Patch Management

From Nice to Have to Necessity

JAMF NATION LIVE

Agenda

1 | What is Patch Management?

Why do we want to do this?

2 | Patching Software

What are the considerations around patch management? How do we do it with Jamf Pro?

3 | Jamf &

Take a quick look at Installomator and Autopkg

4 | OS Patching

Patching the OS is hard, you want the best experience for the user.

Patch management is the process of distributing and applying updates to software

We **update** for new **features** or to patch the *Common* ***Vulnerabilities*** *and Exposures* **(CVE)**

JAMF NATION LIVE

Security

JAMF NATION LIVE

JAMF NATION LIVE

jamf.com

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets[New] www.itsecdb

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles

External Links :
NVD Website
CWE Web Site

View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :
Go

Google » Chrome : Security Vulnerabilities (Execute Code)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **116** Page : 1 (This Page) 2 3

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Ava
1	CVE-2021-30599	843		Exec Code	2021-08-26	2021-11-30	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.														
2	CVE-2021-30598	843		Exec Code	2021-08-26	2021-11-30	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.														
3	CVE-2021-21224	843		Exec Code	2021-04-26	2021-06-01	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.														
4	CVE-2020-6572	416		Exec Code	2021-01-14	2021-01-21	9.3	None	Remote	Medium	Not required	Complete	Complete	Comp
Use after free in Media in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to execute arbitrary code via a crafted HTML page.														
5	CVE-2020-6537	843		Exec Code	2020-09-21	2021-03-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Type confusion in V8 in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.														
6	CVE-2020-6443	345		Exec Code	2020-04-13	2020-07-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Insufficient data validation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to execute arbitrary code via a crafted HTML page.														
7	CVE-2020-6417			Exec Code	2020-02-11	2020-02-17	4.6	None	Local	Low	Not required	Partial	Partial	Part
Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via a crafted registry entry.														
8	CVE-2019-13735	787		Exec Code	2019-12-10	2019-12-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Out of bounds write in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.														
9	CVE-2019-13726	119		Exec Code Overflow	2019-12-10	2019-12-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Buffer overflow in password manager in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code via a crafted HTML page.														
10	CVE-2019-13725	416		Exec Code	2019-12-10	2019-12-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Use-after-free in Bluetooth in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code via a crafted HTML page.														
11	CVE-2019-13693	416		Exec Code	2019-11-25	2019-11-26	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
Use after free in IndexedDB in Google Chrome prior to 77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.														
12	CVE-2019-5790	190		Exec Code Overflow	2019-05-23	2019-06-28	6.8	None	Remote	Medium	Not required	Partial	Partial	Part
An integer overflow leading to an incorrect capacity of a buffer in JavaScript in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.														
13	CVE-2019-5789	190		Exec Code Overflow	2019-05-23	2020-08-24	9.3	None	Remote	Medium	Not required	Complete	Complete	Comp

Windows Server

JAMF NATION LIVE

jamf.com

macOS devices not able to authenticate to Active Directory due to CVE-2021-42287

English

jamf Solutions Industries Pricing Resources Contact Log in Start Trial

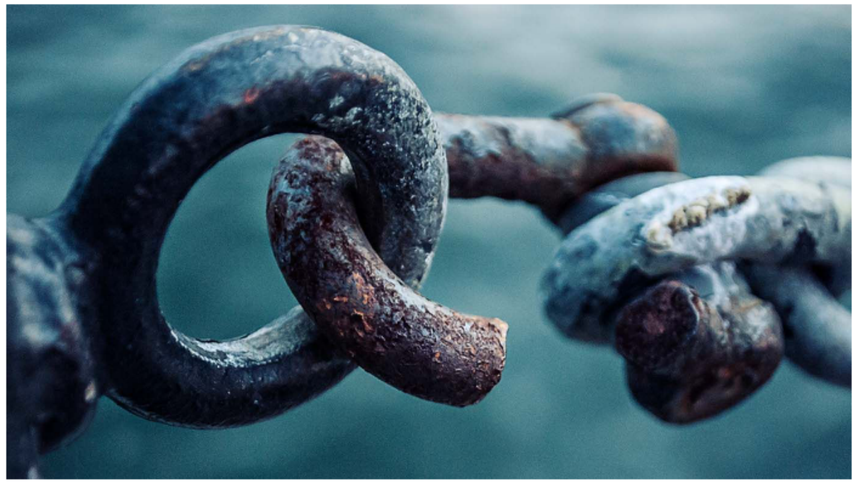
Jamf Blog

April 27, 2022 by Sean Rabbitt

Advisory: macOS devices bound to Active Directory and CVE-2021-42287

Security

The remediation for a serious security vulnerability in Microsoft Active Directory (AD) prevents Apple macOS from binding. Affected machines will lose the ability to communicate with AD domain controllers, resulting in user lockout and potential data loss.



SHARE

Update to binding error fix:

An update to CVE-2021-42287 was made available by Microsoft in the form of a new patch that corrects the broken bind functionality that existed previously. A full breakdown of the solution is available from Jamf.

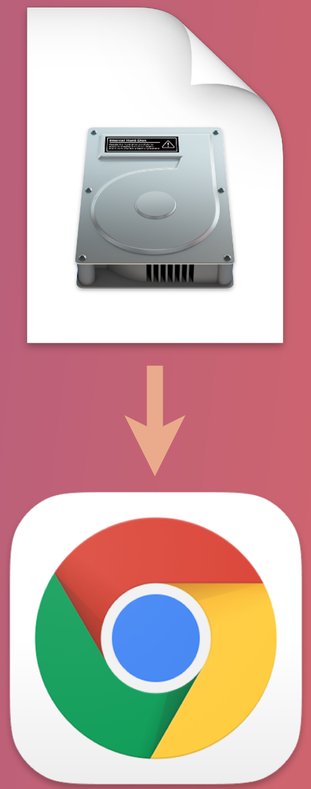
How do we perform **Patch Management?**

Installation Cycle

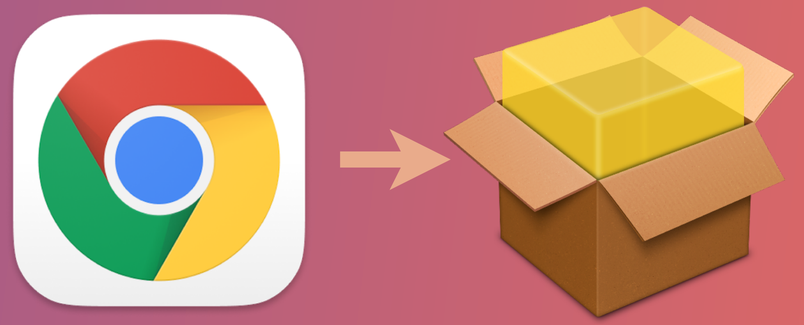
Google Chrome

Download
Extract
Package
Upload
Configure
Deploy

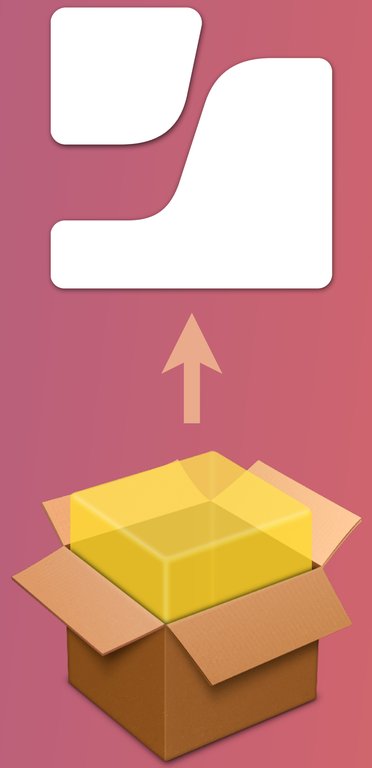
Download
Extract
Package
Upload
Configure
Deploy



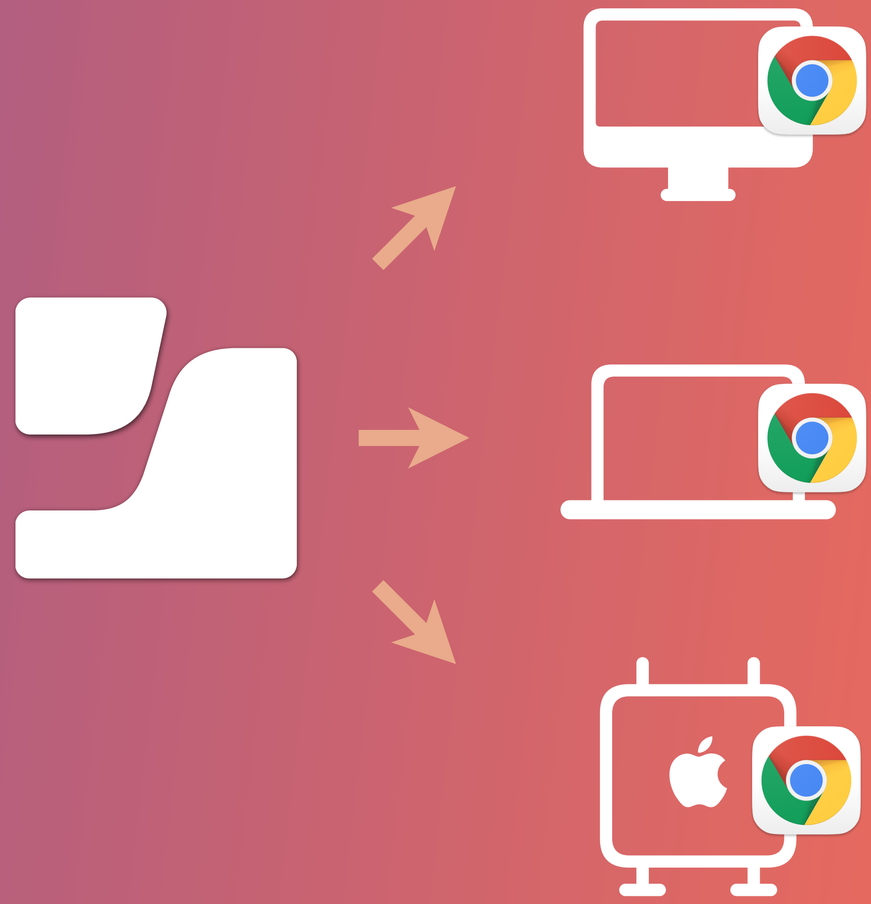
Download
Extract
Package
Upload
Configure
Deploy



