Application Security

Objectives:

At the end of this episode, I will be able to:

1. Describe macOS security features including gatekeeper, application sandboxes, and digital signatures.
2. Describe and configure macOS privacy controls.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Application Security

    - Digitally Signed
    - 64-bit
    - Bundles

        - Bundles can contain anything
        - Related files grouped together into a single file
        - `*.app`
        - Can easily be copied into `/Applications` eliminating the need for an installer
        - `app` files are really just folders with an icon
        - `Ctrl-Click -> Show Package Contents`

- GateKeeper

    - Restricts which apps are allowed to run
    - `System Preferences -> Security & Privacy -> General`

        - App Store
        - App Store and identified developers

    - Can be overridden by an administrator

        - Control-Click -> Open

- Application Sandboxing

    - Protected memory

        - A sandboxed application has a protected memory space
        - No other application is allowed to access that space
        - Ensures one application cannot crash another

    - Preferences / Application Support isolation

        - Files associated with the application are removed from the common locations to isolated locations on the drive
        - Old - `/Users/username/Library/Preferences`
        - New - `/Users/username/Library/Containers/<application>/Data/Library/Preferences`

- Privacy Controls

    - `Apple Menu` -> `System Preferences` -> `Security & Privacy` -> `Privacy`
    - Enable/Disable Location Services
    - Control which apps can access contacts, calendars, and reminders
    - Enable accessibility access for apps

- System Information

    - `/Applications/Utility/System Information`
    - Displays data regarding your system
    - *Software* section details all installed software