

업무서버의 중요자료 탈취방지 및 랜섬웨어 예방을 위한

FilingBox MEGA 제품소개서





업무서버의 중요자료 탈취방지 및 랜섬웨어 예방을 위한

FilingBox MEGA

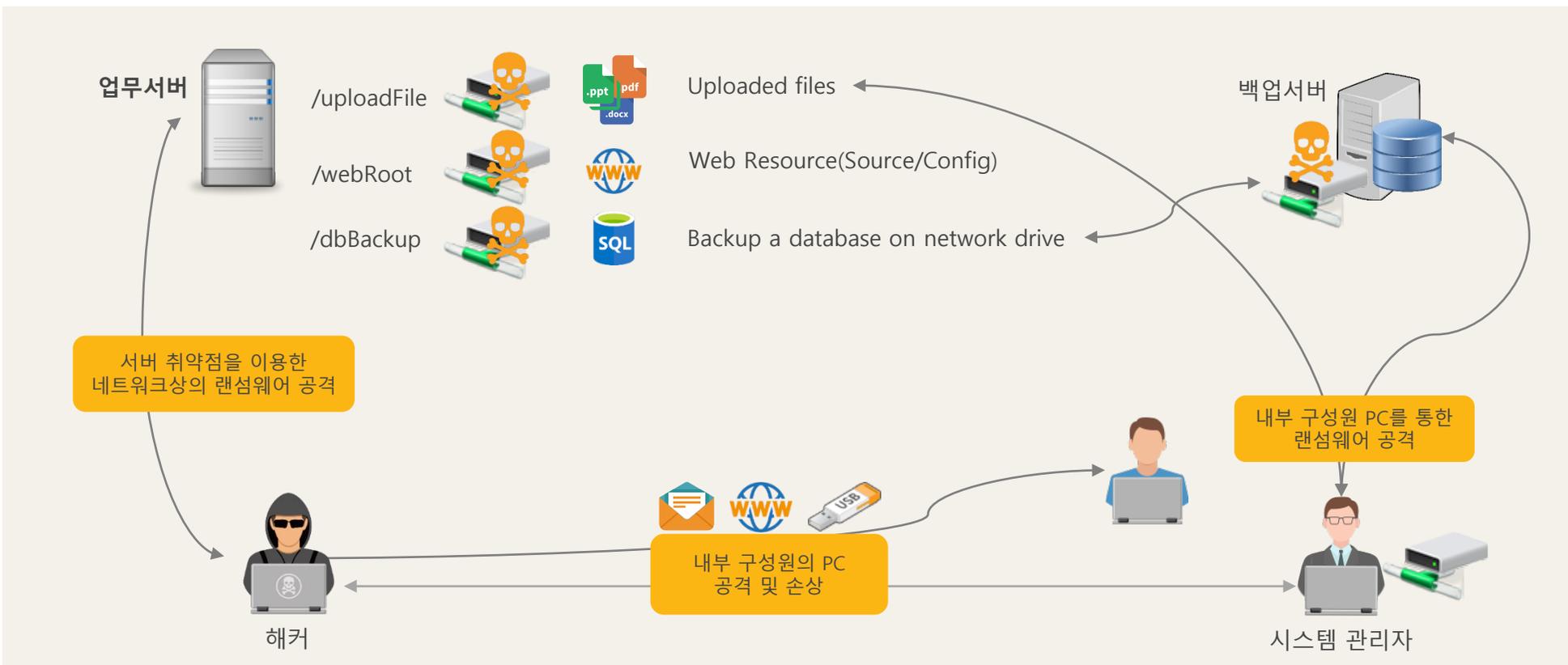


목차

- 1 업무서버의 데이터 관리 현황
- 2 FilingBox MEGA 개요
- 3 FilingBox MEGA 구성
- 4 FilingBox MEGA 특징점
- 5 FilingBox MEGA 적용예시
- 6 FilingCloud™ 소개

