GLUESYS

랜섬웨어 침해 예방 백업 솔루션

AnySecurity ZERO

㈜글루시스

AGENDA

제1장. 제안 개요

제2장. 솔루션 소개

제3장. 주요 기능

제4장. 구축 사이트

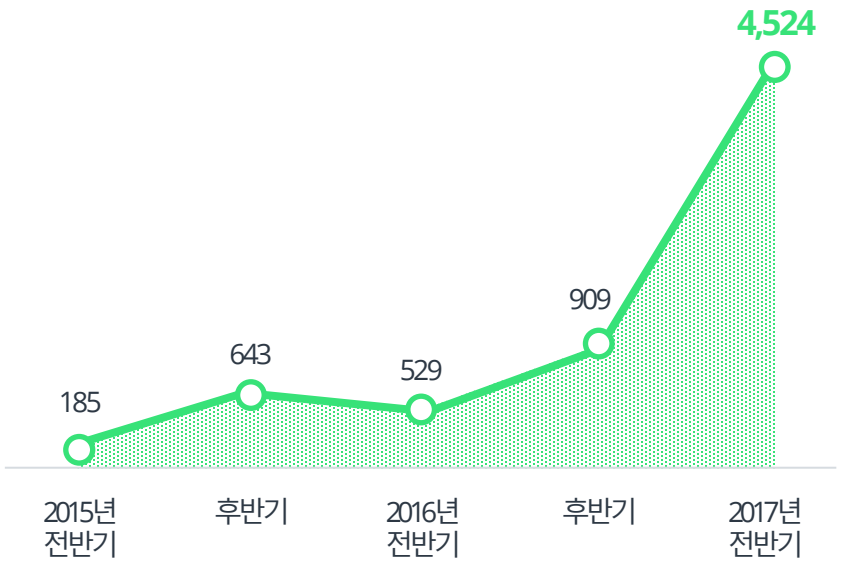
랜섬웨어 현황

신종, 변종 등 다양한 랜섬웨어의 확산으로 전 세계적인 피해 급증

전 세계 150여 개국 약 30만대의 PC를 감염시킨 워너크라이(WannaCry)를 포함, 2017년에만 3건의 대규모 공격

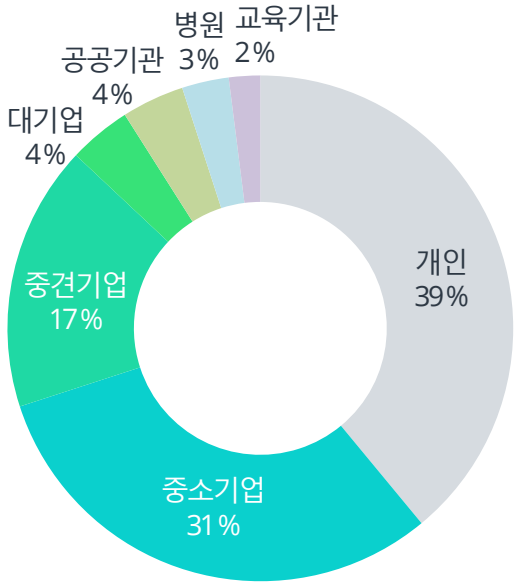
국내 랜섬웨어 피해 상담 현황

자료 : 과학기술정보통신부, 한국인터넷진흥원 (단위 : 건)



랜섬웨어 감염 업종 별 현황

자료 : 한국랜섬웨어침해대응센터



랜섬웨어 주요 피해 사례

2017년의 경우, 랜섬웨어 공격 대상의 26%가 기업 컴퓨터로, 이 중 65%는 데이터 전체 또는 상당량에 대한 액세스 권한 유실 대가를 지불한 기업 6곳 중 1곳이 데이터 복구에 실패

