

# Patch Management

From Nice to Have to Necessity

The logo for JAMF NATION LIVE is contained within a white rectangular border. It features a white circle to the left of the text. The text is stacked in three lines: "JAMF", "NATION", and "LIVE", all in a bold, white, sans-serif font.

● 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)*





**Security**

# CVE Details

The ultimate security vulnerability datasource

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

[Log In](#) [Register](#)

Vulnerability Feeds & Widgets <sup>New</sup> [www.itsecdb.com](#)

- [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](#)  
[Bugtrag Entries](#)  
[CWE Definitions](#)  
[About & Contact](#)  
[Feedback](#)  
[CVE Help](#)  
[FAQ](#)  
[Articles](#)

- External Links :**  
[NVD Website](#)  
[CWE Web Site](#)

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

**View BID :**

## 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.	Avail.
1	<a href="#">CVE-2021-30599</a>	<a href="#">843</a>		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	<a href="#">CVE-2021-30598</a>	<a href="#">843</a>		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	<a href="#">CVE-2021-21224</a>	<a href="#">843</a>		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	<a href="#">CVE-2020-6572</a>	<a href="#">416</a>		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	<a href="#">CVE-2020-6537</a>	<a href="#">843</a>		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	<a href="#">CVE-2020-6443</a>	<a href="#">345</a>		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	<a href="#">CVE-2020-6417</a>			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	<a href="#">CVE-2019-13735</a>	<a href="#">787</a>		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	<a href="#">CVE-2019-13726</a>	<a href="#">119</a>		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	<a href="#">CVE-2019-13725</a>	<a href="#">416</a>		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	<a href="#">CVE-2019-13693</a>	<a href="#">416</a>		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	<a href="#">CVE-2019-5790</a>	<a href="#">190</a>		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	<a href="#">CVE-2019-5789</a>	<a href="#">190</a>		Exec Code Overflow	2019-05-23	2020-08-24	9.3	None	Remote	Medium	Not required	Complete	Complete	Com



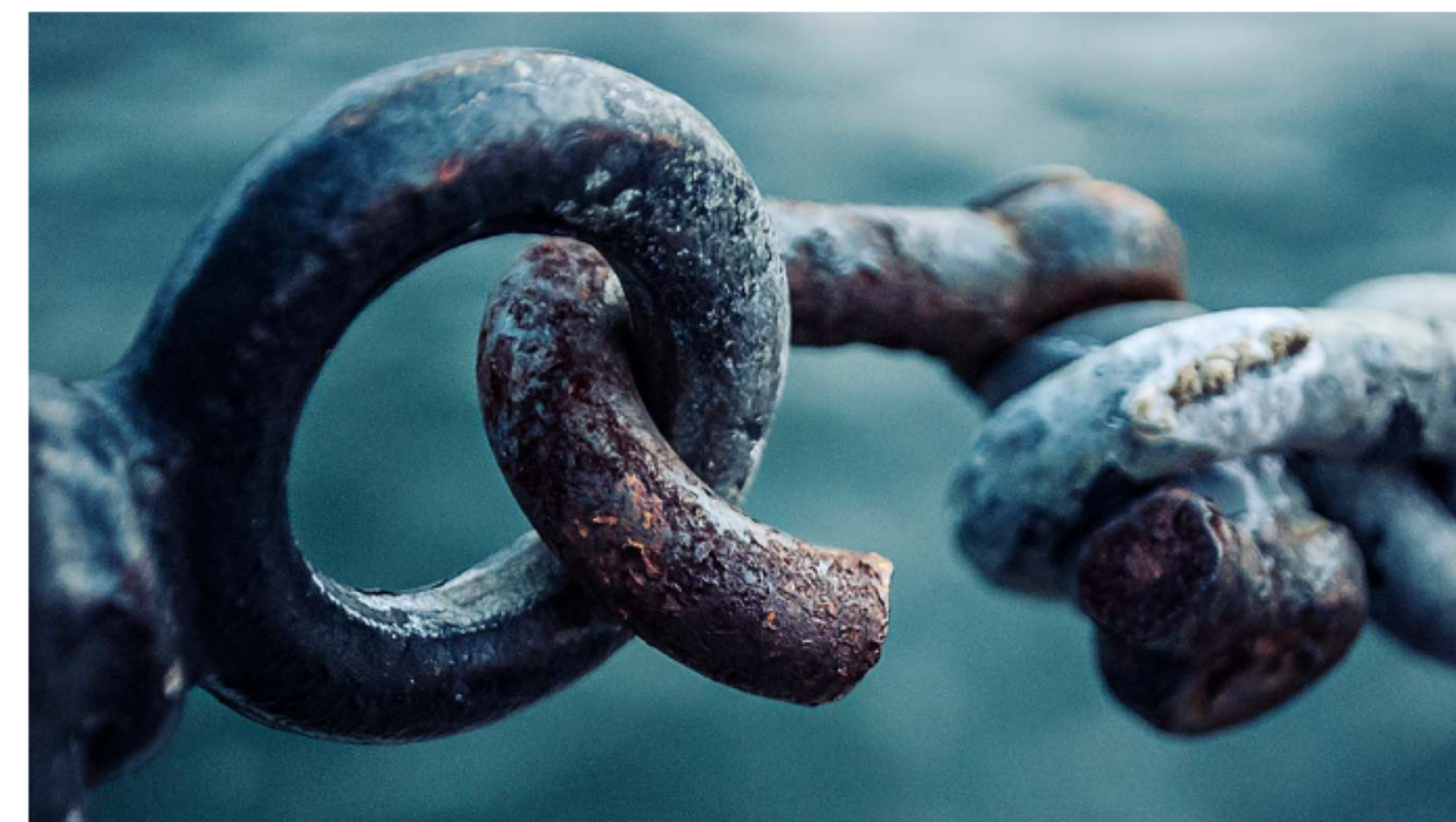
## Jamf Blog

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.



#### 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.

SHARE





How do we perform  
**Patch**  
**Management?**



# Installation Cycle



Google Chrome

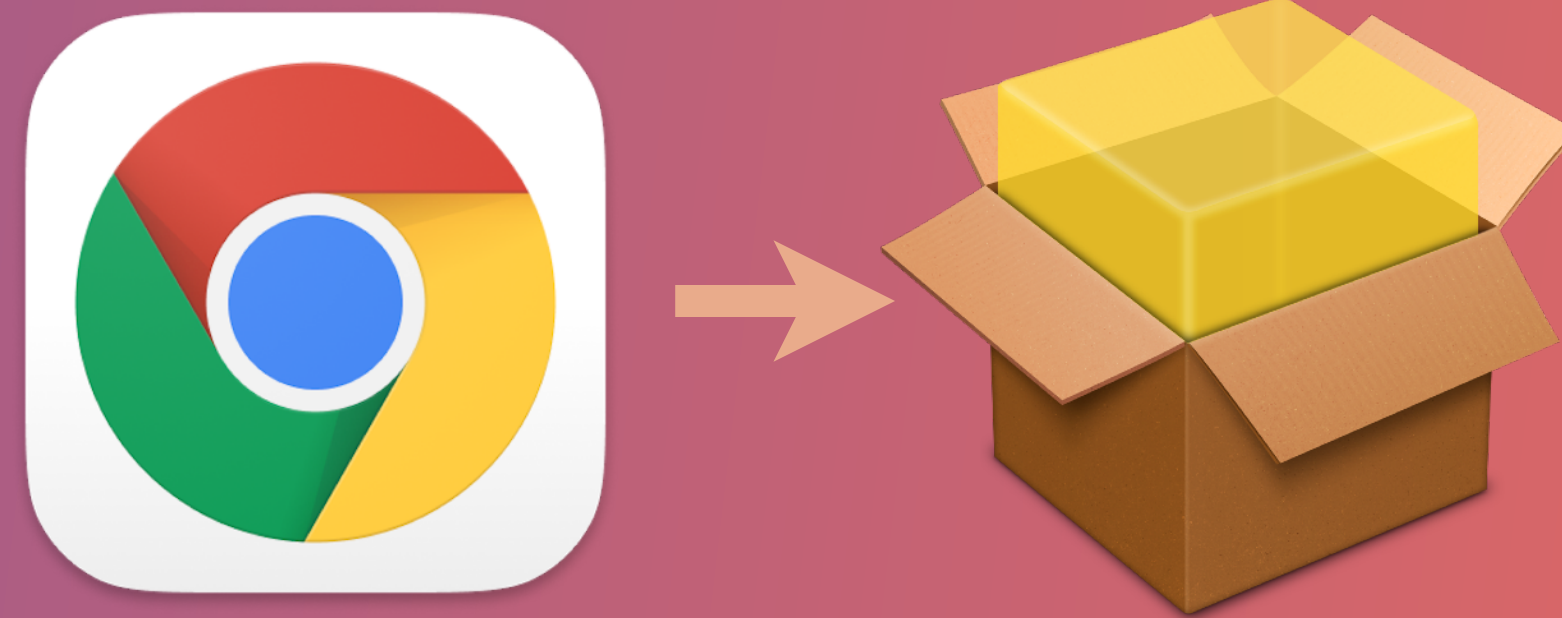
Download  
Extract  
Package  
Upload  
Configure  
Deploy



