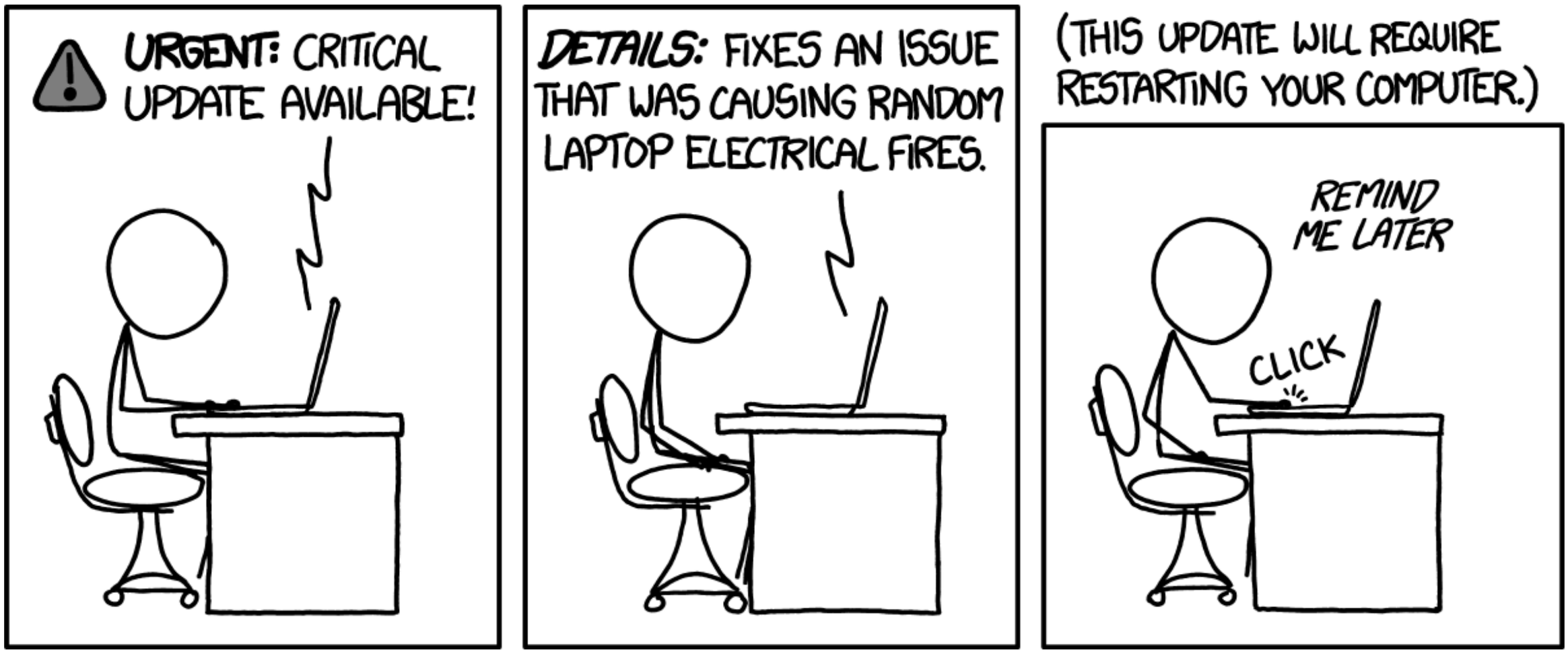
Keepers of the Machines:

Examining How Sys Admins Manage Software Updates

Frank Li
Nathan Malkin

Lisa Rogers

Arunesh Mathur
Marshini Chetty



Source: *https://www.xkcd.com/1328/*

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

BIZ & IT —

Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

DAN GOODIN - 9/13/2017, 8:12 PM

TechRepublic

Drupalgeddon 2 wreaking havoc on 900+ sites because IT still hasn't applied updates

By **Brandon Vigliarolo**  in **Security**

on June 7, 2018, 7:38 AM PST

Despite the fact that the Drupal exploit was reported-and patched-in March 2018, some 115,000 websites are still vulnerable.

16 Aug

Large Insurance Company Settles for $5.5 Million over "Failed To Patch" Data Breach

Stu Sjouwerman

A large insurance company (Nationwide) agreed to pay a total of $5.5 Million to settle charges brought by 32 states resulting from the loss of critical consumer information attributable to a criminal data breach.

Nationwide®

Prior Work: End User Patching

Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences

Rick Wash, Er
De

{wash,e

Betrayed By Updates: How Negative Experiences Affect Future Security

Kami Vaniea, Emilee Rader, Rick Wash
Department of Telecommunication, Information Studies, and Media

{v

Tales of Software Updates: The process of updating software

Kami Vaniea
The University of Edinburgh

Yasmeen Rashidi
Indiana University
USA
edu

"They Keep Coming Back Like Zombies": Improving Software Updating Interfaces

Arunesh Mathur Josefine Engel

Sonam Sobti
sonam.sobti9@gmail.com

shini Chetty
ini@umd.edu

Information Studies
e Park

Quantifying Users' Beliefs about Software Updates

Arunesh Mathur*, Nathan Malkin†, Marian Harbach‡, Eyal Peer§ and Serge Egelman‡†
*Princeton University †University of California, Berkeley
‡International Computer Science Institute §Consumers Behavioral Insights Lab, Bar-Ilan University, Israel
amathur@cs.princeton.edu nmalkin@cs.berkeley.edu mharbach@icsi.berkeley.edu
eyal.peer@biu.ac.il egelman@cs.berkeley.edu

Prior Work: End User Patching

Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences

Rick Wash, Er
De

{wash,

Betrayed By Updates: How Negative Experiences Affect Future Security

Media

are Updates: dating software

Yasmeen Rashidi
Indiana University
USA
edu

bies": Improving faces

Arunesh Mathur Josefine Engel

Sonam Sobti
sonam.sobti9@gmail.com

shini Chetty
ini@umd.edu
Information Studies
e Park

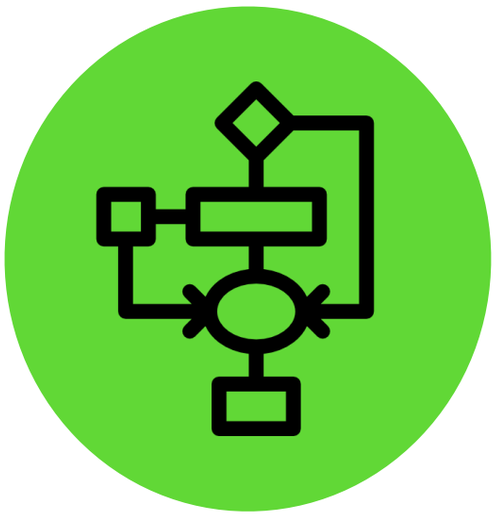
What about sys admins?

Quantifying Users' Beliefs about Software Updates

Arunesh Mathur*, Nathan Malkin†, Marian Harbach‡, Eyal Peer§ and Serge Egelman‡†
*Princeton University †University of California, Berkeley
‡International Computer Science Institute §Consumers Behavioral Insights Lab, Bar-Ilan University, Israel
amathur@cs.princeton.edu nmalkin@cs.berkeley.edu mharbach@icsi.berkeley.edu
eyal.peer@biu.ac.il egelman@cs.berkeley.edu

Research Questions

Update Processes



What are the update steps, processes, and workflows of admins?

Impact On Effectiveness

What are the consequences of admin actions / decisions?

Study Method

Multi-part user study

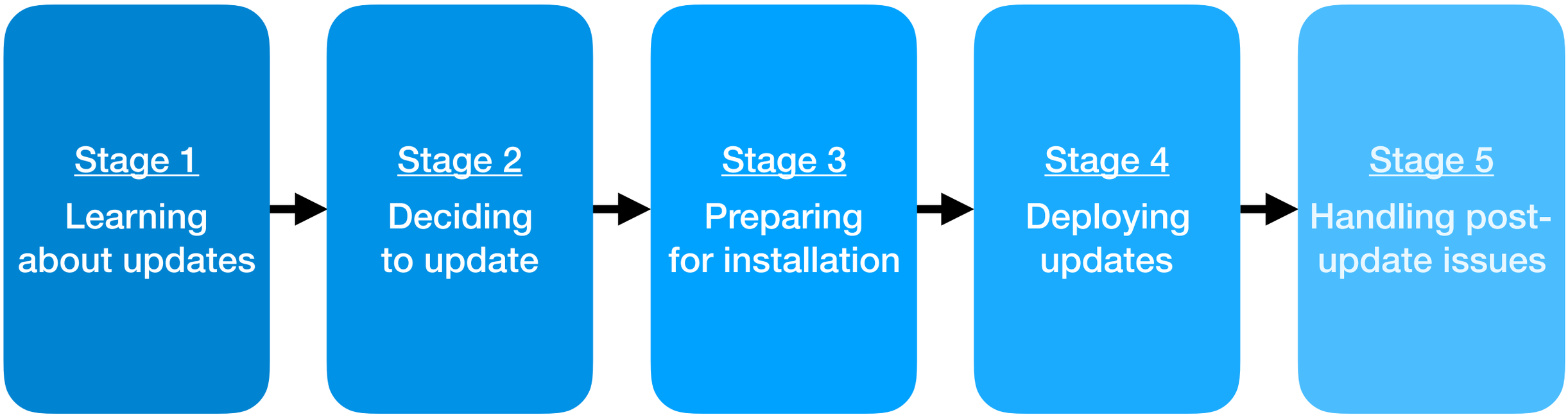
1. Pilot interviews (n=7)
2. Online Survey (n=102)
3. Semi-structured interviews (n=17)

