Acronis

#CyberFit

백업 데이터 어디까지 믿을 수 있나?

사이버 복원력 관점에서의 제로 트러스트

아크로니스코리아 문수호 사이버 보호 전문 컨설턴트

더욱 복잡해지는 위협 환경

80%

사이버 범죄에 공격 받은 회사들

57%

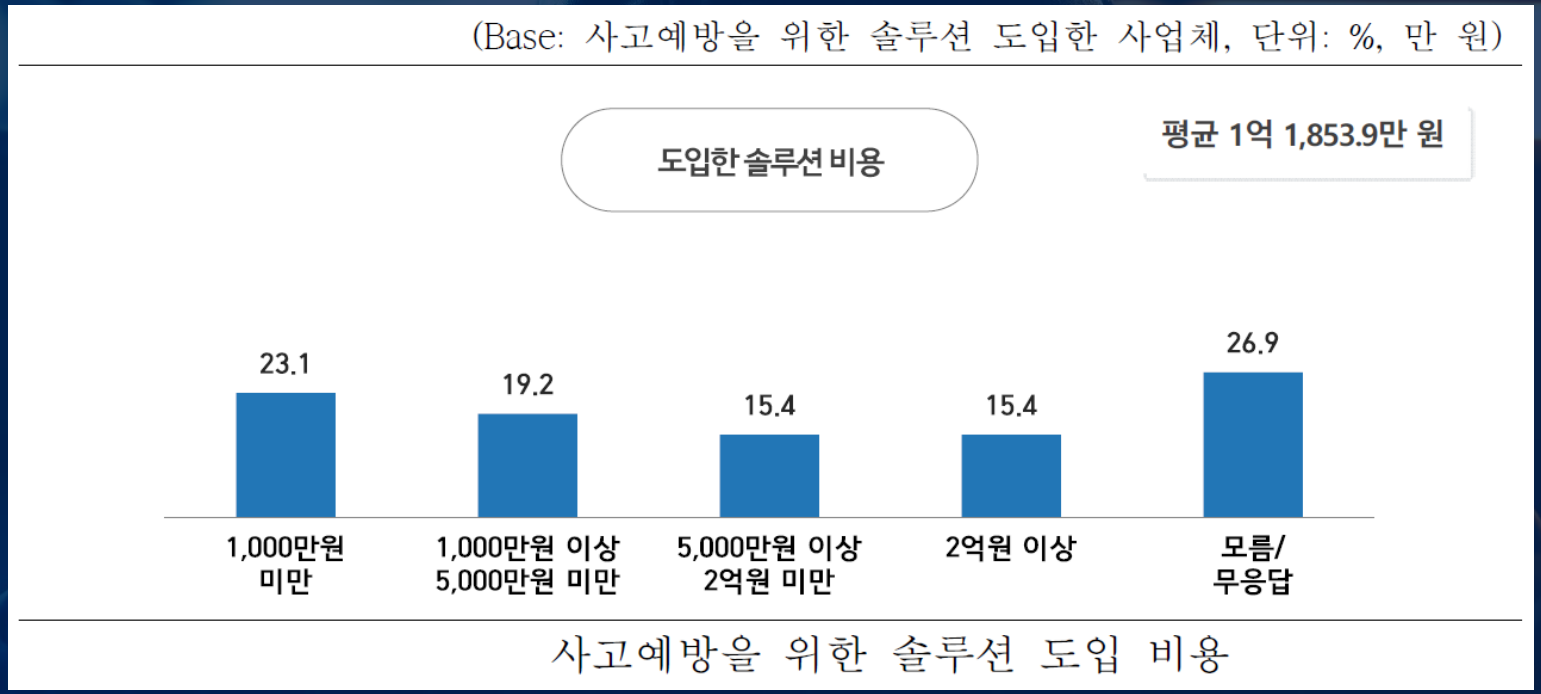
기존 안티바이러스 솔루션에서 놓친 공격 비율

69%

위협의 방어보다 관리 도구에 더 많은 시간을 사용하는 비율

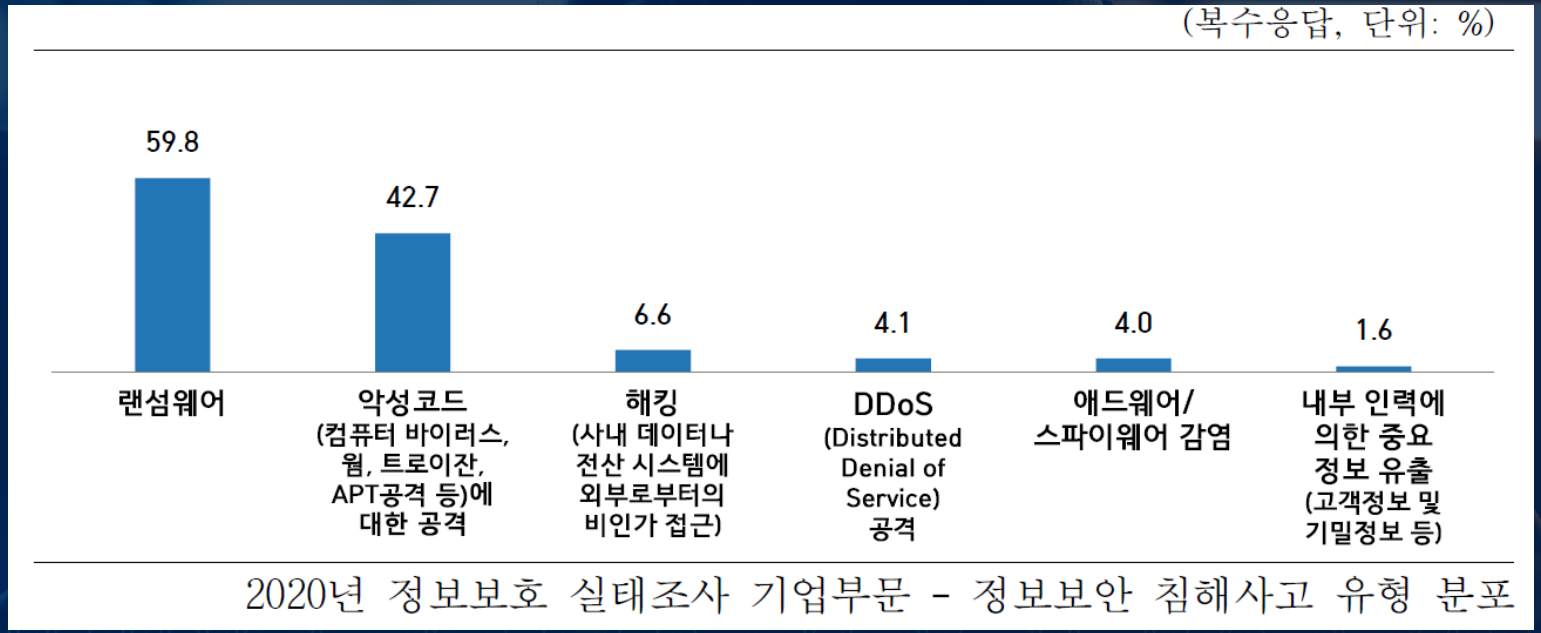
Sources: Acronis Cyberthreats Report 2022, Acronis Cyber Readiness Report, 2020, FBI