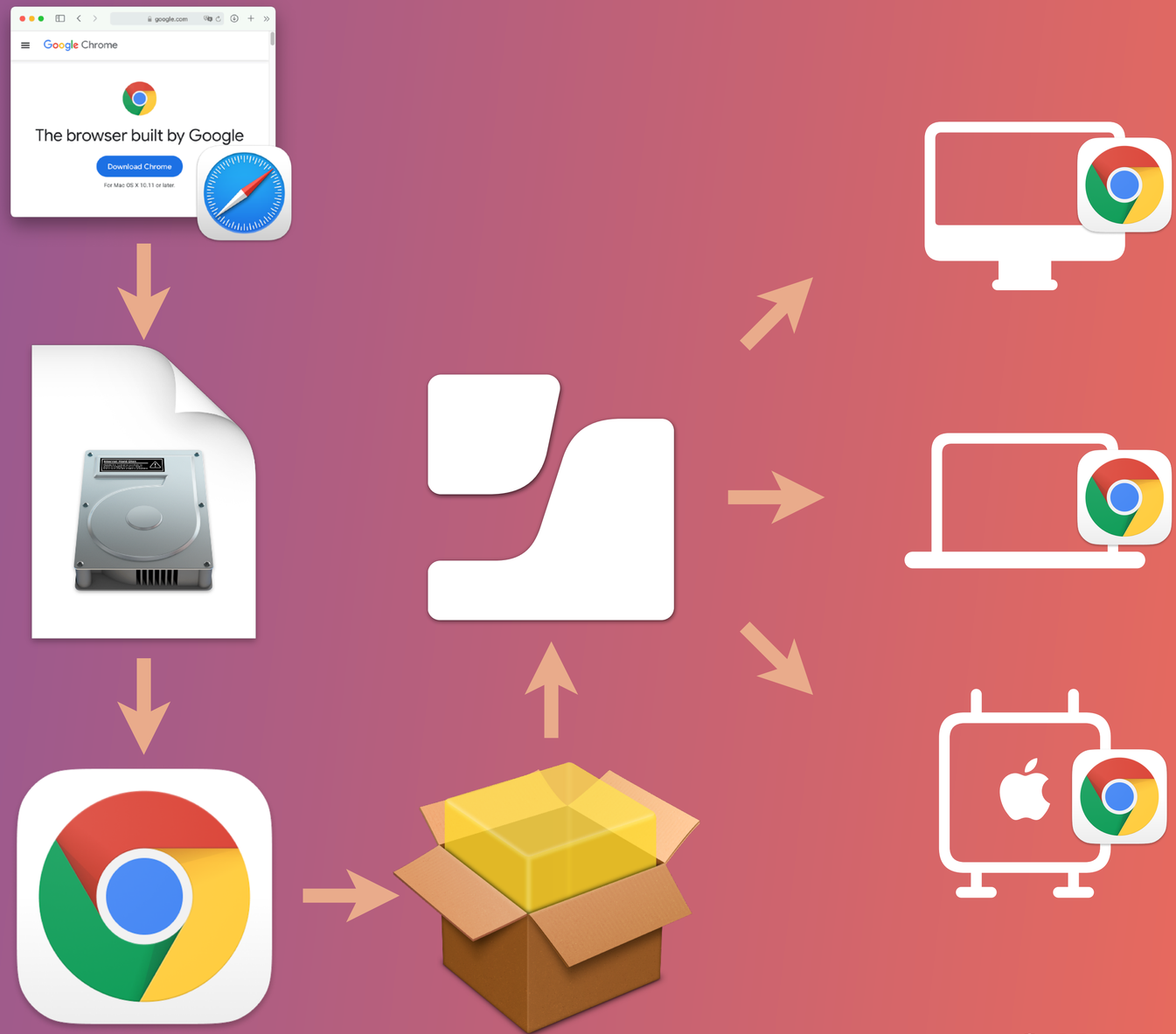
Download
Extract
Package
Upload
Configure
Deploy



