Objective-See
a non-profit 501(c)(3) foundation.

tools

blog

Support Us!

OverSight

This website uses cookies to improve your experience.   Okay!

Mac malware often spies on users by recording audio and video sessions...sometimes in an **undetected** manner.

OverSight monitors a mac's mic and webcam, alerting the user when the internal mic is activated, or whenever a process accesses the webcam.

↓ **download**

🖥️ **Supported OS:** `macOS 12+`

⚙️ **Current version:** `2.2.2` (**change log**)

🔓 **Zip's SHA-1:** `205FBEFA6888CE1E76A5A53B1D4B65FEAA87D89E`

📄 **Source Code:** **OverSight**

Looking for an older version (compatible with older versions of macOS)?

Start here!

One of the most insidious actions of malware, is abusing the audio and video capabilities of an infected host to record an unknowing user. Macs, of course, are not immune; malware such as `FruitFly`, `Crisis`, `Mokes`, and others, all attempt to spy on Mac users. OverSight constantly monitors a system, alerting a user whenever the internal microphone is activated, or the built-in webcam is accessed. And yes, while the webcam's LED will turn on whenever a session is initially started, new research has shown that malware can surreptitious piggyback into such existing sessions (FaceTime, Skype, Google Hangouts, etc.) and record both audio and video - without fear of detection.
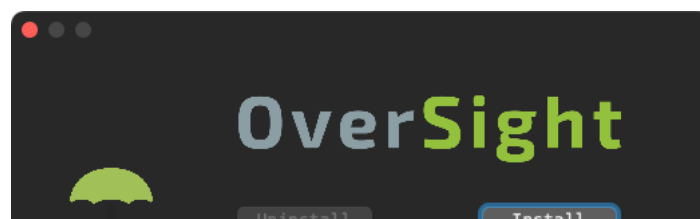
INSTALLING OVERSIGHT

Note:
Due to the mechanism used by OverSight to monitor for mic and webcam access, it can only be installed for accounts with **administrative privileges** (which is the default for accounts on macOS).

To install OverSight, first **download** the zip archive containing the application. Depending on your browser, you may need to manually unzip the application by double-clicking on the zipped archive:
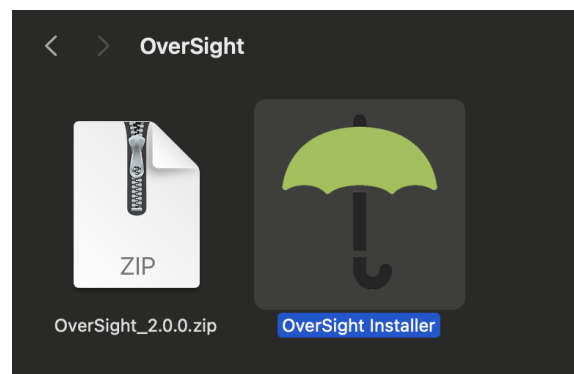
Then, simply double-click on `'OverSight_Installer.app'`. Click "Install" to install the tool (or "Upgrade" if you have an older version already installed):


This website uses cookies to improve your experience.

OverSight can also be installed via the command-line. Just execute the installer application with the `-install` flag:

```
//install
$ sudo OverSight_Installer.app/Contents/MacOS/OverSight_Installer -install
OVERSIGHT: install ok!
```

As part of the installation process, you might be prompted by macOS to all OverSight to show notifications and alerts. OverSight should be allowed, this is the mechanism that it used to notify you whenever something accesses the mic or webcam!
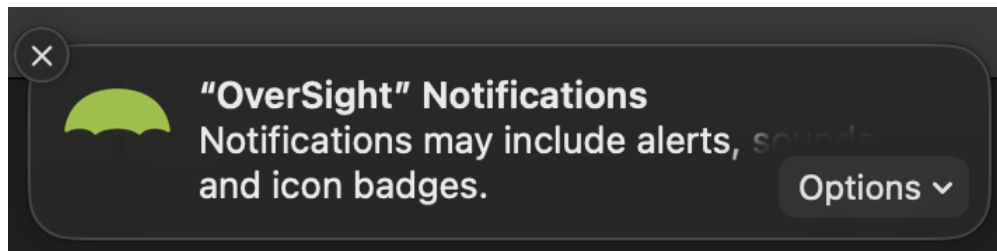

