

# Acronis

#CyberFit

# Acronis Cyber Protect Cloud

통합 사이버 보호솔루션 소개

아크로니스 코리아  
전현근 부장

# Acronis

#CyberFit

- 2003년 설립 22주년
- 전세계 150개국 600만+
- 34개 지사 2000명+
- 54개의 전용 데이터 센터



# 아크로니스 전용 클라우드 데이터 센터 보유 현황

대한민국, 서울 데이터센터 오픈 (21년 3월 25일)

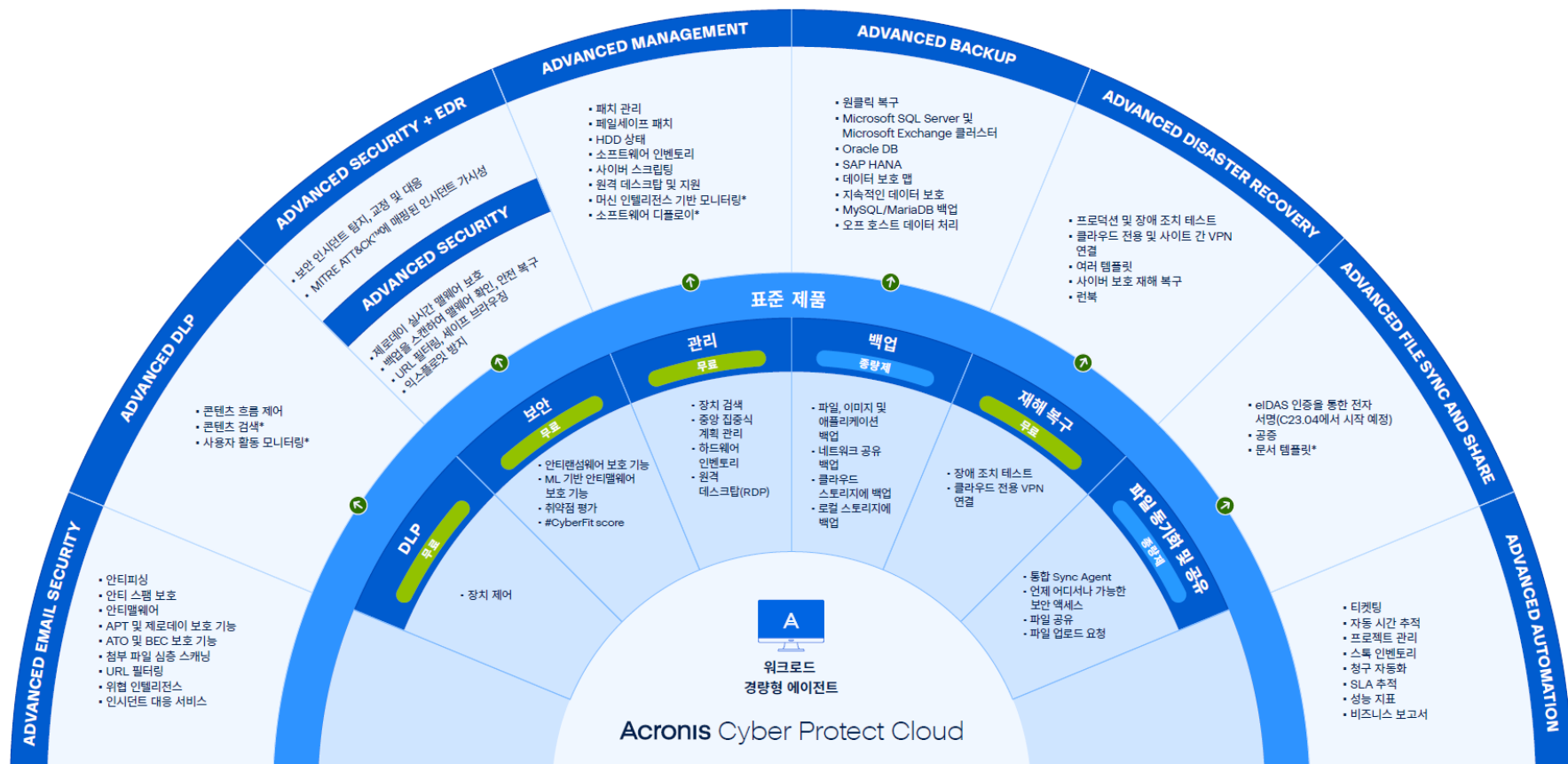
47+7

데이터센터



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

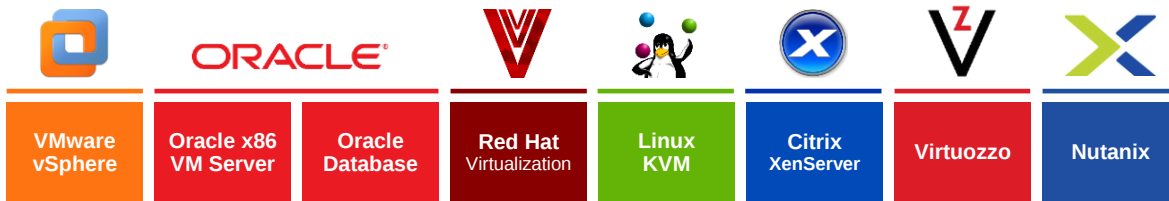
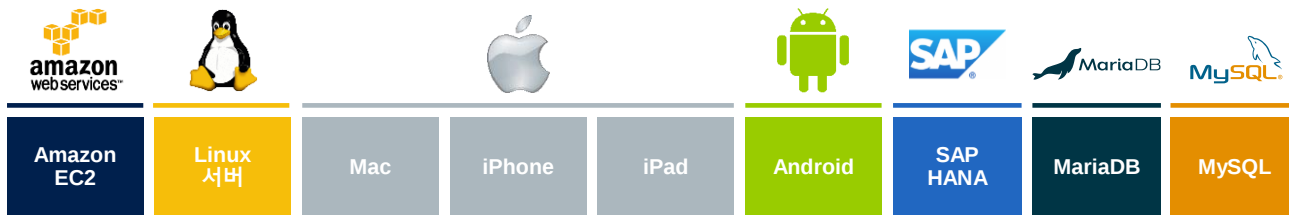
# 하나의 솔루션으로 원하는 가치 그 이상을



## 클라우드 백업 복구 솔루션

백업 및 복구

# 인프라에서 SaaS 앱에 이르기까지 20+개 이상의 워크로드 유형에 대한 보호 제공



단 하나의 솔루션을 사용하여 사이버 보호 제공 간소화



# 전체 이미지 및 파일 수준 백업

## 몇 번의 클릭으로 개별 파일 백업 또는 전체 비즈니스 보호

- **파일 수준 백업:** 이 옵션을 사용해 특정 데이터를 보호하고, 백업 크기를 줄이며 스토리지 공간을 절약
- **전체 이미지 백업:** 시스템 전체를 하나의 파일로 쉽게 백업하여 베어 메탈 복원 보장
- 데이터 재해 발생 시 모든 정보를 새 하드웨어로 손쉽게 복원 가능