Download
Extract
Package
Upload
Configure
Deploy

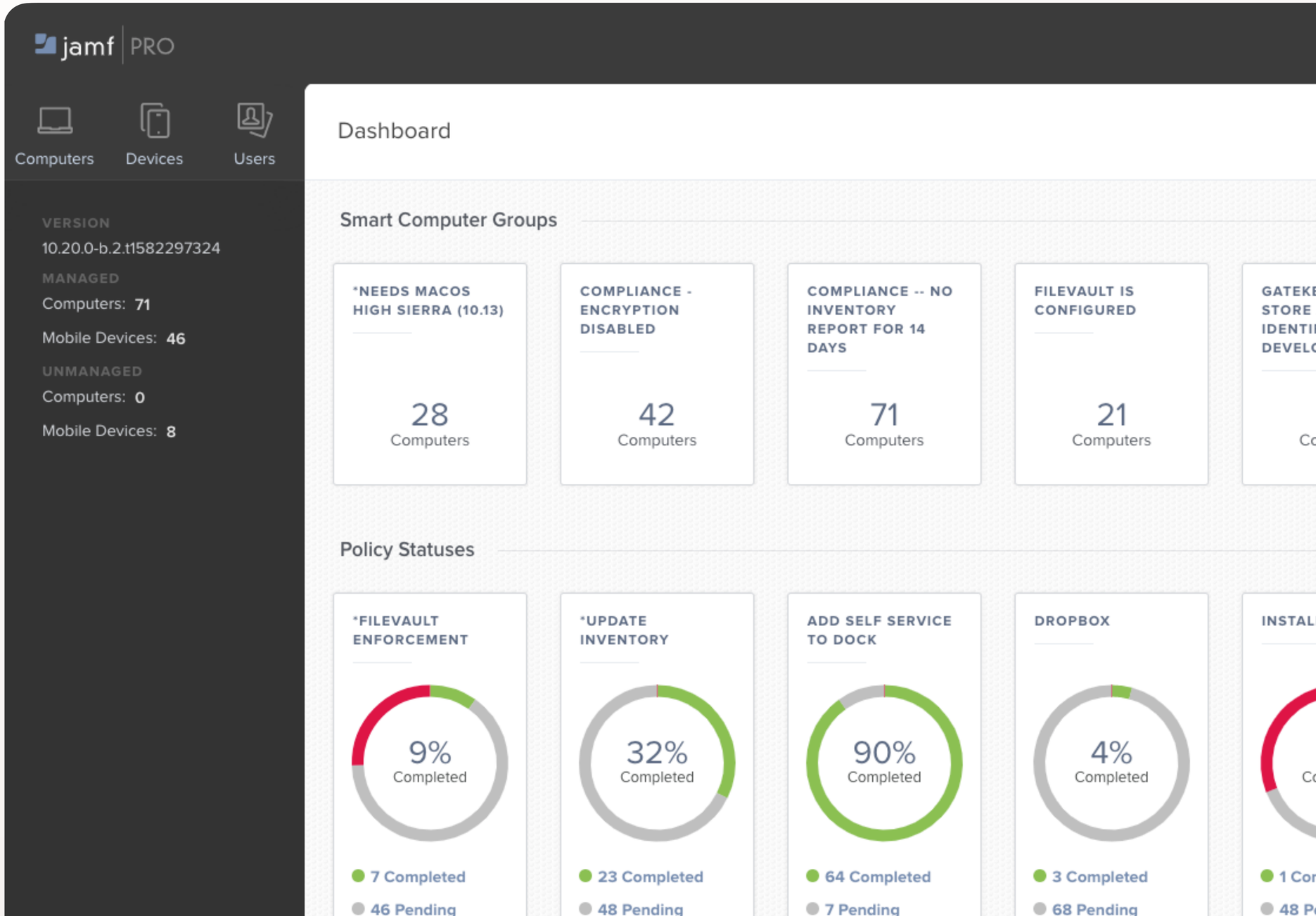


Download
Extract
Package
Upload
Configure
Deploy



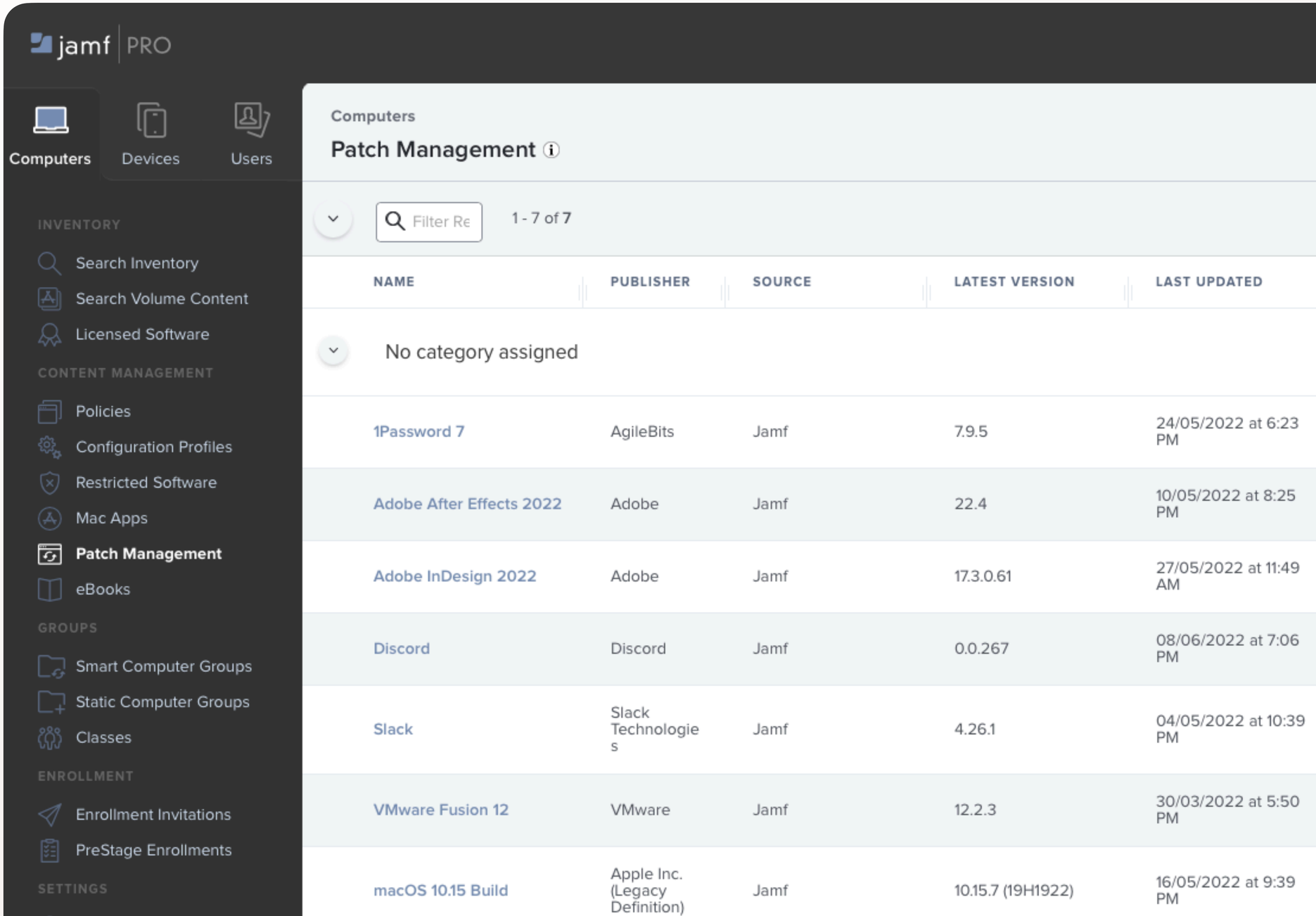
JAMF NATION LIVE

Jamf Pro



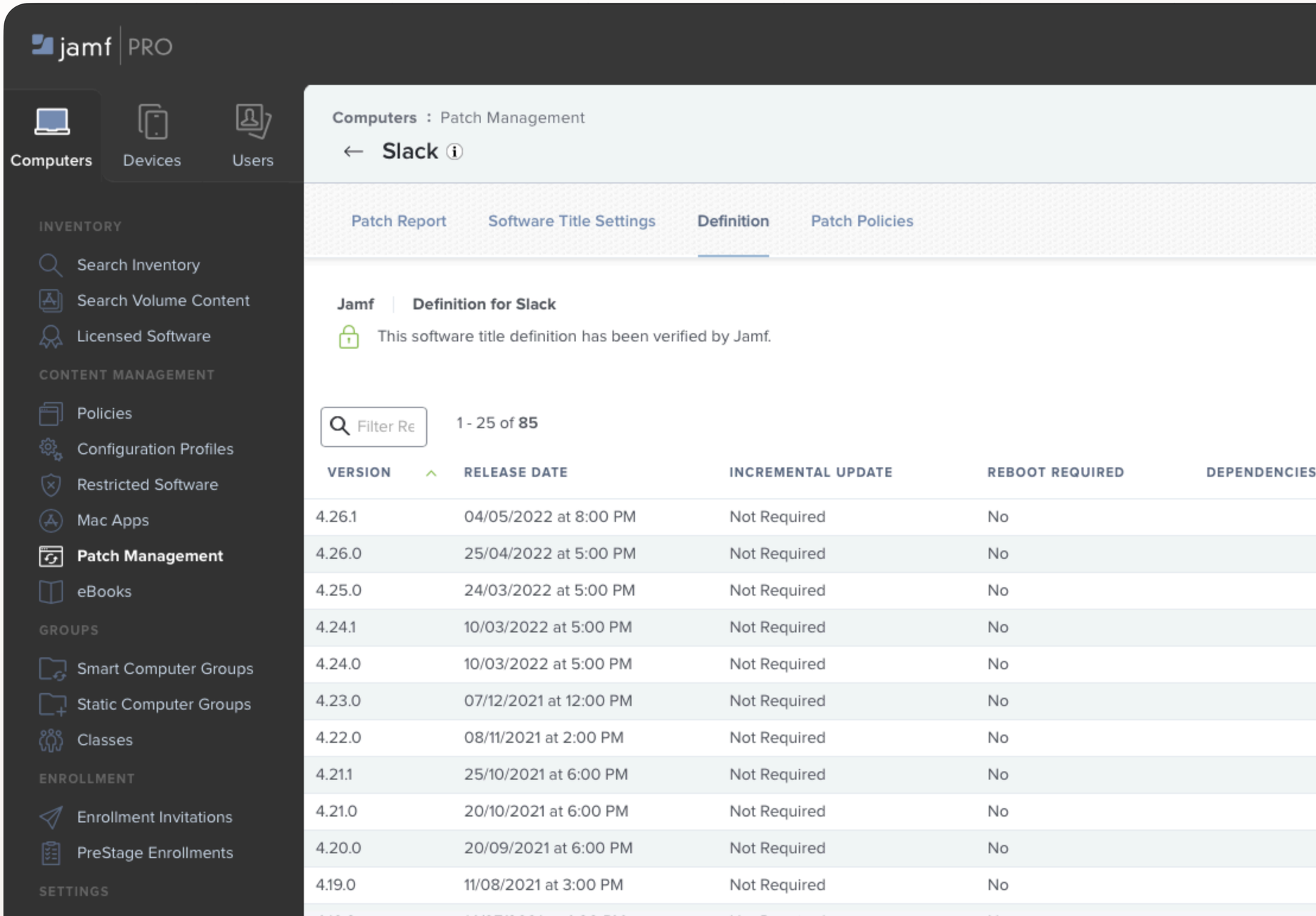
JAMF NATION LIVE

Jamf Pro



JAMF NATION LIVE

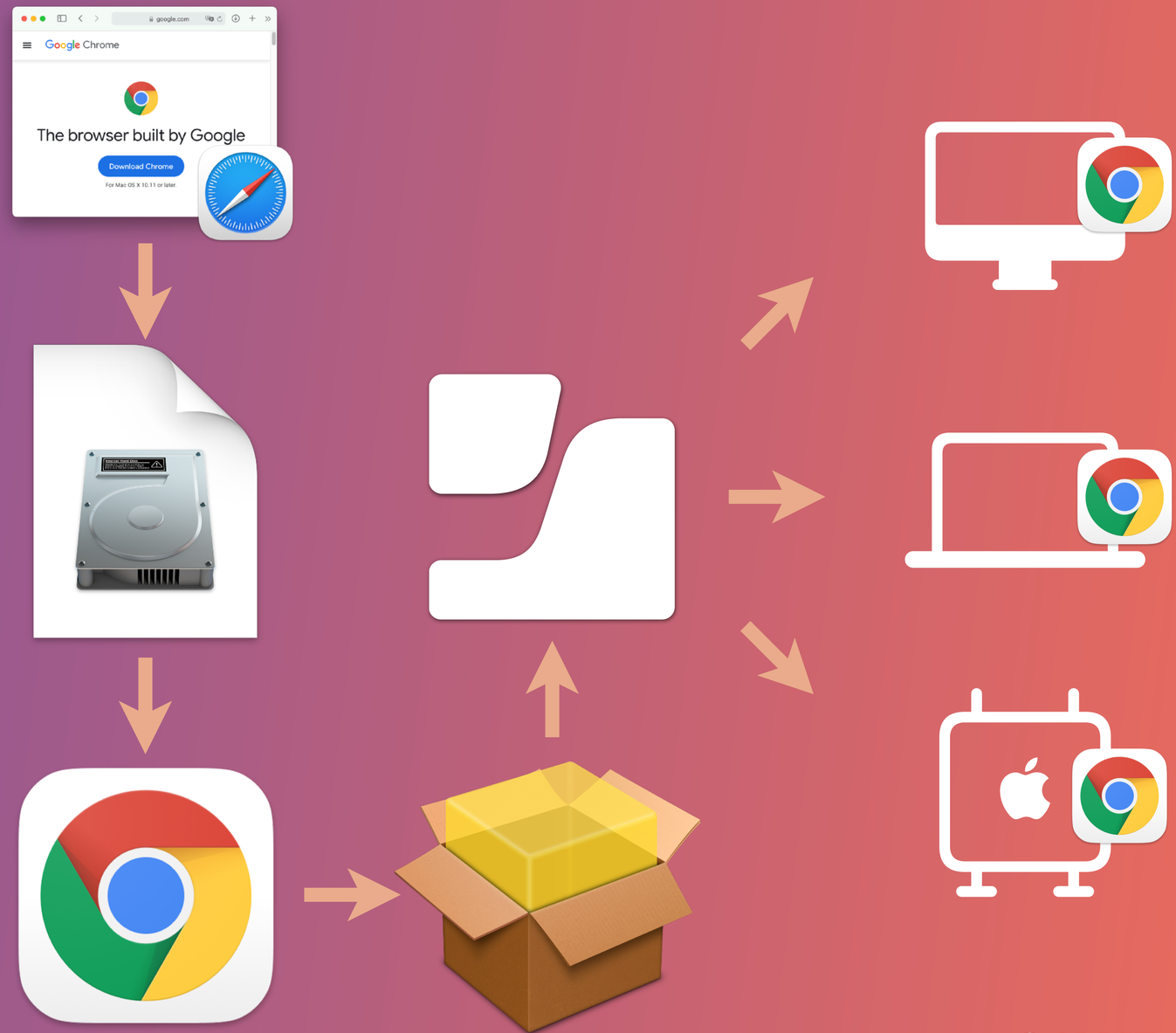
Jamf Pro



VERSION	RELEASE DATE	INCREMENTAL UPDATE	REBOOT REQUIRED	DEPENDENCIES
4.26.1	04/05/2022 at 8:00 PM	Not Required	No	
4.26.0	25/04/2022 at 5:00 PM	Not Required	No	
4.25.0	24/03/2022 at 5:00 PM	Not Required	No	
4.24.1	10/03/2022 at 5:00 PM	Not Required	No	
4.24.0	10/03/2022 at 5:00 PM	Not Required	No	
4.23.0	07/12/2021 at 12:00 PM	Not Required	No	
4.22.0	08/11/2021 at 2:00 PM	Not Required	No	
4.21.1	25/10/2021 at 6:00 PM	Not Required	No	
4.21.0	20/10/2021 at 6:00 PM	Not Required	No	
4.20.0	20/09/2021 at 6:00 PM	Not Required	No	
4.19.0	11/08/2021 at 3:00 PM	Not Required	No	

