

# 설치: 에이전트

## 개요

OS 별 App Control 에이전트 설치 방법에 대한 문서입니다.

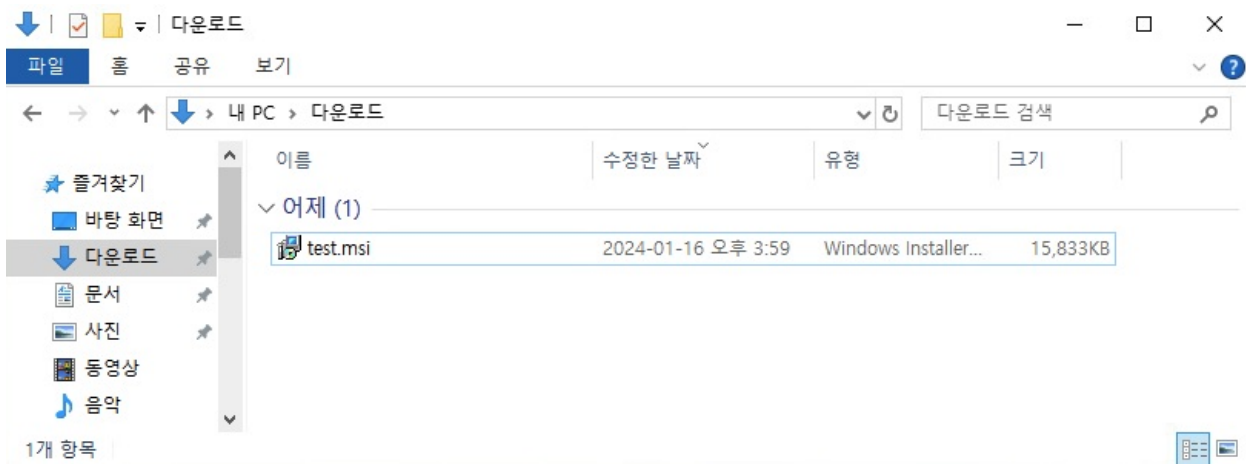
## 진행 방법

에이전트 다운로드 : <https://IP or FQDN/hostpkg>

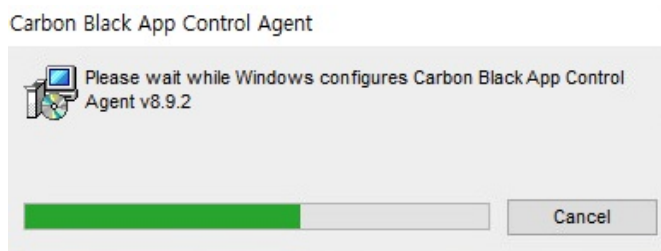
### 1. Windows 에이전트 설치

에이전트 호환성 : <https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-appc-oer-winagent-desktop/GUID-A22FCC4B-CA35-4DDF-AA52-A101581E34F4.html>

#### 1.1 GUI 설치



- 사용자 PC에서 다운로드 받은 'App Control 에이전트 (정책명.msi)' 실행



- 설치 진행

작업 관리자

파일(F) 옵션(O) 보기(V)

프로세스 성능 앱 기록 시작프로그램 사용자 세부 정보 서비스

| 이름  | 상태 | 18% CPU | 43% 메모리 | 40% 디스크   | 0% 네트워크 |
|---|----|---------|---------|-----------|---------|
| <b>앱 (2)</b>  |    |         |         |           |         |
| > Windows 탐색기                                       |    | 0%      | 79.8MB  | 0MB/s     | 0Mbps   |
| > 작업 관리자  |    | 0%      | 20.4MB  | 0MB/s     | 0Mbps   |
| <b>백그라운드 프로세스 (53)</b>                              |    |         |         |           |         |
| > Antimalware Service Executable                    |    | 0.2%    | 198.8MB | 0.6MB/s   | 0Mbps   |
| Application Frame Host                              |    | 0%      | 5.1MB   | 0MB/s     | 0Mbps   |
| Carbon Black App Control™ Agent Executable(32비트)    |    | 17.0%   | 34.7MB  | 101.4MB/s | 0Mbps   |
| Carbon Black App Control Agent                      |    |         |         |           |         |
| COM Surrogate                                       |    | 0%      | 0.1MB   | 0MB/s     | 0Mbps   |
| > COM Surrogate                                     |    | 0%      | 0.2MB   | 0MB/s     | 0Mbps   |
| CTF Loader  |    | 0%      | 2.3MB   | 0MB/s     | 0Mbps   |
| Google Crash Handler                                |    | 0%      | 0.4MB   | 0MB/s     | 0Mbps   |
| Google Crash Handler(32비트)                          |    | 0%      | 0.4MB   | 0MB/s     | 0Mbps   |
| > Microsoft Distributed Transaction Coordinator 서비스 |    | 0%      | 0.1MB   | 0MB/s     | 0Mbps   |

간단히(D) 작업 끝내기(E)