Create protection plan

New protection plan (1) Cancel Create

**Backup** Entire machine to C://backups, Monday to Friday at 11:00 PM

What to back up Entire machine

Continuous data protection (CDP) Off

Where to back up C://backups

Schedule Monday to Friday at 11:00 PM

How long to keep Monthly: 6 months  
Weekly: 4 weeks  
Daily: 7 days

Encryption Off

Convert to VM Disabled

Application backup Disabled

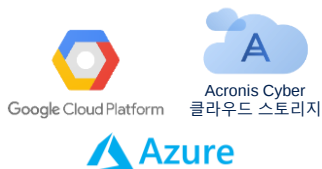
+ Add location

Backup options Change

**이유** 유연한 백업 옵션으로 비즈니스 연속성을 보장하고 다운타임 및 데이터 손실 방지

# 유연한 스토리지 옵션

데이터 자주권 또는 비용 요구 사항 충족



세 개의 토큰 클라우드  
스토리지 옵션

## 클라우드 스토리지



기타 퍼블릭 클라우드  
(게이트웨이를 통해)



자체 또는 서드 파티  
클라우드 스토리지

## 온-프레미스 스토리지



로컬 디스크



SMB/CIFS/DFS 및  
NFS 공유



Acronis  
Cyber Infrastructure

”

다른 솔루션을 선택했을 때는 고객에게 어떤 특정한 것은 할 수 없을 것이라고 말해야 하는 상황이 생겼습니다. **Acronis는 완전한 유연성을 보장하므로** 우리는 최적의 사용자 환경을 제공할 수 있습니다.

**Jason Amato,**  
Centorrino Technologies의  
마케팅 관리자

# 백업을 간편하게 Public Cloud storage에 저장

파트너와 고객의 Azure 스토리지에 간편하게 저장

따로 게이트웨이나 다른 인프라(커넥터등) 설치 없이 바로 백업 데이터를 저장 할 수 있습니다.

## Details

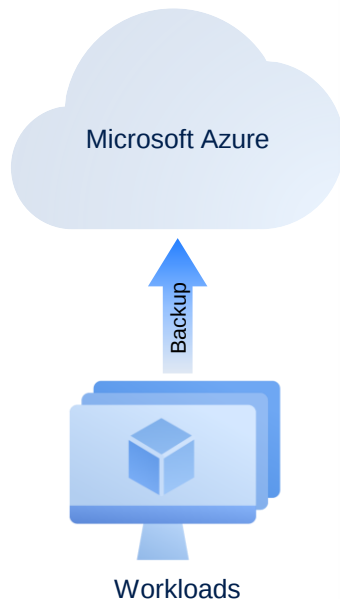
- 최초 접속 시 OAuth-based authentication on Azure.
- Azure-specific permissions, applications, users and roles are configured automatically upon user consent (authenticate only once).
- 스토리지 타입: Storage v2 + Premium Block Blobs.
- Access tiers: Hot + Cool only.

## Scenarios

- Backup and restore Windows/Linux and/or VMs data to/from Microsoft Azure storage, including Disk/volume (Physical + Virtual), Files/folders
- Recover to bare metal via bootable media by registering it on the management server for remote management.

## Licensing

- Advanced Backup license

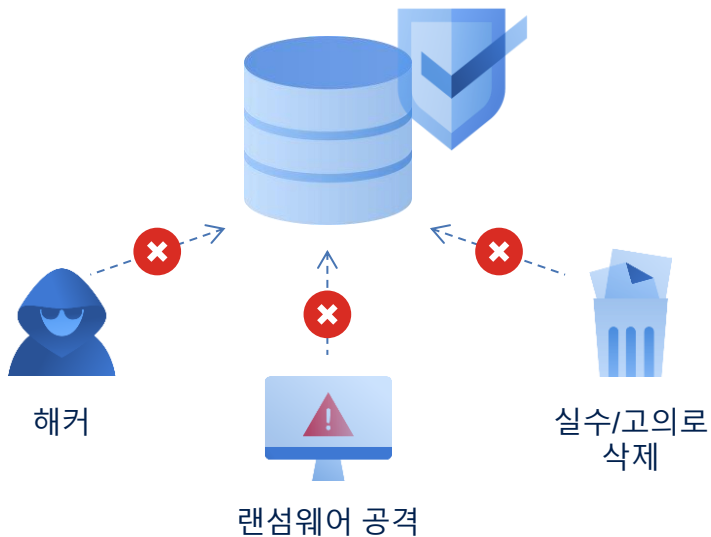


The screenshot shows the 'Add location' dialog box with the 'Public clouds' tab selected. The configuration details are as follows:

| Field                      | Value                        |
|----------------------------|------------------------------|
| Cloud                      | Microsoft Azure              |
| Location name              | Microsoft Azure Storage      |
| Microsoft Azure connection | Microsoft Azure connection 1 |
| Storage account            | Azure backup storage west    |
| Region                     | Default (us-east1)           |
| Container type             | New container (selected)     |
| Container                  |                              |
| Access tier                | Default (Hot)                |
| Folder type                | New folder (selected)        |
| Folder                     |                              |

An 'Add' button is located at the bottom right of the dialog.

# 변조 불가능한 백업데이터



## 사용 사례:

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

다음 위치에서 탐색할 미션: maltest 변경 4개 백업

검색

유형

변경 불가 스토리지

지정된 보관 기간 동안 삭제된 백업을 저장합니다. 이러한 백업의 내용을 복구할 수는 있지만 백업 파일을 변경하거나 원래 스토리지로 백업 파일을 다시 이동할 수는 없습니다. 보관 기간이 종료되면 변경 불가능 스토리지의 백업이 영구히 삭제됩니다.

보존 기간 지정

보존 기간이 종료되면 변경 불가능 스토리지의 백업이 영구히 삭제됩니다.

14 일 **최대 999일 까지 저장 가능**

변경 불가능 스토리지 모드

☒ 거버넌스 모드

관리자는 이 테넌트의 변경 불가능 스토리지 모드와 설정을 항상 변경할 수 있습니다.

☐ 규제 준수 모드

이 옵션은 선택하고 나면 변경할 수 없습니다.

