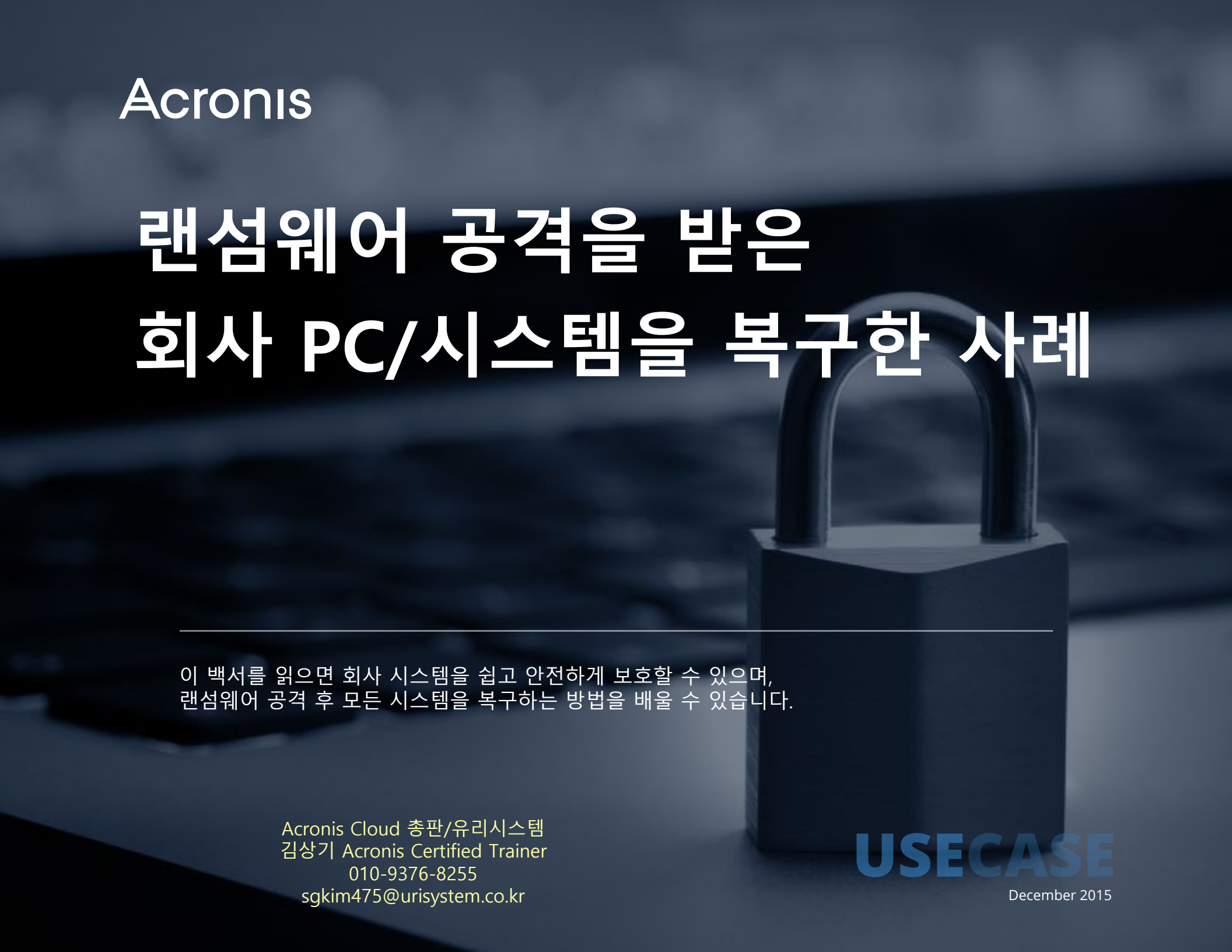

Acronis

# 랜섬웨어 공격을 받은 회사 PC/시스템을 복구한 사례

이 백서를 읽으면 회사 시스템을 쉽고 안전하게 보호할 수 있으며,
랜섬웨어 공격 후 모든 시스템을 복구하는 방법을 배울 수 있습니다.

Acronis Cloud 총판/유리시스템
김상기 Acronis Certified Trainer
010-9376-8255
sgkim475@urisystem.co.kr

USECASE

December 2015

# Introduction 소개

Data는 조직의 생명선입니다. 데이터를 분류하고 중앙집중화하려고 노력하는 것과는 상관없이, 귀사의 사용자들은 당신이 모르는 중요한 데이터를 항상 각자의 PC에  가지고 있습니다. 산업 분석가에 따르면, 회사의 중요한 데이터 중 최대 80%가 서버가 아닌 PC에 저장됩니다.

