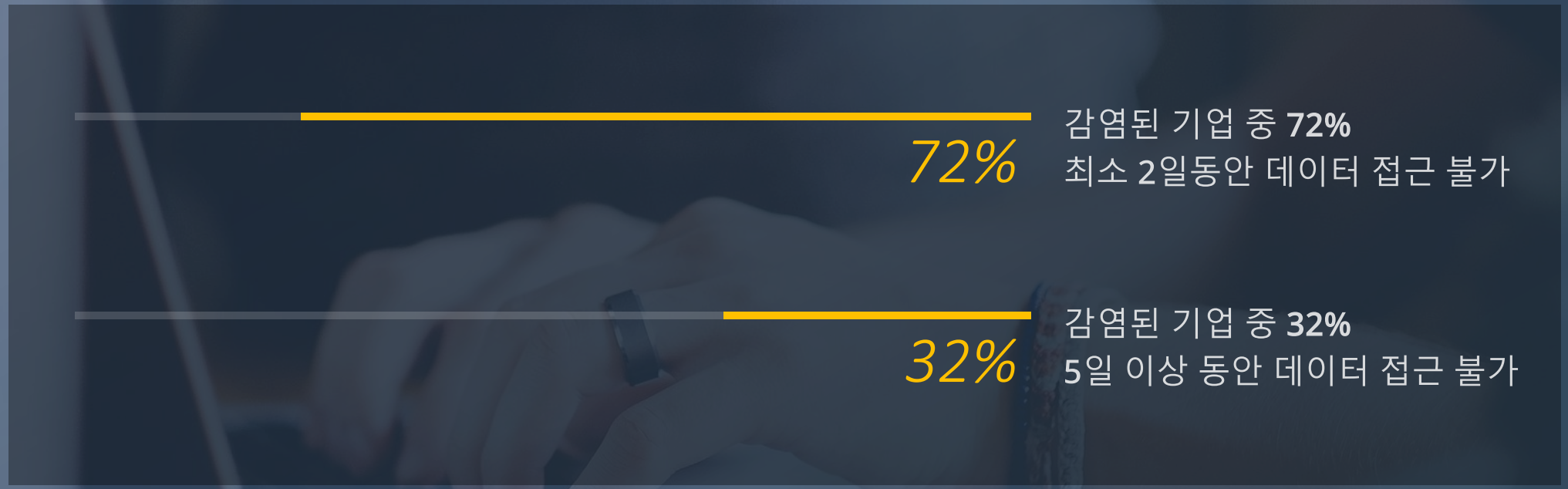
문서중앙화로 추진하는 랜섬웨어 피해 차단 100% 전략

cloudoc NETID Internet Solution Company

I.What is Ransomware?

랜섬웨어 피해 상황

랜섬웨어로 인한 업무 마비 기간



출처 미국 정보 보안 업체 로그리듬(Logrhythm)

통계

70%

요구액을 지불한 피해 기업 70%

42%

랜섬웨어로 인한 손실 데이터의 복구율 42%

50%

피해기업의 50%는 $10,000~$40,000 지불

출처 미국 정보 보안 업체 코모도 SSL(Heimdalsecurity)

랜섬웨어 공격 절차

스팸메일을 통해 감염

악성파일(코드) 다운로드
사용자의 드라이브에 있는 문서 감염

랜섬웨어 경고창 발생

데이터 복구 비용 지불

출처 미국 정보 보안 업체 코모도 SSL(Comodosslstore)

