

FROM 🤖 TO 😊 EASING THE PAIN OF MAC SOFTWARE UPDATES

How the Orchard infrastructure keeps OS X
applications patched and secure, automatically

Ben Goodstein

Senior Systems Administrator

NSMS Unix Services Team

ben.goodstein@it.ox.ac.uk

twitter: @fuzzylogiq

github: fuzzylogiq

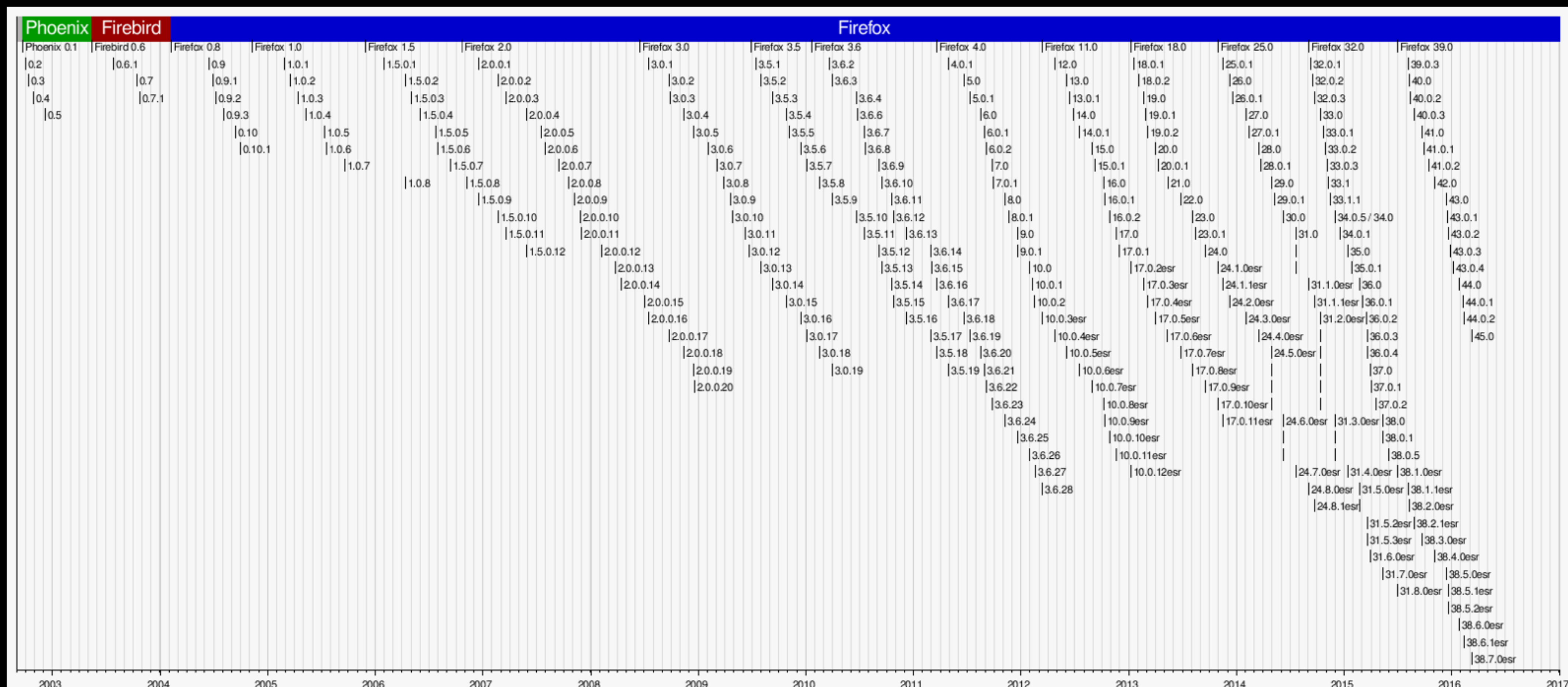
THE (GOOD OLD) BAD OLD DAYS

- Applications infrequently updated
- Physical media
- Security less of a concern for app developers and Mac admins
- Smaller catalogue of software to maintain
- Yearly refresh with updated image with software manually updated was considered sufficient

THE CURRENT ZEITGEIST

- Agile development means important app updates released regularly
- Security of prime concern to app developers and, increasingly, Mac admins
- Apple themselves releasing OS updates more regularly with critical security fixes
- Customers expect and want new features faster

FIREFOX RELEASES 2003-2017



DOING IT ALL BY HAND

- Manual download
- Manual packaging
- Copy to clients or bake into image
- Slow and frustrating

WHAT'S NEEDED?