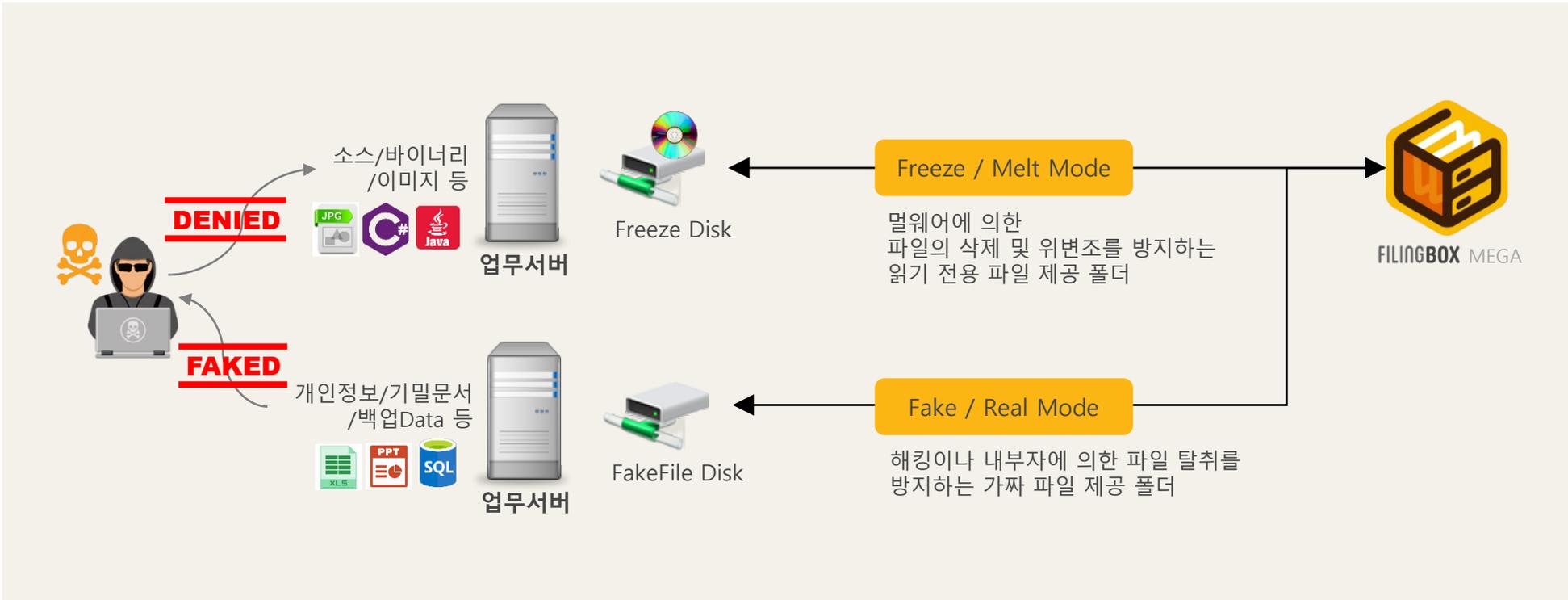
네트워크에 연결된 업무서버는 언제나 해킹 및 랜섬웨어 공격에 노출

많은 비즈니스가 인터넷에 연결되면서 서버 내의 데이터는 언제나 해커에게 탈취되거나 암호화될 수 있습니다. 해커는 개인 PC 를 공격하기 보다는 한번의 공격으로 인해 치명적인 문제를 일으킬 수 있는 병원, 학교, 중소기업 등을 공격하여 더 큰 돈을 벌려고 합니다. 업무서버가 네트워크에 연결되어 있다는 것은 언제든지 해커의 공격이 가능하다는 뜻으로 이를 예방할 수 있는 근본적인 대안이 필요합니다.



