발생하면서 절반 가량 매장 운영을 중단한 가운데 백업은 돼있지만

일부 백업서버도 감염된 것으로 파악..."

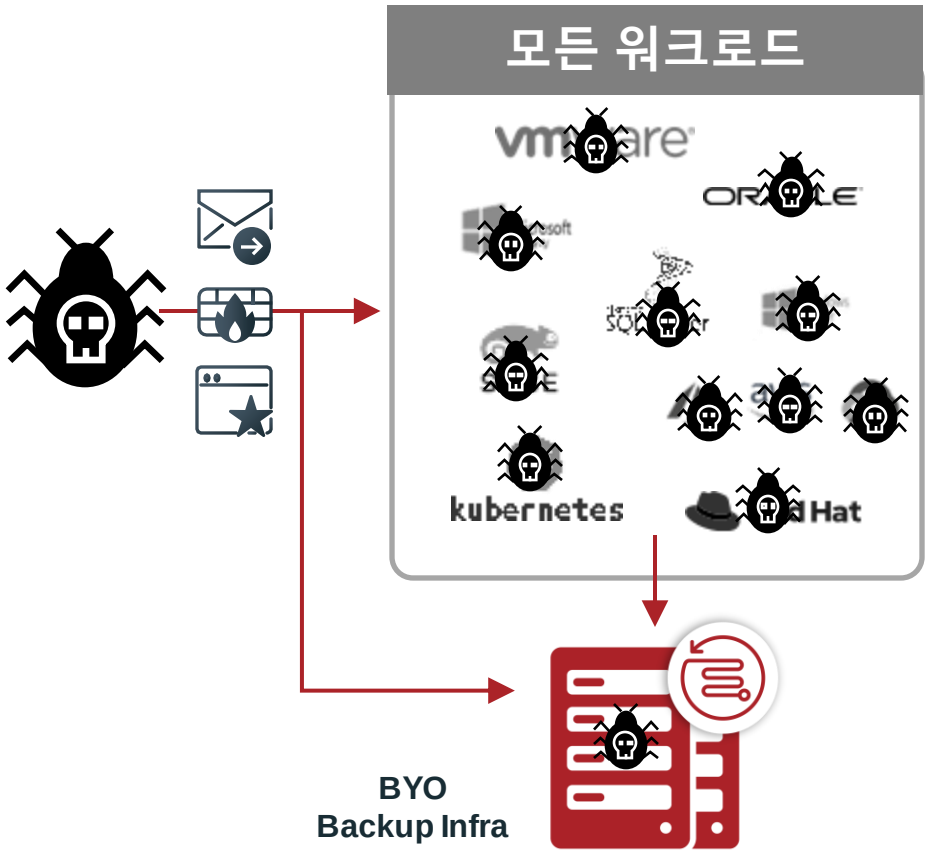
백업 서버 침해 원인

- BYO 구성의 데이터 보호 환경
- 보안에 취약한 Windows 기반
- 백업 서버 및 데이터에 대한 보안성 부재

※ 자료 출처: 중앙일보, YTN, NEWS 1, 전자신문

VERITAS ASCEND SOLUTION DAYS

백업은 모든 상황에서 데이터를 **복원(생존)**할 수 있어야만 합니다.



하드웨어 장애

사용자 실수

물리적 재해

Compliance
(장기보존)

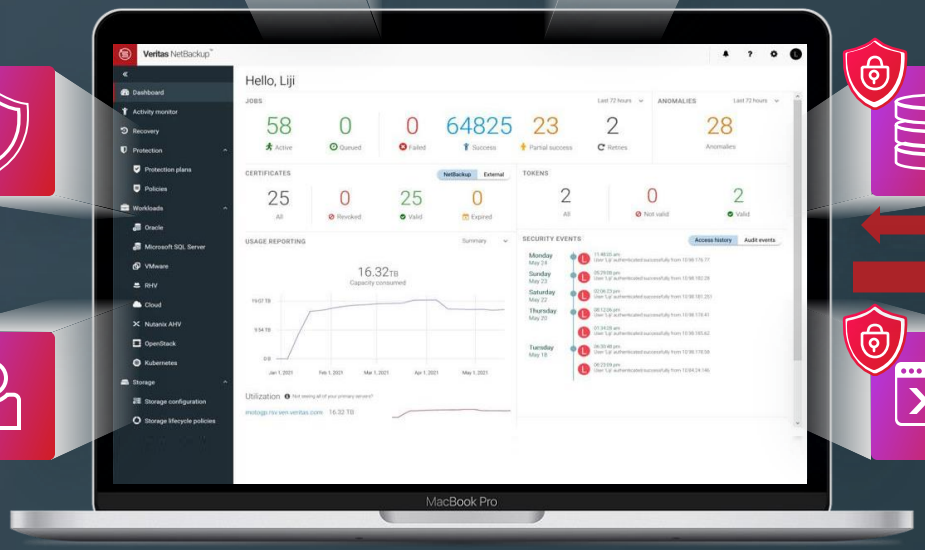
VERITAS ASCEND SOLUTION DAYS

Network

Application

Immutable

User



Storage

Pull 방식의 복제

Operating System
(Hardening)

Isolated Recovery Environment

Air-Gap
(/w Immutable)

- 관리포인트 증가에 따른 보안 취약성 완화
- 기존 환경과 이원화된 보안된 환경으로의 격리
- 격리된 환경기반 복구 환경 제공(IRE)

VERITAS ASCEND SOLUTION DAYS

공격 전

Veritas는 격리된 환경 기반에서 중요한 데이터를 식별 및 관리하고 백업중 실시간으로 이상 징후를 탐지 및 보고

공격 중

Multi-Layer 보안 강화된 환경에서 자산을 안전하게 보호 및 격리하여 안전한 사본을 유지

공격 후

실시간 멀웨어 검사 기능을 통해 Clean한 데이터 복구를 보장하여 안전하고 신속하게 프로덕션 환경을 복구

Quiz.

이번 세션을 통해 백업 인프라에 대한 보안성이 매우 중요하다라는 것을 알았습니다.
그 무엇도 신뢰하지 말라는 의미의 보안 아키텍처를 이르는 용어는 무엇일까요?

“Air-Gap”

“Zero-Trust”

“Immutable”

“Native-Trust”

THANK YOU

VERITAS ASCEND SOLUTION DAYS