사이버 공격의 타겟이 된 국내 기업들



출처: 사이버 침해사고의 사회적 비용 추정 연구, 한국인터넷진흥원(KISA), 2021년 12월

사이버 공격의 타겟이 된 국내 기업들

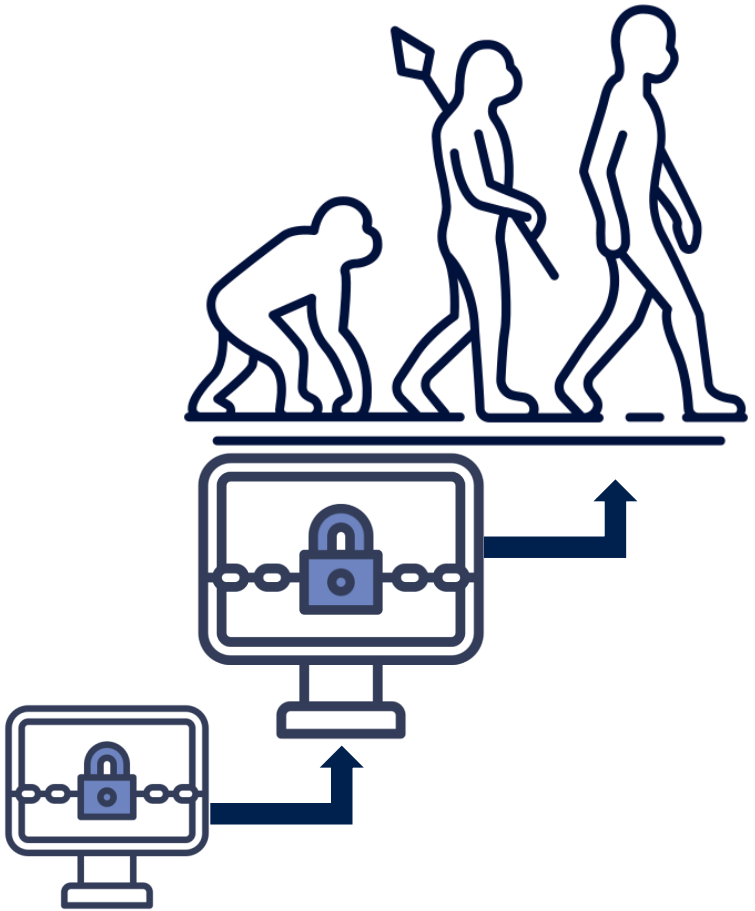


출처: 사이버 침해사고의 사회적 비용 추정 연구, 한국인터넷진흥원(KISA), 2021년 12월

랜섬웨어는 끊임없이 진화 중?

랜섬웨어에 걸리지 않는 것이 중요하다

요즘 공격자들은 다양한 조직들을 다양한 수법으로 공략하고 있으며, 어떤 식으로 피해를 입혀야 가장 큰 피해를 입고, 따라서 협상에 응할 가능성이 높은 지를 잘 이해한다



랜섬웨어 '갈수록 악랄'...데이터 훔치고 파괴까지

- ✓ 데이터를 유출하거나 시스템 파일을 감염시키는 공격 방식
- ✓ 암호화 대신 데이터 삭제 시도
- ✓ IT 장비만을 대상으로 하는 것이 아니라 클라우드 시스템 업체를 공격해 해당 시스템을 사용하는 이용자들을 한꺼번에 공격

백업데이터, 한번 의심해 보세요

랜섬웨어로부터 보호하기 위해 대다수의 기업이 백업 전략에 기반해 데이터를 관리 중
하지만 이렇게 저장한 백업 데이터를 실제로 복구해 본 경험은 극히 적다.

Q1. 백업 데이터만 있으면 랜섬웨어 대응이 될까?

Q2. 백업 데이터는 해킹으로부터 안전한가?

Q3. 백업 데이터를 저장한 곳은 안전한가?

Q4. 백업 데이터로 복구는 잘 되는가?

Q5. 다른 요인으로 데이터 손상은 없을까?

백업 데이터만 있으면 랜섬웨어 대응이 될까?

백업 데이터가 최후의 보루가 되지 못한 사례

2017년 영국 NHS(국민건강보험서비스) 사례
WannaCry 랜섬웨어 공격 이후 백업 데이터를 가지고 있었음에도 완전한 복구에 실패, 결국 몸값을 지불.

2021년 Colonial Pipeline 사례
백업 데이터를 가지고 있음에도 백업 복구에 실패,
결국 랜섬웨어 몸값을 지불.

백업은 사이버 공격에 대한 가장 믿음직스러운 방어책
하지만 그건 제대로 관리가 되었을 때의 이야기.

백업 데이터가 최후의 보루가 되기 위해서는

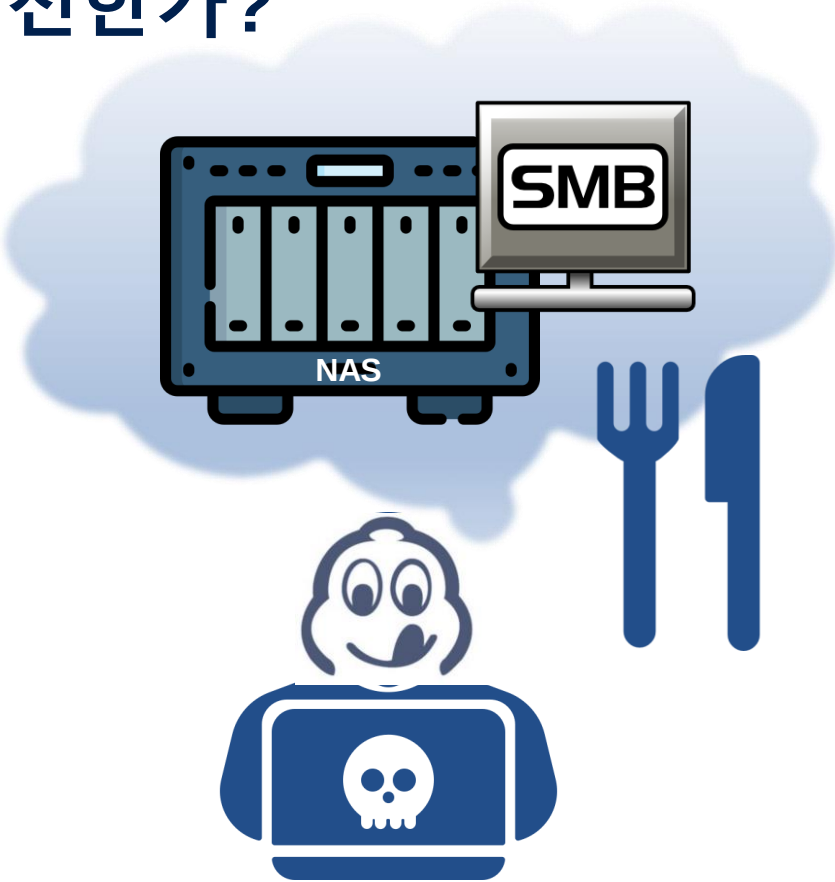
- ✓ 백업 데이터와 저장소가 안전한지 검증
- ✓ 지속적으로 백업 데이터의 무결성 검증
- ✓ 평소에 모의 훈련을 통해 최적의 복구 프로세스 수립
- ✓ 3.2.1 정책에 맞게 백업 데이터 관리