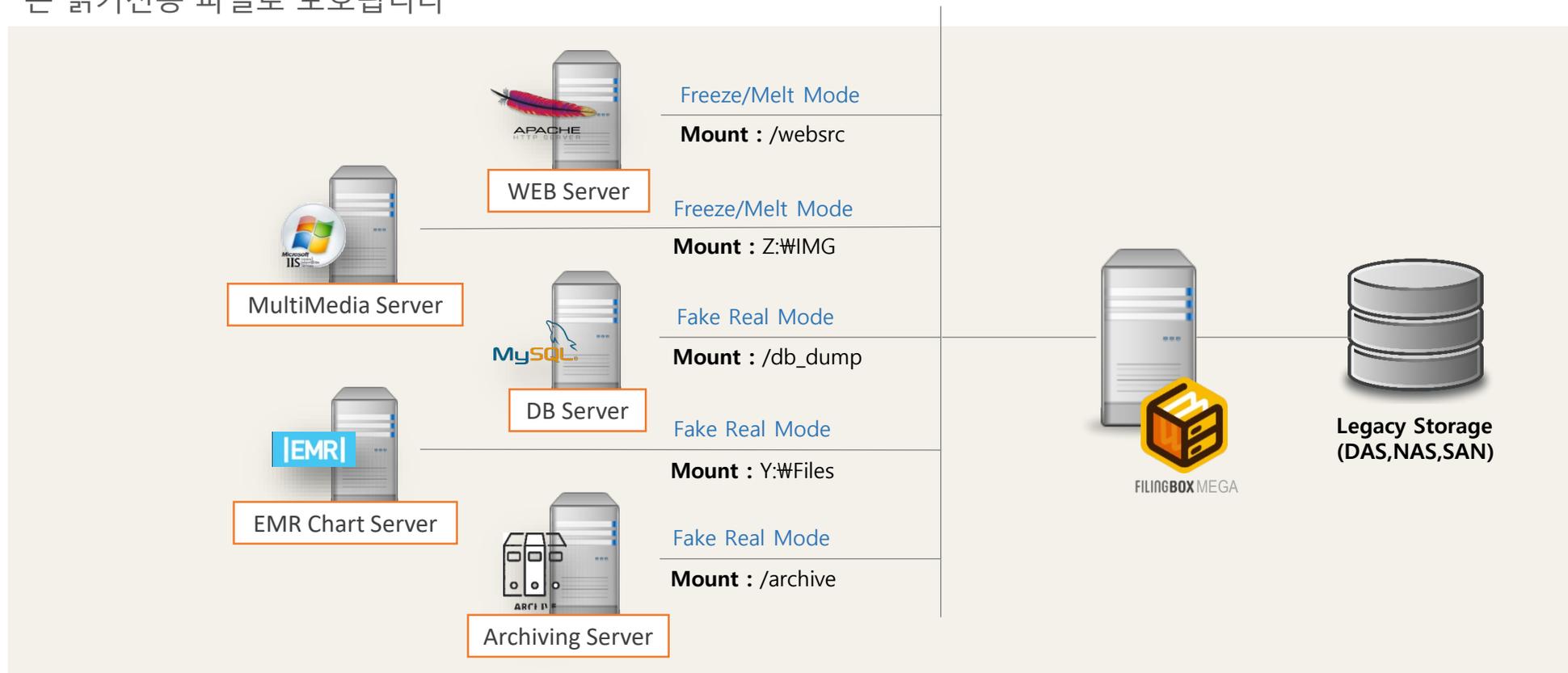
서버가 공격받더라도 데이터를 보호하는 스토리지 프로텍션 기술

FilingBox MEGA는 리눅스나 윈도우 서버에 대한 데이터 탈취나 랜섬웨어 공격을 네트워크 스토리지 관점에서 무력화 시키는 서버용 스토리지 프로텍션 기술입니다. 스토리지 프로텍션 기술은 네트워크나 엔드포인트 레벨에서 데이터를 보호하는 종래 기술과 달리 데이터를 보관하고 있는 스토리지 관점에서 데이터를 보호하는 보안 기술입니다. 스토리지에서 서버와 연결되는 폴더를 생성할때 해당 폴더에서 데이터 탈취 공격을 무력화되도록 하는 Fake 모드로 폴더를 설정하거나, 랜섬웨어 공격을 원천차단하는 Freeze 모드로 설정할 수 있습니다.