2017년 주요 랜섬웨어 사건

구분	워너크라이 (Wanna Cry)	'나야나' 사태 (에레보스 변종)	페트야 (Petya)
시기	2017년 4월	2017년 6월	2017년 6월
피해 대상	윈도우 OS 기반 PC	리눅스 OS 기반 서버	윈도우 OS 기반 PC
방식	윈도우 파일 공유에 사용되는 SMB 원격코드 취약점 악용	APT 공격으로 개인 정보 탈취 후 게이트웨이 서버, 웹 서버에 공격 거점 마련, 고객서버 랜섬웨어 감염	
암호화 대상	일반 문서 파일부터 압축파일, DB, 가상머신 파일 등	-	데이터 파일 포함 PC 부팅 불가능하도록 MBR(마스터 부트 레코드) 파일 감염
피해 규모	전 세계 150개국 컴퓨터 30만 대	고객서버 153대 감염 3,400여 개 업체 홈페이지 마비 해커에 13억 원 어치 비트코인 지급	유럽 국가 상당수 국내에는 피해사례 접수 없음
종합	자기 복제와 인터넷 연결만으로 감염	리눅스 타겟의 변종, APT 공격 결합	감염 시 부팅 자체 불가, 복구 불가

랜섬웨어 방어, 왜 힘든가?

최근 비트코인 등 가상화폐 가치 상승이 랜섬웨어의 급격한 증가 원인

랜섬웨어는 사후탐지(감염 후 탐지)를 통해 대처가 가능한 과거 악성코드와 달리 사후 탐지 무의미

無 잠복기

잠복기 없이
감염되는 즉시 악성 행위 발생

손쉬운 목적 달성

다른 악성코드와 달리
데이터 암호화 후 랜섬 요구하면 끝

감염 후 복구 불가

랜섬웨어 감염 시 데이터를 포기하거나
랜섬 지급 방법 밖에 없음

사전 차단과 데이터 백업 만이 유일한 대응 방안!

체계적인 대응 필요

진화하는 변종 랜섬웨어 및 예측 불가능한 공격에 대해 기존의 백신 및 보안 솔루션만으로 대응하기에는 한계 有
랜섬웨어 사전 탐지부터 안전한 데이터 백업까지 보다 효과적이고 체계적인 대응 방식 필요

단계 별 랜섬웨어 대응 방식

랜섬웨어 탐지

악성 행위 실시간 감시 및
패턴 분석

사전 차단

랜섬웨어 행위 차단 및 알림,
DB 등록

로컬 백업

사용자 파일 암호화 및
주기적인 백업

클라우드 백업

실시간 클라우드 백업 및
중앙 관리

애니시큐리티 제로(AnySecurity ZERO)

랜섬웨어 사전 차단과 중요 데이터 보호를 한번에!

랜섬웨어에 의한 암호화 행위 탐지 및 차단

사내 중요 문서 및 파일은 중앙 스토리지(클라우드)에 자동 백업하여 신속한 파일 복구 지원

랜섬웨어 사전 차단

- 행위 기반 랜섬웨어 탐지로 랜섬웨어 유입 및 파일 훼손 사전 차단
- 실시간 DB 매칭 감시로 랜섬웨어 유입 사전 차단 및 랜섬웨어 판단 시 프로세스 중지 후 파일 삭제