II.Against Ransomware

01 ClouDoc의 랜섬웨어 차단

랜섬웨어 대응

01 **WhiteList로 차단**

- Application Whitelisting
- DLL WhiteListing

02 **IO 패턴 차단**

- 서버엔진에서 랜섬웨어 입출력 패턴으로 자동 차단

03 **자동 버전관리**

- MS Office, CAD를 비롯한 모든 문서 수정 시 자동 버전관리

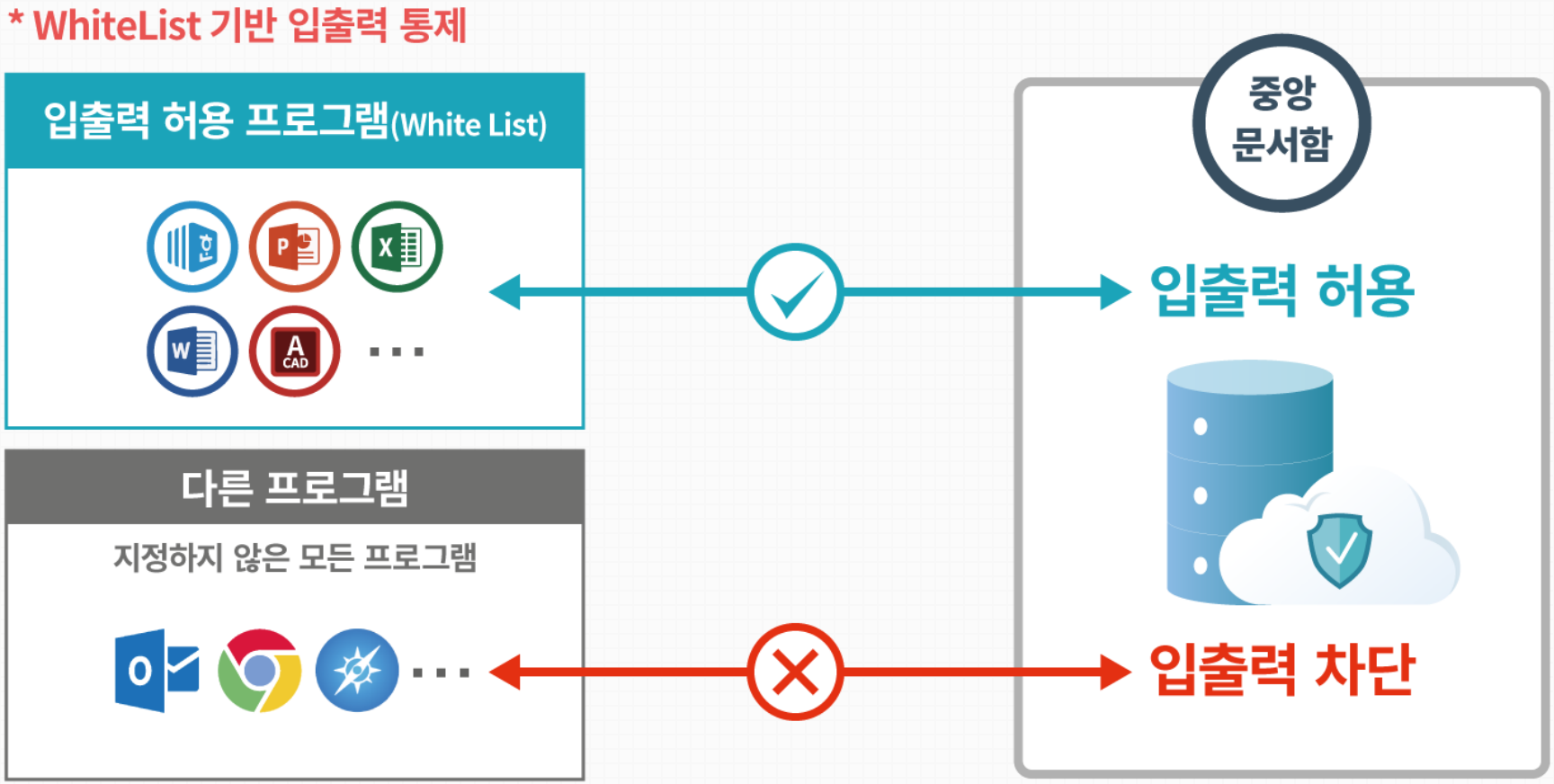
04 **백업**

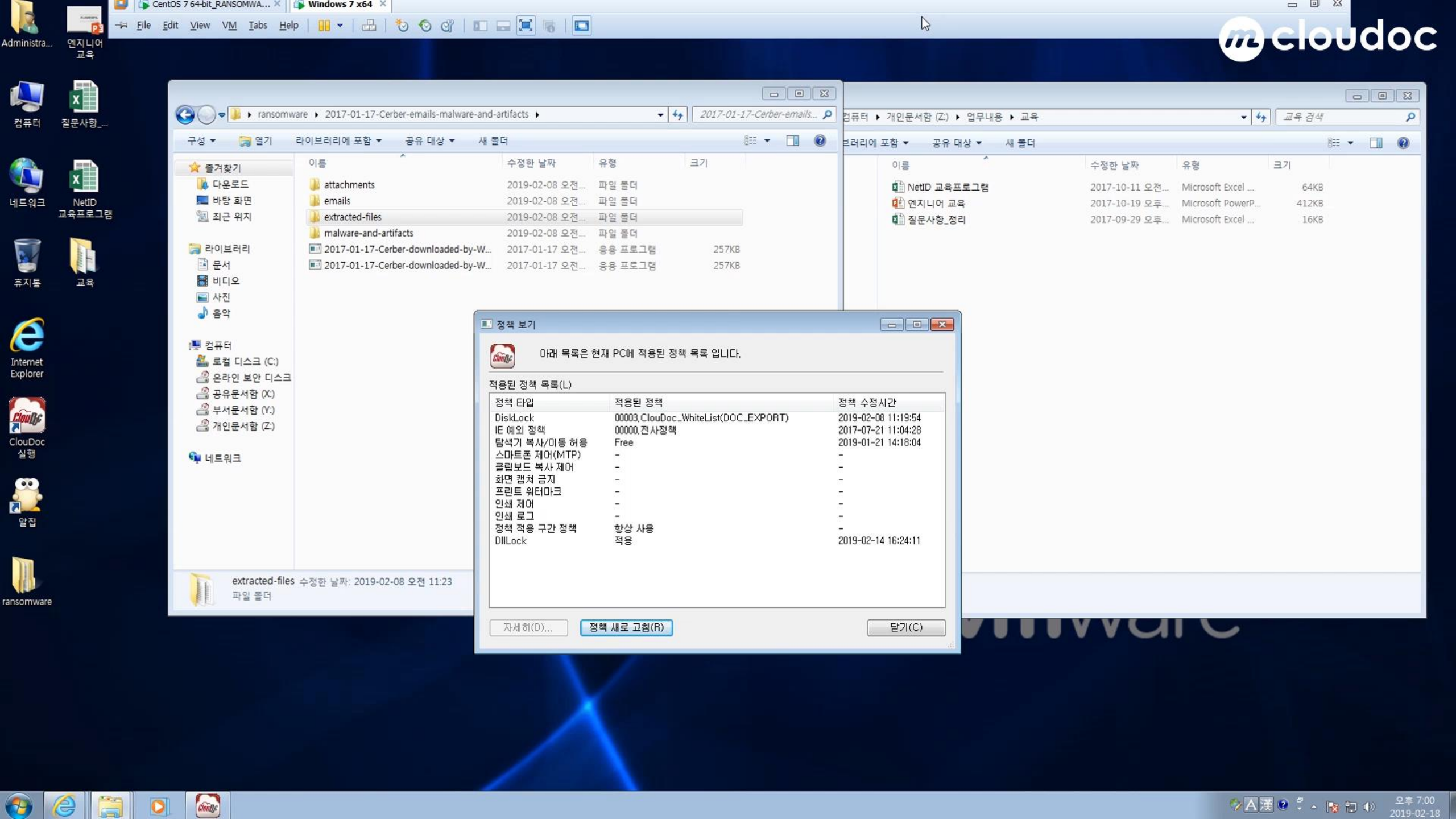
- 365일 날짜별 폴더구조 그대로 증분 백업

02 ClouDoc의 랜섬웨어 대응 1-1

Application WhiteListing

로컬디스크가 아닌 중앙 문서함의 드라이브에 대한 디스크 입출력을 통제

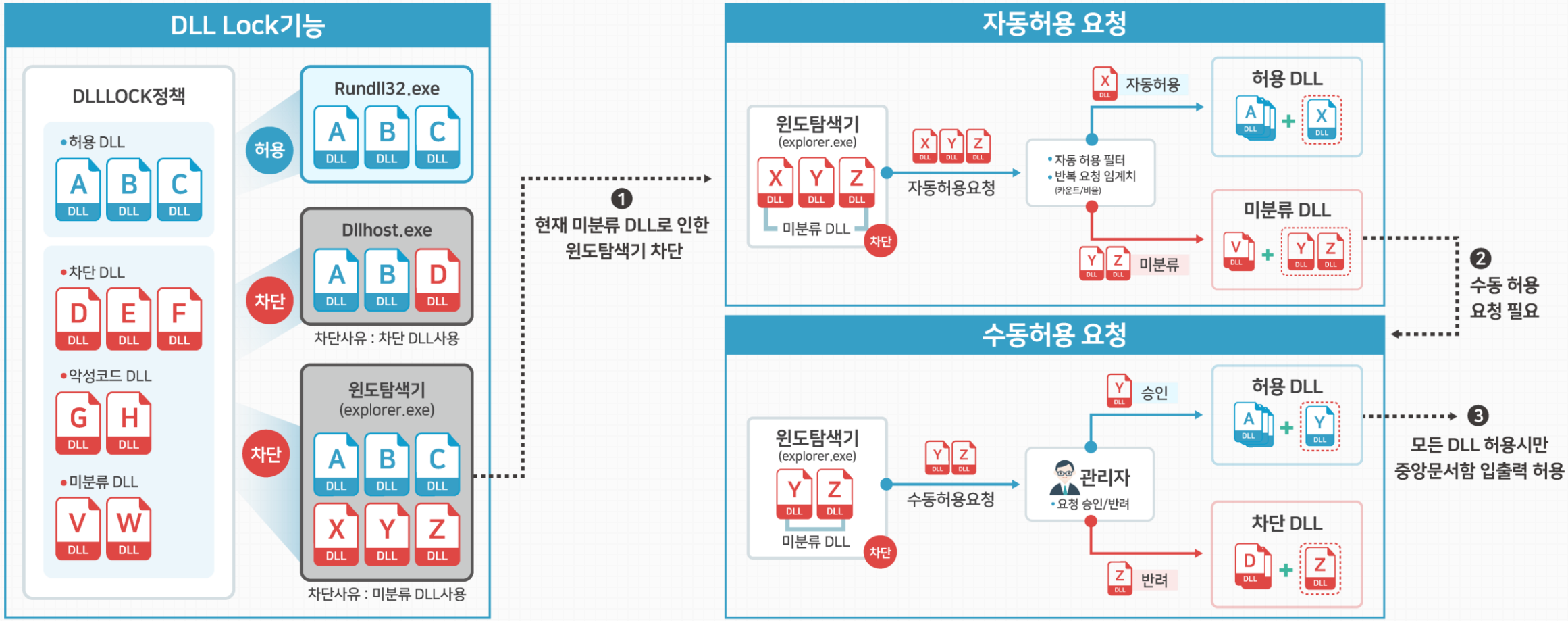


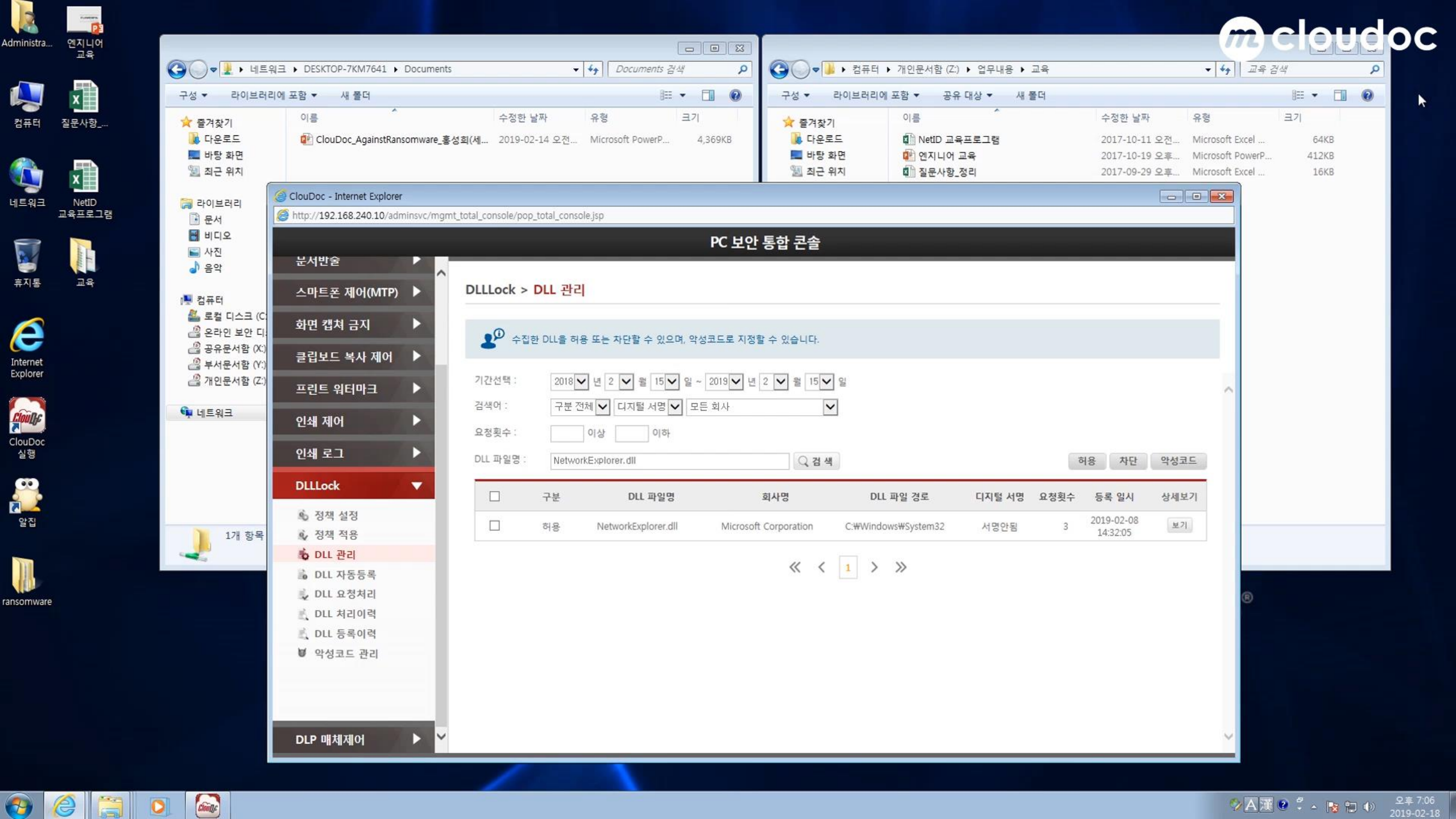

CentOS 7 64-bit_RANSOMWA...
Windows 7 x64
File Edit View VM Tabs Help
cloudoc
Administra...