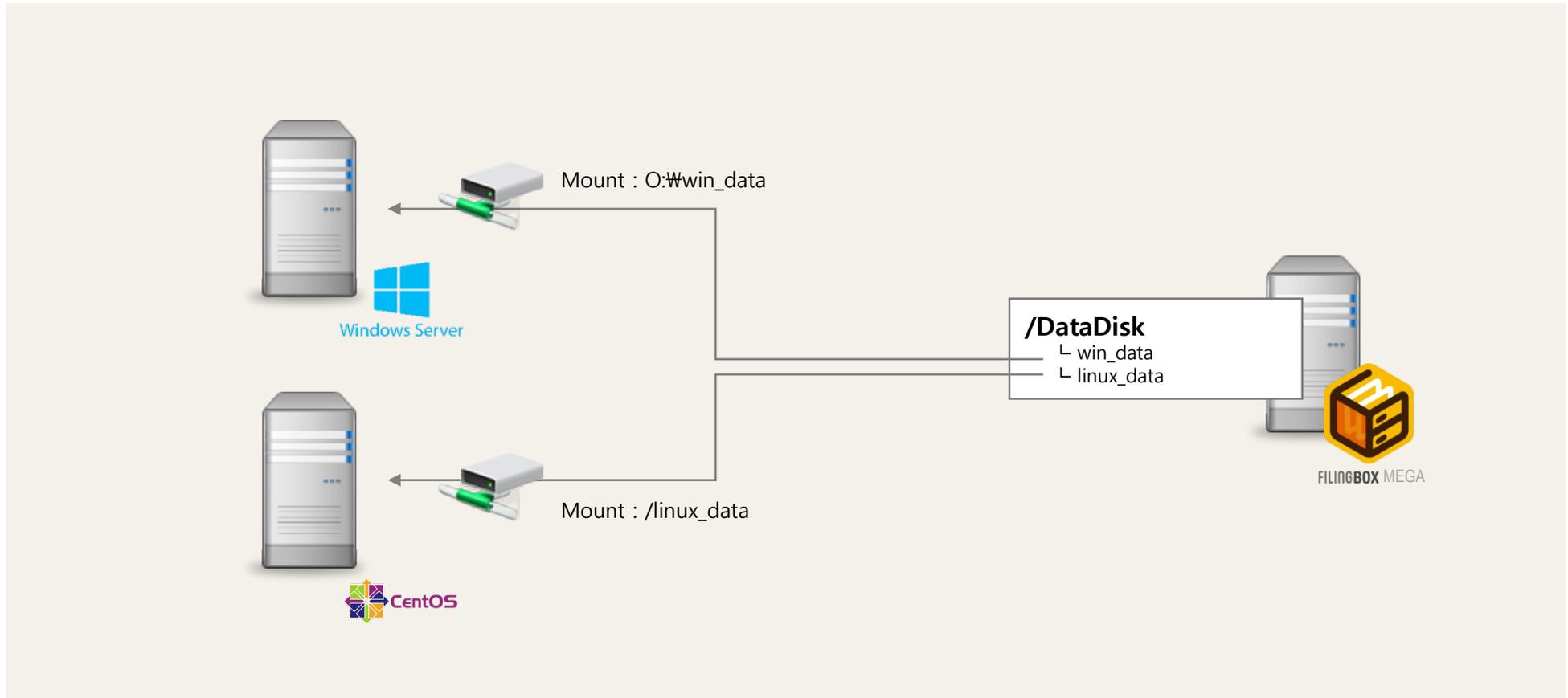
다양한 목적의 업무서버를 지원

FilingBox MEGA는 업무서버에 필요한 저장 공간을 폴더별로 할당하여 특정 서버에서 네트워크 스토리지로 사용합니다. 각 업무 서버에 제공되는 폴더는 서버의 데이터 보호 목적에 맞게 가짜 파일이 제공되는 Fake 모드 또는 읽기 전용 파일이 제공되는 Freeze 모드로 설정할 수 있습니다. 기존 일반스토리지에서 업무서버의 데이터를 보관하고 있는 경우 FilingBox MEGA를 통하여 재구성하면 기존 스토리지내 모든 데이터가 MEGA에 의해서 가짜 파일 또는 읽기전용 파일로 보호됩니다



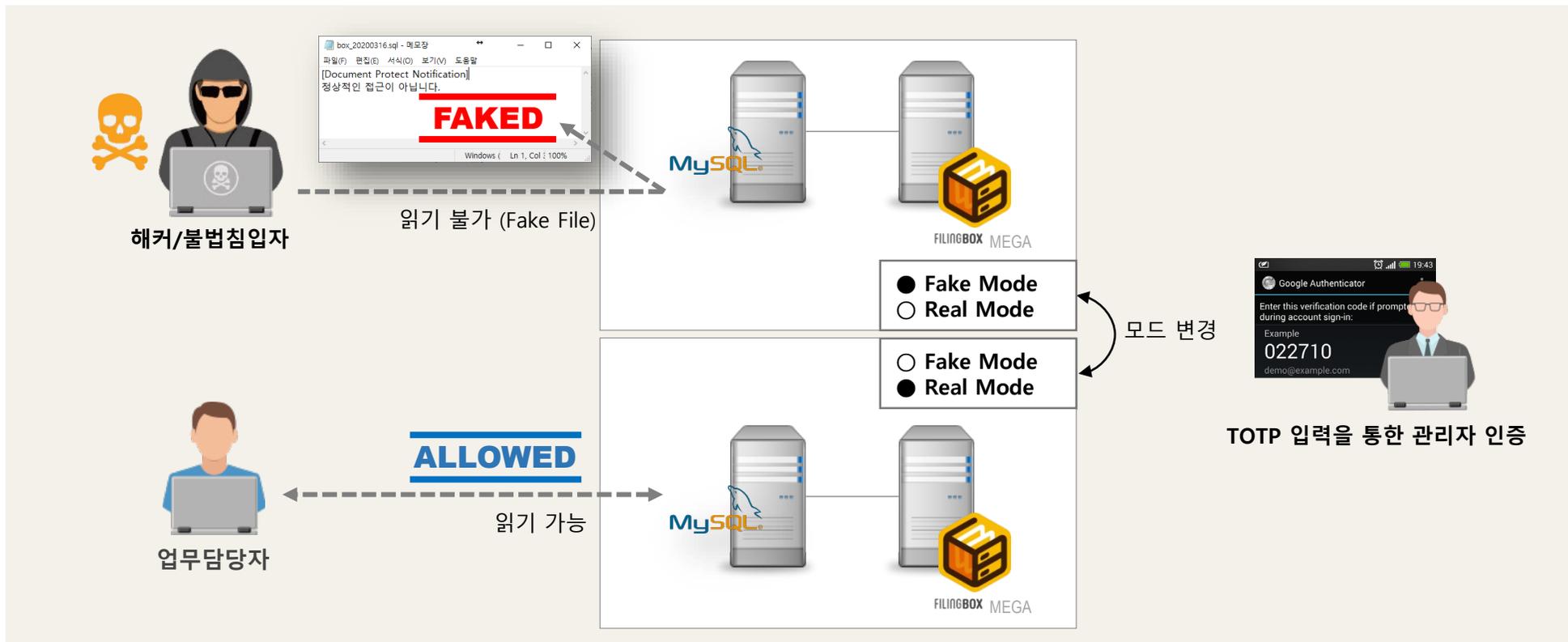
4.1 Windows 및 Linux 서버 네트워크 드라이브 (Freeze/Melt , Fake/Real Mode)