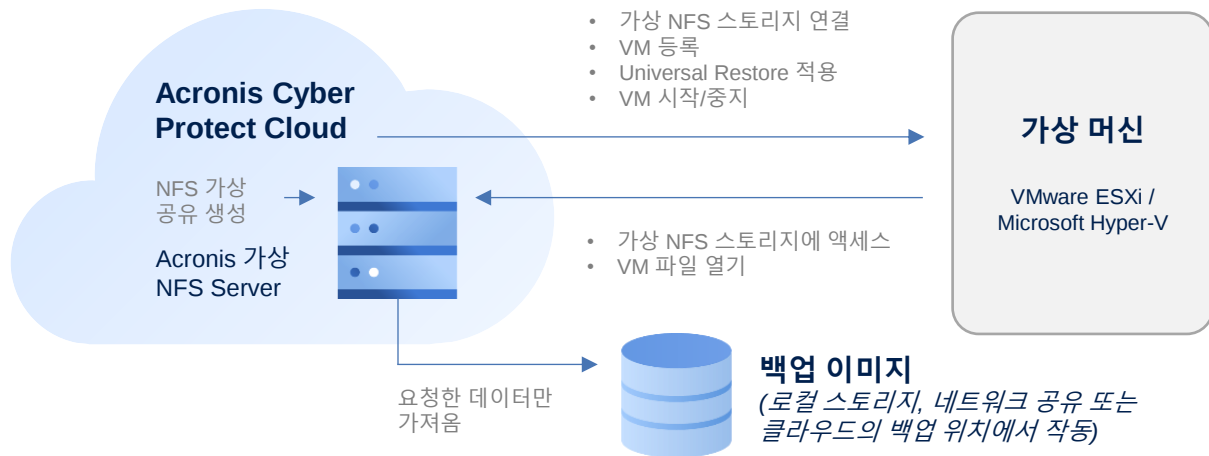
이 테넌트의 변경 불가능 스토리지 모드를 더 이상 변경할 수 없으며 보존 기간을 수정할 수 없습니다.

취소 저장

# Acronis Instant Restore를 통한 업계 최고의 RTO

Acronis Instant Restore는 데이터를 이동하지 않고 기존 Microsoft Hyper-V 또는 VMware vSphere ESXi 호스트의 백업 스토리지에서 직접 Windows 또는 Linux 시스템(실제 또는 가상)을 시작하여 몇 초 만에 시스템을 복구할 수 있는 특허 기술입니다.

## 작동 방식



## 이점

- 초 단위 RTO
- 가상, 실제 또는 클라우드 서버, Windows 또는 Linux 복구
- 네트워크 사용량 감소

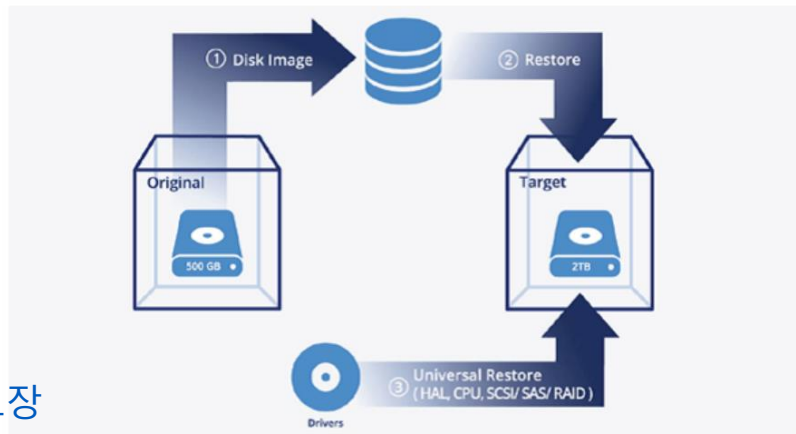
# Acronis Universal Restore

## Windows 및 Linux 시스템을 이기종 하드웨어로 복원

- 베어 메탈 실제, 가상 또는 클라우드 환경을 포함하는 이기종 하드웨어로 쉽고 빠르게 시스템 복구
- Acronis Universal Restore는 디스크 이미지를 있는 그대로 복구한 후 새 하드웨어 플랫폼을 분석하고 새 요구 사항에 맞게 Windows 또는 Linux 설정을 조정

## 이유

- 몇 번의 클릭으로 빠르고 쉬운 시스템 마이그레이션 보장
- RTO 감소
- 값비싼 다운타임 최소화



## 엔드포인트 장치의 완벽한 보안

사이버 보호 및 관리

# 크게 확장된 안티맬웨어 기능

## 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

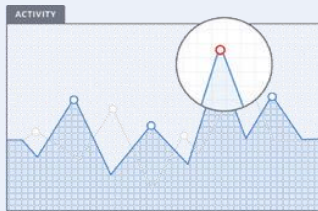
온액세스  
감지

Windows 보안 센터와 기본적으로 통합

**이유** 공격 후 복구뿐 아니라 다운타임 및 데이터 손실을 적극적으로 방지

# 랜섬웨어 보호 (Active Protection)

## Acronis Active Protection



- 아크로니스 로컬/클라우드
- 데이터베이스 명단에 의한 검출

휴리스틱엔진을 기반으로 동작 패턴 탐지

- 감지 - 악성 프로세스에 대한 경보를 생성
- 차단 - 악성 프로세스를 중지
- 복원 - 캐시를 사용하여 변경 사항을 복원

랜섬웨어 공격에서 백업 파일의 자체 보호

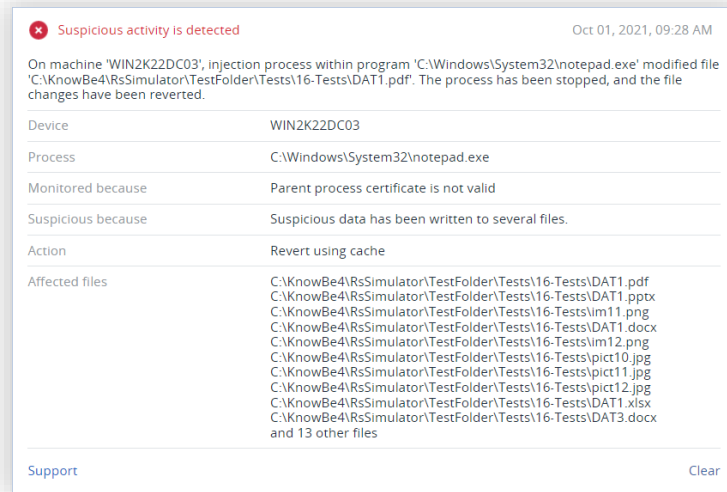
- 각 백업 대상 장비별 설정 가능
- NFS 및 CIFS(SMB) 네트워크 공유 보호
- 외장 하드 및 USB 보호



# 아크로니스 정적 AI 분석기

## 위협이 실행되기 전에 포착하는 차세대 정적 분석

- Windows 실행 파일(exe) 및 동적 링크 라이브러리(DLL)를 검사하여 실행 전에 악성 프로세스 여부를 확인합니다.
- 머신 러닝 모델 - 샌드박스 및 기타 보안 도구를 통해 Acronis Cloud Brain에서 수백만 개의 악성 파일과 깨끗한 파일에 대해 교육
- 맬웨어에 대한 사전 보호 계층
- 지속적인 개선(매시간 새 모델을 교육)