TrendMicro[1]  은 직원 중 56 %가 중요한 데이터를 노트북과 같은 개인용 장치에 자주 또는 자주 저장하는 것으로 나타났습니다. 이 회사 뿐만 아니라 거의 모든 회사에 적용되는 확실한 사실은 대부분의 CEO가 중요한 회사 문서를 회사 서버에 저장하지 않고 자기의 PC에 저장하며, 보호하지 않는다는 것입니다.

이제, 새로운 위협,Ransomware가 있습니다

Ransomware는 사용자가 몸값을 지불할 때까지 파일 및 시스템에 대한 액세스를 차단하는 악성 프로그램입니다.

Ransomware의 첫 사례는 13년 9월 5일에 발생했습니다. 이 사건에서는 해커가 암호 해독 키를 제공하는 대신 몸값을 지불하도록 요구하는 형태로 많은 시스템에 악영향을 끼쳤습니다.

2013 년의  4 개월 동안, 지불된 몸값은 3 천만 달러를 넘어 섰습니다.

2014 년 Zerolocker, Cryptowall 및 Sypeng이 가장 주목할만한 랜선웨어 사례가 있었습니다. 2015 년에 CTB-Locker는 추적 할 수없는 비트코인으로 몸값 지불을 요구하기 시작했습니다.

2015 년 2 월 McAfee Labs 위협 보고서에 따르면 매 분기마다 평균 155 %의 Ransomware 유형이 증가합니다.

Bromium[2] 조사에 따르면 ransomware는 230 가지 이상의 서로 다른 유형의 컴퓨터 파일을 대상으로 할 수 있으며 CEO의 파일이 이 목록에 포함되어 있습니다.

바이러스 백신 및 방화벽은 적절한 수준의 보호를 제공할 수 있습니다. 그러나 PC가 랜섬웨어의 영향을 받으면 거의 대부분의 경우에서 몸값을 지불하게 됩니다. 대가를 지불하지 않는 유일한 방법은  저장된 데이터의 백업 복사본을 만드는 것입니다. 예를 들어, USB 드라이브에 저장된 로컬 백업조차도 암호화되어 쓸모 없게 만들 수 있습니다.

다음 사례는 한 회사가 어떻게 회사 PC를 보호하고 랜스웨어 공격 이후에 모든 시스템을 복구했는지 설명합니다.

1. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/sb_5-reasons-why-small-business-lose-critical-data.pdf
2. http://www.bromium.com/company/press-releases/bromium-research-reveals-sophisticated-crypto-ransomware-menace.html

# Ransomware 고객 사례

**The Company's PCs (회사 PC)**

이 회사는 한 중앙 사무실에 150 명의 직원이 일하고 있습니다. 직원은 유선 및 무선 인프라를 통해 중앙 데이터 센터에 연결된 Windows® 기반 랩탑과 데스크톱을 혼합하여 사용했습니다.

이 회사는 중앙 집중식 스토리지, 문서 관리 시스템 및 수많은 비즈니스 응용 프로그램을 사용하지만, 최대 80 %의 PC에는 회사의 중앙 저장소에 복사되지 않은 중요한 회사 데이터를 각각의 PC에 가지고 있습니다.

**The Company's Backup Policy (회사의 백업정책)**

회사의 PC 백업 정책은 전사적 차원의 재해 복구 계획의 하위 정책의 하나입니다. PC백업 정책은 비즈니스 연속성 전략을 정의하고, IT 장비가 통신, 비즈니스 및 금융, 재무, 감사 및 규정 준수, 물류, 인력 등 모든 회사 운영을 지원해야한다는 내용으로 구성되어 있습니다.

IT 부서는 회사 데이터의 상당 부분이 직원 데스크탑 및 랩톱에 저장되어 있음을 인지하고 있었습니다. 이러한 이유로 회사는 모든 개인 컴퓨팅 장치를 회사의 백업 정책의 범위에 포함 시켰습니다.

**The Company's Backup Products (백업제품)**

이 회사는 Acronis® Backup Cloud를 사용하여 사용자의 PC를 보호합니다. 또한, 기본 데이터 센터에서 다른 플랫폼의 백업 및 복구를 지원하기 위해서 Acronis Backup Cloud를 사용합니다.