독립서버에 FilingBox MEGA 서버 소프트웨어를 설치 한 후 기존 윈도우나 리눅스 서버에서 FilingBox MEGA 클라이언트 소프트웨어를 설치하면 FilingBox MEGA 내 폴더를 서버의 네트워크 드라이브로 연결할 수 있습니다. FilingBox MEGA는 Windows 및 Linux 서버 OS를 지원합니다.



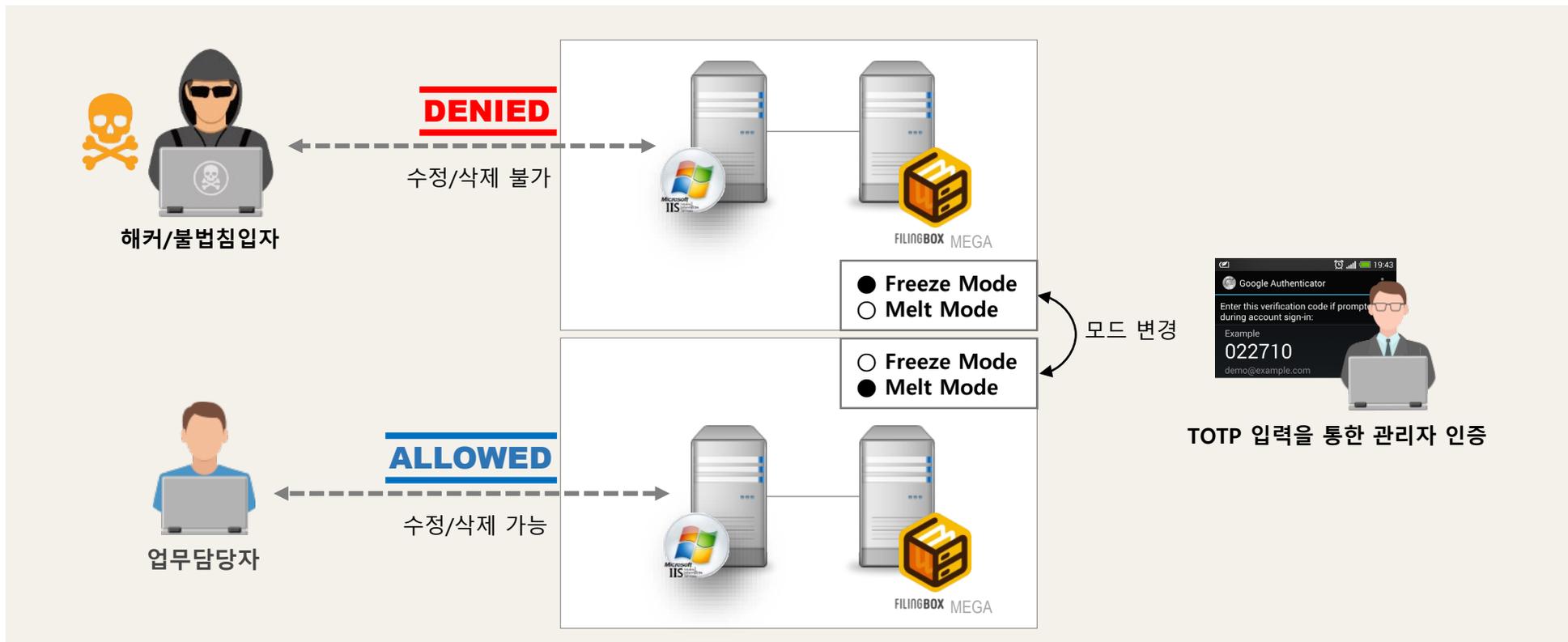
4.2 중요자료 탈취방지 (Fake/Real Mode)

