

# macOS tamper protection using Jamf extension attributes

Updated on 16 Aug 2024 • 1 Minute to read

The Cyberhaven Sensor has built-in checks that are automatically reported on the Endpoints Sensors page in the Cyberhaven Console. The platform reports the status of the endpoints where the integrity self-check has failed on the Endpoint Sensors page.

The steps described in this article are optional and only required when you want to provide additional protection and automated remediation actions when the Cyberhaven macOS Sensor was tampered with. While this article is for Jamf, you could adapt it to other MDMs that provide the ability to run scripts.

1. Create an extension attribute in Jamf using the script located at `/Applications/Cyberhaven.app/Contents/Resources/status.sh` (you can obtain this script from a valid install of Cyberhaven or by downloading it from [here](#) script. The script will output **ERROR** if the user tampered with the installation, or **OK** otherwise.

## Cyberhaven status

**Display Name** Display name for the extension attribute

Enabled (script input type only)

**Description** Description for the extension attribute

Checks that Cyberhaven is active. Can be used to reinstall Cyberhaven if it is inactive.

**Data Type** Type of data being collected

**Inventory Display** Category in which to display the extension attribute in Jamf Pro

**Input Type** Input type to use to populate the extension attribute

```
1 #!/bin/bash
2
3 set -o pipefail
4 set -e
5 #set -x
6
7
8 trap 'cleanup $? $LINENO' ERR
9
10 cleanup() {
11     echo "<result>ERROR</result>"
12     exit 1
13 }
14
15
16 if [ $UID -ne 0 ]; then
17     echo "Please run this script as root (with sudo)"
18     exit 1
19 fi
20
21 FILE_SENSOR_ID="io.cyberhaven.lightbeam.FileOperationsSensor"
```

2. Create a Smart Group and select the extension attribute "Cyberhaven status" you just created and the ERROR value as the criteria.

# ← Cyberhaven reinstall

- Options
- Scope
- Self Service
- User Interaction

Show in Jamf Pro Dashboard



General >



Packages  
1 Package

## General

**Display Name** Display name for the policy

Cyberhaven reinstall

Enabled

**Category** Category to add the policy to

None ▾

**Trigger** Event(s) to use to initiate the policy

Startup

When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

Login

When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

Logout

When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

Network State Change

When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

Enrollment Complete

Immediately after a computer completes the enrollment process

Recurring Check-in

At the recurring check-in frequency configured in Jamf Pro

Custom

At a custom event

**Execution Frequency** Frequency at which to run the policy

Once per computer ▾

3. Finally, select the smart group you just created in the scope.

Computers : Policies

## ← Cyberhaven reinstall

Options **Scope** Self Service User Interaction

---

Targets Limitations

**Target Computers**  
Computers to deploy the policy to  
Specific Computers ▼

**Target Users**  
Users to deploy the policy to  
Specific Users ▼

TARGET	TYPE
Cyberhaven needs reinstall	Smart Computer Group

Now Cyberhaven will automatically be reinstalled on all computers where the Cyberhaven installation was tampered with.

← Previous  
Advanced Tamper Protection for Windows and...

Next →  
Uninstalling the Sensor with 'Uninstall Protect...