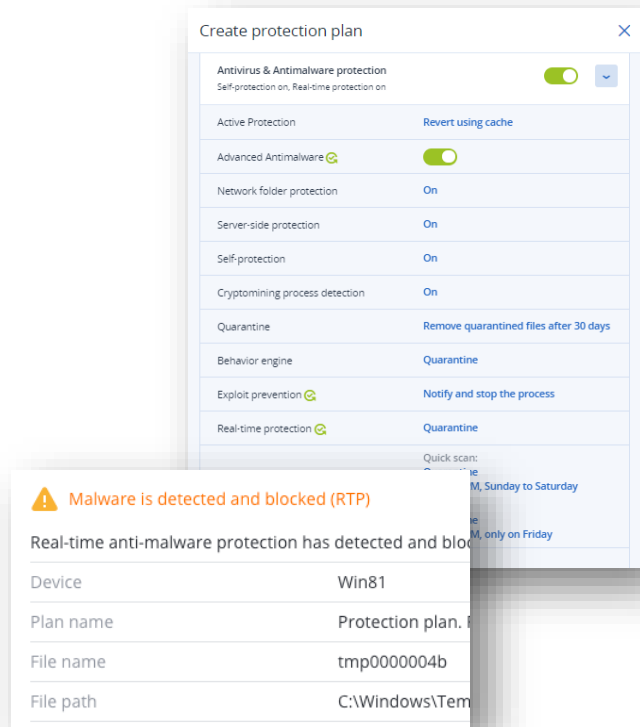


**이유** 실행 없이 트리거되는 맬웨어 감지

# 시그니처 기반 감지

## 더 빠르고 더 효율적인 감지

- 더 빠른 감지를 위한 AI 및 행동 기반 감지
- 향상된 로컬 서명 기반 감지(Advanced Security):
- 감지율 개선
- 감지 속도 개선
- 인터넷 연결이 열악한 경우에도 로컬 감지



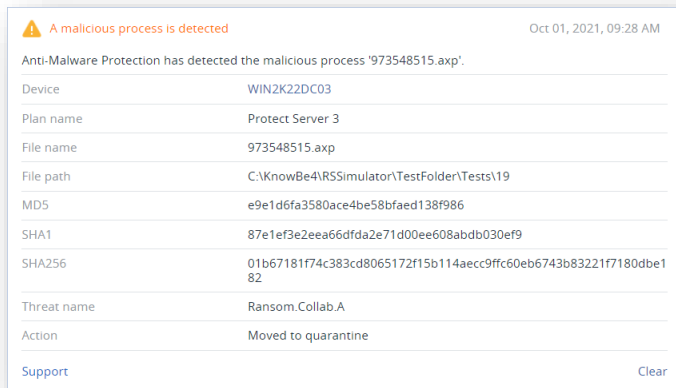
**이유** 보호 속도와 품질 개선으로 즉시 찾아낼 수 있는 맬웨어의 수를 늘림

# 행동 기반 감지

## 정교한 위협을 포착하기 위한 강력한 행동 휴리스틱스

의심스러운 커널 수준 이벤트와 Windows OS에서 발생하는 이벤트 전체를 분석하여 감지 회피 동작이 있는 악성 공격을 감지

- 파일리스, 메모리 및 스크립트 기반 공격(APT 침입의 일부)을 효과적으로 처리
- 동적 감지 규칙 - 다형성 및 난독화된 맬웨어 포착
- 파일 암호화를 위해 symlink를 사용하는 새로운 맬웨어 기법 (예: RIPlace)은 가장 경쟁력 있는 기술을 통해 감지 회피
- 알려지지 않은, 새로운, 진화한 위협을 효과적으로 감지



A screenshot of a Windows Security notification. At the top, it says "A malicious process is detected" with a yellow warning icon. The notification text states: "Anti-Malware Protection has detected the malicious process '973548515.axp'." Below this is a table with details of the detected process. At the bottom left is a "Support" link and at the bottom right is a "Clear" button.

|             |                                                                  |
|-------------|------------------------------------------------------------------|
| Device      | WIN2K22DC03                                                      |
| Plan name   | Protect Server 3                                                 |
| File name   | 973548515.axp                                                    |
| File path   | C:\KnowBe4\RSSimulator\TestFolder\Tests\19                       |
| MD5         | e9e1d6fa3580ace4be58bfaed138f986                                 |
| SHA1        | 87e1ef3e2eea66dfda2e71d00ee608abdb030ef9                         |
| SHA256      | 01b67181f74c383cd8065172f15b114aecc9ffc60eb6743b83221f7180dbe182 |
| Threat name | Ransom.Collab.A                                                  |
| Action      | Moved to quarantine                                              |

**이유** 감지 회피 동작을 사용하는 정교한 공격 방지

# Acronis Cyber Protect Cloud

#CyberFit

## 어드밴스드 시큐리티 + 엔드포인트 탐지 및 대응(EDR)

엔드포인트 보안을 간소화하면서도  
더 강력하게 제공하고자 하는  
서비스 업체를 위해 만들어졌습니다.

1

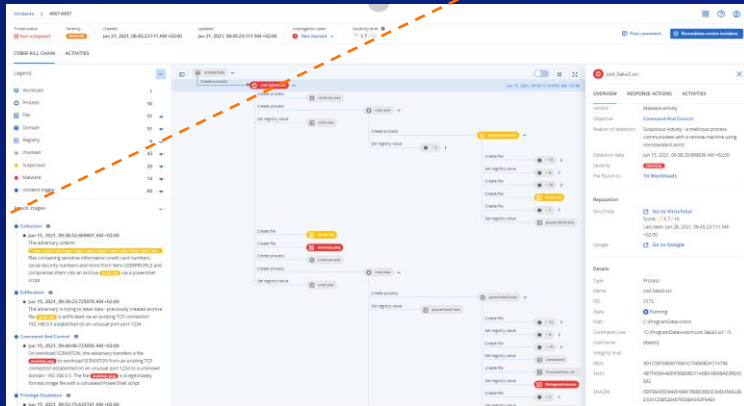
공격 단계 별로 진행 되는 쉽고  
편한 보안 사고 분석

2

다양한 대응 방안을 통한 비즈니스  
연속성 확보

3

디플로이, 관리, 확장이 간편한 통합  
플랫폼 및 에이전트로 손쉽게  
서비스 시작



### Attack stages

#### Collection

- Jun 15, 2021, 09:38:52:669601 AM +02:00  
The adversary collects  
files containing sensitive information credit card numbers, social security numbers and more from %env:USERPROFILE% and compresses them into an archive **draft.zip** via a powershell script

#### Exfiltration

- Jun 15, 2021, 09:39:23:725078 AM +02:00  
The adversary is trying to steal data - previously created archive file **draft.zip** is exfiltrated via an existing TCP connection 192.168.0.5 established on an unusual port port:1234

#### Command And Control

- Jun 15, 2021, 09:40:06:723056 AM +02:00  
On workload SCRANTON, the adversary transfers a file: **monkey.png** to workload SCRANTON from an existing TCP connection established on an unusual port 1234 to an unknown domain: 192.168.0.5. The file **monkey.png** is a legitimately formed image file with a concealed PowerShell script