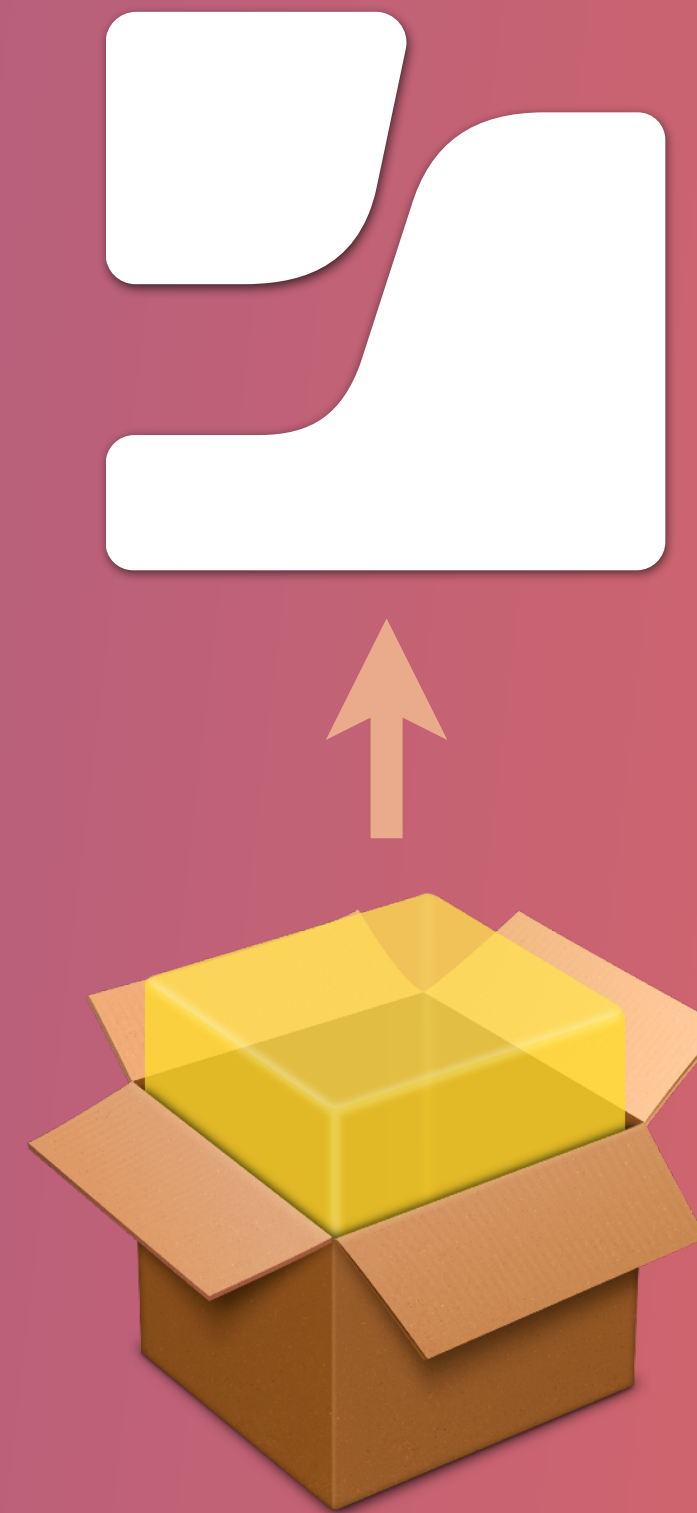
Download  
Extract  
Package  
Upload  
Configure  
Deploy



Download  
Extract  
Package  
Upload  
Configure  
Deploy



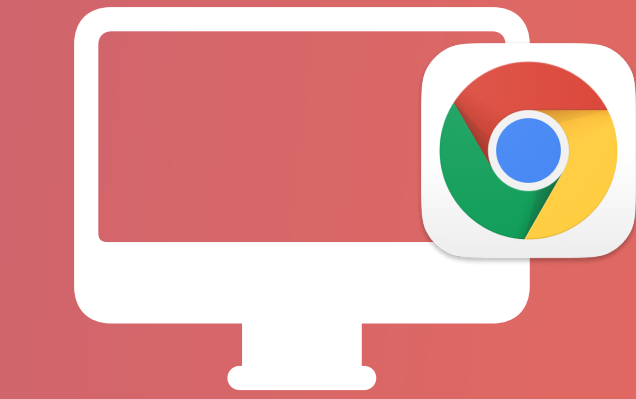
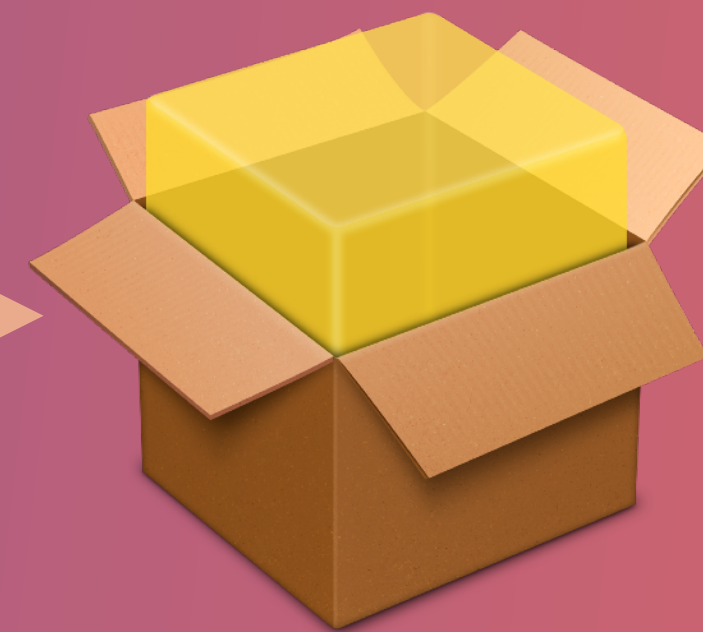
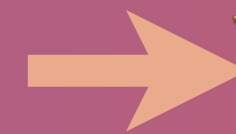
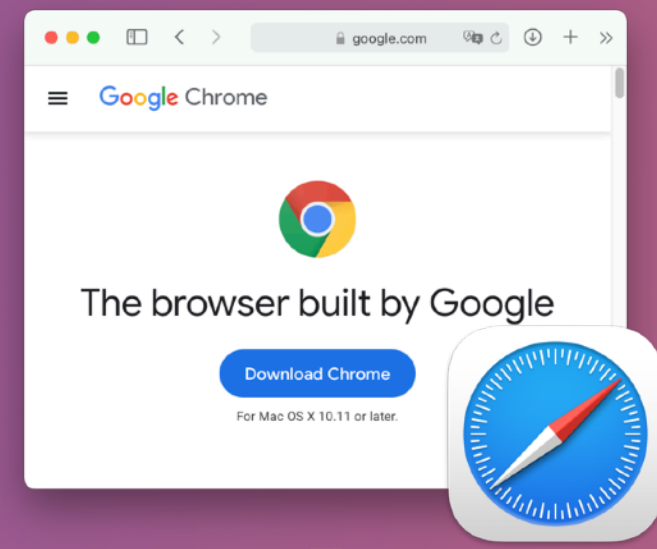
Download  
Extract  
Package  
Upload  
Configure  
Deploy



Download  
Extract  
Package  
Upload  
Configure  
Deploy



Download  
Extract  
Package  
Upload  
Configure  
Deploy



# Jamf Pro

The screenshot displays the Jamf Pro dashboard interface. On the left is a dark sidebar with navigation icons for Computers, Devices, and Users, and system information including version (10.20.0-b.2.t1582297324), managed devices (71 Computers, 46 Mobile Devices), and unmanaged devices (0 Computers, 8 Mobile Devices). The main content area is titled 'Dashboard' and is divided into two sections: 'Smart Computer Groups' and 'Policy Statuses'. The 'Smart Computer Groups' section contains five cards with titles like '\*NEEDS MACOS HIGH SIERRA (10.13)', 'COMPLIANCE - ENCRYPTION DISABLED', 'COMPLIANCE -- NO INVENTORY REPORT FOR 14 DAYS', 'FILEVAULT IS CONFIGURED', and 'GATEKEEPER STORE IDENTIFICATION DEVELOPMENT'. Each card shows a count of computers (28, 42, 71, 21, and partially visible 1 respectively). The 'Policy Statuses' section contains five cards with titles like '\*FILEVAULT ENFORCEMENT', '\*UPDATE INVENTORY', 'ADD SELF SERVICE TO DOCK', 'DROPBOX', and 'INSTALL...'. Each card features a donut chart showing completion percentages (9%, 32%, 90%, 4%, and partially visible 100% respectively) and a breakdown of completed and pending counts (e.g., 7 Completed, 46 Pending for FileVault Enforcement).

**jamf | PRO**

Computers Devices Users

**Dashboard**

**Smart Computer Groups**

- \*NEEDS MACOS HIGH SIERRA (10.13)**  
28 Computers
- COMPLIANCE - ENCRYPTION DISABLED**  
42 Computers
- COMPLIANCE -- NO INVENTORY REPORT FOR 14 DAYS**  
71 Computers
- FILEVAULT IS CONFIGURED**  
21 Computers
- GATEKEEPER STORE IDENTIFICATION DEVELOPMENT**  
1 Computers

**Policy Statuses**

- \*FILEVAULT ENFORCEMENT**  
9% Completed  
7 Completed, 46 Pending
- \*UPDATE INVENTORY**  
32% Completed  
23 Completed, 48 Pending
- ADD SELF SERVICE TO DOCK**  
90% Completed  
64 Completed, 7 Pending
- DROPBOX**  
4% Completed  
3 Completed, 68 Pending
- INSTALL...**  
100% Completed  
1 Completed, 48 Pending

# Jamf Pro

jamf | PRO

Computers | Devices | Users

INVENTORY

- Search Inventory
- Search Volume Content
- Licensed Software

CONTENT MANAGEMENT

- Policies
- Configuration Profiles
- Restricted Software
- Mac Apps
- Patch Management**
- eBooks

GROUPS

- Smart Computer Groups
- Static Computer Groups
- Classes

ENROLLMENT

- Enrollment Invitations
- PreStage Enrollments

SETTINGS

Computers

### Patch Management ⓘ

Filter Re 1 - 7 of 7

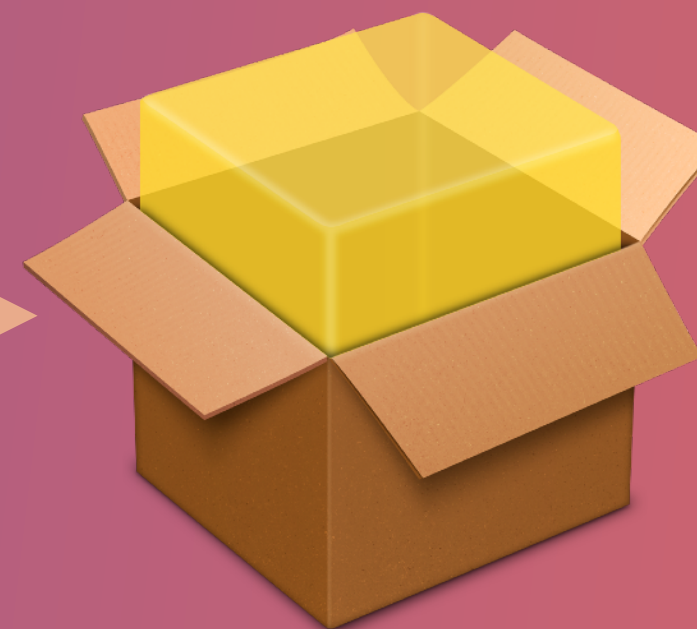
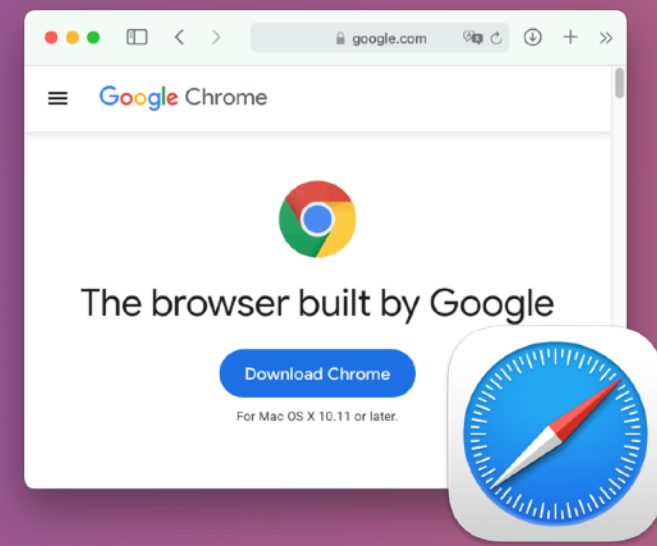
NAME	PUBLISHER	SOURCE	LATEST VERSION	LAST UPDATED
No category assigned				
1Password 7	AgileBits	Jamf	7.9.5	24/05/2022 at 6:23 PM
Adobe After Effects 2022	Adobe	Jamf	22.4	10/05/2022 at 8:25 PM
Adobe InDesign 2022	Adobe	Jamf	17.3.0.61	27/05/2022 at 11:49 AM
Discord	Discord	Jamf	0.0.267	08/06/2022 at 7:06 PM
Slack	Slack Technologies	Jamf	4.26.1	04/05/2022 at 10:39 PM
VMware Fusion 12	VMware	Jamf	12.2.3	30/03/2022 at 5:50 PM
macOS 10.15 Build	Apple Inc. (Legacy Definition)	Jamf	10.15.7 (19H1922)	16/05/2022 at 9:39 PM

