

Acronis

IT 보안 관리,
통합 사이버 보호로
얼마나 편해질 수 있을까

전현근, 아크로니스코리아

더욱 복잡해지는 위협 환경



400%

코로나19 팬데믹 중 사이버
범죄 증가율



57%

기존 안티바이러스
솔루션에서 놓친 공격 비율



69%

위협의 방어보다 관리 도구에
더 많은 시간을 사용하는 비율

출처: Acronis Cyberthreats Report 2021, FBI

원격 및 재택 근무자에 치명적인 **사이버 위협**



서비스 제공업체가 직면한 사이버 보안 과제

가장 약한 연결고리는 사용자

- 88%의 침해 원인은 **엔드포인트 공격**

새로운 공격 대상이 된 MSP

- 37%의 MSP가 작년 대비 **사이버 범죄에 더 취약해졌다** 여겨
- 25%의 MSP가 **지난 12개월간 사이버 보안 이슈 발생 경험**

출처: FBI; "State of endpoint security risk", Ponemon Institute, "Cost of Data Breach Report", "Psychology of Human Error", 스탠퍼드 대학교, "The State of MSP Cyber security in 2019", Vanson Bourne, "MSP Benchmark Survey, Kaseya, "2021 MSP Threat Report", Perch, Alert (TA18-276B), DHS

사이버 위협 대처방안



- 차세대 보안 기술
- 실시간 장치 보호
- AV 업데이트



- 취약성 평가
- OS 및 응용SW 업데이트
- 패치 관리
- 중앙 집중 관리



- 최후의 보루 백업
- 다양한 형태의 백업
- 안전한 복구

이 모든 기술을 적재적시에 운영해야 하는 과제는 누구의 몫?

Acronis

사이버 위협 예방
누구의 몫일까

IT 관리자의 일상

1

초기 설정

신규 사용자 온보딩

새 장치 구성

2

엔드포인트 데이터 보호

중요 데이터/서비스
액세스 제공

다운타임 최소화

3

모니터링, 보고 & 관리

SW & HW
모니터링
및 관리

OS,
소프트웨어
업데이트

보고서
준비

4

트러블슈팅, 원격 지원

원격 연결
원격 지원

시스템 복제
데이터 이전



IT 관리자의 3대 고충



피해자 명단

- IT 엔지니어
- IT 비즈니스 담당자
- IT 고객

1) 초기 설정 및 구성

당신이 해결해야 할 것

- 더 쉽고 빠른 사용자 온보딩
- 필요한 리소스 감소
- 완벽한 초기 보안 세팅

지금 당신에게 필요한 것

- 장치 자동 검색
- 원격 에이전트 및 보호 계획 설치

장치 자동 검색 및 보호계획 적용 까지 한번에

1. 장치 검색

- 네트워크 기반
- AD 기반
- 수동으로 추가

2. 장치 목록

- 검색된 장치 목록
- 장치 선택

3. 검색 후 작업

- 작업 선택
- 에이전트 설치
- 보호 계획 적용

4. 자격 증명

- 장치에 대한 자격 증명
- 사용자 지정

5. 연결

- 장치 등록 후 연결

The screenshot displays the Acronis Cyber Protect console interface, illustrating the workflow for device search and management. The main window shows a list of devices with columns for selection, IP address, and name. The '검색 후 작업' (After Search Action) window is open, showing the '검색 방법 선택' (Select Search Method) step, where '네트워크 기반' (Network-based) is selected. The '자격 증명' (Credentials) window is also open, showing the '자격 증명 제공' (Provide Credentials) step, where '도메인 사용자 이름' (Domain user name) is entered. The '연결' (Connect) window is also open, showing the '연결' (Connect) step, where the '연결' (Connect) button is highlighted.