백업 데이터를 저장한 곳은 안전한가?

해킹에 가장 취약한 부분 중 하나인 NAS, SMB

엔드포인트와 네트워크 보안은 열심히 하지만 정작 랜섬웨어 대처에 가장 중요하고 강력한 방어 대책인 백업에 대한 저장소는 안중에 없다.

NAS는 기업 네트워크 내에서 그리 단단하지 않은 장비 중 하나, 봇넷으로 감염시킨 후 NAS를 통해 기업의 네트워크에 접속하는 해킹 공격이 급증



NAS 저장소, SMB protocol 은 이른바 해킹 맛집

- ✓ 랜섬웨어 워너크라이 보안 패치 진행하지 않은 기업이 다수
- ✓ 보안에 취약함에도 여전히 SMB 1.0 사용하는 기업이 다수 (68%가 여전히 SMB v1을 사용 중 2022)

백업 데이터로 복구는 잘 되는가?

백업 데이터 실제로 복구해 보신 적 있나요?

백업 정책을 수립할 때 백업주기, 저장위치, 복구 절차를 계획하지만, 실제로 복구하는 경우는 극히 드물다.
그리고 여러가지 외적, 내적 요인들로 인해 실제 장애 상황에서 복구를 시도할 때 실패가 빈번하다.

복구가 실패하는 이유

- ✓ 백업데이터의 불완전성
- ✓ 백업 데이터의 오래된 버전 사용
- ✓ 복구 과정의 기술적 제한

백업 데이터로 복구는 잘 되는가?

복구 시 비즈니스 연속성, 보장할 수 있나요?

재해 상황에서 가장 급선무인 작업은 바로 복구.

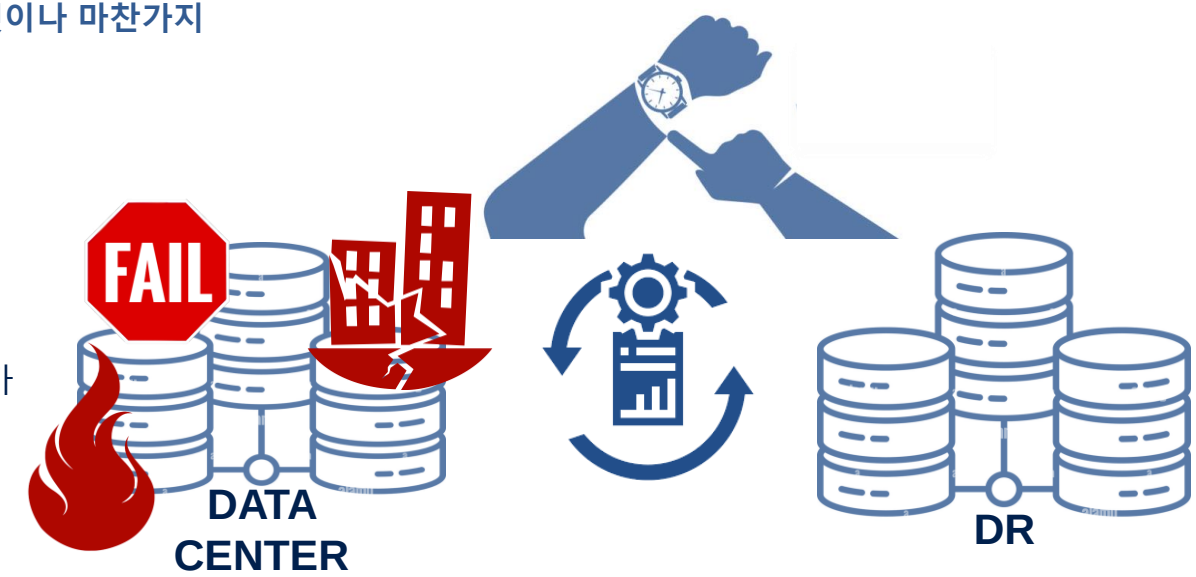
그 중에서도 속도가 가장 중요한데, 백업 파일을 복구하는 데 며칠, 몇 주 또는 몇 개월이 걸린다면 사실상 복구에 실패한 것이나 마찬가지

DR이 어려운 이유

프로세스의 한계 : 의사결정, 부서간 책임, 모의훈련 절차에 필요한 프로세스의 부제

경제적 비용의 부담 : 인프라의 구성, Fail-over/back 에 걸리는 인적,물적 자원의 소모가 상당하다.

예측의 어려움 : 일시적인 장애인지 DR전환이 필요한지 예측이 어렵다.



다른 요인으로 데이터 손상은 없을까?

그럼에도 불구하고 복구가 실패하는 또 다른 이유는?

- ✓ **저장 장치 오류** : 백업 데이터를 저장하는 장치 자체에서 문제가 발생 할 수 있다. 물리적인 손상, 전원 공급 장애, 소프트웨어 문제등
- ✓ **인간의 실수** : 백업 데이터를 관리하는 사람이 실수로 삭제하거나 백업을 수행하지 않거나 잘못된 백업 시간을 설정한 경우
- ✓ **자연 재해** : 백업 데이터를 저장하는 물리적 장소가 자연 재해로 손상될 수 있다.