- '작업 관리자' 또는 '서비스' 확인하여 에이전트 설치 확인

## 1.2 CLI 설치

- 클라이언트 등록 코드 확인 방법 (기본 값 : 비활성화)  
: [App Control] 웹 콘솔 접속 > [Settings] - [System Configuration] - [Security] 메뉴 이동 > 'Client Registration Code' 확인

선택 관리자: 명령 프롬프트

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\colleague1\Downloads

C:\Users\colleague1\Downloads>msiexec.exe /i test.msi /qn /norestart /L*v "C:\Agentinstall.txt"

C:\Users\colleague1\Downloads>
```

### 1.2.1 클라이언트 등록 코드 비활성화

```
# 설치 프로그램 경로 지정 후 설치
msiexec.exe /i "C:\Path\To\PolicyInstaller.msi" /qn /norestart /L*v "C:\Temp\AgentInstall.log"
```

```
# 설치 프로그램 다운로드 URL 지정 후 설치
msiexec /i "https://IP or FQDN/hostpkg/pkg.php?pkg=PolicyInstallerLink.msi" /qn /norestart /L*v "C:\Temp\AgentInstall.log"
```

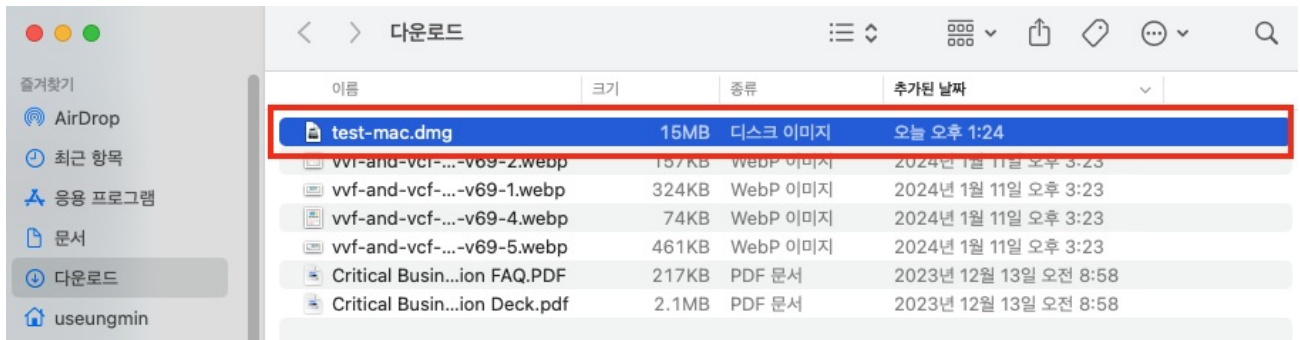
### 1.2.2 클라이언트 등록 코드 활성화