Recruitment: social media, email lists, Reddit, LISA

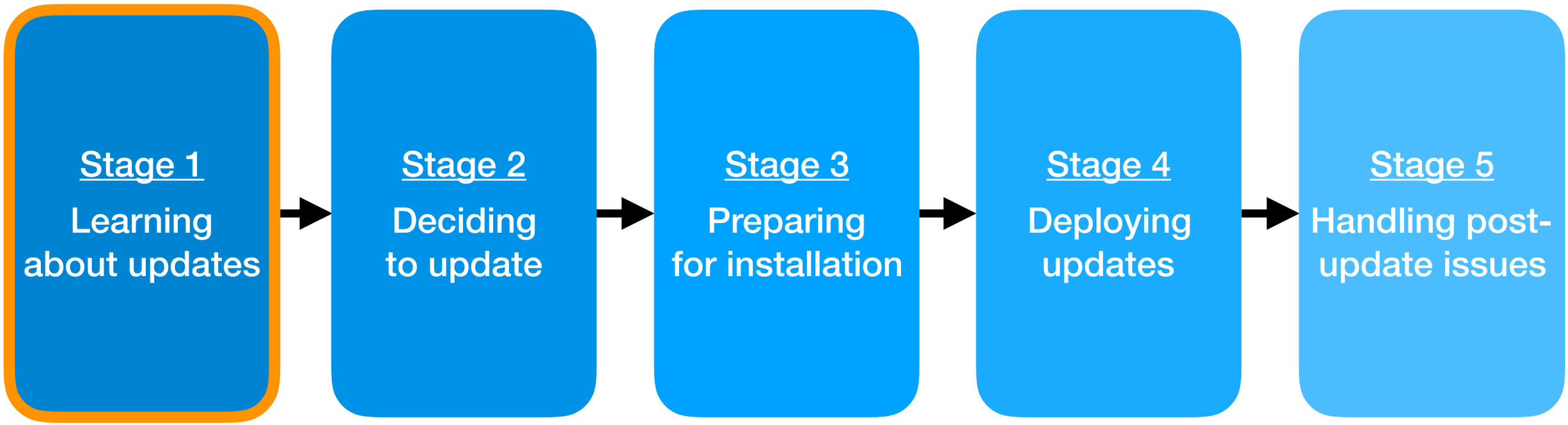
Screening: 18+ yrs old, US residents, employed as admin for 1+ yr at org with 5+ employees