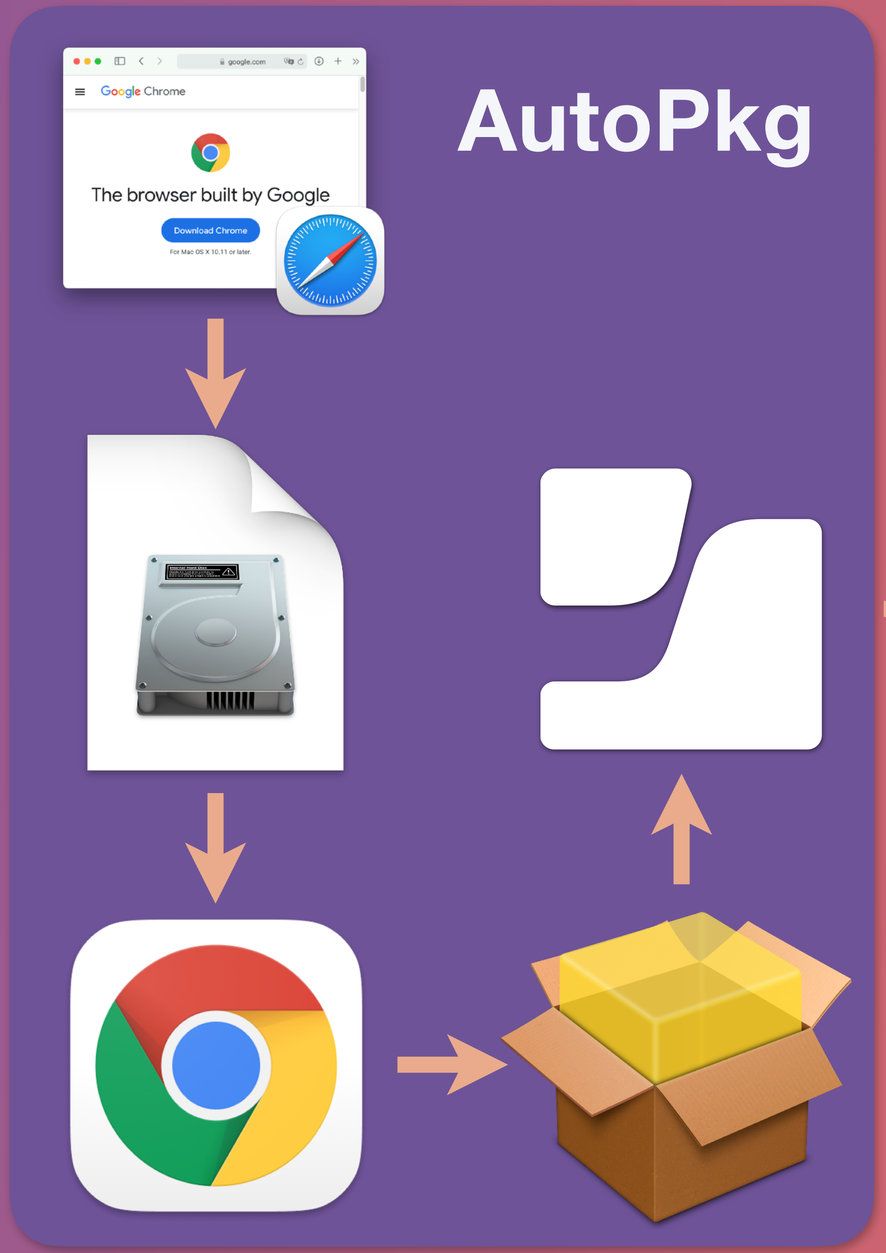
JAMF NATION LIVE

Download
Extract
Package
Upload
Configure
Deploy

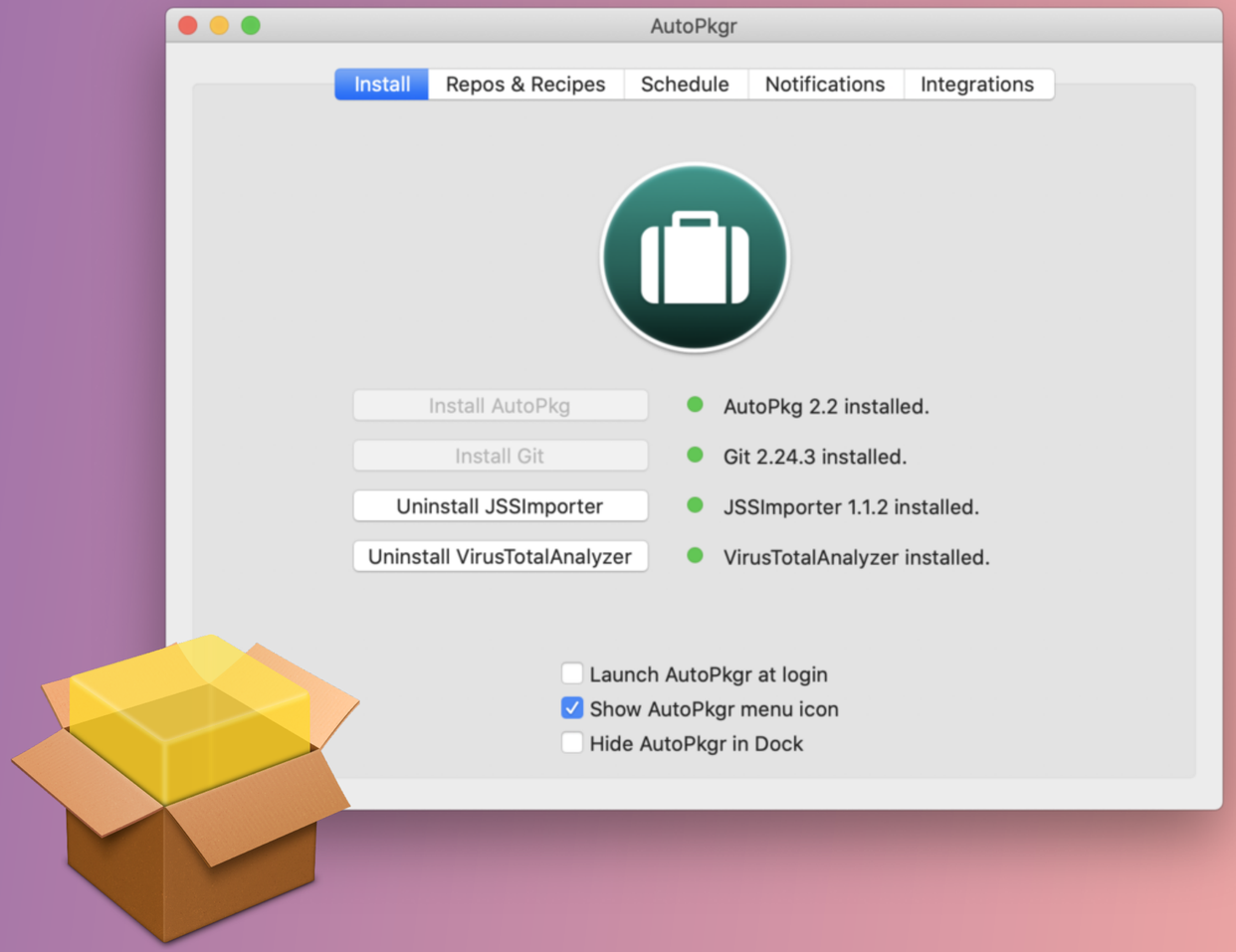


JAMF NATION LIVE

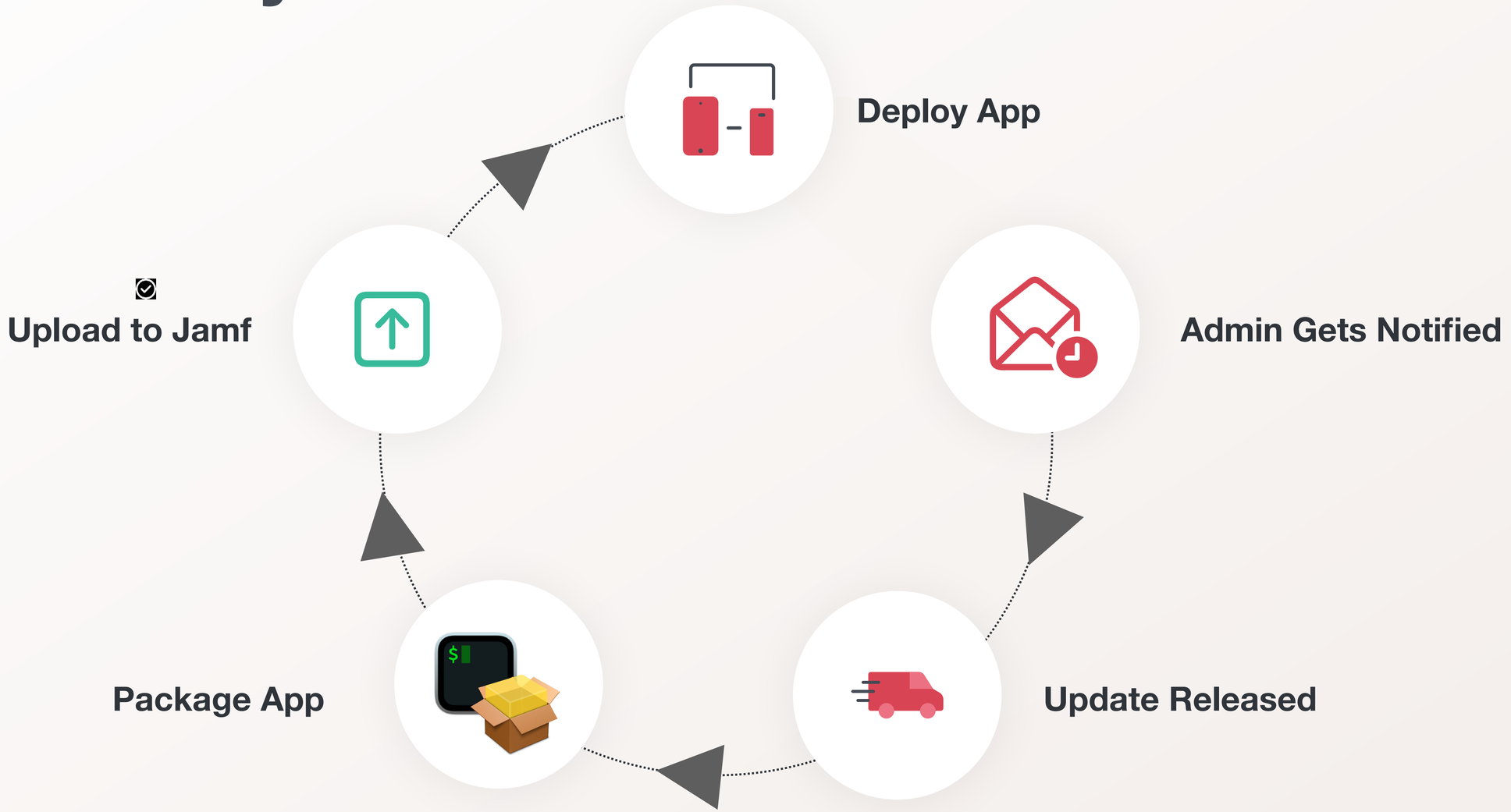
Download
Extract
Package
Upload
Configure
Deploy



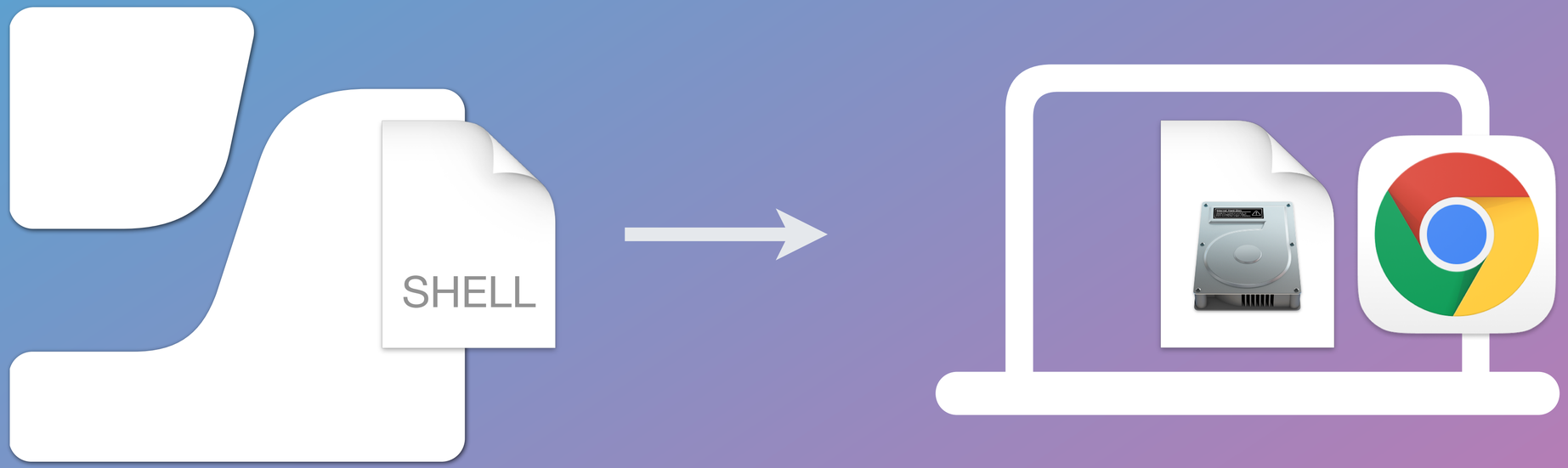
AutoPkgr


AutoPkgr
Install
Repos & Recipes
Schedule
Notifications
Integrations
Install AutoPkg
AutoPkg 2.2 installed.
Install Git
Git 2.24.3 installed.
Uninstall JSSImporter
JSSImporter 1.1.2 installed.
Uninstall VirusTotalAnalyzer
VirusTotalAnalyzer installed.
Launch AutoPkgr at login
Show AutoPkgr menu icon
Hide AutoPkgr in Dock