```
# 설치 프로그램 경로 지정 후 설치
msiexec.exe /i "PolicyInstaller.msi" B9_REGISTRATION_CODE=등록 코드goeshere /qn /norestart /L*v "C:\Temp\AgentInstall.log"
```

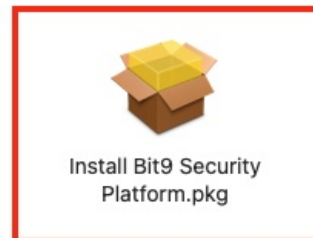
```
# 설치 프로그램 다운로드 URL 지정 후 설치
msiexec /i "https://YourServer/hostpkg/pkg.php?pkg=PolicyInstallerLink.msi" B9_REGISTRATION_CODE=등록 코드 /qn /norestart /L*v "C:\Temp\AgentInstall.log"
```

## 2. MAC 에이전트 설치

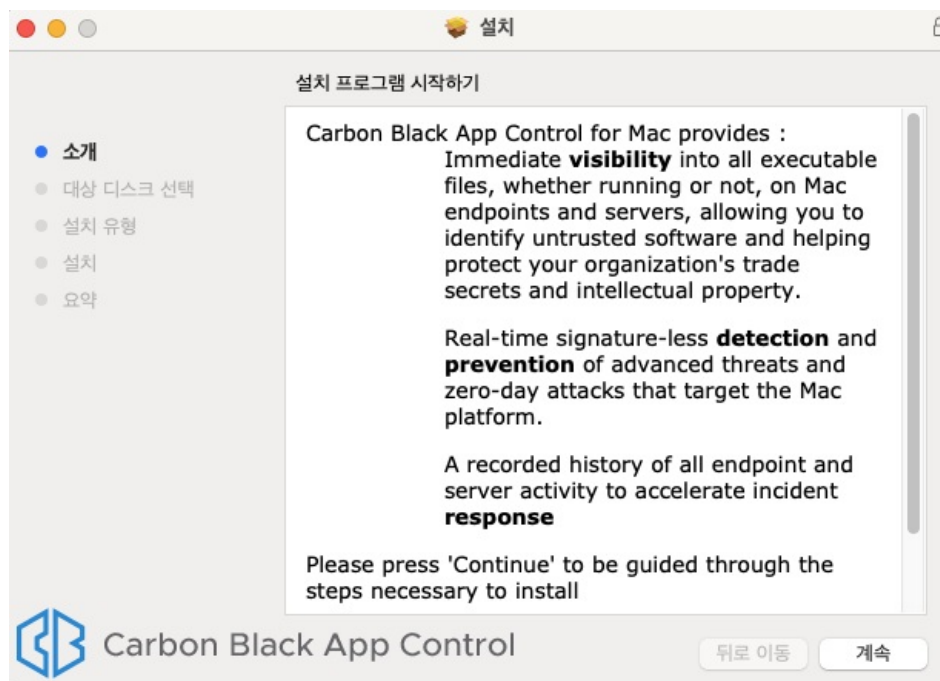