Analysis Approach: inductive thematic analysis

Update Process Stages

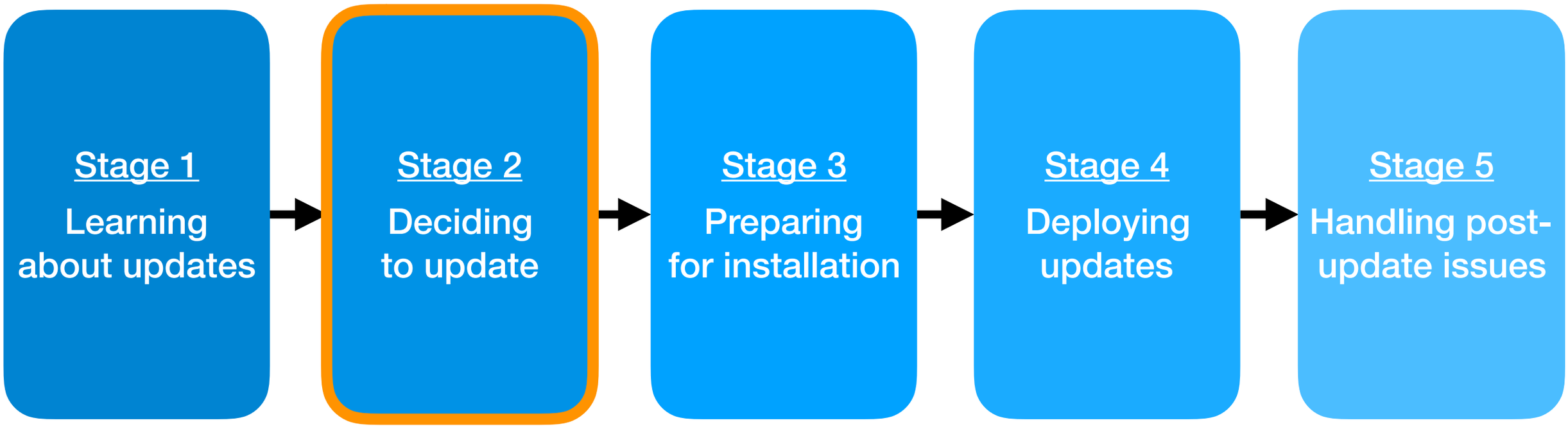


Update Process Stages



- Proactive search
- Update info spread out

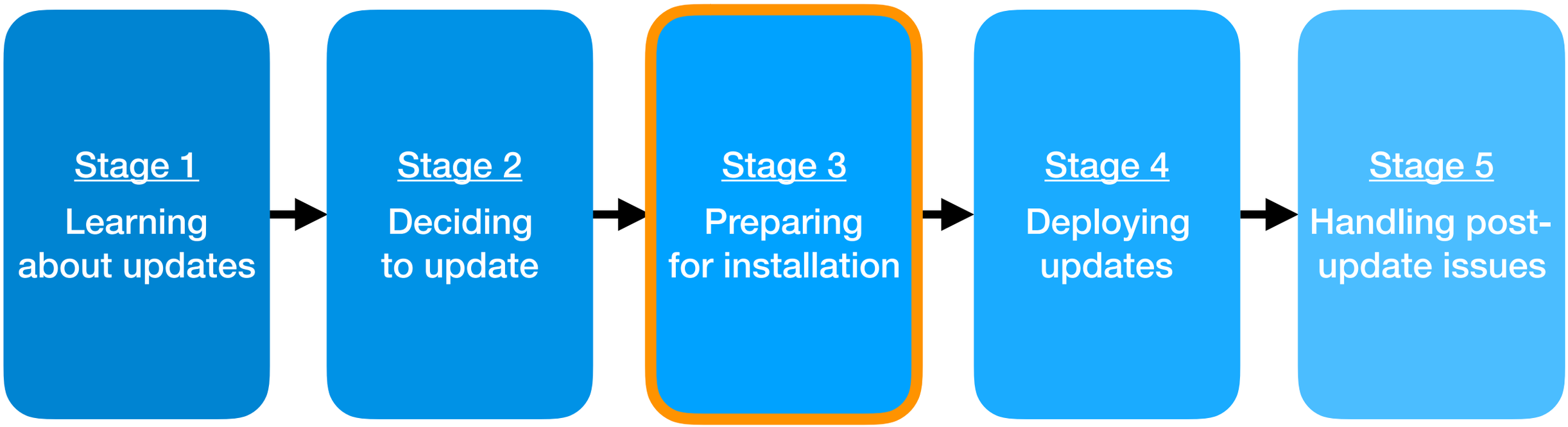
Update Process Stages



- Proactive search
- Update info spread out

- Prioritize by update type

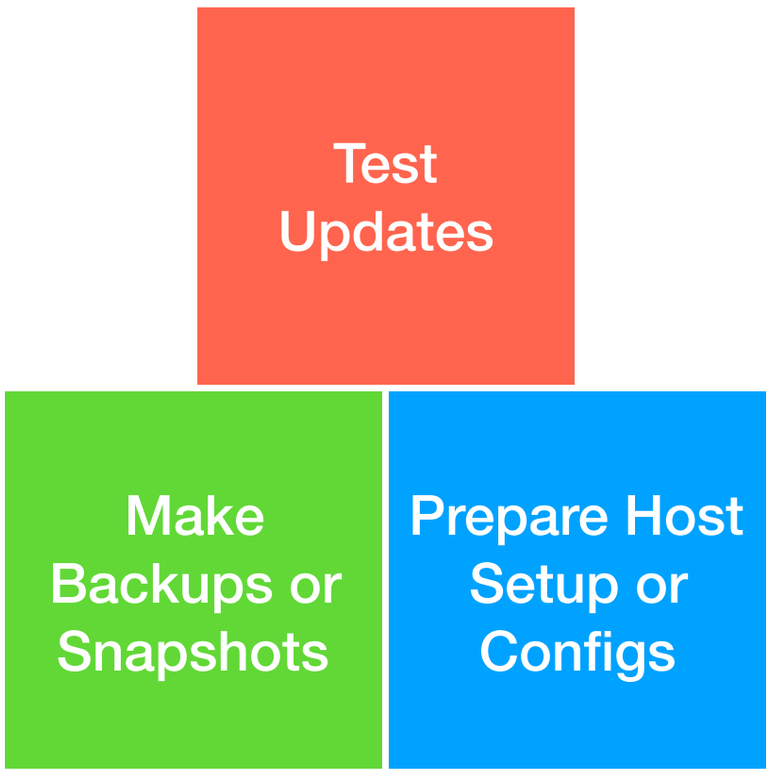
Update Process Stages



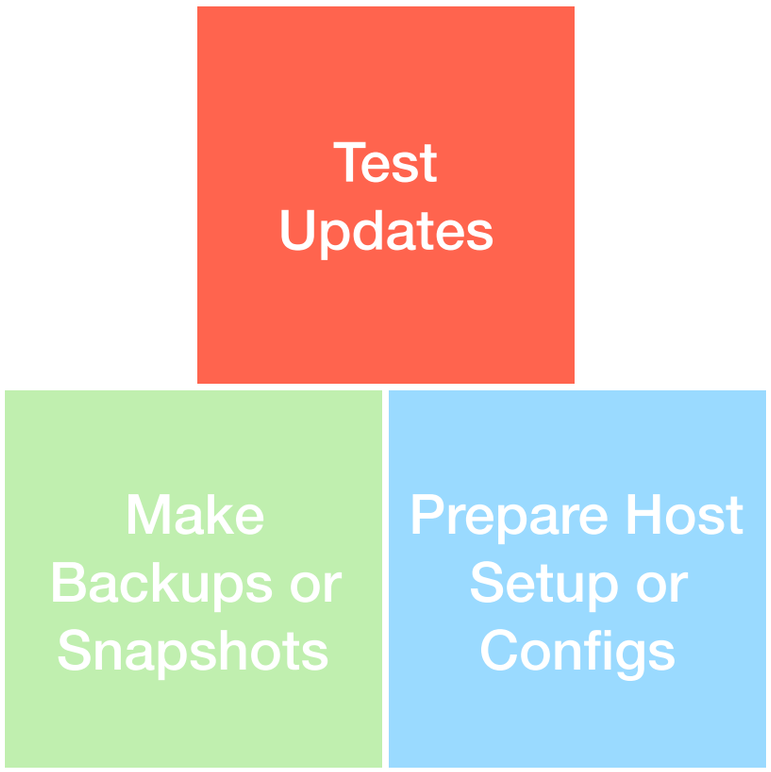
- Proactive search
- Update info spread out

- Prioritize by update type

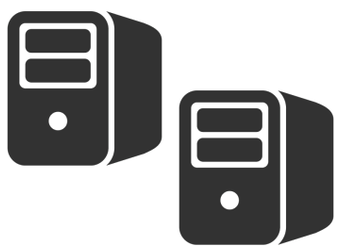
3. Preparing For Installation



3. Preparing For Installation

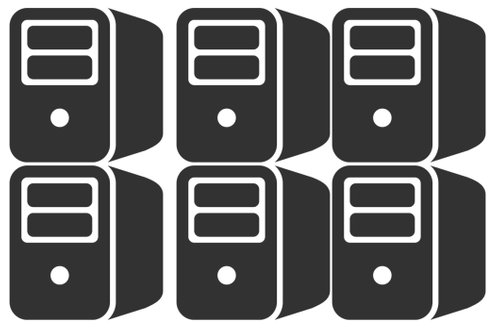


- No Testing (≈10% in survey)
- Dedicated Test Environment
  (1/3 in survey, 1/2 in interview)
- Staggered Deployment
  (1/2 in survey, 2/3 in interview)



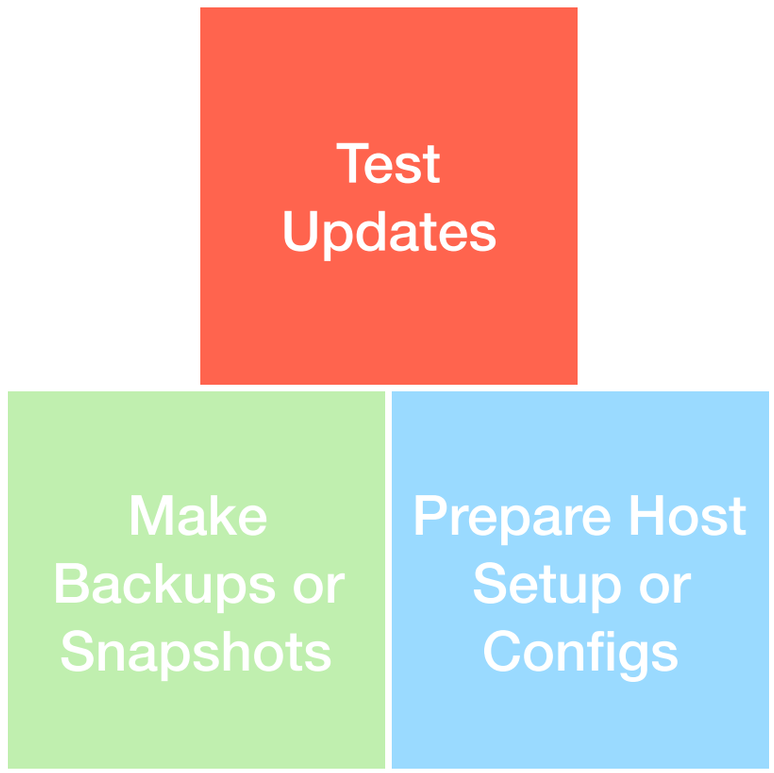
Admin Machines

Developer Machines

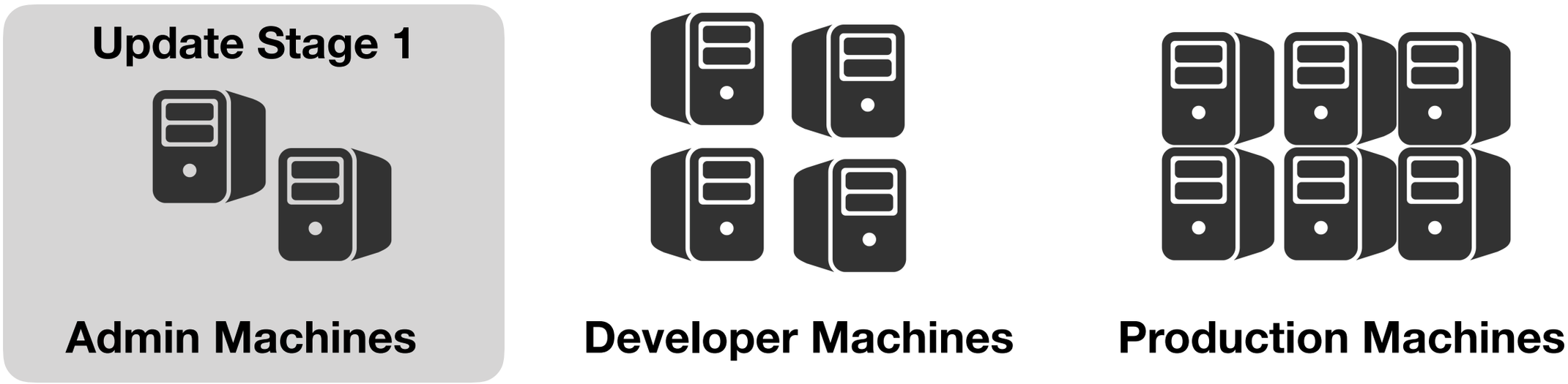


Production Machines

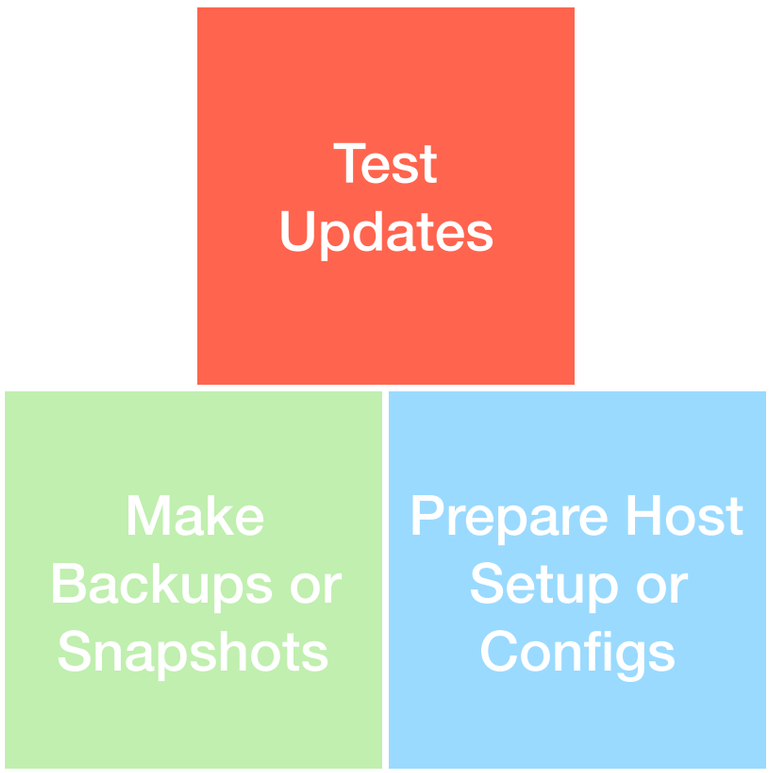
3. Preparing For Installation



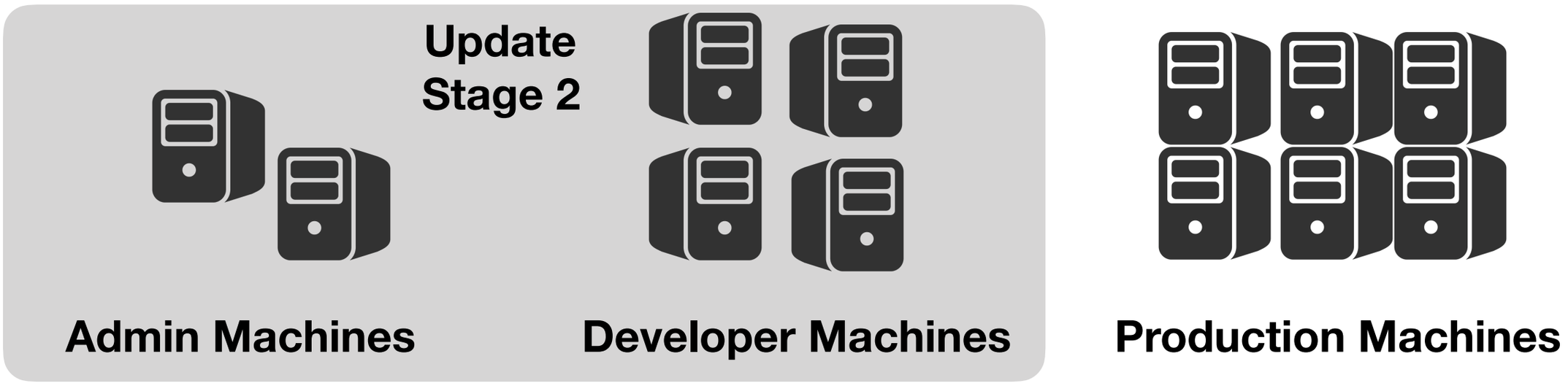
- No Testing (≈10% in survey)
- Dedicated Test Environment
  (1/3 in survey, 1/2 in interview)
- Staggered Deployment
  (1/2 in survey, 2/3 in interview)