Acronis Any Data Engine으로 구동되는 Acronis Backup Cloud는 디스크 이미지 기술을 사용하여 Windows, Linux® 및 하이퍼 바이저 환경에 대한 빠른 백업 및 복구 기능을 제공하여 운영 체제, 응용 프로그램, 구성 및 데이터가 포함한 시스템의 전체 이미지를 저장합니다.

Acronis AnyData Engine은 모든 Acronis 제품에 제공되는 원천기술로, 가상, 물리적, 클라우드 및 모바일 환경에서 데이터를 캡처, 저장, 복구, 제어 및 액세스 할 수 있습니다. 각 제품은 특정 작업 부하에 최적화되어 있지만 전체 솔루션과 완벽하게 조화를 이룹니다. 동일한 통합 콘솔을 사용하여 각 제품을 구성, 설치 및 유지 관리합니다.

회사는 Acronis Backup Cloud를 사용하여 여러 시스템을 보호합니다. 하나의 콘솔로 여러 시스템을 관리하는 Acronis Management Server (AMS)를 사용하여 전체 인프라에서 모든 데이터의 백업 및 복구를 관리합니다.

Acronis Backup Cloud를 사용하면 IT 팀이 랩톱 및 데스크톱을 손쉽게 백업하고 파일, 폴더 또는 전체 시스템을 복구 할 수 있습니다. 이 회사에서 제품을 사용하기 시작한 이후로 다음과 같은 작업을 수행할 수 있었습니다.

- 다운 타임을 줄이고 직원 생산성을 향상
- Acronis의 유연한 복구 옵션으로 재해 복구를 단순화하고 비즈니스 연속성을 보장됨
- 설치, 구성 및 관리가 쉬운 하나의 완벽한 솔루션으로 IT 운영을 간소화시킴.

- Acronis Backup Cloud를 사용하여 전체 데이터 센터를 보호.
- 콘솔에 장애가 발생해도 모든 PC (및 다른 모든 시스템)의 백업 및 복구가 여전히 완벽하게 작동하기 때문에, 단일 실패 지점을 제거가 가능.

**Backup Source Systems (백업 원본 시스템)**

Acronis AnyData Engine의 강력한 기능을 활용하는 Acronis Backup Cloud는 약 8TB의 비압축 데이터를 캡처하여 전체 시스템 백업을 실행합니다. 이 제품의 차등 및 증분 백업을 사용하면 변경 사항만 백업되므로 스토리지 공간을 최적화하는데 도움이 됩니다. 이 회사의 일일 평균 데이터 변경 비율은 약 1.5 %입니다. 일일 증분 백업은 120GB의 데이터를 캡처하고 ,주간으로는 600GB의 데이터를 캡처합니다.

**The Backup Storage Policy**
**(백업 저장소 정책)**

회사는 초기에 모든 시스템을 로컬 NAS 장치에 백업한 다음 백업을 Acronis Cloud에 복사합니다. IT 관리를 단순화하기 위해, Acronis Backup Cloud는 동일한 백업 계획에 백업 및 스테이징을 포함합니다.

이 하이브리드 백업 접근법은 Acronis의 권장 3-2-1 백업 전략이 반영되었습니다. 백업 데이터의 사본 한 부를 Off-site에 저장하여 두 가지 유형의 미디어에서 세 위치의 모든 데이터를 유지 관리합니다. (여기서 세 위치는 프로덕션 시스템, NAS의 백업 및 Acronis Cloud의 백업)

**하나의 PC에서 파일이 손실되거나 사용자가 소수의 파일만 잃어버린 경우, IT 부서에서는 로컬 백업 복사본에서 해당 파일을 복구 할 수 있습니다. 주요 이벤트가 발생하면 IT 부서는 Acronis Cloud에서 백업 복사본을 복원합니다.**

**The Backup Schedule (백업 스케줄)**

Acronis Backup Cloud는 회사의 요구에 맞는 GFS (Grandfather-Father-Son) 순환 구성표를 지원합니다. 이 기능을 사용하여 회사는 매월 모든 데이터의 전체 백업, 주간 차등 백업 및 일일 증분 백업을 실행하여 스토리지 요구 사항을 최소화하고 백업 시간을 단축 할 수 있습니다. 이 기능을 사용하여 이 회사는 매월 모든 데이터의 전체 백업, 주간 차등 백업 및 일일 증분 백업을 실행하여 스토리지 요구사항을 최소화하고 백업 시간을 단축 할 수 있습니다.