선택	이름	IP 주소
<input checked="" type="checkbox"/>	10.82.30.1	
<input checked="" type="checkbox"/>	10.82.30.50	
<input checked="" type="checkbox"/>	10.82.30.57	
<input checked="" type="checkbox"/>	10.82.30.64	
<input checked="" type="checkbox"/>	10.82.30.66	

2) 데이터 보호

당신이 해결해야 할 것

- 사이버 위협 방어
- 다운타임 최소화
- 운영 비용 절감

지금 당신에게 필요한 것

- 단일 보호 솔루션과 공급업체
- 차세대 보안 솔루션

차세대 사이버 보안 기술로 해결

Acronis Cyber Protect

Acronis Cyber Backup



Acronis Active Protection

랜섬웨어 방지,
크립토재킹 방지, AI 및
ML 지원



Acronis 정적 AI 분석기

온액세스 및
주문형 감지



Acronis 안티맬웨어 엔진

모든 맬웨어
(클라우드 및 로컬
감지)



Acronis Behavioral Engine

온액세스
감지

3) 유연한 모니터링 및 리포팅

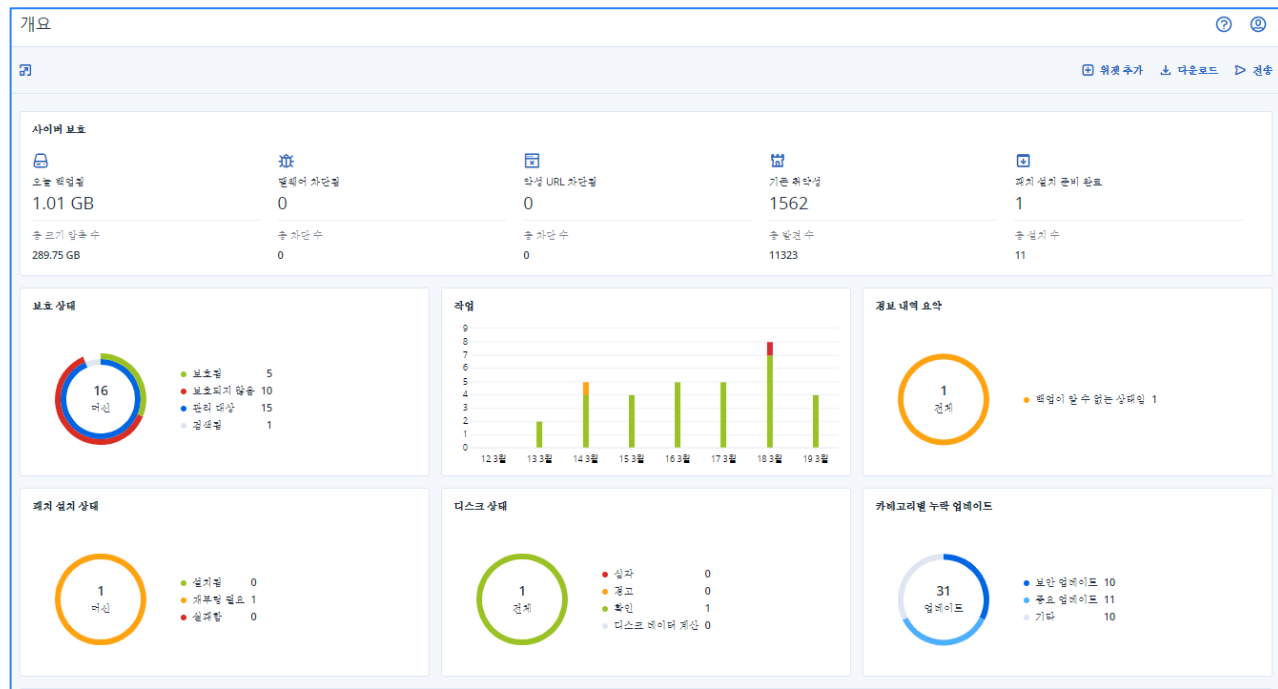
당신이 해결해야 할 것

- 전체 IT 인프라 모니터링
- 정기 업데이트
- 주기적인 보고서 발행

지금 당신에게 필요한 것

- 단일 창
- 신속한 운영 관리
- 보고서 제공 기능

한눈에 보이는 모니터링



- 사이버 보호 현황
- 하드웨어 상태
- 보안 업데이트 상태
- 작업 이력
- 활성화 된 경보
- 패치 상태
- 사용자 정의 가능한
대시보드 위젯