Moreover, one recent versions of macOS, you will have to manually set OverSight's notification style to "Alerts" via the System Preference application:
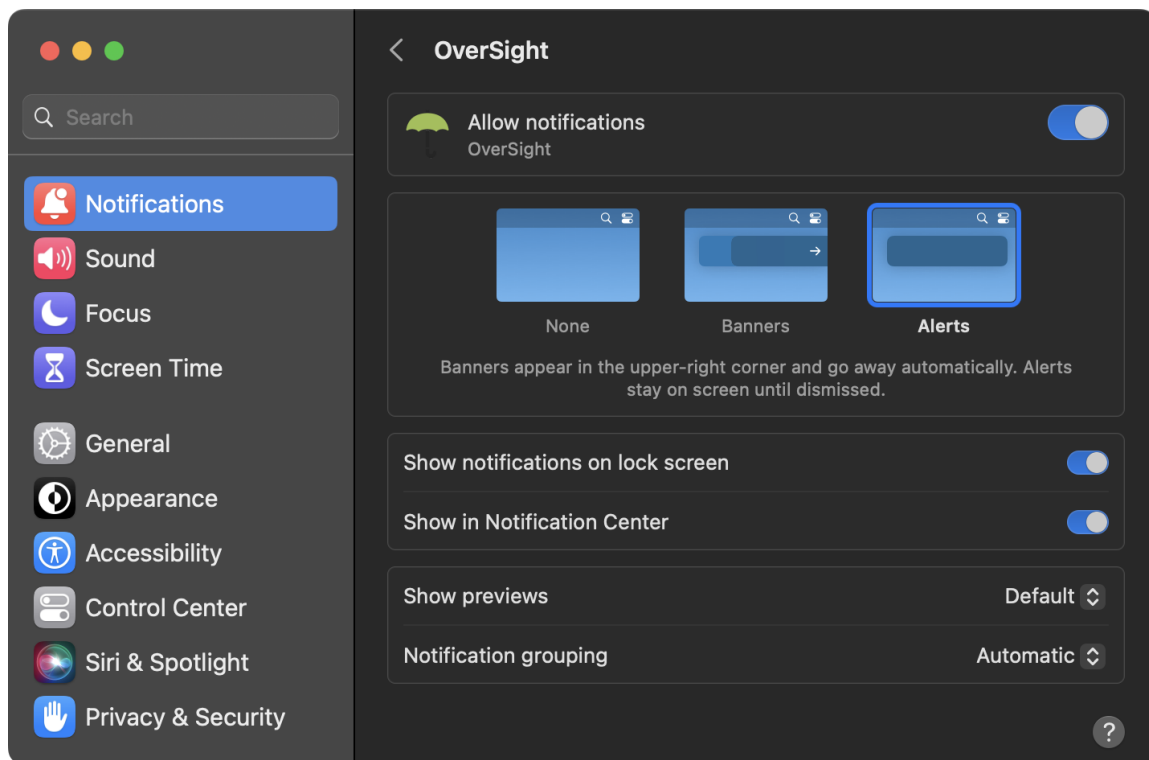

🚧 USING OVERSIGHT (ALERTS)