## 2.1 GUI 설치



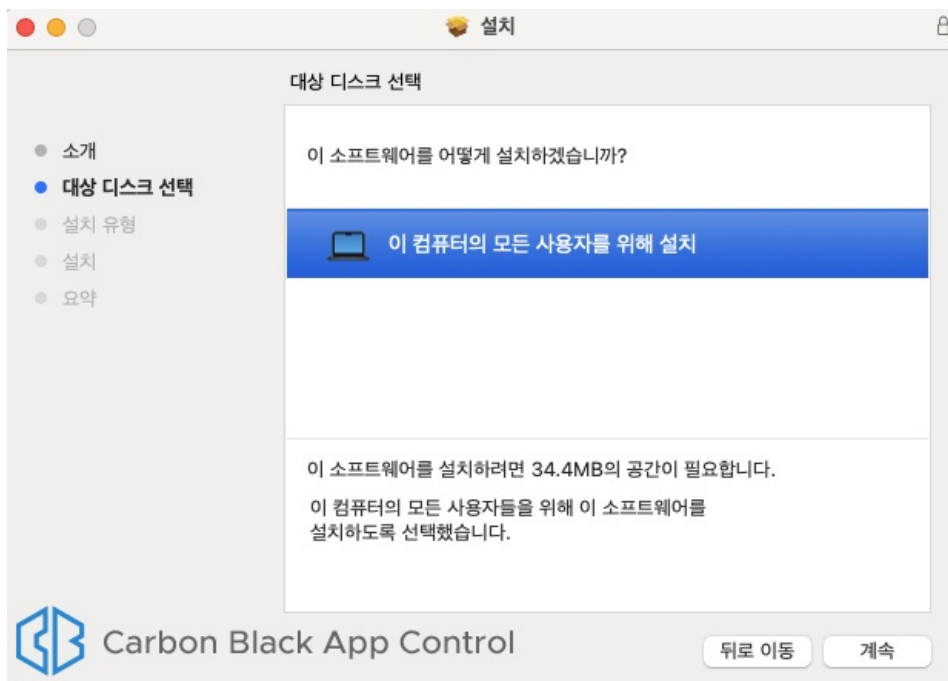
- 사용자 PC에서 다운로드 받은 'App Control 에이전트 (정책명.dmg)' 실행



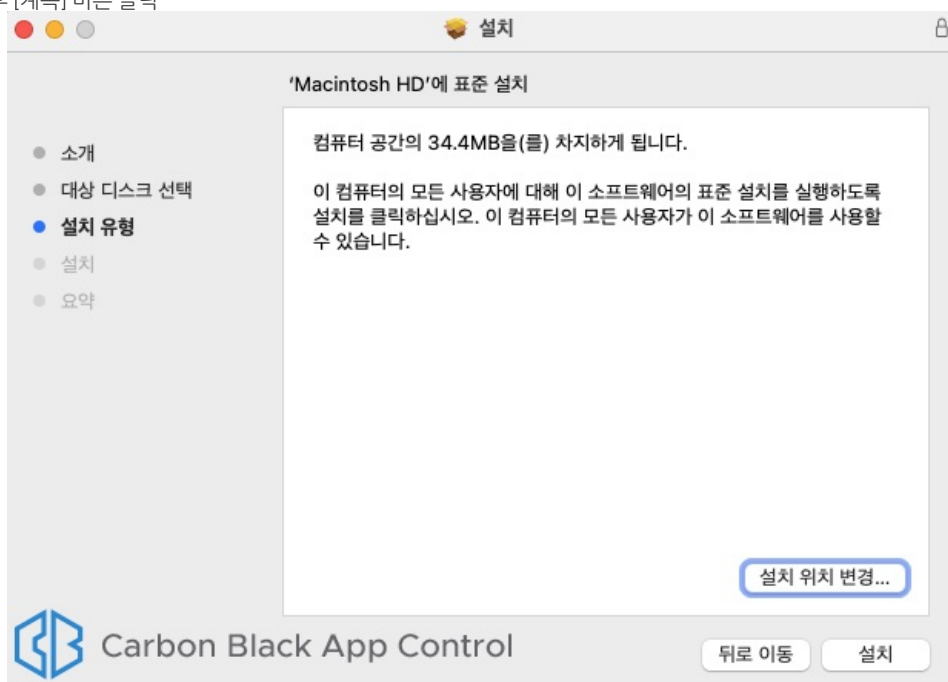
- 'Install Bit9 Security Platform.pkg' 파일 더블클릭하여 실행



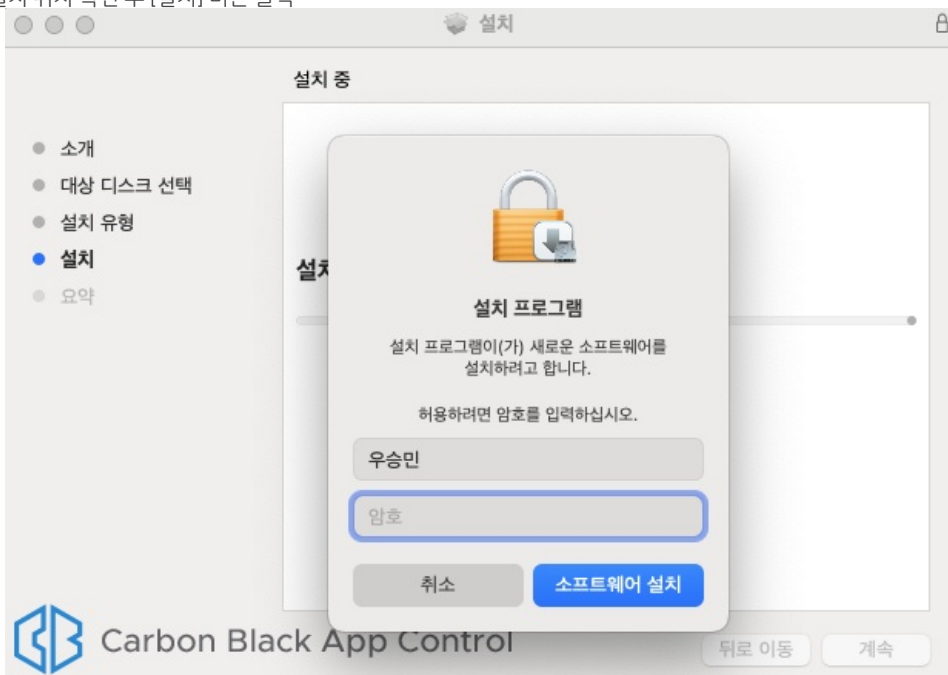
- [계속] 버튼을 클릭하여 설치 프로그램 시작



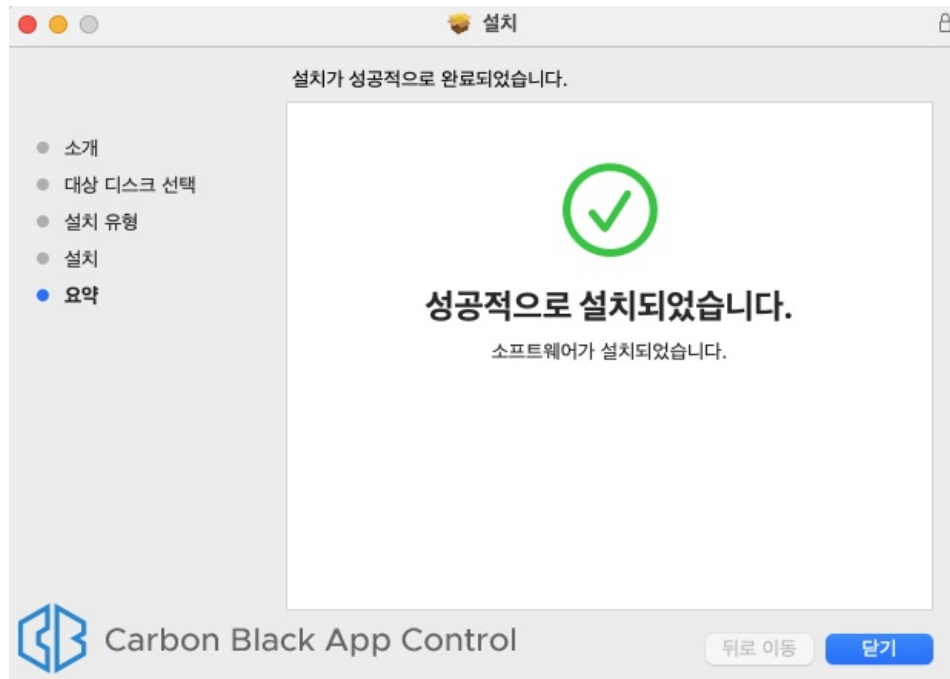
- 설치 유형 확인 후 [계속] 버튼 클릭



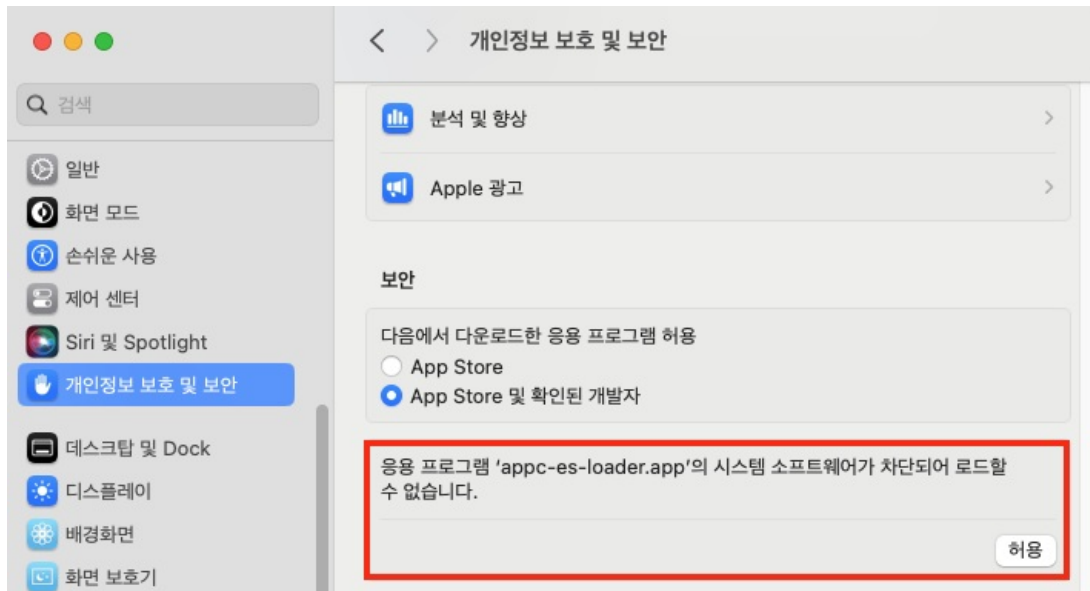
- 설치 사이즈 및 설치 위치 확인 후 [설치] 버튼 클릭