#### Privilege Escalation

- Jun 15, 2021, 09:52:15:633741 AM +02:00  
To obtain higher-level privileges, the adversary is making registry modification to a known Microsoft process **control.exe** using a powershell command. User Account Control (UAC) is bypassed by starting a system Microsoft process **control.exe** that in return is spawning a child process **powershell.exe** with elevated privileges

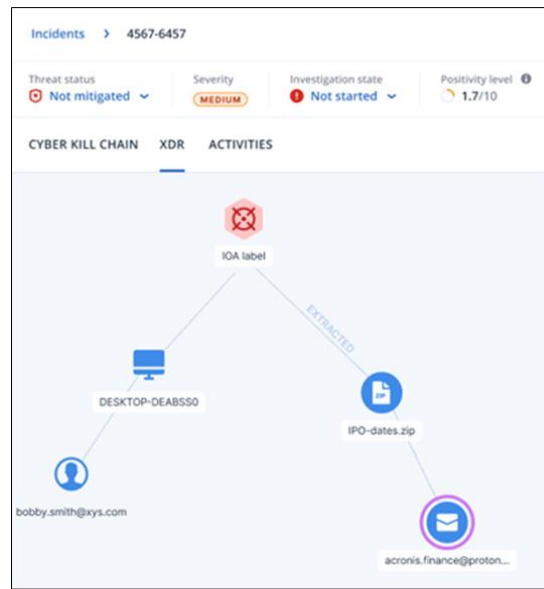
# Extended Detection and Response (XDR)

## Value for partners

보안 서비스를 제공하는 MSP는 불충분하고  
불완전한 보호 또는 비용이 많이 들고 복잡한 솔루션. XDR은 다음을 제공하여 이  
문제를 해결합니다.

MSP를 위해 특별히 제작된 완벽하고 기본적으로 통합되는 매우 효율적인 솔루션.

- 엔드포인트, 이메일, Entra ID 및 M365 애플리케이션(SharePoint, OneDrive, Teams)을 포괄하는 광범위한 가시성을 통해 취약한 공격 표면 전반에서 **클라이언트 환경에 대한 보호를 확장하여** 정교한 위협 환경으로부터 보호합니다.
- 사이버 보안, 데이터 보호 및 엔드포인트 관리 전반에 걸쳐 **기본적으로 통합**됩니다. XDR은 탁월한 비즈니스 연속성을 위해 취약한 공격 표면을 보호하도록 설계되었습니다.
- **고효율**, 보안 서비스를 쉽게 시작, 관리, 확장 및 제공할 수 있습니다. 또한 XDR에는 AI 기반 인시던트 분석 및 원클릭 응답이 포함되어 있어 쉽게 조사할 수 있습니다.
- **MSP를 위한 설계**, 모든 서비스를 위한 단일 에이전트와 콘솔, 그리고 추가 도구를 기술 스택에 통합할 수 있는 사용자 지정 가능한 플랫폼이 포함되어 있습니다.



# 독립적인 보안 테스트: 2020년에 시작됨

- Virus Bulletin에서 Endpoint Anti-Malware 솔루션으로 승인  
VB100 인증, 100% 탐지율, 2020년 6월부터 최신까지(2개월  
에 한 번) 오경보 제로
- AV-Comparatives는 Acronis Cyber Protect  
를 2020년 7월과 12월, 2021년 6월과 10월에 승인된 비즈  
니스 보안으로, 2021년 11월에는 ATP Enterprise 인증으로  
선정했습니다.
- ICSA 연구소는 2020년 7월부터 2023년 연구소 폐쇄까지(월  
간) 제품을 Endpoint Anti-Malware로 인증했습니다.
- OPSWAT 골드 및 플래티넘 인증, 2021년 3월/7월 이후



Products were allowed to download updates during the course of the test. The ver  
refer to those at the start of the test.

#### Acronis Cyber Protect

|                     |            |
|---------------------|------------|
| Windows 7 version   | 12.5.23140 |
| Windows 10 version  | 12.5.23140 |
| WildList detection  | 100.0%     |
| False positive rate | 0.000%     |
| Diversity Test rate | 100.00%    |



#### Acronis True Image 2021

|                     |             |
|---------------------|-------------|
| Windows 7 version   | Build 30480 |
| Windows 10 version  | Build 30480 |
| WildList detection  | 99.9%       |
| False positive rate | 0.000%      |
| Diversity Test rate | 100.00%     |



*Certified*  
Since July 2020

| ICSA Labs                  |                 |               |
|----------------------------|-----------------|---------------|
| "Collection 2020" Test Set |                 |               |
| Detected<br>44,717         | Total<br>44,725 | Eff<br>99.98% |

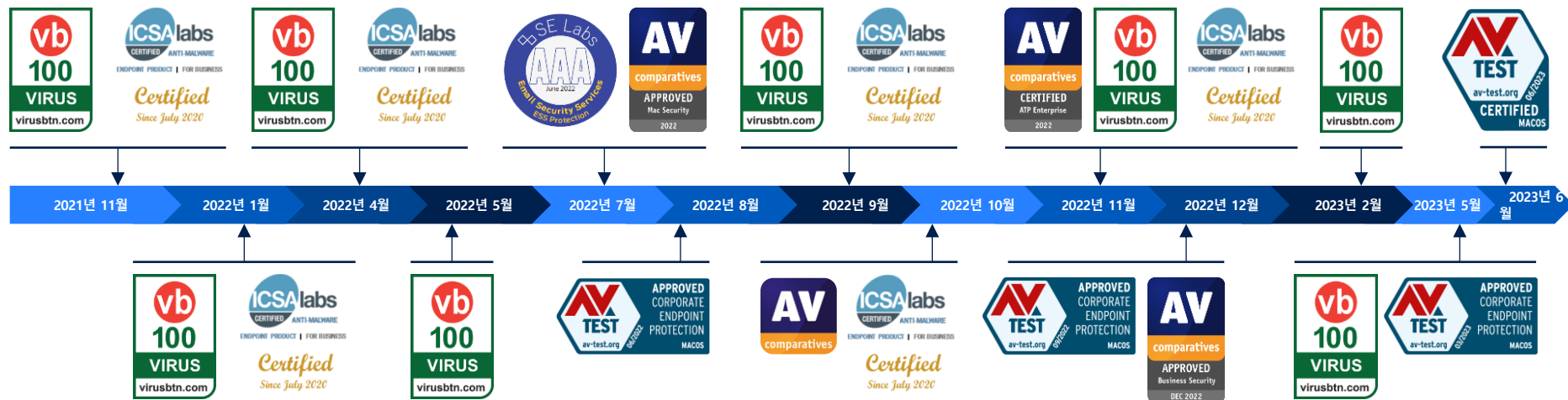
| False Positive Testing |
|------------------------|
| 0 False Positives      |



In their final analysis of Acronis True Image 2021, AV-TEST noted that "These results would definitely be enough to get certified and reach a high score in the official AV-TEST certification test."