엔지니어 교육
컴퓨터
질문사항_...
네트워크
NetID 교육프로그램
휴지통
교육
Internet Explorer
ClouDoc 실행
알집
ransomware
ransomware ▸ 2017-01-17-Cerber-emails-malware-and-artifacts ▸
구성 열기 라이브러리에 포함 공유 대상 새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
로컬 디스크 (C:)
온라인 보안 디스크
공유문서함 (X:)
부서문서함 (Y:)
개인문서함 (Z:)
네트워크
이름 수정한 날짜 유형 크기
attachments 2019-02-08 오전... 파일 폴더
emails 2019-02-08 오전... 파일 폴더
extracted-files 2019-02-08 오전... 파일 폴더
malware-and-artifacts 2019-02-08 오전... 파일 폴더
2017-01-17-Cerber-downloaded-by-W... 2017-01-17 오전... 응용 프로그램 257KB
2017-01-17-Cerber-downloaded-by-W... 2017-01-17 오전... 응용 프로그램 257KB
extracted-files 수정한 날짜: 2019-02-08 오전 11:23
파일 폴더
컴퓨터 ▸ 개인문서함 (Z:) ▸ 업무내용 ▸ 교육
교육 검색
이름 수정한 날짜 유형 크기
NetID 교육프로그램 2017-10-11 오전... Microsoft Excel ... 64KB
엔지니어 교육 2017-10-19 오후... Microsoft PowerP... 412KB
질문사항_정리 2017-09-29 오후... Microsoft Excel ... 16KB
정책 보기
아래 목록은 현재 PC에 적용된 정책 목록 입니다.
적용된 정책 목록(L)
정책 타입 적용된 정책 정책 수정시간
DiskLock 00003.ClouDoc_WhiteList(DOC_EXPORT) 2019-02-08 11:19:54
IE 예외 정책 00000.전사정책 2017-07-21 11:04:28
탐색기 복사/이동 허용 Free 2019-01-21 14:18:04
스마트폰 제어(MTP) - -
클립보드 복사 제어 - -
화면 캡쳐 금지 - -
프린트 워터마크 - -
인쇄 제어 - -
인쇄 로그 - -
정책 적용 구간 정책 항상 사용 -
DllLock 적용 2019-02-14 16:24:11
자세히(D)...
정책 새로 고침(R)
닫기(C)
오후 7:00
2019-02-18