안전한 클라우드 백업

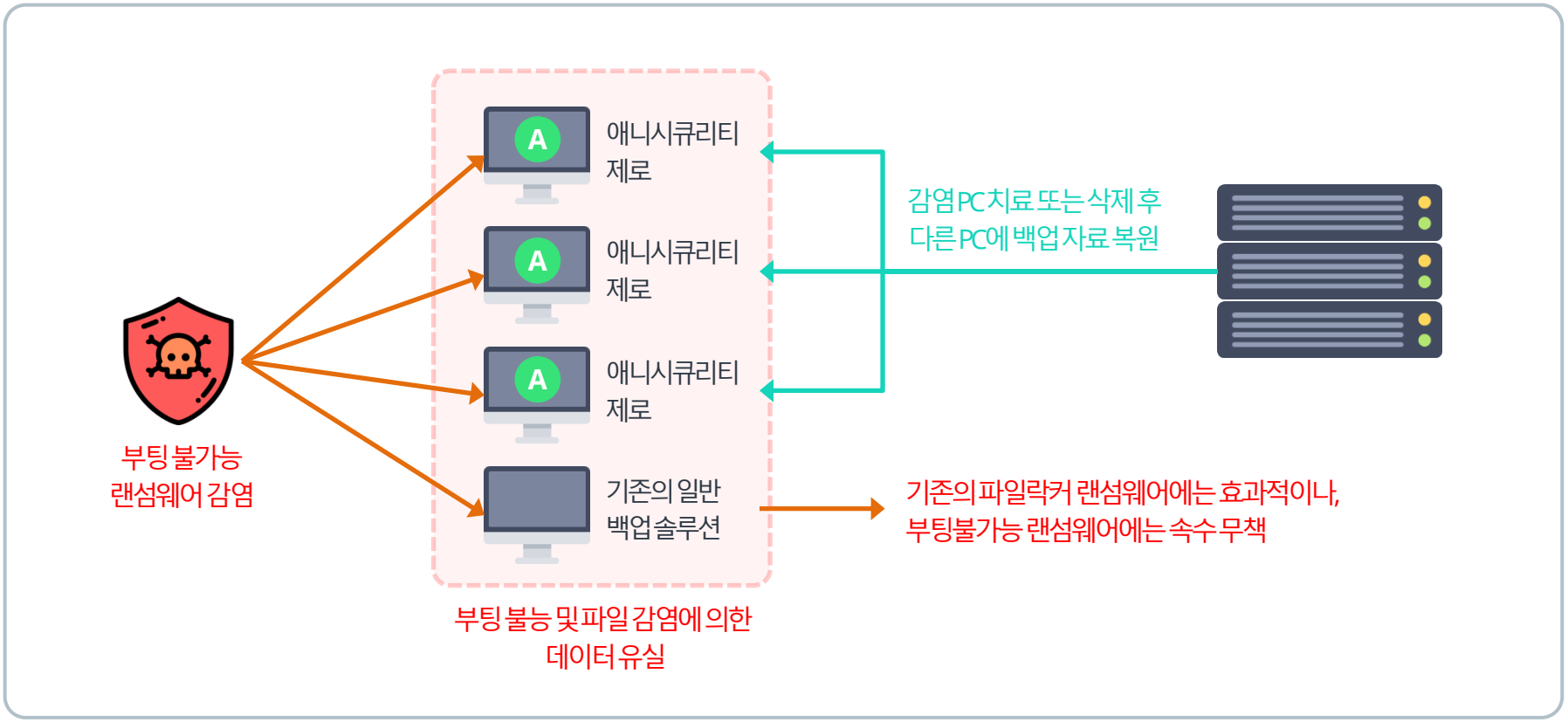
- 클라우드(중앙 스토리지)에 PC 중요 데이터 파일 자동 백업
- 데이터 암호화 백업을 통해 랜섬웨어에 의한 파일 변조 방지
- 특정 폴더 및 확장자 선택 백업 가능

신속한 파일 복구

- 마우스 우클릭 만으로 파일 복원 가능
- 복원 파일의 저장 경로 설정 및 복원 상태 확인 가능
- 저장 시점에 따라 버전 별로 관리되어, 원하는 시점의 파일 복원 가능

왜 클라우드 백업인가?

암호화된 백업 파일을 사용자의 PC가 아닌 클라우드 스토리지에 저장하므로,
사용자 PC가 랜섬웨어에 감염되어 파일 손상 및 부팅 불능이 되어도 안전한 데이터 보호 가능



주요 기능 및 장점

더욱 안전한 클라우드 백업

중요 데이터를 클라우드에 백업하여 랜섬웨어에 의한 파일 훼손 및 PC 부팅시스템 훼손에도 안전하게 보호할 수 있습니다.

랜섬웨어 감지 및 자동 차단

랜섬웨어 행위 분석 및 실시간 DB 매칭 감시를 통해 랜섬웨어를 자동 차단하여 파일 훼손을 사전에 방지합니다.

암호화로 더욱 강력한 백업

데이터를 암호화 시켜 클라우드에 백업함으로써, 랜섬웨어에 의한 파일 변조를 방지합니다.

외부 요인에 대한 데이터 보호

랜섬웨어에 의한 데이터 훼손 뿐 아니라 물리적 충격 및 기타 재해로 인한 PC 데이터 손실도 사전에 방지합니다.

업무 환경에 맞는 효율적인 백업

업무 환경에 맞게 실시간/스케줄 백업이 가능하며, 특정 폴더/확장자만 선택 백업할 수 있어 효율적으로 관리할 수 있습니다.