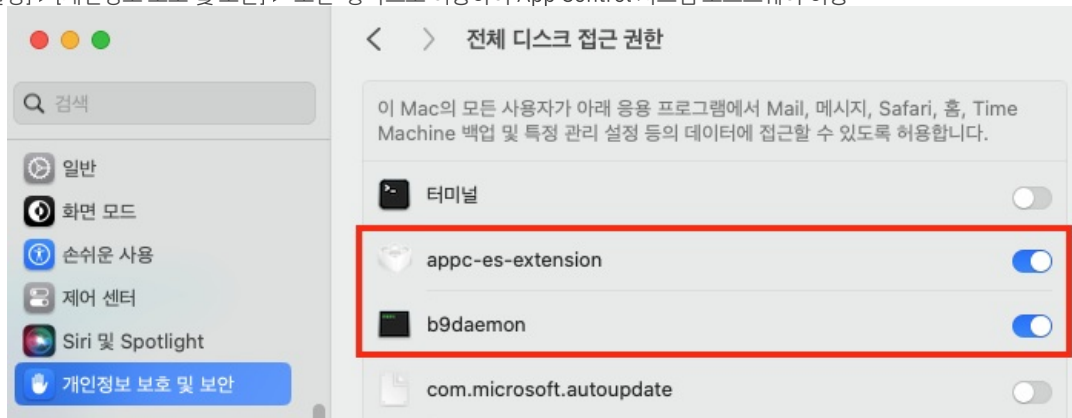
- 사용자 암호 입력 후 [소프트웨어 설치] 버튼 클릭



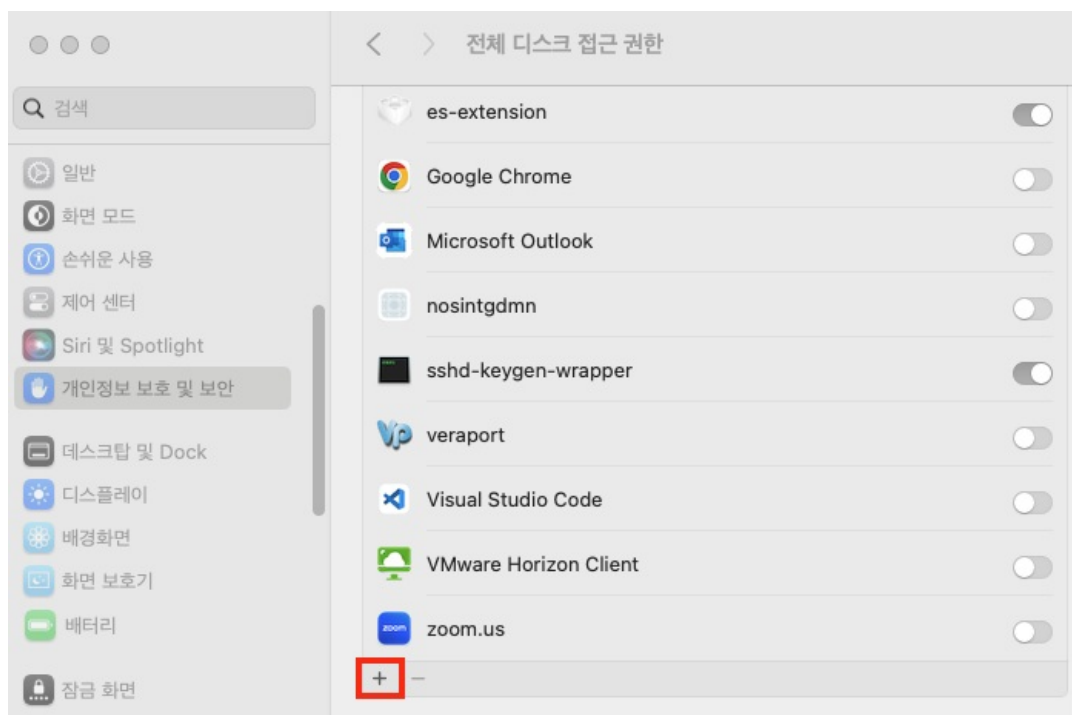
- 설치 완료 확인 후 [닫기] 버튼 클릭하여 설치 프로세스 종료



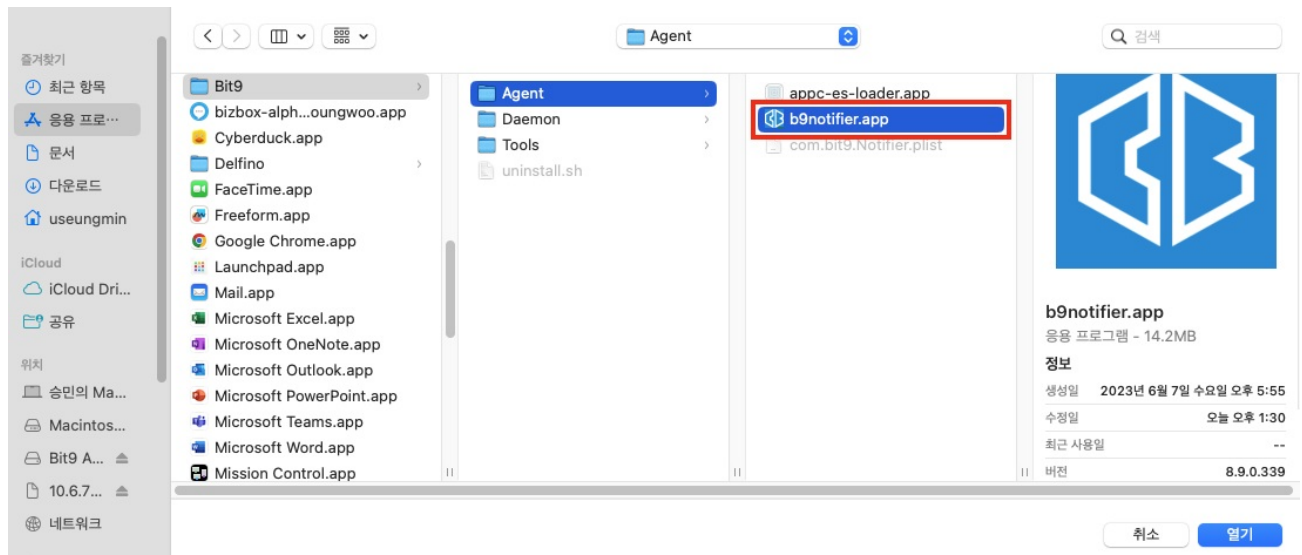
- [시스템 설정] > [개인정보 보호 및 보안] > '보안' 항목으로 이동하여 App Control 시스템 소프트웨어 허용



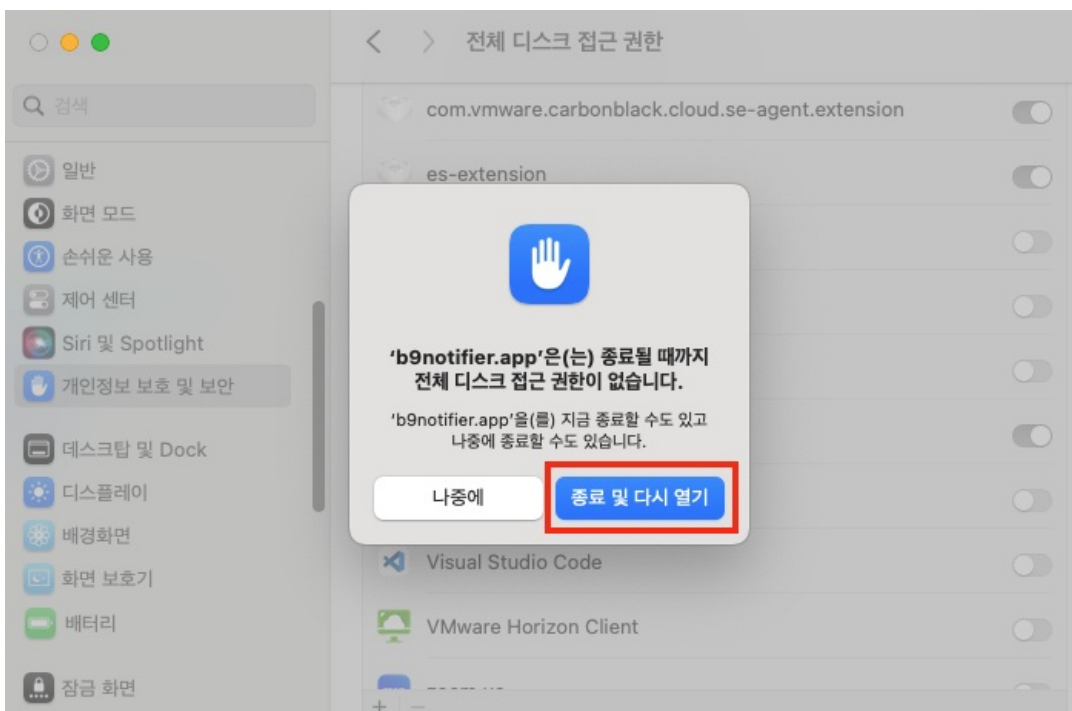
- [시스템 설정] > [개인정보 보호 및 보안] > [전체 디스크 접근 권한] 메뉴로 이동하여 App Control 프로그램 권한 허용



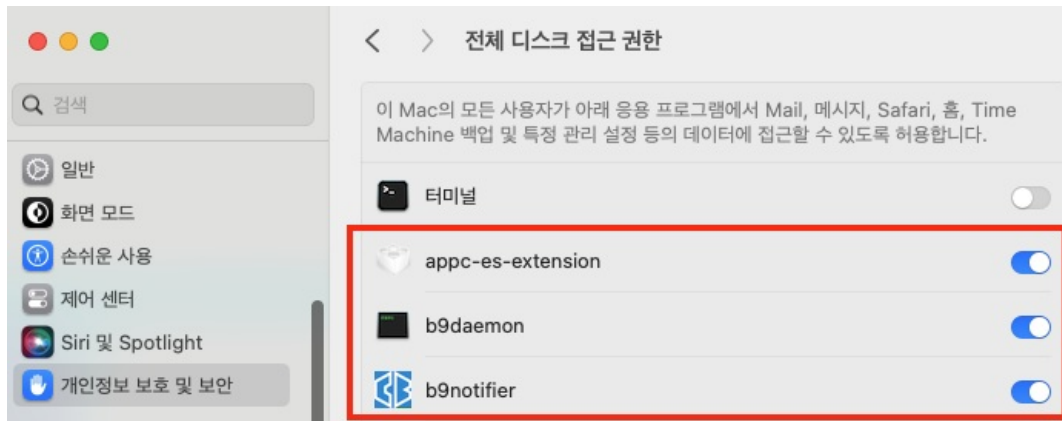
- [시스템 설정] > [개인정보 보호 및 보안] > [전체 디스크 접근 권한] > [+ (추가)] 버튼 클릭



- [팝업창] > [응용 프로그램] > [Bit9] > [Agent] > [b9notifier.app] 선택 및 [열기] 버튼 클릭



- b9notifier.app 프로그램의 전체 디스크 접근 권한을 허용하기 위해 [종료 및 다시 열기] 버튼 클릭



- b9notifier.app 프로그램의 전체 디스크 접근 권한 확인

### 3. Linux 에이전트 설치

에이전트 호환성 : <https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-appc-oer-linuxagent/GUID-CEDA5E05-2D84-4D58-BCD8-0F0FFA517AD2.html>

#### 3.1 CLI 설치