02 ClouDoc의 랜섬웨어 대응 1-2

DLL WhiteListing

허용하지 않은 DLL이 기존의 정상적인 프로그램에 의해 적재되면, 중앙문서함을 사용하지 못하도록 하는 기능

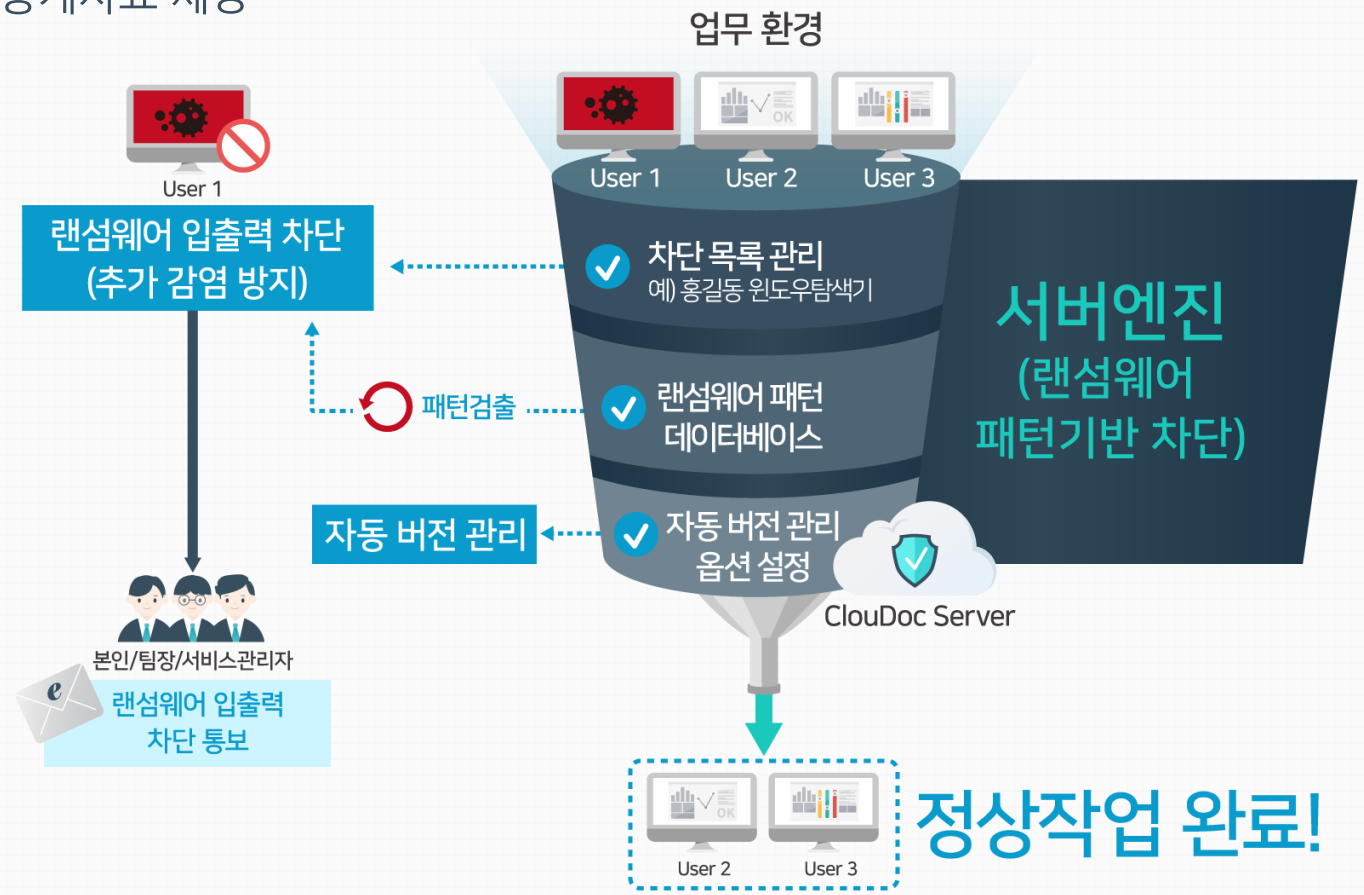



cloudoc
Administra...
엔지니어 교육
컴퓨터
질문사항_...
네트워크
NetID 교육프로그램
휴지통
교육
Internet Explorer
ClouDoc 실행
알집
ransomware
네트워크 ▸ DESKTOP-7KM7641 ▸ Documents
Documents 검색
구성 ▾ 라이브러리에 포함 ▾ 새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
로컬 디스크 (C:)
온라인 보안 디...
공유문서함 (X:)
부서문서함 (Y:)
개인문서함 (Z:)
네트워크
이름 수정한 날짜 유형 크기
ClouDoc_AgainstRansomware_홍성희(세... 2019-02-14 오전... Microsoft PowerP... 4,369KB
1개 항목
컴퓨터 ▸ 개인문서함 (Z:) ▸ 업무내용 ▸ 교육
교육 검색
구성 ▾ 라이브러리에 포함 ▾ 공유 대상 ▾ 새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
이름 수정한 날짜 유형 크기
NetID 교육프로그램 2017-10-11 오전... Microsoft Excel ... 64KB
엔지니어 교육 2017-10-19 오후... Microsoft PowerP... 412KB
질문사항_정리 2017-09-29 오후... Microsoft Excel ... 16KB
ClouDoc - Internet Explorer
http://192.168.240.10/adminsvc/mgmt_total_console/pop_total_console.jsp
PC 보안 통합 콘솔
문서반출
스마트폰 제어(MTP)
화면 캡쳐 금지
클립보드 복사 제어
프린트 워터마크
인쇄 제어
인쇄 로그
DLLLock
정책 설정
정책 적용
DLL 관리
DLL 자동등록
DLL 요청처리
DLL 처리이력
DLL 등록이력
악성코드 관리
DLP 매체제어
DLLLock > DLL 관리
수집한 DLL을 허용 또는 차단할 수 있으며, 악성코드로 지정할 수 있습니다.
기간선택 : 2018 년 2 월 15 일 ~ 2019 년 2 월 15 일
검색어 : 구분 전체 디지털 서명 모든 회사
요청횟수 : 이상 이하
DLL 파일명 : NetworkExplorer.dll 검 색
허용 차단 악성코드
구분 DLL 파일명 회사명 DLL 파일 경로 디지털 서명 요청횟수 등록 일시 상세보기
허용 NetworkExplorer.dll Microsoft Corporation C:₩Windows₩System32 서명안됨 3 2019-02-08 14:32:05 보기
1
오후 7:06
2019-02-18

02 ClouDoc의 랜섬웨어 대응 2

서버 엔진용 랜섬웨어 차단 기능(IO패턴차단)

- ✓ 서버엔진에 랜섬웨어 행동 패턴으로 의심가는 사용자 작업인 경우, 중앙문서함에 대한 디스크 입출력을 차단
- ✓ 의심 및 차단 내용을 본인, 팀장, 서비스 관리자에게 E-mail로 통보
- ✓ 랜섬웨어 관련 통계자료 제공