멀웨어나 해커에 의해서 서버내 중요 데이터가 외부로 탈취되는 경우, 기업이나 기관에 치명적인 사고로 이어질 수 있습니다. FilingBox MEGA는 폴더별로 Fake/Real 모드를 제공하여 루트 계정을 포함한 서버내 그 어떤 계정에서 해당 폴더내 파일 접속을 시도하더라도 가짜 파일을 서버에 제공하여 데이터 탈취 사고를 근본적으로 예방합니다. FilingBox MEGA의 관리자가 OTP코드를 입력하여 해당 폴더의 권한을 Fake 모드에서 Real 모드로 전환한 경우에만 진짜 파일 접속이 가능해 집니다.



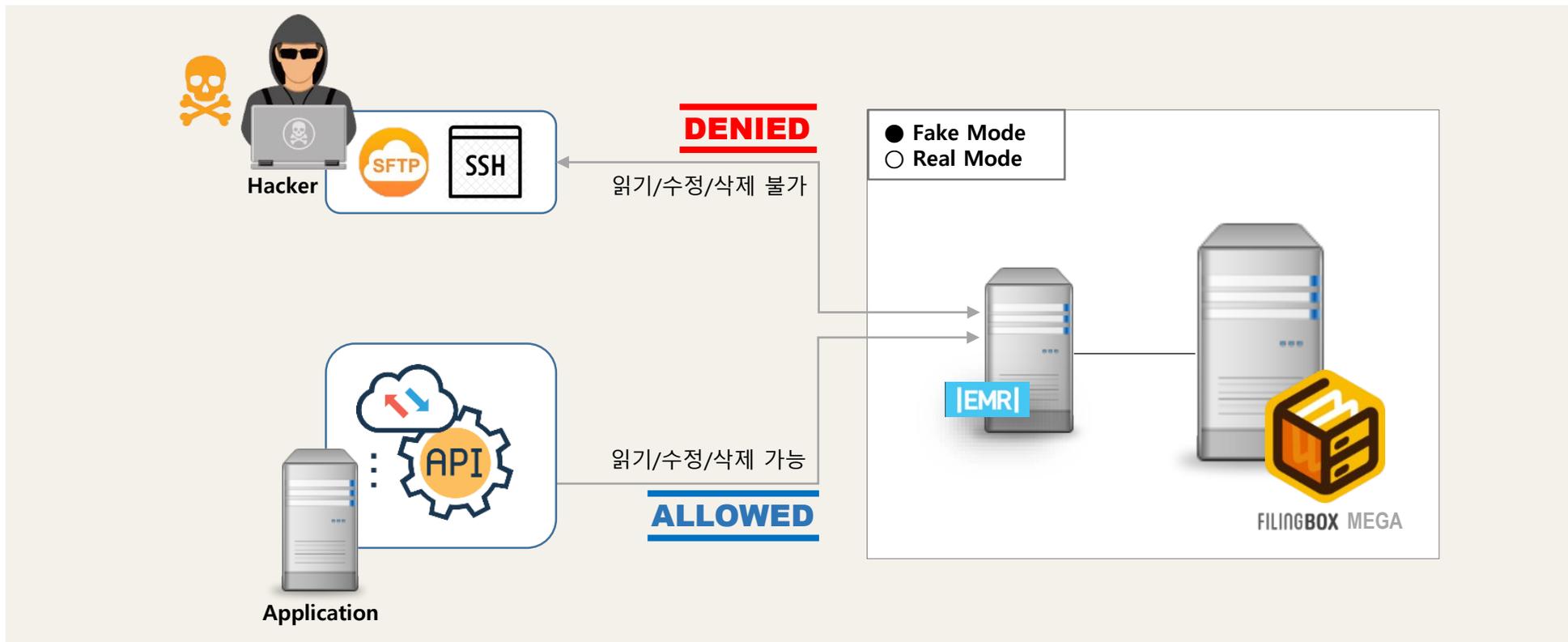
4.3 중요자료 위변조 방지 (Freeze/Melt Mode)

랜섬웨어나 해커에 의해서 서버내 중요 데이터가 암호화되는 경우, 기업이나 기관에 치명적인 업무중단으로 이어질 수 있습니다. FilingBox MEGA는 폴더별로 Freeze/Melt 모드를 제공하여 루트 계정을 포함한 서버내 그 어떤 계정에서 데이터 변경을 시도하더라도 읽기전용으로 파일을 서버에 제공하여 랜섬웨어 사고를 근본적으로 예방합니다. FilingBox MEGA의 관리자가 OTP코드를 입력하여 해당 폴더의 권한을 Freeze 모드에서 Melt 모드로 전환한 경우에만 파일 수정이 가능해 집니다.