알아서 보고서 작성까지



PDF OR
Excel
보고서 생성

사용자 정의
보고서 생성

월간/주간 등
주기 설정



가치 증명

4) 지원 및 관리

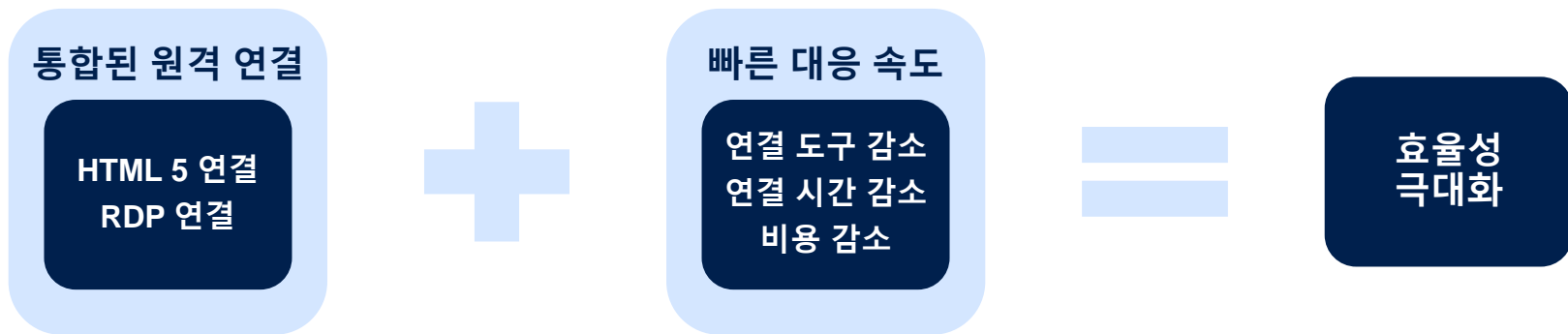
당신이 해결해야 할 것

- 트러블 슈팅 효율 향상
- 원활한 원격 지원
- 최신 프로그램 유지

지금 당신에게 필요한 것

- 통합된 원격 접속 기능
- 취약성 검색
- 중앙 집중식 패치 관리

통합된 원격지원 관리



All devices + Add ≡ ⌘ ? 🔍

Search Selected: 1 / Loaded: 2 / Total: 2

<input type="checkbox"/>	Type	Name ↑	Account	Status	Last backup	Next backup	Agent
<input type="checkbox"/>	VM	DESKTOP-HHNKBMQ	GreenTorch	✖ Suspicious activity ...	Dec 30 06:11:28 PM	Dec 31 12:51:15 PM	DESKTOP-HHNK...
<input type="checkbox"/>	VM	Win81	GreenTorch	⚠ Malware is detecte...	Nov 11 10:40:20 PM	Not scheduled	Win81

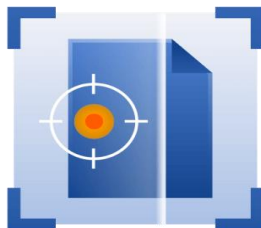
Protect
Recovery
Connect via RDP client
Connect via HTML5 client