02 ClouDoc의 랜섬웨어 대응 3-1

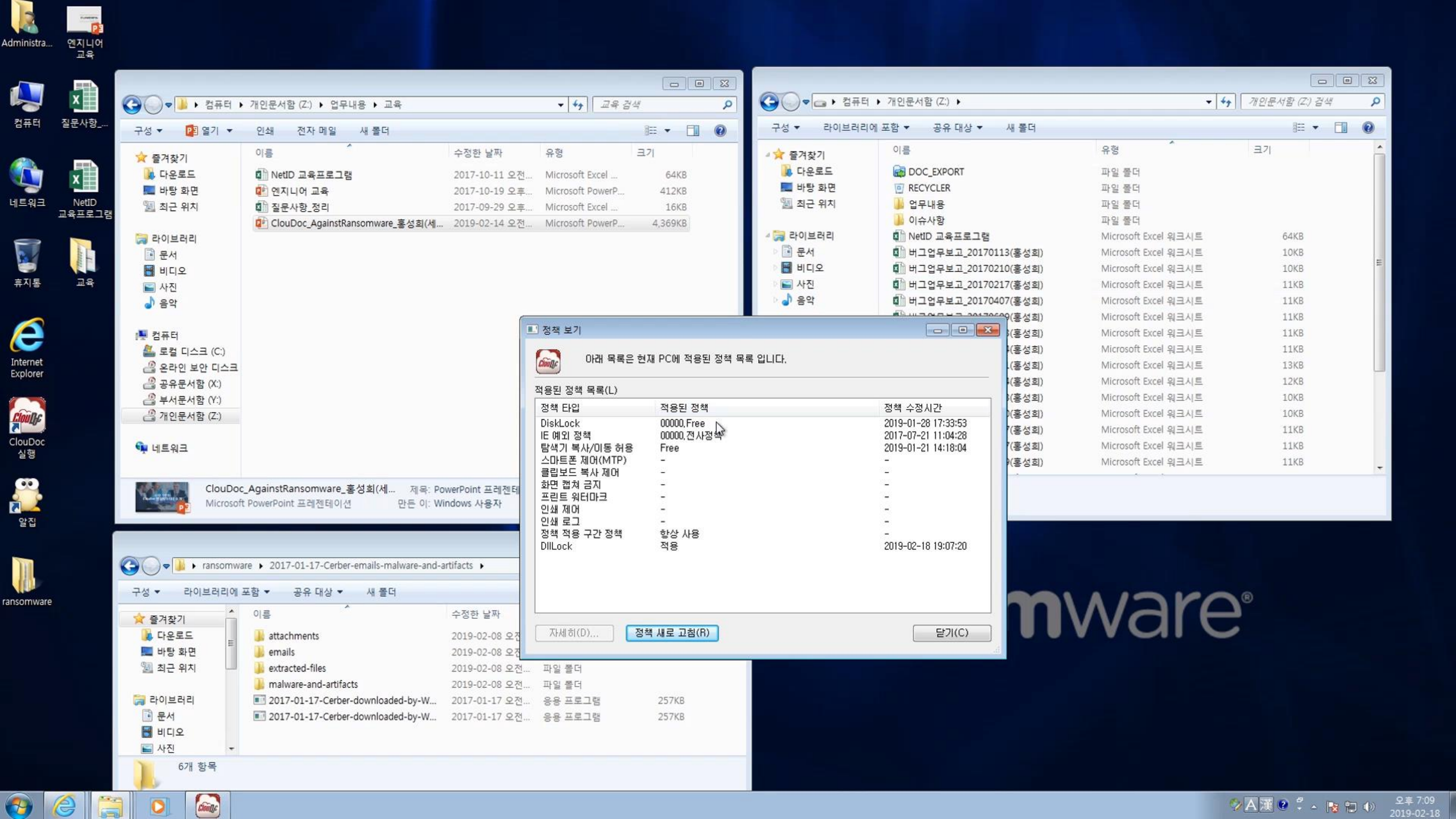
모든 종류의 문서에 대한 자동 버전관리

- ✓ 랜섬웨어에 의해 문서에 암호화가 진행되어도 문서 버전 관리 기능으로 이전 버전으로 복구
- ✓ 특정 문서가 아닌 모든 종류에 대한 문서 버전관리

02 ClouDoc의 랜섬웨어 대응 3-2

보관된 정상 문서의 일괄복원

- ✓ 랜섬웨어 감염 또는 일반적인 사용자 오류로 인해 자동 버전 관리된 문서의 일괄 복원 기능을 제공
- ✓ 문서함 별, 경로 별, 파일 별, 사용자 별, 프로세스 별 문서 일괄 복원 기능을 제공 -> 감염 문서만 정확하게 복원 가능!


Administra...
엔지니어 교육
컴퓨터
질문사항_...
네트워크
NetID 교육프로그램
휴지통
교육
Internet Explorer
ClouDoc 실행
알집
ransomware
컴퓨터 ▸ 개인문서함 (Z:) ▸ 업무내용 ▸ 교육
교육 검색
구성 열기 인쇄 전자 메일 새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
로컬 디스크 (C:)
온라인 보안 디스크
공유문서함 (X:)
부서문서함 (Y:)
개인문서함 (Z:)
네트워크
이름 수정한 날짜 유형 크기
NetID 교육프로그램 2017-10-11 오전... Microsoft Excel ... 64KB
엔지니어 교육 2017-10-19 오후... Microsoft PowerP... 412KB
질문사항_정리 2017-09-29 오후... Microsoft Excel ... 16KB
ClouDoc_AgainstRansomware_홍성희(세... 2019-02-14 오전... Microsoft PowerP... 4,369KB
ClouDoc_AgainstRansomware_홍성희(세... 제목: PowerPoint 프레젠테
Microsoft PowerPoint 프레젠테이션 만든 이: Windows 사용자
컴퓨터 ▸ 개인문서함 (Z:) ▸
개인문서함 (Z:) 검색
구성 라이브러리에 포함 공유 대상 새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