# Jamf Pro

The screenshot displays the Jamf Pro web interface. The top navigation bar includes the Jamf Pro logo and three main menu items: Computers, Devices, and Users. A left-hand sidebar contains several categories: INVENTORY (Search Inventory, Search Volume Content, Licensed Software), CONTENT MANAGEMENT (Policies, Configuration Profiles, Restricted Software, Mac Apps, Patch Management, eBooks), GROUPS (Smart Computer Groups, Static Computer Groups, Classes), ENROLLMENT (Enrollment Invitations, PreStage Enrollments), and SETTINGS. The main content area is titled 'Computers : Patch Management' and shows a breadcrumb trail '← Slack ⓘ'. Below this, there are tabs for 'Patch Report', 'Software Title Settings', 'Definition' (which is selected), and 'Patch Policies'. The 'Definition for Slack' section features a green lock icon and the text 'This software title definition has been verified by Jamf.' Below this is a search filter box labeled 'Filter Re' and a pagination indicator '1 - 25 of 85'. A table lists the software title versions with columns for VERSION, RELEASE DATE, INCREMENTAL UPDATE, REBOOT REQUIRED, and DEPENDENCIES.

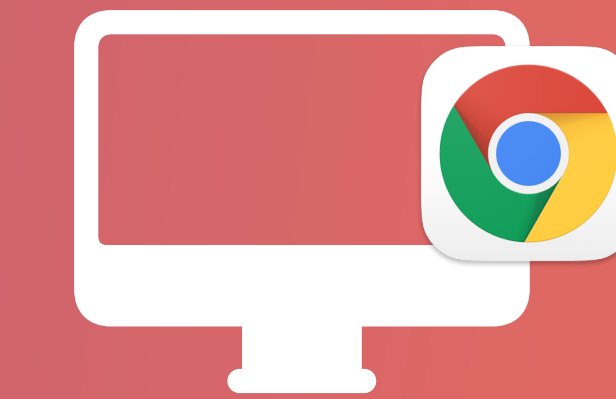
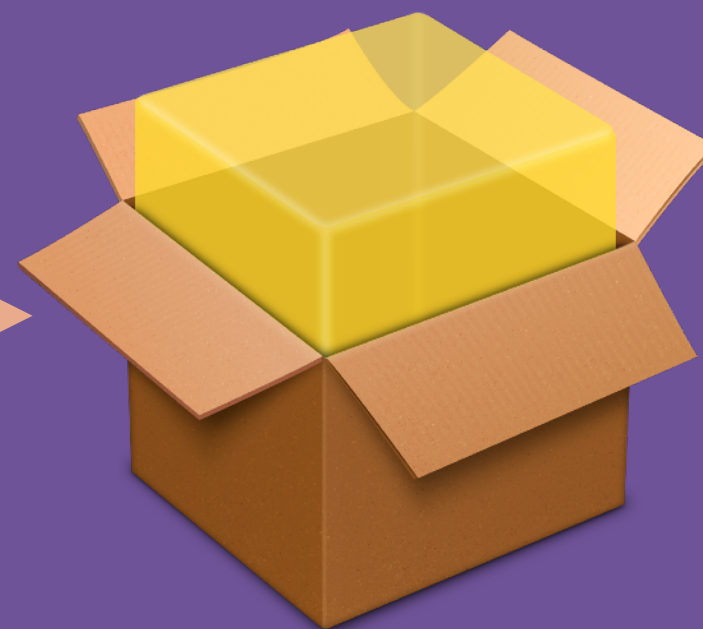
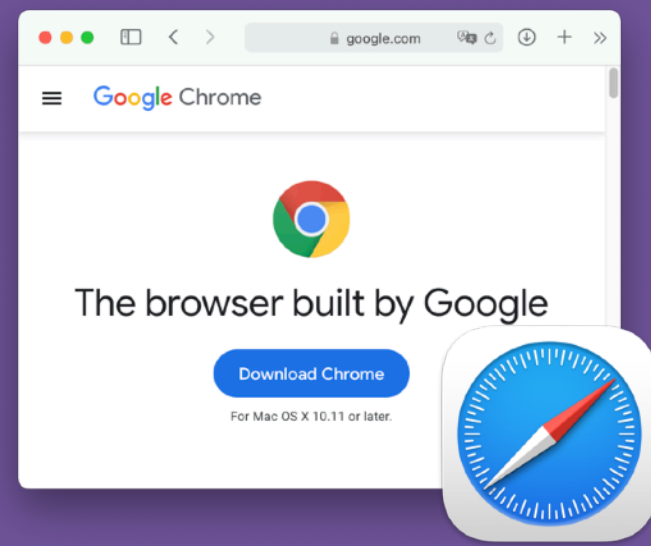
VERSION	RELEASE DATE	INCREMENTAL UPDATE	REBOOT REQUIRED	DEPENDENCIES
4.26.1	04/05/2022 at 8:00 PM	Not Required	No	
4.26.0	25/04/2022 at 5:00 PM	Not Required	No	
4.25.0	24/03/2022 at 5:00 PM	Not Required	No	
4.24.1	10/03/2022 at 5:00 PM	Not Required	No	
4.24.0	10/03/2022 at 5:00 PM	Not Required	No	
4.23.0	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	