Acronis

#CyberFit

아크로니스의 데이터 보호 전략

사이버 복원력 관점에서의 제로 트러스트

[체크리스트] 사이버 복원력 관점의 제로 트러스트

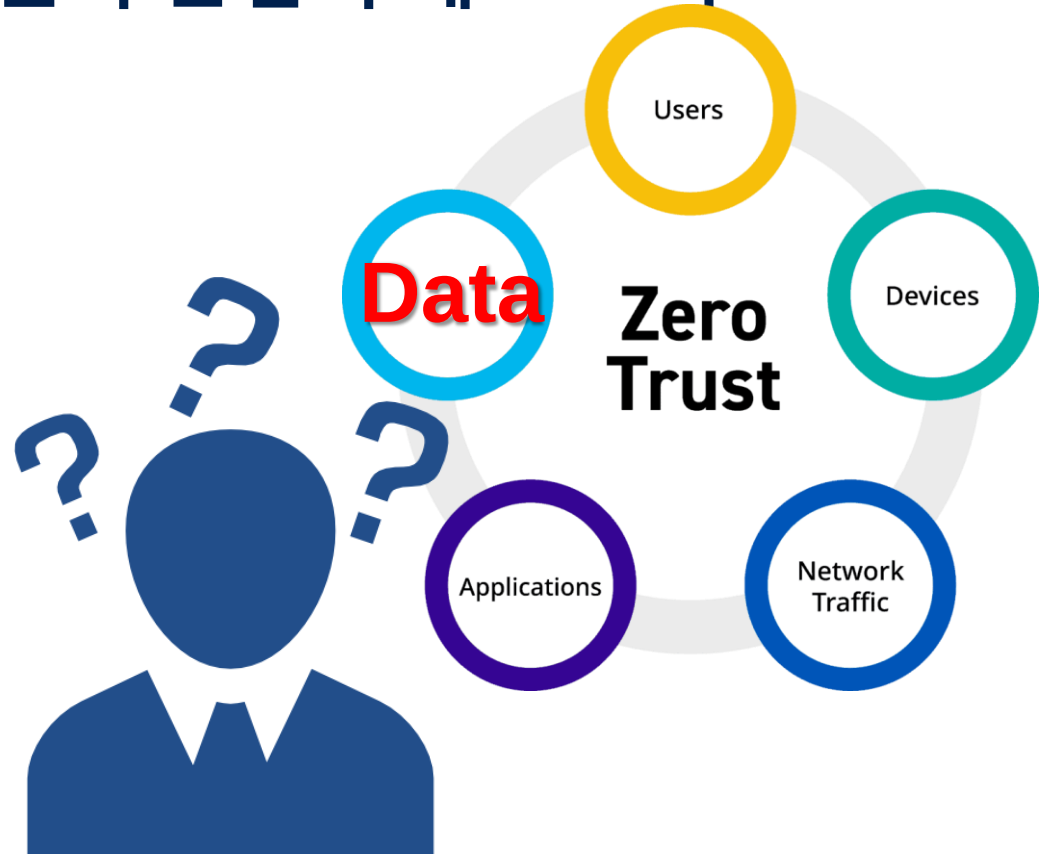
Q1. 백업 데이터만 있으면 랜섬웨어 대응이 될까?

Q2. 백업 데이터는 해킹으로부터 안전한가?

Q3. 백업 데이터를 저장한 곳은 안전한가?

Q4. 백업 데이터로 복구는 잘 되는가?

Q5. 다른 요인으로 데이터 손상은 없을까?



다중 계층 보호를 통해

아크로니스 Security

Acronis Active Protection

랜섬웨어 방지,
크립토재킹 방지

정적 AI 분석 엔진

시그니처 탐지 엔진

행동 기반 엔진

랜섬웨어&맬웨어로부터 깨끗한 데이터

Acronis 백업

백업 데이터 맬웨어 스캔

Acronis 다중 계층식 통합 보호

여러 방어 계층을 통합하여 사이버 공격의 모든 단계에서 위협을 예방 및 교정

다중 계층 보호의 장점

- ✓ **대처능력** : 보안과 백업 기술을 중첩해서 사용하여 다양한 위협으로 부터 보호가 가능하다.
- ✓ **복구능력** : 데이터 손실, 인프라 장애로 부터 빠르게 대응이 가능하다.

백업 데이터는 해킹으로부터 안전한가?

해킹으로부터 백업 데이터와 에이전트를 보호

보안, 백업 에이전트, 프로세스 등을 무력화 시키는 것은 해커들이 대부분의 시스템에서 접근하는 첫번째 단계 보안과 백업 및 복구 서비스를 중단하기 위해 에이전트, 백업 파일, 백업 소프트웨어, Windows Volume Shadow Copy 서비스 또는 클라우드 스토리지를 대상으로 하는 랜섬웨어 방지가 필요하다.

스스로를 방어하는 Acronis 소프트웨어

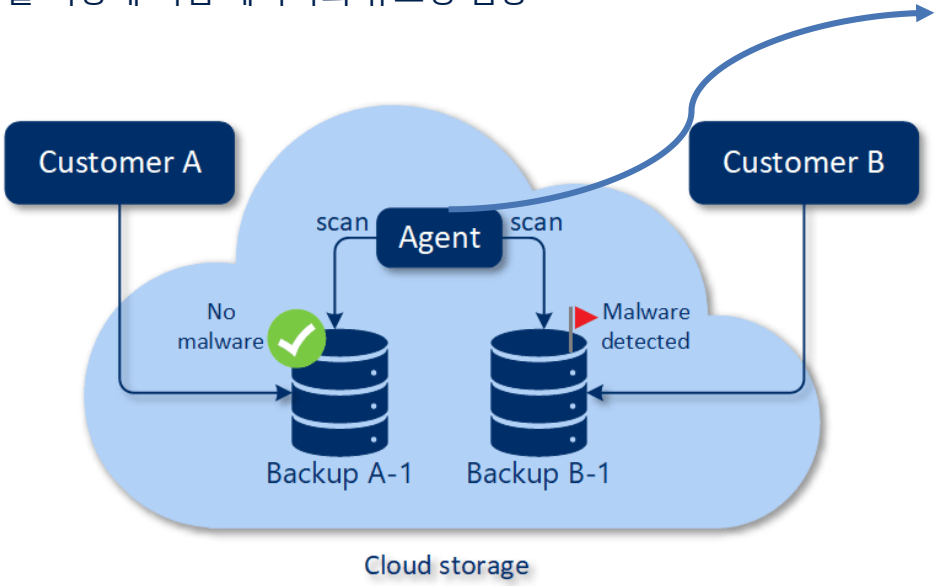
- ✓에이전트 자체 보호
- ✓백업 자체 보호
- ✓프로세스 자체 보호

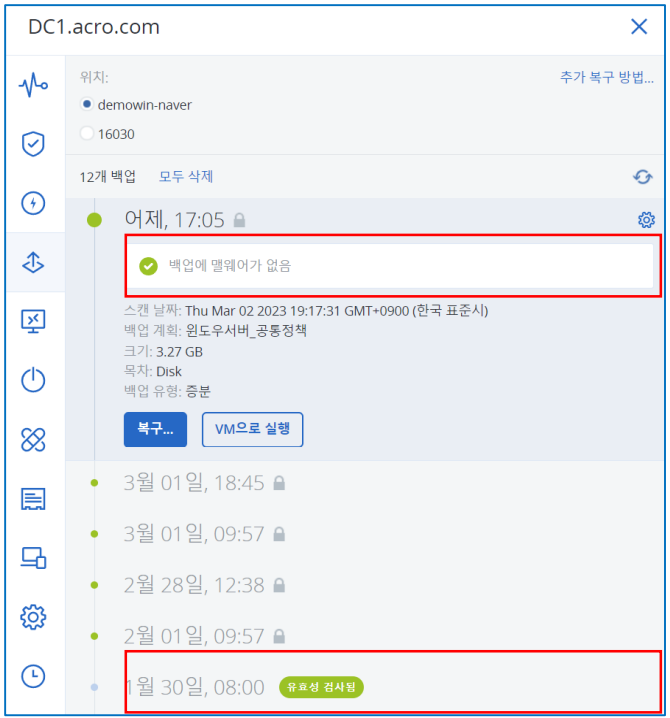
백업 데이터를 저장한 곳은 안전한가?