이름 유형 크기
DOC_EXPORT 파일 폴더
RECYCLER 파일 폴더
업무내용 파일 폴더
이슈사항 파일 폴더
NetID 교육프로그램 Microsoft Excel 워크시트 64KB
버그업무보고_20170113(홍성희) Microsoft Excel 워크시트 10KB
버그업무보고_20170210(홍성희) Microsoft Excel 워크시트 10KB
버그업무보고_20170217(홍성희) Microsoft Excel 워크시트 11KB
버그업무보고_20170407(홍성희) Microsoft Excel 워크시트 11KB
정책 보기
아래 목록은 현재 PC에 적용된 정책 목록 입니다.
적용된 정책 목록(L)
정책 타입 적용된 정책 정책 수정시간
DiskLock 00000,Free 2019-01-28 17:33:53
IE 예외 정책 00000,전사정책 2017-07-21 11:04:28
탐색기 복사/이동 허용 Free 2019-01-21 14:18:04
스마트폰 제어(MTP) - -
클립보드 복사 제어 - -
화면 캡쳐 금지 - -
프린트 워터마크 - -
인쇄 제어 - -
인쇄 로그 - -
정책 적용 구간 정책 항상 사용 -
DllLock 적용 2019-02-18 19:07:20
자세히(D)...
정책 새로 고침(R)
닫기(C)
ransomware ▸ 2017-01-17-Cerber-emails-malware-and-artifacts ▸
구성 라이브러리에 포함 공유 대상 새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
이름 수정한 날짜
attachments 2019-02-08 오전...
emails 2019-02-08 오전...
extracted-files 2019-02-08 오전... 파일 폴더
malware-and-artifacts 2019-02-08 오전... 파일 폴더
2017-01-17-Cerber-downloaded-by-W... 2017-01-17 오전... 응용 프로그램 257KB
2017-01-17-Cerber-downloaded-by-W... 2017-01-17 오전... 응용 프로그램 257KB
6개 항목
mware®
오후 7:09
2019-02-18