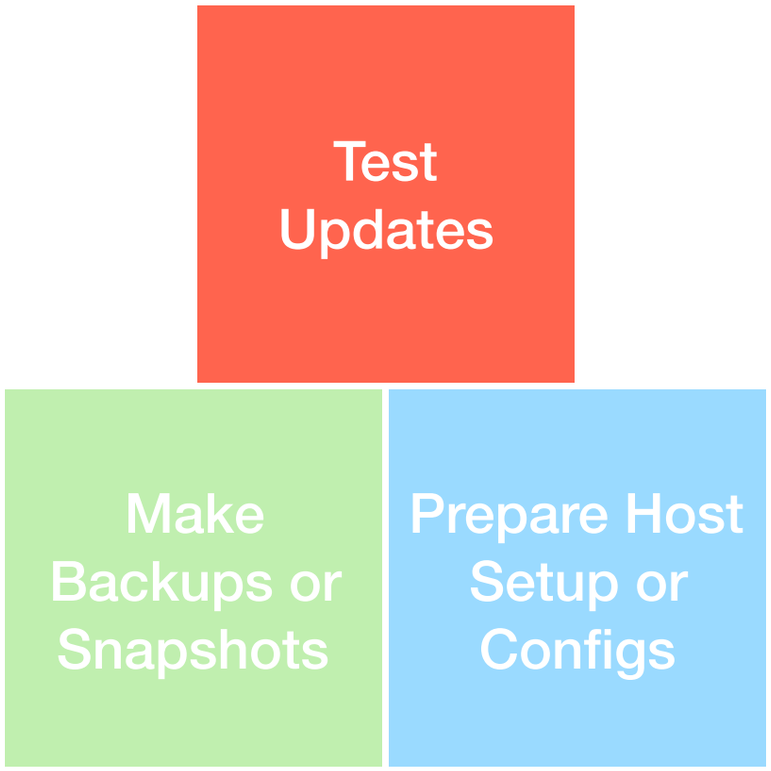
3. Preparing For Installation



- No Testing (≈10% in survey)
- Dedicated Test Environment
  (1/3 in survey, 1/2 in interview)
- Staggered Deployment
  (1/2 in survey, 2/3 in interview)



3. Preparing For Installation



- No Testing (≈10% in survey)
- Dedicated Test Environment
  (1/3 in survey, 1/2 in interview)
- Staggered Deployment
  (1/2 in survey, 2/3 in interview)

3. Preparing For Installation

- No Testing (≈10% in survey)

Test

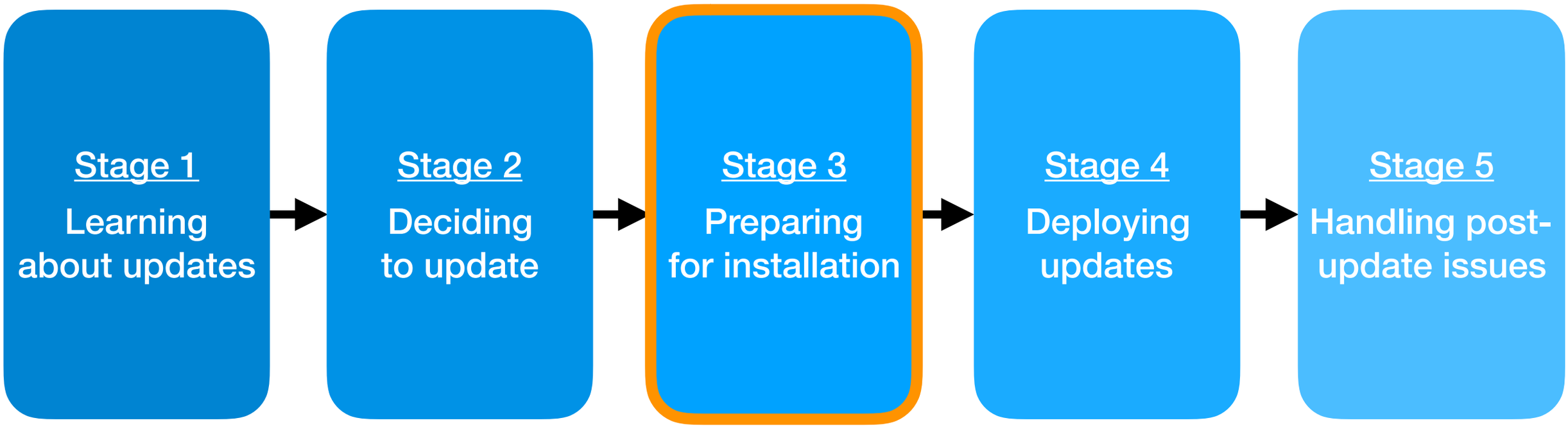
Dedi nt
(1/3 in

Stag
(1/2 in

Patch dev/test servers first. Let the systems run for a few weeks before patching production.

Install on non-important machines and let them bake for 1+ months.