Download  
Extract  
Package  
Upload  
Configure  
Deploy

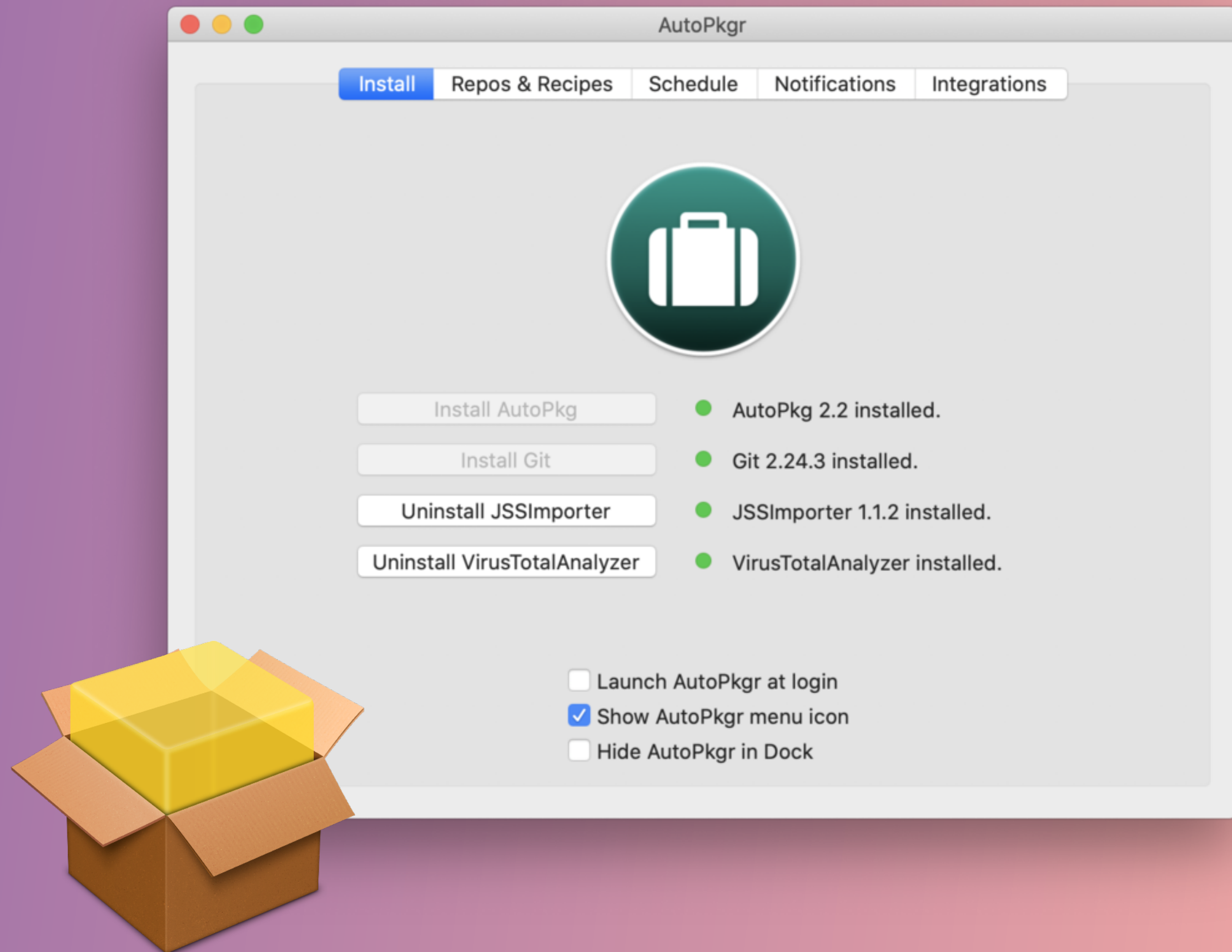


Download  
Extract  
Package  
Upload  
Configure  
Deploy

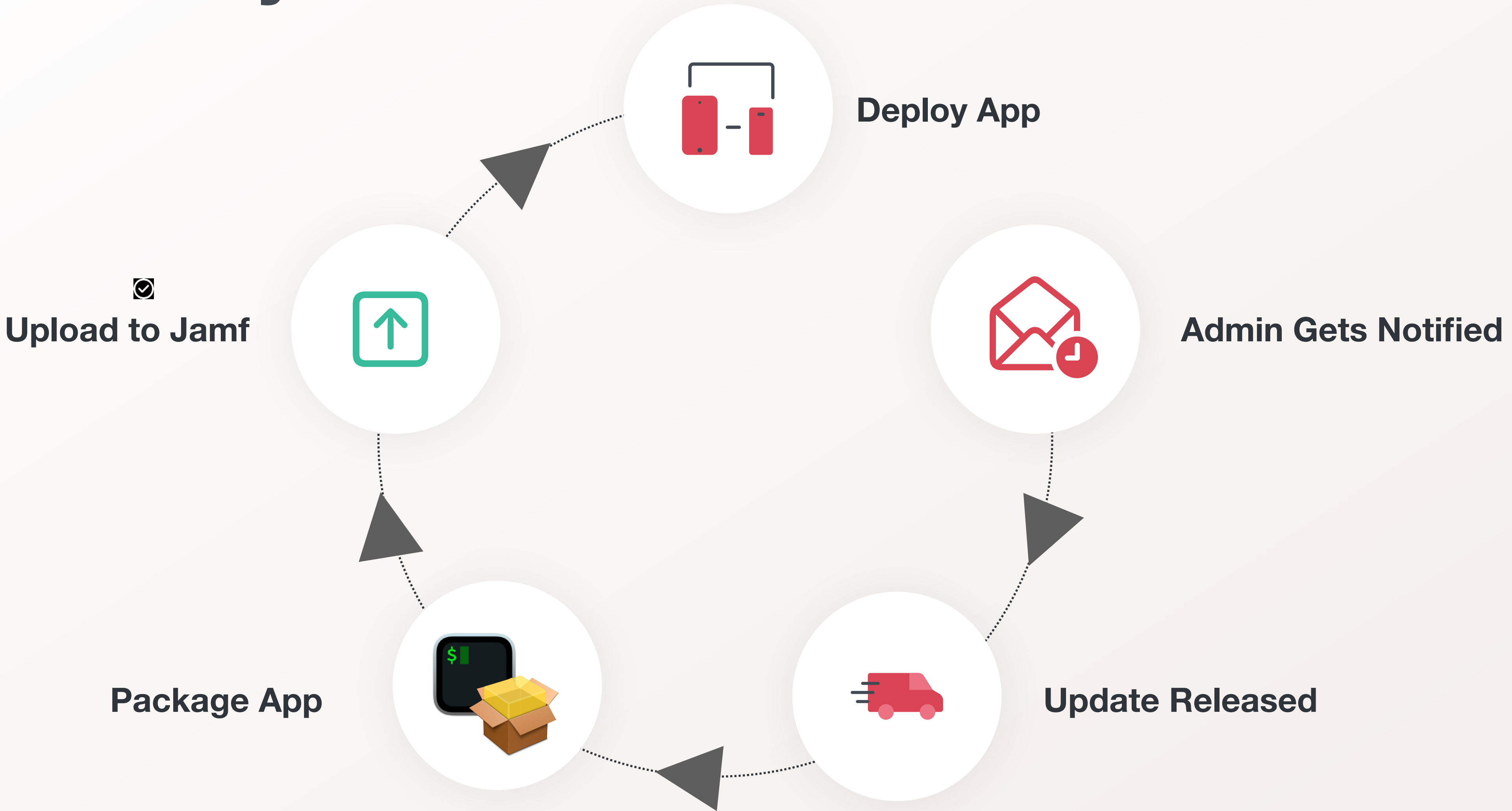
# AutoPkg

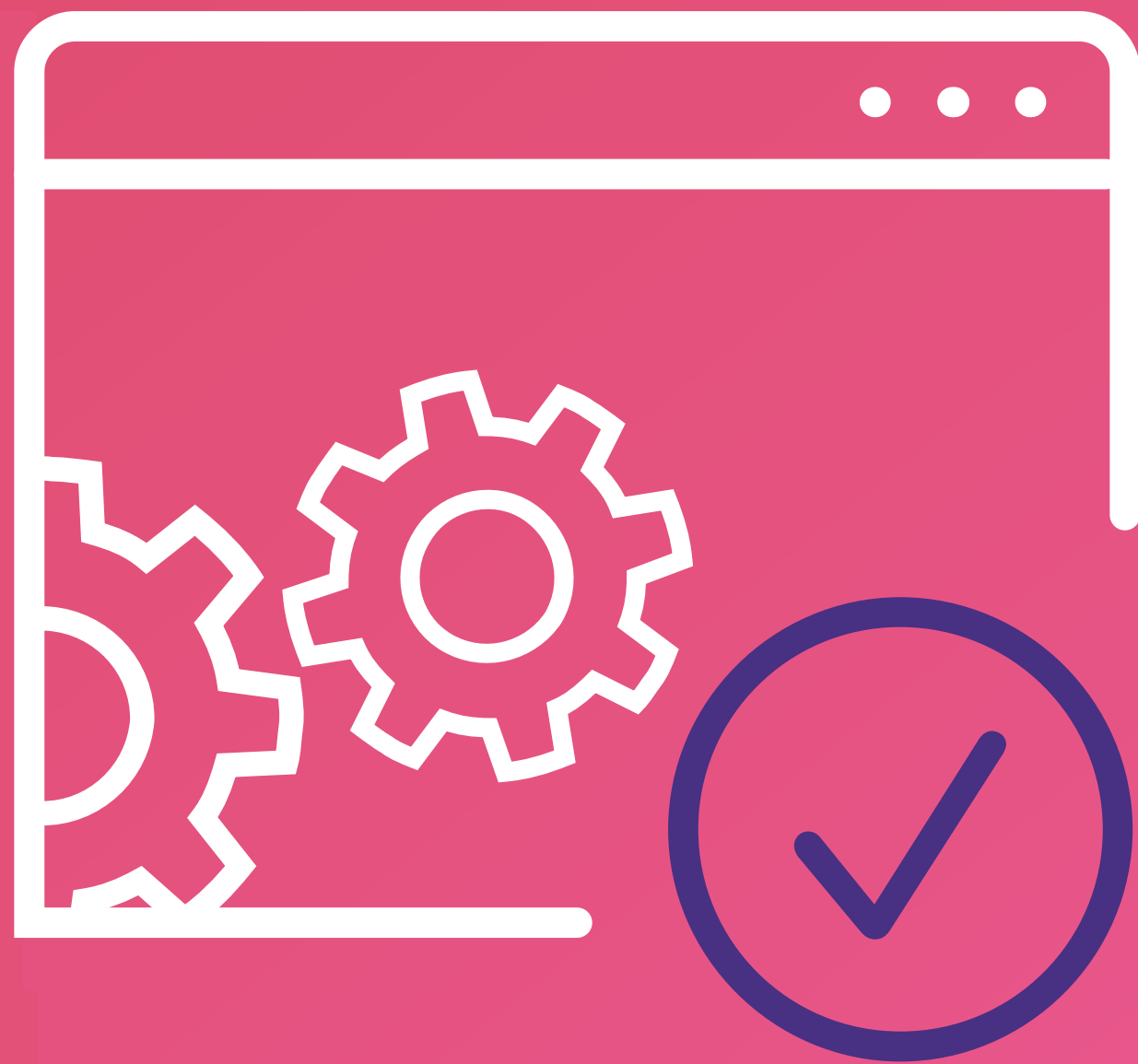


# AutoPkgr

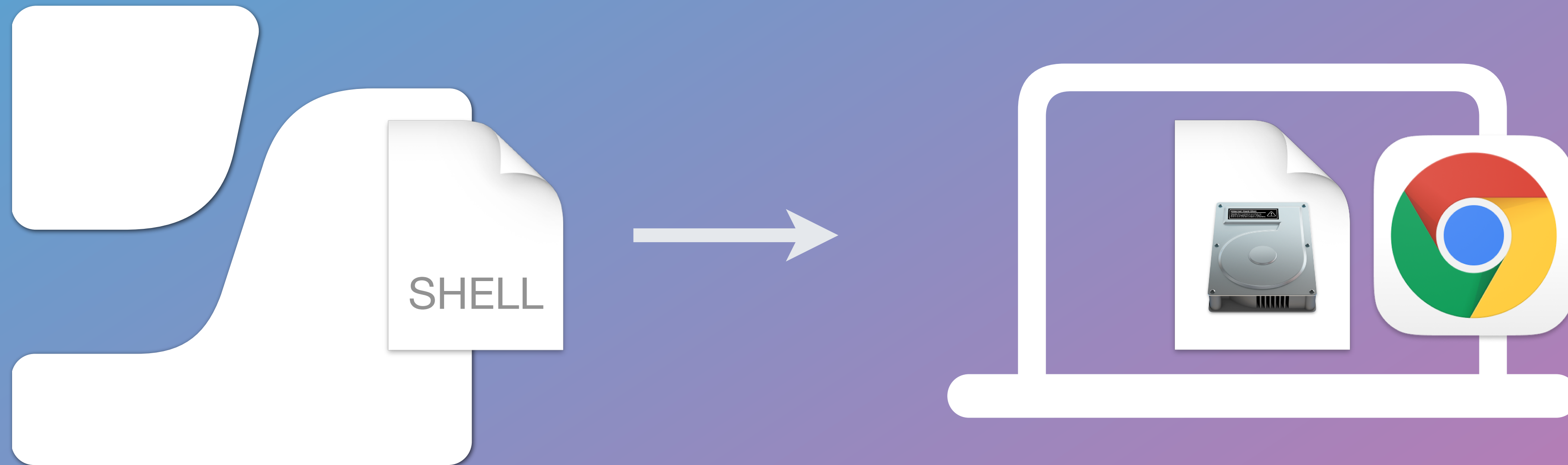


# Installation Cycle





# Installomator



# Installomator

- ▶ Over 400+ Applications
- ▶ [https:// downloads](https://downloads)
- ▶ Gatekeeper Verification
  - ▶ Apple Developer ID Signature
  - ▶ Notarization