백업 데이터의 무결성을 검증하자

백업에서 감염된 파일 검사 및 복구, 파일 자체의 손상 여부 검사

✓ 백업 데이터에 대해 멜웨어 스캔 가능
✓ 체크섬 검사를 이용해 백업 데이터의 유효성 검증



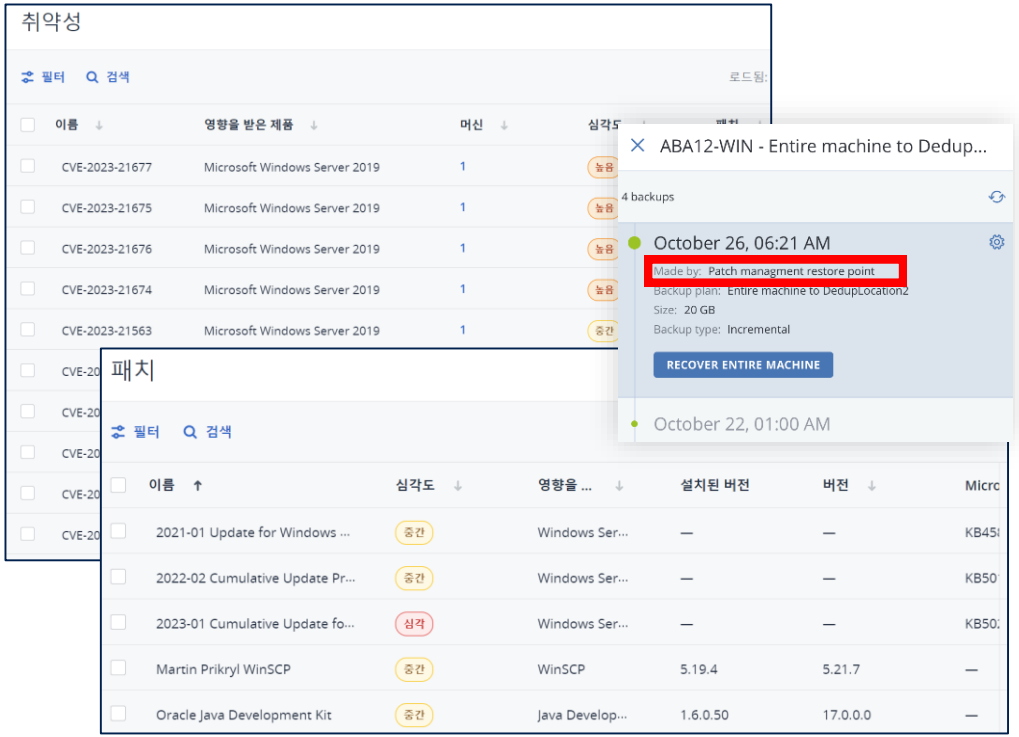


백업 데이터를 저장한 곳은 안전한가?

최신 패치를 적용해 SMB, NAS 취약점을 보안하자

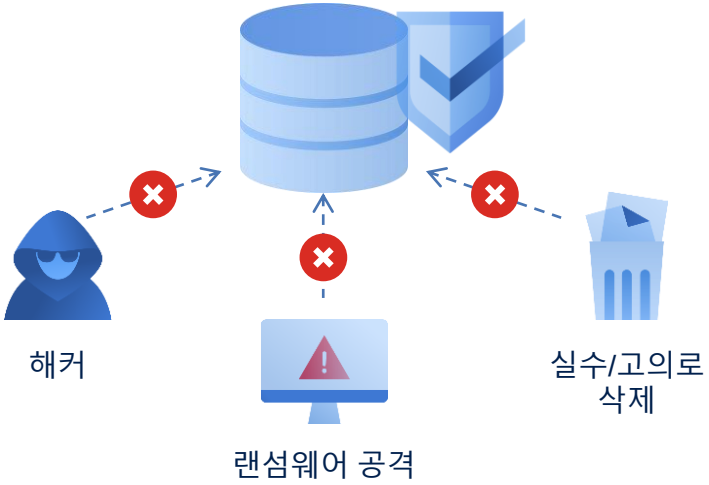
취약성 평가, 패치 관리 & 페일세이프 복구

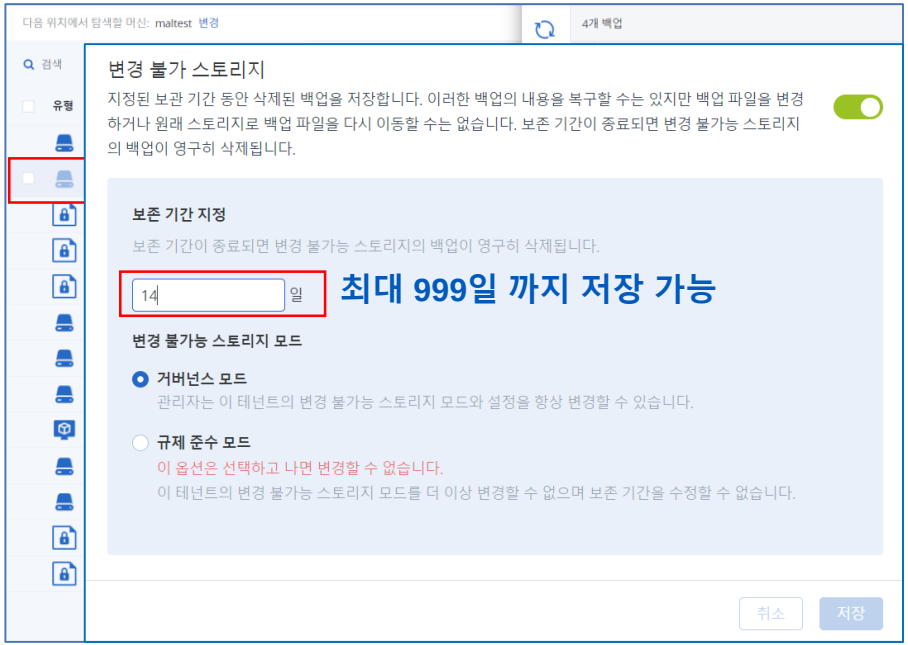
✓취약성 평가, 관련 패치 및 자동화 기능 제공
✓패치 실패 시 패치 직전의 상태로 롤백 할 수 있도록 패치 전에 자동으로 백업 가능



백업 데이터를 저장한 곳은 안전한가?