Update Process Stages

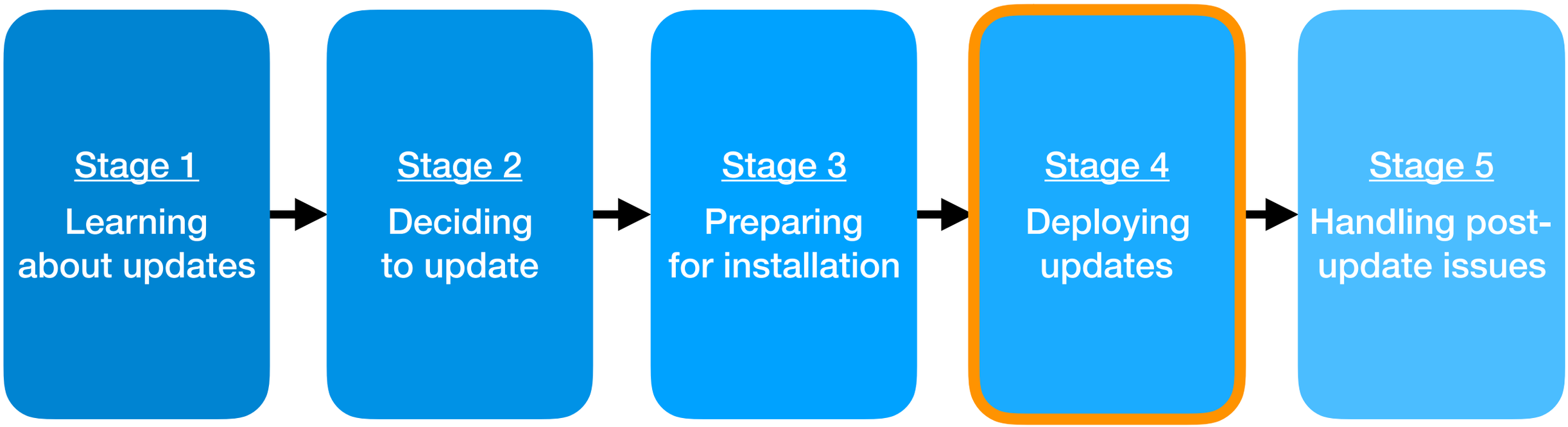


- Proactive search
- Update info spread out

- Prioritize by update type

- Widespread testing
- Testing can delay update

Update Process Stages

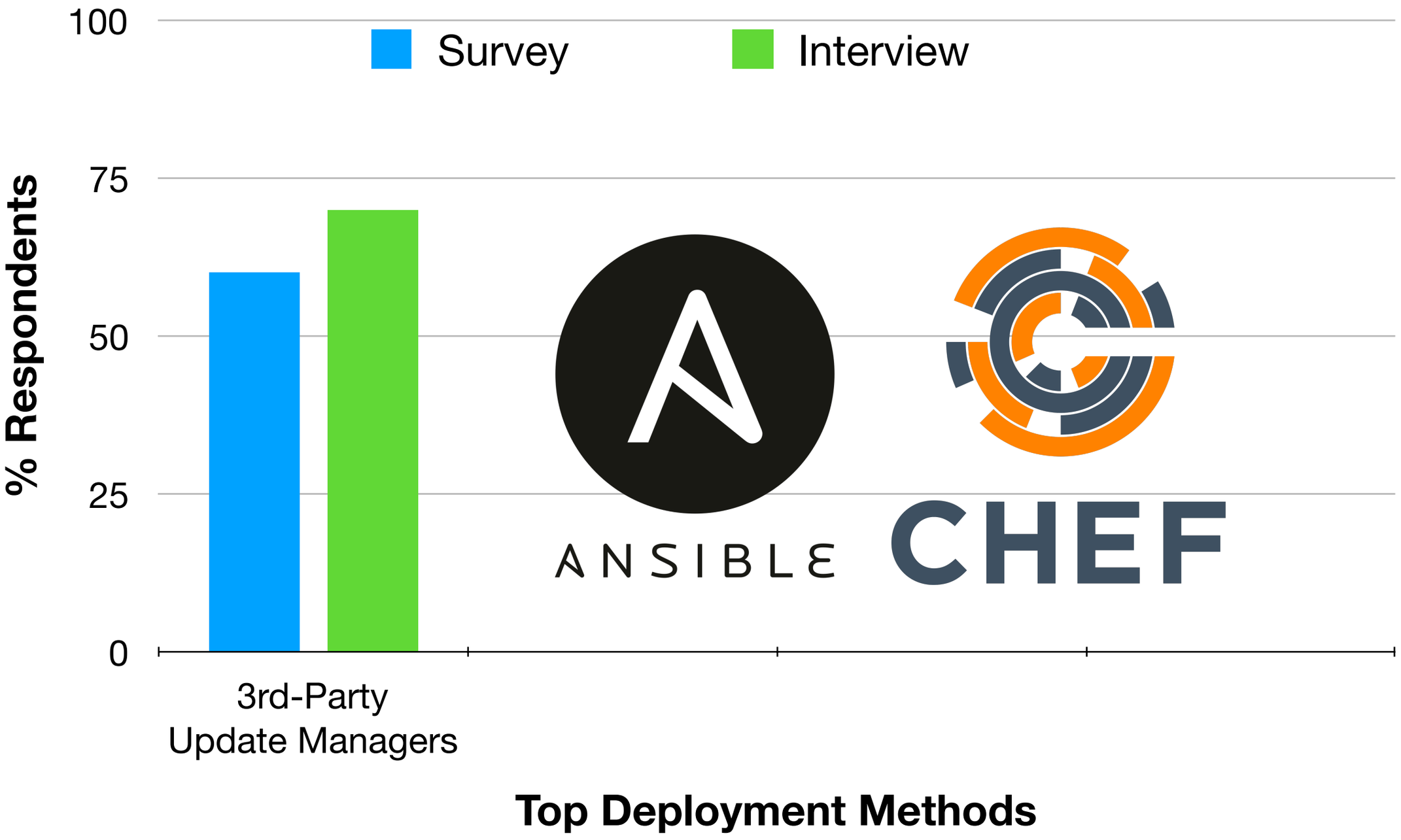


- Proactive search
- Update info spread out

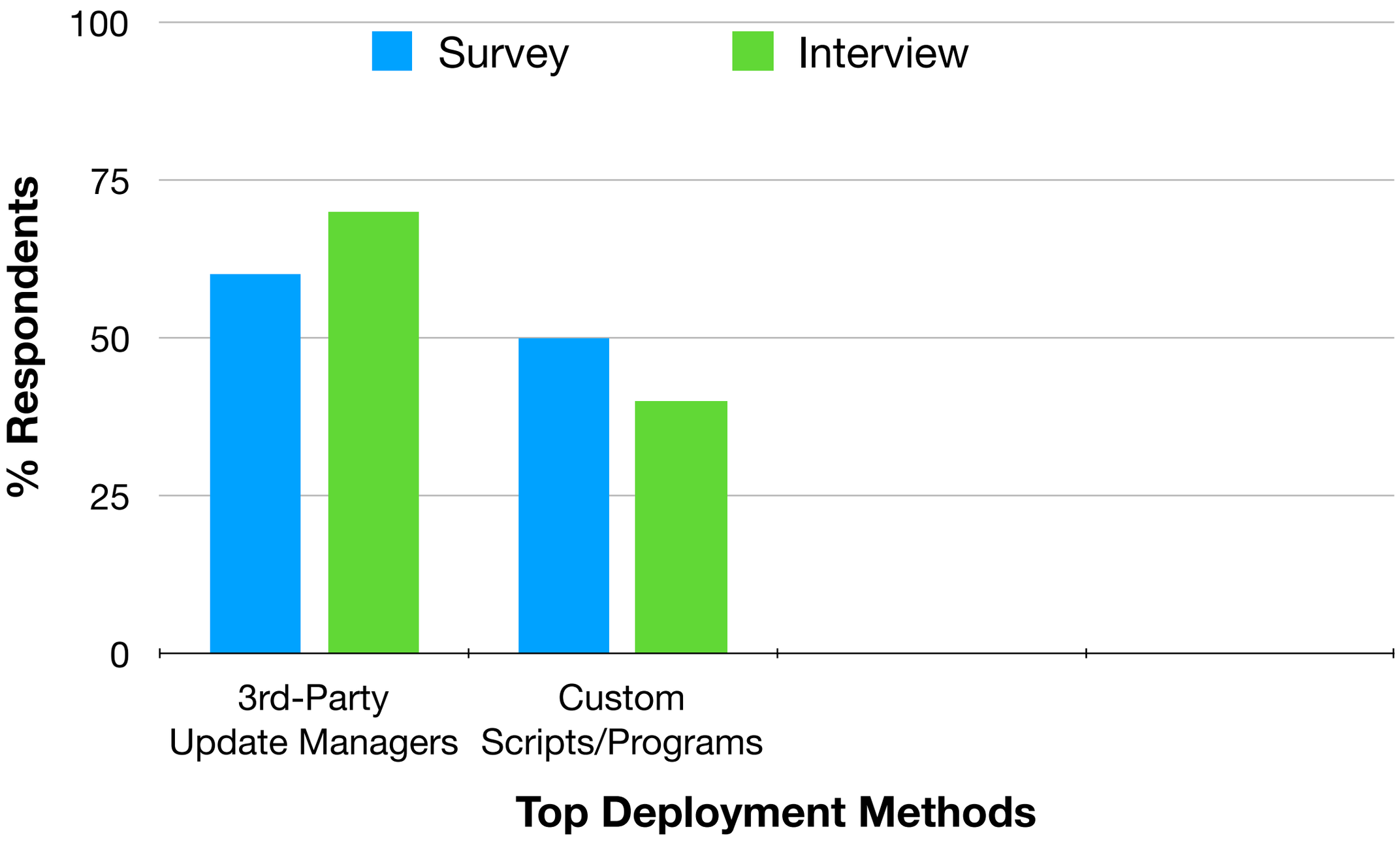
- Prioritize by update type

- Widespread testing
- Testing can delay update

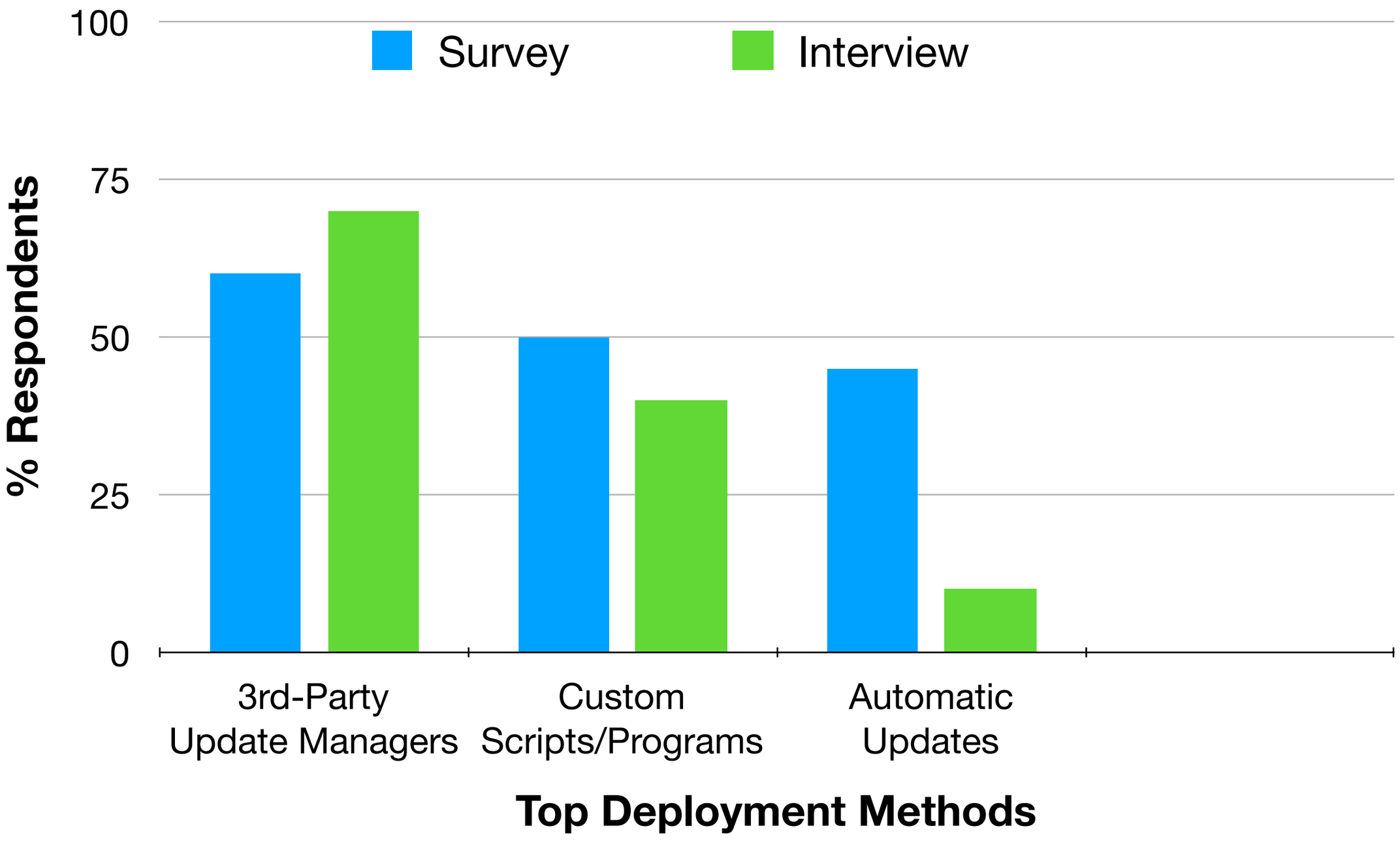
4. Deploying Updates



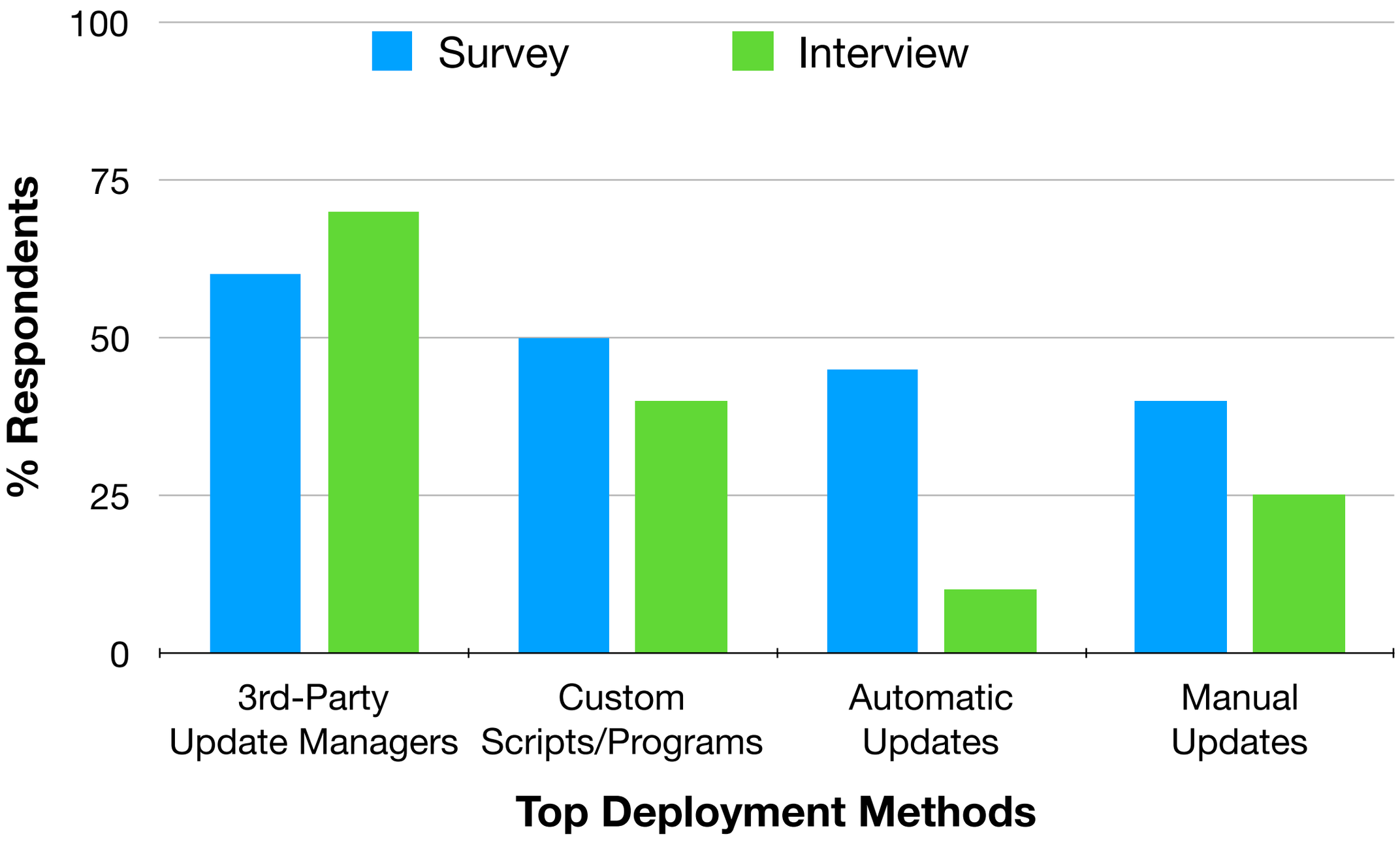
4. Deploying Updates



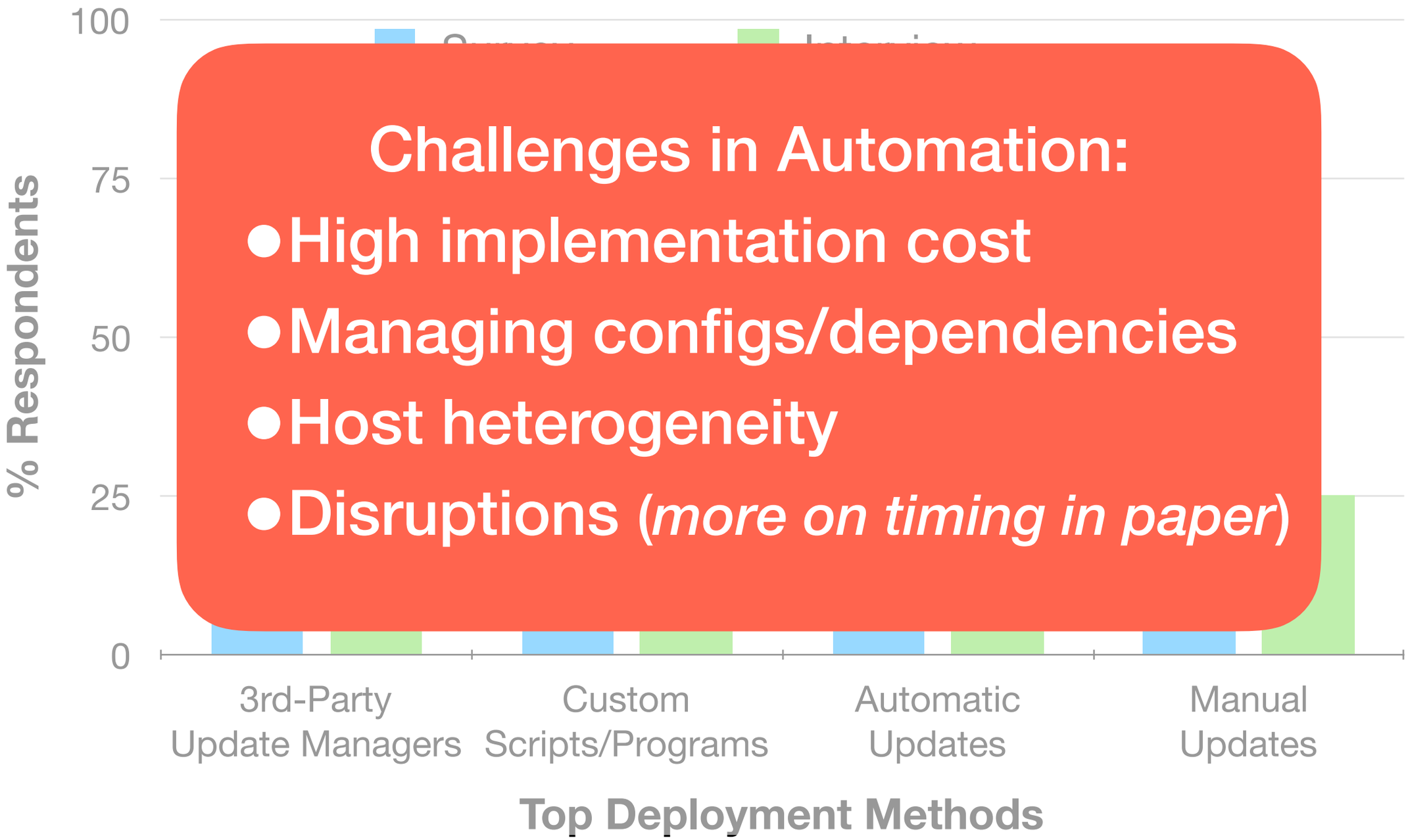
4. Deploying Updates