4.4 Fake Mode에서 전용 API를 통한 진짜 파일 접근

업무서버내 특정 업무프로그램에 한하여 FilingBox MEGA내 파일의 읽기/수정/삭제 등이 필요한 경우 전용 API를 통해서 진짜 파일의 접근이 가능합니다. 일반적인 Console 에 의한 접근, FTP, SFTP, SSH 등의 접근을 통해서 는 파일의 접근이 불가능하나, 서버내 업무프로그램이 FilingBox MEGA의 전용 API를 통해 파일에 접근하는 경우에만 파일 접근이 가능합니다. Fake Mode가 유지되면서도 서버내 업무 프로그램에 한하여 파일 열람, 수정, 삭제가 가능 하도록 API를 제공합니다.

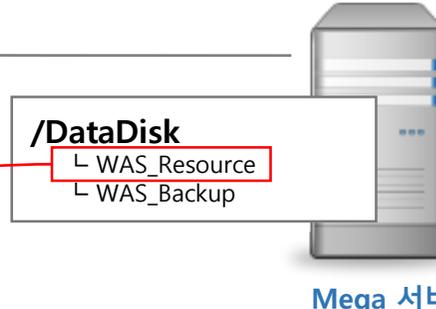


위변조 방지 모드 구성 (웹소스/바이너리/이미지 등 서버리소스 보호)

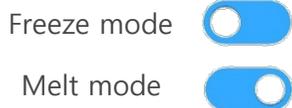
1. File System 연결 : WAS_Resource 폴더를 z_mega 폴더로 마운트



```
drwxr-xr-x. 9 root root 109 2월 27 18:07 storage
dr-xr-xr-x. 13 root root 0 2월 25 10:17 sys
drwxrwxrwt. 9 root root 192 3월 16 15:07 tmp
drwxr-xr-x. 13 root root 155 10월 15 16:14 usr
drwxr-xr-x. 20 root root 282 10월 15 16:22 var
drwxr-xr-x. 2 root root 6 3월 16 15:07 z_mega
[root@bmw-mega ~]#
```



2. 폴더 관리모드 설정



파일 수정/삭제 불가능

파일 수정/삭제 가능

ALLOWED

DENIED

```
-rwxr--r--. 1 root root 675 9월 30 17:52 del0tpActn.jsp
-rwxr--r--. 1 root root 634 9월 30 17:52 initErrActn.jsp
-rwxr--r--. 1 root root 10323 11월 11 12:42 login.jsp
-rwxr--r--. 1 root root 2056 9월 30 17:52 loginActn.jsp
-rwxr--r--. 1 root root 16824 11월 11 12:42 mod0tp.jsp
-rwxr--r--. 1 root root 989 9월 30 17:52 mod0tpActn.jsp
-rwxr--r--. 1 root root 17264 11월 11 12:42 reg0tp.jsp
-rwxr--r--. 1 root root 1021 9월 30 17:52 reg0tpActn.jsp
-rwxr--r--. 1 root root 11521 11월 11 12:42 view0tp.jsp
```

3. 수정/삭제 불가



침입자(해커)

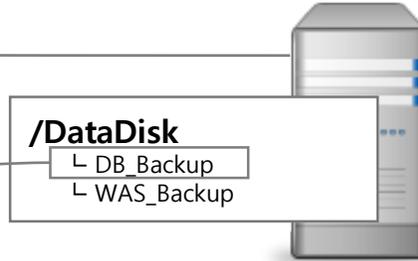
탈취 방지 모드 구성 (DB Dump 및 백업파일 보호)

1. File System 연결 : DB_Backup 폴더를 z_mega 폴더로 마운트



DB 서버
MySQL

```
drwxr-xr-x. 9 root root 109 2월 27 18:07 storage
dr-xr-xr-x. 13 root root 0 2월 25 10:17 sys
drwxrwxrwt. 9 root root 192 3월 16 15:07 tmp
drwxr-xr-x. 13 root root 155 10월 15 16:14 usr
drwxr-xr-x. 20 root root 282 10월 15 16:22 var
drwxr-xr-x. 2 root root 6 3월 16 15:07 z_mega
[root@bmw-mega /]#
```