해커의 악의적인 행동으로부터 보호 가능한 저장소





변조 불가능한 백업 데이터 저장소

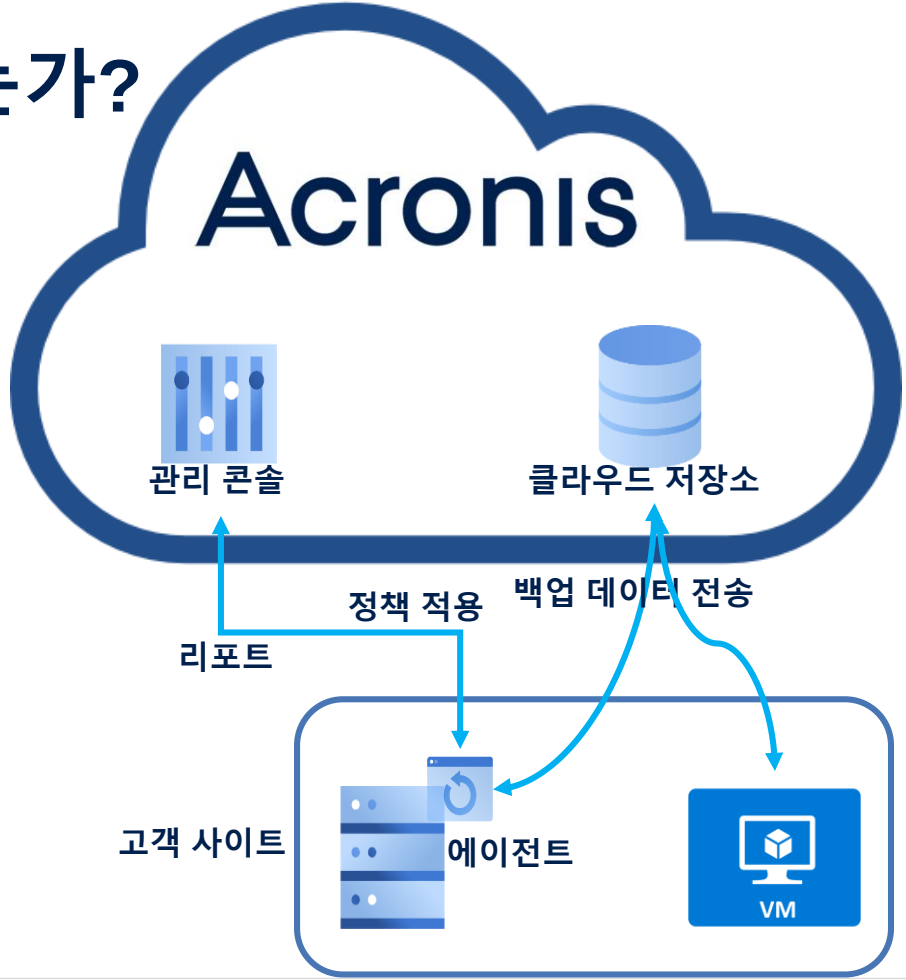
- ✓해커의 데이터 삭제 시도 무효화
- ✓랜섬웨어에 영향 받지 않음
- ✓실수/고의로 지워진 데이터 삭제 지연

백업 데이터로 복구는 잘 되는가?

간편한 복구 테스트 – 몇 초 만에 다시 실행

Acronis Instant Restore 기술

- ✓ 대상에 영향을 끼치지 않으면서 백업 데이터를 다른 VM에 복구 가능
- ✓ 고객의 가상화 환경에서 백업 데이터를 사용해 복구 및 테스트 가능
- ✓ VM이 몇 초 만에 실행되며 빠르게 백그라운드에서 데이터를 호스트로 이동

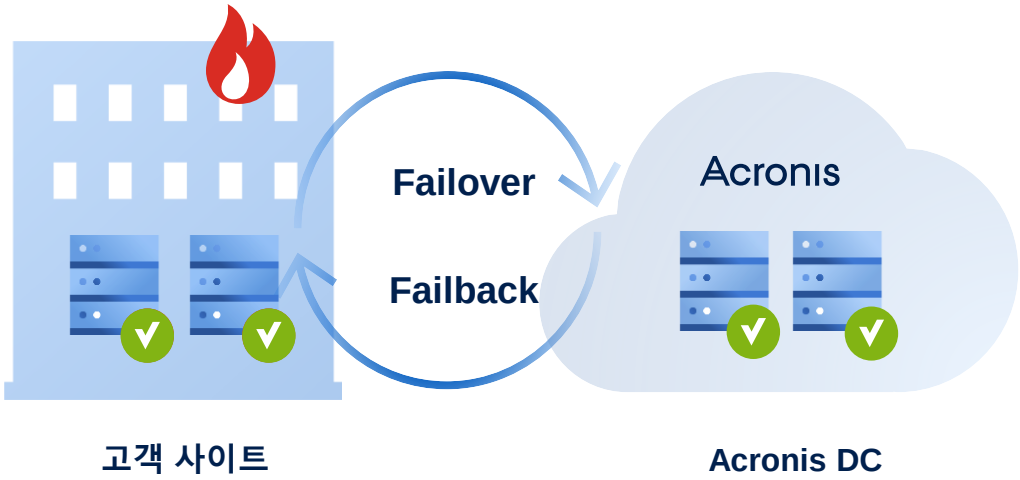


다른 요인으로 데이터 손상은 없을까?

모든 재해 상황에 신속한 사이버 복원력 - 아크로니스 DR-as-a-Service

Acronis DR

- ✓ 재해 복구 인프라를 DRaaS 로 제공
- ✓ 테스트 및 프로덕션 환경 제공
- ✓ 유연한 네트워크 구성 방식(VPN-appliance, IPsec)
- ✓ 런북을 통한 대규모 오케스트레이션 기능 제공



정리

1. 백업 데이터만 있으면 랜섬웨어 대응이 될까?
   답 : 백업 데이터로 인해 완벽한 복구, 정해진 RTO 내 정상화가 가능하다면 대응이 된다. 하지만 이를 위해서는 검증되어야 할 요건들이 있다. 각 요건들이 충실히 이행되지 않는 한 랜섬웨어 대응이 현실적으로 불가능하다.

2. 백업 데이터는 해킹으로부터 안전한가?
   답 : 백업 데이터는 해커들의 1순위 목표이다. 백업 데이터의 훼손, 에이전트의 강제종료 등으로 부터 보호 가능해야 하며 사용자의 실수로 지워진 백업 데이터에 대해서 복구가 가능해야 한다. 지속적으로 백업 데이터의 무결성을 검증하는 작업이 필요하다.