많은 직원들이 노트북을 집에 가지고 출장을 가기 때문에 IT는 업무 일 동안 랩톱을 백업합니다. 데스크톱 백업은 업무 시간 이후에 시작됩니다.

IT 팀은 각 개별 PC를 백업 할 정확한 시간을 정의 할 필요가 없습니다. Acronis Backup Advanced는 정의 된 기간 동안 개별 PC 백업 시간을 무작위로 자동 배포합니다.

IT 부서는 백업 윈도우에 대한 정전 기간을 정의 할 필요가 없습니다. Acronis는 스냅 샷 기술을 사용하므로 백업은 사용자에게 투명하며 비즈니스 운영에는 영향을 미치지 않습니다. Acronis의 디스크 이미징 기술은 파일이 열려 있어도 모든 데이터를 일관성있게 백업합니다.

성능이 낮은 시스템을 사용하는 사용자에게 미치는 영향을 줄이기 위해 IT는 백업 리소스 사용을 제한 할 수 있습니다.

# Ransomware 공격 및 복구일지

**랜섬웨어는 이 회사 내의 수많은 컴퓨터에 영향을 미쳤습니다. 그리고 이 회사의 IT부서는 복구 계획을 바로 실행했습니다. 다음은 이와 관련된 타임라인입니다.**

**Day 1**

10:30am
**랜섬웨어 공격이 시작됨.**
IT부서는 아직 공격사실을 인지하지 못함.

10:42am
**공격에 대한 첫번째 보고가 IT부서에게 전달됨. JU헬프데스크가 응답함.**
IT부서는 감염된 PC를 네트워크에서 단절시킴.

10:51am
**사용자들이 7개 더 많은 랜섬웨어 감염PC을 보고함.**
IT부서는 감염된 규모를 파악하고, 회사 네트워크를 차단함. 그리고 전사적인 점검을 시작

**전사점검을 완료.**
12:07pm
IT부서는 23대의 컴퓨터가 감염되었음을 확인.

**IT팀은 네트워크를 재시작함.**
12:18pm
IT팀은 모든 감염된 PC를 종료하고 LAN에서 차단시킴.

**IT팀은 Acronis Support Team에 연락.**
12:27pm
IT팀은 Acronis에게 감염된 23대의 PC에 대한 백업 데이터가 저장된 대규모 복구 하드디스크(HDD)를 보내도록 요청함.

**Acronis 가 복구용 HDD를 송부함.**
3:45pm
Acronis 지원팀은 23개 PC의 백업본(923GB)을 외장HDD에 복사한 후 야간 택배로 회사에 송부함.

**Day 2**

8:33am — **HDD가 회사에 도착.**

8:51am — **IT팀은 중앙 스토리지에 HDD를 복사함.**
IT팀은 병렬복구를 용이하도록 백업을 고성능 중앙 스토리지에 복사함.

9:05am — **첫번째 백업은 스토리지에 복사; 첫번째 PC복구가 시작됨.**
IT팀은 Acronis Bootable Media로 감염PC를 부팅함.
네트워크는 여전히 중단된 상태.

9:07am — **첫번째 부팅이 완료됨.**
Acronis Backup Cloud가 PC에 로드됨. IT팀이 테트워크에 연결시키고 복구 프로세스를 시작함.

9:53am — **첫번째 복구가 완료됨.**
첫번째 기계가 복원되고 재부팅됨

10:02am — **첫번째 PC가 복원됨.**
중앙스토리지로 백업의 복사본이 계속 복사함.

12:37pm — **모든 백업이  중앙 스토리지로 복사됨.**
15 기계가 복구됨.

2:29pm — **마지막 감염 PC가 복구됨.**
23대의 모든 기계가 복구됨. 랜섬웨어는 발견되지 않았습니다.

# Summary 요약

Ransomware은 상당수의 직원 PC에 영향을 주었지만 회사는 이에 준비되어 있었습니다.

IT 팀은 백업 소스 시스템, 백업 스토리지 정책, 백업 일정 및 백업 기간에 대한 세부 정보가 포함 된 PC 복구 계획을 기획 운영해 왔습니다. 관리 팀은 PC 복구 계획을 승인했으며 IT팀은 다양한 시나리오를 사용하여 정기적으로 시나리오 테스트를 진행했습니다.

복구 시나리오는 IT 엔지니어가 PC를 복구하고 사용자를 생산적인 상태로 복원하기 위해 취한 단계를 명확하게 제시합니다.