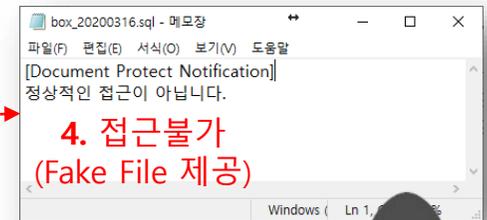
Mega 서버

2. DB Dump

```
[root@bmw-mega /]# mysqldump -u root -p box > /z_mega/box_20200316.sql
```

```
drwxr-xr-x. 9 root root 109 2월 27 18:07 storage
dr-xr-xr-x. 13 root root 0 2월 25 10:17 sys
drwxrwxrwt. 9 root root 192 3월 16 15:07 tmp
drwxr-xr-x. 13 root root 155 10월 15 16:14 usr
drwxr-xr-x. 20 root root 282 10월 15 16:22 var
drwxr-xr-x. 2 root root 6 3월 16 15:07 z_mega
[root@bmw-mega /]#
```

```
[root@bmw-mega z_mega]# ls -al
한계 28
drwxr-xr-x. 2 root root 30 3월 16 15:34 .
dr-xr-xr-x. 21 root root 282 3월 16 15:07 ..
-rwxr--r--. 1 root root 28042 3월 16 15:33 box_20200316.sql
```



3. 해킹 및 읽기 시도



탈취 방지 모드 구성 (기밀문서, 개인정보파일 등 중요문서 보호)

1. File System 연결 : SecureFolder 폴더를 z_mega 폴더로 마운트



업무용 웹서버

```
drwxr-xr-x.  9 root root  109  2월  27 18:07 storage
dr-xr-xr-x. 13 root root   0  2월  25 10:17 sys
drwxrwxrwt.  9 root root  192  3월  16 15:07 tmp
drwxr-xr-x. 13 root root  155 10월  15 16:14 usr
drwxr-xr-x. 20 root root  282 10월  15 16:22 var
drwxr-xr-x.  2 root root   6  3월  16 15:07 z_mega
[root@bmw-mega /]#
```



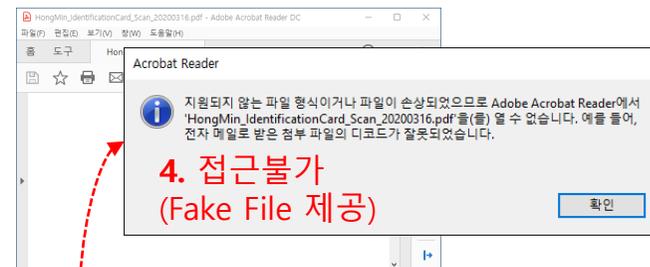
Mega 서버

2. 개인정보문서 업로드(웹) 및 저장



```
drwxr-xr-x.  9 root root  109  2월  27 18:07 storage
dr-xr-xr-x. 13 root root   0  2월  25 10:17 sys
drwxrwxrwt.  9 root root  192  3월  16 15:07 tmp
drwxr-xr-x. 13 root root  155 10월  15 16:14 usr
drwxr-xr-x. 20 root root  282 10월  15 16:22 var
drwxr-xr-x.  2 root root   6  3월  16 15:07 z_mega
[root@bmw-mega /]#
```

```
[root@bmw-mega z_mega]# ll
한 계  4
-rwxr--r--. 1 root root  5  3월  16 18:44 HongMin_IdentificationCard_Scan_20200316.pdf
```



3. 해킹 및 읽기 시도



Company & Business Overview

- **FilingCloud™란?**

사무실보다 안전하고 체계적이며 스마트한 업무 환경을 제공하는 기업용 솔루션 전문 브랜드입니다.



FilingCloud™ Products

- FilingBox Enterprise : 협업을 위한 랜섬웨어 예방 기업용 디스크
- FilingBox MEGA : 업무서버의 데이터를 완벽히 보호하는 서버용 파일링박스
- AutoPassword Ent. : 협업을 위한 AutoPassword™ 인증 솔루션
- Access Manager : 협업을 위한 PC 사용자 관리 시스템

웹사이트: www.filingcloud.co.kr 이메일: support@filingcloud.co.kr 전화: 02-6925-1304



- 회 사 명 : (주) 나무소프트
- 미 션: 협업을 위한 클라우드 서비스 제공
- 설 립 일 : 2001년 9월 (2004년 11월 법인 전환)
- 주 소: 서울특별시 금천구 디지털로 130 남성프라자 1308~1311호