Installation Cycle



Installomator



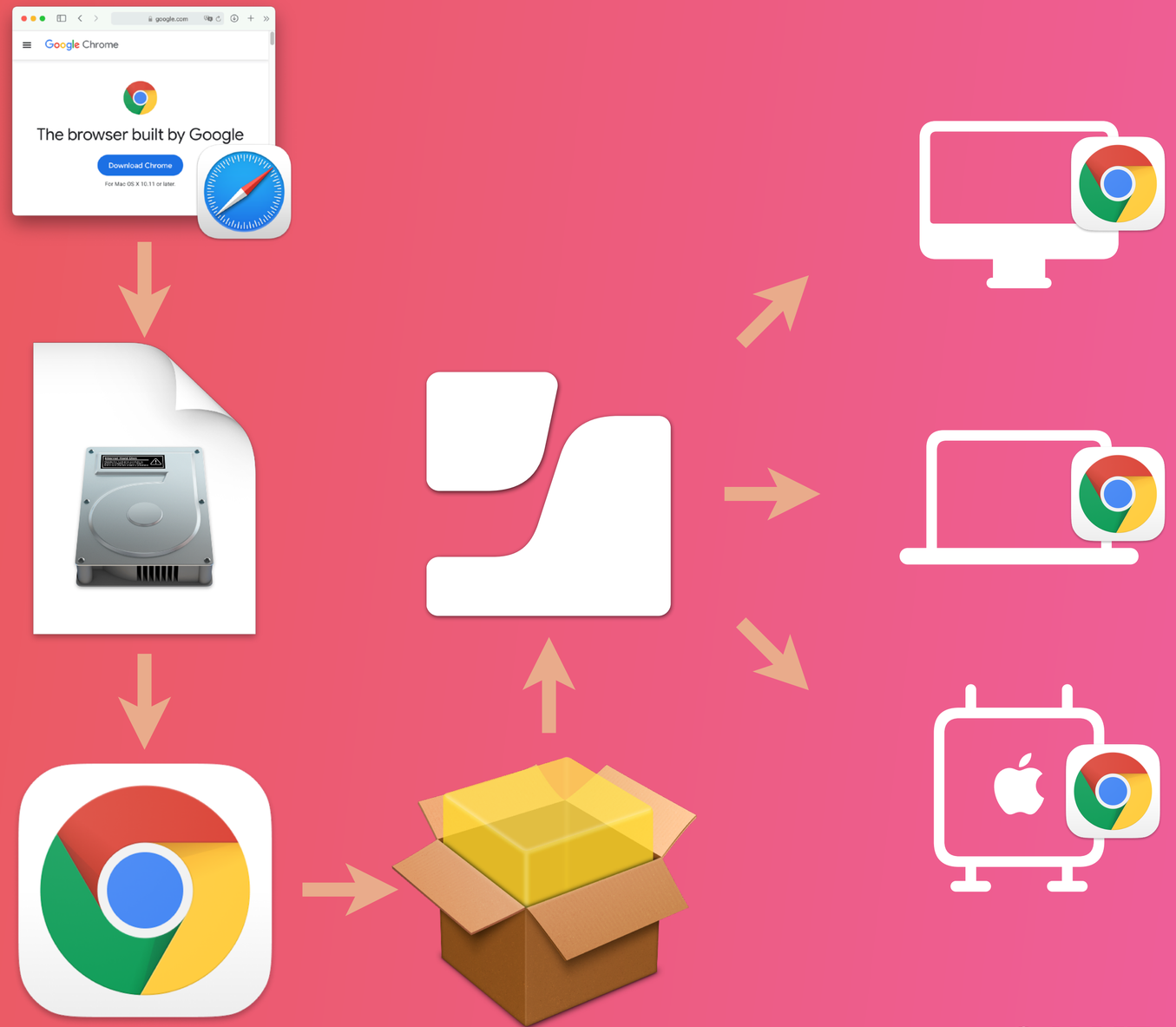
Installomator

- Over 400+ Applications
- https:// downloads
- Gatekeeper Verification
  - Apple Developer ID Signature
  - Notarization