3. 백업 데이터를 저장한 곳은 안전한가?
   답: 백업 데이터가 저장되는 NAS, SMB는 해킹공격에 매우 취약하다. 보안이 취약한 로컬 저장소 외 안전한 장소에 백업 데이터를 소산해 둬야 한다.

4. 백업 데이터로 복구는 잘 되는가?
   답: 백업 데이터의 무결성이 보장된다고 해도 여러가지 요인들로 인해 복구가 실패할 가능성이 있다. 지속적인 모의 복구 훈련이 수행되어 복구가 잘됨을 검증해야 한다.

5. 다른 요인으로 데이터 손상은 없을까?
   답: 백업 데이터에서 발생하는 문제 외 자연재해, 하드웨어의 손상, 사용자의 실수로 발생하는 데이터 손상이 있을 수 있다. 백업 복구 시스템은 백업 데이터 뿐 아니라 복구 서버의 가용성이 보장되어야 한다. 기존 사이트 내 DR을 구축하여 다양한 요인으로 부터 발생하는 복구 실패를 예방할 수 있다.

백업과 보안, 관리가 통합된 솔루션

Acronis Cyber Protect Cloud

차세대 사이버보안

제로 데이 공격 방지를 위한 고급 AI 기반 행동 감지 엔진

+

안정적인 백업 및 복구

보안 포렌식을 위한 전체 이미지 및 파일 수준 백업, 재해 복구 및 메타데이터 수집

+

엔터프라이즈 보호 관리

URL 필터링, 취약점 평가, 패치 관리, 원격 관리, 드라이브 상태

통합의 효과 = 보안 & 생산성 향상 + 운영 비용 절감 효과
IT 관리자를 위한 탁월한 관리 효율성

Acronis

#CyberFit

[부록] 아크로니스의 통합 사이버 보호 소개

주요 정보 및 사이버 보호 체크리스트 및 2023 주요 행사 안내

아크로니스가 특별한 이유는 무엇일까요?

데이터 보호와 사이버 보안을 통합하여 모든 데이터, 애플리케이션 및 시스템을 보호하는 최초이자 유일한 사이버 보호 기업입니다.

Acronis는 백업, 복구 및 차세대 AI 기반 맬웨어 방어 및 보호 관리를 하나의 솔루션으로 통합합니다. 이러한 통합 및 자동화는 생산성을 높이고 TCO를 절감하는 동시에 완벽한 사이버 보호를 제공합니다.

하나의 에이전트, 하나의 웹 기반 관리 콘솔 및 하나의 라이센스를 통해 통합되지 않은 솔루션과 관련된 복잡성과 위험을 제거하는 동시에 **예방, 감지, 대응, 복구 및 포렌식**이라는 5가지 주요 사이버 보호 단계를 활용할 수 있습니다.

Acronis

#CyberFit

360도 올어라운드 통합 사이버 보호

백업·복구·보안·시스템 관리를 하나로

견고한 3단계 보호 아키텍처

사전 예방적 보호	Prevent	✓ 취약성 평가 및 패치 관리 ✓ URL 필터링
실행 중 능동적 보호	Detect	✓ 맬웨어로부터 보호 (동작, 휴리스틱스) ✓ 메모리 기반 공격 탐지 (AI/ML 기반)
사후 대응적 보호	Respond	✓ 데이터 백업 및 복구 ✓ 원격 관리

아크로니스의 검증된 MSP 플랫폼 비즈니스 이력

제품 개발 단계부터 MSP 서비스 기업을 고려하였습니다.

SaaS 비즈니스의 핵심은 반복수익(MRR·ARR)의 확보

아크로니스의 단일화된 통합 사이버 보호 솔루션을 기반으로
교차·상향판매(upsell & cross-sell)가 용이합니다.
사용자 만족도를 높이는 통합 리포팅 기능, 풍부한 교육과
마케팅 리소스가 고객 이탈 방지와 신뢰 관계 구축을 위해 제공됩니다.

사이버 보호 비용이 최대 50% 절감됩니다.

여러 벤더의 포인트 솔루션을 구매하는 대신, 통합 솔루션으로
비용을 절감할 수 있습니다. 관리를 간소화하고 워크플로 자동화를 개선하며,
도구 패치 작업을 사용하여 보안 위험 발생을 줄일 수 있습니다.
단일 라이센스, 단일 에이전트, 직관적인 단일 콘솔을 통한 제어 및 배포 등
통합형 솔루션으로 통합의 위력을 누려보세요.

서비스 공급 업체를 위한 50개 이상의 플랫폼 통합

ConnectWise · Kaseya · Autotask · ATERA
Microsoft 365 · Google Workspace · MariaDB

20년 동안 동급 최고의 기술 제공

20,000개 이상의 서비스 제공 업체
750,000개 이상의 기업체
26개 언어
150개 이상의 국가

아크로니스의 검증된 통합 사이버 보호 기술력

Approved corporate endpoint protection for macOS

Gold medal for Endpoint protection

Editors' choice

VB100 certified

AV-TEST participant and test winner

ICSA Labs endpoint anti-malware certified

AV-Comparatives participant and test winner

Anti-Malware Testing Standards Organization member

VirusTotal member

Microsoft Virus Initiative member

감지율 100%

VB100 인증 테스트에서 아크로니스는 맬웨어를 100% 감지했으며 오탐률은 0%였습니다.

오탐 0%

AV 비교 테스트에서 아크로니스는 오탐 0건을 기록한 단 4가지 솔루션 중 하나였습니다.

고성능 100%

아크로니스는 AV-TEST의 8가지 성능 카테고리 모두에서 매우 빠름 또는 빠름 성능 등급을 받았습니다.

데이터 보호와 보안 전용 인프라를 갖춘 유일한 벤더

전세계 스포츠팀과의 파트너십과 통합 사이버 보호 현황

40+
스포츠팀

20,000+
보호 워크로드 수

5PB+
보호 데이터

Unlimited
서비스 제공업체와의 사업기회 창출

아직도 클라우드 백업을 위해 값비싼 CSP를 사용하시나요?

데이터 보호 전용 클라우드 데이터센터 를 보유한 벤더, **아크로니스** 뿐입니다.

- 네트워크 비용 **없음**
- 데이터 보관 기간 **무제한**
- 데이터 저장 위치 **선택권**
- 복구 비용 **없음**

아크로니스의 통합 사이버 보호는 계속 진화합니다.