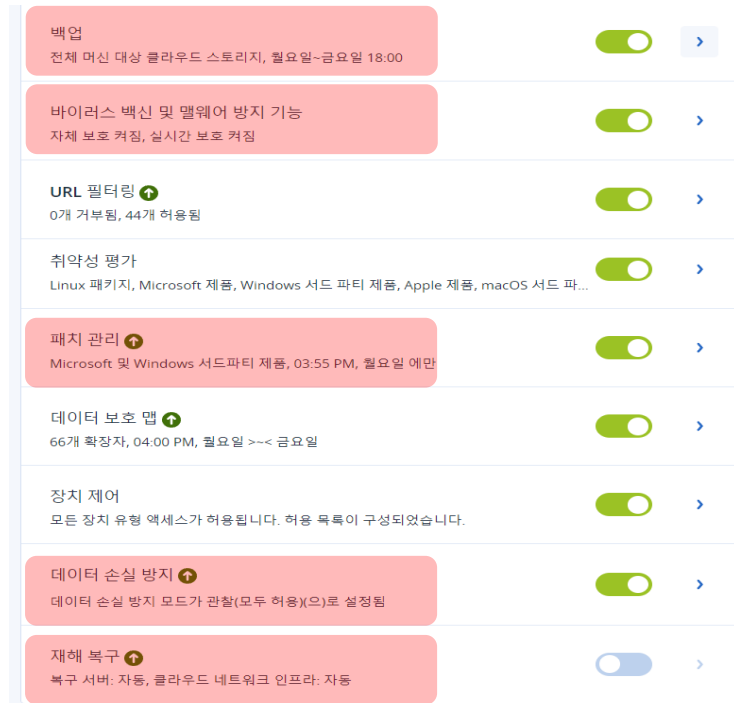


# VB100, ICSA Labs, AV-Comparatives 평가로 입증



# 단일로 제공하는 통합

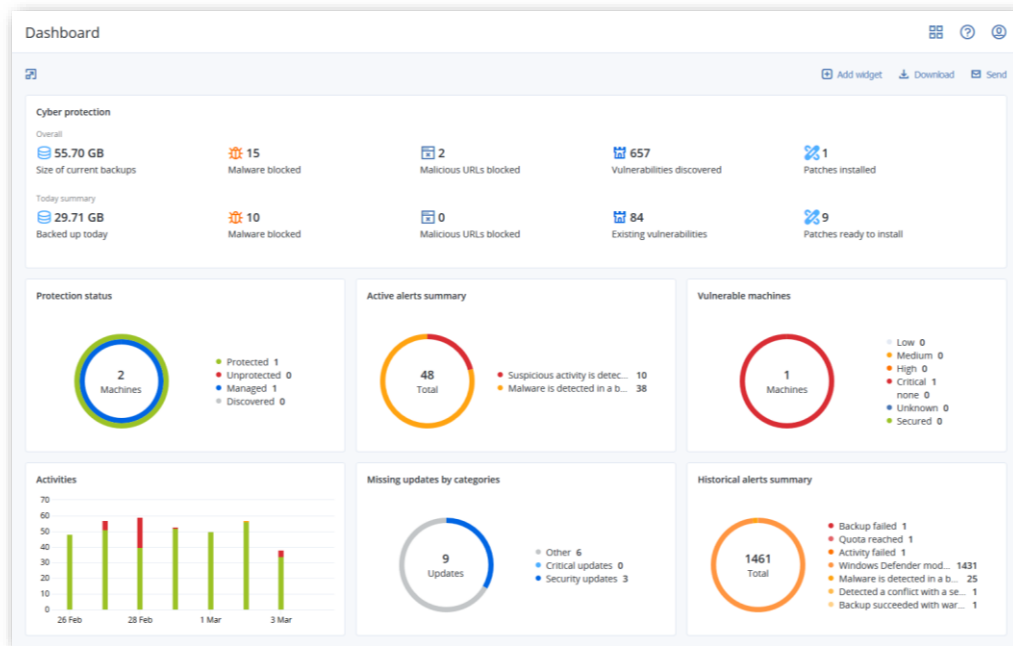
- 단일 UI, 정책 : 관리의 용이, 간단한 사용
- 단일 에이전트 : 설치의 용이, 충돌 우려 없음
- 단일 라이선스 : 비용의 감소
- 단일 공급업체 : 신속하고 효율적인 서포트
- 버튼 형태로 간단하게 ON/OFF