```
useungmin — root@rpm-minion:/tmp/agent — ssh root@10.6.71.11 — 93x16

[root@rpm-minion agent]# wget http://cbac.seungmin.test/hostpkg/pkg.php?php=test-redhat.tgz
--2024-01-17 03:18:23-- http://cbac.seungmin.test/hostpkg/pkg.php?php=test-redhat.tgz
Resolving cbac.seungmin.test (cbac.seungmin.test)... 10.6.71.17
Connecting to cbac.seungmin.test (cbac.seungmin.test)|10.6.71.17|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1525 (1.5K) [text/html]
Saving to: 'pkg.php?php=test-redhat.tgz'

100%[=====] 1,525 --.-K/s in 0s

2024-01-17 03:18:23 (230 MB/s) - 'pkg.php?php=test-redhat.tgz' saved [1525/1525]
```

- Linux 에 App Control 설치 프로그램 업로드 (SSH 또는 Wget 이용)

```
useungmin — root@rpm-minion:/tmp/agent — ssh root@10.6.71.11 — 76x22

[root@rpm-minion agent]# tar -xvzf test-redhat.tgz
test-redhat/server.conf
test-redhat/configlist.xml
test-redhat/configlist_v2.xml
test-redhat/b9install.sh
test-redhat/b9install.asc
test-redhat/bit9cs.asc
test-redhat/bit9cs_sha2.asc
test-redhat/b9agentRedhat6.rpm
test-redhat/b9agentRedhat7.rpm
test-redhat/b9agentRedhat8.rpm
test-redhat/b9agentRedhat9.rpm
test-redhat/b9notifierRedhat6.rpm
test-redhat/b9notifierRedhat7.rpm
test-redhat/b9notifierRedhat8.rpm
test-redhat/b9notifierRedhat9.rpm
[root@rpm-minion agent]#
```

- 설치 프로그램 압축 해제