PREVIEW

Introducing
Jamf App Catalog

Download
Extract
Package
Upload
Configure
Deploy



JAMF NATION LIVE

Downloa

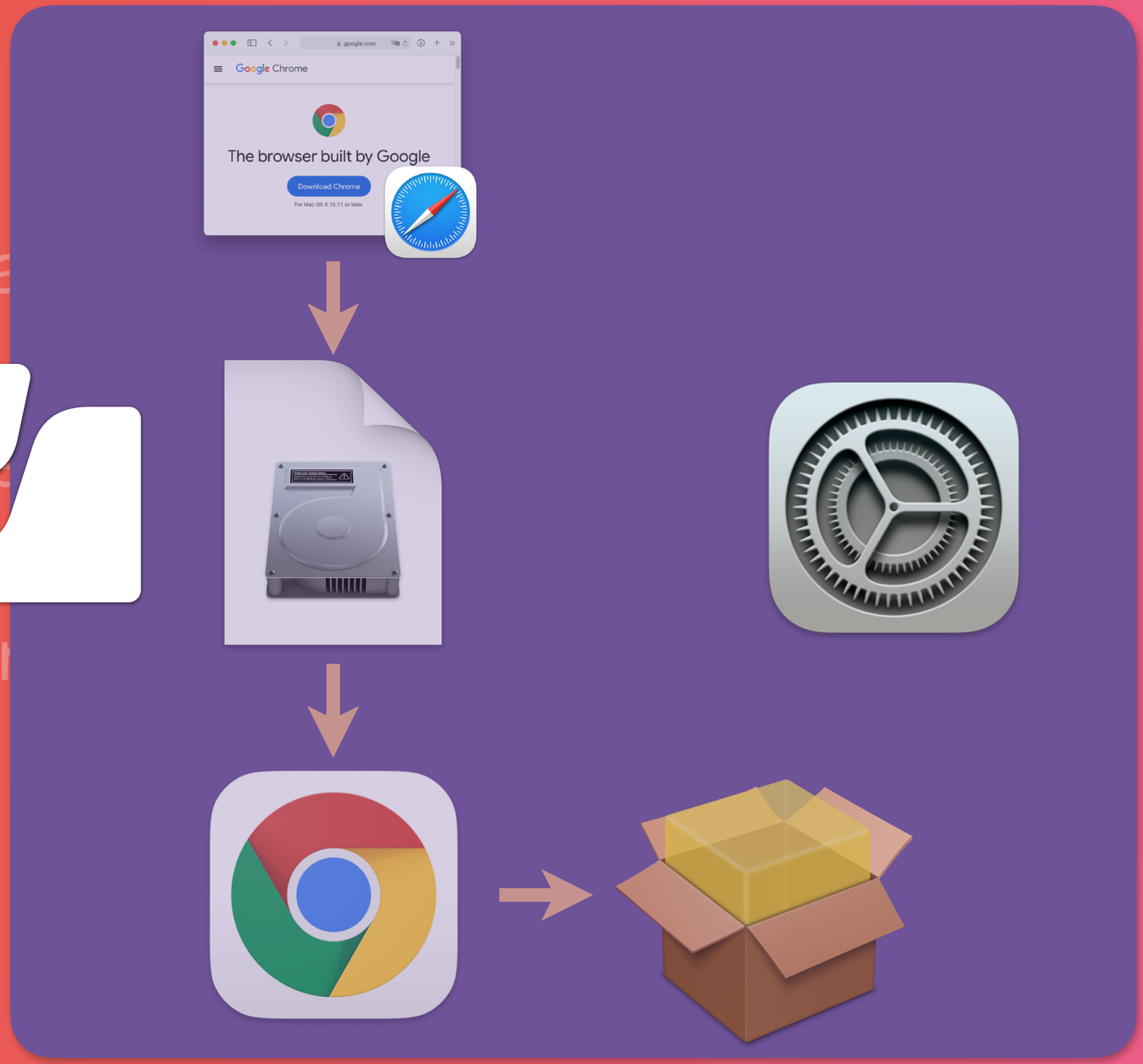
Extract

Packag

Uploa

Configur

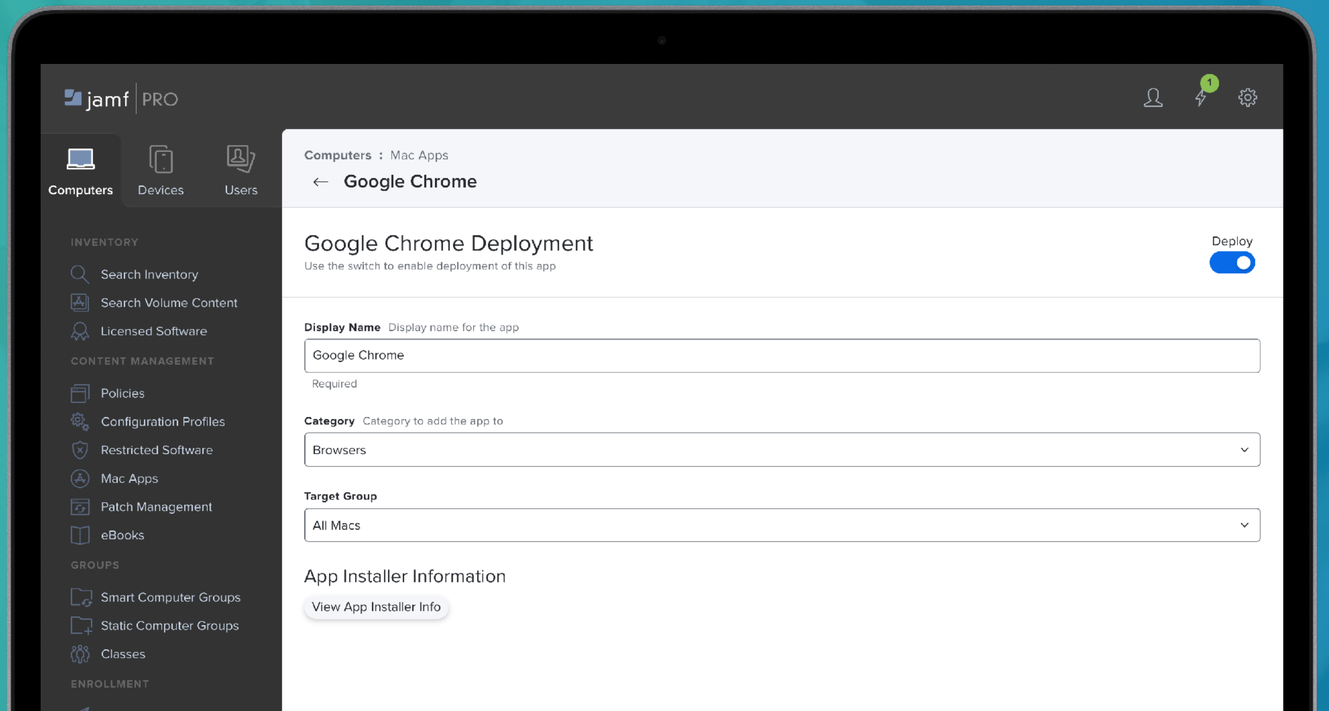
Deploy



InstallEnterpriseApplication

App Lifecycle Management Simplified

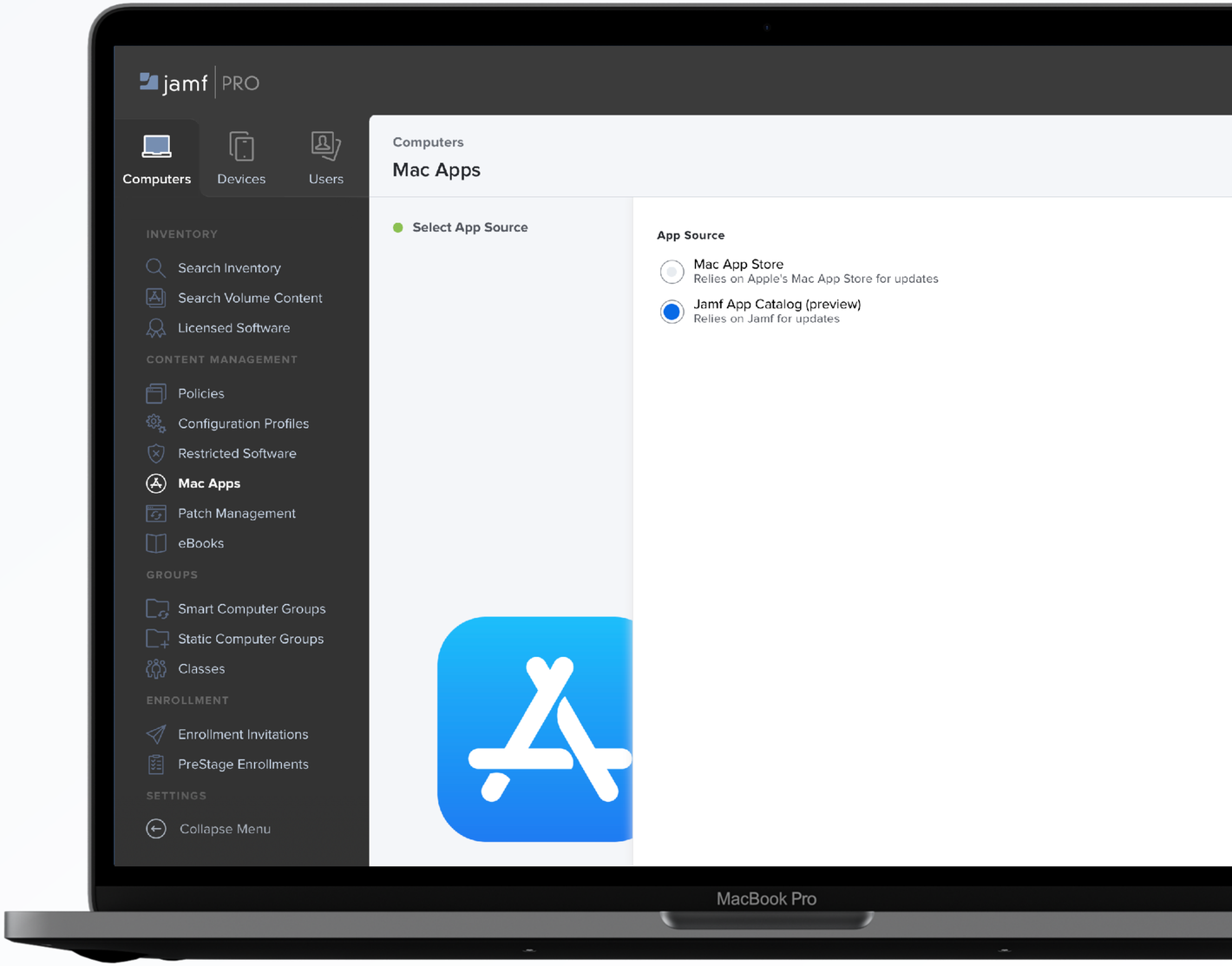
App Installers offer a streamlined alternative to complex workflows required to patch third party apps.



JAMF NATION LIVE

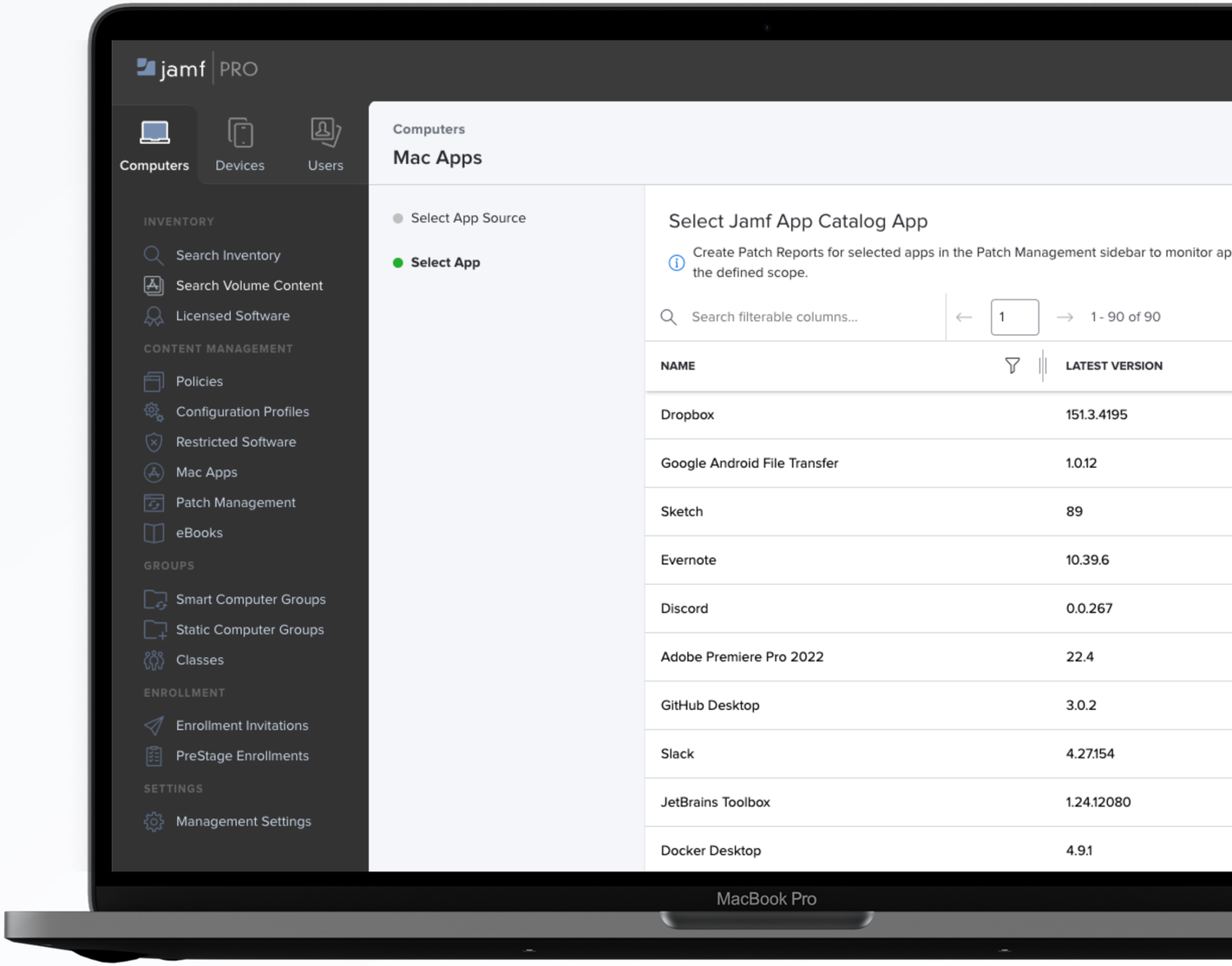
App Lifecycle Management
Jamf Pro

- App Installers for streamlined app installation and updates
- Patch definition feed for comprehensive third party app tracking
- Title Editor for custom app title management



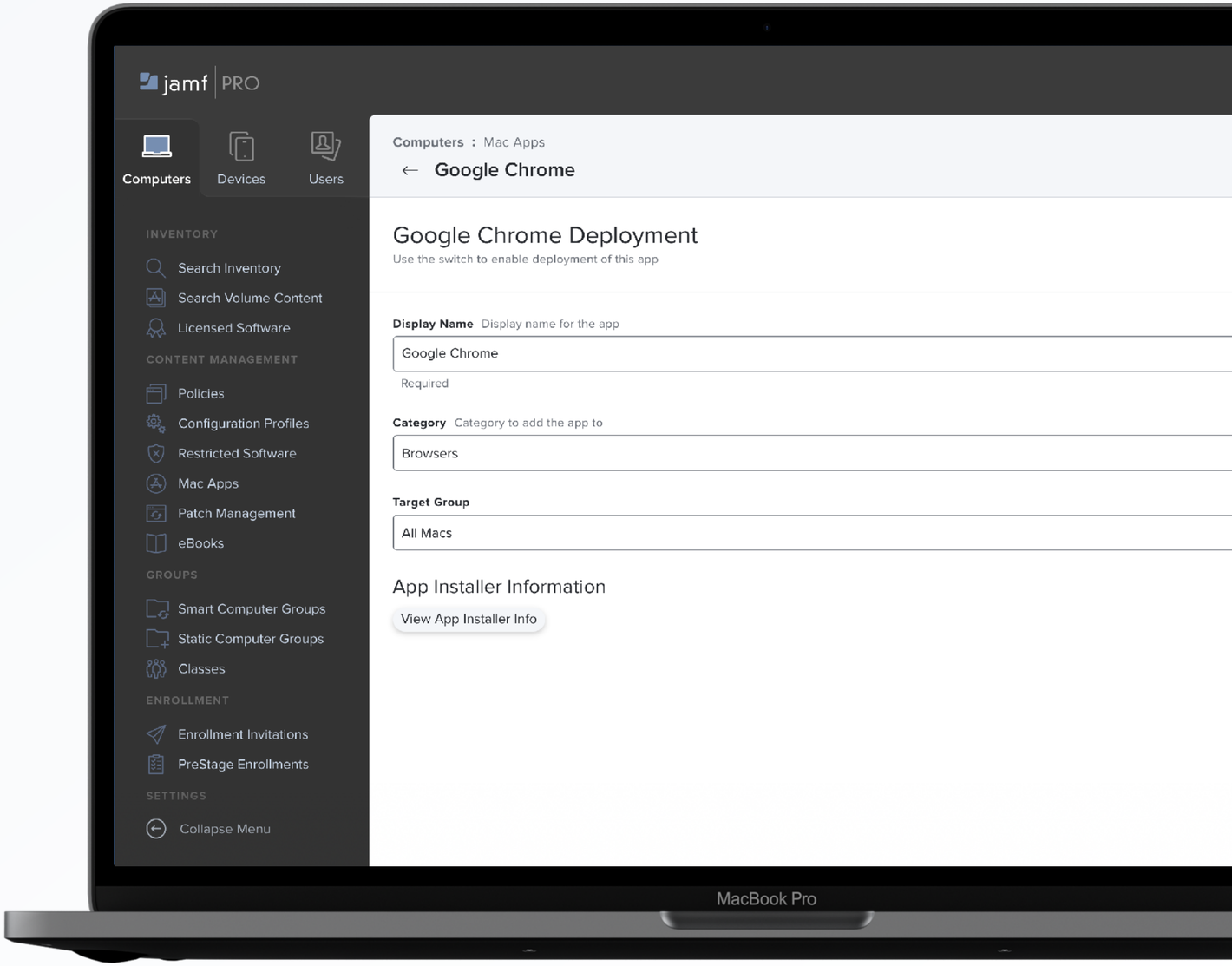
App Lifecycle Management
Jamf Pro

- App Installers for streamlined app installation and updates
- Patch definition feed for comprehensive third party app tracking
- Title Editor for custom app title management