변경이력관리 히스토리 백업

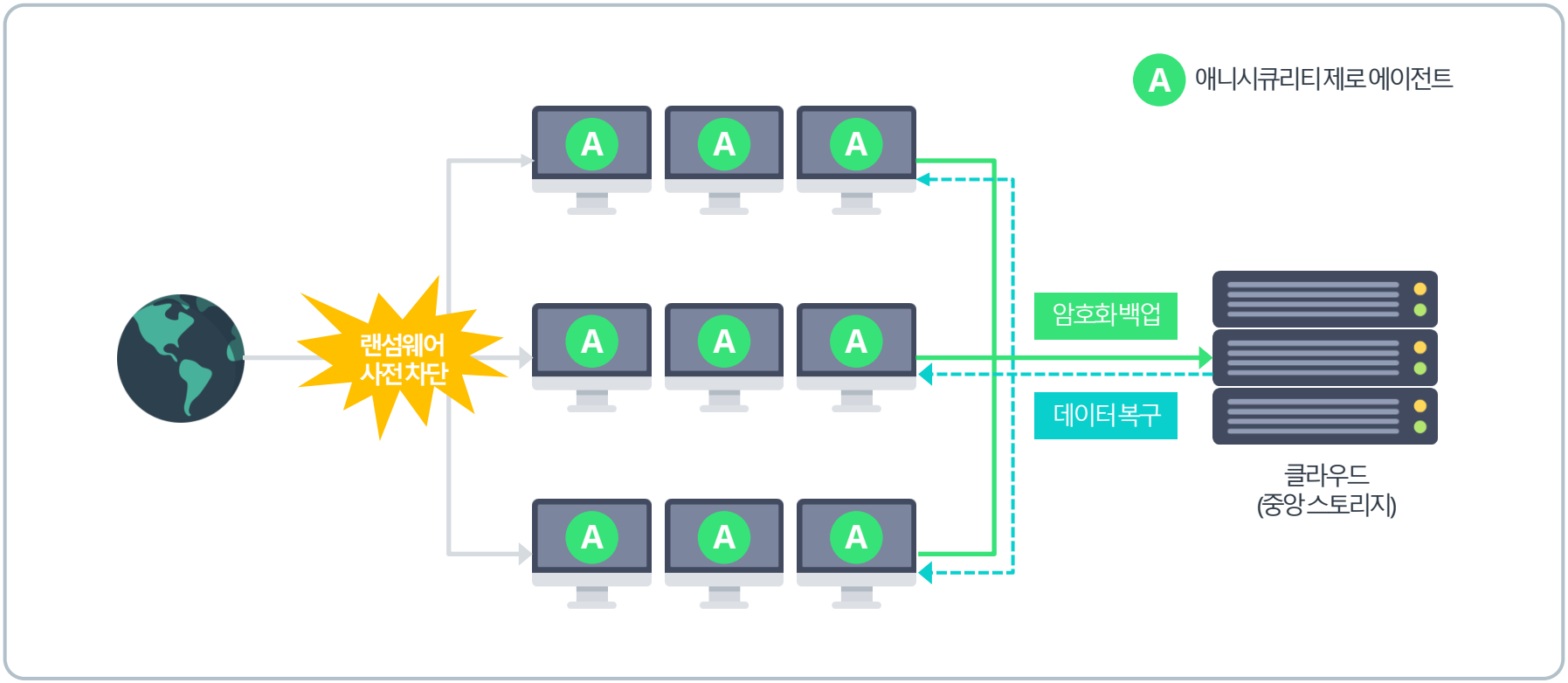
데이터가 여러 번 백업되어도 파일 버전별로 관리되므로, 데이터 유실/손상 시 특정 시점으로 복원이 가능합니다.