```

useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 96x24
[root@localhost test-redhat]# gpg --dearmor bit9cs_sha2.asc
[root@localhost test-redhat]# gpg --no-default-keyring --homedir . --keyring bit9cs_sha2.asc.gpg
--verify b9install.asc b9install.sh
gpg: WARNING: unsafe permissions on homedir '/home/test-redhat'
gpg: Signature made Mon Nov 27 21:41:04 2023 KST
gpg: using RSA key E7892ECDFDC509C6
gpg: /home/test-redhat/trustdb.gpg: trustdb created
gpg: Good signature from "build (carbonblack) <contact@carbonblack.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 3567 6AEE 452F 91A6 0D2F 4A43 E789 2ECD FDC5 09C6

```

- gpg키 인증 통한 설치 스트립트 유효성 검사  
- "Good signature from "build (carbonblack)"" 메시지 확인

버전 별 Public Key 다운로드 : <https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-ac-announcements/GUID-123F59D1-E2C4-431F-8CEE-5D924CF83F13.html>

```

useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 98x26
[root@localhost test-redhat]# sh ./b9install.sh -n
Installing App Control agent package

Starting the App Control Daemon
Completed agent install on Thu, 18 Jan 2024 10:41:34 +0900

Running scriptlet: nss-3.90.0-4.el8.x86_64 9/9
Running scriptlet: b9agent-8.7.20-1.el8.x86_64 9/9
Verifying : nspr-4.35.0-1.el8.x86_64 1/9
Verifying : nss-3.90.0-4.el8.x86_64 2/9
Verifying : nss-softokn-3.90.0-4.el8.x86_64 3/9
Verifying : nss-softokn-freebl-3.90.0-4.el8.x86_64 4/9
Verifying : nss-sysinit-3.90.0-4.el8.x86_64 5/9
Verifying : nss-util-3.90.0-4.el8.x86_64 6/9
Verifying : libicu-60.3-2.el8_1.x86_64 7/9
Verifying : unzip-6.0-46.el8.x86_64 8/9
Verifying : b9agent-8.7.20-1.el8.x86_64 9/9

Installed:
b9agent-8.7.20-1.el8.x86_64 libicu-60.3-2.el8_1.x86_64
nspr-4.35.0-1.el8.x86_64 nss-3.90.0-4.el8.x86_64
nss-softokn-3.90.0-4.el8.x86_64 nss-softokn-freebl-3.90.0-4.el8.x86_64
nss-sysinit-3.90.0-4.el8.x86_64 nss-util-3.90.0-4.el8.x86_64
unzip-6.0-46.el8.x86_64

Complete!

```

- 설치 진행 및 설치 완료

```

useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 98x26
[root@localhost test-redhat]# systemctl status b9daemon.service
● b9daemon.service - AppC b9daemon service
   Loaded: loaded (/usr/lib/systemd/system/b9daemon.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-01-18 10:41:34 KST; 4min 3s ago
 Main PID: 2444 (b9daemon)
    Tasks: 36 (limit: 49612)
   Memory: 1.0G
    CGroup: /system.slice/b9daemon.service
            └─2444 /opt/bit9/bin/b9daemon

Jan 18 10:41:30 localhost.localdomain systemd[1]: Starting AppC b9daemon service...
Jan 18 10:41:30 localhost.localdomain b9daemon[2370]: b9daemon called by start
Jan 18 10:41:30 localhost.localdomain b9daemon[2370]: Checking b9k_87201 Driver
Jan 18 10:41:30 localhost.localdomain b9daemon[2370]: Looking if modules directory is updated
Jan 18 10:41:34 localhost.localdomain b9daemon[2370]: insmod /lib/modules/4.18.0-193.el8.x86_64>
Jan 18 10:41:34 localhost.localdomain b9daemon[2370]: insmod /lib/modules/4.18.0-193.el8.x86_64>
Jan 18 10:41:34 localhost.localdomain b9daemon[2370]: Starting b9daemon: [ OK ]
Jan 18 10:41:34 localhost.localdomain systemd[1]: Started AppC b9daemon service.

```

- 센서 동작 확인

```
useungmin — root@localhost:/home/test-redhat — ssh root@10.6.71.112 — 98x26
[root@localhost test-redhat]# ps aux | grep b9
root      2431  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-WatchdogServ]
root      2432  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-ContextManag]
root      2433  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-DeviceTracki]
root      2434  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-ProcessTrack]
root      2435  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-DirtyTrackin]
root      2436  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-RefCountClea]
root      2437  0.0  0.0      0      0 ?        S    10:41   0:00 [b9-restart-daem]
root      2444  5.7  1.1 2528696 92604 ?        Ssl  10:41   0:45 /opt/bit9/bin/b9daemon
root      11128  0.0  0.0    9180    972 pts/0    S+   10:54   0:00 grep --color=auto b9
```

- 에이전트 프로세스 동작 확인

🔄버전 #17  
★생성 15 1월 2024 13:34:35  
✍수정 18 4월 2025 17:06:16