Once OverSight is installed, it will be running and is set to automatically start each time you log in. By default, when running OverSight adds an icon (☂) to the status menu. Clicking on this icon will display a menu with various information and configuration options:
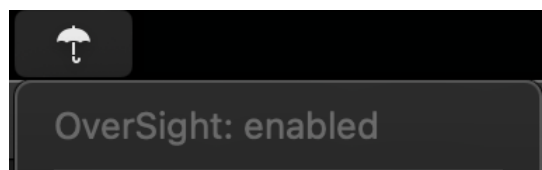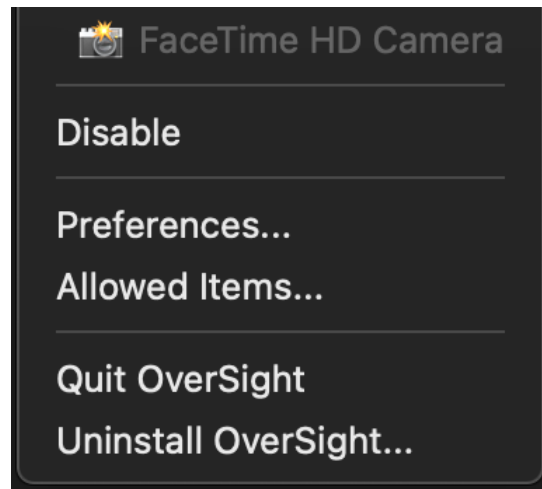
While OverSight is running, anytime the internal microphone is activated, or a process accesses the built-in webcam, OverSight will alert you of this fact.

Below is an example of an OverSight camera alert, generated when an application (Zoom) has activated the webcam:
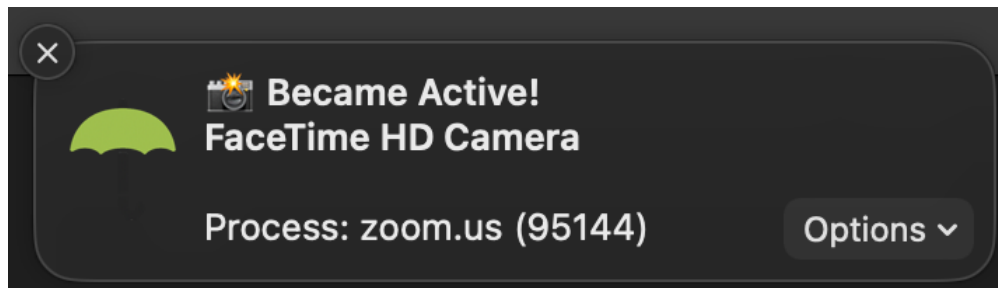
> **Note:**
> In some cases OverSight cannot identify the process responsible for activating the mic or webcam. When this (rarely?) occurs, a more generic alert will be shown.

The alert will contain the name of the device (mic or camera that triggered the event, as well as the name and process identifier of the process responsible for the alert (i.e. 'Zoom'). Clicking on "Options" in the notification allows one to either allow the process once, allow it always, or terminate it via the 'Block' option.
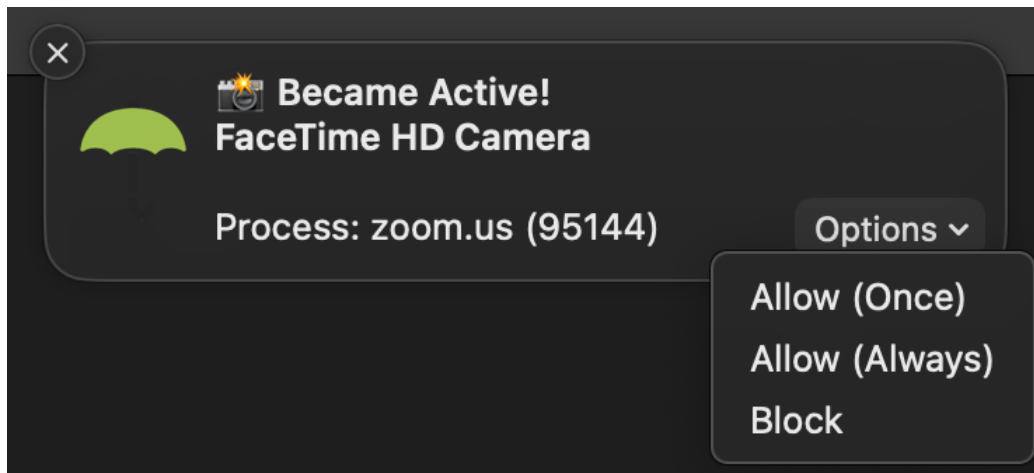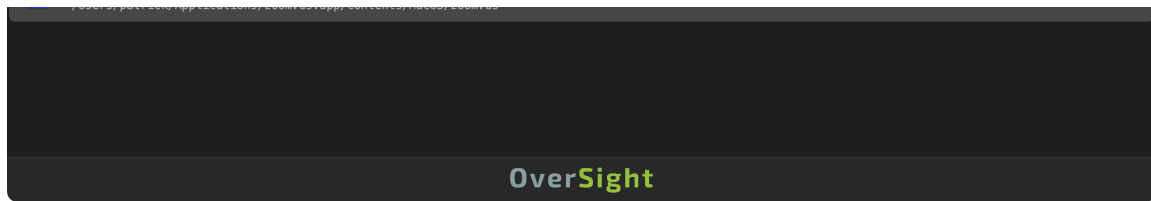