4. Deploying Updates



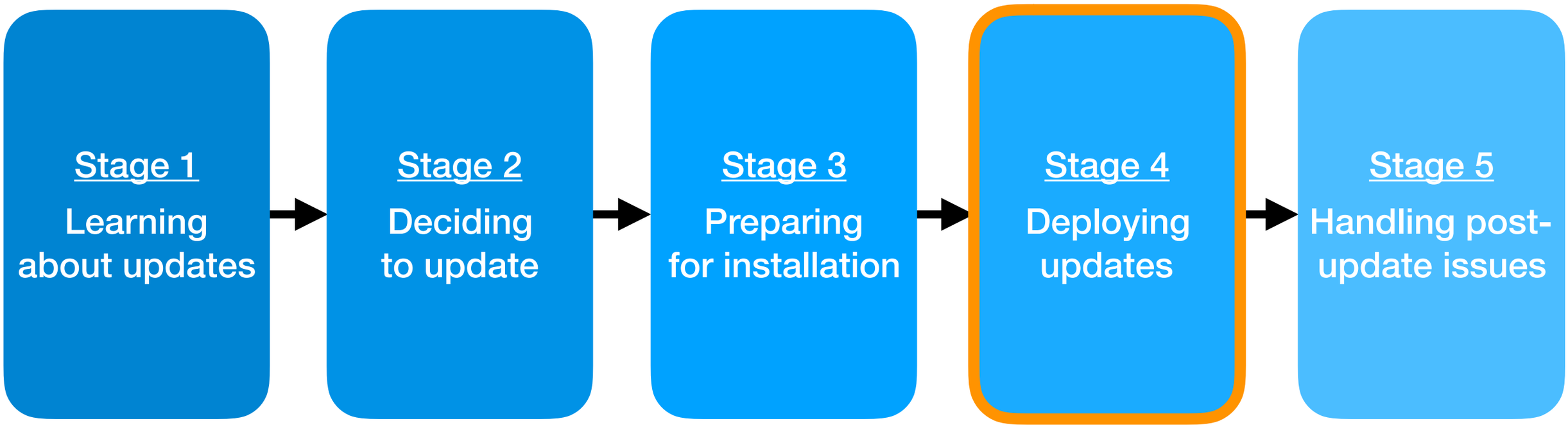
4. Deploying Updates



Challenges in Automation:

- High implementation cost
- Managing configs/dependencies
- Host heterogeneity
- Disruptions (*more on timing in paper*)

Update Process Stages



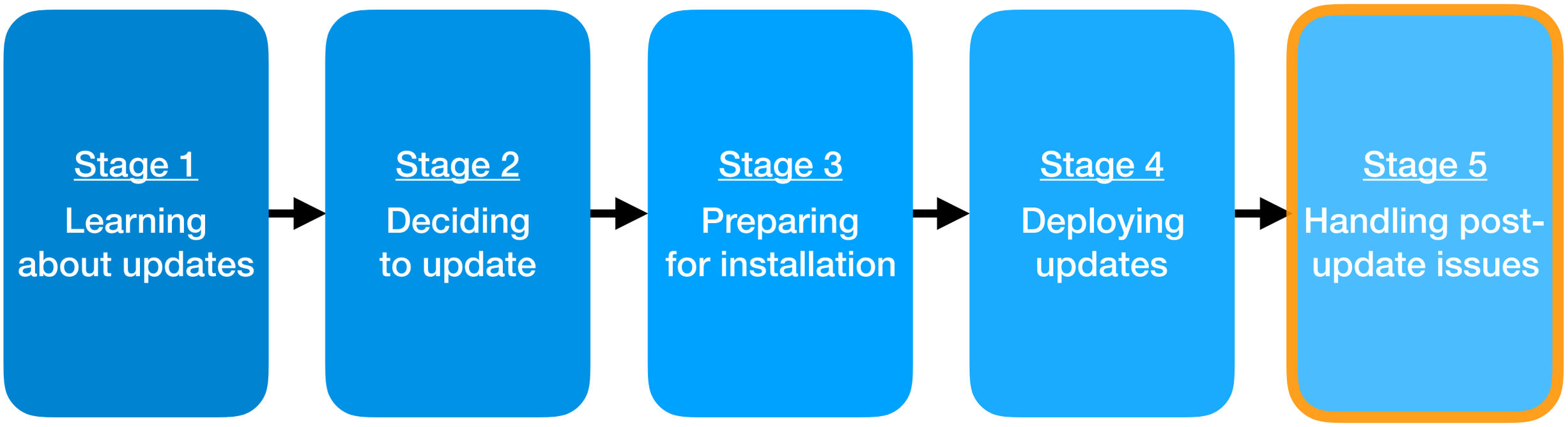
- Proactive search
- Update info spread out

- Prioritize by update type

- Widespread testing
- Testing can delay update

- Deploying + automation hard

Update Process Stages



- Proactive search
- Update info spread out

- Prioritize by update type

- Widespread testing
- Testing can delay update