- Inventory
- Packaging
- Testing
- Installation & Updating
- Automation

INVENTORY

- Needs to be regularly updated and accurate
- Needs to describe computer's location, ownership, hardware and software usefully
- JSS, Sal, Absolute Manage, Filewave

PACKAGING

- Needs to be repeatable with predictable results
- GUI: Whitebox Packages, JAMF Composer
- Command line: The Luggage, autopkg, pkgbuild

INSTALLATION & UPDATING

- Needs to work closely with inventory to ensure it's always up-to-date
- Must be aware of app versions and intelligently assess need for updates
- munki, JSS, Filewave, etc.

TESTING

- Updates can break functionality
- Need internal and user testing
- Various methods: testing/production, unstable/testing/stable etc.
- JSS, munki, Google Experiments

ORCHARD INFRASTRUCTURE

- JSS (a.k.a. Casper) for inventory
- autopkg for packaging
- munki (the Orchard Software Centre) for installation & updating
- plus some magic to glue it all together



JSS (A.K.A. CASPER)

- Great for inventory, MDM (mobile device management), settings management & imaging
- Easy to use web-based front end
- Comprehensive REST API



JSS (A.K.A. CASPER)

- Not so great for software packaging or patching
- No built-in concept of 'release channels' for staging and testing updates
- Laborious import process
- MYSQL string comparisons of application version numbers 😞



AUTOPKG

- Reliably and repeatably downloads and packages software using 'recipes'
- Open source
- Recipes are reusable, configurable, extensible
- Large community
- Command-line client - GUI 'autopkgr' available



AUTOPKG

- Reasonably idempotent
- Integrates well with munki
- Flat file format (plists) allows easy Git collaboration
- Easy automation (hence the name!)
- Steep learning curve