Clicking "Allow (Always)" ensure instruct OverSight to ignore future device access (e.g. the camera) for that specific application.

USING OVERSIGHT (RULES)

Any approved applications can be viewed via OverSight's "Allowed Items..." menu option:

This website uses cookies to improve your experience.

To remove any approved application, simply click the 'x' button in its row.

⚙ USING OVERSIGHT (PREFERENCES)

In order to configure OverSight, simply click on its icon (⬆) in the status menu. Then click on 'Preferences...':

This preferences window will also be shown if you run `OverSight.app` from the `/Applications` folder.

- Start at Login:
  This preference specifies whether OverSight should be started automatically at login, or not. This preferences is on by default meaning OverSight will provide continual protection.

- No Icon Mode:
  By default, OverSight will create an (⬆) in the status menu. Enabling this preferences will remove this icon, though OverSight will still be running, providing protection. If you wish to re-enable the status bar menu icon, run `OverSight.app` from the `/Applications`, and uncheck this preference.

- Ignore External Devices:
  This preference specifies whether or not OverSight will alert you when external mics or cameras are activate/deactivated.

- Disable 'Inactive' Alerts:
  When this preference is checked, OverSight will not display an alert when a mic or camera is deactivated.

Clicking on the "View Allowed Items" button will open a window that displays all allowed applications.

The "Action" tab of the OverSight's preferences window allow you to specify an script of binary that will be

Note:

The specified binary or script is executed via the shell.

If you enable the "Pass Arguments" option, OverSight will pass various parameters (such as device and process that triggered the event). This can be useful if your script/binary needs to different actions based on type of event.

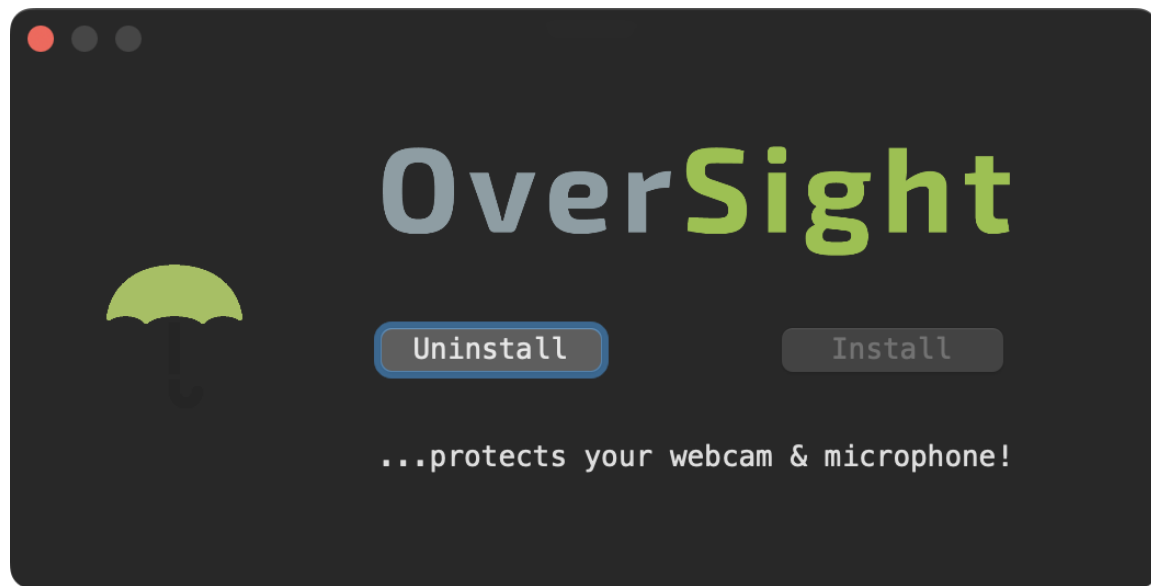Finally, the "Update" tab allow you to disable the check for new versions of OverSight.