이유 더 적은 노력과 자동화로 더 나은 보호 제공

# 유연한 모니터링 및 보고

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

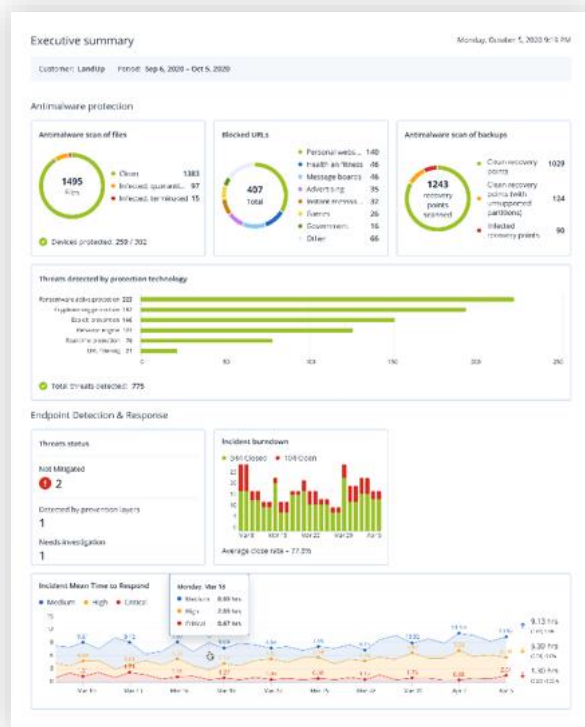


**이유** 단일 창, 더 빠른 운영, MSP 가치 입증 지원 및 갱신 간소화

# 알아서 보고서 작성까지

## 매달 또는 매주 만들어지는 리포트를 이용한 고객 소통

- 엑셀 및 PDF 형태로 다운로드
- 사용자 정의 형태의 리포트 항목
- 자동/수동 리포트 전달
- 리포트 주기 설정

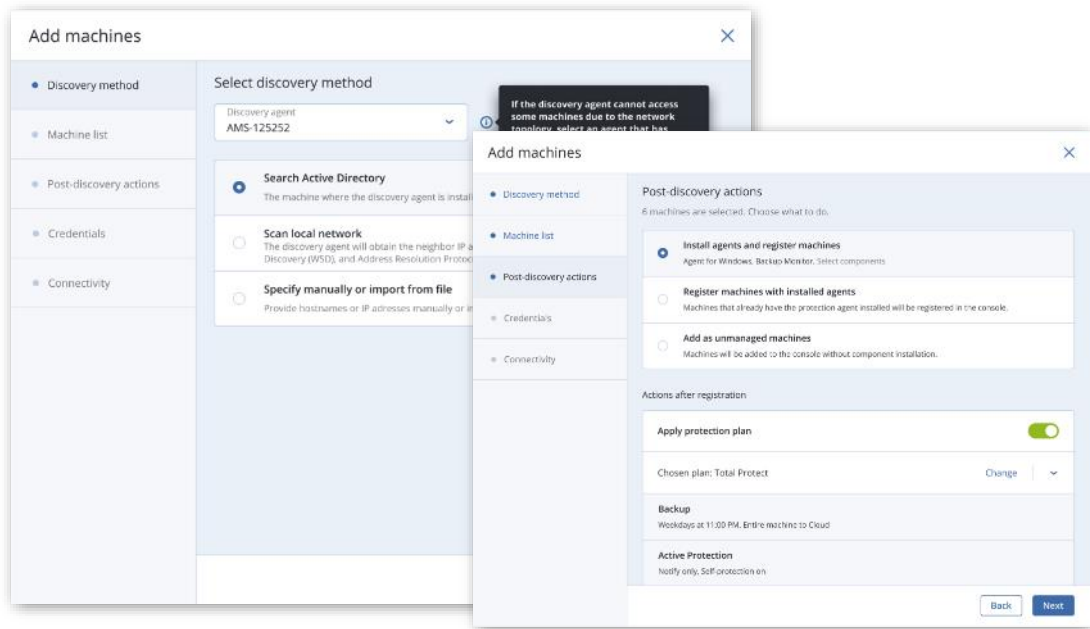


**이유** 시스템의 중요 지표들을 손쉽게 생성 및 전달

# 장치 자동 검색 및 원격 에이전트 설치

클라우드 및 온-프레미스 모두에서 한 번에 여러 에이전트를 설치하는 프로세스 간소화

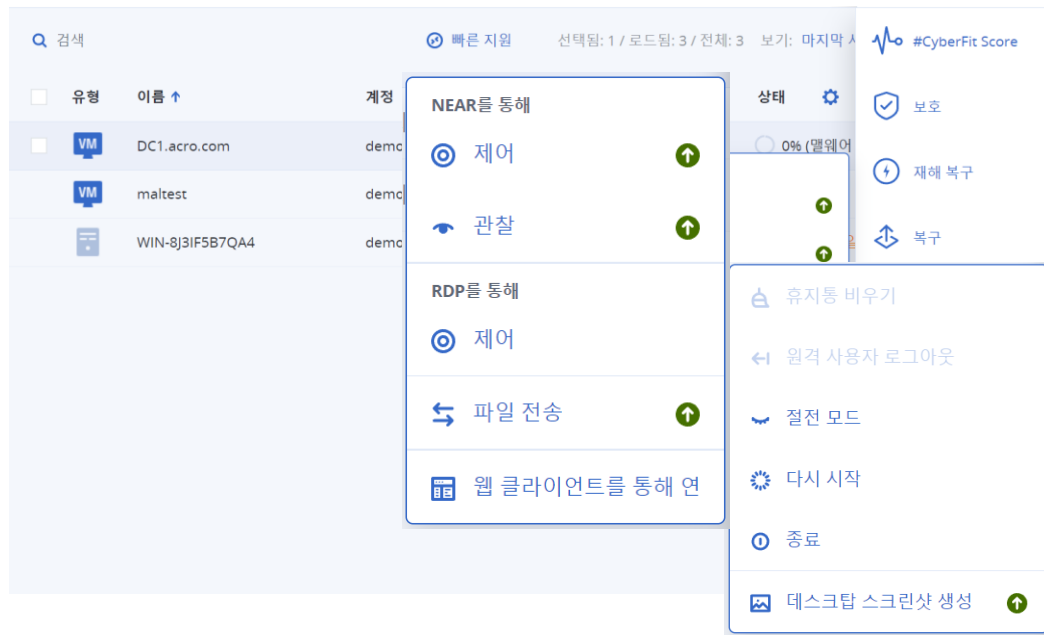
- 네트워크 기반 검색
- Active Directory 기반 검색
- 파일에서 컴퓨터 목록 가져오기
- 보호 계획 자동 적용
- 검색 마법사를 사용하여 일괄 원격 에이전트 설치



이유 더 쉽고 빠른 온보딩. 더 적은 리소스 필요. 완벽한 보호.

# 원격 데스크톱 및 원격 지원

- HTML5 연결 — 브라우저를 통해 원격 제어 가능
- RDP 연결 — 기존의 RDP 기능
- NEAR 연결 — 아크로니스 고유 기술, 양 방향 AES 암호화 통신 지원
- 파일 전송 — GUI 기반 파일 전송 클라이언트
- 휴지통 비우기, 절전모드, 다시 시작, 종료 기능 제공



**장점** 통합 도구로 원격 지원 및 시스템 관리 간소화

# Acronis

#CyberFit

## WHY Acronis ?

# 통합 보안 및 관리 기능을 갖춘 토탈 솔루션

## 데이터 보호



- 운영체제 및 Application 백업
- 재해복구(Disaster Recovery)

## 보안



- 바이러스 백신 + 멀웨어 방지
- DLP (Data Loss Prevention)
- EDR (Endpoint Detection and Response)