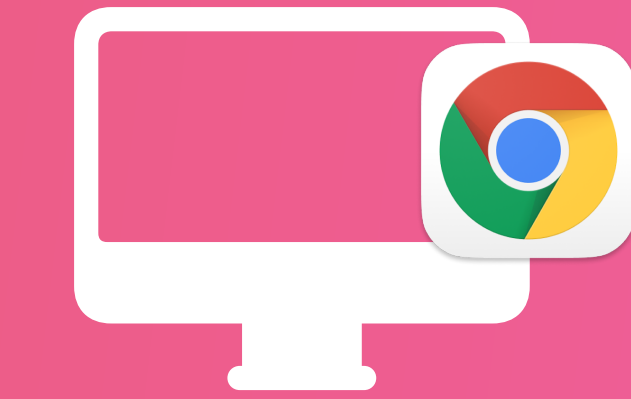
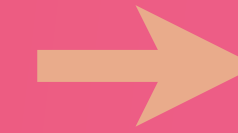
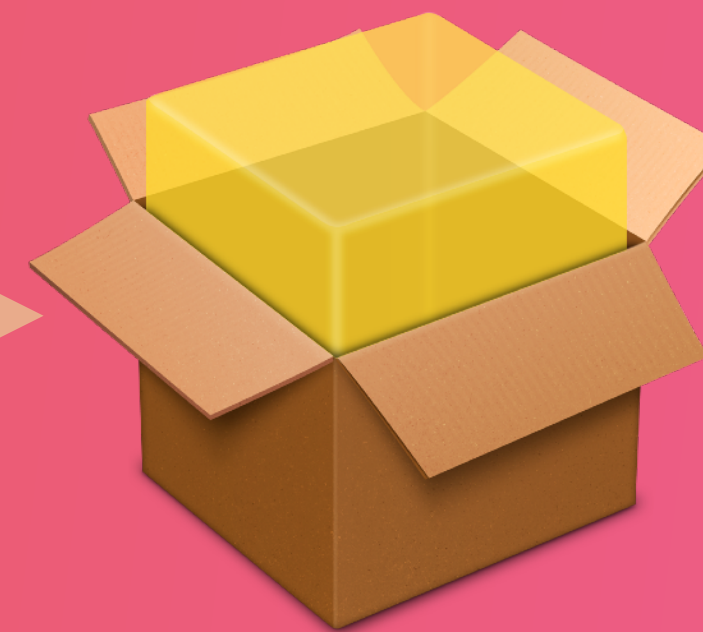
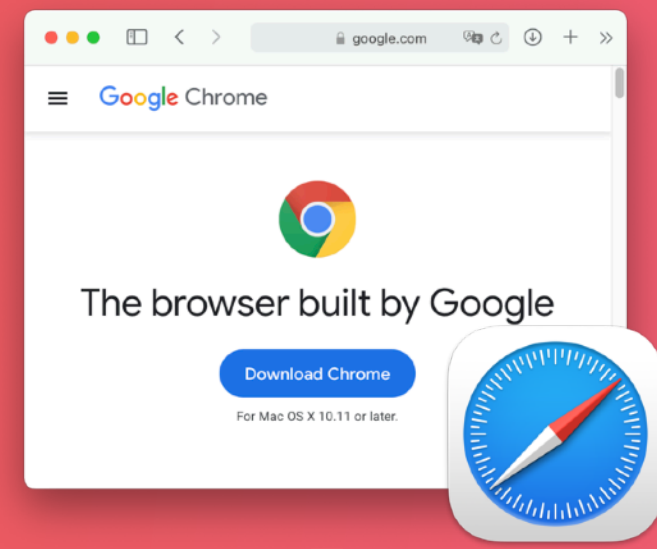


**PREVIEW**

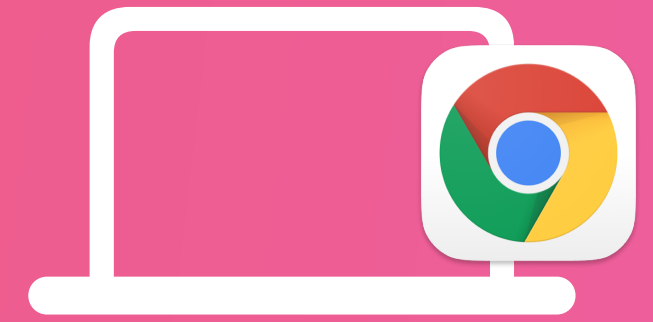
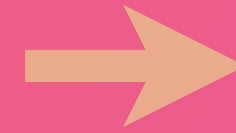
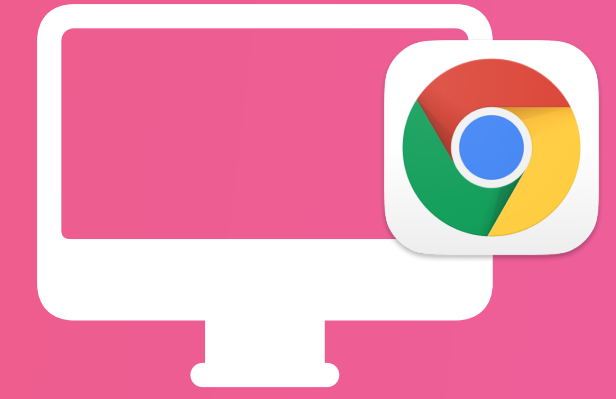
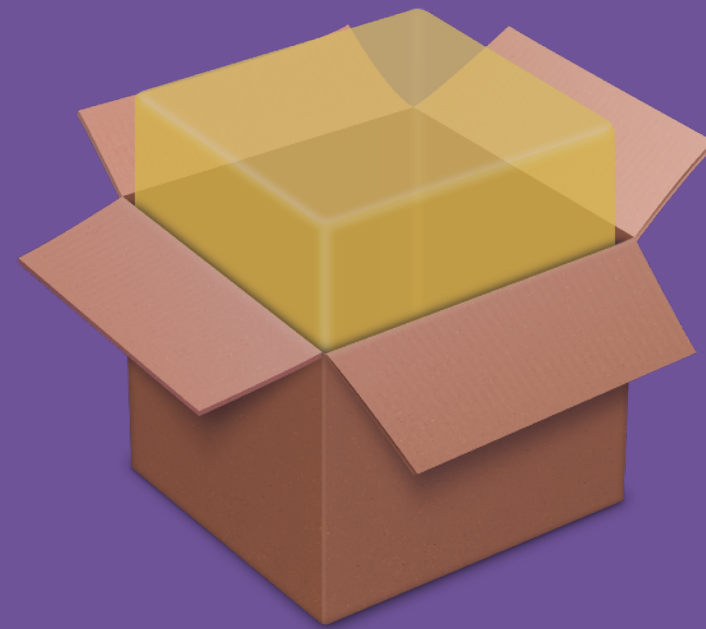
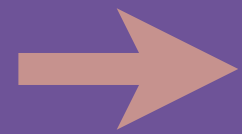
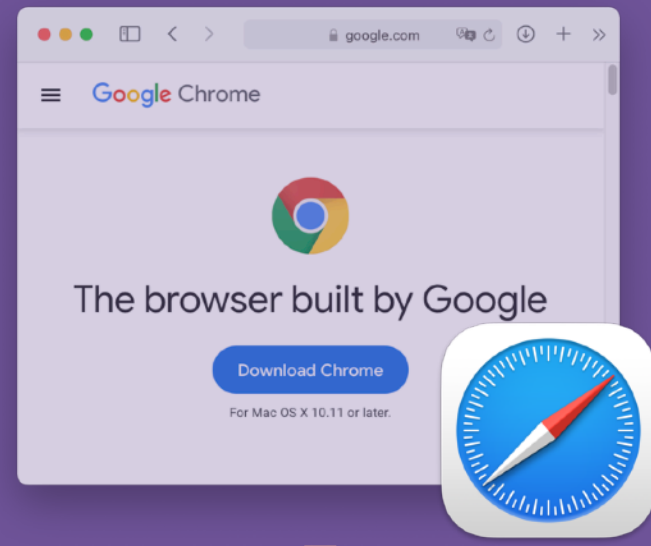
# Introducing Jamf App Catalog



Download  
Extract  
Package  
Upload  
Configure  
Deploy

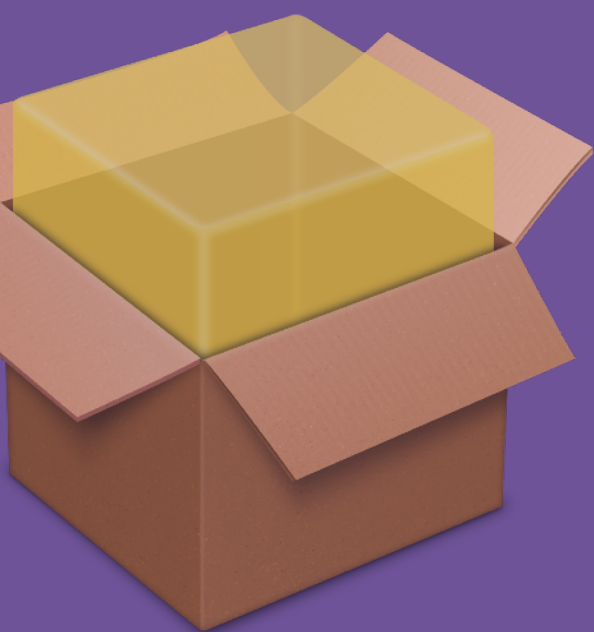
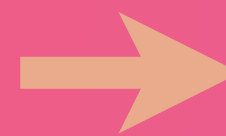
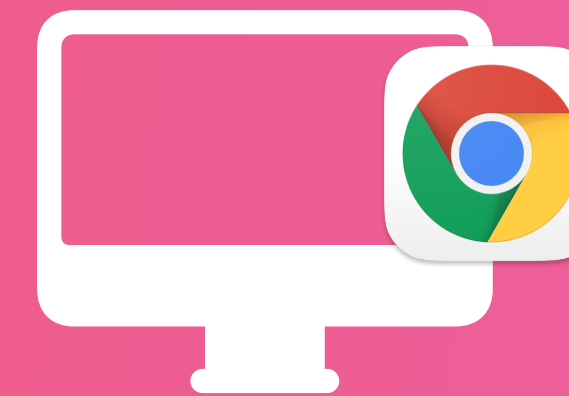