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Description</key>
  <string>Download recipe for Firefox. Finds and downloads a Firefox release.
Values for RELEASE correspond to directories here: http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/
Some useful values are: 'latest', 'latest-10.0esr', 'latest-esr', 'latest-3.6', 'latest-beta'
LOCALE corresponds to directories at http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/$RELEASE/mac/
Examples include 'en-US', 'de', 'ja-JP-mac', 'sv-SE', and 'zh-TW'
No idea if all Firefox builds are available in all the same localizations, so you may need to verify that any particular
combination is offered.</string>
  <key>Identifier</key>
  <string>com.github.autopkg.download.firefox-rc-en_US</string>
  <key>Input</key>
  <dict>
    <key>RELEASE</key>
    <string>latest</string>
    <key>LOCALE</key>
    <string>en_US</string>
    <key>NAME</key>
    <string>Firefox</string>
  </dict>
  <key>MinimumVersion</key>
  <string>0.2.0</string>
  <key>Process</key>
  <array>
    <dict>
      <key>Arguments</key>
      <dict>
        <key>product_name</key>
        <string>firefox</string>
        <key>release</key>
        <string>%RELEASE%</string>
        <key>locale</key>
        <string>%LOCALE%</string>
      </dict>
      <key>Processor</key>
      <string>MozillaURLProvider</string>
    </dict>
    <dict>
      <key>Arguments</key>
      <dict>
        <key>filename</key>
        <string>%NAME%.dmg</string>
      </dict>
      <key>Processor</key>
      <string>URLDownloader</string>
    </dict>
    <dict>
      <key>Processor</key>
      <string>EndOfCheckPhase</string>
    </dict>
  </array>
</dict>
</plist>
```




MUNKI (THE ORCHARD SOFTWARE CENTRE)



- Great for software installation and patching
- Open source (so customisable)
- Repo is just a collection of packages and metadata on a web server



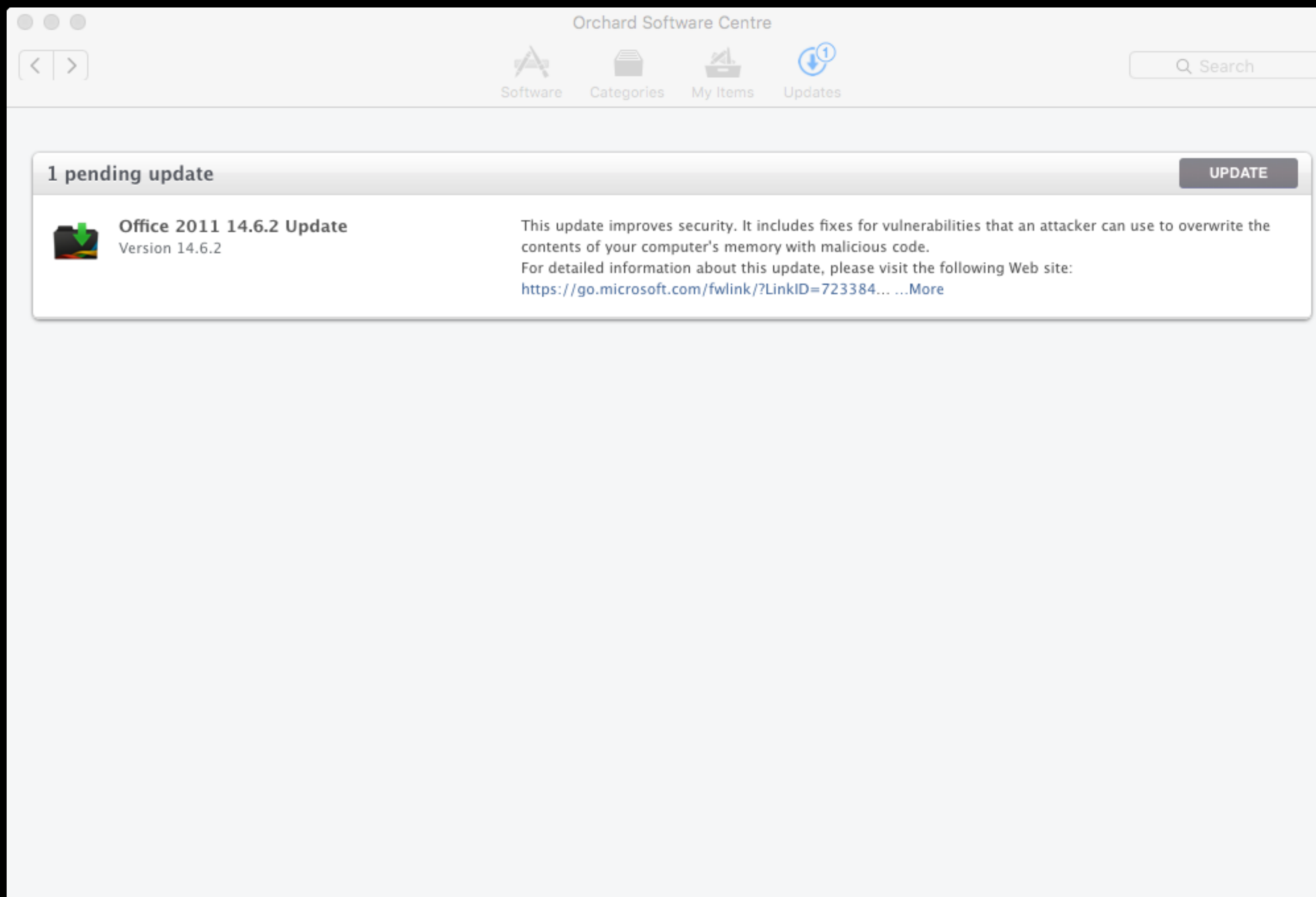
MUNKI (THE ORCHARD SOFTWARE CENTRE)



- 'Magic' is done on client
- Catalogs and Manifests
 - Catalogs list all software available to computer
 - Manifests detail what should be installed from catalogs
- Familiar user interface for optional installs
- Many other useful features – steep learning curve for the admin



MUNKI (THE ORCHARD SOFTWARE CENTRE)



BRINGING IT ALL TOGETHER

- manana to allow the JSS to inform munki's decisions
- munki-staging for automating testing stages

MANANA

- manana dynamically changes munki manifest client receives from server based on JSS computer record
- deliver software based on inventory
- munki preflight/postflight ensures integrity with inventory

MANANA

<input type="checkbox"/>	Computer Attribute Mapping
<input type="checkbox"/>	If Group matches Location: Saïd Business School: Sainsbury Library then add manifest: sbs_library_customisations
<input type="checkbox"/>	If Group matches BSG-ROQ-AV Mac Minis then add manifest: bsg_av_customisations
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add manifest: orchard_testing
<input type="checkbox"/>	If Site matches IT Services – ITLP then add manifest: itservices_itlp_site_customisations
<input type="checkbox"/>	If Site matches Department of Computer Science (DCS) then add manifest: dcs_site_customisations
<input type="checkbox"/>	If Site matches NSMS then add package: Wireshark to optional_installs
<input type="checkbox"/>	Extension Attribute: If Software: Adobe Creative Cloud Licence matches Orchard Device Licence then add manifest: adobe_creative_cloud_device
<input type="checkbox"/>	If Group matches Settings: Management Option MMP (All OS) then add package: Office_2011_Update to managed_updates
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Testing then add catalog: stable
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: stable
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: testing
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: unstable
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Testing then add catalog: testing
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Stable then add catalog: stable



Inventory	Management	History
<div> <div> <i>i</i> General nsms-fargo </div> <div> Hardware 13-inch MacBook Pro (Early 2015) </div> <div> Operating System Mac OS X 10.11.3 </div> <div> User and Location ouit0354 </div> <div> Purchasing </div> <div> Storage 2 Drives </div> <div> Extension Attributes </div> <div> Disk Encryption 1 of 2 Partitions Encrypted </div> <div> Peripherals 0 Peripherals </div> <div> Licensed Software 2 Matches </div> <div> Applications 212 Applications </div> </div> <div> <div>Config: Orchard Software Centre</div> <div>-Auto With User Prompts-</div> <div> Config: Release Channel Stable </div> <div>Config: Sassafra Keyserver</div> <div>-none-</div> <div>Config: Software Installation</div> <div>-On-</div> <div>Config: Software Updates</div> <div>-On-</div> <div>HFS: Host Name</div> <div></div> <div>HFS: Password</div> <div></div> <div>Software: Adobe Acrobat Version</div> <div>-none-</div> <div>Software: Adobe Creative Cloud Licence</div> <div>-None-</div> <div>Software: Adobe CS6 Edition</div> <div>-none-</div> <div>Software: Apple Aperture Version</div> <div>-none-</div> </div>		
<div> <div>Done</div> <div>History</div> <div>Autorun Data</div> <div>Delete</div> </div>		