02 ClouDoc의 랜섬웨어 대응 4

백업 / 백업 온라인

- ✓ 특정 폴더 및 파일만 지정하여 신속한 복원.
- ✓ 365일 날짜 별 폴더 구조 그대로 증분백업.
- ✓ ClouDoc Backup : 사내구축하여 전용으로 사용.
- ✓ BackupDoc : 클라우드서비스 또는 사내 구축도 가능. 단일 서비스에 여러 고객사 등록하여 백업 가능.
  각 고객사별 암호화 키, 전용 관리자페이지 제공, 클라우드 서비스 형태로 이용 가능.

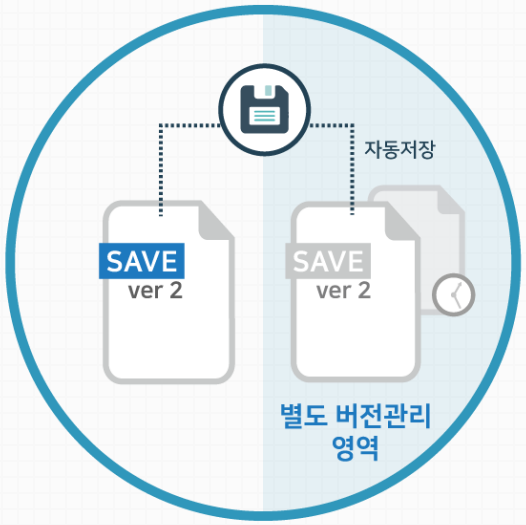
cloudoc Backup	BackupDoc
사내구축 (On-Premise)	사내구축 (On-Premise) 클라우드 서비스
단일기업 서비스	단일기업 / 복수기업 서비스
NFS / CIFS 프로토콜	HTTPS 프로토콜
영구라이선스	월과금 또는 영구라이선스
백업 위치 : 로컬	백업 위치 : 로컬 또는 원격
LAN 구간 백업	LAN / WAN 구간 백업

III.Conclusion

03 왜 ClouDoc 랜섬웨어 대응이 좋은가?

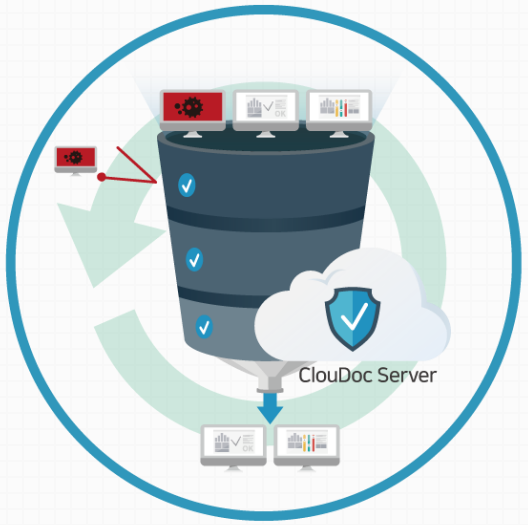
완벽한 WhiteList 방식

보안성이 강한 해쉬값 기반의
Application WhiteList,
DLL WhiteList



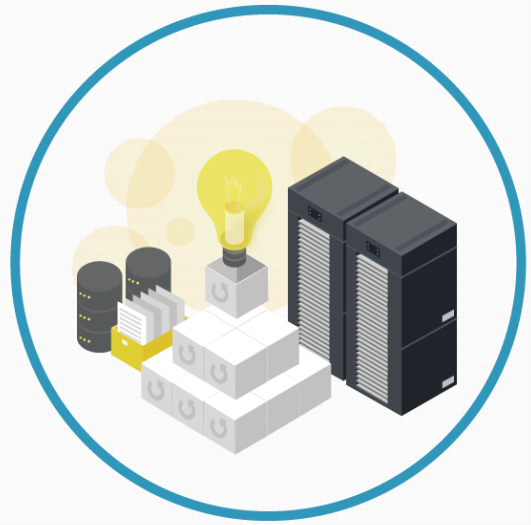
랜섬웨어에 한 발 앞선 대응

최근 랜섬웨어 추세에 따라
문서 종류에 관계없이
자동 버전관리로 피해 최소화



지능적인 대응

랜섬웨어 Disk IO 패턴에
기반한 지능적인 입출력 차단



유연한 사후 대응

다양한 백업솔루션을 제공하여
고객사 상황에 맞는
백업 방식을 선택