솔루션 구성도

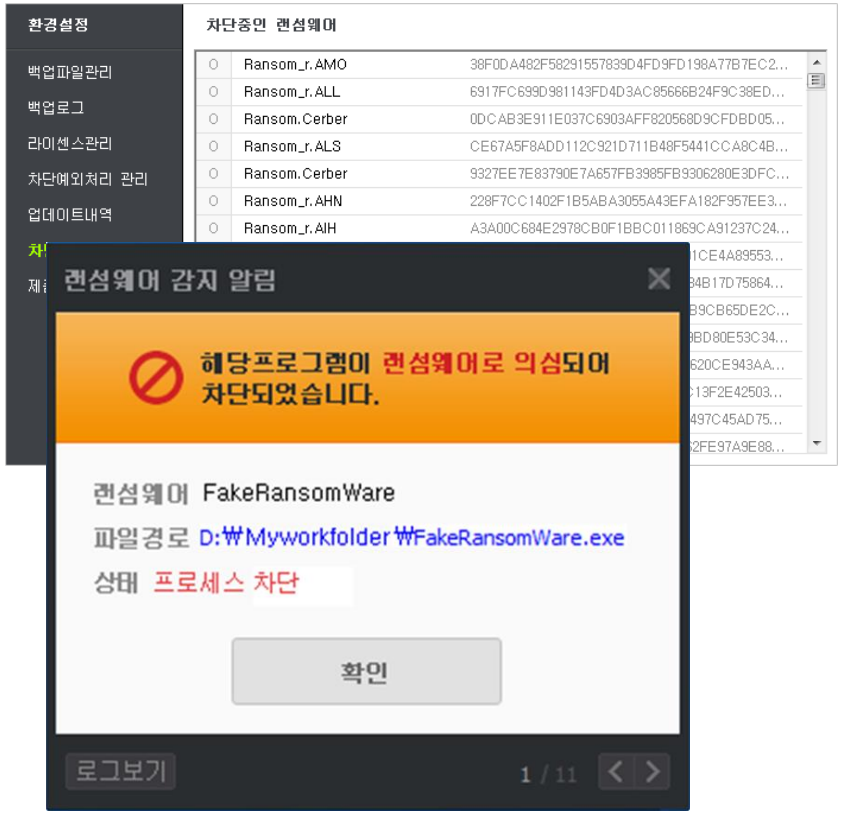
네트워크로 연결된 클라우드(중앙 스토리지)에 사내 PC의 백업 파일 자동 저장

개인 PC의 저장 공간 확보 및 파일 훼손, 삭제, 랜섬웨어에 의한 파일 변조에 더욱 안전

*** 백업 시에만 클라우드에 연결되기 때문에, 중앙 스토리지로 랜섬웨어가 유입될 확률이 타 제품에 비해 현저히 낮음**



랜섬웨어 사전 차단



행위 기반 랜섬웨어 탐지

- 랜섬웨어의 악성코드 행위가 탐지되면 랜섬웨어 자동 차단 및 알림 메시지 전송
- 랜섬웨어에 의한 암호화 행위 탐지 시 자동 차단을 통해 파일 훼손 방지

실시간 DB 매칭 감시

- 실시간으로 프로세스에서 실행되는 목록 자동 감시
- 자체 보유한 랜섬웨어 DB로 감지된 프로세스 해시값 검사
- 검사 결과 랜섬웨어로 판단되면 프로세스 중지 후 파일 삭제

* 랜섬웨어 DB는 지속적으로 업데이트됩니다.