사전 예방적 보호 관리



패치 관리

OS 및 응용SW 대한 관리
자동 패치 승인 및 스케줄링
페일세이프(Fail-safe) 패치



취약성 평가

잠재적인 위협 식별
시스템 위험 수준 파악
다양한 OS 및 서드파티 지원



URL 필터링

인터넷 액세스 관리
44개 카테고리 목록
사용자 정의 사이트

5) 안전한 백업/복구

당신이 해결해야 할 것

- 백업 대상 선별
- 백업 데이터 관리
- 안전한 복구

지금 당신에게 필요한 것

- 편리한 백업 관리
- 유연한 저장 위치
- 백업 데이터 검사

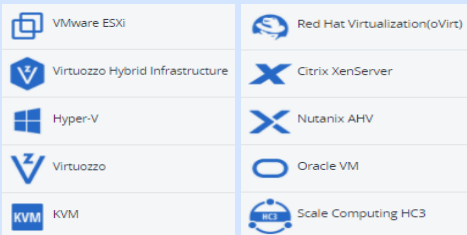
최후의 보루는 백업

다양한 워크로드

PC/서버/모바일 장치



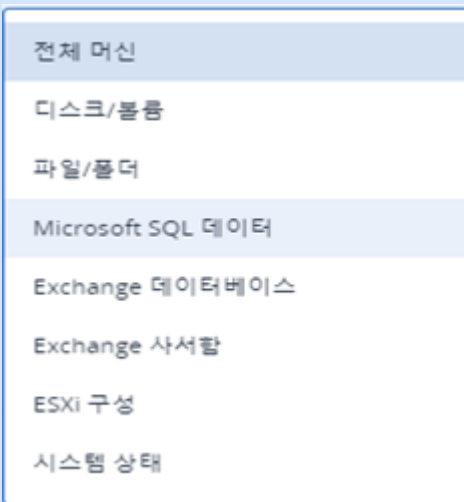
가상화 장치



응용 프로그램

다양한 백업 대상

백업 대상



유연한 백업 저장

클라우드



기타 퍼블릭 클라우드
(게이트웨이를 통해)

온프레미스



간단하고 다양한 복구 방안



Acronis

결국은 통합

백업+보안+IT 관리의 통합

단일

라이선스
인터페이스
콘솔
에이전트
지원 체계

관리자 워크로드



시스템 가용성



데이터 보호 전용 클라우드 데이터 센터의 효용 가치

네트워크
비용
ZERO

데이터
보관 기간
무제한

복구 비용
ZERO

데이터
저장 위치
선택권

아크로니스 전용 클라우드 데이터 센터 보유 현황

대한민국, 서울 데이터센터 오픈 (21년 3월 25일)

41+7

데이터센터



✓ 네트워크 비용 무 ✓ 데이터 보관 기간 무제한 ✓ 데이터 저장 위치 선택권 ✓ 복구 비용 무

Acronis

실제 사이버 보호 사례 소개

사례 1: 법률 사무소

문제의 배경

- 신형 바이러스 감염
- 레거시 AV 솔루션 탐지 실패

문제가 끼친 영향

- 인프라 시스템의 속도 저하
- 임직원의 생산성 50%이상 감소

개선책

- 백업에서 맬웨어를 직접 검색하고 시스템 맬웨어를 복원할 수 있는 **통합 사이버 보호 솔루션** 사용

Acronis Cyber Protect로 80,000 USD 절감
1주일 내 시스템 복구 완료

사례 2: 의료 연구소

문제의 배경

- 레거시 AV 솔루션이 고객 고유의 소프트웨어 오탐 및 경고 발생

문제가 끼친 영향

- IT 관리자가 매번 소프트웨어 업데이트 시 오탐 문제 해결에 2시간 이상 소비
- 임직원 및 연구 인력도 해결 시까지 업무 중단

개선책

- 오탐 방지를 위한 **자동 화이트리스트 업데이트** 기능 사용

Acronis Cyber Protect로 연간 60,000 USD 절감

결론은 Acronis Cyber Protect Cloud – 통합 사이버 보호



Acronis Cyber Foundation

#CyberFit

아크로니스는 ESG 경영을 통한
지속 가능한 성장을 추구합니다.

**Create, Spread and Protect
Knowledge With Us!**

아크로니스 사이버 재단 주요 활동

- 지구촌 교육 취약 계층 지원
- 소외된 지역 사회 아동에게 전문 교육
기회를 제공

www.acronis.org