- Deploying + automation hard

5. Handling Post-Update Issues

98% in survey have dealt with buggy updates.

I stopped applying updates because it was becoming more of a problem to apply them than not to. Production machines, they don't get updates.

5. Handling Post-Update Issues

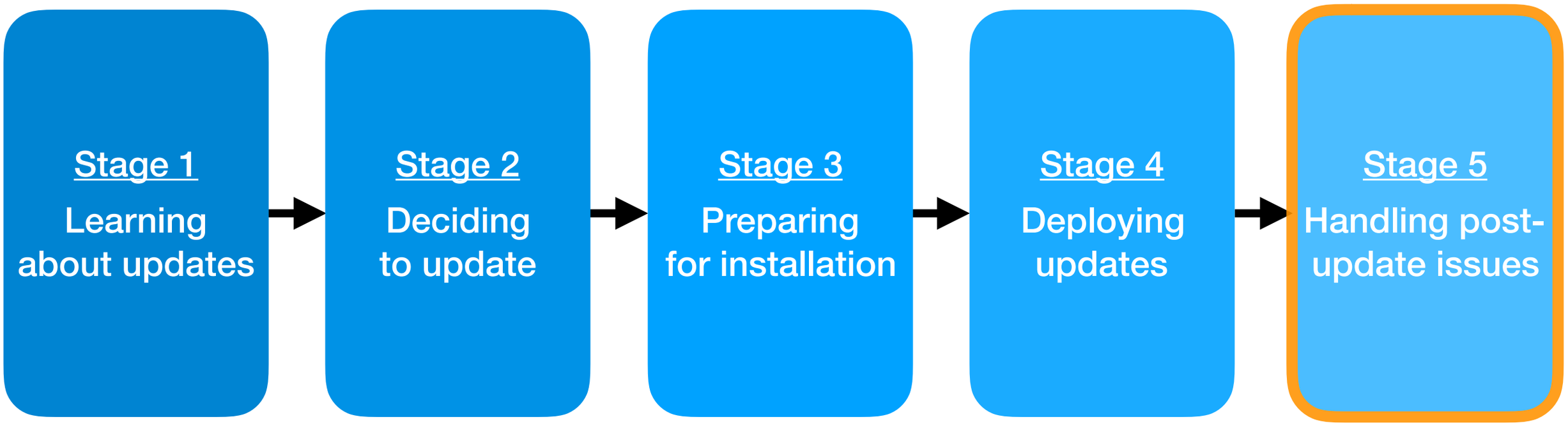
98% in survey have dealt with buggy updates.

I stopped applying updates because it was becoming more of a problem to apply them than not to. Production machines, they don't get updates.

Most rollback to snapshot or revert update.

5-15% try to work around update issues.