안전한 클라우드 백업

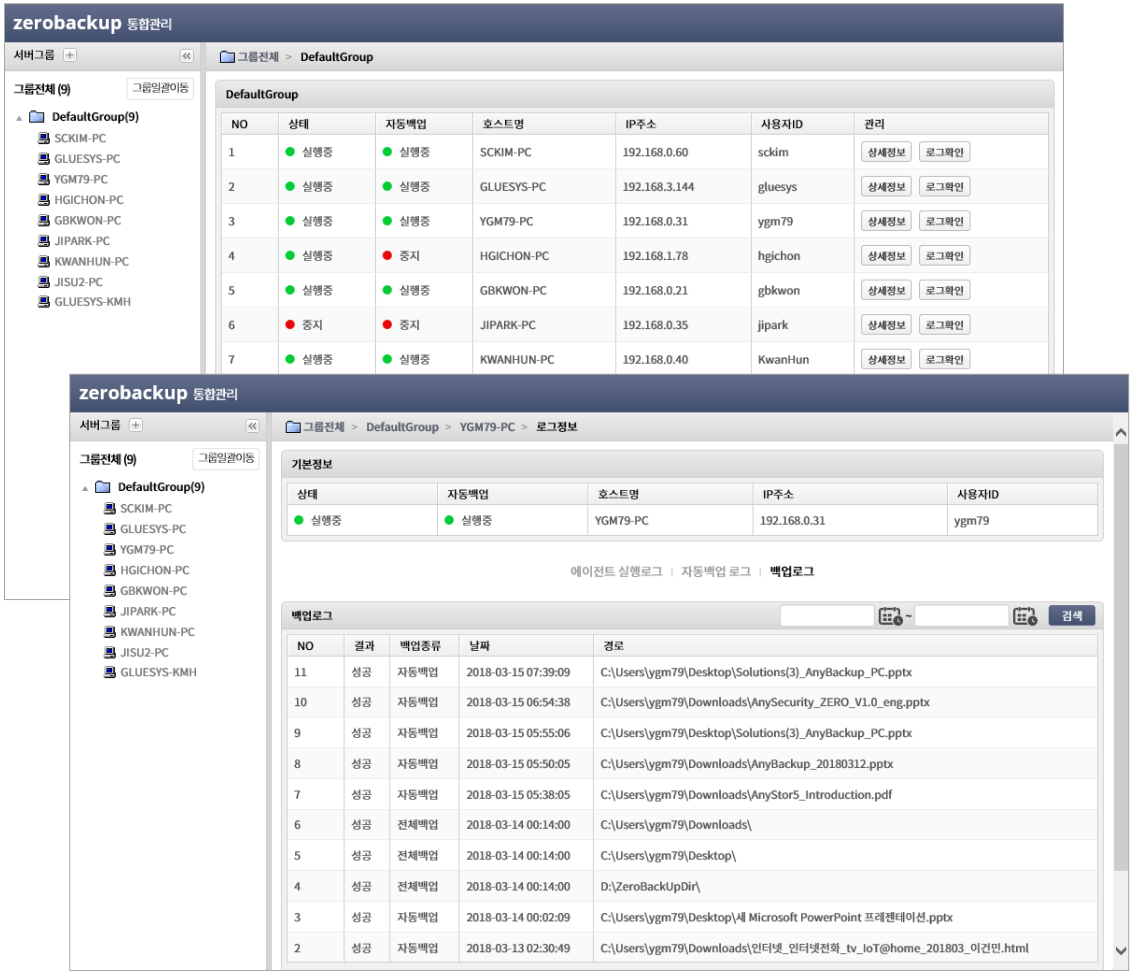
강력한 데이터 보호

- 사내 업무 PC의 중요 데이터를 클라우드에 자동 백업
- 백업 시 데이터를 암호화하여 랜섬웨어에 의한 파일 변조 방지
- 랜섬웨어 외 사용자 실수, 물리적 충격 및 기타 재해로 인한 PC 데이터 손실로 부터 데이터 보호
- 실시간 또는 스케줄 백업을 통해 효율적으로 백업
- 특정 폴더 및 확장자만 선택적으로 백업하여 백업 용량 관리
- 백업 시에만 클라우드로 연결되기 때문에, 중앙 스토리지에 랜섬웨어 유입 확률 낮음

신속한 데이터 복구

- 백업된 모든 파일의 신속한 복구 가능
- 복원 파일의 저장 경로 설정 및 복원 상태 확인 가능
- 백업 파일의 버전 관리를 통해 원하는 시점의 파일 복원 가능

효율적인 중앙 모니터링



에이전트 설정 및 로그 확인

- 관제 대상으로 등록된 PC의 에이전트 설치 및 작동 여부 확인 가능
- 에이전트 PC를 그룹 별로 관리 가능
- 에이전트 별 자동백업 폴더, 백업 드라이브, 백업 확장자 등 설정값 확인 가능
- 에이전트 실행로그, 자동백업 로그, 백업 로그 모니터링 지원

주요 구축 사이트

㈜와이티엔	㈜웹캐시	㈜웹캐시피트	㈜쿠콘
㈜마루인터넷	㈜몰스토어	㈜제이에스컴즈	㈜뉴스제주

감사합니다.

제품문의

연락처 : 070-8787-5376 / 이메일 : sales1 @gluesys.com