App Lifecycle Management
Jamf Pro

- App Installers for streamlined app installation and updates
- Patch definition feed for comprehensive third party app tracking
- Title Editor for custom app title management



JAMF NATION LIVE

App Lifecycle Management **Simplified**

Step 1: Choose an App Installer

Step 2: Choose your scope

(There is no Step 3)

Leverage a single streamlined workflow for your apps

- Simple alternative to policies and patch management
- Support for the most prominent and important apps your users rely on
- Included for all Jamf Pro Cloud subscription customers

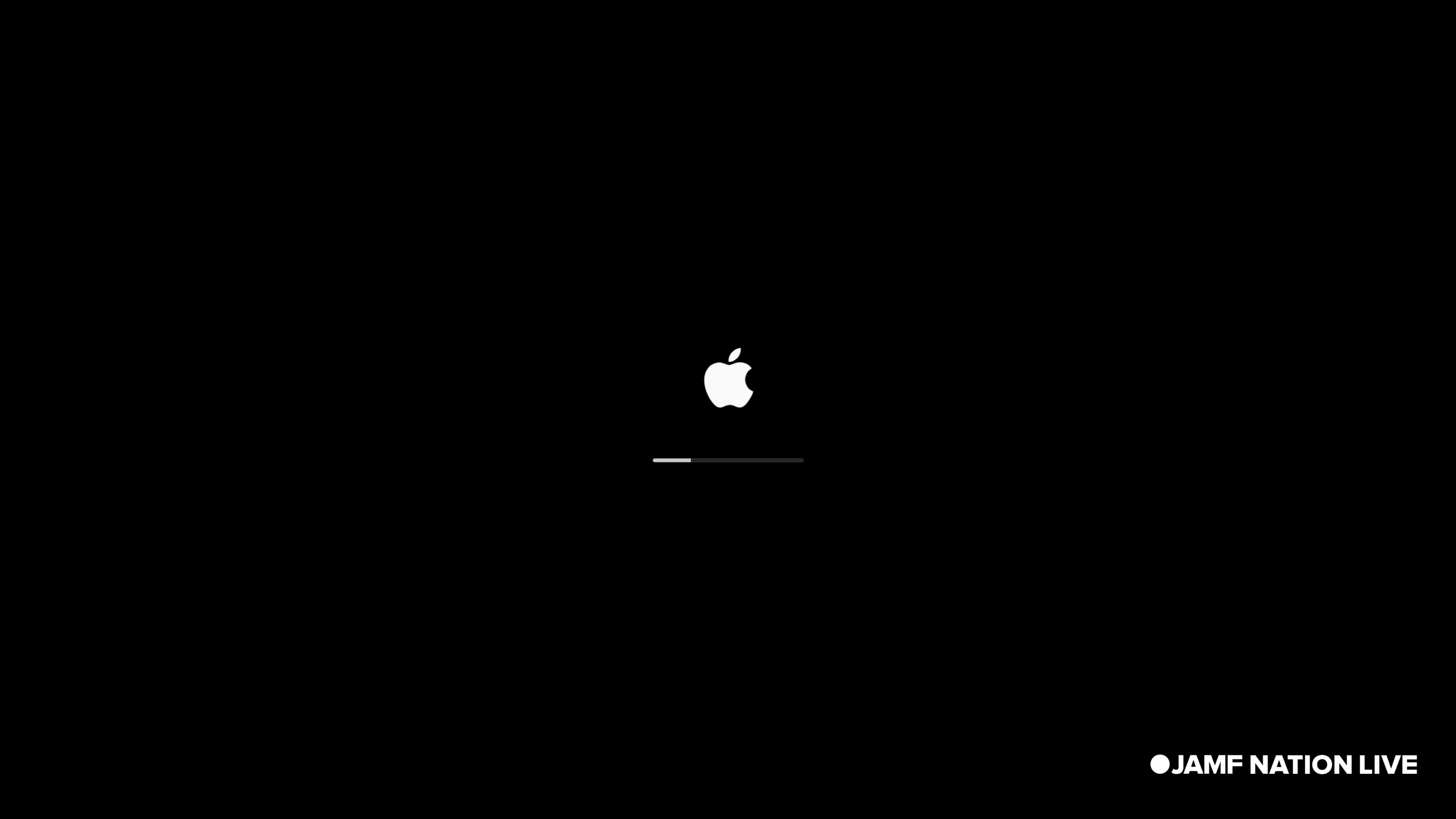
Jamf takes on the burden and complexity of app updates

- Jamf sources all updates
- Jamf repackages when needed
- Jamf validates security of package
- Jamf verifies installation
- Jamf makes the latest updates available

JAMF NATION LIVE

macOS Updates

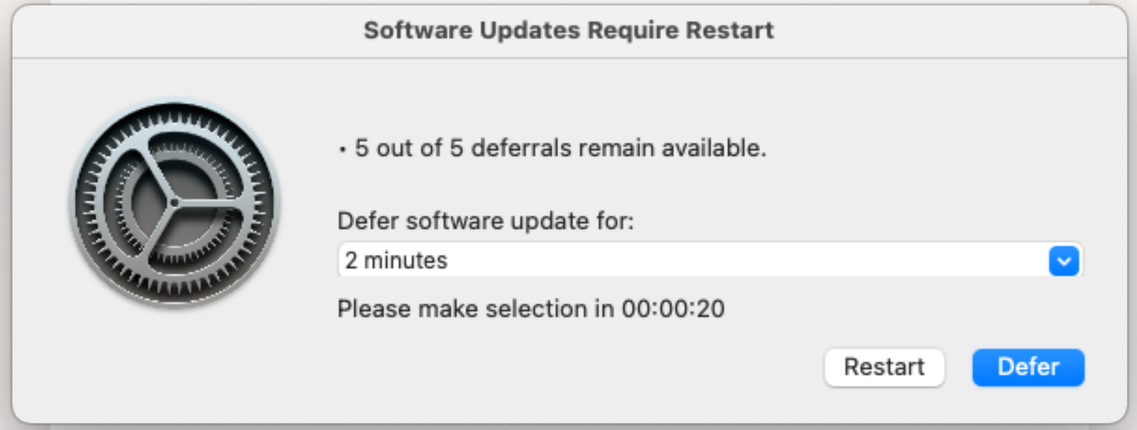

Mac OS
Starting Up...