Update Process Stages



- Proactive search
- Update info spread out

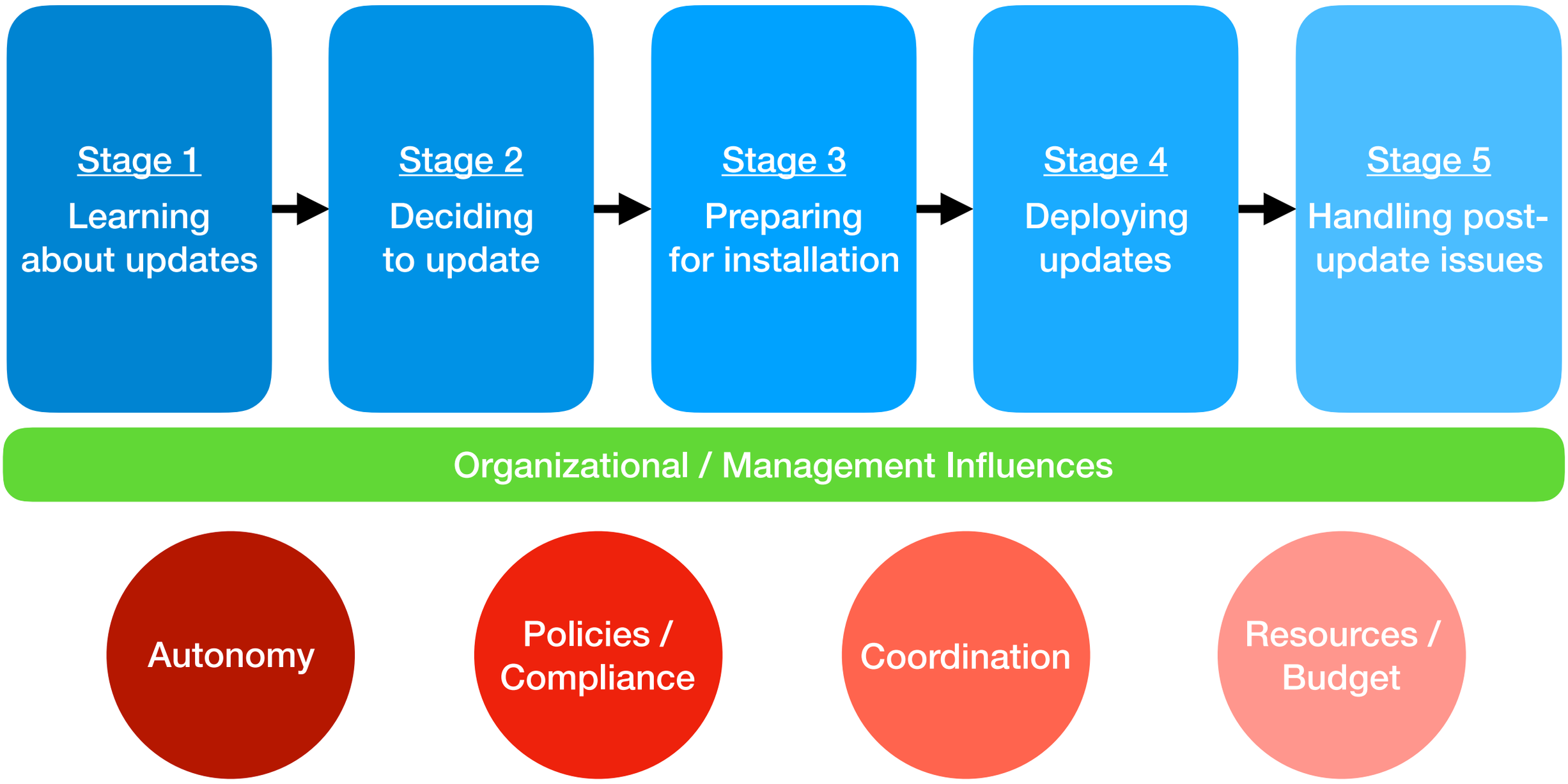
- Prioritize by update type

- Widespread testing
- Testing can delay update

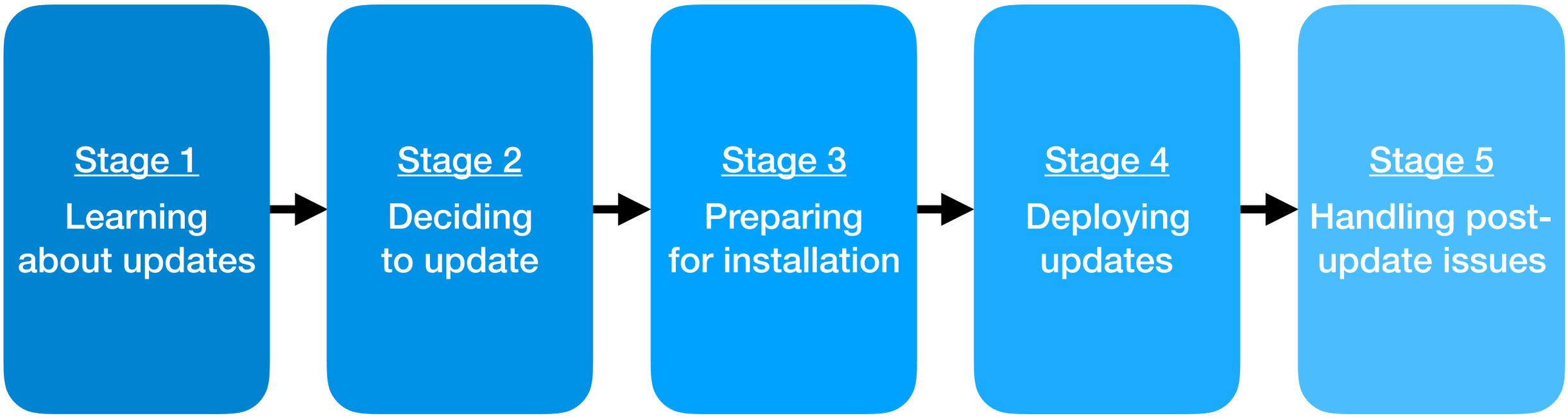
- Deploying + automation hard

- Most undo update, vulnerable

Update Process Stages



Where Next?


Stage 1
Learning about updates
Stage 2
Deciding to update
Stage 3
Preparing for installation
Stage 4
Deploying updates
Stage 5
Handling post-update issues
Organizational / Management Influences
• Proactive search
• Update info spread out
• Prioritize by update type
• Widespread testing
• Testing can delay update
• Deploying + automation hard
• Most undo update, vulnerable

Where Next?

Stage 1

Learning about updates

Improve information retrieval:

- Centralized source
- Outreach campaigns

Stage 4

eploying pdates

Stage 5

Handling post-update issues

Organizational / Management Influences

- Proactive search
- Update info spread out

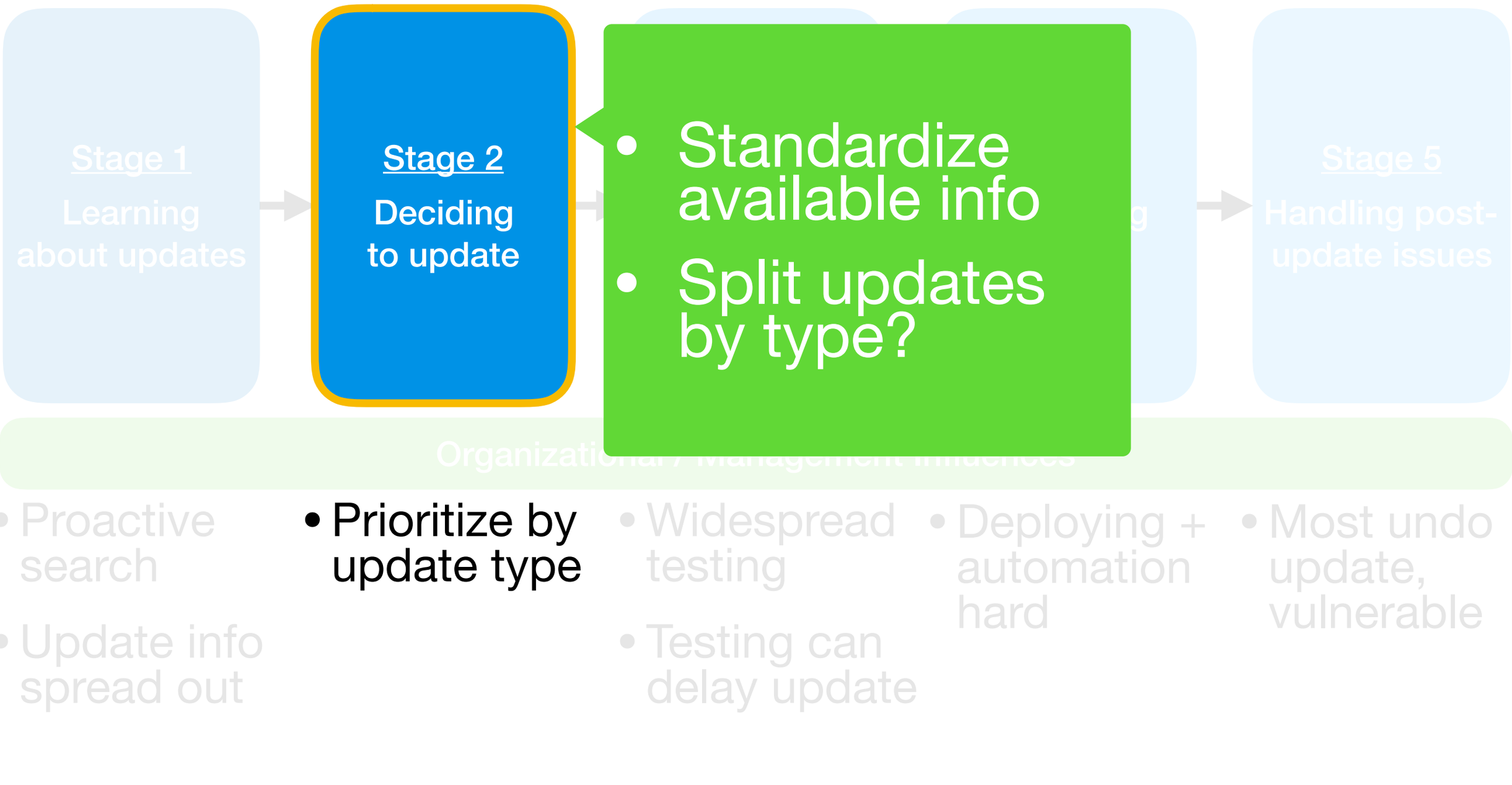
- Prioritize by update type

- Widespread testing
- Testing can delay update

- Deploying + automation hard

- Most undo update, vulnerable

Where Next?


Stage 1
Learning about updates
Stage 2
Deciding to update
Stage 5
Handling post-update issues
• Standardize available info
• Split updates by type?
Organizational / Management influences
• Proactive search
• Update info spread out
• Prioritize by update type
• Widespread testing
• Testing can delay update
• Deploying + automation hard
• Most undo update, vulnerable

Where Next?

Advance technical + usability aspects of update tools/ systems

Stage 3
Preparing for installation

Stage 4
Deploying updates

Stage 5
Handling post-update issues

Organizational / Management Influences

- Proactive search
- Update info spread out
- Prioritize by update type
- Widespread testing
- Testing can delay update
- Deploying + automation hard
- Most undo update, vulnerable

Where Next?

Evaluate organizational influences in depth

Organizational / Management Influences

Stage 1
Learning about updates

- Proactive search
- Update info spread out

Stage 5
Handling post-update issues

- Most undo update, vulnerable

Where Next?

Further investigate sys admins specifically 

Make information retrieval + processing easier:

- Centralized source
- Outreach campaigns
- Standardize available info
- Split update types (?)

Advance technical + usability aspects of update technology

Evaluate org influences

Thanks!

frankli@berkeley.edu
@frankli714