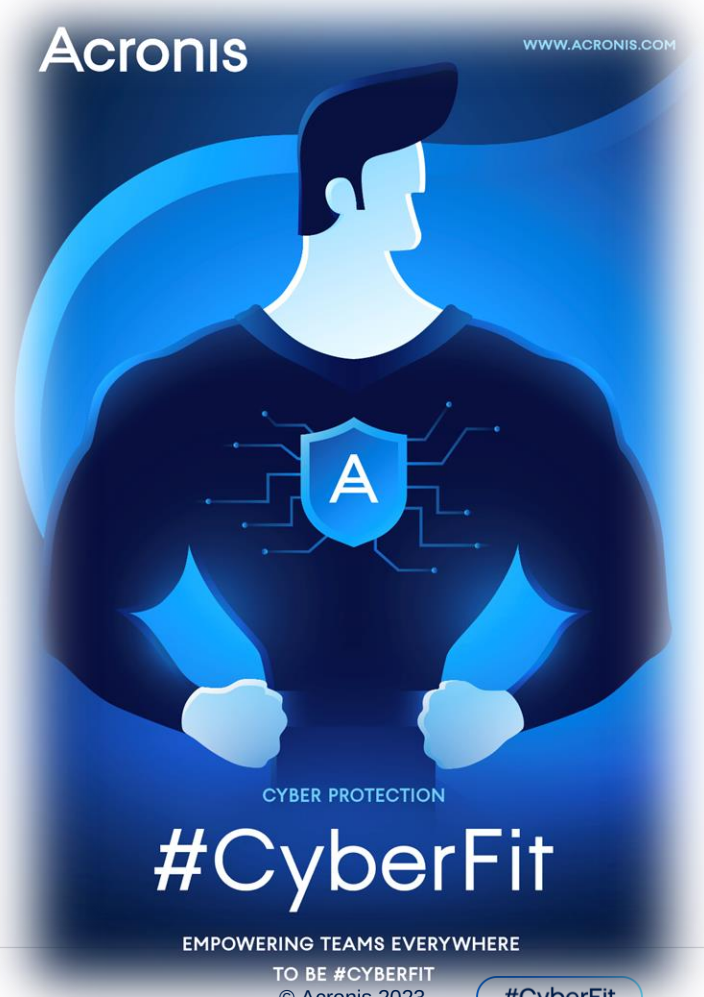
어제의 기능으로 판단하지 마세요.

항상 최신의 기능으로 확인하세요.

사이버보호 체크리스트 & 제품 체험 가이드

사이버 보호 제대로 하고 계십니까?
바로 지금, 직접 체크해 보세요.

- ☑ 글로벌 악성 샘플 수집으로 빠른 업데이트가 가능합니까?
- ☑ 데이터 보호를 위한 글로벌 클라우드 데이터 센터 이용이 가능하여 신종 사이버 위협에 신속한 대응이 가능합니까?
- ☑ 사용자 기반 침입 방지 시스템을 통한 다중 계층 보안 기능을 제공합니까?
- ☑ 취약점 평가 및 패치 관리를 통해 강화된 보안 성능을 제공합니까?
- ☑ 월 단위 제품 업데이트를 통해 기능을 확장하여 새로운 보안 위협에 빠르게 대응합니까?
- ☑ 단일 서비스에 통합 보호 기능을 제공하여 단일 에이전트 및 단일 보호 계획을 통해 사이버 보호가 가능합니까?
- ☑ 자체 단일 엔진을 사용하여 애플리케이션을 최적화 할 수 있습니까?
- ☑ 호환 및 충돌의 문제 발생 시 빠른 수정이 가능합니까?
- ☑ 다양한 OS와 애플리케이션, 오픈소스 DB까지 보호가 가능합니까?
- ☑ 엔드포인트 제어 기능을 통한 사용자 제한 기능으로 차별화된 보안을 제공합니까?



이제 직접 사용해 볼 시간!

Acronis Cyber Protect Cloud 30일 무료 평가판 등록 및 계정 활성화 방법

1. 등록 양식 작성

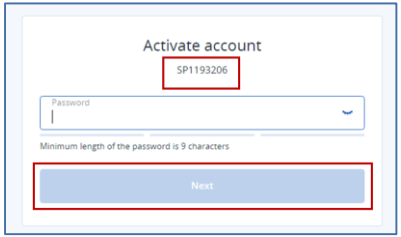
[트라이얼 바로가기]

- **국가** : Korea
- **데이터 센터 위치**: Korea 선택

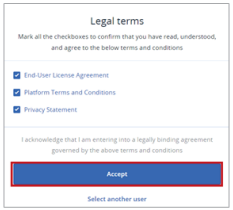
2. 메일로 **계정 활성화 링크** 확인

- 메일 수신에 **최대 10분**까지 소요
- 메일 수신에 문제시 **다른 메일 주소**로 등록해 보십시오

3. **계정 활성화 및 암호 설정**

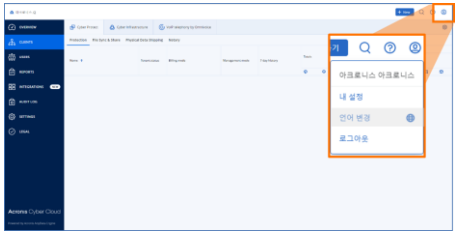


- Activate account 아래 코드가 **본인의 계정 ID**
- 암호 생성조건에 따라 암호 설정 후 Next 클릭



- 사용자 약관 및 정책 사항 체크 후 Accept

4. 사이버 프로텍트 **콘솔 화면 접속**



- 언어가 영문으로 나올 시 **언어 변경**을 클릭하여 **한국어**로 변경하실 수 있습니다.
- **로그아웃** 후 다시 정상적으로 **로그인**이 되는지 확인해 보세요.

혼자서 쉽게 따라해 보는 통합 IT 백업과 보안 관리
주제별 가이드 영상 모음

통합 사이버 보호 서비스 직접 만들어 보기

영상 보기

온보딩

에이전트 설치 및 콘솔 둘러보기

취약성 평가 및 패치 관리

랜섬웨어 대응

백업 구성하기

원격 지원

보고서 구성하기

끊임없이 진화하는 위협 환경에서 사이버 보호를 관리하는 것은 쉬운 일이 아닙니다.
귀사를 제대로 도와드릴 수 있는 전문가를 만나세요.
아크로니스는 고객이 가치를 느낄 수 있는 솔루션을 통해 클라우드 SaaS 비즈니스 엑셀러레이터로서 여러분을 MSP로 탈바꿈해 드릴 수 있는 전문가를 보유하고 있습니다.

아크로니스 전문가와 상담을 받으려면

Team-Sales-Korea@acronis.com

빠르게 전화로 연락!

Acronis 채진주 과장
010-2311-5500

Acronis

당신의 생활을 바꾸는 아크로니스 웨비나

백업과 보안이 하나로, 한방에!
실전 데모로 보여드림

라이브 데모
웨비나 등록하기

2023년
아찾세 시리즈

"아크로니스의 찾아가는 세미나"

당신의 데이터와 보안에 대한 고민,
아크로니스가 직접 해결해 드립니다.

30초 설문에 응답하세요.
아크로니스가 직접 찾아갑니다.