Download  
Extract  
Package  
Upload  
Configure  
Deploy



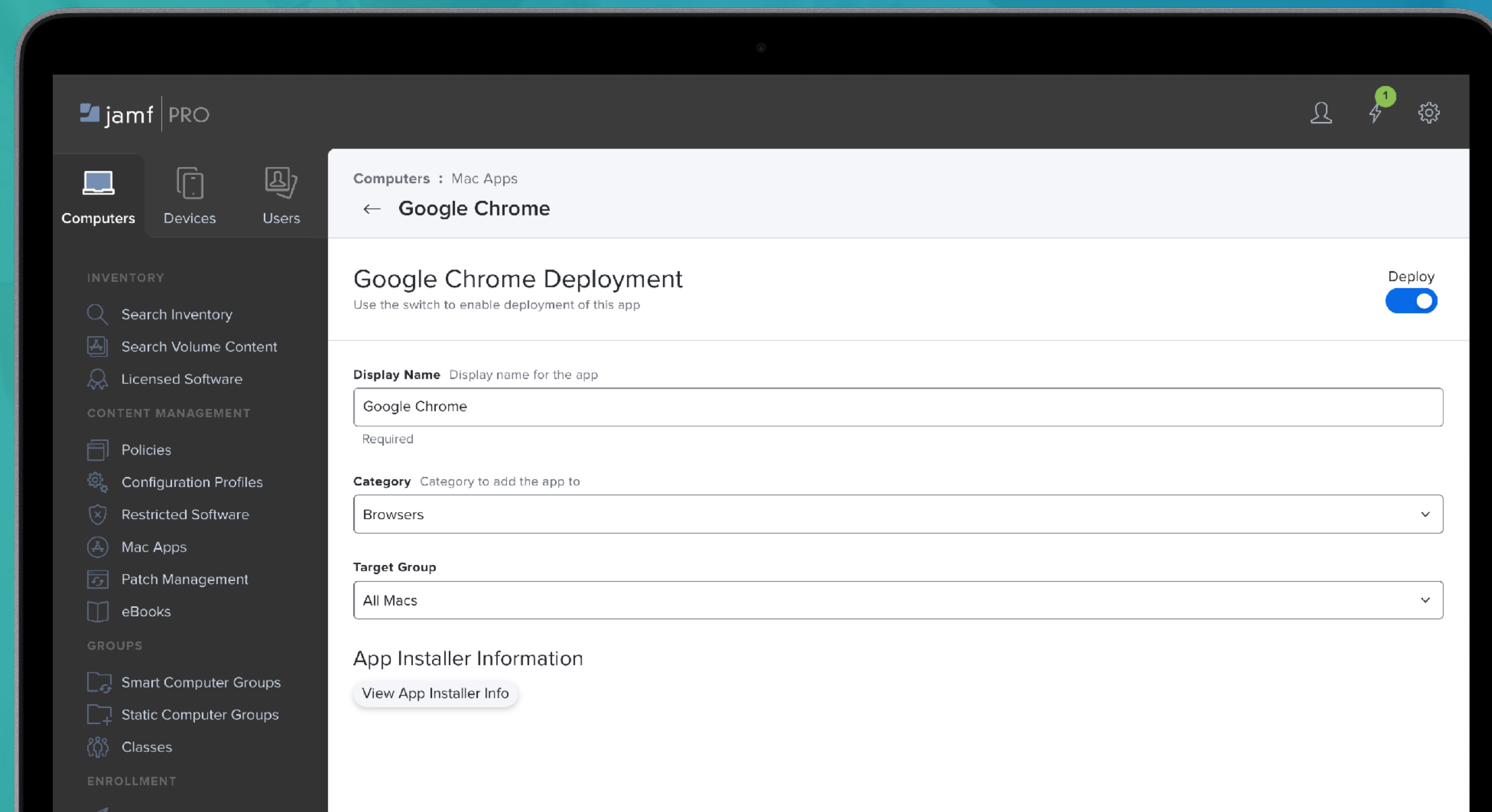


**InstallEnterpriseApplication**



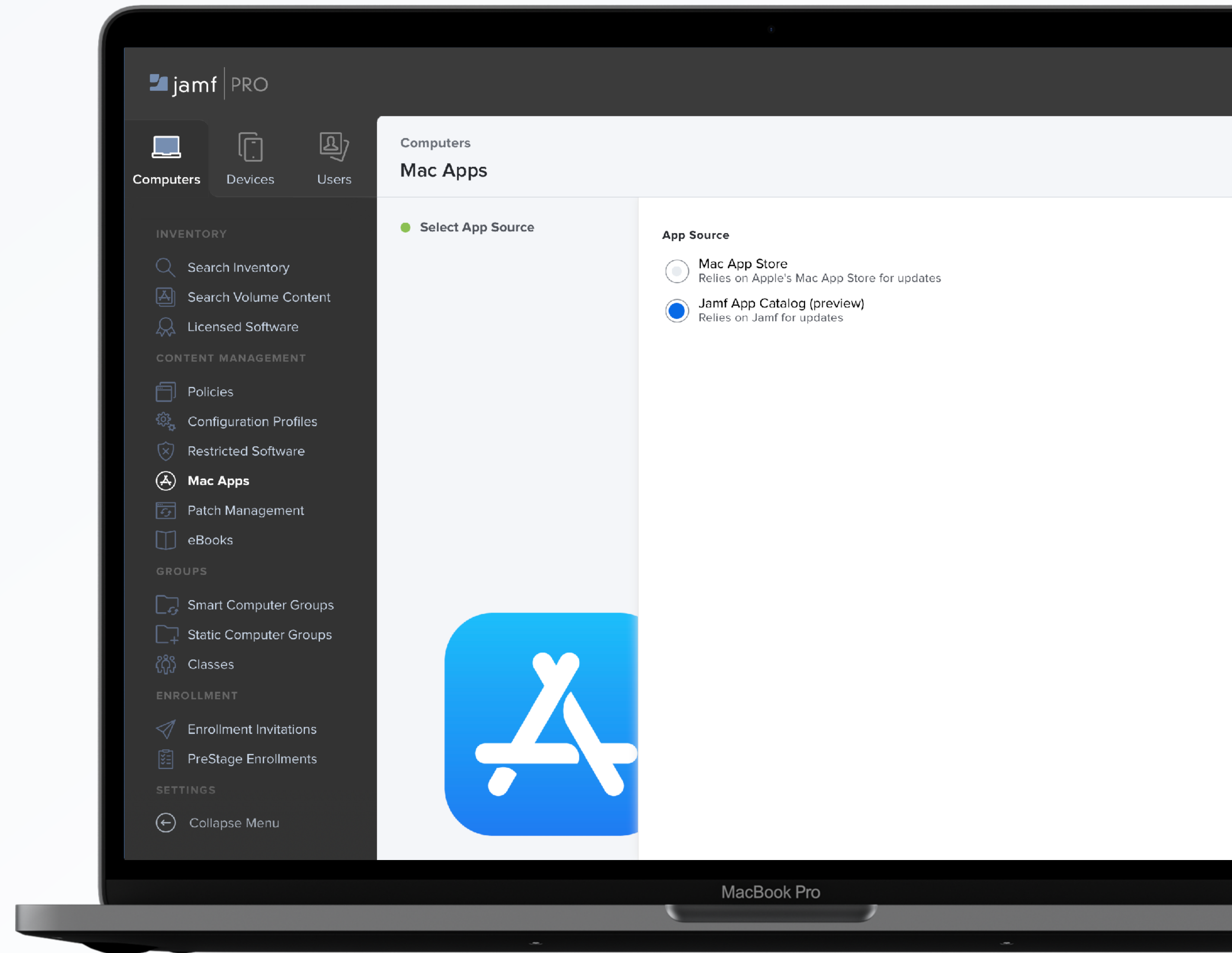
# App Lifecycle Management Simplified

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



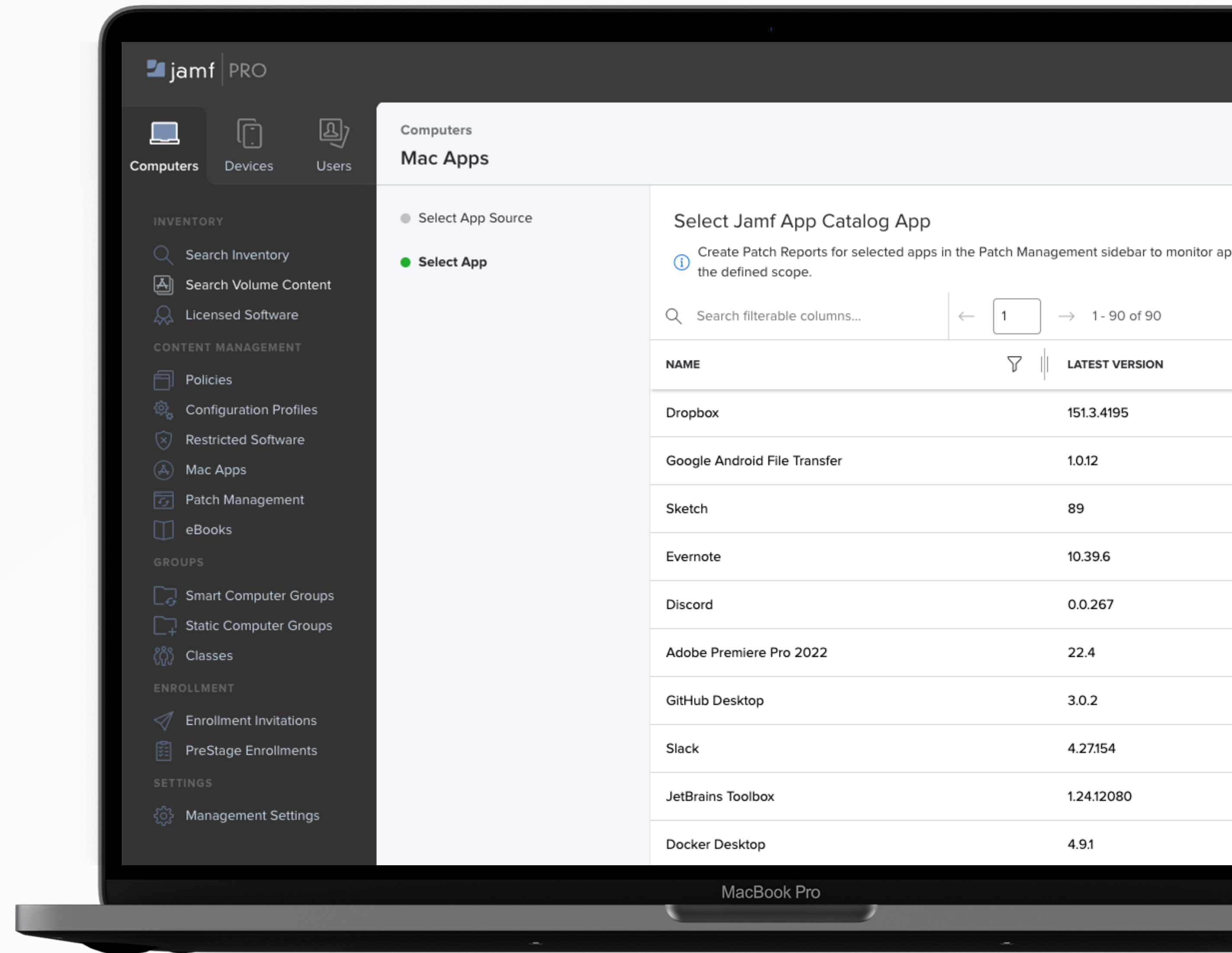
# App Lifecycle Management Jamf Pro

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



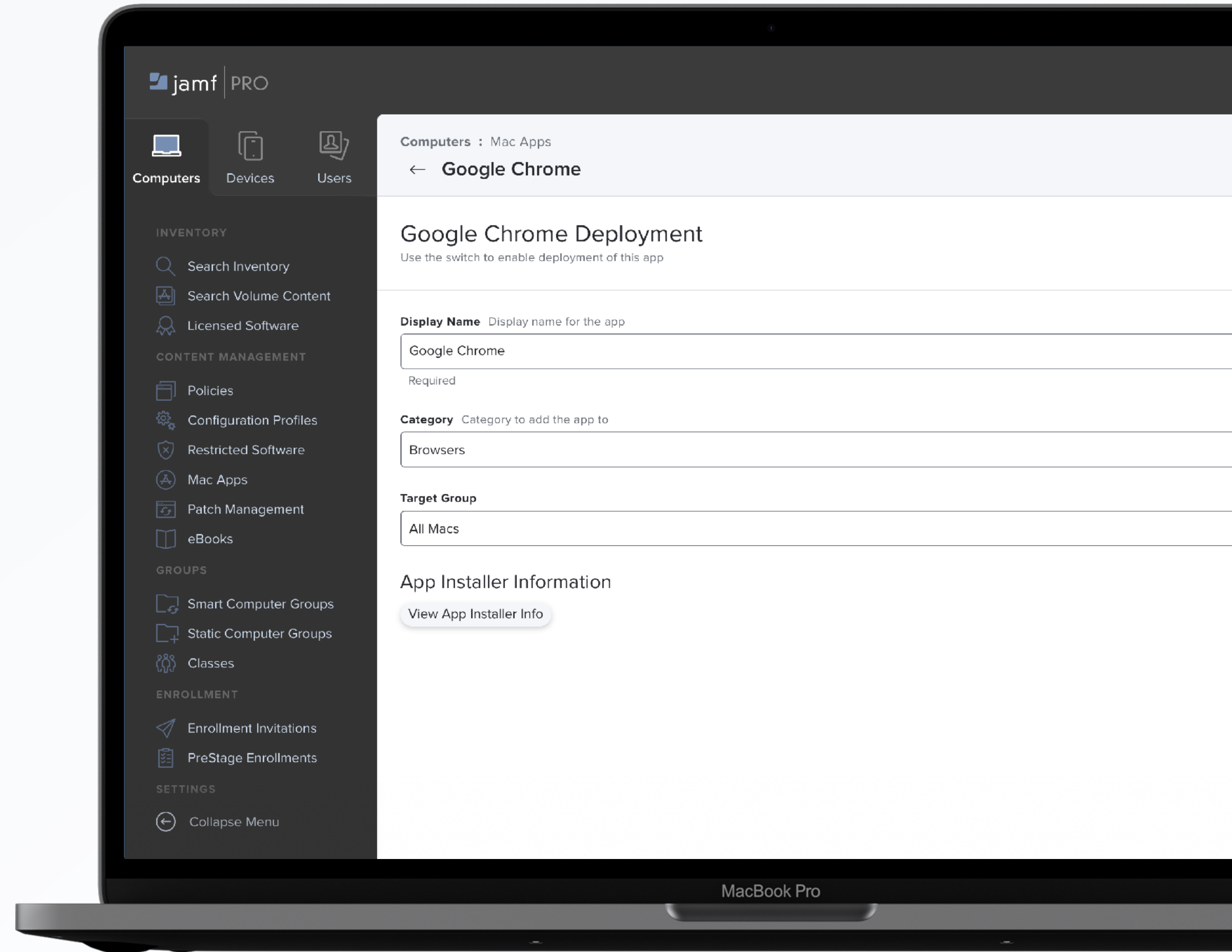
# App Lifecycle Management Jamf Pro

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

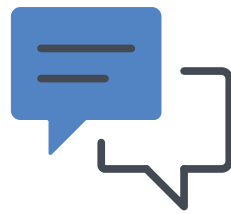


# App Lifecycle Management Jamf Pro

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



# 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





## macOS Updates






# Software Updates

Some great external tools

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

**Software Updates Require Restart**




• 5 out of 5 deferrals remain available.

Defer software update for:

2 minutes

Please make selection in 00:00:20

## Nudge



**Your device requires a security update**  
A friendly reminder from your local IT team


**Your device will restart during this update**   
Updates can take around 30 minutes to complete

**Important Notes**

A fully up-to-date device is required to ensure that IT can accurately protect your device.

If you do not update your device, you may lose access to some items necessary for your day-to-day tasks.

To begin the update, simply click on the Update Device button and follow the provided steps.