JAMF NATION LIVE

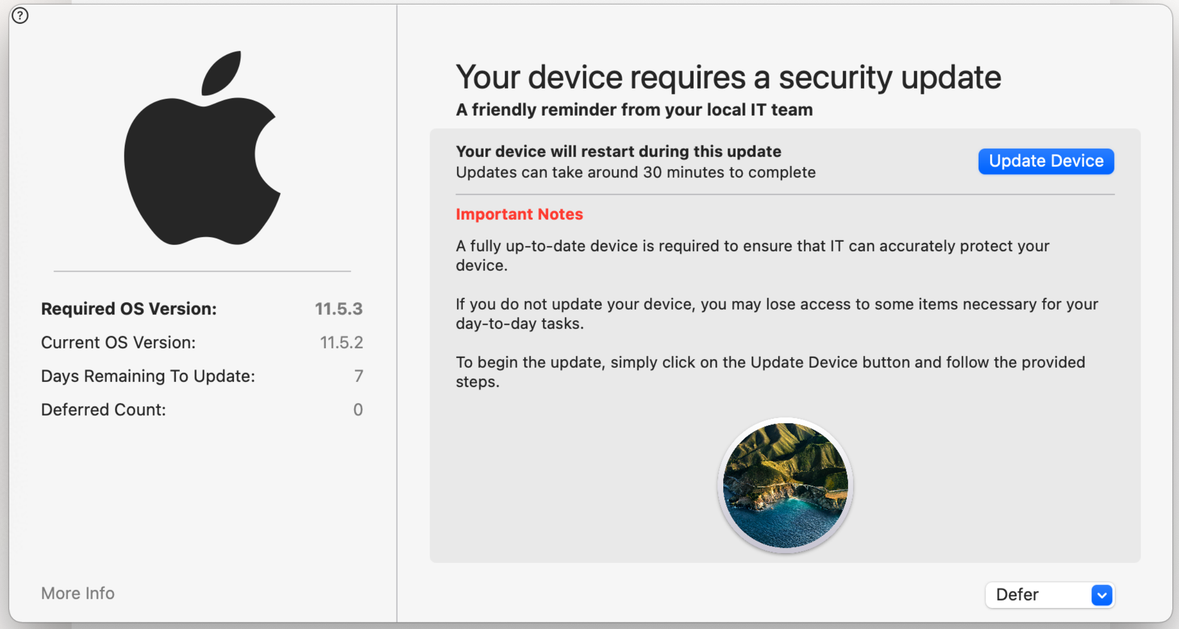
Software Updates

Some great external tools

S.U.P.E.R.M.A.N



Nudge

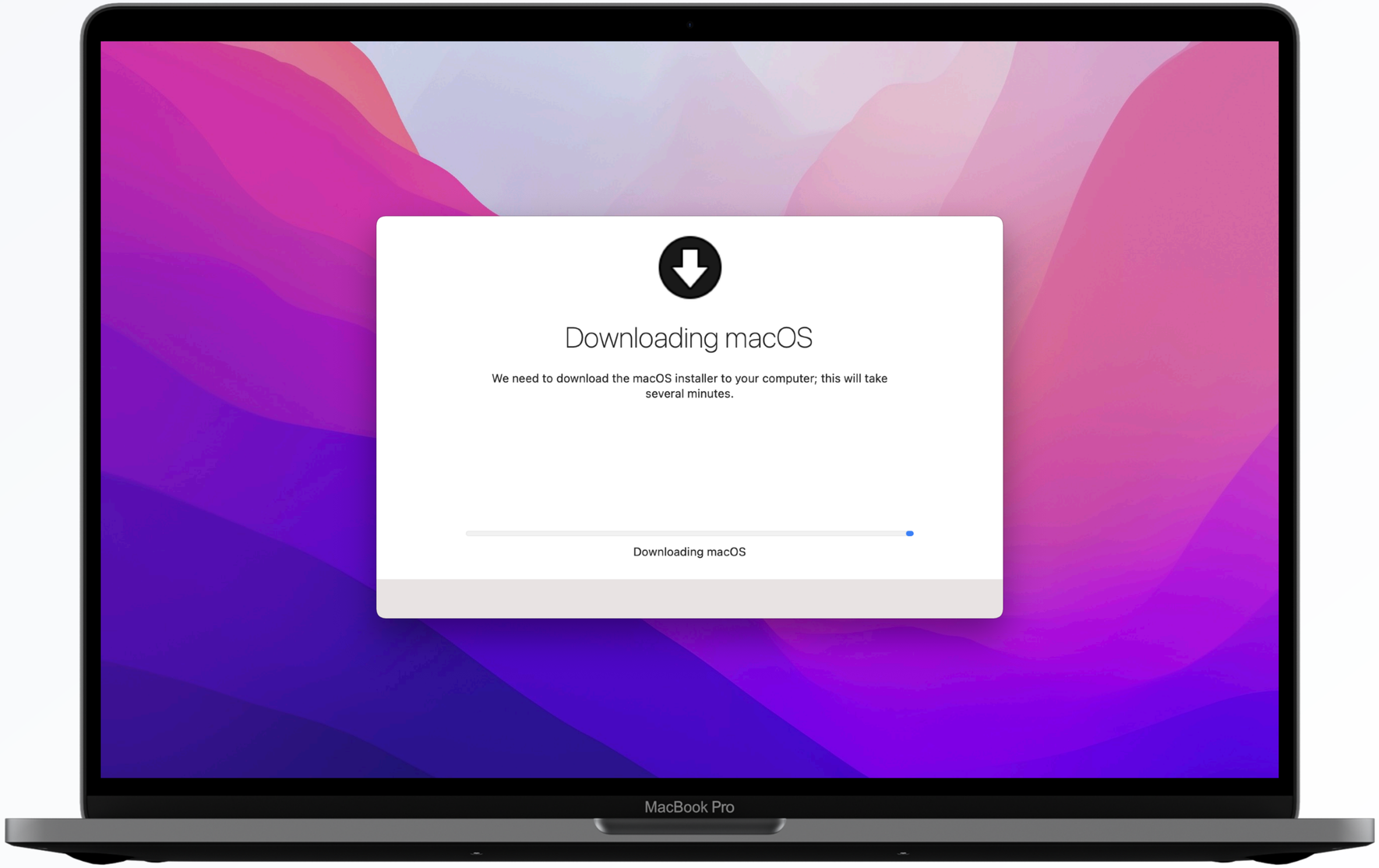


More then just a name…

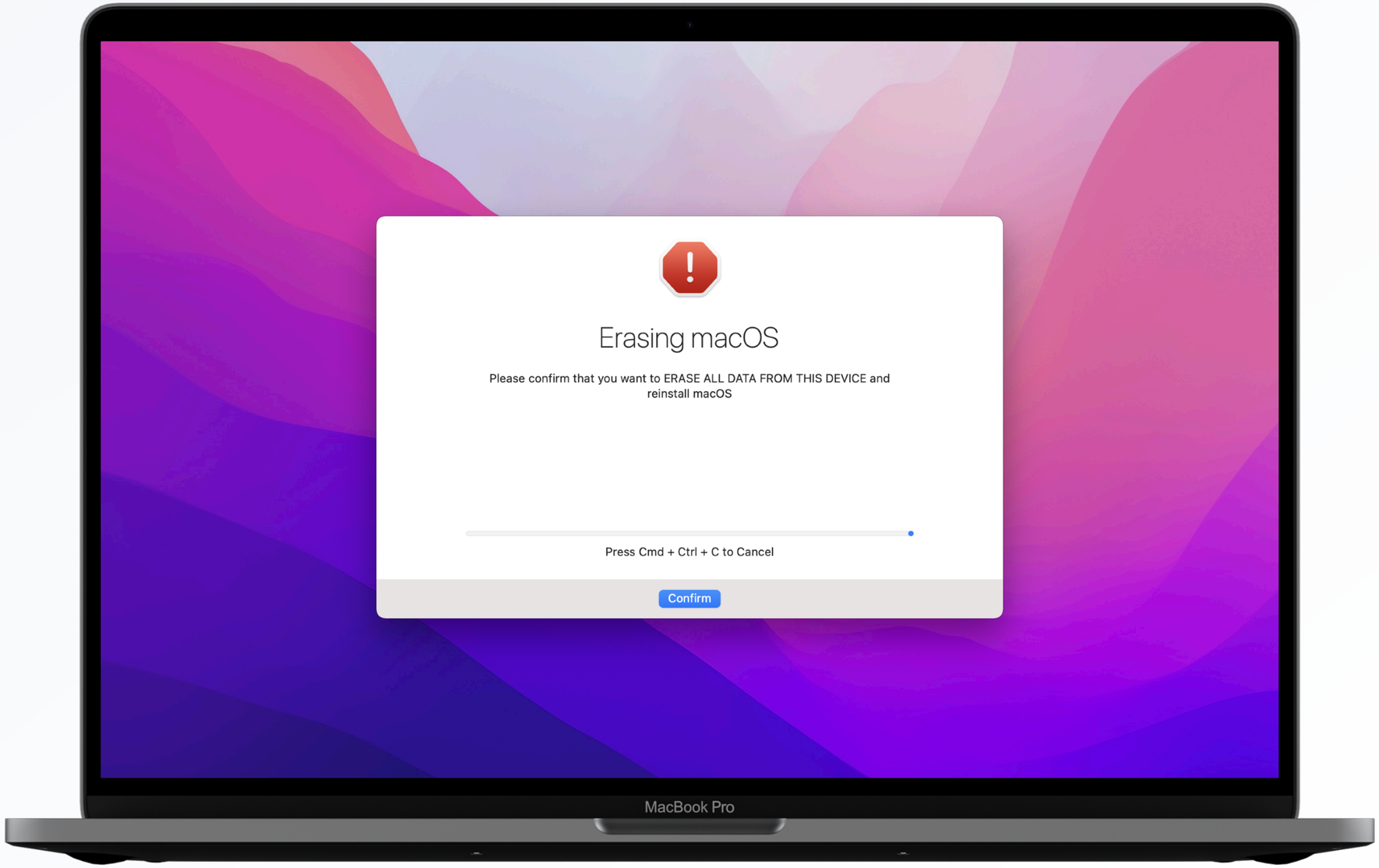
erase-install.sh

JAMF NATION LIVE

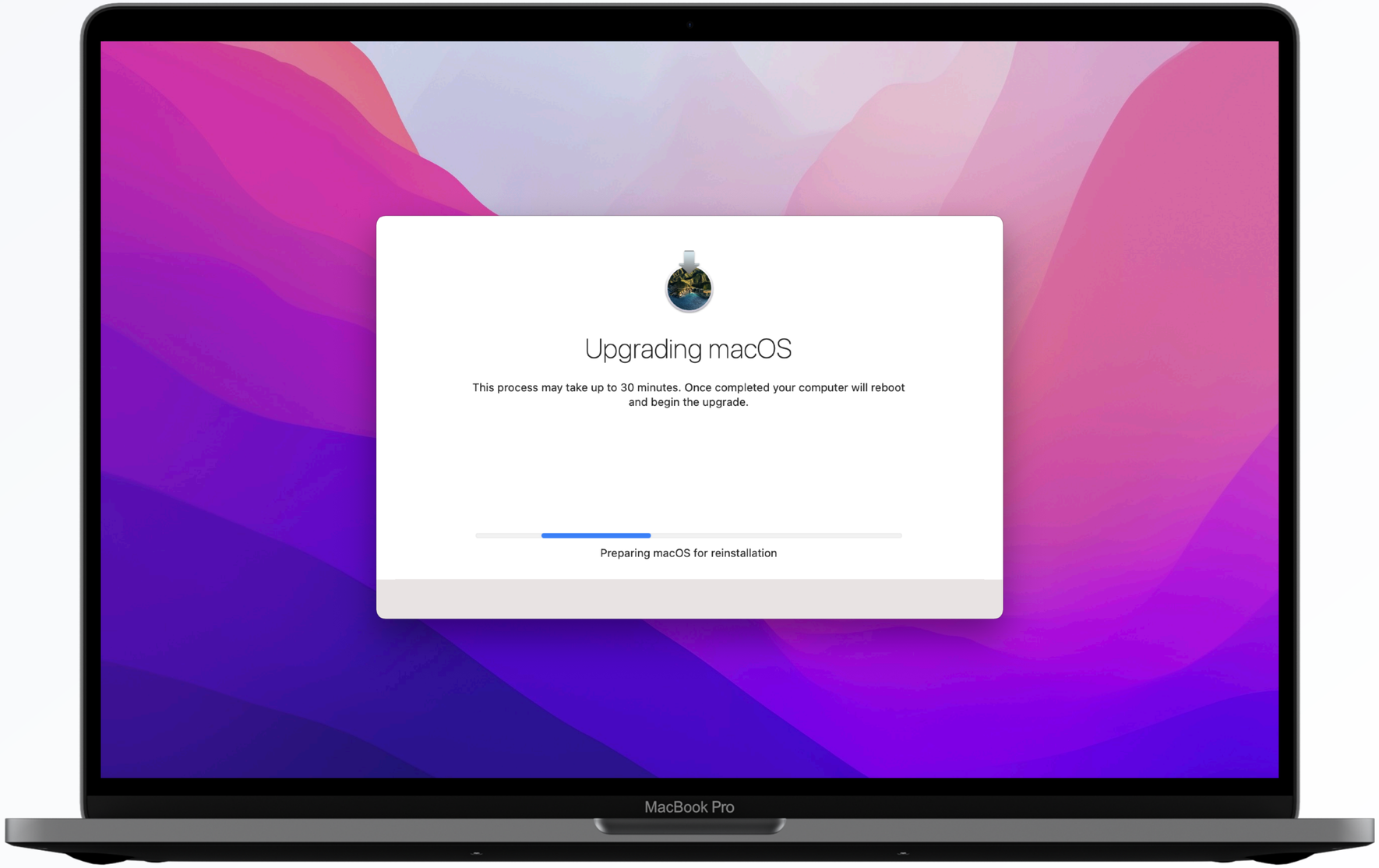
Download the macOS installer



Start again?


Erasing macOS
Please confirm that you want to ERASE ALL DATA FROM THIS DEVICE and reinstall macOS
Press Cmd + Ctrl + C to Cancel
Confirm
MacBook Pro

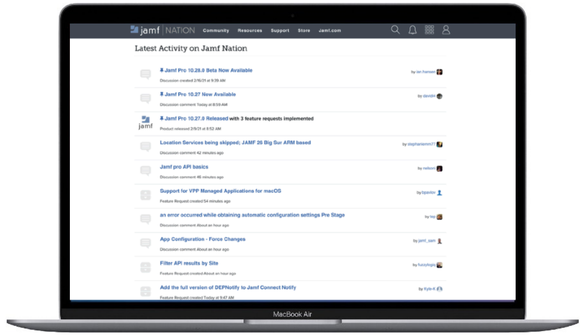
Upgrade


Upgrading macOS
This process may take up to 30 minutes. Once completed your computer will reboot and begin the upgrade.
Preparing macOS for reinstallation
MacBook Pro

Jamf Nation and Jamf Marketplace

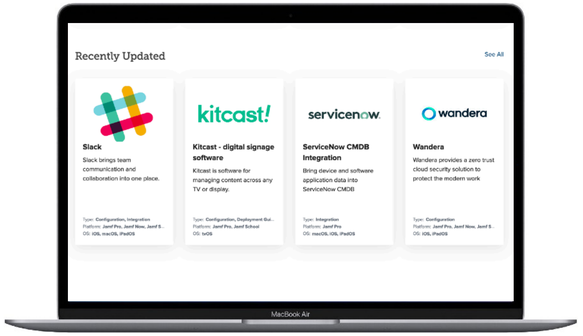
Expanded Ecosystem and Support Strengthen the Jamf Platform and Improve Jamf Efficiency

Jamf Nation



- 100,000+ Jamf Nation members
- Largest online community of Apple IT administrators in the world
- Jamf Nation User Conference (JNUC) is largest Apple IT administrator event
- Builds a social community while improving Jamf efficiency

Jamf Marketplace



- Hundreds of applications, integrations, solutions and consultants
- Enabled by Jamf APIs and facilitated by Jamf developer relations
- Evidence of Jamf's market leadership
- Builds a solution ecosystem that strengthens Jamf retention

Thank You