```
...  
<plist version="1.0">  
<dict>  
  <key>catalogs</key>  
  <array>  
    <string>stable</string>  
  </array>  
...
```


MANANA

<input type="checkbox"/>	Computer Attribute Mapping
<input type="checkbox"/>	If Group matches Location: Saïd Business School: Sainsbury Library then add manifest: sbs_library_customisations
<input type="checkbox"/>	If Group matches BSG-ROQ-AV Mac Minis then add manifest: bsg_av_customisations
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add manifest: orchard_testing
<input type="checkbox"/>	If Site matches IT Services – ITLP then add manifest: itservices_itlp_site_customisations
<input type="checkbox"/>	If Site matches Department of Computer Science (DCS) then add manifest: dcs_site_customisations
<input type="checkbox"/>	If Site matches NSMS then add package: Wireshark to optional_installs
<input type="checkbox"/>	Extension Attribute: If Software: Adobe Creative Cloud Licence matches Orchard Device Licence then add manifest: adobe_creative_cloud_device
<input type="checkbox"/>	If Group matches Settings: Management Option MMP (All OS) then add package: Office_2011_Update to managed_updates
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Testing then add catalog: stable
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: stable
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: testing
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: unstable
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Testing then add catalog: testing
<input type="checkbox"/>	Extension Attribute: If Config: Release Channel matches Stable then add catalog: stable



Inventory	Management	History
General nsms-fargo		
Hardware 13-inch MacBook Pro (Early 2015)		
Operating System Mac OS X 10.11.3		
User and Location ouit0354		
Purchasing		
Storage 2 Drives		
Extension Attributes		
Disk Encryption 1 of 2 Partitions Encrypted		
Peripherals 0 Peripherals		
Licensed Software 2 Matches		
Applications 212 Applications		
Config: Orchard Software Centre -Auto With User Prompts-		
Config: Release Channel Unstable		
Config: Sassafra Keyserver -none-		
Config: Software Installation -On-		
Config: Software Updates -On-		
HFS: Host Name <input type="text"/>		
HFS: Password <input type="text"/>		
Software: Adobe Acrobat Version -none-		
Software: Adobe Creative Cloud Licence -None-		
Software: Adobe CS6 Edition -none-		
Software: Apple Aperture Version -none-		

Done History Autorun Data Delete

```
...  
<plist version="1.0">  
<dict>  
  <key>catalogs</key>  
  <array>  
    <string>unstable</string>  
    <string>testing</string>  
    <string>stable</string>  
  </array>  
...  

```

DEMO

MUNKI-STAGING

- python script – relies on a Trello board
- Manual or automatic staging of packages
- Drag and drop or 'due dates'

USEFUL LINKS

- Casper/JSS - <http://www.jamsoftware.com>
- munki - <https://github.com/munki/munki/wiki>
- munkiadmin - <https://github.com/hjuutilainen/munkiadmin>
- munkiwebadmin - <https://github.com/munki/munkiwebadmin> and <https://github.com/munki/mwa2>
- autopkg - <https://github.com/autopkg/autopkg/wiki>
- autopkgr - <http://www.lindegroup.com/autopkgr>
- munki-staging - <https://github.com/ox-it/munki-staging>
- manana - <https://github.com/ox-it/manana>
- Orchard autopkg recipes - <https://github.com/ox-it/orchard-recipes>