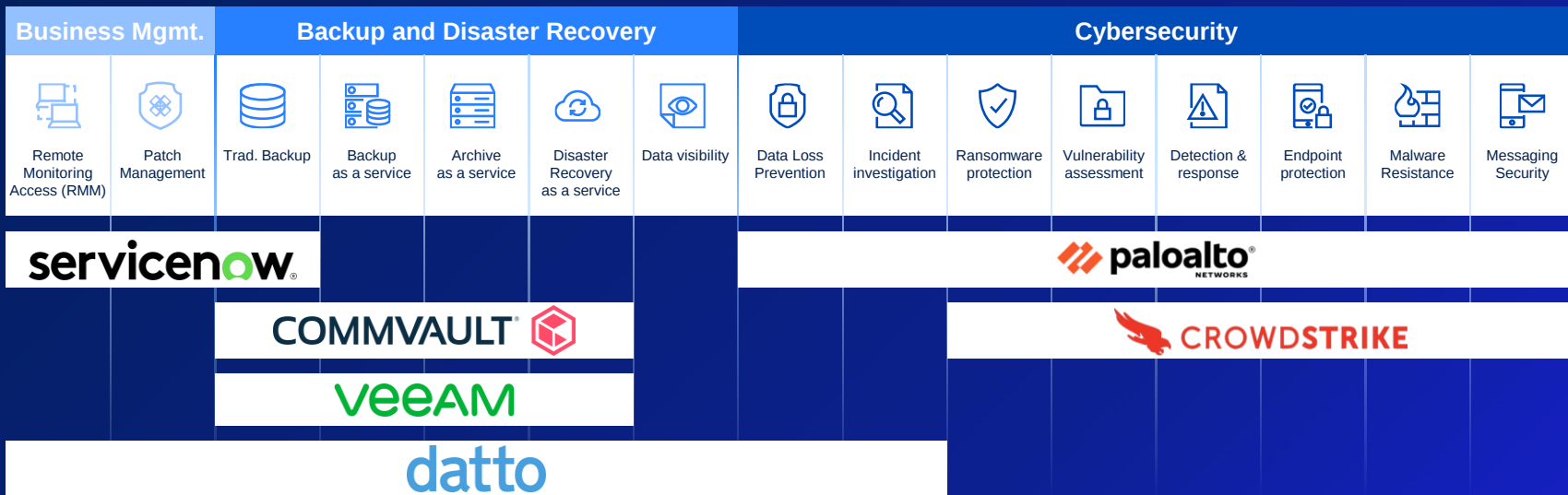
## 관리



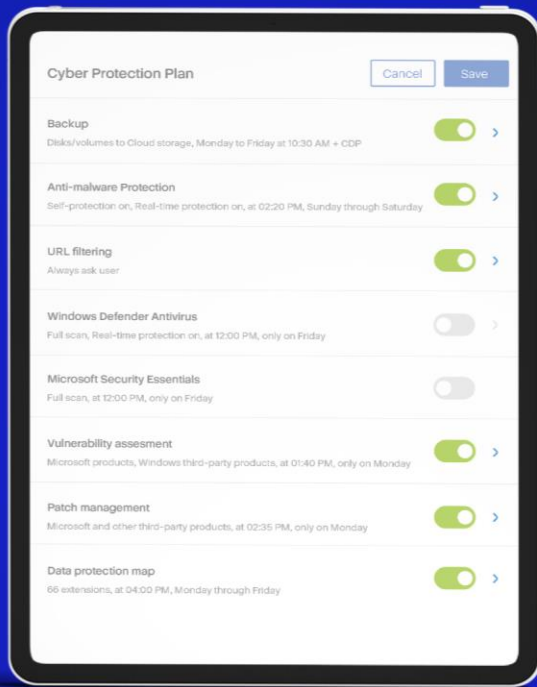
- 패치 관리
- 고객사 자산 관리
- 원격접속 및 제어

# 동종 업계 중 가장 폭넓은 통합 기능을 제공

# A



# ...그것도 너무나 간편한 인터페이스로 제공합니다.



# Acronis

#CyberFit

## 구축 사례

# Acronis Cyber Protect Cloud 구축 모델

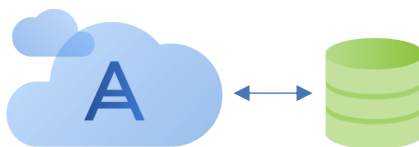
## Acronis-hosted



Acronis Cloud 스토리지가 포함된  
턴키 SaaS 솔루션

- No Cloud Infra
- Acronis Cyber Cloud 포털로  
모든 기능 사용

## Hybrid



자체 Cloud 스토리지에  
대한 활용

- Acronis 파트너가 운영하는  
Cloud 스토리지 활용
- Acronis Cyber Cloud 포털로  
스토리지를 제외한 모든 기능

## SP-hosted (on-premise 구축 모델)



서비스 제공업체 호스팅

- 서비스 제공업체가 운영하는  
Cloud 스토리지
- 서비스 제공업체에서 호스팅하는  
Acronis Cyber Cloud 시스템

# 국내 주요 고객사 및 판매 실적 (온프레미스 중심)

국내 4,000여 기업, 교육 및 공공 고객의 시스템 백업 환경에 대한 구축 경험을 가지고 있고,  
대형 전산 센터에서 제조설비라인 서버까지 검증된 사례를 바탕으로 안정된 백업 환경 구축 지원을 보장합니다.

| 제조                                                       | 공공                                                       | 금융                                                                                                   | 건설                                                                   | 기술                                                                               | 유통                                                           |
|----------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------|
| <br><br><br><br><br><br><br><br><br><br><br><br><br><br> | <br><br><br><br><br><br><br><br><br><br><br><br><br><br> | <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br> | <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br> | <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br> | <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br> |

# 국내 주요 고객사 및 판매 실적 (온프레미스 중심)

국내 4,000여 기업, 교육 및 공공 고객의 시스템 백업 환경에 대한 구축 경험을 가지고 있고,  
대형 전산 센터에서 제조설비라인 서버까지 검증된 사례를 바탕으로 안정된 백업 환경 구축 지원을 보장합니다.

## 서버 및 가상화 통합 관리

### 삼성그룹사

- 전자, 디스플레이, 전기, 병원, SDS, SDI, 제일모직

### LG그룹사

- 전자, 디스플레이, LGU+, 이노텍, 하우스시스, CNS

### SK텔레콤

### SK C&C

### GS건설

### LS산전

현대자동차, 현대오트모버

현대중공업

현대모비스

현대산업개발

롯데백화점

한국암웨이

포스코

한진중공업

대림산업

### KDB산업은행

KDB캐피탈

KB은행

신한은행

SC은행

전북은행

KEB하나은행

우리카드

신한카드

KEB하나카드

현대카드/캐피탈

삼성화재

동부화재보험

라이나생명

푸르덴셜생명

KRX한국거래소

KB투자증권

하나대투증권

한국스마트카드

### 국가정보자원관리원

국세청

관세청

조달청

헌법재판소

우정사업본부

교육과학기술부

대통령기록관

국회도서관

국회사무처

서울특별시청

한국방송공사

한국수자원공사

인천국제공항공사

한국가스공사

한국수력원자력

한국교육학술정보원

강원랜드

## 데스크탑 통합 관리

### 한국수출입은행

메리츠화재

현대해상화재

한국투자증권

현대하이캐피탈

현대자동차손해사정

더케이손해보험

메리츠종합금융증권

삼우종합건축사무소

포스코 A&C

만도헬라일렉트로닉스

롯데리아

한국철도공사(코레일)

농어촌공사

대검찰청

한국수력원자력

정보통신정책연구원

양천구청

성균관대삼성병원

# 아크로니스 클라우드 국내 주요 도입 기관

## 공공/금융



국민건강보험공단  
담배인삼공사  
한국정보통신기술협회  
한국의약품수출입협회  
약학정보원

## 제조/유통



GS 칼텍스  
아모레퍼시픽  
LB Smicon  
슈프리마  
삼천리  
바디프렌드  
우남건설  
태영산업  
골든듀  
범한산업  
미주제강  
캐논코리아  
코리아로지스

## 인터넷/통신



메가존  
카페24  
디딤365  
NHN  
가비아  
NETKTI  
후이즈  
아이네트호스팅  
콘텐츠브릿지  
하이파킹  
온라인투어  
영림원소프트랩

## 방송/교육/엔터



한국낚시채널  
창의와탐구  
선데이토즈  
샘터  
중부대학교  
건양사이버대학교  
대전외국인학교

## 헬스케어



이룸  
바이오녹스  
울산엘리아병원  
하늘병원  
동백성루카병원  
보아스이비인후과  
김승일 의원 외 병원 다수  
비트컴퓨터(전국 약국 체인)  
셀트리온 헬스케어

# Acronis Cyber Foundation Program

**Share the success of  
your growing  
business by helping  
others**



Get your free  
CSR in a Box  
training kit