**Acronis Backup Cloud를 사용하여 IT 팀은 PC 복구 계획에 명시된 모든 시나리오 및 비즈니스 목표를 달성하고 28 시간 만에 모든 사용자에게 생산성을 복원했습니다.**

IT 팀은 PC뿐만 아니라, 기본 데이터 센터의 백업 및 복구를 지원하기 위해 Acronis Backup Cloud를 사용합니다.

- Windows 서버 : 이미지 및 / 또는 파일 기반 백업은 Windows Server 운영 체제를 실행하는 전체 시스템을 보호.
- VMware 및 Hyper-V 가상 호스트 : 에이전트없는 백업은 가상 Microsoft® Exchange, SQL Server®, SharePoint® 및 Active Directory®를 비롯한 VMware® 및 Hyper-V® 가상 시스템을 보호.
- Microsoft Exchange 서버 : 중요한 전자 메일 및 공동 작업 시스템을 보호하는 데이터베이스 및 사서함의 응용 프로그램 수준 백업
- Microsoft SQL Server : 응용 프로그램 인식 복원을 사용하여, 단일 데이터베이스 / 콘텐츠 데이터베이스부터 전체 시스템까지 Single pass 백업이 Microsoft SQL Server를 보호함.
- Microsoft SharePoint 팜 : 단일 경로 백업은 단일 데이터베이스 / 콘텐츠 데이터베이스에서 전체 서버로의 응용 프로그램 인식 복원을 사용하여 SharePoint 팜의 모든 서버 역할을 보호함.
- 
- Active Directory Domain Controller : 일관된 Single-pass 백업/복구로 도메인 컨트롤러, Active Directory 데이터베이스, 시스템 볼륨 및 로그를 보호함.
- Cloud Backup add-on: 전체 데이터 센터는 안전하고 확장 가능한 Off-site 클라우드 백업으로 보호됨. 초기 시딩 및 대규모 복구 프로그램을 사용하면 대용량 데이터를 쉽게 이동하고 네트워크 병목 현상을 피할 수 있슴.

Acronis Backup Cloud는시스템이 회사 내이던, 클라우드이던, 원격 오피스이던 관계없이 데이터를 보호하기 위해 백업, 베어메탈 복원 및 시스템 복구 등의 기능이 결합된 Acronis AnyData Engine을 기반으로 합니다. Acronis Backup Cloud를 사용하면 백업 및 재해 복구를 단순화하고 시스템을 복구하고 비즈니스를 다시 시작하고 실행하기위한 IT 시간과 노력을 크게 줄일 수 있습니다.

# Acronis Backup Cloud를 선택해야 하는 **5가지 이유**

1. **Quickly capture:** 특허받은 이미지 기반 백업을 사용하여 PC의 모든 것을 빠르게 캡처함.
2. **Restore**: 대규모 공격이나 재난이 발생하면 전체 시스템을 신속하게 복원.
3. **Recover:** 개별 파일, 폴더, 응용 프로그램 또는 전체 시스템을 모든 하드웨어 또는 가상 컴퓨터 (VM)로 복구.
4. **Ensure:** Acronis의 풍부한 기능으로 비즈니스 연속성 및 재해 복구 보호를 보장.
5. **Simplify:** 클라우드 및 중앙 집중식 데이터 보호 관리로 IT 관리를 간소화

# About Acronis

Acronis는 백업, 재해 복구 및 보안 액세스 솔루션을 통해 차세대 데이터 보호 표준을 주도하는 회사입니다. AnyData Engine에 기반을 둔 Acronis는 가상, 물리적, 클라우드 및 모바일과 같은 모든 환경에서 모든 파일, 애플리케이션 및 운영 체제를 쉽고 완벽하고 안전하게 백업합니다.

2002 년에 설립 된 Acronis는 130여 국가에서 5 백만 명이 넘는 소비자와 300,000 개의 기업의 데이터를 보호합니다. Acronis Computing, TechTarget 및 IT Professional이 선정한 100 개 이상의 특허를 통해 Acronis 제품은 여러 차례 '올해의 최고의 제품'으로 선정되었으며 마이그레이션, 복제 및 복제 등 다양한 기능을 제공합니다.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.

Acronis

**Acronis Cloud 총판/유리시스템**
**김상기 Acronis Certified Trainer**
**010-9376-8255**
**sgkim475@urisystem.co.kr**

**For additional information, please visit http://www.acronis.com**

To purchase products, please visit http://www.acronis.com or search online for an authorised reseller.
Acronis office details can be found at http://www.acronis.com/company/worldwide.html