🖥 UNINSTALLING OVERSIGHT

To uninstall OverSight, select the "Uninstall OverSight..." from its Status Bar menu:
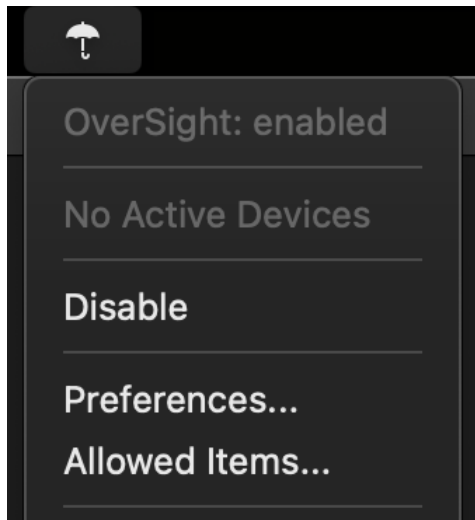
...this will launch the uninstaller:

Clicking the 'Uninstall' button will both stop and remove OverSight from your Mac. OverSight can also be uninstalled via the command-line. Just execute the installer application with the `-uninstall` flag:

```
//uninstall
$ sudo OverSight_Installer.app/Contents/MacOS/OverSight_Installer -uninstall
OVERSIGHT: uninstall ok!
```

FAQs

Q: Are there versions of OverSight compatible with older versions of macOS?

A: While the currently version requires macOS 12+ (due to changes by Apple), older versions of OverSight work on previous versions of macOS. Please note, they however are not officially (still) supported:

- macOS 10.15+: **Version 2.0.2**
- pre-macOS 10.15: **Version 1.2.0**

Q: OverSight tells me there's an update, but the update isn't compatible with my version of macOS?

A: Due to changes in macOS, the current version of OverSight requires macOS 12+. And while newer versions of OverSight will take your version of macOS into account when checking for an update, older versions do not.

If possible it is (from a security point of view), recommended to upgrade to the latest versions of macOS - which OverSight is compatible with. If this is not an option, you can turn off automatic updates checks via OverSight's preferences.

Q: How can I tell if OverSight is installed and running?

A: When started, OverSight adds an icon (☂) to the status menu. The presence of this icon, indicates that the process is running (unless you've told it to run in 'No Icon' mode). One can also check if it's running, via the `Activity Monitor.app`, just look for a running process named `OverSight.app`.

Q: Why can't OverSight detect what process is using the mic/webcam?

A: While there is no direct way to determine what process is using the webcam or mic, OverSight can almost always figure this via indirect means. If it fails to identify any process (but can still detect that the webcam/mic was activated), Oversight will still generate a notification stating the device was activated. However, this notification will not contain any process information, nor of course, the ability to 'allow'/'block' the process.

Q: How is OverSight different than other tools (such as MicroSnitch)?

A: OverSight is unique in a variety of ways:

When your webcam's LED light randomly comes on, you'd want to know what process triggered that, right?

- OverSight provides the means to either 'allow' or 'block' a process that is accessing the mic/webcam

- OverSight allows one to "approve a" process, allowing access to either the mic or webcam without any subsequent alerts

- OverSight can detect secondary 'consumer' processes that may be piggy-backing off a legitimate webcam session in order to stealthily record the user without detection. (See: **"Getting Duped: Piggybacking on Webcam Streams for Surreptitious Recordings"** for details on this novel attack).

Q: Any other questions?

A: Feel free to shoot us an email at **contact@objective-see.com**.

This website uses cookies to improve your experience.