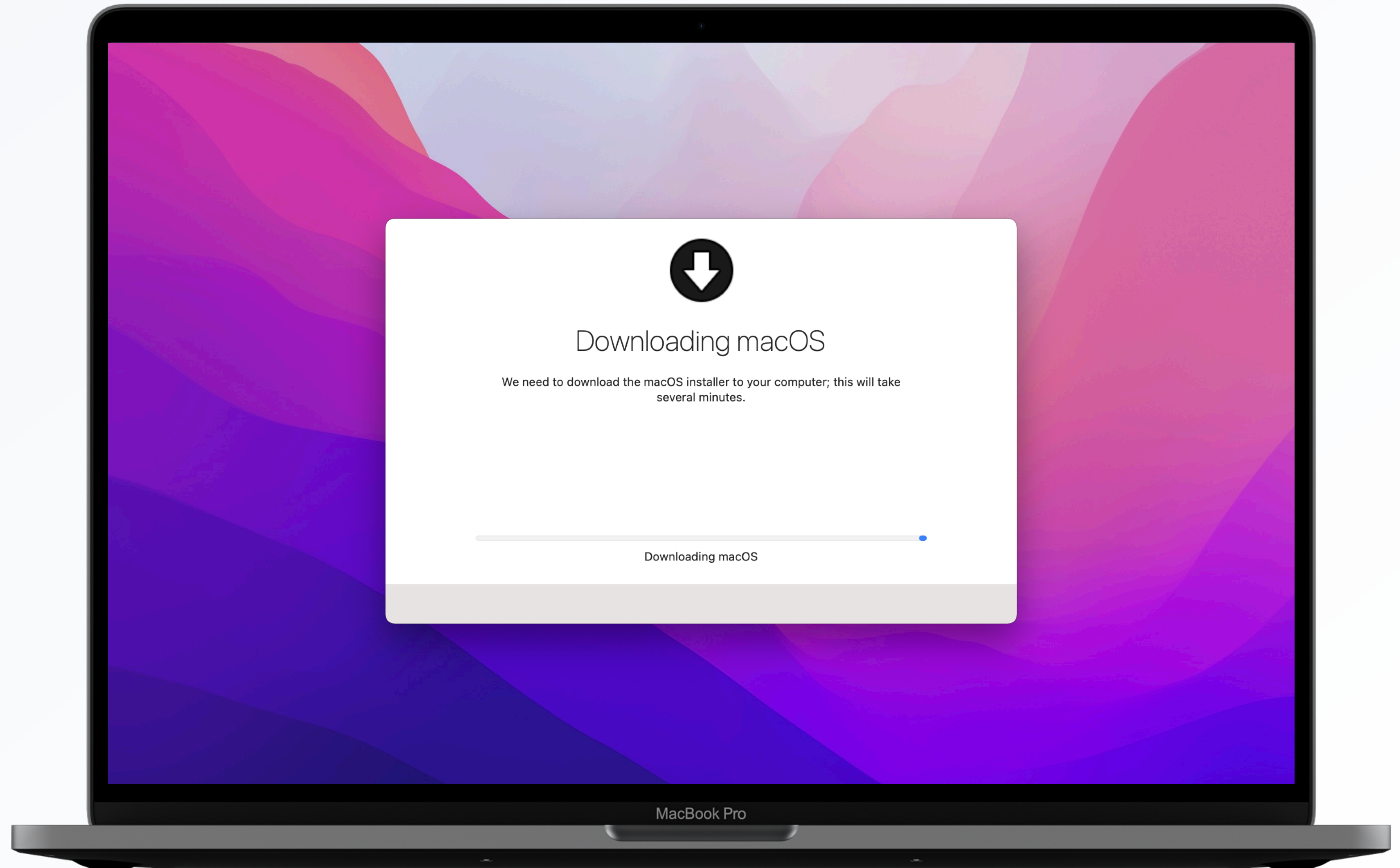
More Info

# More than just a name...

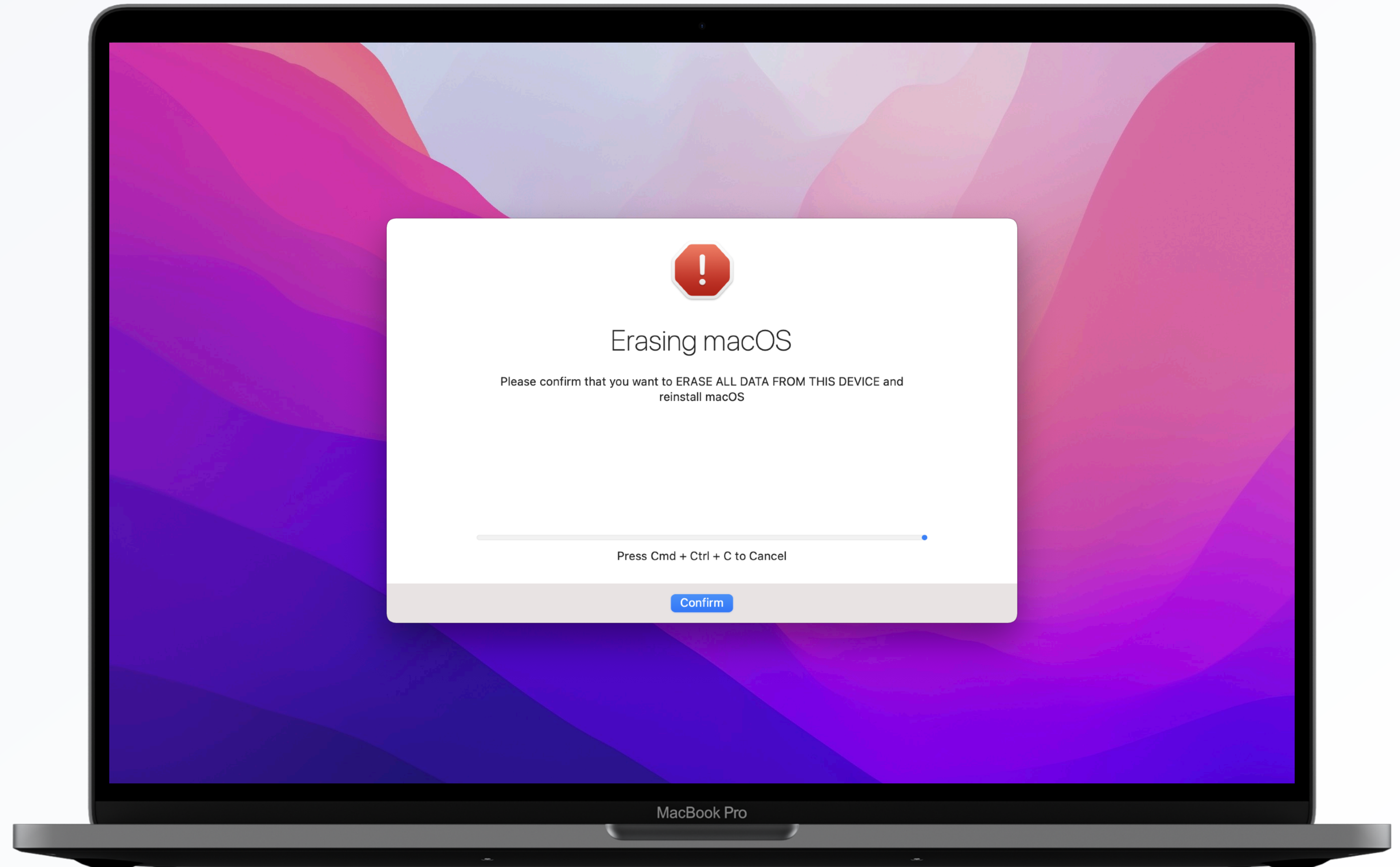


**erase-install.sh**

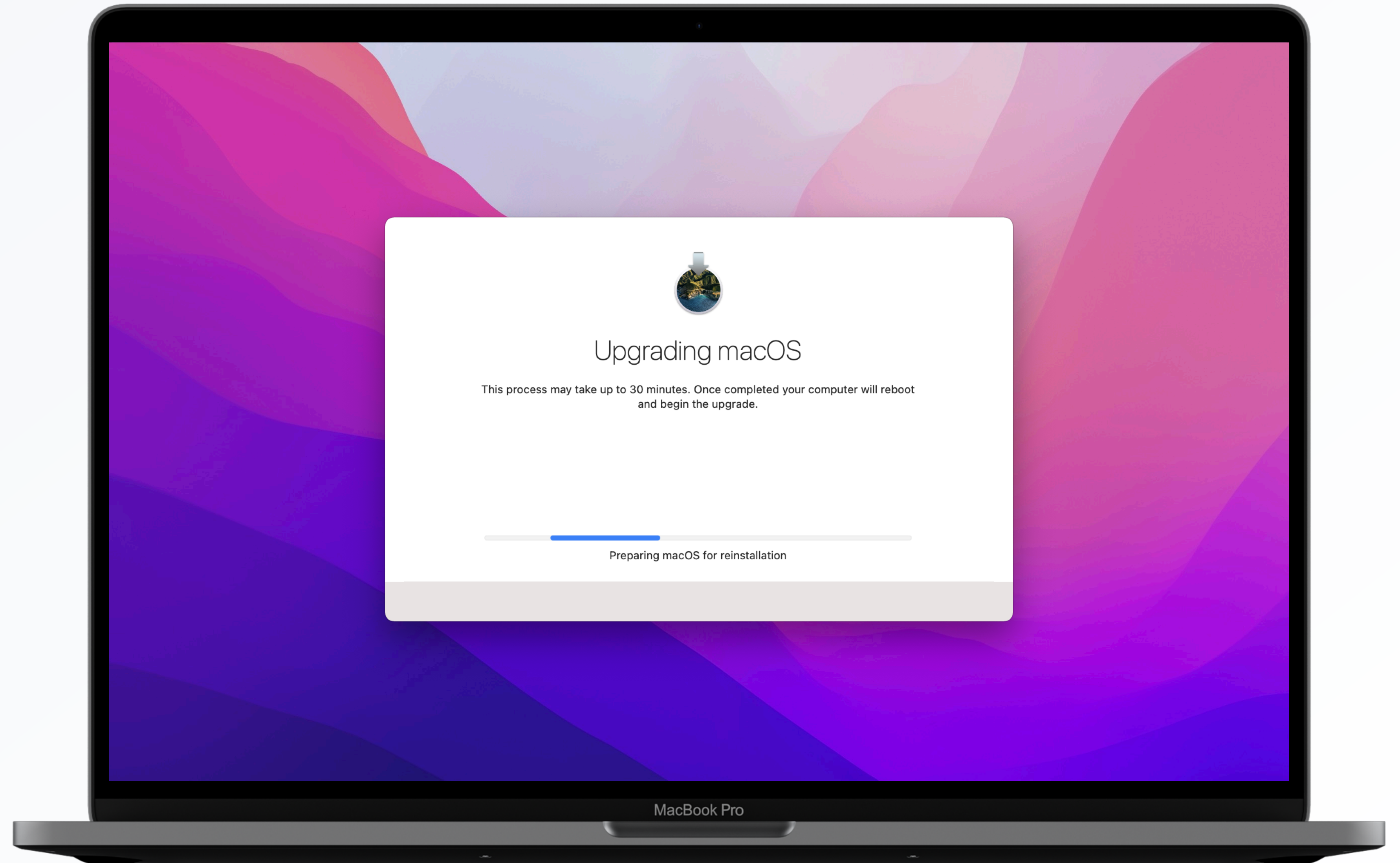
# Download the macOS installer



# Start again?



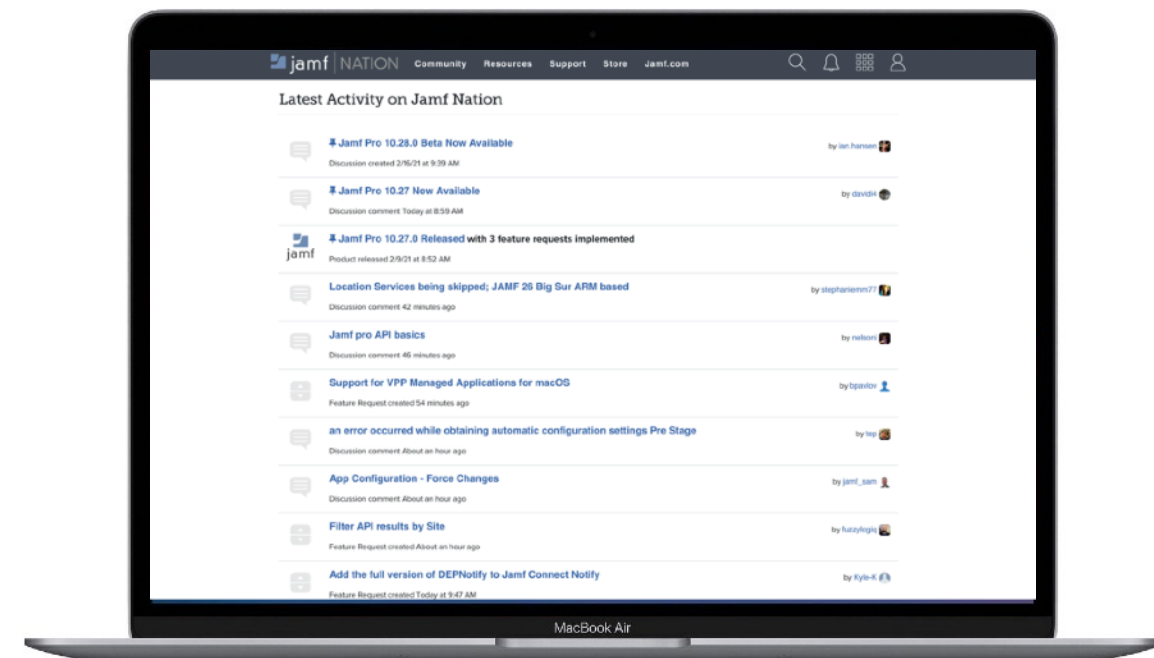
# Upgrade



# Jamf Nation and Jamf Marketplace

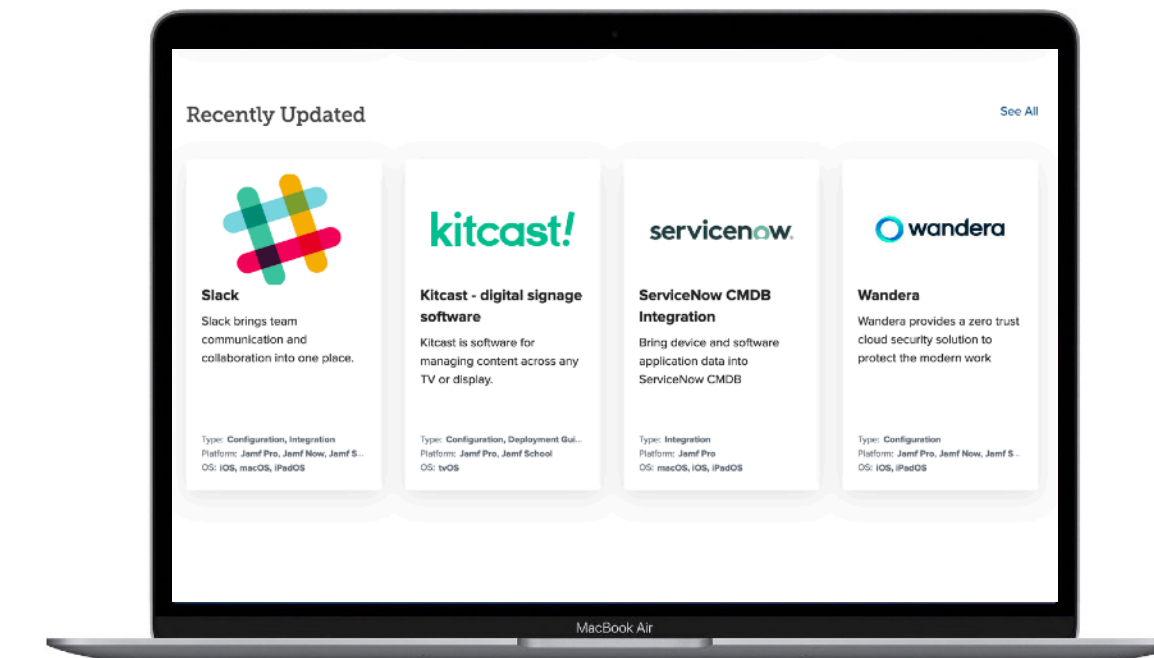
Expanded Ecosystem and Support Strengthen the Jamf Platform and Improve Jamf Efficiency

## 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

